# Microsoft Security Intelligence Report

## *Global Threat Assessments for 117 countries/regions*

*An in-depth perspective on
software vulnerabilities and exploits,
malicious code threats, and
potentially unwanted software
in 2010. With new data covering
July through December*

## Microsoft Security Intelligence Report

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

## Authors

**Doug Cavit**
*Microsoft Trustworthy Computing*

**Joe Faulhaber**
*Microsoft Malware Protection Center*

**Vinny Gullotto**
*Microsoft Malware Protection Center*

**Jeff Jones**
*Microsoft Trustworthy Computing*

**Jimmy Kuo**
*Microsoft Malware Protection Center*

**Michelle Meyer**
*Microsoft Trustworthy Computing*

**Daryl Pecelj**
*Microsoft IT Information Security and Risk Management*

**Anthony Penta**
*Microsoft Windows Safety Platform*

**Tim Rains**
*Microsoft Trustworthy Computing*

**Javier Salido**
*Microsoft Trustworthy Computing*

**Christian Seifert**
*Bing*

**Frank Simorjay**
*Microsoft Trustworthy Computing*

**Holly Stewart**
*Microsoft Malware Protection Center*

**Matt Thomlinson**
*Microsoft Security Response Center*

**Jossie Tirado Arroyo**
*Microsoft IT Information Security and Risk Management*

**Scott Wu**
*Microsoft Malware Protection Center*

**Jeff Williams**
*Microsoft Malware Protection Center*

**Terry Zink**
*Microsoft Forefront Online Protection for Exchange*

## Contributors

**Lawren Ahuna**
*Microsoft IT Information Security and Risk Management*

**Eva Chow**
*Microsoft IT Information Security and Risk Management*

**Enrique Gonzalez**
*Microsoft Malware Protection Center*

**Cristin Goodwin**
*Microsoft Legal and Corporate Affairs*

**Satomi Hayakawa**
*CSS Japan Security Response Team*

**Yuhui Huang**
*Microsoft Malware Protection Center*

**CSS Japan Security Response Team**
*Microsoft Japan*

**John Lambert**
*Microsoft Security Engineering Center*

**Eric Leonard**
*Microsoft IT Information Security and Risk Management*

**Laura Lemire**
*Microsoft Legal and Corporate Affairs*

**Ken Malcolmson**
*Microsoft Trustworthy Computing*

**Charles McColgan**
*Microsoft ISD*

**Don Nguyen**
*Microsoft IT Information Security and Risk Management*

**Price Oden**
*Microsoft IT Information Security and Risk Management*

**Kathy Phillips**
*Microsoft Legal and Corporate Affairs*

**Hilda Larina Ragragio**
*Microsoft Malware Protection Center*

**Tareq Saade**
*Microsoft Malware Protection Center*

**Richard Saunders**
*Microsoft Trustworthy Computing*

**Marc Seinfeld**
*Microsoft Malware Protection Center*

**Jasmine Sesso**
*Microsoft Malware Protection Center*

**Norie Tamura (GOMI)**
*CSS Japan Security Response Team*

**Gilou Tenebro**
*Microsoft Malware Protection Center*

# About This Report

## Scope

The *Microsoft® Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, malicious and potentially unwanted software, and security breaches. Past reports and related resources are available for download at www.microsoft.com/sir. We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their organizations, software, and users.

## Reporting Period

In this volume of the *Microsoft Security Intelligence Report*, statistics about malware families and infections are reported on a quarterly basis and other statistics continue to be reported on a half-yearly basis, with a focus on 2010.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, respectively, where *yy* indicates the calendar year and n indicates the half or quarter. For example, 1H10 represents the first half of 2010 (January 1 through June 30), and 2Q10 represents the second quarter of 2010 (April 1 through June 30). To avoid confusion, please pay attention to the reporting period or periods being referenced when considering the statistics in this report.

## Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware and potentially unwanted software. For information about this standard, see “Microsoft Malware Protection Center Naming Standard” on the MMPC website.

## Contents

**About This Report** ..... 4
Scope ..... 4
Reporting Period ..... 4
Conventions ..... 4

Albania ..... 17
Infection Trends (CCM) ..... 18
Threat Categories ..... 19
Threat Families ..... 20

Algeria ..... 21
Infection Trends (CCM) ..... 22
Threat Categories ..... 23
Threat Families ..... 24

Angola ..... 25
Infection Trends (CCM) ..... 26
Threat Categories ..... 27
Threat Families ..... 28

Argentina ..... 29
Infection Trends (CCM) ..... 30
Threat Categories ..... 31
Threat Families ..... 32

Australia ..... 33
Infection Trends (CCM) ..... 34
Threat Categories ..... 35
Threat Families ..... 36

Austria ..... 37
Infection Trends (CCM) ..... 38
Threat Categories ..... 39
Threat Families ..... 40

Azerbaijan ..... 41
Infection Trends (CCM) ..... 42
Threat Categories ..... 43
Threat Families ..... 44

Bahamas ..... 45
Infection Trends (CCM) ..... 46
Threat Categories ..... 47
Threat Families ..... 48

Bahrain ..... 49
Infection Trends (CCM) ..... 50
Threat Categories ..... 51
Threat Families ..... 52

**Bangladesh** .......... **53**
- Infection Trends (CCM) .......... 54
- Threat Categories .......... 55
- Threat Families .......... 56

**Barbados** .......... **57**
- Infection Trends (CCM) .......... 58
- Threat Categories .......... 59
- Threat Families .......... 60

**Belarus** .......... **61**
- Infection Trends (CCM) .......... 62
- Threat Categories .......... 63
- Threat Families .......... 64

**Belgium** .......... **65**
- Infection Trends (CCM) .......... 66
- Threat Categories .......... 67
- Threat Families .......... 68

**Bolivia** .......... **69**
- Infection Trends (CCM) .......... 70
- Threat Categories .......... 71
- Threat Families .......... 72

**Bosnia and Herzegovina** .......... **73**
- Infection Trends (CCM) .......... 74
- Threat Categories .......... 75
- Threat Families .......... 76

**Brazil** .......... **77**
- Infection Trends (CCM) .......... 78
- Threat Categories .......... 79
- Threat Families .......... 80

**Brunei** .......... **81**
- Infection Trends (CCM) .......... 82
- Threat Categories .......... 83
- Threat Families .......... 84

**Bulgaria** .......... **85**
- Infection Trends (CCM) .......... 86
- Threat Categories .......... 87
- Threat Families .......... 88

**Cameroon** .......... **89**
- Infection Trends (CCM) .......... 90
- Threat Categories .......... 91
- Threat Families .......... 92

**Canada** .......... **93**
- Infection Trends (CCM) .......... 94
- Threat Categories .......... 95

Threat Families ........ 96

**Chile** ........ **97**
Infection Trends (CCM) ........ 98
Threat Categories ........ 99
Threat Families ........ 100

**China** ........ **101**
Infection Trends (CCM) ........ 102
Threat Categories ........ 103
Threat Families ........ 104

**Colombia** ........ **105**
Infection Trends (CCM) ........ 106
Threat Categories ........ 107
Threat Families ........ 108

**Costa Rica** ........ **109**
Infection Trends (CCM) ........ 110
Threat Categories ........ 111
Threat Families ........ 112

**Croatia** ........ **113**
Infection Trends (CCM) ........ 114
Threat Categories ........ 115
Threat Families ........ 116

**Cyprus** ........ **117**
Infection Trends (CCM) ........ 118
Threat Categories ........ 119
Threat Families ........ 120

**Czech Republic** ........ **121**
Infection Trends (CCM) ........ 122
Threat Categories ........ 123
Threat Families ........ 124

**Denmark** ........ **125**
Infection Trends (CCM) ........ 126
Threat Categories ........ 127
Threat Families ........ 128

**Dominican Republic** ........ **129**
Infection Trends (CCM) ........ 130
Threat Categories ........ 131
Threat Families ........ 132

**Ecuador** ........ **133**
Infection Trends (CCM) ........ 134
Threat Categories ........ 135
Threat Families ........ 136

**Egypt** ........ **137**

Infection Trends (CCM) .......... 138
Threat Categories .......... 139
Threat Families .......... 140

**El Salvador .......... 141**
Infection Trends (CCM) .......... 142
Threat Categories .......... 143
Threat Families .......... 144

**Estonia .......... 145**
Infection Trends (CCM) .......... 146
Threat Categories .......... 147
Threat Families .......... 148

**Finland .......... 149**
Infection Trends (CCM) .......... 150
Threat Categories .......... 151
Threat Families .......... 152

**France .......... 153**
Infection Trends (CCM) .......... 154
Threat Categories .......... 155
Threat Families .......... 156

**Georgia .......... 157**
Infection Trends (CCM) .......... 158
Threat Categories .......... 159
Threat Families .......... 160

**Germany .......... 161**
Infection Trends (CCM) .......... 162
Threat Categories .......... 163
Threat Families .......... 164

**Ghana .......... 165**
Infection Trends (CCM) .......... 166
Threat Categories .......... 167
Threat Families .......... 168

**Greece .......... 169**
Infection Trends (CCM) .......... 170
Threat Categories .......... 171
Threat Families .......... 172

**Guadeloupe .......... 173**
Infection Trends (CCM) .......... 174
Threat Categories .......... 175
Threat Families .......... 176

**Guatemala .......... 177**
Infection Trends (CCM) .......... 178
Threat Categories .......... 179
Threat Families .......... 180

**Honduras** .......... **181**
Infection Trends (CCM) .......... 182
Threat Categories .......... 183
Threat Families .......... 184

**Hong Kong** .......... **185**
Infection Trends (CCM) .......... 186
Threat Categories .......... 187
Threat Families .......... 188

**Hungary** .......... **189**
Infection Trends (CCM) .......... 190
Threat Categories .......... 191
Threat Families .......... 192

**Iceland** .......... **193**
Infection Trends (CCM) .......... 194
Threat Categories .......... 195
Threat Families .......... 196

**India** .......... **197**
Infection Trends (CCM) .......... 198
Threat Categories .......... 199
Threat Families .......... 200

**Indonesia** .......... **201**
Infection Trends (CCM) .......... 202
Threat Categories .......... 203
Threat Families .......... 204

**Iraq** .......... **205**
Infection Trends (CCM) .......... 206
Threat Categories .......... 207
Threat Families .......... 208

**Ireland** .......... **209**
Infection Trends (CCM) .......... 210
Threat Categories .......... 211
Threat Families .......... 212

**Israel** .......... **213**
Infection Trends (CCM) .......... 214
Threat Categories .......... 215
Threat Families .......... 216

**Italy** .......... **217**
Infection Trends (CCM) .......... 218
Threat Categories .......... 219
Threat Families .......... 220

**Jamaica** .......... **221**
Infection Trends (CCM) .......... 222
Threat Categories .......... 223

Threat Families ... 224

**Japan** ... **225**
Infection Trends (CCM) ... 226
Threat Categories ... 227
Threat Families ... 228

**Jordan** ... **229**
Infection Trends (CCM) ... 230
Threat Categories ... 231
Threat Families ... 232

**Kazakhstan** ... **233**
Infection Trends (CCM) ... 234
Threat Categories ... 235
Threat Families ... 236

**Kenya** ... **237**
Infection Trends (CCM) ... 238
Threat Categories ... 239
Threat Families ... 240

**Korea** ... **241**
Infection Trends (CCM) ... 242
Threat Categories ... 243
Threat Families ... 244

**Kuwait** ... **245**
Infection Trends (CCM) ... 246
Threat Categories ... 247
Threat Families ... 248

**Latvia** ... **249**
Infection Trends (CCM) ... 250
Threat Categories ... 251
Threat Families ... 252

**Lebanon** ... **253**
Infection Trends (CCM) ... 254
Threat Categories ... 255
Threat Families ... 256

**Libya** ... **257**
Infection Trends (CCM) ... 258
Threat Categories ... 259
Threat Families ... 260

**Lithuania** ... **261**
Infection Trends (CCM) ... 262
Threat Categories ... 263
Threat Families ... 264

**Luxembourg** ... **265**

Infection Trends (CCM) ........ 266
Threat Categories ........ 267
Threat Families ........ 268

Macao S.A.R. ........ 269
Infection Trends (CCM) ........ 270
Threat Categories ........ 271
Threat Families ........ 272

Malaysia ........ 273
Infection Trends (CCM) ........ 274
Threat Categories ........ 275
Threat Families ........ 276

Malta ........ 277
Infection Trends (CCM) ........ 278
Threat Categories ........ 279
Threat Families ........ 280

Martinique ........ 281
Infection Trends (CCM) ........ 282
Threat Categories ........ 283
Threat Families ........ 284

Mauritius ........ 285
Infection Trends (CCM) ........ 286
Threat Categories ........ 287
Threat Families ........ 288

Mexico ........ 289
Infection Trends (CCM) ........ 290
Threat Categories ........ 291
Threat Families ........ 292

Moldova ........ 293
Infection Trends (CCM) ........ 294
Threat Categories ........ 295
Threat Families ........ 296

Mongolia ........ 297
Infection Trends (CCM) ........ 298
Threat Categories ........ 299
Threat Families ........ 300

Morocco ........ 301
Infection Trends (CCM) ........ 302
Threat Categories ........ 303
Threat Families ........ 304

Nepal ........ 305
Infection Trends (CCM) ........ 306
Threat Categories ........ 307
Threat Families ........ 308

Netherlands ........ 309
Infection Trends (CCM) ........ 310
Threat Categories ........ 311
Threat Families ........ 312

Netherlands Antilles ........ 313
Infection Trends (CCM) ........ 314
Threat Categories ........ 315
Threat Families ........ 316

New Zealand ........ 317
Infection Trends (CCM) ........ 318
Threat Categories ........ 319
Threat Families ........ 320

Nicaragua ........ 321
Infection Trends (CCM) ........ 322
Threat Categories ........ 323
Threat Families ........ 324

Nigeria ........ 325
Infection Trends (CCM) ........ 326
Threat Categories ........ 327
Threat Families ........ 328

Norway ........ 329
Infection Trends (CCM) ........ 330
Threat Categories ........ 331
Threat Families ........ 332

Oman ........ 333
Infection Trends (CCM) ........ 334
Threat Categories ........ 335
Threat Families ........ 336

Pakistan ........ 337
Infection Trends (CCM) ........ 338
Threat Categories ........ 339
Threat Families ........ 340

Palestinian Authority ........ 341
Infection Trends (CCM) ........ 342
Threat Categories ........ 343
Threat Families ........ 344

Panama ........ 345
Infection Trends (CCM) ........ 346
Threat Categories ........ 347
Threat Families ........ 348

Paraguay ........ 349
Infection Trends (CCM) ........ 350
Threat Categories ........ 351

Threat Families ........................................ 352

Peru ........................................ 353
Infection Trends (CCM) ........................................ 354
Threat Categories ........................................ 355
Threat Families ........................................ 356

Philippines ........................................ 357
Infection Trends (CCM) ........................................ 358
Threat Categories ........................................ 359
Threat Families ........................................ 360

Poland ........................................ 361
Infection Trends (CCM) ........................................ 362
Threat Categories ........................................ 363
Threat Families ........................................ 364

Portugal ........................................ 365
Infection Trends (CCM) ........................................ 366
Threat Categories ........................................ 367
Threat Families ........................................ 368

Puerto Rico ........................................ 369
Infection Trends (CCM) ........................................ 370
Threat Categories ........................................ 371
Threat Families ........................................ 372

Qatar ........................................ 373
Infection Trends (CCM) ........................................ 374
Threat Categories ........................................ 375
Threat Families ........................................ 376

Romania ........................................ 377
Infection Trends (CCM) ........................................ 378
Threat Categories ........................................ 379
Threat Families ........................................ 380

Russia ........................................ 381
Infection Trends (CCM) ........................................ 382
Threat Categories ........................................ 383
Threat Families ........................................ 384

Saudi Arabia ........................................ 385
Infection Trends (CCM) ........................................ 386
Threat Categories ........................................ 387
Threat Families ........................................ 388

Senegal ........................................ 389
Infection Trends (CCM) ........................................ 390
Threat Categories ........................................ 391
Threat Families ........................................ 392

Singapore ........................................ 393

Infection Trends (CCM) ... 394
Threat Categories ... 395
Threat Families ... 396

Slovakia ... 397
Infection Trends (CCM) ... 398
Threat Categories ... 399
Threat Families ... 400

Slovenia ... 401
Infection Trends (CCM) ... 402
Threat Categories ... 403
Threat Families ... 404

South Africa ... 405
Infection Trends (CCM) ... 406
Threat Categories ... 407
Threat Families ... 408

Spain ... 409
Infection Trends (CCM) ... 410
Threat Categories ... 411
Threat Families ... 412

Sri Lanka ... 413
Infection Trends (CCM) ... 414
Threat Categories ... 415
Threat Families ... 416

Sweden ... 417
Infection Trends (CCM) ... 418
Threat Categories ... 419
Threat Families ... 420

Switzerland ... 421
Infection Trends (CCM) ... 422
Threat Categories ... 423
Threat Families ... 424

Syria ... 425
Infection Trends (CCM) ... 426
Threat Categories ... 427
Threat Families ... 428

Taiwan ... 429
Infection Trends (CCM) ... 430
Threat Categories ... 431
Threat Families ... 432

Tanzania ... 433
Infection Trends (CCM) ... 434
Threat Categories ... 435
Threat Families ... 436

**Thailand** .... 437
Infection Trends (CCM) .... 438
Threat Categories .... 439
Threat Families .... 440

**Trinidad and Tobago** .... 441
Infection Trends (CCM) .... 442
Threat Categories .... 443
Threat Families .... 444

**Tunisia** .... 445
Infection Trends (CCM) .... 446
Threat Categories .... 447
Threat Families .... 448

**Turkey** .... 449
Infection Trends (CCM) .... 450
Threat Categories .... 451
Threat Families .... 452

**Uganda** .... 453
Infection Trends (CCM) .... 454
Threat Categories .... 455
Threat Families .... 456

**Ukraine** .... 457
Infection Trends (CCM) .... 458
Threat Categories .... 459
Threat Families .... 460

**United Arab Emirates** .... 461
Infection Trends (CCM) .... 462
Threat Categories .... 463
Threat Families .... 464

**United Kingdom** .... 465
Infection Trends (CCM) .... 466
Threat Categories .... 467
Threat Families .... 468

**United States** .... 469
Infection Trends (CCM) .... 470
Threat Categories .... 471
Threat Families .... 472

**Uruguay** .... 473
Infection Trends (CCM) .... 474
Threat Categories .... 475
Threat Families .... 476

**Venezuela** .... 477
Infection Trends (CCM) .... 478
Threat Categories .... 479

Threat Families ... 480

**Vietnam** ... **481**

Infection Trends (CCM) ... 482

Threat Categories ... 483

Threat Families ... 484

# Albania

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

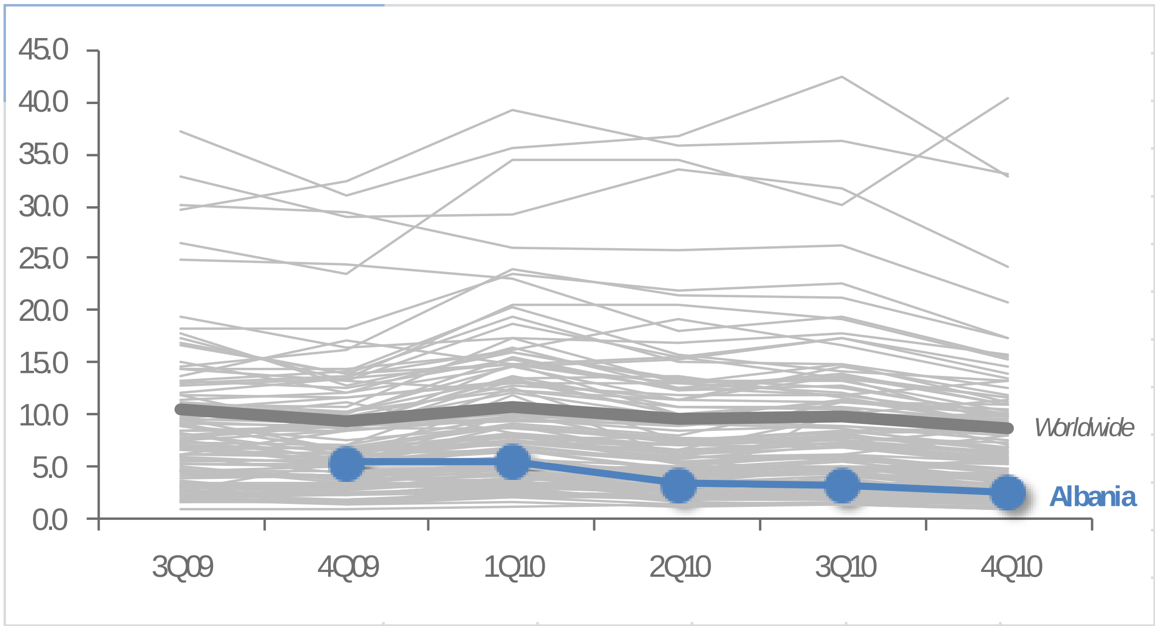
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Albania in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Albania and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 5.6 | 3.3 | 3.1 | 2.6 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.20 | | | |
| Malware hosting sites per 1000 hosts | 3.25 | | 7.48 | |
| Percentage of sites hosting drive-by downloads | 0.094% | | | |

## Infection Trends (CCM)

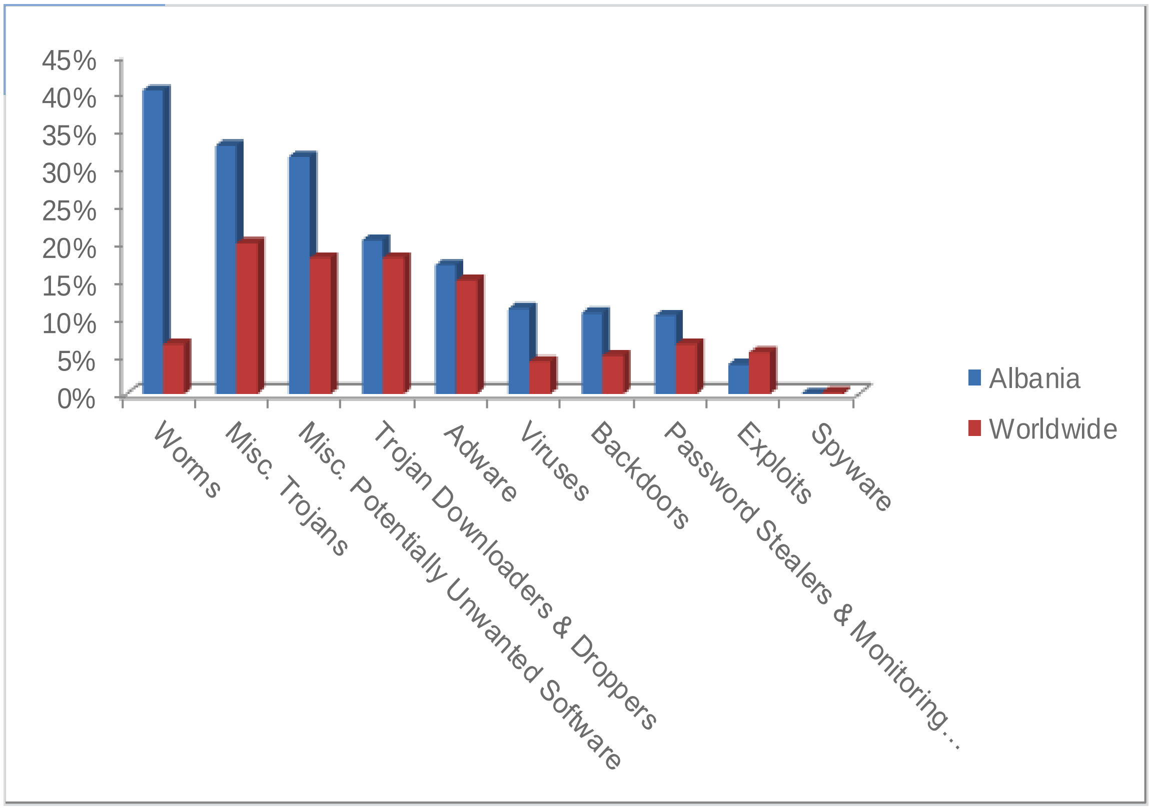
The MSRT detected malware on 2.6 of every 1,000 computers scanned in Albania in 4Q10 (a CCM score of 2.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Albania over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Albania and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Albania in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Albania in 4Q10 was Worms, which affected 40.3 percent of all cleaned computers, down from 45.3 percent in 3Q10.
- The second most common category in Albania in 4Q10 was Misc. Trojans, which affected 32.9 percent of all cleaned computers, up from 29.6 percent in 3Q10.
- The third most common category in Albania in 4Q10 was Misc. Potentially Unwanted Software, which affected 31.5 percent of all cleaned computers, up from 27.8 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Albania in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 21.1% |
| 2 | Win32/Rimecud | 18.2% |
| 3 | Win32/Sality | 11.1% |
| 4 | Win32/Taterf | 10.5% |
| 5 | Helompy | 10.3% |
| 6 | JS/Pornpop | 7.5% |
| 7 | Win32/Vobfus | 7.4% |
| 8 | Win32/Conficker | 7.0% |
| 9 | Win32/Renos | 7.0% |
| 10 | Win32/Frethog | 5.7% |

- The most common threat family in Albania in 4Q10 was Win32/Autorun, which affected 21.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Albania in 4Q10 was Win32/Rimecud, which affected 18.2 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Albania in 4Q10 was Win32/Sality, which affected 11.1 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Albania in 4Q10 was Win32/Taterf, which affected 10.5 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Algeria

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

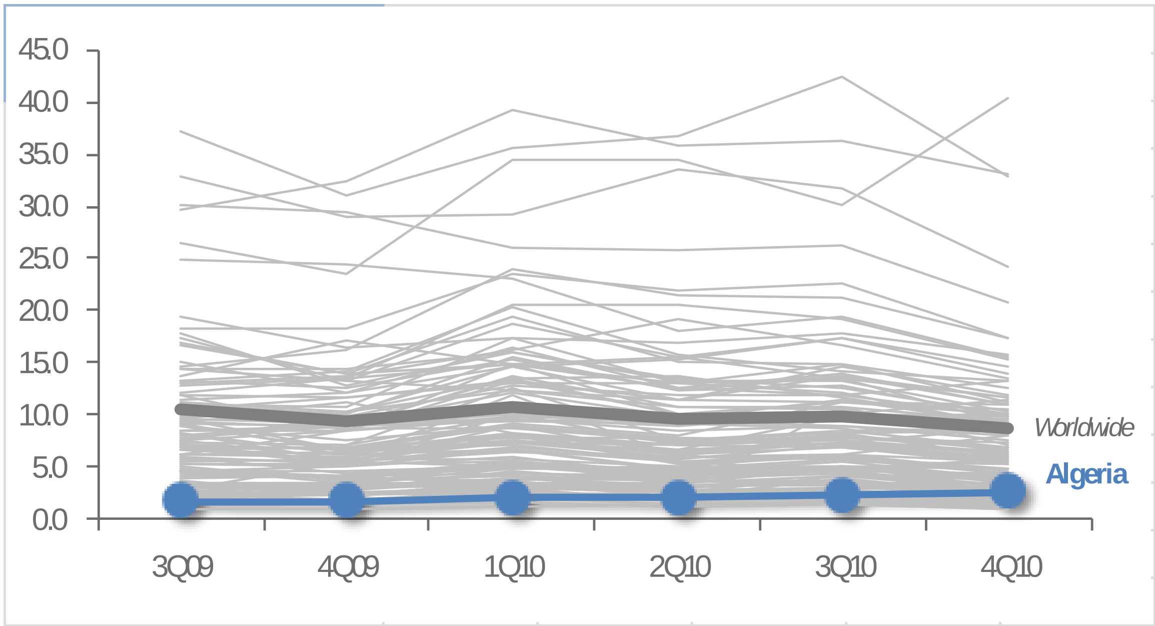
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Algeria in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Algeria and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">2.2</td><td colspan="3">2.1</td><td colspan="3">2.4</td><td colspan="3">2.7</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">29.35</td><td colspan="6">2.10</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">119.50</td><td colspan="6"></td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.305%</td><td colspan="4">0.281%</td><td colspan="4">0.195%</td></tr>
</table>

## Infection Trends (CCM)

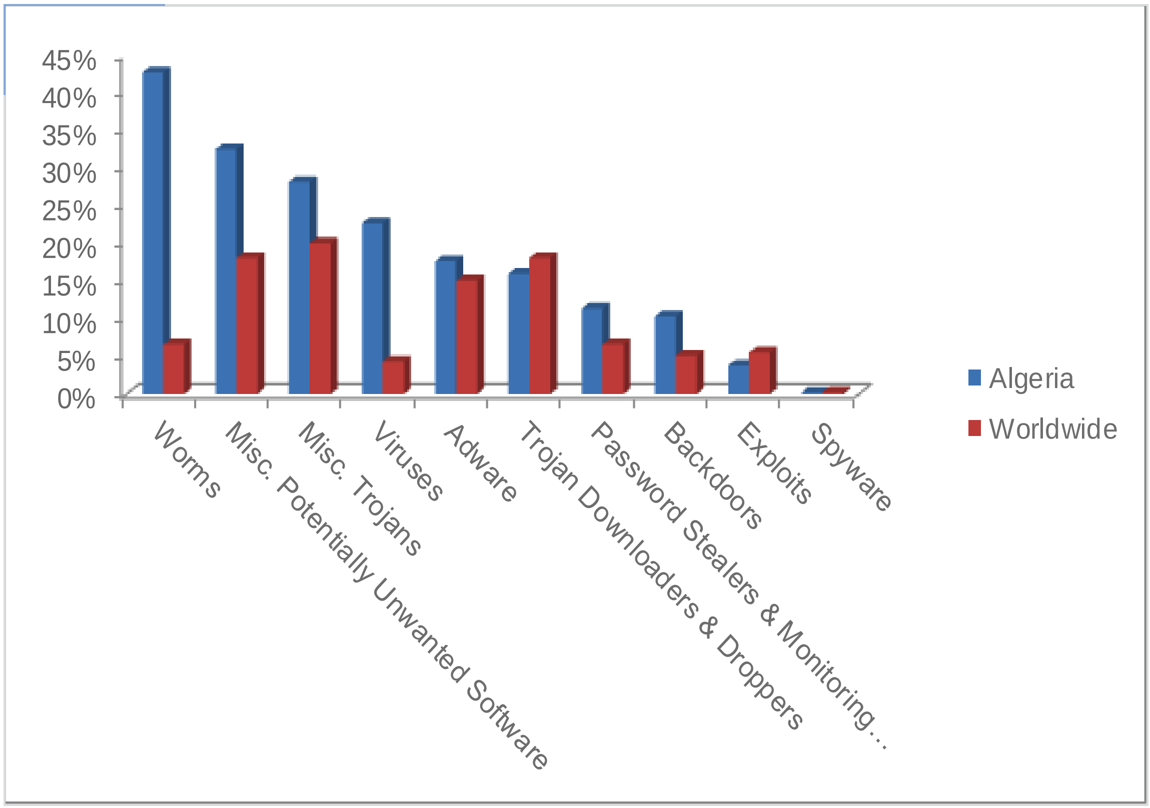
The MSRT detected malware on 2.7 of every 1,000 computers scanned in Algeria in 4Q10 (a CCM score of 2.7, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Algeria over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Algeria and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Algeria in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Algeria in 4Q10 was Worms, which affected 42.7 percent of all cleaned computers, up from 41.3 percent in 3Q10.
- The second most common category in Algeria in 4Q10 was Misc. Potentially Unwanted Software, which affected 32.5 percent of all cleaned computers, up from 28.0 percent in 3Q10.
- The third most common category in Algeria in 4Q10 was Misc. Trojans, which affected 28.1 percent of all cleaned computers, up from 25.8 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Algeria in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---:|
| 1 | Win32/Autorun | 20.7% |
| 2 | Win32/Sality | 19.3% |
| 3 | Win32/Taterf | 11.6% |
| 4 | Win32/Vobfus | 9.2% |
| 5 | Win32/Conficker | 8.0% |
| 6 | Win32/Frethog | 7.8% |
| 7 | JS/Pornpop | 7.3% |
| 8 | Win32/Rimecud | 7.3% |
| 9 | Win32/Mabezat | 6.7% |
| 10 | Win32/Zwangi | 6.2% |

- The most common threat family in Algeria in 4Q10 was Win32/Autorun, which affected 20.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

- The second most common threat family in Algeria in 4Q10 was Win32/Sality, which affected 19.3 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

- The third most common threat family in Algeria in 4Q10 was Win32/Taterf, which affected 11.6 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

- The fourth most common threat family in Algeria in 4Q10 was Win32/Vobfus, which affected 9.2 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

# Angola

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

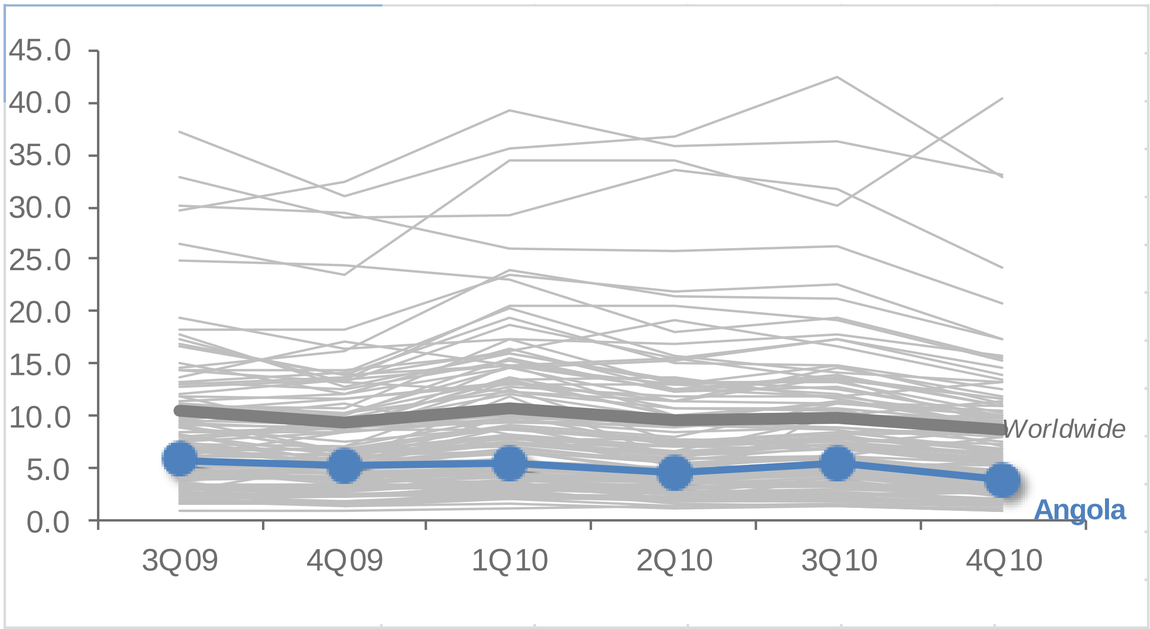
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Angola in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Angola and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 5.4 | 4.6 | 5.5 | 3.9 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | | | | |
| Malware hosting sites per 1000 hosts | 0.84 | | | |
| Percentage of sites hosting drive-by downloads | 0.154% | 0.201% | | |

## Infection Trends (CCM)

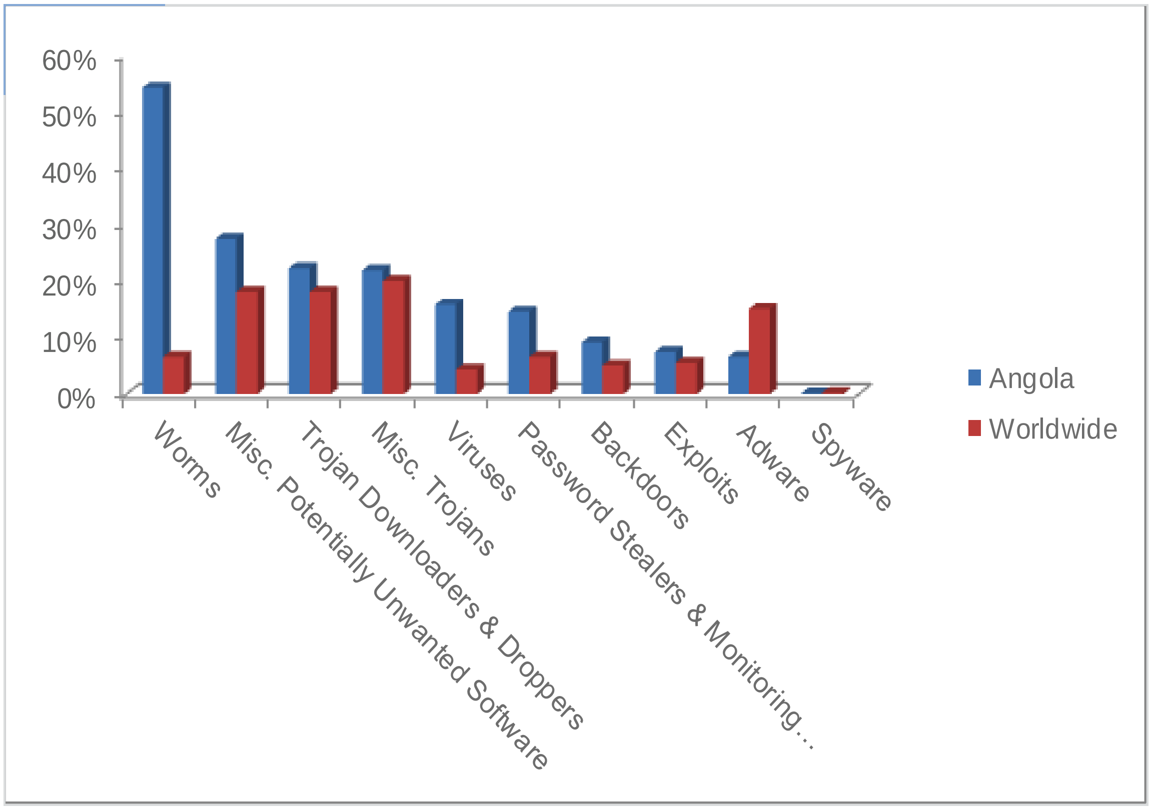
The MSRT detected malware on 3.9 of every 1,000 computers scanned in Angola in 4Q10 (a CCM score of 3.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Angola over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Angola and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Angola in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Angola in 4Q10 was Worms, which affected 54.2 percent of all cleaned computers, down from 54.9 percent in 3Q10.
- The second most common category in Angola in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.5 percent of all cleaned computers, up from 22.2 percent in 3Q10.
- The third most common category in Angola in 4Q10 was Trojan Downloaders & Droppers, which affected 22.3 percent of all cleaned computers, up from 20.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Angola in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Vobfus | 30.1% |
| 2 | Win32/Autorun | 21.7% |
| 3 | Win32/Rimecud | 10.4% |
| 4 | Win32/Virut | 8.7% |
| 5 | Win32/Renos | 7.4% |
| 6 | Win32/Banload | 7.2% |
| 7 | Helompy | 6.5% |
| 8 | Win32/Bancos | 6.2% |
| 9 | Win32/Conficker | 6.2% |
| 10 | Win32/Chir | 6.1% |

- The most common threat family in Angola in 4Q10 was Win32/Vobfus, which affected 30.1 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The second most common threat family in Angola in 4Q10 was Win32/Autorun, which affected 21.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Angola in 4Q10 was Win32/Rimecud, which affected 10.4 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Angola in 4Q10 was Win32/Virut, which affected 8.7 percent of cleaned computers. Win32/Virut is a family of file-infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server.

# Argentina

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

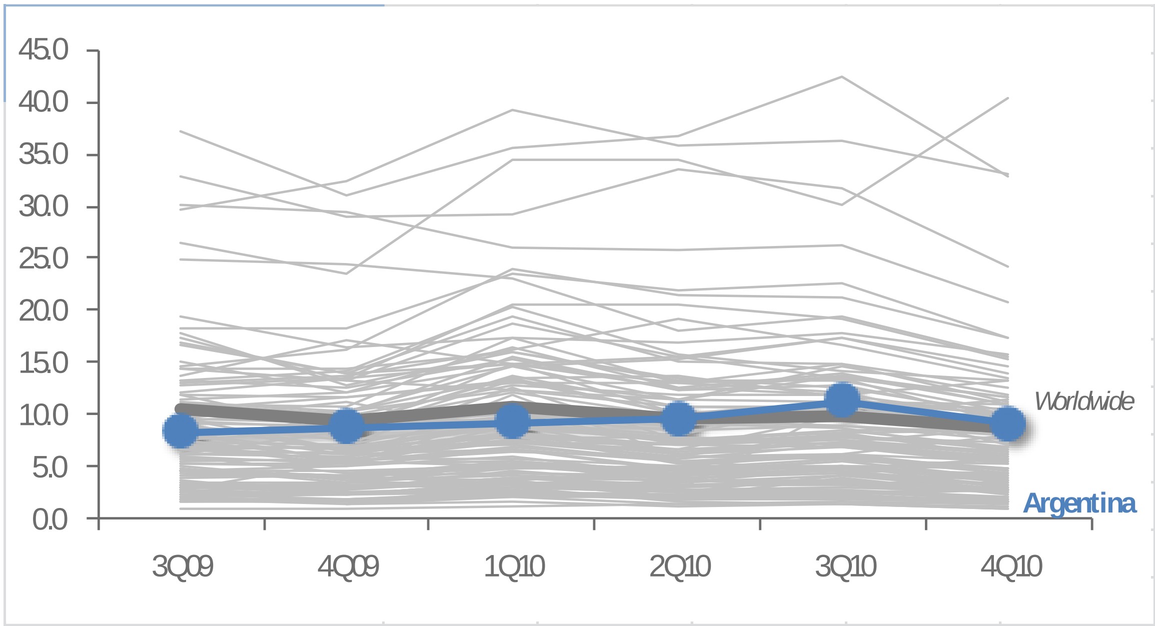
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Argentina in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Argentina and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 9.3 | 9.7 | 11.4 | 9.2 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.19 | | 0.15 | |
| Malware hosting sites per 1000 hosts | 0.19 | | 0.33 | |
| Percentage of sites hosting drive-by downloads | | 0.099% | 0.097% | |

## Infection Trends (CCM)

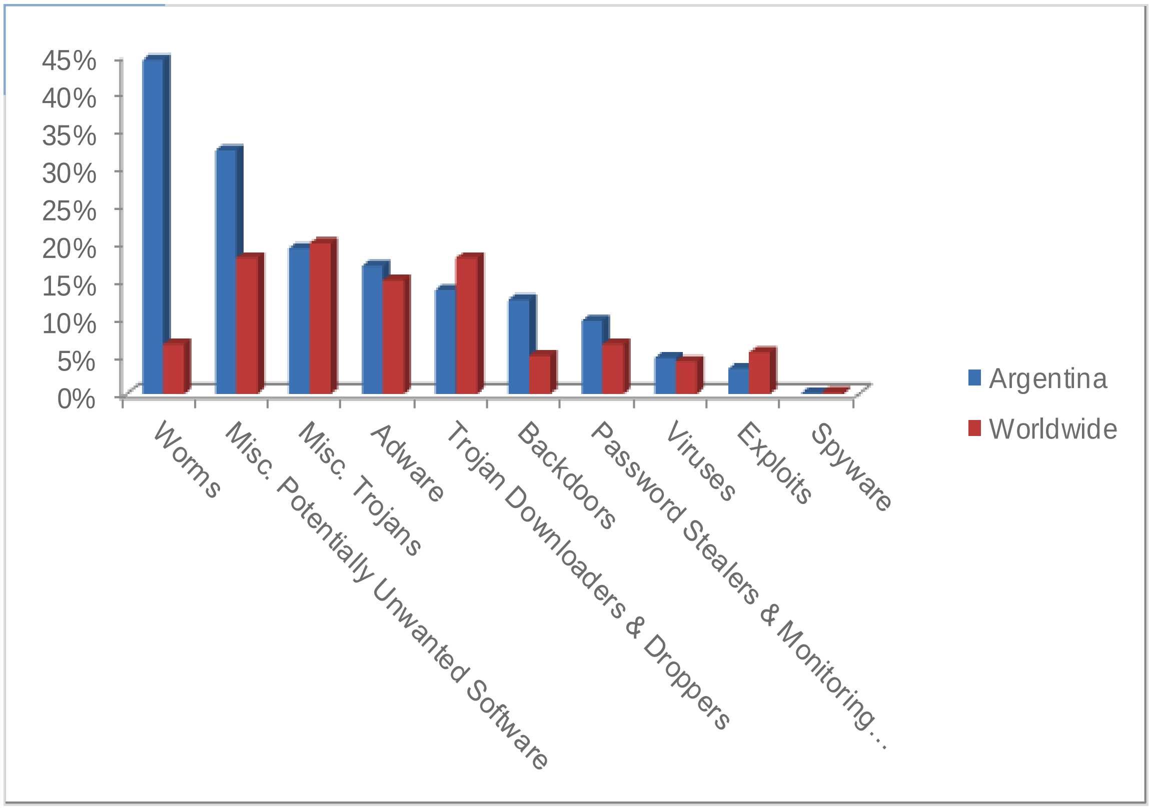
The MSRT detected malware on 9.2 of every 1,000 computers scanned in Argentina in 4Q10 (a CCM score of 9.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Argentina over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Argentina and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Argentina in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Argentina in 4Q10 was Worms, which affected 44.3 percent of all cleaned computers, up from 41.0 percent in 3Q10.
- The second most common category in Argentina in 4Q10 was Misc. Potentially Unwanted Software, which affected 32.3 percent of all cleaned computers, down from 32.5 percent in 3Q10.
- The third most common category in Argentina in 4Q10 was Misc. Trojans, which affected 19.3 percent of all cleaned computers, down from 19.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Argentina in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | IRC/Prune | 18.9% |
| 2 | Win32/Autorun | 15.8% |
| 3 | JS/Pornpop | 9.7% |
| 4 | Win32/Conficker | 8.5% |
| 5 | Win32/Taterf | 7.1% |
| 6 | Win32/IRCbot | 6.4% |
| 7 | Win32/Keygen | 4.9% |
| 8 | Win32/Frethog | 4.6% |
| 9 | Win32/Zwangi | 4.1% |
| 10 | Win32/Rimecud | 4.1% |

- The most common threat family in Argentina in 4Q10 was IRC/Prune, which affected 18.9 percent of cleaned computers. IRC/Prune is a detection for an Internet Relay Chat (IRC) configuration script commonly named “mirc.ini”. The script attempts to distribute a VBScript copy of the worm to other users who connect to IRC channels.
- The second most common threat family in Argentina in 4Q10 was Win32/Autorun, which affected 15.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Argentina in 4Q10 was JS/Pornpop, which affected 9.7 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Argentina in 4Q10 was Win32/Conficker, which affected 8.5 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

# Australia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

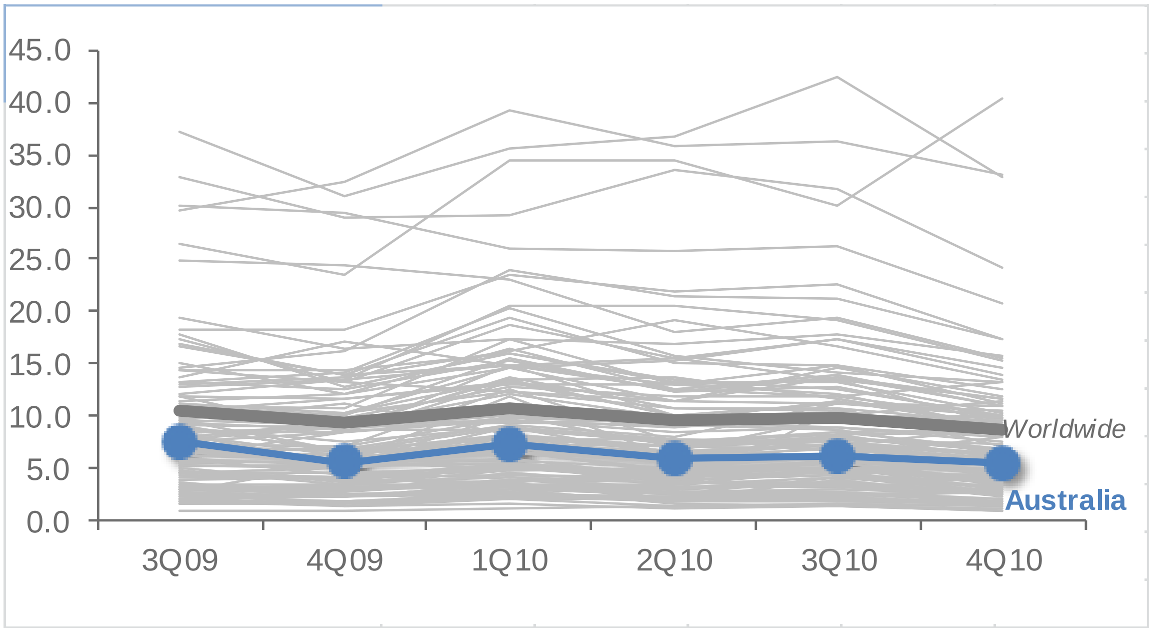
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Australia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Australia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">7.2</td><td colspan="3">5.9</td><td colspan="3">6.2</td><td colspan="3">5.5</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.61</td><td colspan="6">1.79</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.11</td><td colspan="6">0.07</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4"></td><td colspan="4">0.023%</td><td colspan="4">0.039%</td></tr>
</table>

## Infection Trends (CCM)

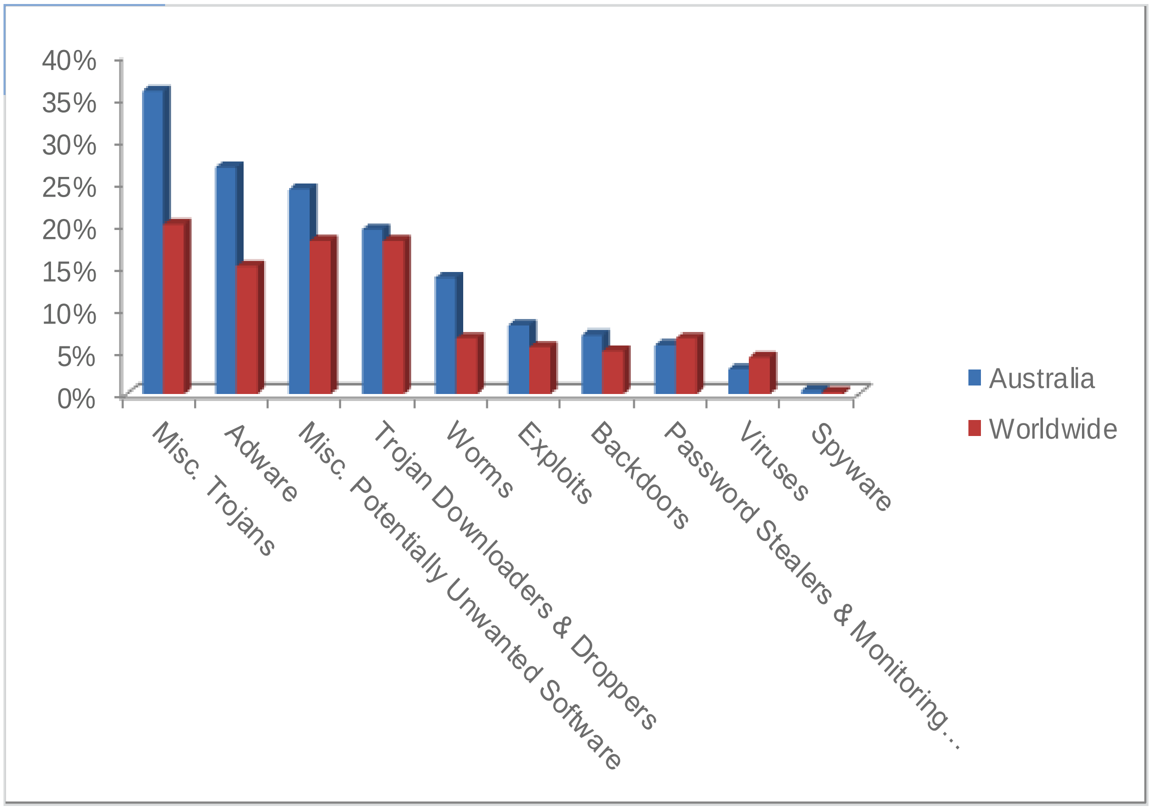
The MSRT detected malware on 5.5 of every 1,000 computers scanned in Australia in 4Q10 (a CCM score of 5.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Australia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Australia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Australia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Australia in 4Q10 was Misc. Trojans, which affected 35.7 percent of all cleaned computers, down from 37.9 percent in 3Q10.
- The second most common category in Australia in 4Q10 was Adware, which affected 26.8 percent of all cleaned computers, up from 23.1 percent in 3Q10.
- The third most common category in Australia in 4Q10 was Misc. Potentially Unwanted Software, which affected 24.2 percent of all cleaned computers, up from 22.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Australia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 14.9% |
| 2 | Win32/FakeSpypro | 6.0% |
| 3 | Win32/ClickPotato | 5.4% |
| 4 | Win32/Renos | 5.1% |
| 5 | Win32/Zwangi | 5.1% |
| 6 | Win32/Autorun | 5.0% |
| 7 | Win32/Hotbar | 4.7% |
| 8 | ASX/Wimad | 4.7% |
| 9 | Win32/Alureon | 3.8% |
| 10 | Java/CVE-2008-5353 | 3.4% |

- The most common threat family in Australia in 4Q10 was JS/Pornpop, which affected 14.9 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Australia in 4Q10 was Win32/FakeSpypro, which affected 6.0 percent of cleaned computers. Win32/FakeSpypro is a rogue security software family distributed under the names Antivirus System PRO, Spyware Protect 2009, and others.
- The third most common threat family in Australia in 4Q10 was Win32/ClickPotato, which affected 5.4 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The fourth most common threat family in Australia in 4Q10 was Win32/Renos, which affected 5.1 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.

# Austria

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

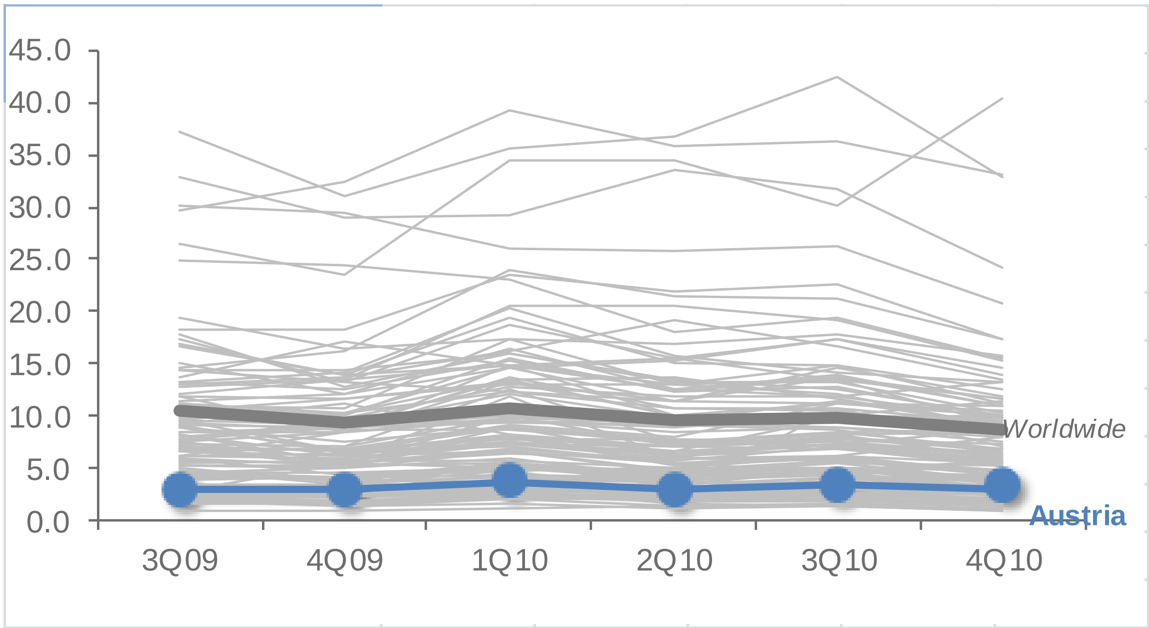
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Austria in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Austria and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">3.8</td><td colspan="3">3.0</td><td colspan="3">3.5</td><td colspan="3">3.3</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.16</td><td colspan="6">0.20</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.30</td><td colspan="6">0.77</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4"></td><td colspan="4">0.029%</td><td colspan="4">0.031%</td></tr>
</table>

## Infection Trends (CCM)

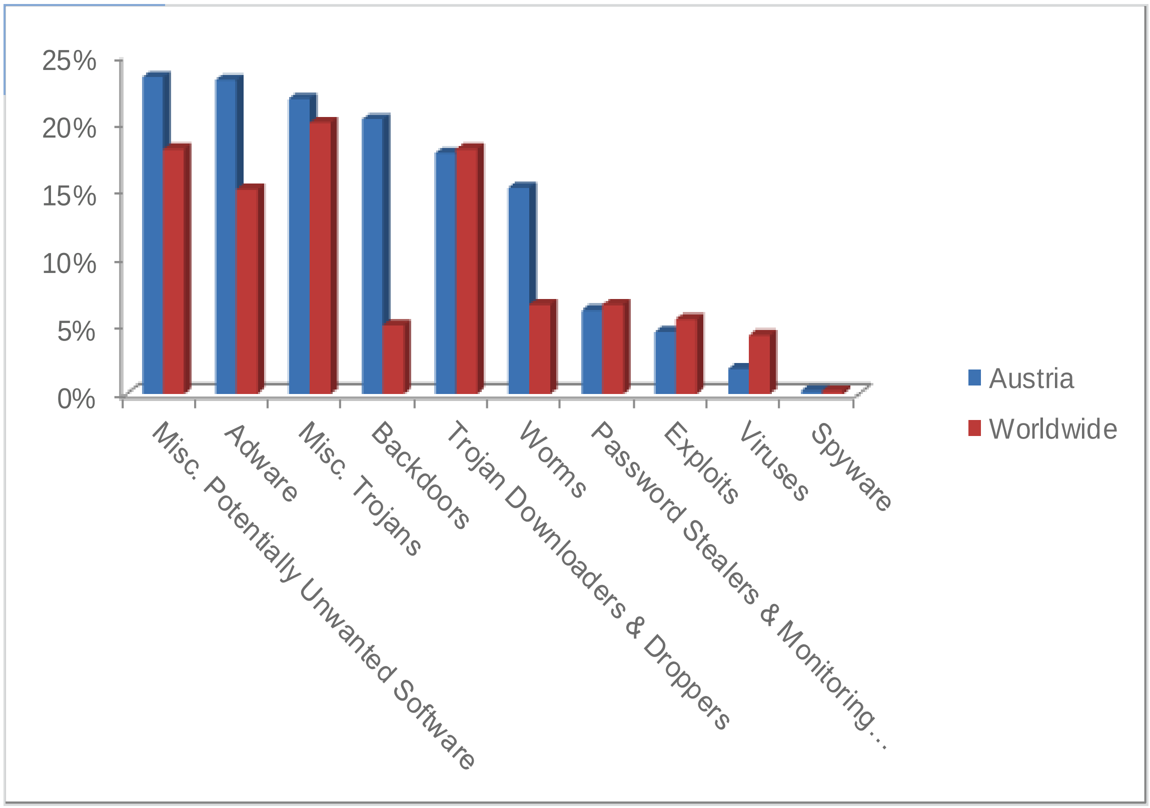
The MSRT detected malware on 3.3 of every 1,000 computers scanned in Austria in 4Q10 (a CCM score of 3.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Austria over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Austria and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Austria in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Austria in 4Q10 was Misc. Potentially Unwanted Software, which affected 23.4 percent of all cleaned computers, down from 26.4 percent in 3Q10.
- The second most common category in Austria in 4Q10 was Adware, which affected 23.1 percent of all cleaned computers, down from 25.8 percent in 3Q10.
- The third most common category in Austria in 4Q10 was Misc. Trojans, which affected 21.8 percent of all cleaned computers, down from 22.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Austria in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/IRCbot | 17.5% |
| 2 | JS/Pornpop | 16.2% |
| 3 | Win32/Renos | 6.9% |
| 4 | Win32/Keygen | 5.5% |
| 5 | Win32/Conficker | 4.2% |
| 6 | Win32/Autorun | 3.4% |
| 7 | ASX/Wimad | 3.1% |
| 8 | Win32/Slenfbot | 2.9% |
| 9 | Win32/Alureon | 2.9% |
| 10 | Win32/Obfuscator | 2.9% |

- The most common threat family in Austria in 4Q10 was Win32/IRCbot, which affected 17.5 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The second most common threat family in Austria in 4Q10 was JS/Pornpop, which affected 16.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Austria in 4Q10 was Win32/Renos, which affected 6.9 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.
- The fourth most common threat family in Austria in 4Q10 was Win32/Keygen, which affected 5.5 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.

# Azerbaijan

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

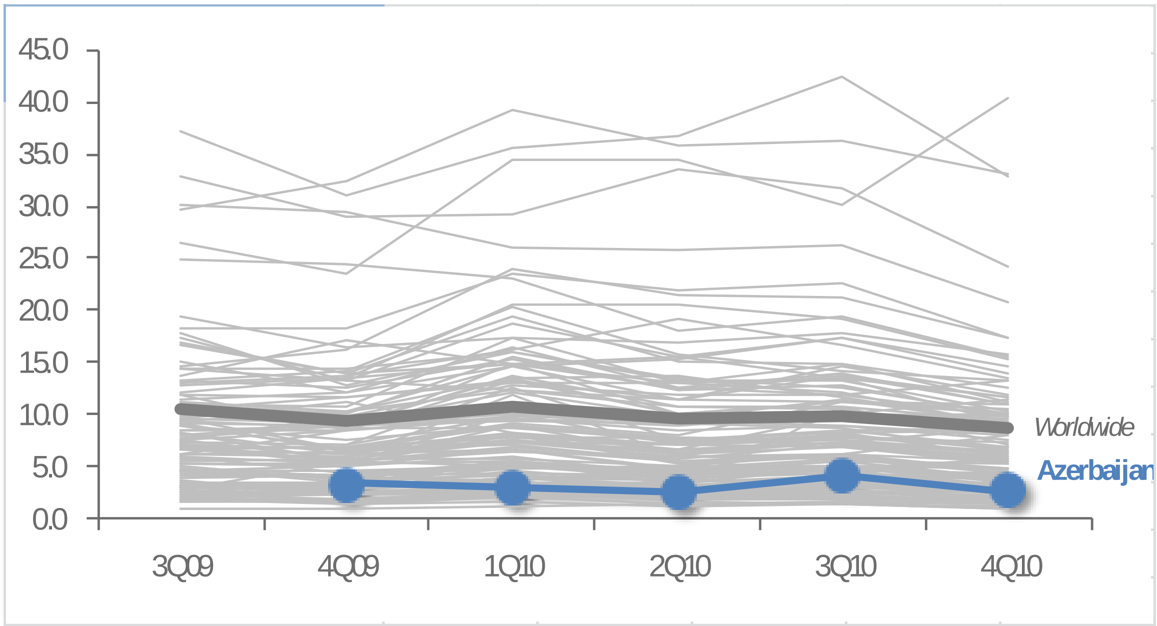
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Azerbaijan in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Azerbaijan and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 2.9 | 2.6 | 4.2 | 2.8 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 2.43 | | 1.14 | |
| Malware hosting sites per 1000 hosts | 4.15 | | 3.43 | |
| Percentage of sites hosting drive-by downloads | 0.412% | 0.330% | 0.255% | |

## Infection Trends (CCM)

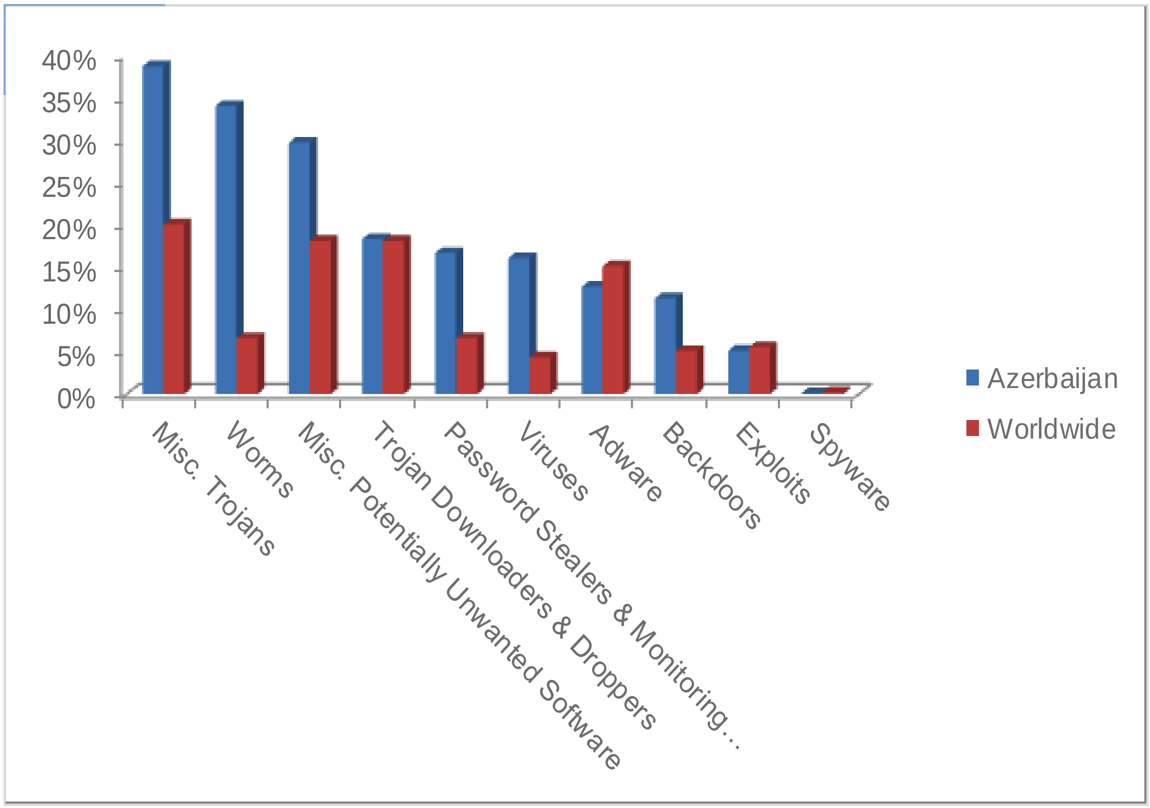
The MSRT detected malware on 2.8 of every 1,000 computers scanned in Azerbaijan in 4Q10 (a CCM score of 2.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Azerbaijan over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Azerbaijan and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Azerbaijan in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Azerbaijan in 4Q10 was Misc. Trojans, which affected 38.7 percent of all cleaned computers, up from 32.6 percent in 3Q10.
- The second most common category in Azerbaijan in 4Q10 was Worms, which affected 34.0 percent of all cleaned computers, up from 31.9 percent in 3Q10.
- The third most common category in Azerbaijan in 4Q10 was Misc. Potentially Unwanted Software, which affected 29.7 percent of all cleaned computers, down from 30.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Azerbaijan in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 19.6% |
| 2 | Win32/Rimecud | 16.3% |
| 3 | Win32/Sality | 14.9% |
| 4 | Win32/Taterf | 11.1% |
| 5 | JS/Pornpop | 9.8% |
| 6 | Win32/Frethog | 8.7% |
| 7 | Win32/Conficker | 7.6% |
| 8 | Win32/Keygen | 5.0% |
| 9 | Win32/IRCbot | 4.4% |
| 10 | Win32/Obfuscator | 4.3% |

- The most common threat family in Azerbaijan in 4Q10 was Win32/Autorun, which affected 19.6 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Azerbaijan in 4Q10 was Win32/Rimecud, which affected 16.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Azerbaijan in 4Q10 was Win32/Sality, which affected 14.9 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Azerbaijan in 4Q10 was Win32/Taterf, which affected 11.1 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Bahamas

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

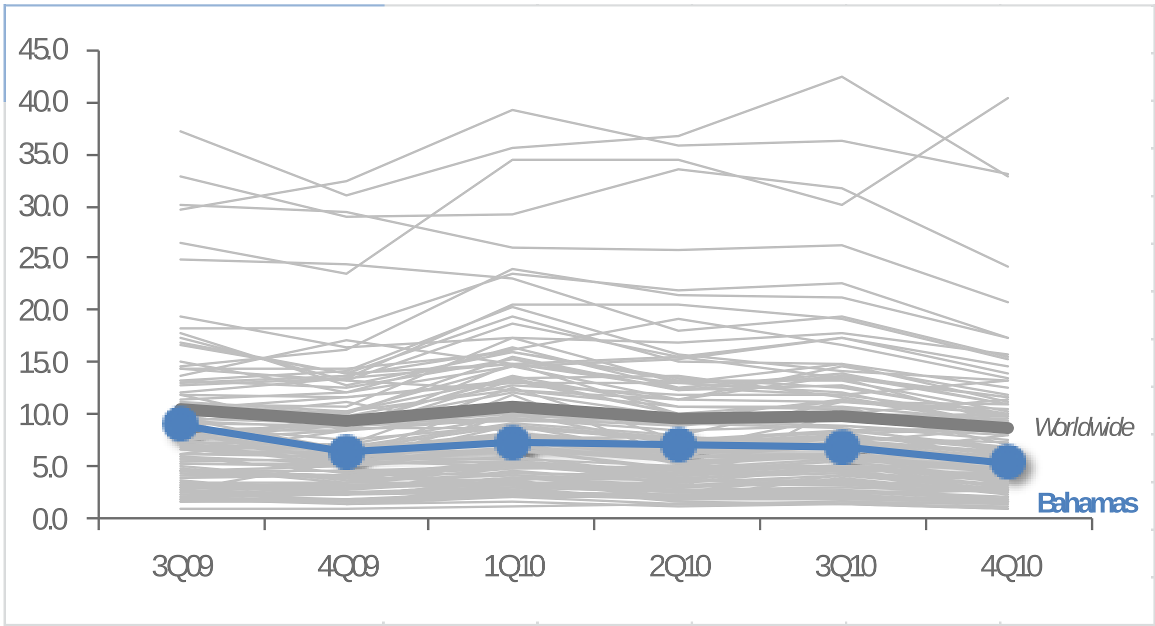
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Bahamas in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Bahamas and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 7.3 | 7.2 | 6.9 | 5.4 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 25365.85 | | 73.17 | |
| Malware hosting sites per 1000 hosts | 8219.51 | | 97.56 | |
| Percentage of sites hosting drive-by downloads | 0.000% | | | |

## Infection Trends (CCM)

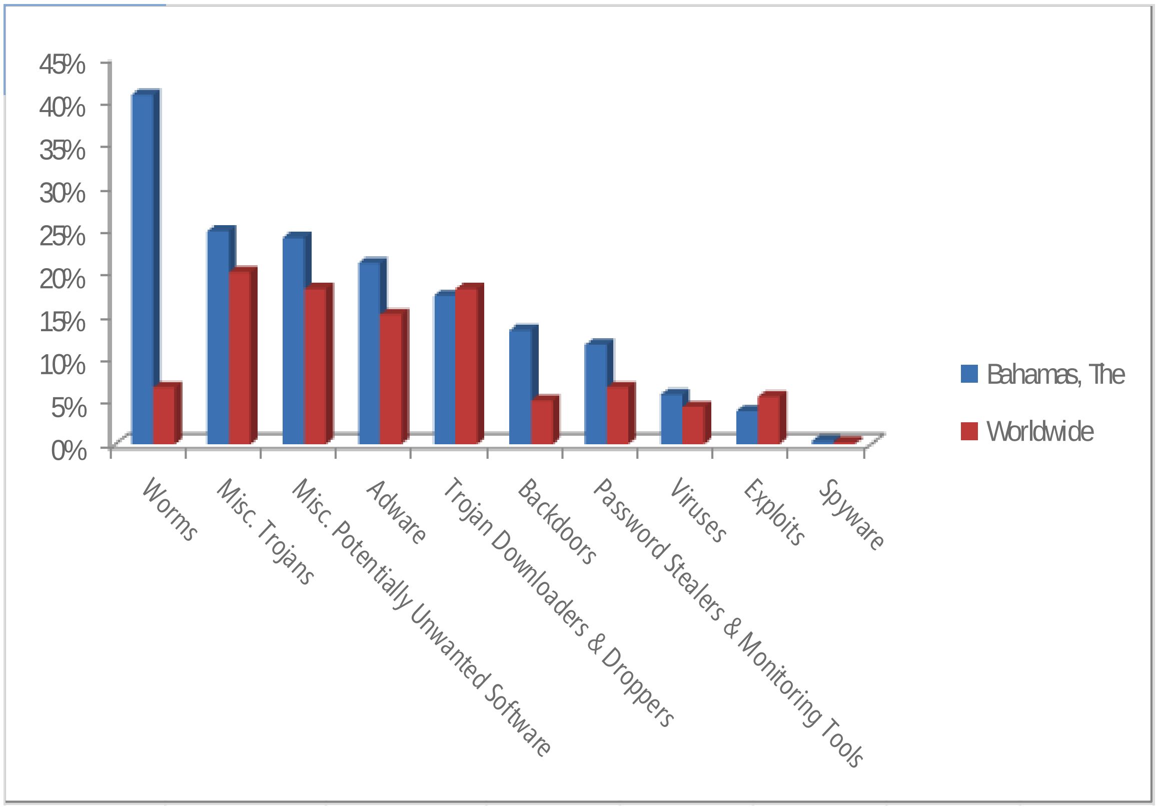
The MSRT detected malware on 5.4 of every 1,000 computers scanned in Bahamas in 4Q10 (a CCM score of 5.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Bahamas over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Bahamas and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Bahamas in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Bahamas in 4Q10 was Worms, which affected 40.6 percent of all cleaned computers, down from 47.5 percent in 3Q10.
- The second most common category in Bahamas in 4Q10 was Misc. Trojans, which affected 24.8 percent of all cleaned computers, up from 24.0 percent in 3Q10.
- The third most common category in Bahamas in 4Q10 was Misc. Potentially Unwanted Software, which affected 24.0 percent of all cleaned computers, up from 20.8 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Bahamas in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 12.6% |
| 2 | Win32/Vobfus | 11.5% |
| 3 | Win32/Taterf | 9.7% |
| 4 | Win32/ClickPotato | 9.1% |
| 5 | Win32/Zwangi | 8.9% |
| 6 | Win32/Rimecud | 8.4% |
| 7 | Win32/IRCbot | 7.7% |
| 8 | Win32/Frethog | 6.3% |
| 9 | Win32/Hotbar | 6.1% |
| 10 | Win32/Renos | 5.8% |

- The most common threat family in Bahamas in 4Q10 was Win32/Autorun, which affected 12.6 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Bahamas in 4Q10 was Win32/Vobfus, which affected 11.5 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The third most common threat family in Bahamas in 4Q10 was Win32/Taterf, which affected 9.7 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Bahamas in 4Q10 was Win32/ClickPotato, which affected 9.1 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user’s browsing habits.

# Bahrain

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

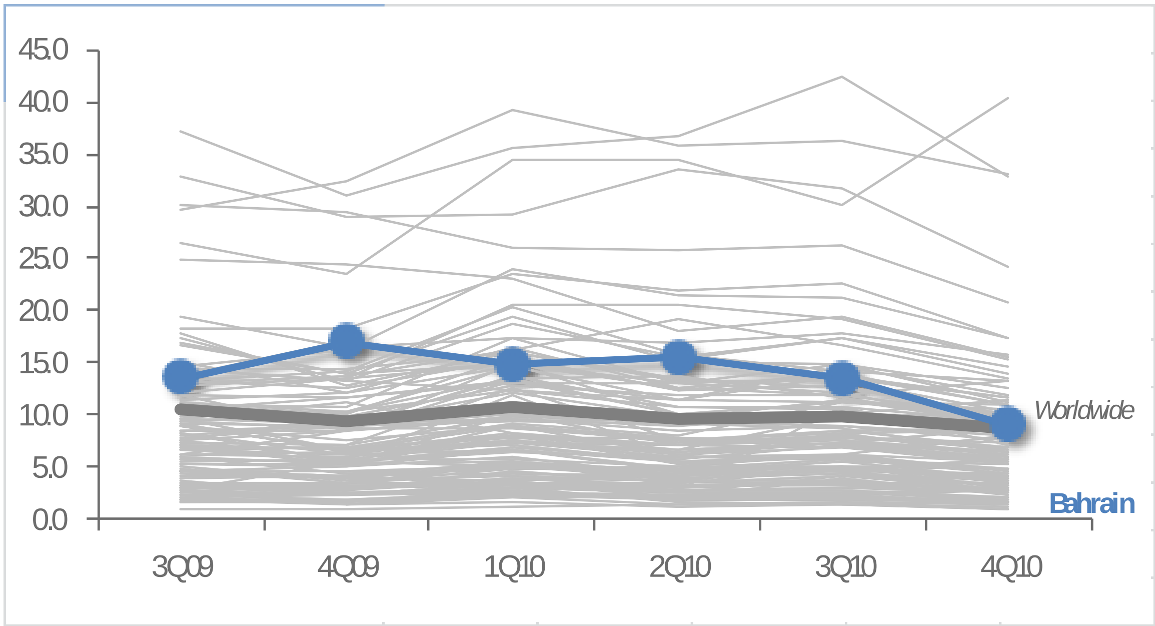
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Bahrain in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Bahrain and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 14.9 | 15.6 | 13.6 | 9.0 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 2.29 | | 0.76 | |
| Malware hosting sites per 1000 hosts | 0.76 | | 1.14 | |
| Percentage of sites hosting drive-by downloads | 0.364% | | | |

## Infection Trends (CCM)

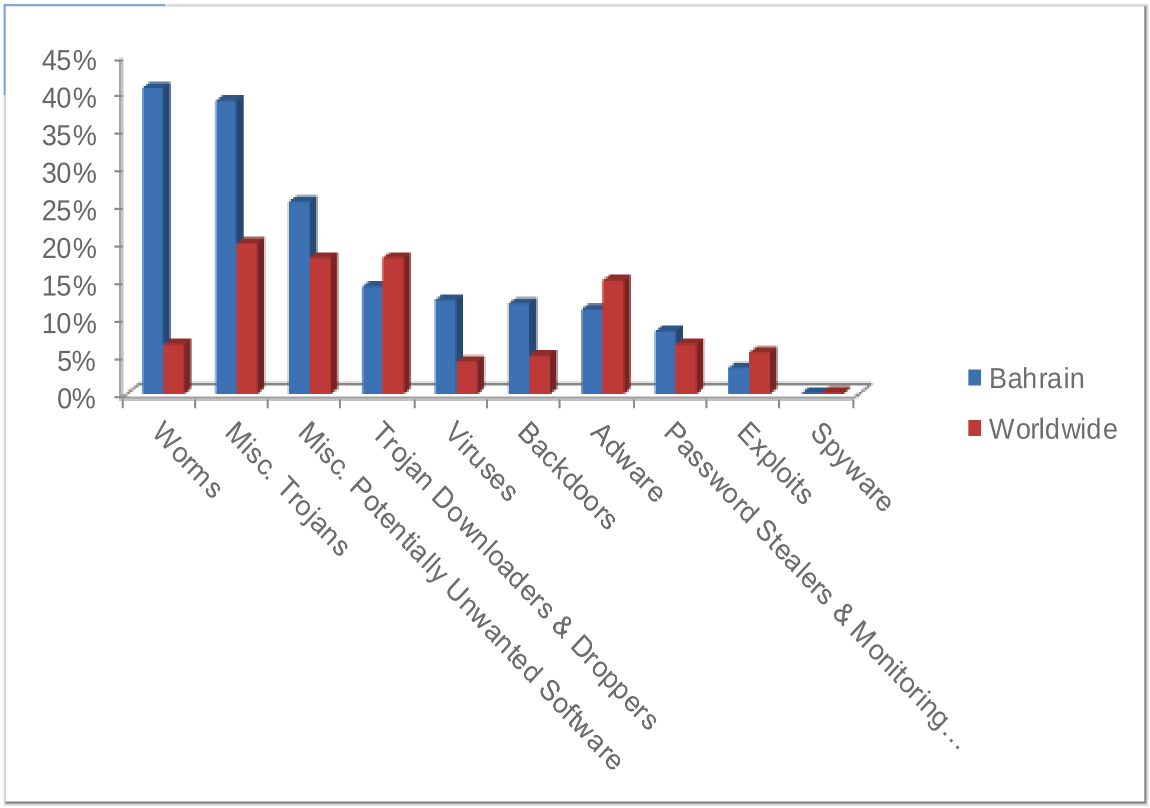
The MSRT detected malware on 9.0 of every 1,000 computers scanned in Bahrain in 4Q10 (a CCM score of 9.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Bahrain over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Bahrain and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Bahrain in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Bahrain in 4Q10 was Worms, which affected 40.6 percent of all cleaned computers, down from 43.2 percent in 3Q10.
- The second most common category in Bahrain in 4Q10 was Misc. Trojans, which affected 38.9 percent of all cleaned computers, up from 33.9 percent in 3Q10.
- The third most common category in Bahrain in 4Q10 was Misc. Potentially Unwanted Software, which affected 25.5 percent of all cleaned computers, up from 20.8 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Bahrain in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 18.9% |
| 2 | Win32/Autorun | 17.4% |
| 3 | Win32/Agent | 9.6% |
| 4 | Win32/Sality | 8.4% |
| 5 | Win32/Nuqel | 8.2% |
| 6 | Win32/Taterf | 6.3% |
| 7 | Giframe | 5.6% |
| 8 | Win32/Mabezat | 5.1% |
| 9 | Win32/Conficker | 5.1% |
| 10 | Sohanad | 4.7% |

- The most common threat family in Bahrain in 4Q10 was Win32/Rimecud, which affected 18.9 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Bahrain in 4Q10 was Win32/Autorun, which affected 17.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Bahrain in 4Q10 was Win32/Agent, which affected 9.6 percent of cleaned computers. Win32/Agent is a generic detection for a number of trojans that may perform different malicious functions. The functionality exhibited by this family is highly variable.
- The fourth most common threat family in Bahrain in 4Q10 was Win32/Sality, which affected 8.4 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Bangladesh

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

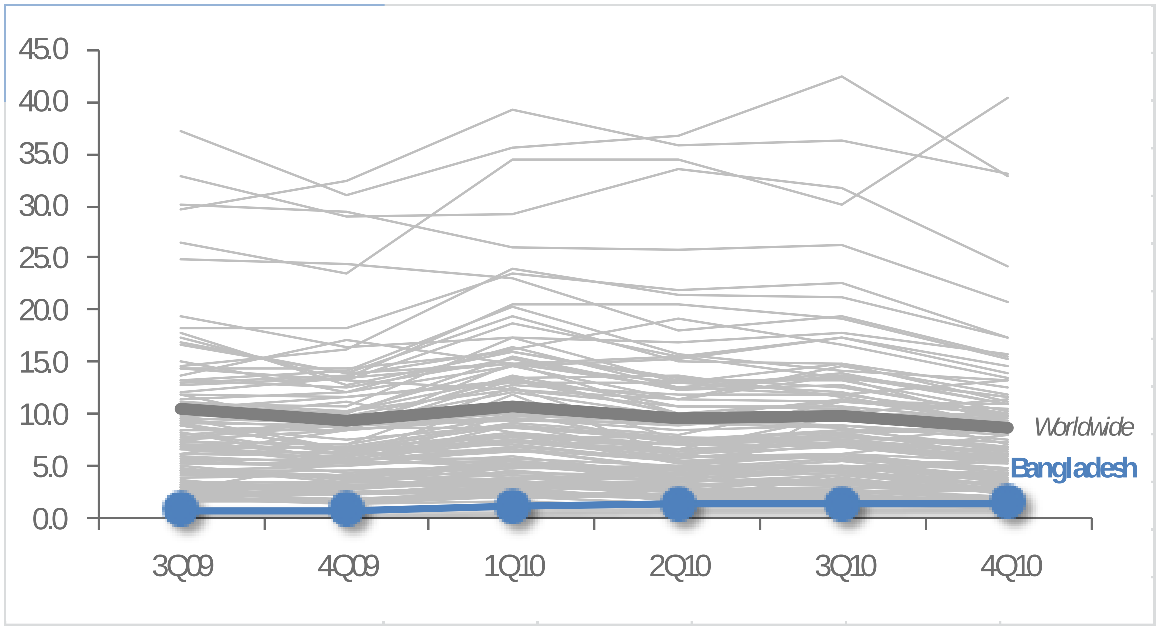
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Bangladesh in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Bangladesh and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 1.2 | 1.5 | 1.5 | 1.5 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 83.33 | | 33.33 | |
| Malware hosting sites per 1000 hosts | 27.08 | | 110.42 | |
| Percentage of sites hosting drive-by downloads | 0.592% | 0.794% | 0.734% | |

## Infection Trends (CCM)

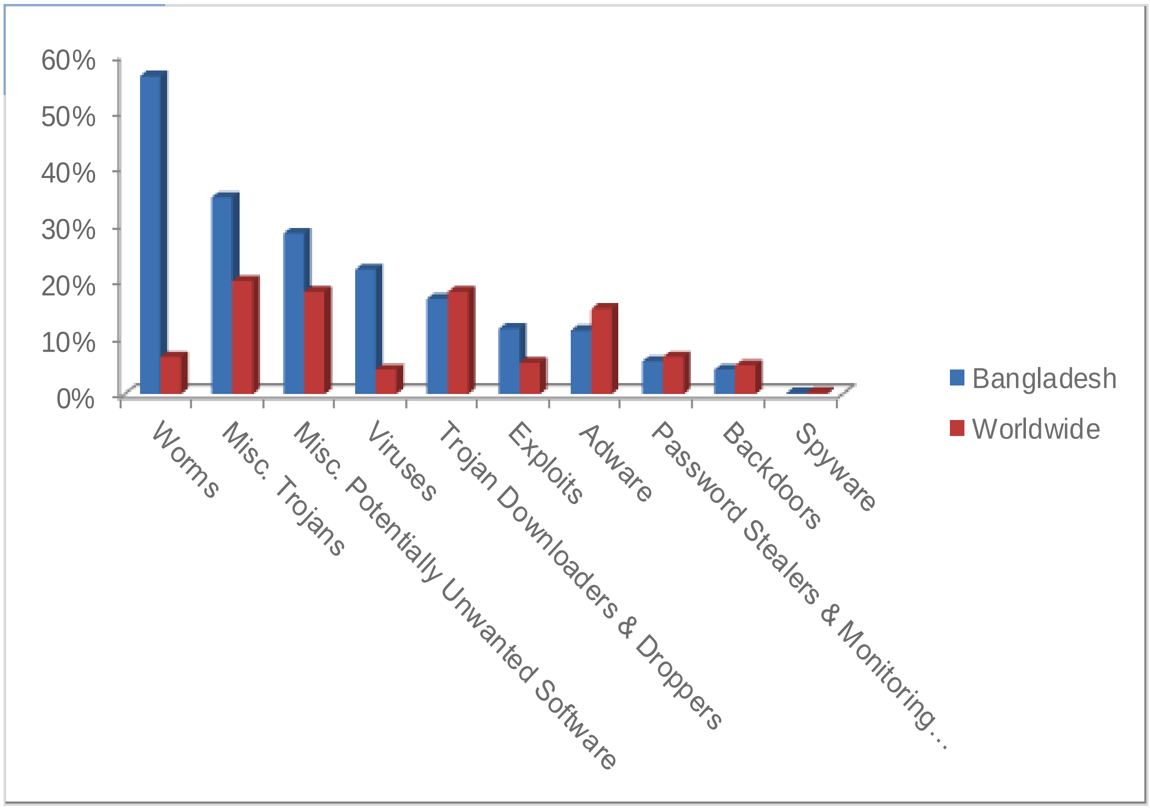
The MSRT detected malware on 1.5 of every 1,000 computers scanned in Bangladesh in 4Q10 (a CCM score of 1.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Bangladesh over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Bangladesh and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Bangladesh in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Bangladesh in 4Q10 was Worms, which affected 56.2 percent of all cleaned computers, down from 61.8 percent in 3Q10.
- The second most common category in Bangladesh in 4Q10 was Misc. Trojans, which affected 34.8 percent of all cleaned computers, up from 28.3 percent in 3Q10.
- The third most common category in Bangladesh in 4Q10 was Misc. Potentially Unwanted Software, which affected 28.4 percent of all cleaned computers, up from 26.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Bangladesh in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 32.7% |
| 2 | Win32/Sality | 22.2% |
| 3 | Win32/Autorun | 21.2% |
| 4 | Win32/Conficker | 14.7% |
| 5 | Win32/Stuxnet | 9.7% |
| 6 | CplLnk | 6.5% |
| 7 | Win32/Taterf | 5.8% |
| 8 | JS/Pornpop | 5.5% |
| 9 | Win32/VB | 5.0% |
| 10 | Win32/CeeInject | 4.5% |

- The most common threat family in Bangladesh in 4Q10 was Win32/Rimecud, which affected 32.7 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Bangladesh in 4Q10 was Win32/Sality, which affected 22.2 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family in Bangladesh in 4Q10 was Win32/Autorun, which affected 21.2 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common threat family in Bangladesh in 4Q10 was Win32/Conficker, which affected 14.7 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

# Barbados

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

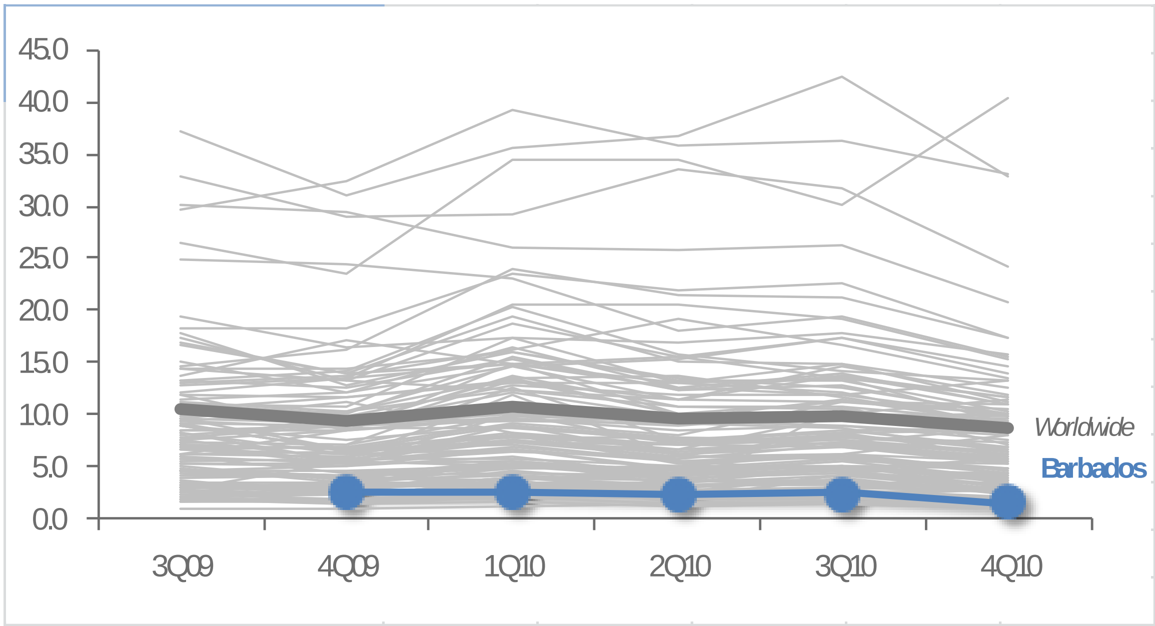
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Barbados in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Barbados and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">2.6</td><td colspan="3">2.2</td><td colspan="3">2.3</td><td colspan="3">1.5</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">48.08</td><td colspan="6">9.62</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6"></td><td colspan="6">9.62</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.280%</td><td colspan="4">0.474%</td><td colspan="4"></td></tr>
</table>

## Infection Trends (CCM)

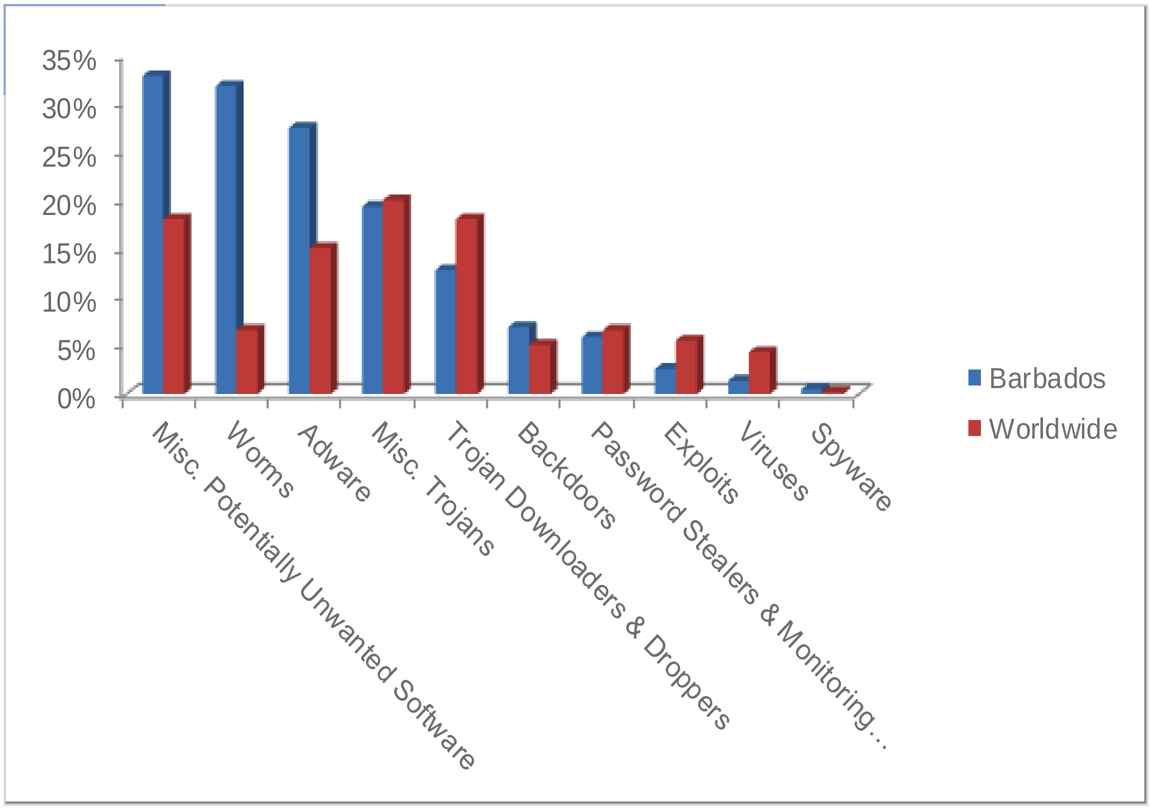
The MSRT detected malware on 1.5 of every 1,000 computers scanned in Barbados in 4Q10 (a CCM score of 1.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Barbados over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Barbados and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Barbados in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Barbados in 4Q10 was Misc. Potentially Unwanted Software, which affected 32.8 percent of all cleaned computers, down from 38.3 percent in 3Q10.
- The second most common category in Barbados in 4Q10 was Worms, which affected 31.8 percent of all cleaned computers, up from 26.5 percent in 3Q10.
- The third most common category in Barbados in 4Q10 was Adware, which affected 27.5 percent of all cleaned computers, up from 22.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Barbados in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 18.1% |
| 2 | Win32/Zwangi | 12.8% |
| 3 | Win32/ClickPotato | 12.6% |
| 4 | Win32/Hotbar | 9.2% |
| 5 | Win32/Vobfus | 6.6% |
| 6 | Win32/Conficker | 5.9% |
| 7 | Win32/Hamweq | 5.2% |
| 8 | JS/Pornpop | 5.2% |
| 9 | Win32/Renos | 4.7% |
| 10 | Win32/Taterf | 4.7% |

- The most common threat family in Barbados in 4Q10 was Win32/Autorun, which affected 18.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Barbados in 4Q10 was Win32/Zwangi, which affected 12.8 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The third most common threat family in Barbados in 4Q10 was Win32/ClickPotato, which affected 12.6 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user’s browsing habits.
- The fourth most common threat family in Barbados in 4Q10 was Win32/Hotbar, which affected 9.2 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

# Belarus

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

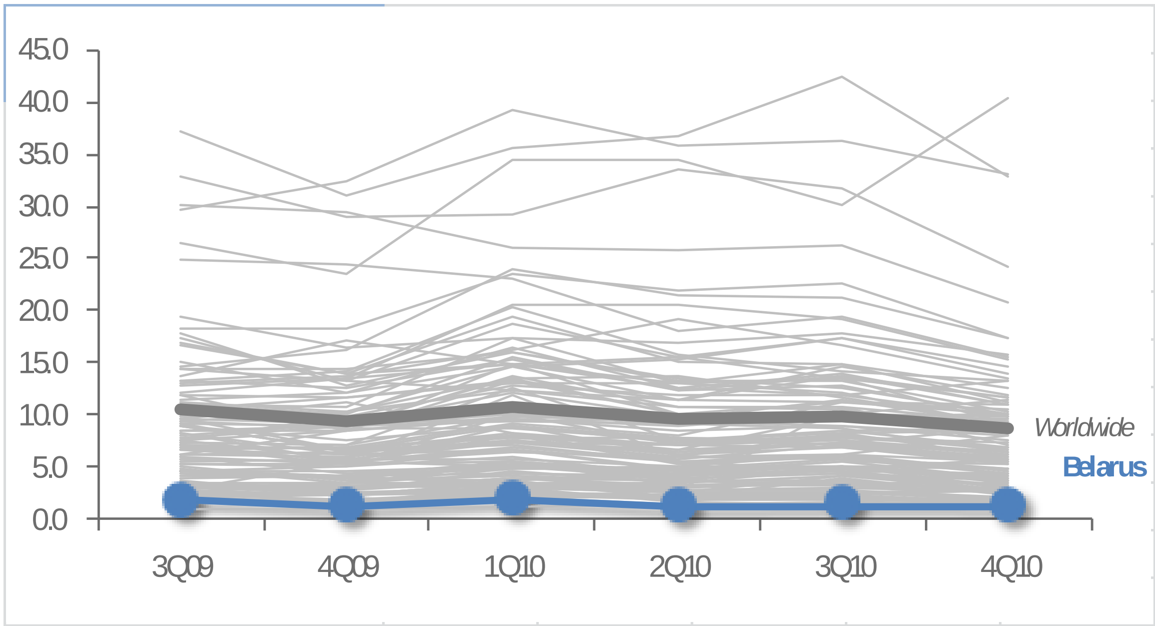
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Belarus in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Belarus and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">2.0</td><td colspan="3">1.3</td><td colspan="3">1.5</td><td colspan="3">1.5</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.98</td><td colspan="6">1.25</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.91</td><td colspan="6">1.41</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.158%</td><td colspan="4">0.099%</td><td colspan="4">0.108%</td></tr>
</table>

## Infection Trends (CCM)

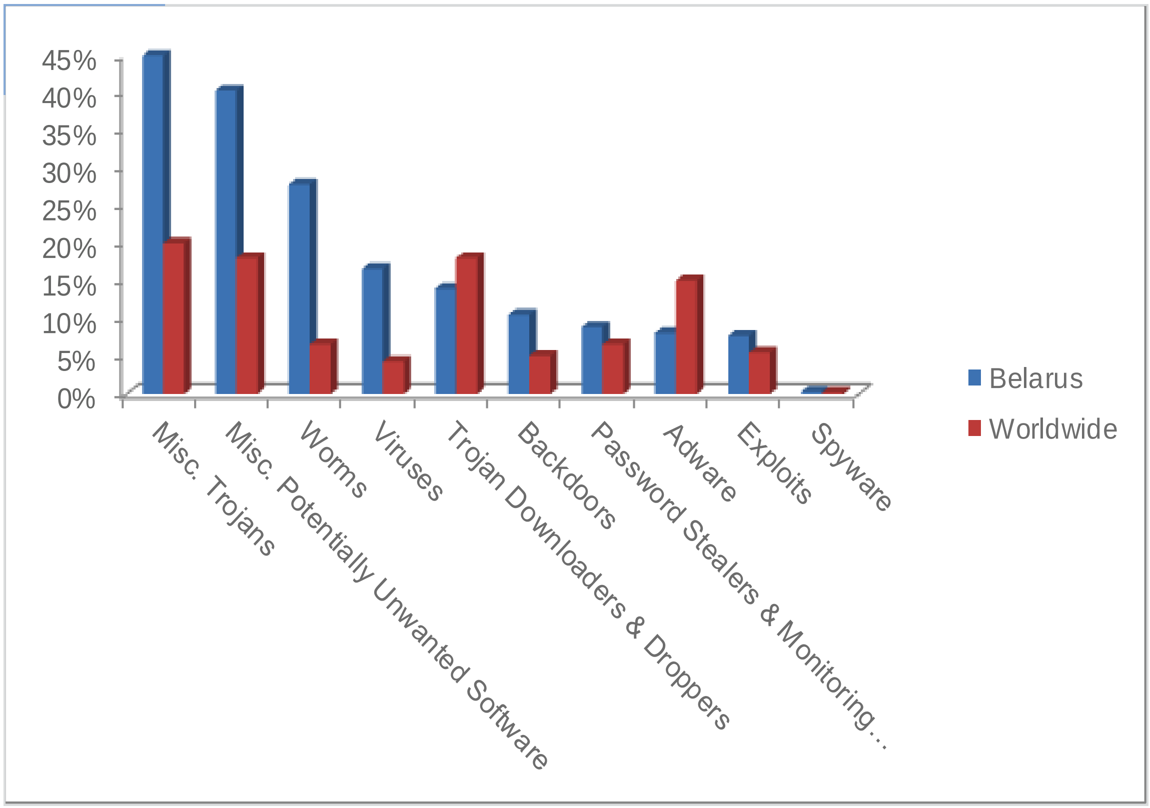
The MSRT detected malware on 1.5 of every 1,000 computers scanned in Belarus in 4Q10 (a CCM score of 1.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Belarus over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Belarus and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Belarus in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Belarus in 4Q10 was Misc. Trojans, which affected 44.9 percent of all cleaned computers, up from 39.1 percent in 3Q10.
- The second most common category in Belarus in 4Q10 was Misc. Potentially Unwanted Software, which affected 40.3 percent of all cleaned computers, up from 38.0 percent in 3Q10.
- The third most common category in Belarus in 4Q10 was Worms, which affected 27.8 percent of all cleaned computers, down from 34.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Belarus in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 20.6% |
| 2 | Win32/Autorun | 17.3% |
| 3 | Win32/Keygen | 12.2% |
| 4 | Win32/Sality | 9.6% |
| 5 | Win32/Obfuscator | 9.0% |
| 6 | Bumat | 5.2% |
| 7 | Win32/Conficker | 4.9% |
| 8 | Win32/Stuxnet | 4.7% |
| 9 | JS/Pornpop | 4.3% |
| 10 | Orsam | 4.1% |

- The most common threat family in Belarus in 4Q10 was Win32/Rimecud, which affected 20.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Belarus in 4Q10 was Win32/Autorun, which affected 17.3 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Belarus in 4Q10 was Win32/Keygen, which affected 12.2 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.
- The fourth most common threat family in Belarus in 4Q10 was Win32/Sality, which affected 9.6 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Belgium

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

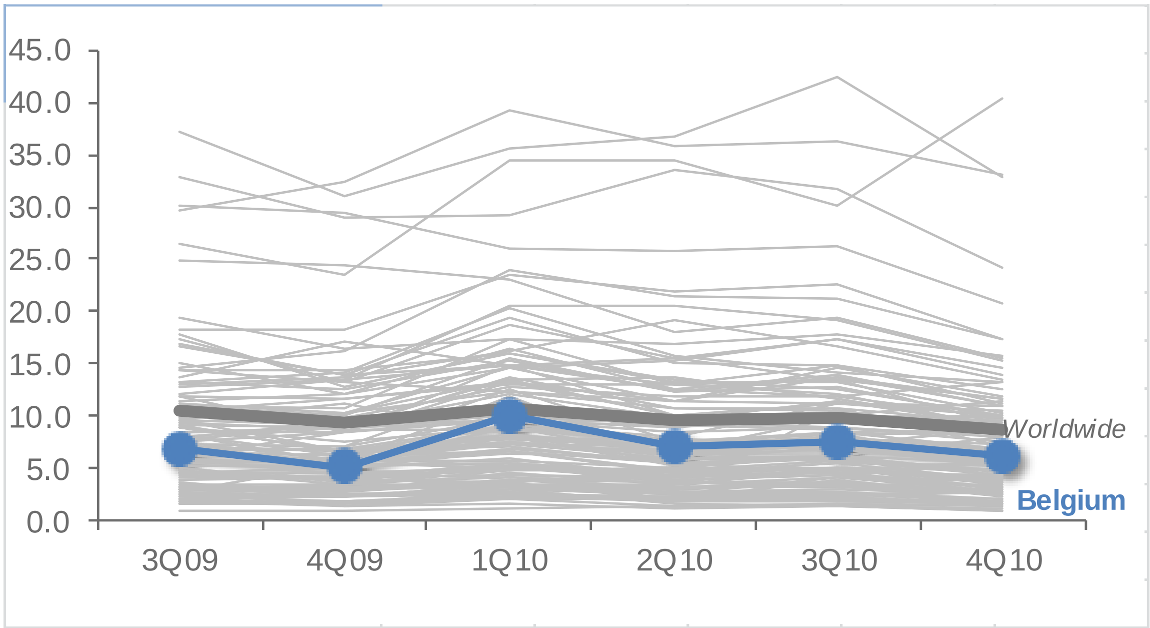
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Belgium in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Belgium and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 10.1 | 7.0 | 7.5 | 6.1 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.23 | | 0.27 | |
| Malware hosting sites per 1000 hosts | 0.52 | | 0.21 | |
| Percentage of sites hosting drive-by downloads | 0.129% | 0.044% | 0.061% | |

## Infection Trends (CCM)

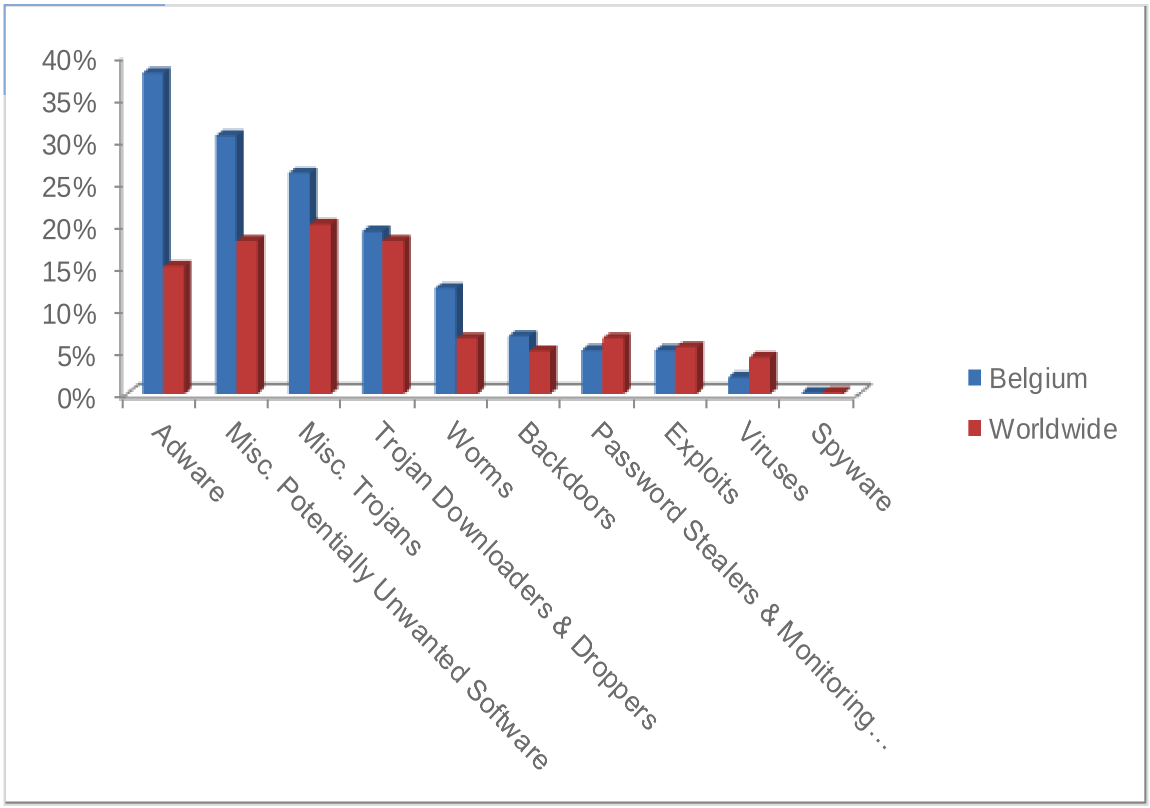
The MSRT detected malware on 6.1 of every 1,000 computers scanned in Belgium in 4Q10 (a CCM score of 6.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Belgium over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Belgium and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Belgium in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Belgium in 4Q10 was Adware, which affected 37.9 percent of all cleaned computers, up from 29.1 percent in 3Q10.
- The second most common category in Belgium in 4Q10 was Misc. Potentially Unwanted Software, which affected 30.5 percent of all cleaned computers, up from 28.8 percent in 3Q10.
- The third most common category in Belgium in 4Q10 was Misc. Trojans, which affected 26.1 percent of all cleaned computers, up from 25.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Belgium in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/ClickPotato | 14.8% |
| 2 | JS/Pornpop | 13.9% |
| 3 | Win32/Zwangi | 13.8% |
| 4 | Win32/Hotbar | 7.5% |
| 5 | ASX/Wimad | 5.8% |
| 6 | Win32/Renos | 5.4% |
| 7 | Win32/Autorun | 3.9% |
| 8 | Win32/IRCbot | 3.6% |
| 9 | Win32/FakeSpypro | 3.5% |
| 10 | Win32/Keygen | 3.5% |

- The most common threat family in Belgium in 4Q10 was Win32/ClickPotato, which affected 14.8 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.

- The second most common threat family in Belgium in 4Q10 was JS/Pornpop, which affected 13.9 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

- The third most common threat family in Belgium in 4Q10 was Win32/Zwangi, which affected 13.8 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

- The fourth most common threat family in Belgium in 4Q10 was Win32/Hotbar, which affected 7.5 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

# Bolivia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

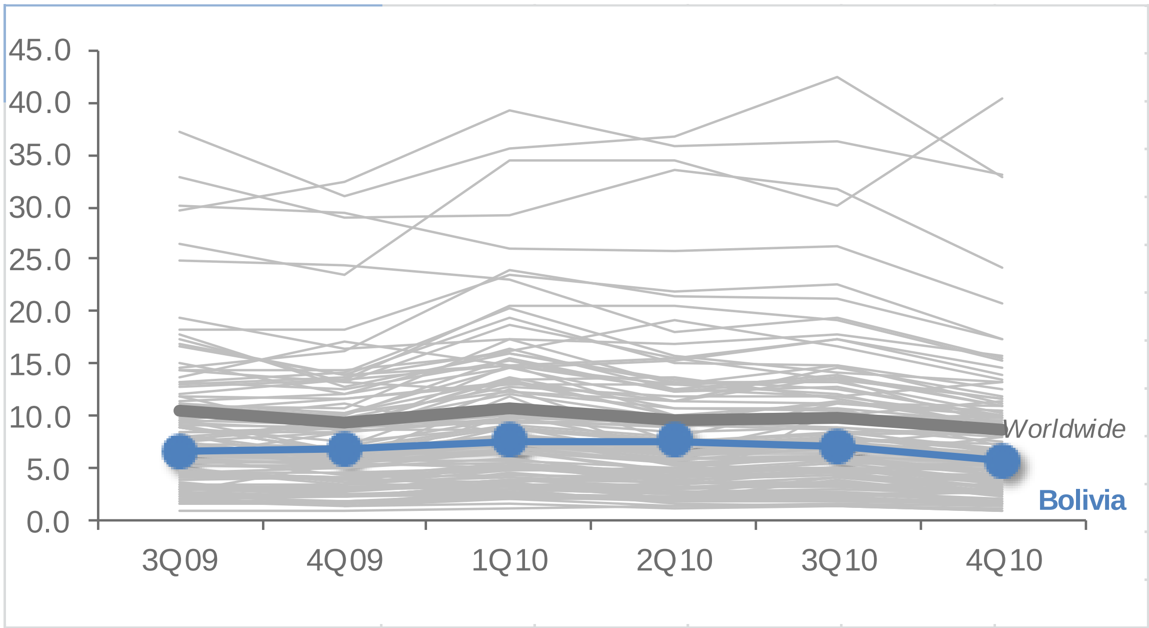
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Bolivia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Bolivia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">7.7</td><td colspan="3">7.8</td><td colspan="3">7.1</td><td colspan="3">5.7</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.18</td><td colspan="6">0.35</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.22</td><td colspan="6">0.50</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.277%</td><td colspan="4">0.024%</td><td colspan="4">0.233%</td></tr>
</table>

## Infection Trends (CCM)

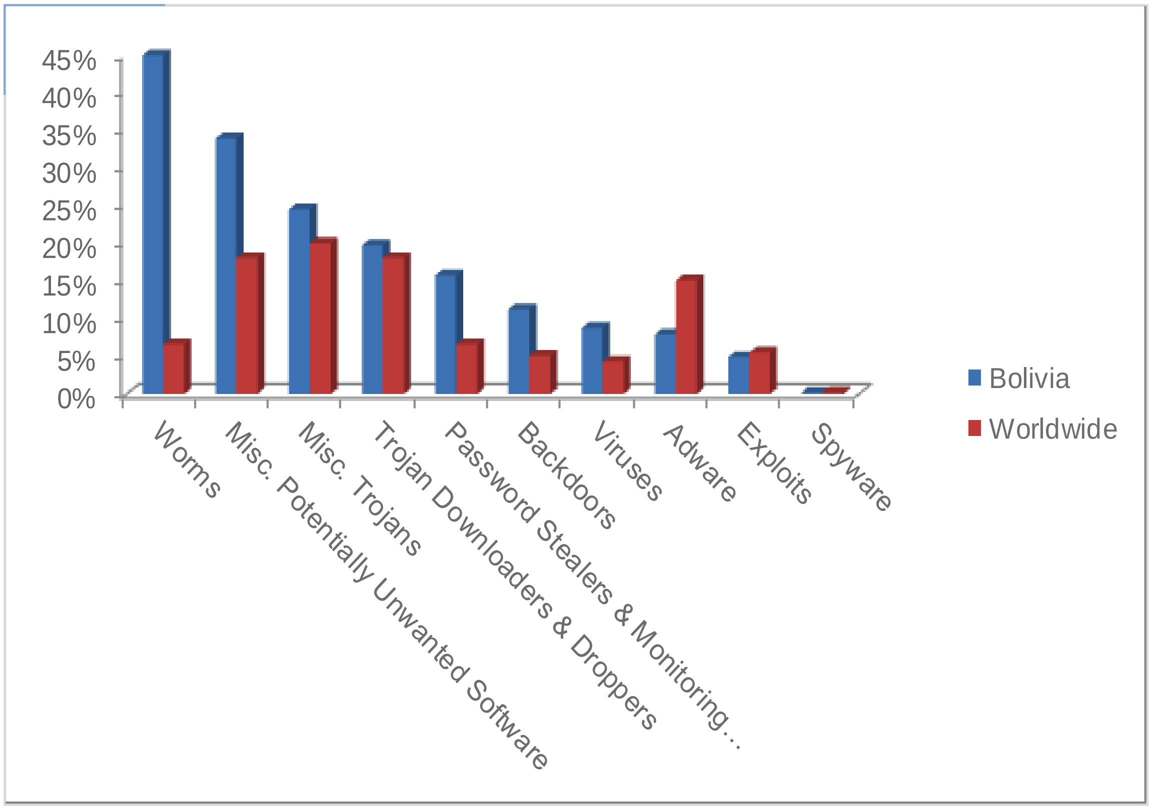
The MSRT detected malware on 5.7 of every 1,000 computers scanned in Bolivia in 4Q10 (a CCM score of 5.7, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Bolivia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Bolivia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Bolivia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Bolivia in 4Q10 was Worms, which affected 44.9 percent of all cleaned computers, down from 51.5 percent in 3Q10.
- The second most common category in Bolivia in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.9 percent of all cleaned computers, up from 30.7 percent in 3Q10.
- The third most common category in Bolivia in 4Q10 was Misc. Trojans, which affected 24.5 percent of all cleaned computers, up from 20.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Bolivia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 19.3% |
| 2 | Win32/Taterf | 15.8% |
| 3 | Win32/Rimecud | 15.2% |
| 4 | Win32/Frethog | 9.7% |
| 5 | Win32/Conficker | 8.8% |
| 6 | Win32/Sality | 8.2% |
| 7 | Win32/IRCbot | 7.8% |
| 8 | Win32/Keygen | 6.9% |
| 9 | Win32/Silly_P2P | 6.4% |
| 10 | Win32/Renos | 6.0% |

- The most common threat family in Bolivia in 4Q10 was Win32/Autorun, which affected 19.3 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Bolivia in 4Q10 was Win32/Taterf, which affected 15.8 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The third most common threat family in Bolivia in 4Q10 was Win32/Rimecud, which affected 15.2 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Bolivia in 4Q10 was Win32/Frethog, which affected 9.7 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

# Bosnia and Herzegovina

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

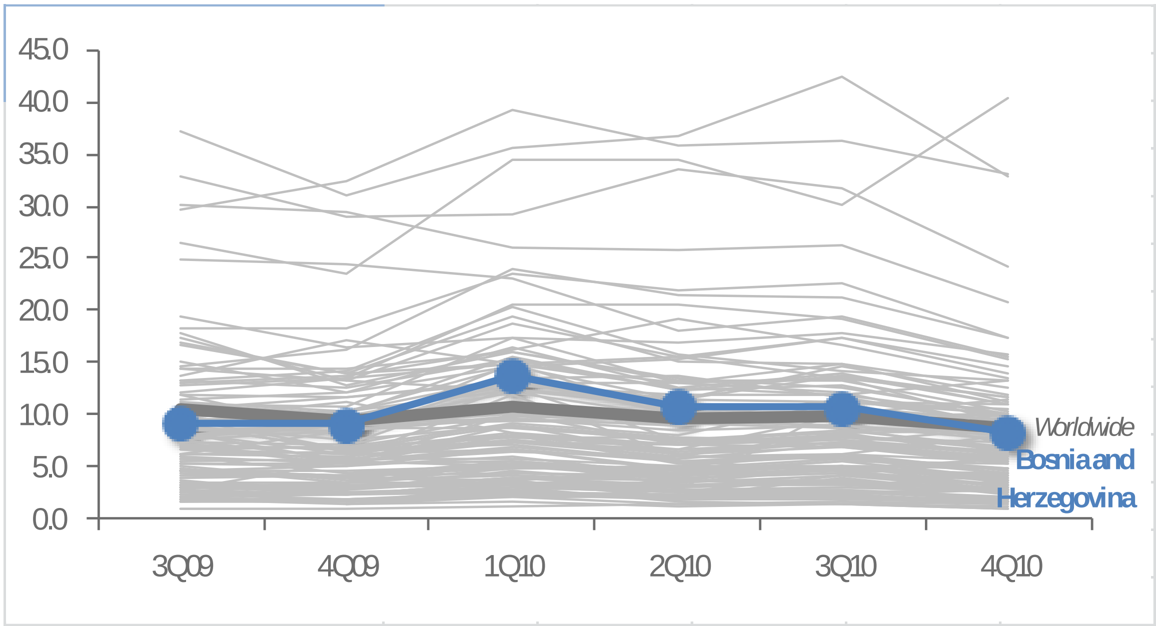
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Bosnia and Herzegovina in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Bosnia and Herzegovina and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">13.7</td><td colspan="3">10.7</td><td colspan="3">10.6</td><td colspan="3">8.3</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.45</td><td colspan="6">0.09</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">4.71</td><td colspan="6">79.94</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.211%</td><td colspan="4">0.084%</td><td colspan="4">0.098%</td></tr>
</table>

## Infection Trends (CCM)

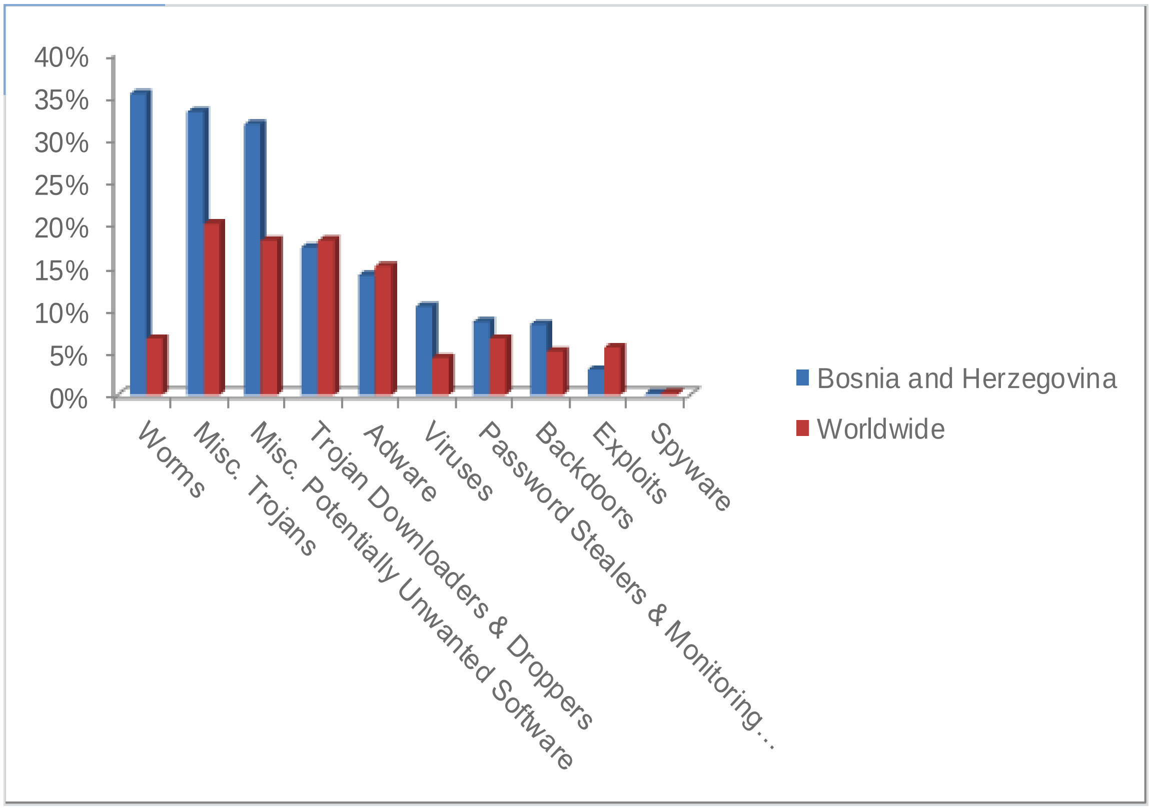
The MSRT detected malware on 8.3 of every 1,000 computers scanned in Bosnia and Herzegovina in 4Q10 (a CCM score of 8.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Bosnia and Herzegovina over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Bosnia and Herzegovina and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Bosnia and Herzegovina in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Bosnia and Herzegovina in 4Q10 was Worms, which affected 35.2 percent of all cleaned computers, down from 40.2 percent in 3Q10.
- The second most common category in Bosnia and Herzegovina in 4Q10 was Misc. Trojans, which affected 33.1 percent of all cleaned computers, up from 27.6 percent in 3Q10.
- The third most common category in Bosnia and Herzegovina in 4Q10 was Misc. Potentially Unwanted Software, which affected 31.6 percent of all cleaned computers, up from 27.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Bosnia and Herzegovina in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 21.5% |
| 2 | Win32/Autorun | 15.0% |
| 3 | JS/Pornpop | 8.3% |
| 4 | Win32/Sality | 7.4% |
| 5 | Win32/Keygen | 6.9% |
| 6 | Win32/Renos | 6.8% |
| 7 | Win32/Taterf | 5.3% |
| 8 | Helompy | 5.2% |
| 9 | Win32/Conficker | 5.1% |
| 10 | Win32/IRCbot | 4.2% |

- The most common threat family in Bosnia and Herzegovina in 4Q10 was Win32/Rimecud, which affected 21.5 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Bosnia and Herzegovina in 4Q10 was Win32/Autorun, which affected 15.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Bosnia and Herzegovina in 4Q10 was JS/Pornpop, which affected 8.3 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Bosnia and Herzegovina in 4Q10 was Win32/Sality, which affected 7.4 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Brazil

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

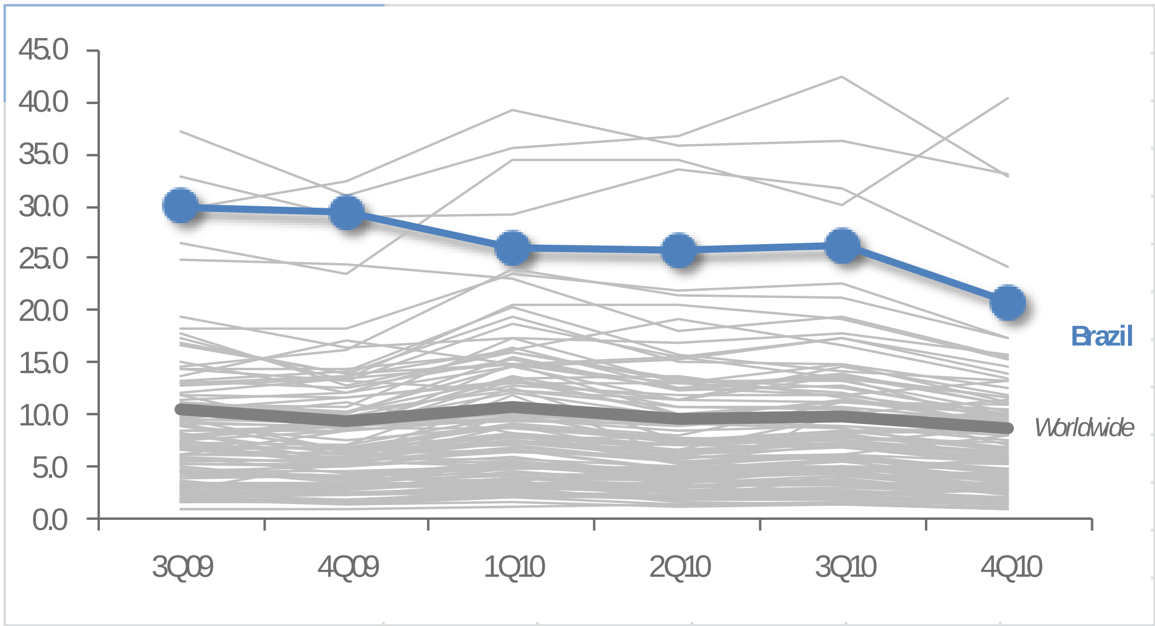
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Brazil in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Brazil and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">26.1</td><td colspan="3">25.8</td><td colspan="3">26.3</td><td colspan="3">20.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.14</td><td colspan="6">0.07</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.52</td><td colspan="6">1.21</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.175%</td><td colspan="4">0.122%</td><td colspan="4">0.096%</td></tr>
</table>

## Infection Trends (CCM)

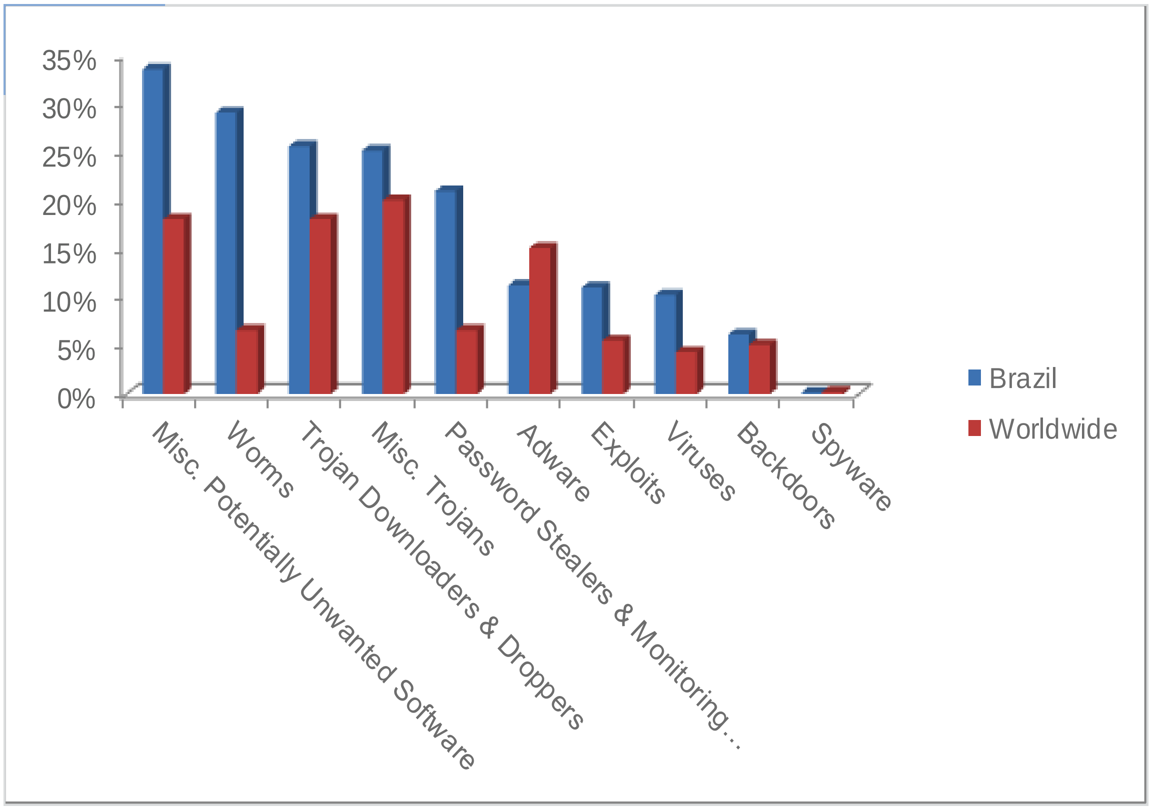
The MSRT detected malware on 20.8 of every 1,000 computers scanned in Brazil in 4Q10 (a CCM score of 20.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Brazil over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Brazil and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Brazil in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Brazil in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.5 percent of all cleaned computers, down from 35.1 percent in 3Q10.
- The second most common category in Brazil in 4Q10 was Worms, which affected 29.0 percent of all cleaned computers, down from 33.2 percent in 3Q10.
- The third most common category in Brazil in 4Q10 was Trojan Downloaders & Droppers, which affected 25.6 percent of all cleaned computers, down from 28.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Brazil in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 20.3% |
| 2 | Win32/Bancos | 14.4% |
| 3 | Win32/Conficker | 9.4% |
| 4 | HTML/IframeRef | 8.5% |
| 5 | Win32/Banload | 7.4% |
| 6 | Win32/Sality | 7.0% |
| 7 | JS/Pornpop | 6.7% |
| 8 | Dynamer | 5.6% |
| 9 | Win32/Keygen | 5.4% |
| 10 | Win32/Rimecud | 4.9% |

- The most common threat family in Brazil in 4Q10 was Win32/Autorun, which affected 20.3 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Brazil in 4Q10 was Win32/Bancos, which affected 14.4 percent of cleaned computers. Win32/Bancos is a data-stealing trojan that captures online banking credentials and relays them to the attacker. Most variants target customers of Brazilian banks.
- The third most common threat family in Brazil in 4Q10 was Win32/Conficker, which affected 9.4 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The fourth most common threat family in Brazil in 4Q10 was HTML/IframeRef, which affected 8.5 percent of cleaned computers. HTML/IframeRef is a generic detection for specially formed IFrame tags that point to remote websites containing malicious content.

# Brunei

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

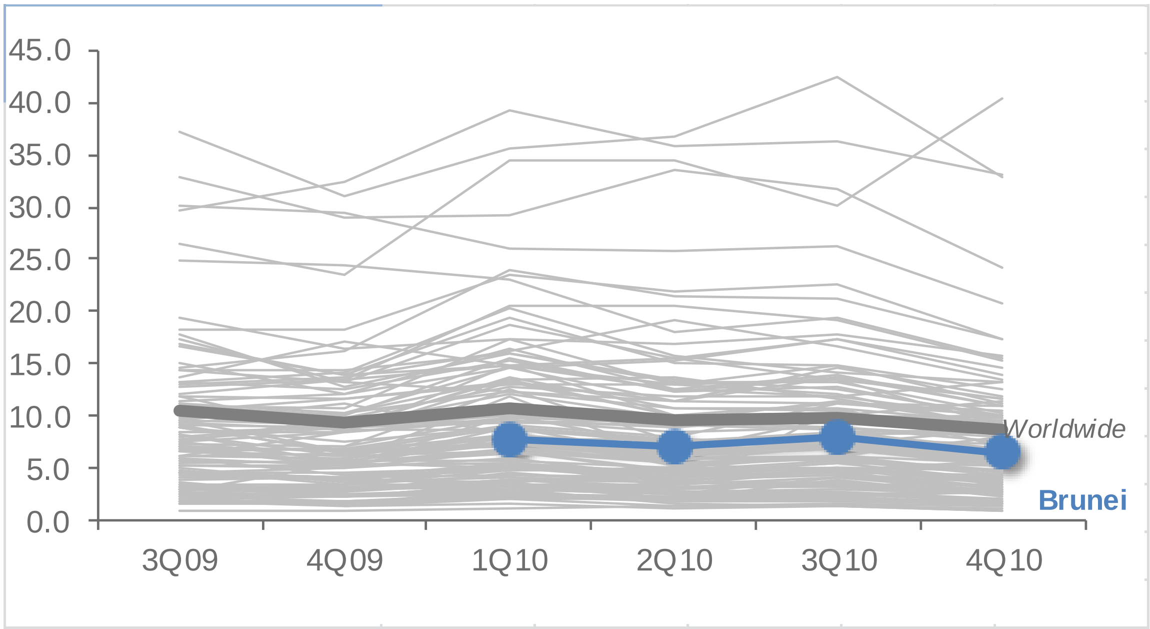
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Brunei in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Brunei and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 7.7 | 7.0 | 8.0 | 6.6 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | | | 0.54 | |
| Malware hosting sites per 1000 hosts | 0.40 | | 0.20 | |
| Percentage of sites hosting drive-by downloads | 0.000% | | | |

## Infection Trends (CCM)

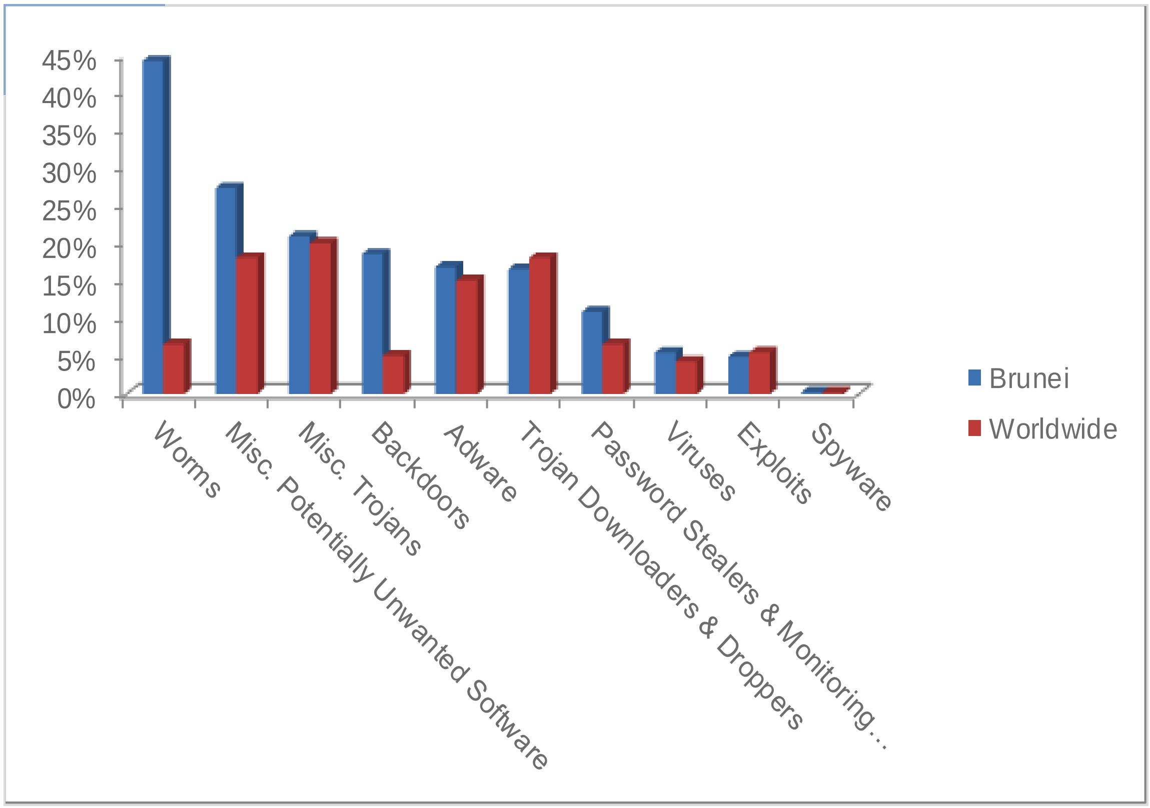
The MSRT detected malware on 6.6 of every 1,000 computers scanned in Brunei in 4Q10 (a CCM score of 6.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Brunei over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Brunei and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Brunei in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Brunei in 4Q10 was Worms, which affected 44.2 percent of all cleaned computers, down from 49.9 percent in 3Q10.
- The second most common category in Brunei in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.3 percent of all cleaned computers, up from 24.1 percent in 3Q10.
- The third most common category in Brunei in 4Q10 was Misc. Trojans, which affected 20.9 percent of all cleaned computers, down from 22.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Brunei in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 25.7% |
| 2 | Win32/Vobfus | 14.9% |
| 3 | Win32/IRCbot | 12.5% |
| 4 | Win32/Taterf | 11.7% |
| 5 | Win32/Conficker | 8.0% |
| 6 | JS/Pornpop | 7.6% |
| 7 | Win32/Frethog | 6.9% |
| 8 | Win32/Renos | 6.1% |
| 9 | Win32/Rimecud | 5.5% |
| 10 | Win32/ClickPotato | 4.7% |

- The most common threat family in Brunei in 4Q10 was Win32/Autorun, which affected 25.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Brunei in 4Q10 was Win32/Vobfus, which affected 14.9 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The third most common threat family in Brunei in 4Q10 was Win32/IRCbot, which affected 12.5 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The fourth most common threat family in Brunei in 4Q10 was Win32/Taterf, which affected 11.7 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Bulgaria

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

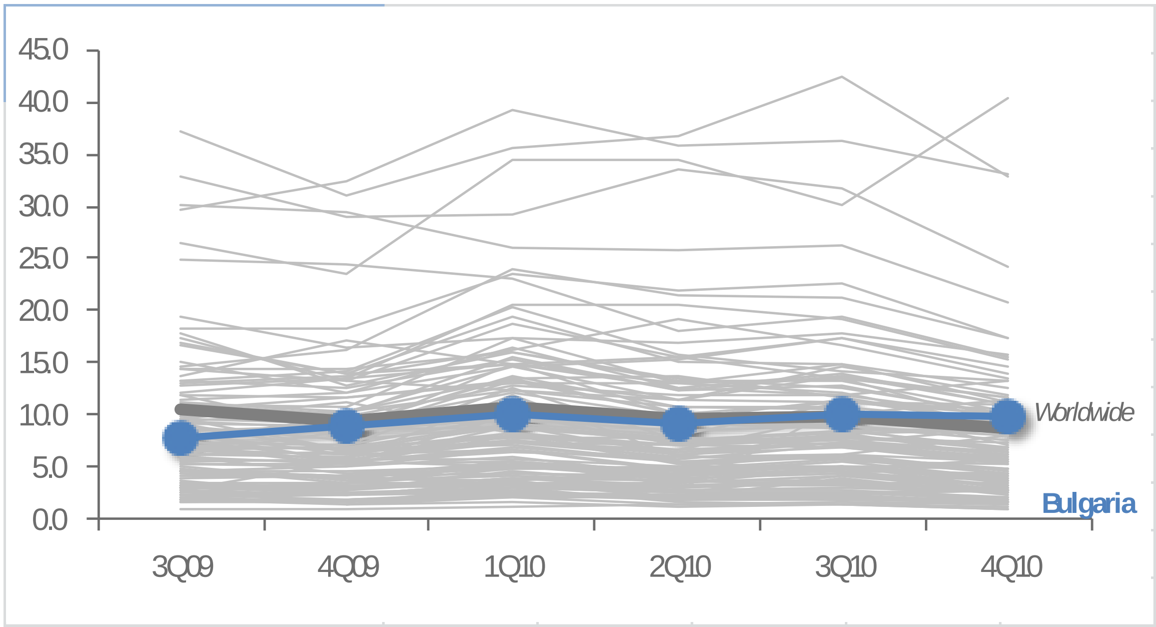
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Bulgaria in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Bulgaria and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 10.0 | 9.0 | 10.1 | 9.9 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 3.88 | | 1.47 | |
| Malware hosting sites per 1000 hosts | 5.09 | | 5.42 | |
| Percentage of sites hosting drive-by downloads | 0.194% | 0.047% | 0.032% | |

## Infection Trends (CCM)

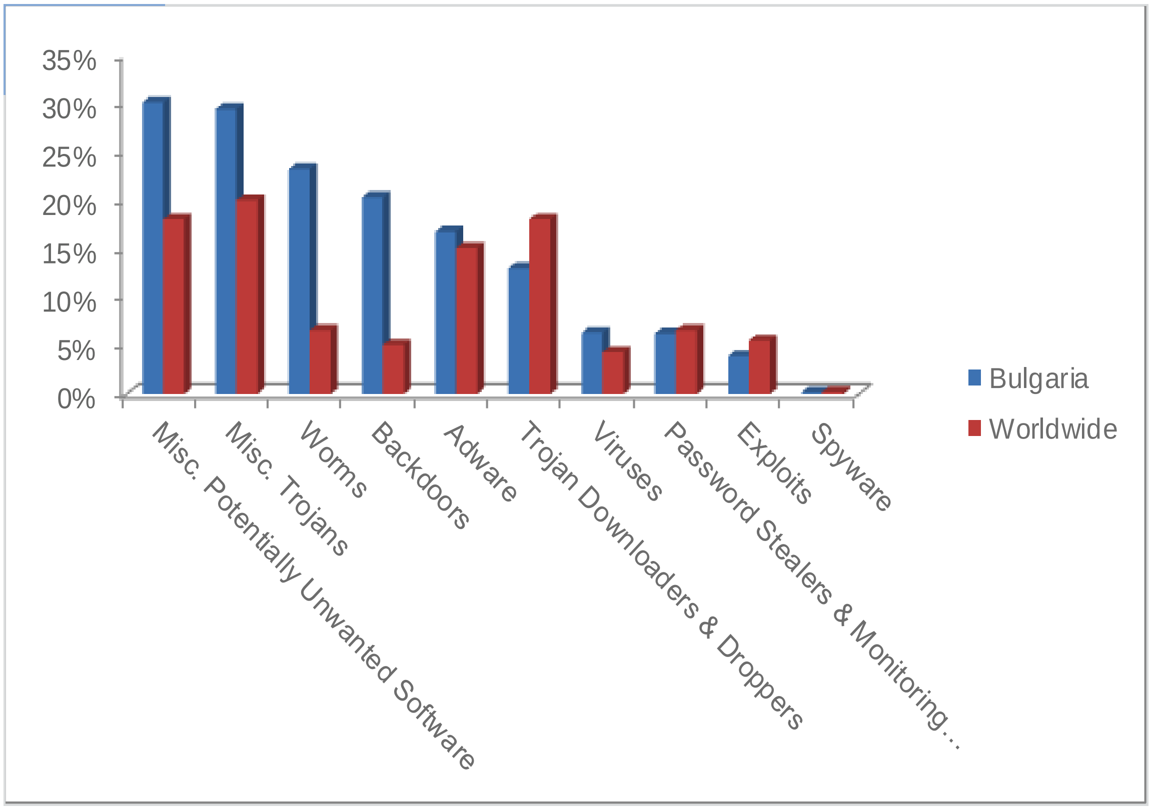
The MSRT detected malware on 9.9 of every 1,000 computers scanned in Bulgaria in 4Q10 (a CCM score of 9.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Bulgaria over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Bulgaria and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Bulgaria in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Bulgaria in 4Q10 was Misc. Potentially Unwanted Software, which affected 30.1 percent of all cleaned computers, down from 32.0 percent in 3Q10.
- The second most common category in Bulgaria in 4Q10 was Misc. Trojans, which affected 29.4 percent of all cleaned computers, down from 31.6 percent in 3Q10.
- The third most common category in Bulgaria in 4Q10 was Worms, which affected 23.2 percent of all cleaned computers, down from 31.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Bulgaria in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/IRCbot | 16.1% |
| 2 | JS/Pornpop | 11.2% |
| 3 | Win32/Autorun | 11.1% |
| 4 | Win32/Keygen | 9.9% |
| 5 | Win32/Rimecud | 7.9% |
| 6 | Win32/Conficker | 6.4% |
| 7 | Win32/Renos | 5.2% |
| 8 | Win32/Obfuscator | 3.9% |
| 9 | Win32/Taterf | 3.3% |
| 10 | Killav | 2.9% |

- The most common threat family in Bulgaria in 4Q10 was Win32/IRCbot, which affected 16.1 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The second most common threat family in Bulgaria in 4Q10 was JS/Pornpop, which affected 11.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Bulgaria in 4Q10 was Win32/Autorun, which affected 11.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common threat family in Bulgaria in 4Q10 was Win32/Keygen, which affected 9.9 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.

# Cameroon

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

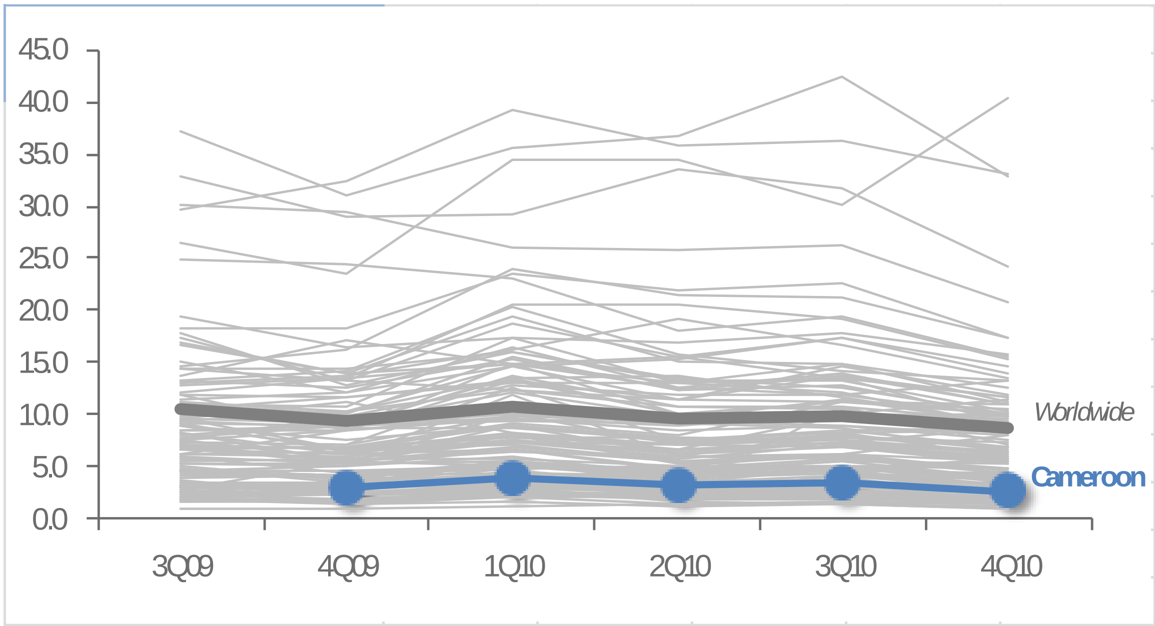
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Cameroon in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Cameroon and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">3.9</td><td colspan="3">3.2</td><td colspan="3">3.3</td><td colspan="3">2.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6"></td><td colspan="6">14.49</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">72.46</td><td colspan="6"></td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.000%</td><td colspan="4">0.072%</td><td colspan="4">0.016%</td></tr>
</table>

## Infection Trends (CCM)

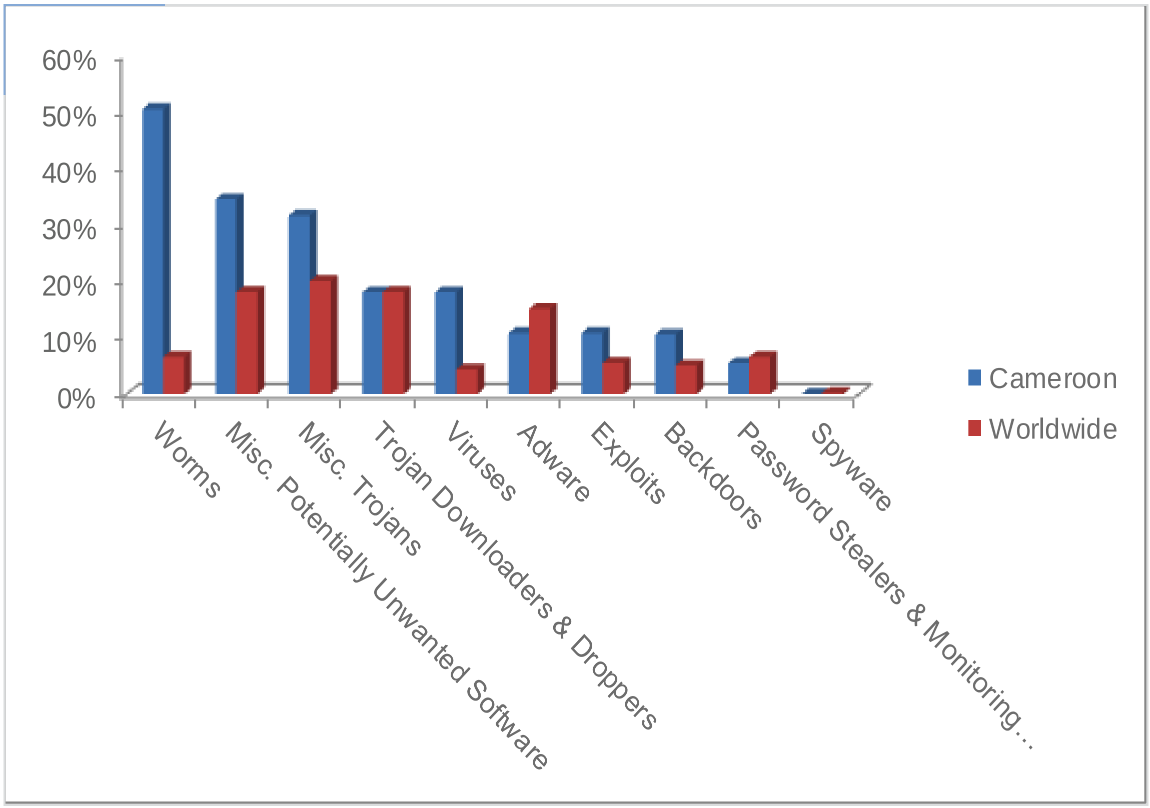
The MSRT detected malware on 2.8 of every 1,000 computers scanned in Cameroon in 4Q10 (a CCM score of 2.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Cameroon over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Cameroon and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Cameroon in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Cameroon in 4Q10 was Worms, which affected 50.4 percent of all cleaned computers, down from 55.9 percent in 3Q10.
- The second most common category in Cameroon in 4Q10 was Misc. Potentially Unwanted Software, which affected 34.5 percent of all cleaned computers, up from 30.5 percent in 3Q10.
- The third most common category in Cameroon in 4Q10 was Misc. Trojans, which affected 31.6 percent of all cleaned computers, up from 28.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Cameroon in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 28.1% |
| 2 | Win32/Rimecud | 22.5% |
| 3 | Win32/Vobfus | 21.9% |
| 4 | Win32/Sality | 9.5% |
| 5 | CplLnk | 8.0% |
| 6 | Win32/Mabezat | 7.7% |
| 7 | Win32/Renos | 7.5% |
| 8 | Win32/Conficker | 6.8% |
| 9 | Win32/Taterf | 6.4% |
| 10 | Win32/Virut | 5.3% |

- The most common threat family in Cameroon in 4Q10 was Win32/Autorun, which affected 28.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Cameroon in 4Q10 was Win32/Rimecud, which affected 22.5 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Cameroon in 4Q10 was Win32/Vobfus, which affected 21.9 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Cameroon in 4Q10 was Win32/Sality, which affected 9.5 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Canada

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

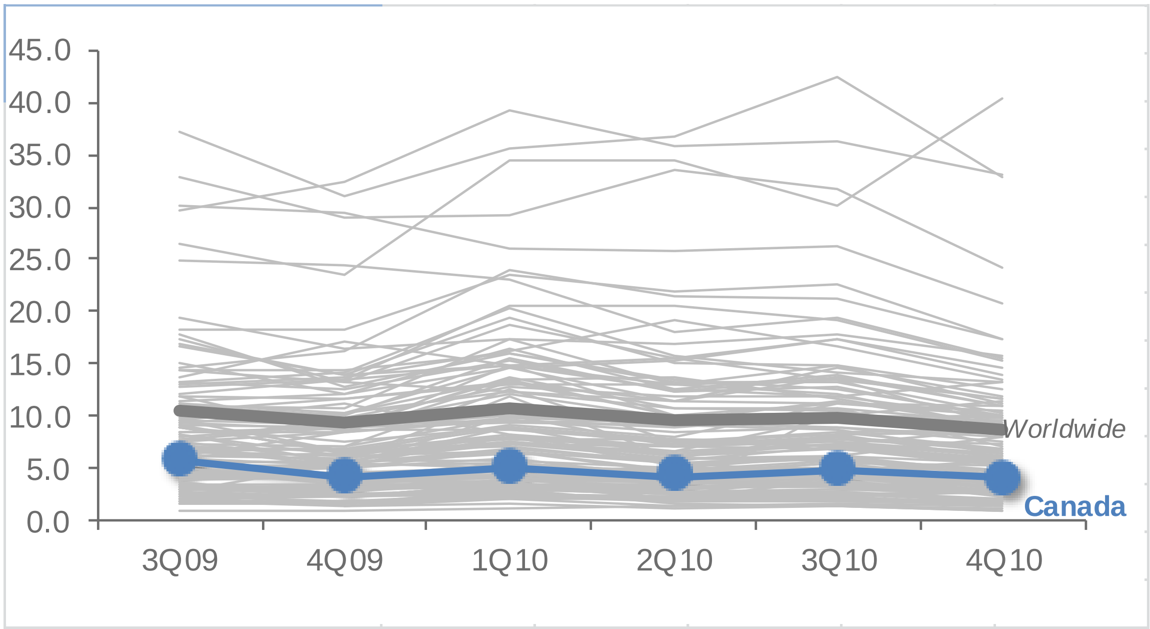
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Canada in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Canada and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 5.2 | 4.5 | 4.9 | 4.2 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 2.30 | | 2.47 | |
| Malware hosting sites per 1000 hosts | 3.73 | | 4.97 | |
| Percentage of sites hosting drive-by downloads | 0.151% | 0.040% | | 0.049% |

## Infection Trends (CCM)

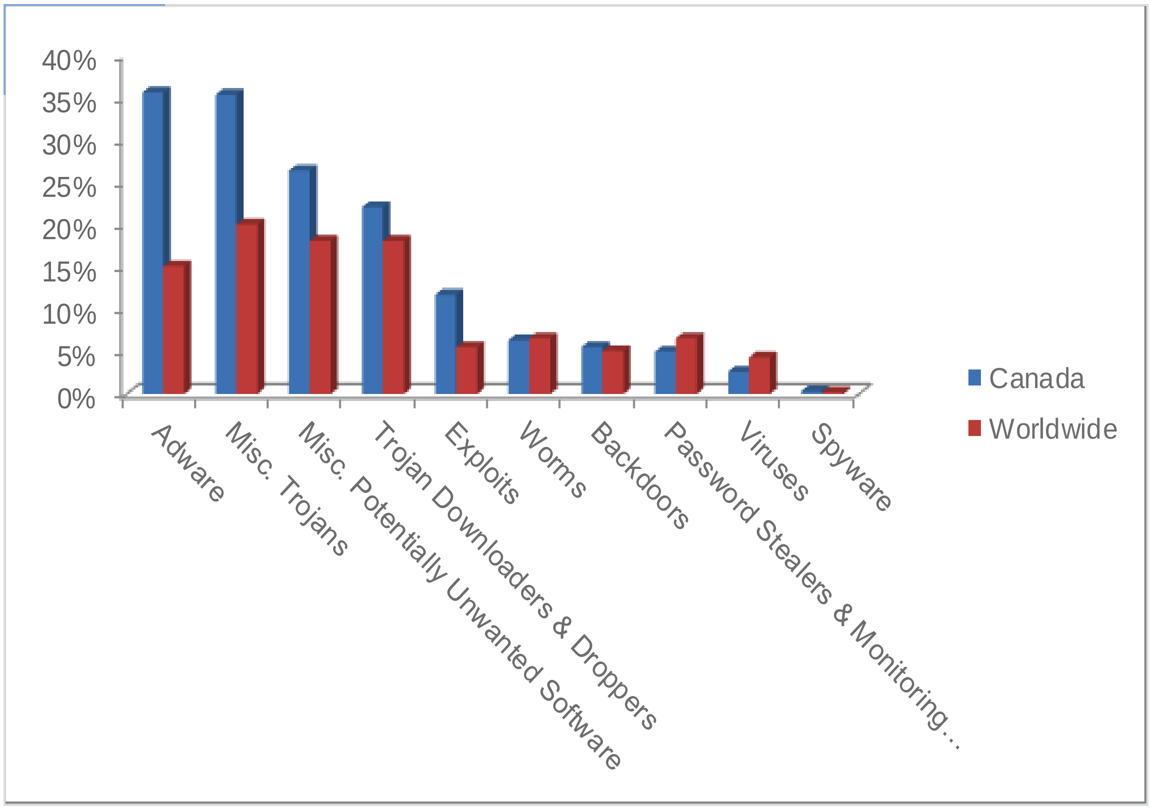
The MSRT detected malware on 4.2 of every 1,000 computers scanned in Canada in 4Q10 (a CCM score of 4.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Canada over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Canada and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Canada in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Canada in 4Q10 was Adware, which affected 35.6 percent of all cleaned computers, down from 41.0 percent in 3Q10.
- The second most common category in Canada in 4Q10 was Misc. Trojans, which affected 35.3 percent of all cleaned computers, up from 29.0 percent in 3Q10.
- The third most common category in Canada in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.3 percent of all cleaned computers, down from 26.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Canada in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 15.2% |
| 2 | Win32/ClickPotato | 12.6% |
| 3 | Win32/Zwangi | 11.0% |
| 4 | Win32/Hotbar | 7.4% |
| 5 | Java/CVE-2009-3867 | 5.9% |
| 6 | Java/CVE-2008-5353 | 5.8% |
| 7 | Win32/Renos | 5.3% |
| 8 | ASX/Wimad | 5.1% |
| 9 | Win32/FakeSpypro | 4.1% |
| 10 | Win32/Hiloti | 4.0% |

- The most common threat family in Canada in 4Q10 was JS/Pornpop, which affected 15.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Canada in 4Q10 was Win32/ClickPotato, which affected 12.6 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Canada in 4Q10 was Win32/Zwangi, which affected 11.0 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in Canada in 4Q10 was Win32/Hotbar, which affected 7.4 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

# Chile

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

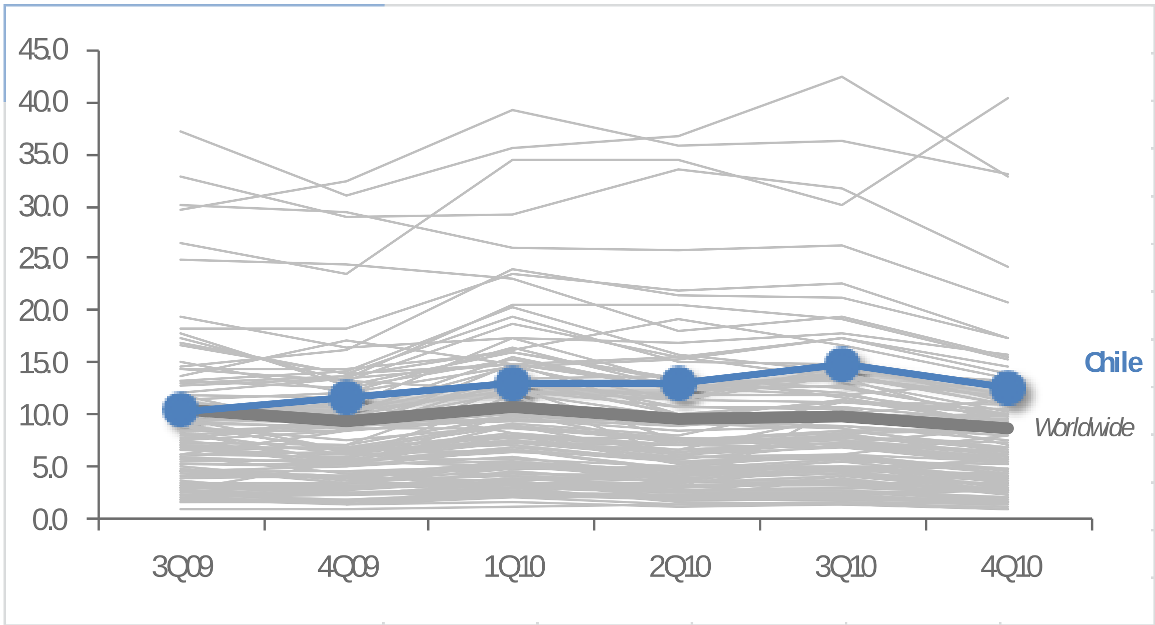
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Chile in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Chile and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 12.9 | 12.9 | 14.9 | 12.5 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.78 | | 0.47 | |
| Malware hosting sites per 1000 hosts | 0.33 | | 0.30 | |
| Percentage of sites hosting drive-by downloads | 0.195% | 0.084% | 0.069% | |

## Infection Trends (CCM)

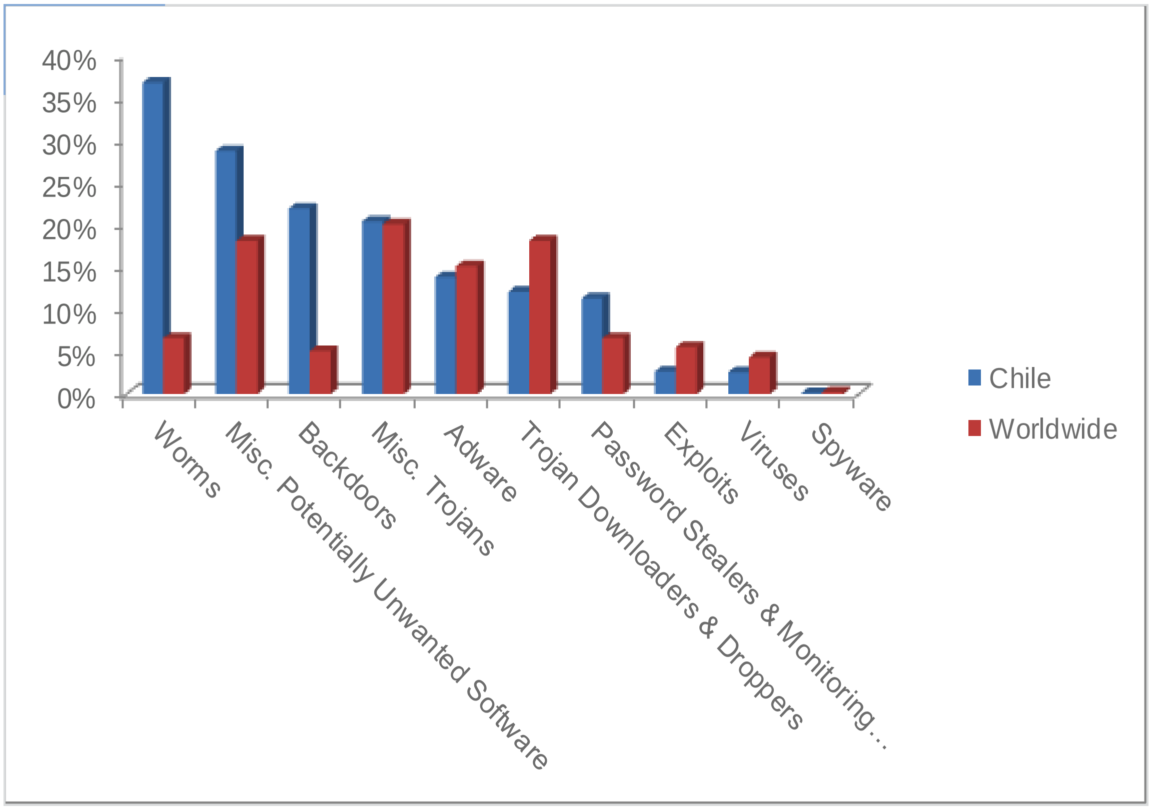
The MSRT detected malware on 12.5 of every 1,000 computers scanned in Chile in 4Q10 (a CCM score of 12.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Chile over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Chile and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Chile in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Chile in 4Q10 was Worms, which affected 36.7 percent of all cleaned computers, down from 40.1 percent in 3Q10.
- The second most common category in Chile in 4Q10 was Misc. Potentially Unwanted Software, which affected 28.7 percent of all cleaned computers, down from 28.7 percent in 3Q10.
- The third most common category in Chile in 4Q10 was Backdoors, which affected 21.9 percent of all cleaned computers, up from 19.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Chile in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 13.1% |
| 2 | Win32/Taterf | 11.4% |
| 3 | Win32/IRCbot | 11.1% |
| 4 | Win32/Rimecud | 9.4% |
| 5 | Sdbot | 8.8% |
| 6 | Win32/Frethog | 6.7% |
| 7 | Win32/Conficker | 5.9% |
| 8 | Win32/Zwangi | 5.2% |
| 9 | JS/Pornpop | 5.1% |
| 10 | Win32/Vobfus | 5.0% |

- The most common threat family in Chile in 4Q10 was Win32/Autorun, which affected 13.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Chile in 4Q10 was Win32/Taterf, which affected 11.4 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The third most common threat family in Chile in 4Q10 was Win32/IRCbot, which affected 11.1 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The fourth most common threat family in Chile in 4Q10 was Win32/Rimecud, which affected 9.4 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# China

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

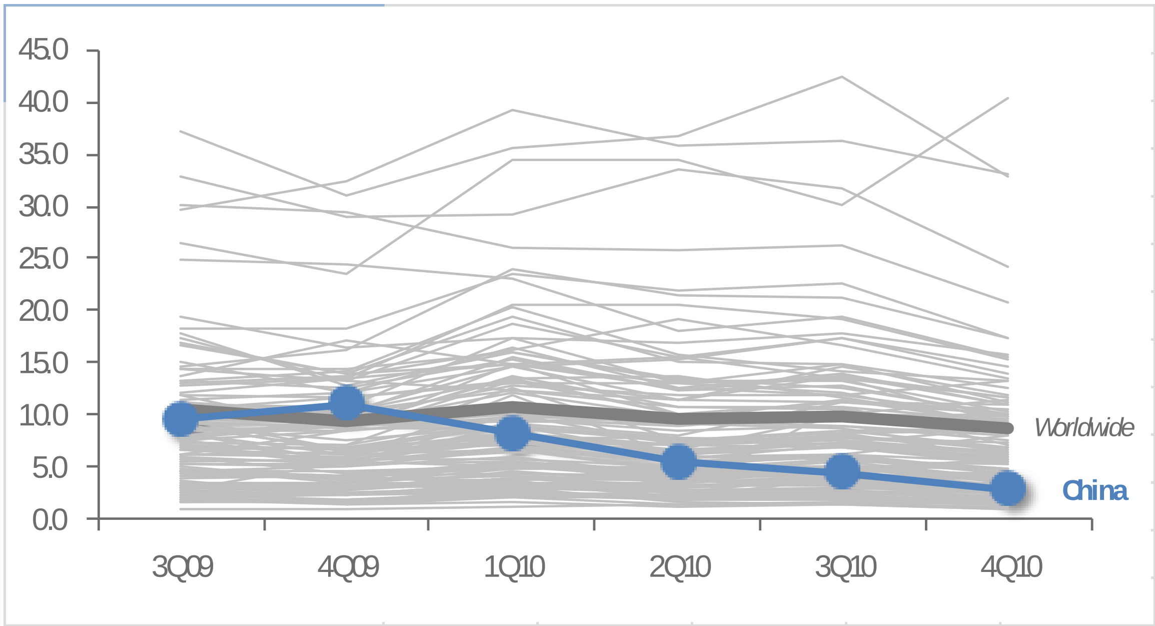
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in China in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in China and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">8.1</td><td colspan="3">5.5</td><td colspan="3">4.5</td><td colspan="3">2.9</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.20</td><td colspan="6">0.31</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">16.51</td><td colspan="6">40.28</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.667%</td><td colspan="4">0.243%</td><td colspan="4">0.214%</td></tr>
</table>

## Infection Trends (CCM)

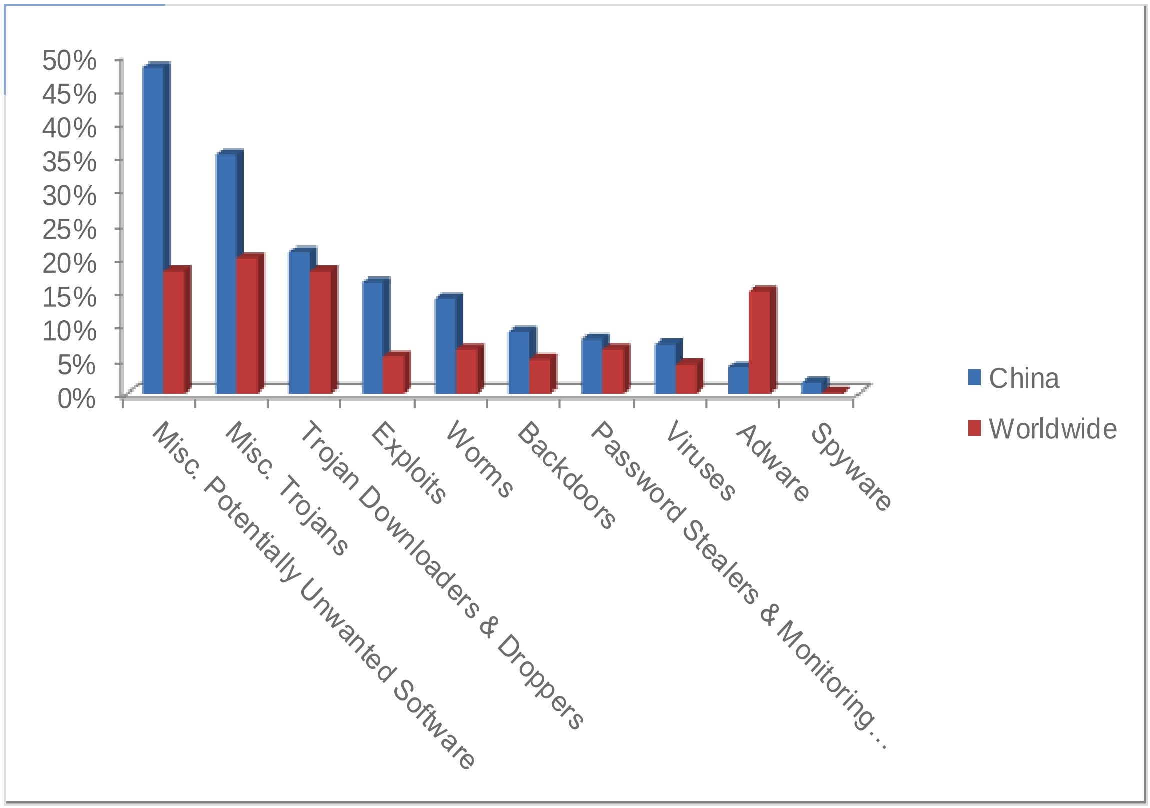
The MSRT detected malware on 2.9 of every 1,000 computers scanned in China in 4Q10 (a CCM score of 2.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for China over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in China and worldwide



## Threat Categories

Malware and potentially unwanted software categories in China in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in China in 4Q10 was Misc. Potentially Unwanted Software, which affected 48.1 percent of all cleaned computers, up from 44.1 percent in 3Q10.
- The second most common category in China in 4Q10 was Misc. Trojans, which affected 35.2 percent of all cleaned computers, up from 34.3 percent in 3Q10.
- The third most common category in China in 4Q10 was Trojan Downloaders & Droppers, which affected 20.9 percent of all cleaned computers, down from 26.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in China in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/BaiduSobar | 15.3% |
| 2 | JS/CVE-2010-0806 | 12.4% |
| 3 | JS/ShellCode | 11.5% |
| 4 | Win32/Sogou | 10.9% |
| 5 | Win32/Conficker | 6.9% |
| 6 | Win32/Jpgiframe | 6.4% |
| 7 | Win32/Obfuscator | 6.3% |
| 8 | Win32/Startpage | 5.7% |
| 9 | Newyx | 5.6% |
| 10 | Orsam | 5.5% |

- The most common threat family in China in 4Q10 was Win32/BaiduSobar, which affected 15.3 percent of cleaned computers. Win32/BaiduSobar is a Chinese-language Web browser toolbar that delivers pop-up and contextual advertisements, blocks certain other advertisements, and changes the Internet Explorer search page.
- The second most common threat family in China in 4Q10 was JS/CVE-2010-0806, which affected 12.4 percent of cleaned computers. JS/CVE-2010-0806 is a detection for malicious JavaScript that attempts to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-018.
- The third most common threat family in China in 4Q10 was JS/ShellCode, which affected 11.5 percent of cleaned computers. JS/ShellCode is a generic detection for JavaScript-enabled objects that contain exploit code and may exhibit suspicious behavior. Malicious websites and malformed PDF documents may contain JavaScript that attempts to execute code without the affected user's consent.
- The fourth most common threat family in China in 4Q10 was Win32/Sogou, which affected 10.9 percent of cleaned computers. Win32/Sogou is a Chinese-language browser toolbar that may display popup advertisements and may download and install additional components without user consent.

# Colombia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

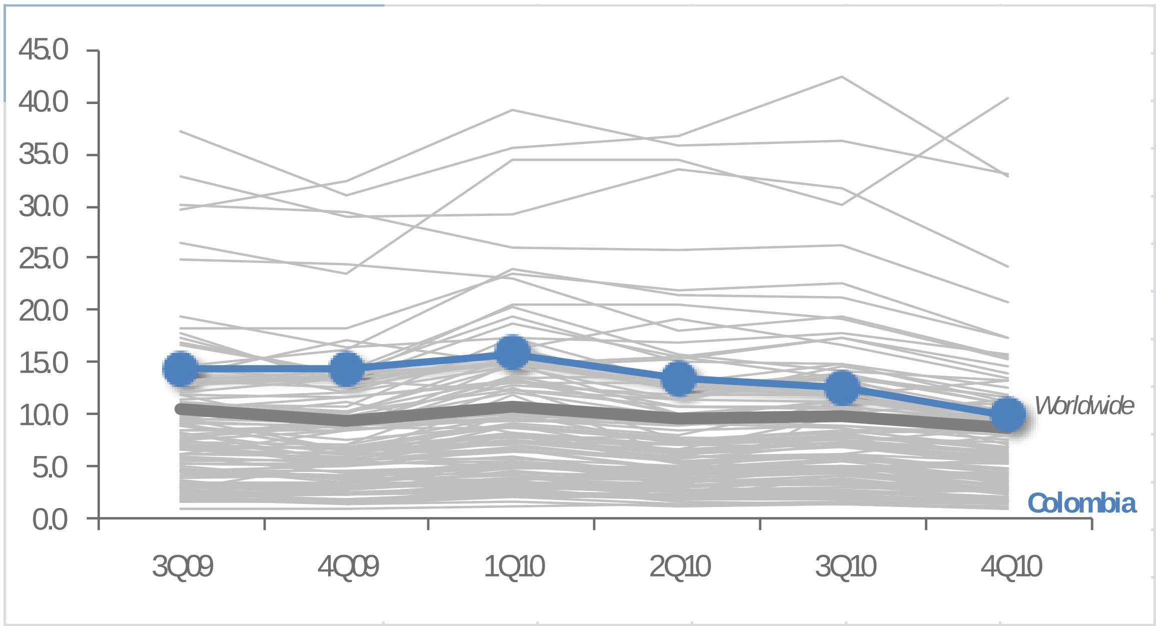
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Colombia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Colombia and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 16.0 | 13.5 | 12.6 | 10.0 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.29 | | 0.29 | |
| Malware hosting sites per 1000 hosts | 0.28 | | 0.52 | |
| Percentage of sites hosting drive-by downloads | 0.248% | 0.081% | 0.083% | |

## Infection Trends (CCM)

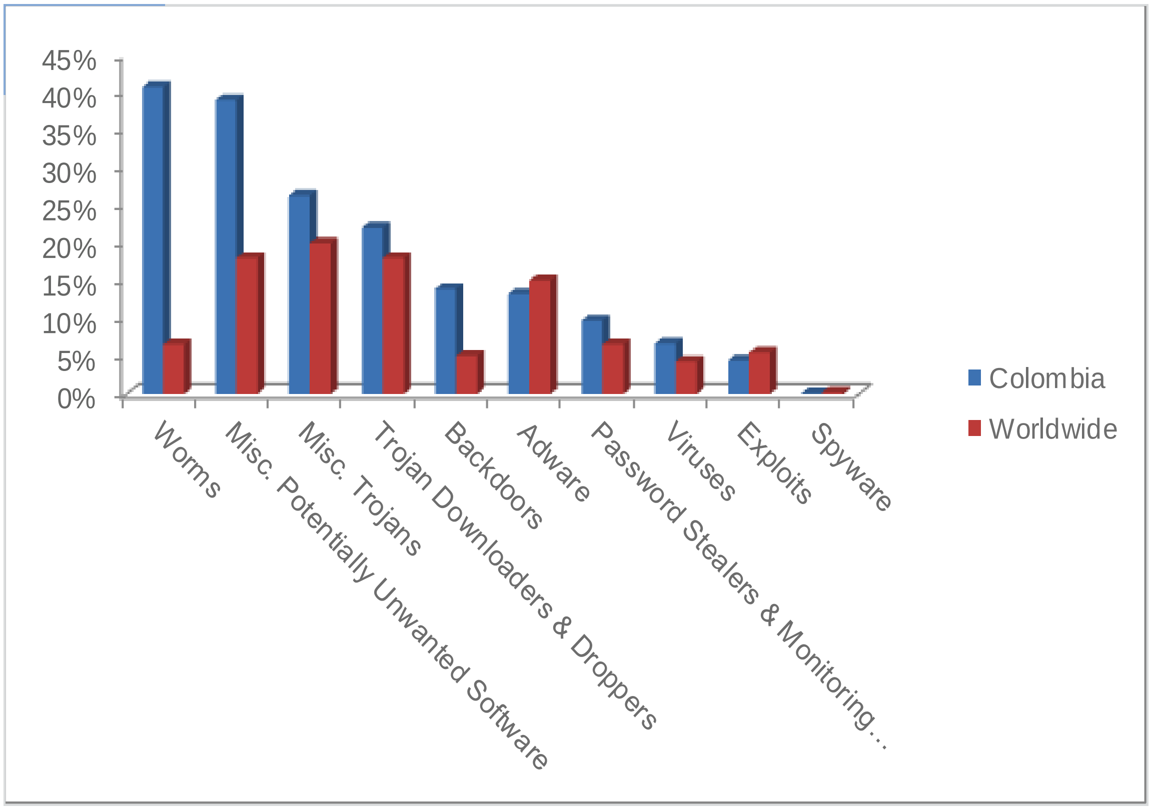
The MSRT detected malware on 10.0 of every 1,000 computers scanned in Colombia in 4Q10 (a CCM score of 10.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Colombia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Colombia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Colombia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Colombia in 4Q10 was Worms, which affected 40.8 percent of all cleaned computers, down from 46.0 percent in 3Q10.
- The second most common category in Colombia in 4Q10 was Misc. Potentially Unwanted Software, which affected 39.0 percent of all cleaned computers, down from 40.5 percent in 3Q10.
- The third most common category in Colombia in 4Q10 was Misc. Trojans, which affected 26.3 percent of all cleaned computers, up from 24.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Colombia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 23.9% |
| 2 | Win32/Rimecud | 14.1% |
| 3 | Win32/Conficker | 9.9% |
| 4 | Win32/IRCbot | 9.1% |
| 5 | Win32/Silly_P2P | 8.4% |
| 6 | Win32/Taterf | 7.8% |
| 7 | Nusump | 7.4% |
| 8 | JS/Pornpop | 7.1% |
| 9 | Win32/Keygen | 7.0% |
| 10 | Win32/VBInject | 6.8% |

- The most common threat family in Colombia in 4Q10 was Win32/Autorun, which affected 23.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Colombia in 4Q10 was Win32/Rimecud, which affected 14.1 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Colombia in 4Q10 was Win32/Conficker, which affected 9.9 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The fourth most common threat family in Colombia in 4Q10 was Win32/IRCbot, which affected 9.1 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.

# Costa Rica

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

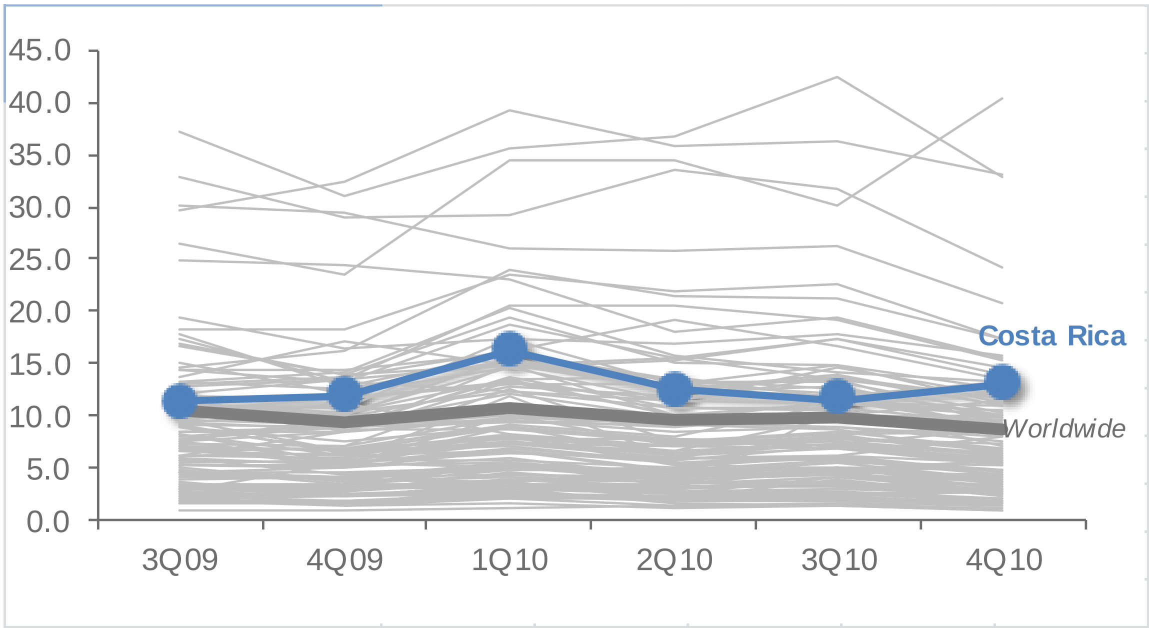
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Costa Rica in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Costa Rica and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 16.4 | 12.6 | 11.9 | 13.2 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.67 | | 0.18 | |
| Malware hosting sites per 1000 hosts | 0.91 | | 0.91 | |
| Percentage of sites hosting drive-by downloads | 0.014% | | | 0.060% |

## Infection Trends (CCM)

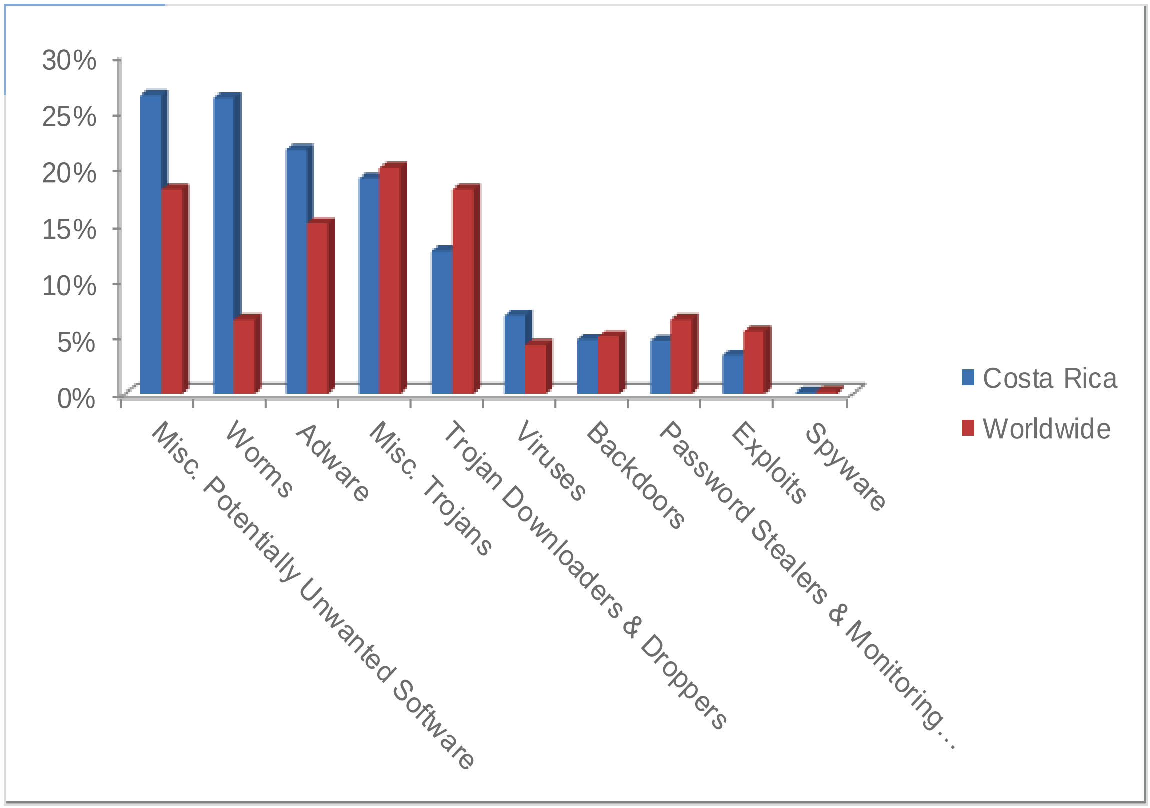
The MSRT detected malware on 13.2 of every 1,000 computers scanned in Costa Rica in 4Q10 (a CCM score of 13.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Costa Rica over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Costa Rica and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Costa Rica in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Costa Rica in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.4 percent of all cleaned computers, down from 50.5 percent in 3Q10.
- The second most common category in Costa Rica in 4Q10 was Worms, which affected 26.2 percent of all cleaned computers, down from 36.5 percent in 3Q10.
- The third most common category in Costa Rica in 4Q10 was Adware, which affected 21.6 percent of all cleaned computers, down from 23.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Costa Rica in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 13.3% |
| 2 | Win32/Autorun | 11.3% |
| 3 | Win32/Conficker | 10.7% |
| 4 | Win32/Zwangi | 6.6% |
| 5 | Win32/Rimecud | 6.1% |
| 6 | Win32/Hotbar | 3.8% |
| 7 | Win32/Renos | 3.7% |
| 8 | Win32/Sality | 3.6% |
| 9 | Win32/Taterf | 3.2% |
| 10 | Win32/Vobfus | 3.2% |

- The most common threat family in Costa Rica in 4Q10 was JS/Pornpop, which affected 13.3 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Costa Rica in 4Q10 was Win32/Autorun, which affected 11.3 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Costa Rica in 4Q10 was Win32/Conficker, which affected 10.7 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The fourth most common threat family in Costa Rica in 4Q10 was Win32/Zwangi, which affected 6.6 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Croatia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

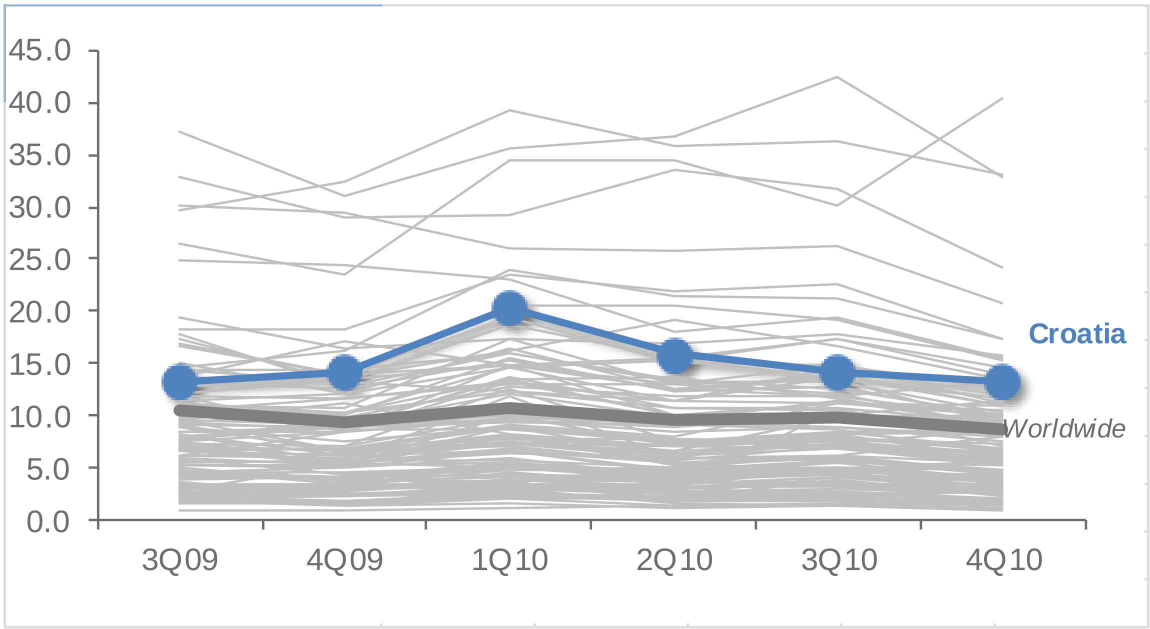
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Croatia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Croatia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">20.4</td><td colspan="3">15.8</td><td colspan="3">14.1</td><td colspan="3">13.4</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.04</td><td colspan="6">0.03</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.11</td><td colspan="6">0.15</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.207%</td><td colspan="4">0.069%</td><td colspan="4">0.080%</td></tr>
</table>

## Infection Trends (CCM)

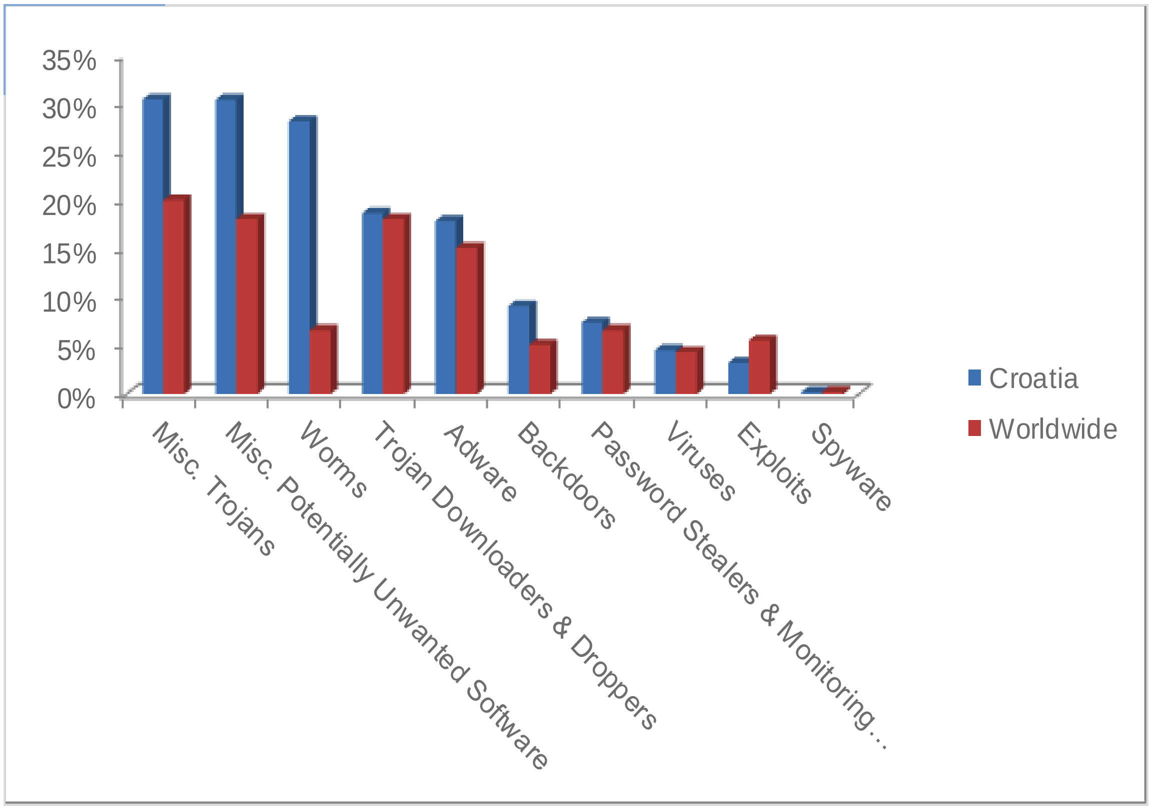
The MSRT detected malware on 13.4 of every 1,000 computers scanned in Croatia in 4Q10 (a CCM score of 13.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Croatia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Croatia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Croatia in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Croatia in 4Q10 was Misc. Trojans, which affected 30.4 percent of all cleaned computers, down from 32.6 percent in 3Q10.
- The second most common category in Croatia in 4Q10 was Misc. Potentially Unwanted Software, which affected 30.4 percent of all cleaned computers, up from 28.6 percent in 3Q10.
- The third most common category in Croatia in 4Q10 was Worms, which affected 28.1 percent of all cleaned computers, up from 25.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Croatia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 12.5% |
| 2 | Win32/Autorun | 11.3% |
| 3 | JS/Pornpop | 11.0% |
| 4 | Win32/Renos | 7.2% |
| 5 | Win32/Keygen | 6.7% |
| 6 | Win32/IRCbot | 5.2% |
| 7 | Win32/Conficker | 4.8% |
| 8 | Win32/Taterf | 4.0% |
| 9 | Win32/Zwangi | 3.5% |
| 10 | Win32/Obfuscator | 3.5% |

- The most common threat family in Croatia in 4Q10 was Win32/Rimecud, which affected 12.5 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Croatia in 4Q10 was Win32/Autorun, which affected 11.3 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Croatia in 4Q10 was JS/Pornpop, which affected 11.0 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Croatia in 4Q10 was Win32/Renos, which affected 7.2 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.

# Cyprus

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

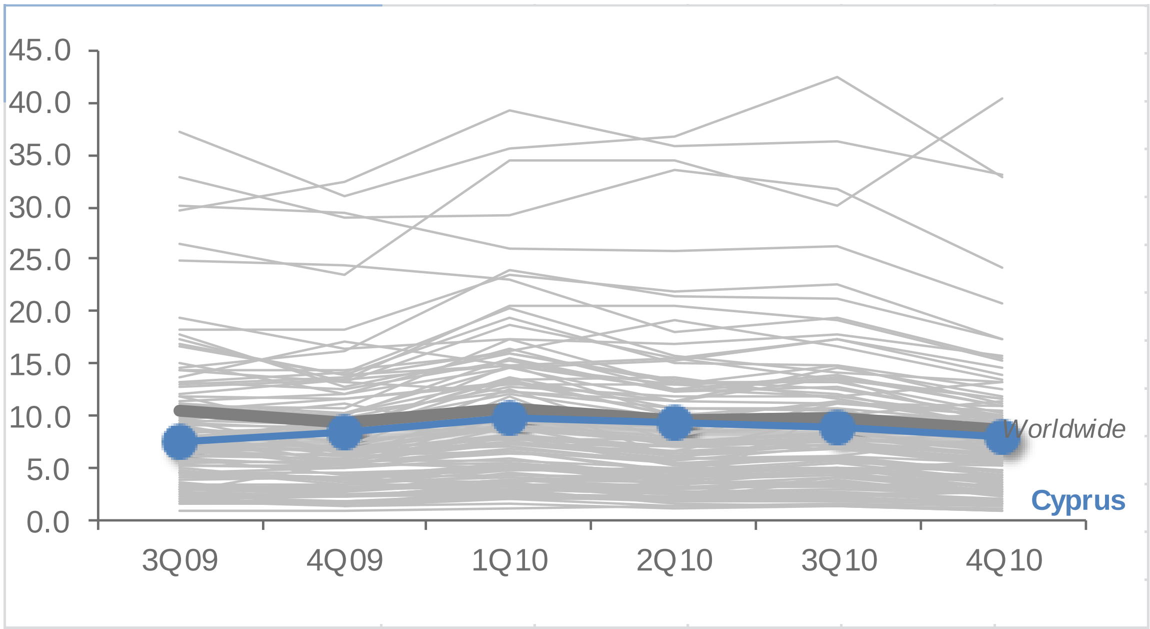
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Cyprus in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Cyprus and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">9.9</td><td colspan="3">9.3</td><td colspan="3">9.0</td><td colspan="3">7.9</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.09</td><td colspan="6">0.14</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">64.27</td><td colspan="6">49.17</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.180%</td><td colspan="4">0.027%</td><td colspan="4"></td></tr>
</table>

## Infection Trends (CCM)

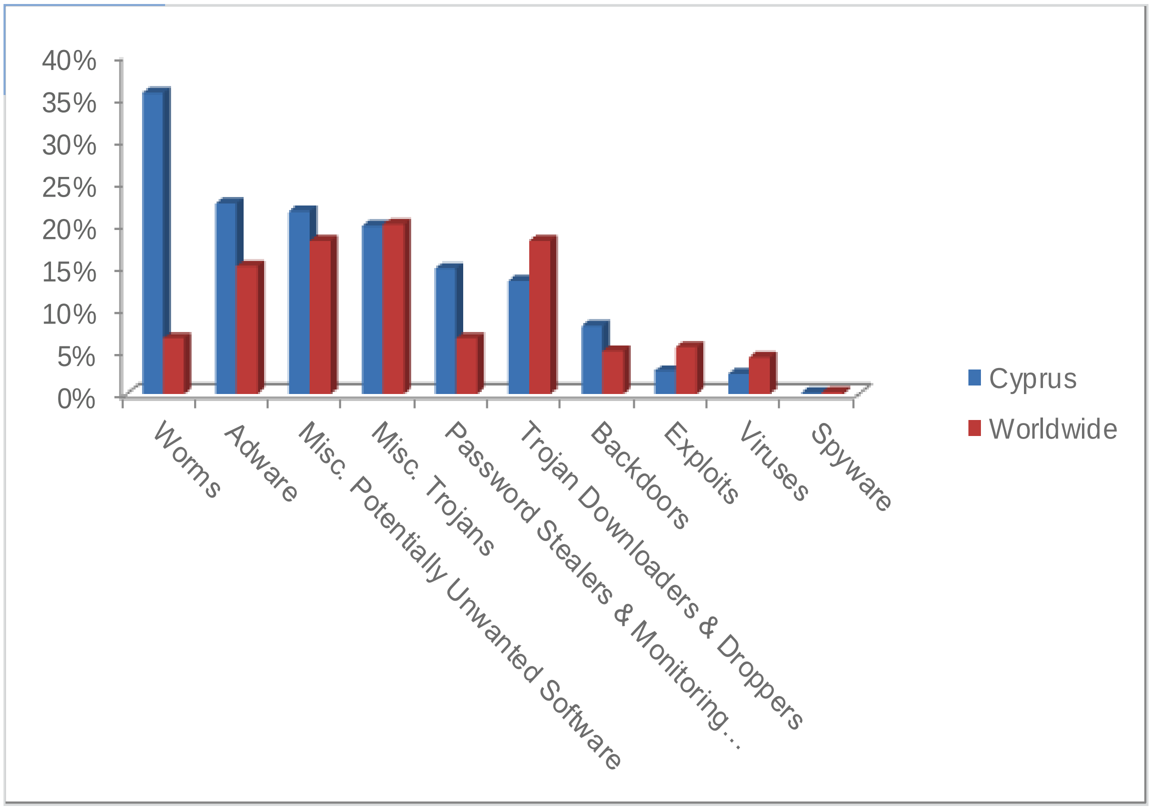
The MSRT detected malware on 7.9 of every 1,000 computers scanned in Cyprus in 4Q10 (a CCM score of 7.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Cyprus over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Cyprus and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Cyprus in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Cyprus in 4Q10 was Worms, which affected 35.5 percent of all cleaned computers, down from 41.9 percent in 3Q10.
- The second most common category in Cyprus in 4Q10 was Adware, which affected 22.5 percent of all cleaned computers, up from 20.5 percent in 3Q10.
- The third most common category in Cyprus in 4Q10 was Misc. Potentially Unwanted Software, which affected 21.6 percent of all cleaned computers, up from 17.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Cyprus in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Taterf | 14.6% |
| 2 | Win32/Frethog | 9.7% |
| 3 | Win32/Rimecud | 8.7% |
| 4 | JS/Pornpop | 8.2% |
| 5 | Win32/Autorun | 7.9% |
| 6 | Win32/Zwangi | 7.2% |
| 7 | Win32/ClickPotato | 7.2% |
| 8 | Win32/Hotbar | 5.8% |
| 9 | Win32/Conficker | 5.7% |
| 10 | Win32/IRCbot | 5.1% |

- The most common threat family in Cyprus in 4Q10 was Win32/Taterf, which affected 14.6 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The second most common threat family in Cyprus in 4Q10 was Win32/Frethog, which affected 9.7 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.
- The third most common threat family in Cyprus in 4Q10 was Win32/Rimecud, which affected 8.7 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Cyprus in 4Q10 was JS/Pornpop, which affected 8.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Czech Republic

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

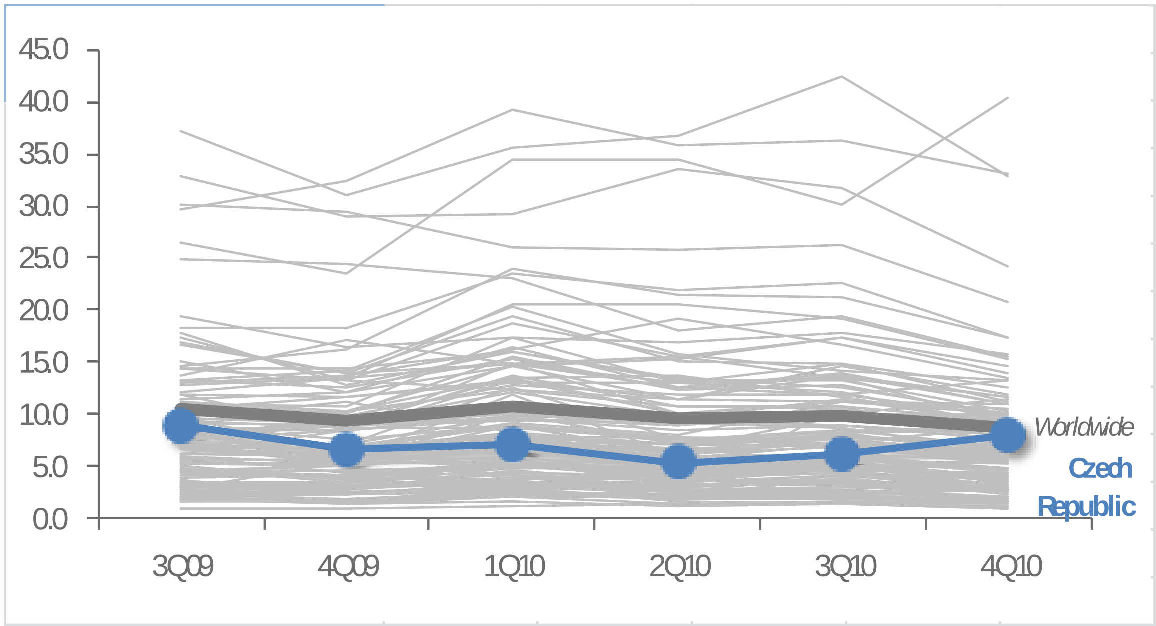
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Czech Republic in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Czech Republic and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">7.1</td><td colspan="3">5.5</td><td colspan="3">6.2</td><td colspan="3">8.0</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.89</td><td colspan="6">0.52</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">4.60</td><td colspan="6">13.36</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.248%</td><td colspan="4">0.127%</td><td colspan="4">0.107%</td></tr>
</table>

## Infection Trends (CCM)

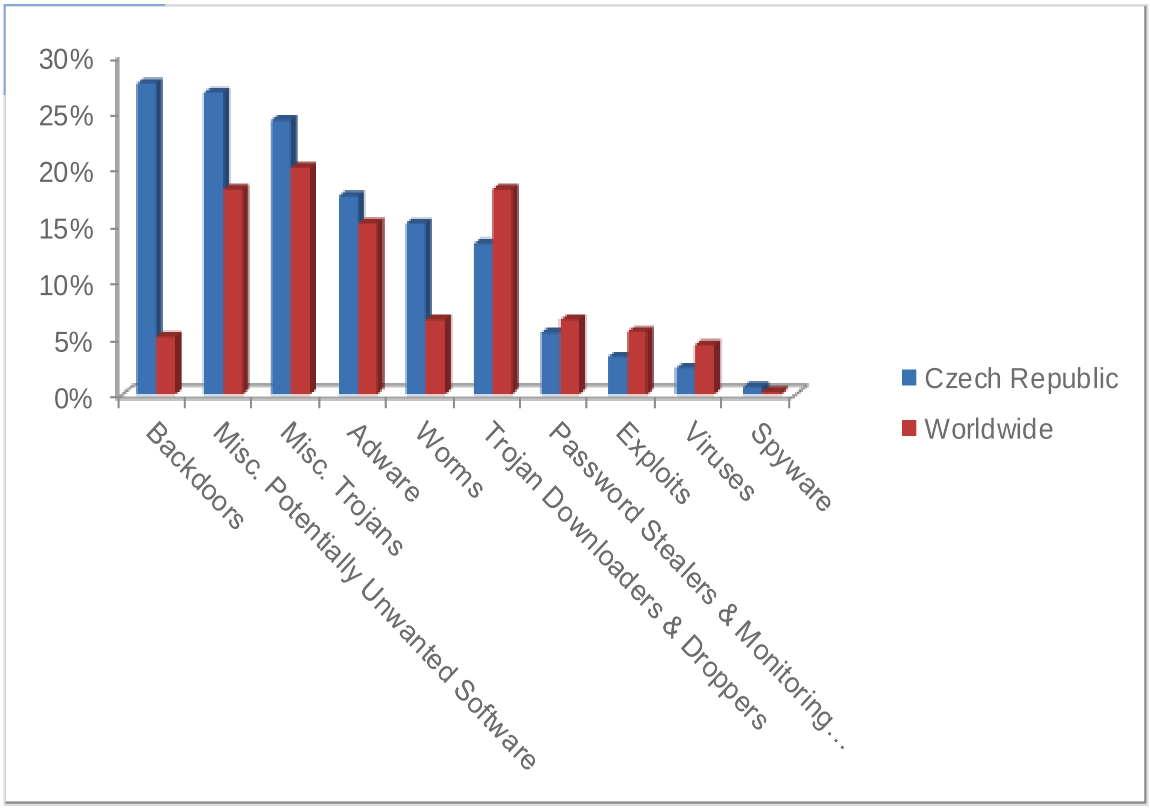
The MSRT detected malware on 8.0 of every 1,000 computers scanned in Czech Republic in 4Q10 (a CCM score of 8.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Czech Republic over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Czech Republic and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Czech Republic in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Czech Republic in 4Q10 was Backdoors, which affected 27.4 percent of all cleaned computers, down from 31.9 percent in 3Q10.
- The second most common category in Czech Republic in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.6 percent of all cleaned computers, down from 29.8 percent in 3Q10.
- The third most common category in Czech Republic in 4Q10 was Misc. Trojans, which affected 24.2 percent of all cleaned computers, up from 21.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Czech Republic in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/IRCbot | 24.3% |
| 2 | JS/Pornpop | 11.4% |
| 3 | Win32/Keygen | 7.6% |
| 4 | Win32/Renos | 5.5% |
| 5 | Win32/Autorun | 5.4% |
| 6 | Win32/Obfuscator | 4.3% |
| 7 | Win32/Slenfbot | 4.3% |
| 8 | Win32/Rimecud | 3.6% |
| 9 | Win32/Conficker | 3.3% |
| 10 | Bumat | 2.3% |

- The most common threat family in Czech Republic in 4Q10 was Win32/IRCbot, which affected 24.3 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The second most common threat family in Czech Republic in 4Q10 was JS/Pornpop, which affected 11.4 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Czech Republic in 4Q10 was Win32/Keygen, which affected 7.6 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.
- The fourth most common threat family in Czech Republic in 4Q10 was Win32/Renos, which affected 5.5 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.

# Denmark

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

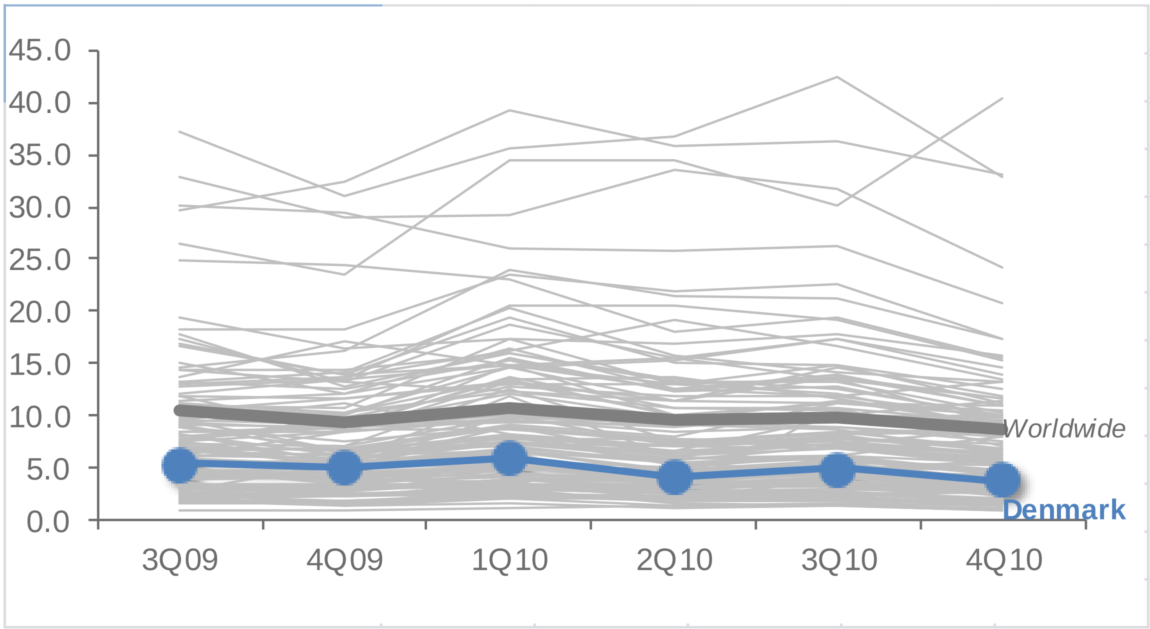
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Denmark in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Denmark and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 6.0 | 4.1 | 4.9 | 3.9 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.32 | | 0.49 | |
| Malware hosting sites per 1000 hosts | 0.41 | | 0.51 | |
| Percentage of sites hosting drive-by downloads | 0.140% | 0.042% | 0.037% | |

## Infection Trends (CCM)

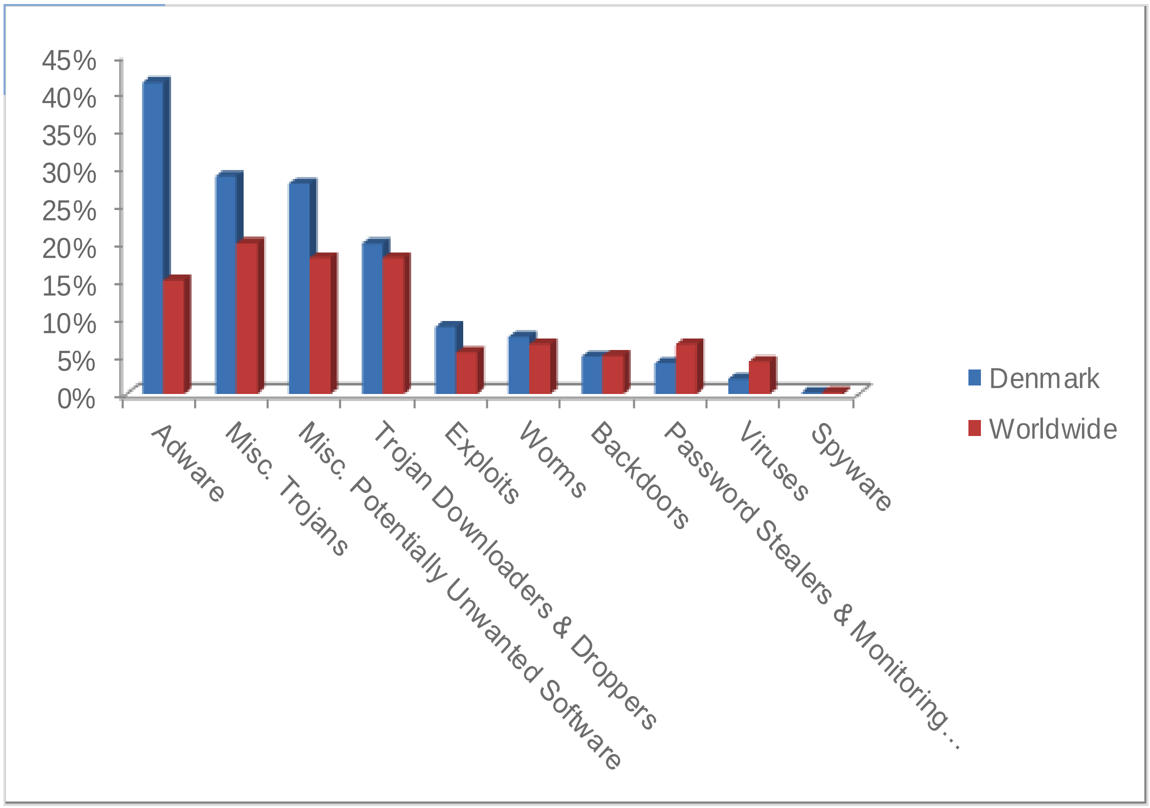
The MSRT detected malware on 3.9 of every 1,000 computers scanned in Denmark in 4Q10 (a CCM score of 3.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Denmark over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Denmark and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Denmark in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Denmark in 4Q10 was Adware, which affected 41.4 percent of all cleaned computers, up from 32.4 percent in 3Q10.
- The second most common category in Denmark in 4Q10 was Misc. Trojans, which affected 28.9 percent of all cleaned computers, down from 31.1 percent in 3Q10.
- The third most common category in Denmark in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.9 percent of all cleaned computers, up from 27.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Denmark in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 27.8% |
| 2 | Win32/ClickPotato | 7.9% |
| 3 | Win32/Renos | 7.1% |
| 4 | Win32/Zwangi | 6.8% |
| 5 | Win32/Keygen | 5.5% |
| 6 | Win32/Hotbar | 5.1% |
| 7 | Java/CVE-2009-3867 | 4.7% |
| 8 | Java/CVE-2008-5353 | 4.1% |
| 9 | Win32/Obfuscator | 3.6% |
| 10 | ASX/Wimad | 3.5% |

- The most common threat family in Denmark in 4Q10 was JS/Pornpop, which affected 27.8 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Denmark in 4Q10 was Win32/ClickPotato, which affected 7.9 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Denmark in 4Q10 was Win32/Renos, which affected 7.1 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.
- The fourth most common threat family in Denmark in 4Q10 was Win32/Zwangi, which affected 6.8 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Dominican Republic

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

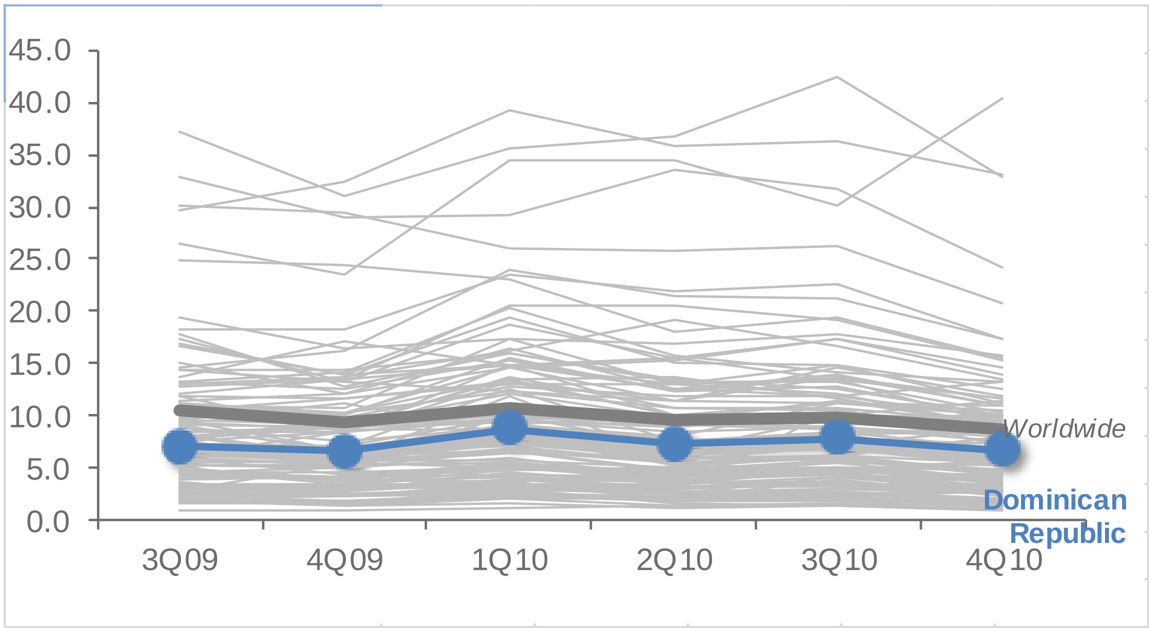
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Dominican Republic in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Dominican Republic and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 8.9 | 7.4 | 7.9 | 6.9 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 2.01 | | 0.11 | |
| Malware hosting sites per 1000 hosts | 0.11 | | 0.12 | |
| Percentage of sites hosting drive-by downloads | 0.214% | 0.041% | 0.078% | |

## Infection Trends (CCM)

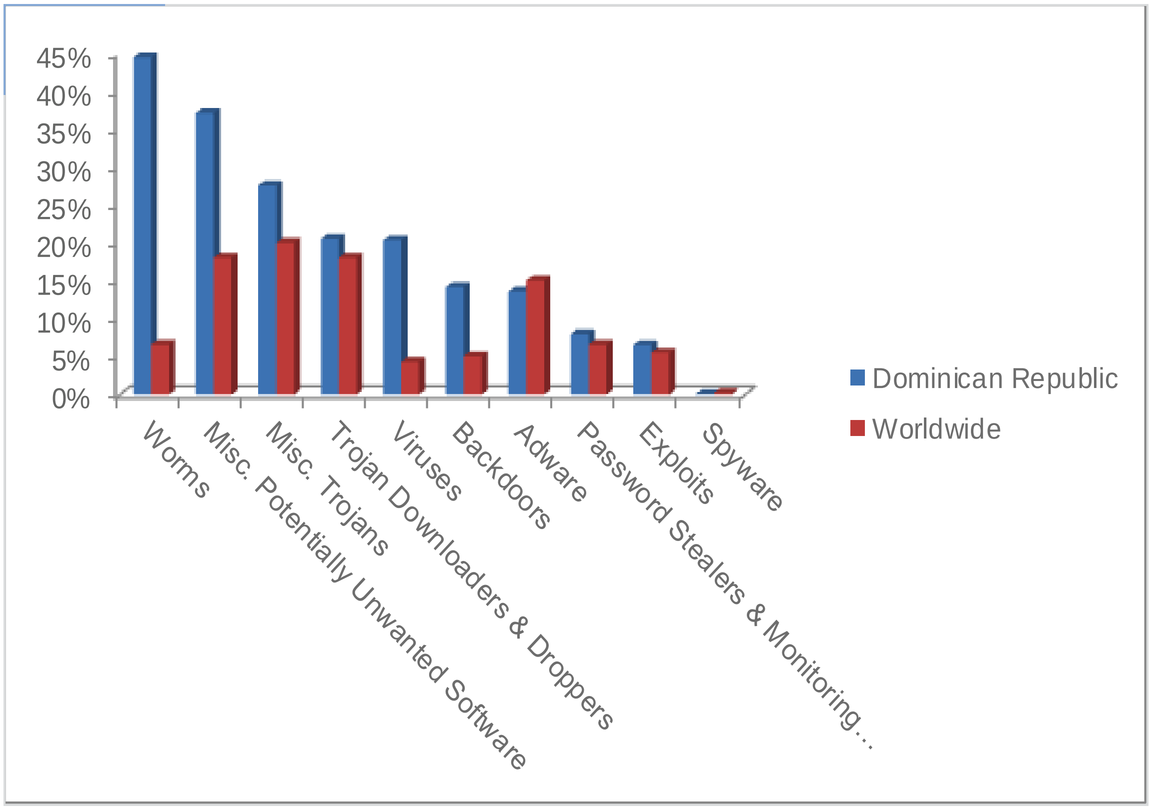
The MSRT detected malware on 6.9 of every 1,000 computers scanned in Dominican Republic in 4Q10 (a CCM score of 6.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Dominican Republic over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Dominican Republic and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Dominican Republic in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Dominican Republic in 4Q10 was Worms, which affected 44.5 percent of all cleaned computers, down from 48.6 percent in 3Q10.
- The second most common category in Dominican Republic in 4Q10 was Misc. Potentially Unwanted Software, which affected 37.1 percent of all cleaned computers, up from 35.6 percent in 3Q10.
- The third most common category in Dominican Republic in 4Q10 was Misc. Trojans, which affected 27.6 percent of all cleaned computers, up from 25.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Dominican Republic in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 24.8% |
| 2 | Win32/Sality | 19.2% |
| 3 | Win32/Rimecud | 16.2% |
| 4 | Win32/Vobfus | 11.6% |
| 5 | Win32/IRCbot | 8.7% |
| 6 | Win32/Silly_P2P | 7.9% |
| 7 | Win32/Taterf | 7.7% |
| 8 | Win32/Brontok | 6.3% |
| 9 | Win32/Hamweq | 5.3% |
| 10 | Win32/Keygen | 5.0% |

- The most common threat family in Dominican Republic in 4Q10 was Win32/Autorun, which affected 24.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Dominican Republic in 4Q10 was Win32/Sality, which affected 19.2 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family in Dominican Republic in 4Q10 was Win32/Rimecud, which affected 16.2 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Dominican Republic in 4Q10 was Win32/Vobfus, which affected 11.6 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

# Ecuador

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

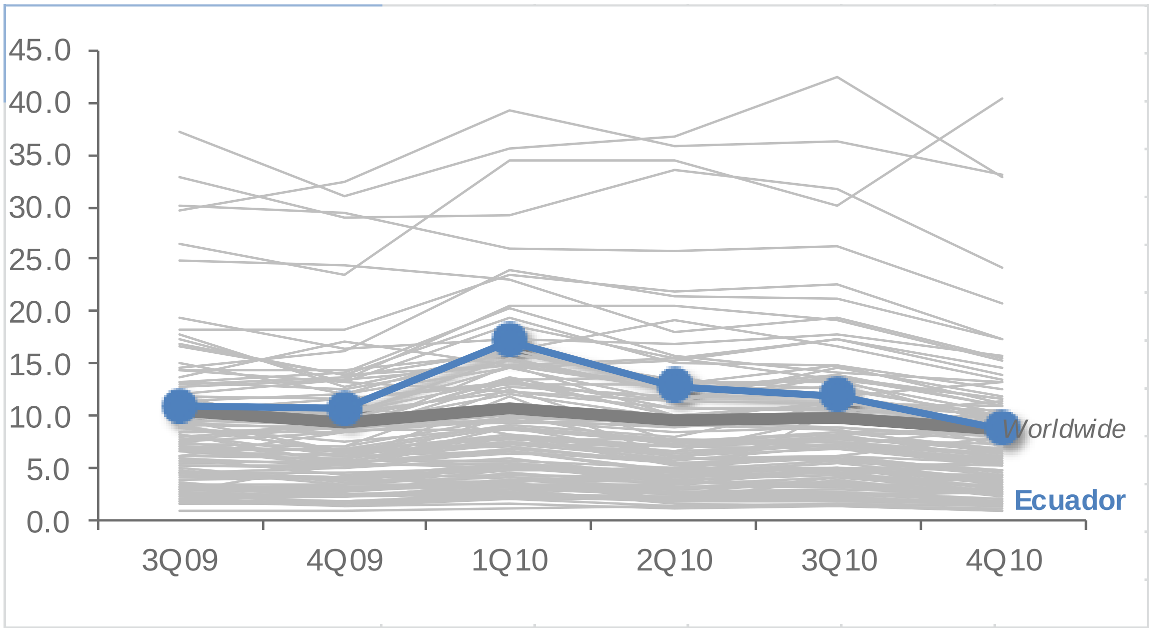
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Ecuador in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Ecuador and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">17.3</td><td colspan="3">12.9</td><td colspan="3">12.0</td><td colspan="3">8.9</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.79</td><td colspan="6">1.34</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.29</td><td colspan="6">0.48</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.130%</td><td colspan="4">0.115%</td><td colspan="4">0.081%</td></tr>
</table>

## Infection Trends (CCM)

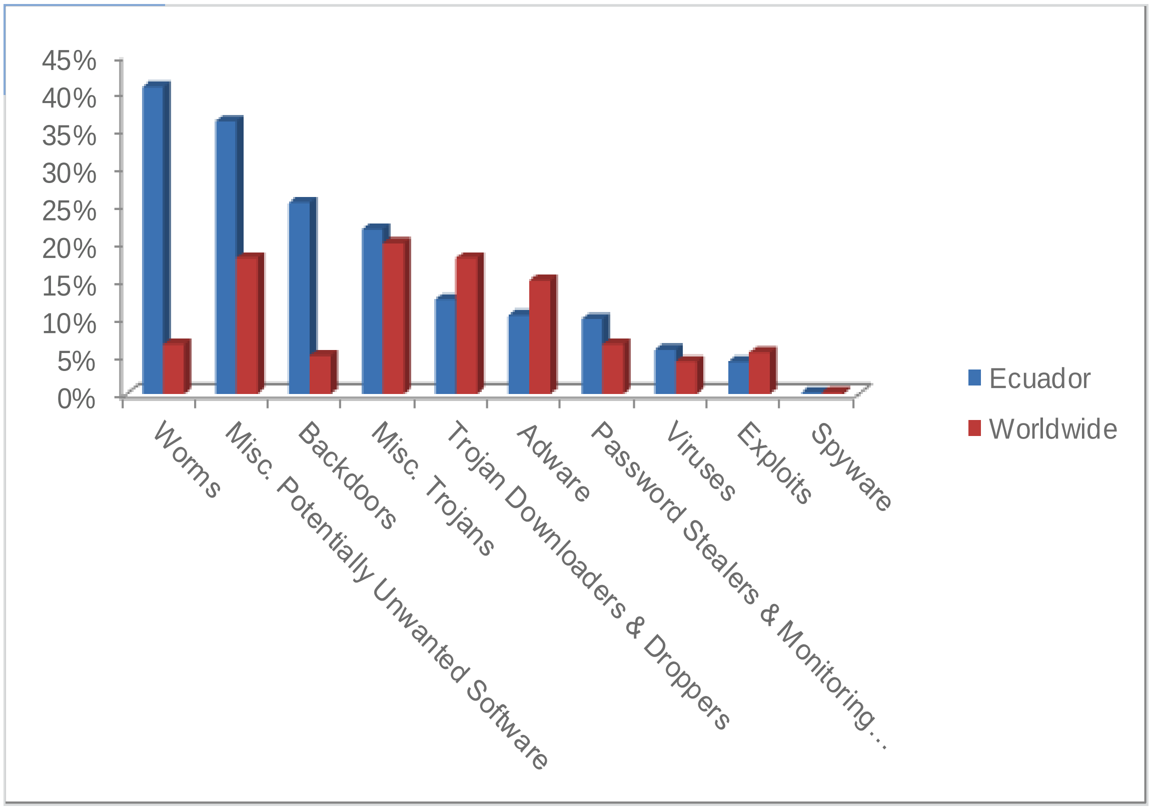
The MSRT detected malware on 8.9 of every 1,000 computers scanned in Ecuador in 4Q10 (a CCM score of 8.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Ecuador over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Ecuador and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Ecuador in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Ecuador in 4Q10 was Worms, which affected 40.8 percent of all cleaned computers, down from 46.8 percent in 3Q10.
- The second most common category in Ecuador in 4Q10 was Misc. Potentially Unwanted Software, which affected 36.2 percent of all cleaned computers, up from 33.5 percent in 3Q10.
- The third most common category in Ecuador in 4Q10 was Backdoors, which affected 25.4 percent of all cleaned computers, up from 20.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Ecuador in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 19.0% |
| 2 | Win32/IRCbot | 14.3% |
| 3 | Win32/Taterf | 12.3% |
| 4 | Win32/Rimecud | 11.0% |
| 5 | Win32/Vobfus | 10.6% |
| 6 | Esfury | 7.1% |
| 7 | Win32/Frethog | 6.3% |
| 8 | Win32/Keygen | 6.2% |
| 9 | Sdbot | 6.1% |
| 10 | Win32/FlyAgent | 6.0% |

- The most common threat family in Ecuador in 4Q10 was Win32/Autorun, which affected 19.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Ecuador in 4Q10 was Win32/IRCbot, which affected 14.3 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The third most common threat family in Ecuador in 4Q10 was Win32/Taterf, which affected 12.3 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Ecuador in 4Q10 was Win32/Rimecud, which affected 11.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Egypt

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

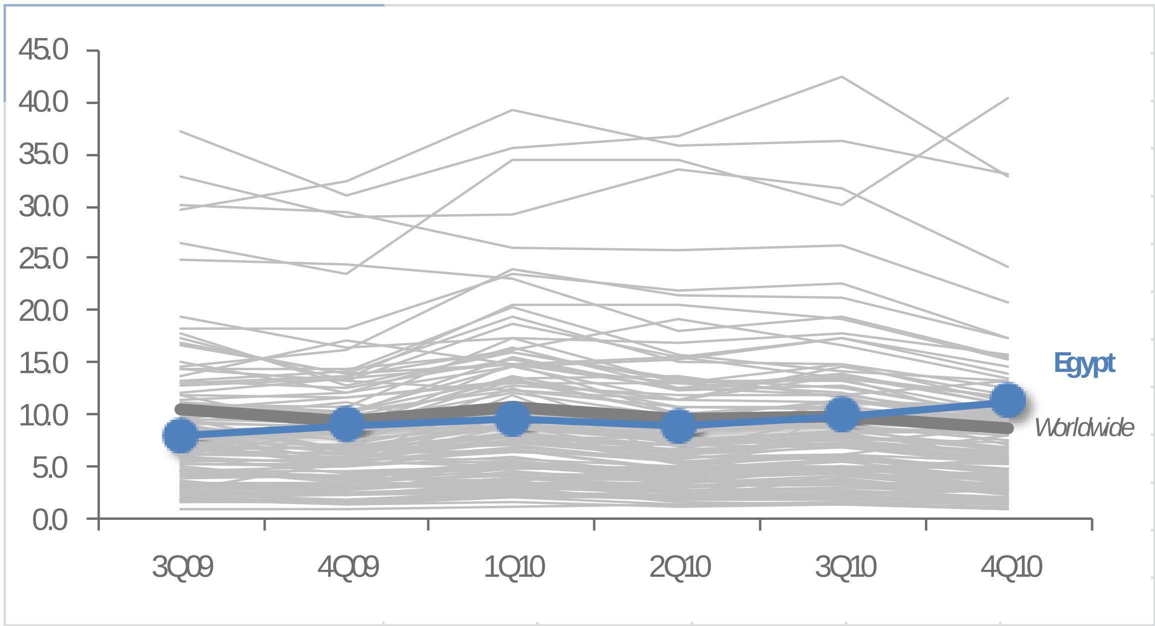
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Egypt in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Egypt and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">9.7</td><td colspan="3">9.0</td><td colspan="3">10.0</td><td colspan="3">11.4</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.29</td><td colspan="6">0.05</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.26</td><td colspan="6">0.57</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.363%</td><td colspan="4">0.155%</td><td colspan="4">0.149%</td></tr>
</table>

## Infection Trends (CCM)

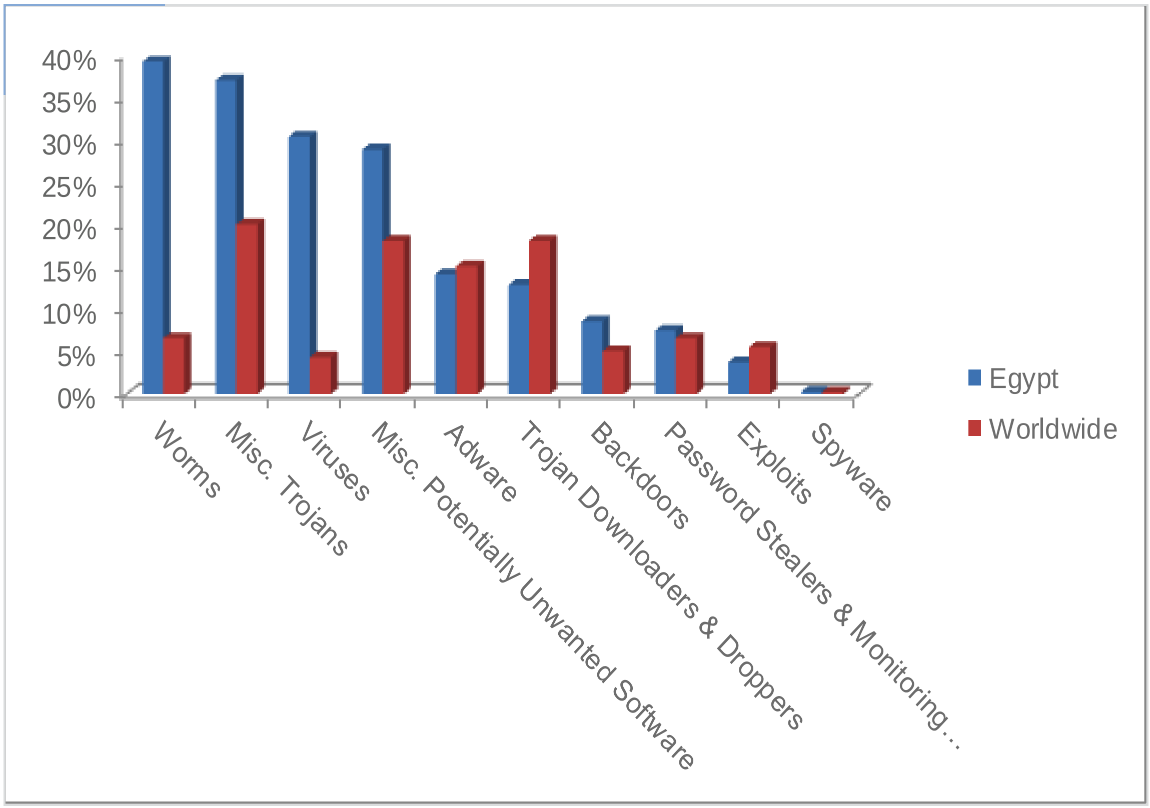
The MSRT detected malware on 11.4 of every 1,000 computers scanned in Egypt in 4Q10 (a CCM score of 11.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Egypt over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Egypt and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Egypt in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Egypt in 4Q10 was Worms, which affected 39.2 percent of all cleaned computers, down from 43.2 percent in 3Q10.
- The second most common category in Egypt in 4Q10 was Misc. Trojans, which affected 37.0 percent of all cleaned computers, up from 35.6 percent in 3Q10.
- The third most common category in Egypt in 4Q10 was Viruses, which affected 30.4 percent of all cleaned computers, up from 24.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Egypt in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Sality | 32.2% |
| 2 | Win32/Autorun | 21.6% |
| 3 | JS/Pornpop | 8.7% |
| 4 | Win32/Rimecud | 7.6% |
| 5 | Win32/Agent | 7.3% |
| 6 | Win32/Conficker | 7.2% |
| 7 | Win32/Keygen | 7.1% |
| 8 | Win32/Taterf | 5.3% |
| 9 | Win32/Virut | 4.3% |
| 10 | Win32/Renos | 4.2% |

- The most common threat family in Egypt in 4Q10 was Win32/Sality, which affected 32.2 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

- The second most common threat family in Egypt in 4Q10 was Win32/Autorun, which affected 21.6 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

- The third most common threat family in Egypt in 4Q10 was JS/Pornpop, which affected 8.7 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

- The fourth most common threat family in Egypt in 4Q10 was Win32/Rimecud, which affected 7.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# El Salvador

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

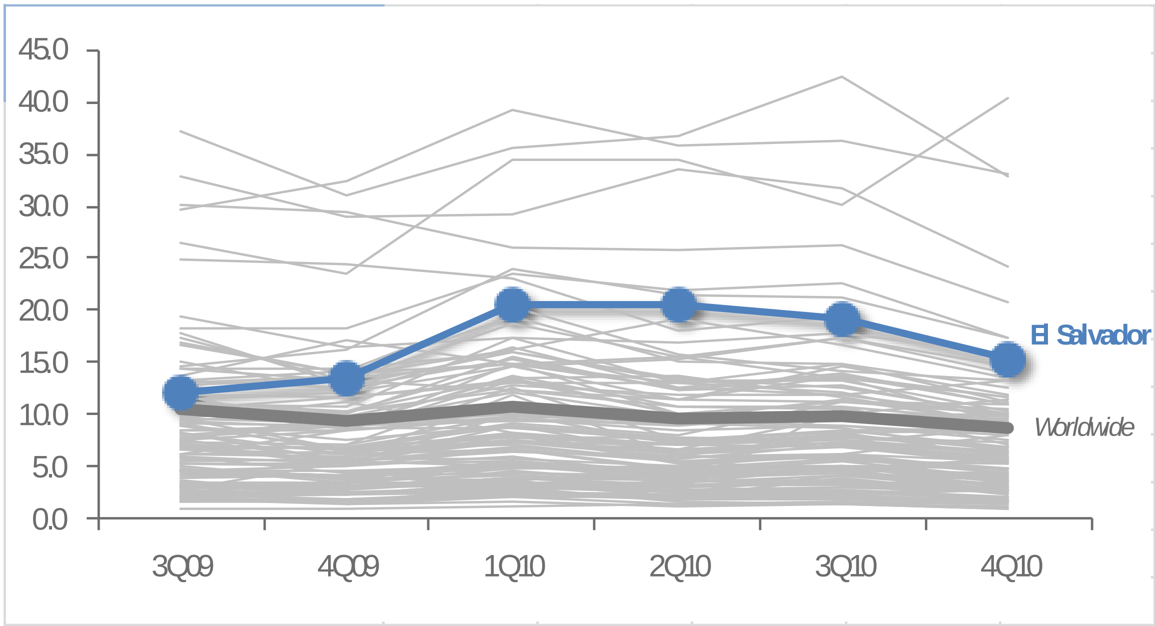
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in El Salvador in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in El Salvador and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 20.6 | 20.5 | 19.1 | 15.2 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 3.76 | | 1.05 | |
| Malware hosting sites per 1000 hosts | 0.87 | | 0.35 | |
| Percentage of sites hosting drive-by downloads | 0.140% | 0.110% | | 0.140% |

## Infection Trends (CCM)

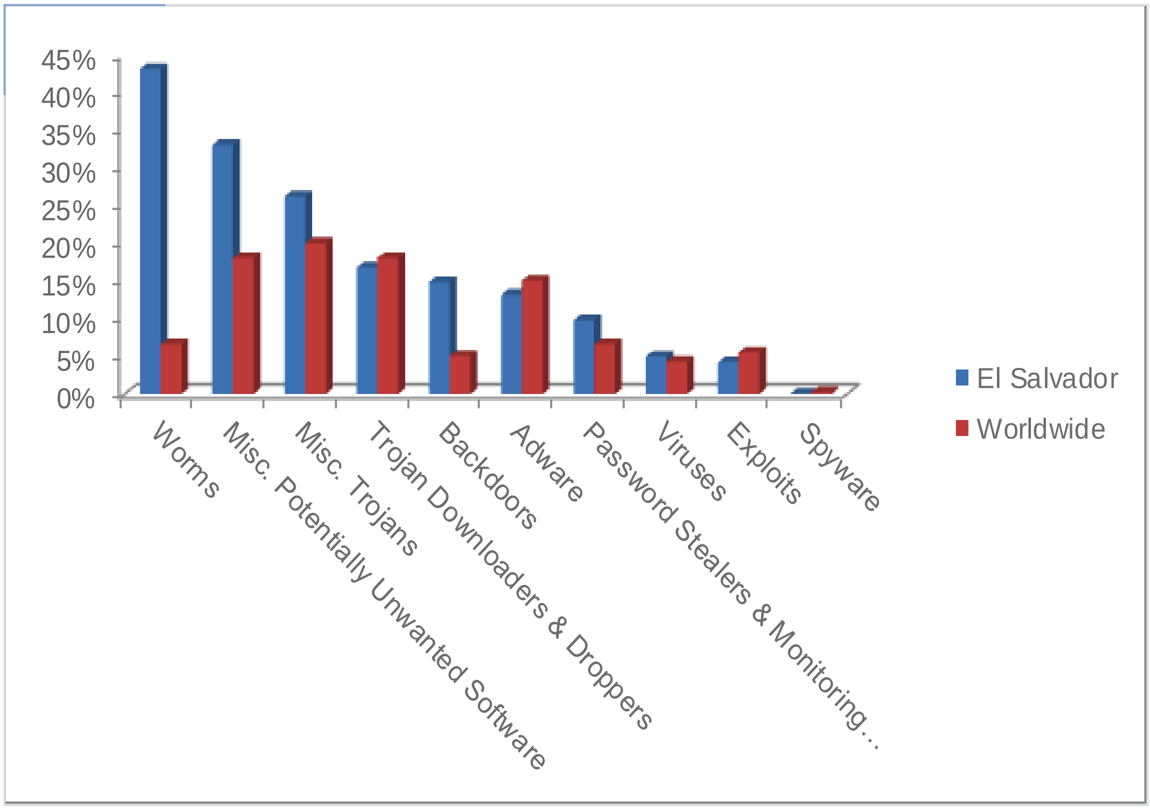
The MSRT detected malware on 15.2 of every 1,000 computers scanned in El Salvador in 4Q10 (a CCM score of 15.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for El Salvador over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in El Salvador and worldwide



## Threat Categories

Malware and potentially unwanted software categories in El Salvador in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in El Salvador in 4Q10 was Worms, which affected 43.1 percent of all cleaned computers, down from 52.9 percent in 3Q10.
- The second most common category in El Salvador in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.1 percent of all cleaned computers, up from 29.9 percent in 3Q10.
- The third most common category in El Salvador in 4Q10 was Misc. Trojans, which affected 26.2 percent of all cleaned computers, up from 23.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in El Salvador in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 19.3% |
| 2 | Win32/Autorun | 18.9% |
| 3 | Win32/Vobfus | 13.5% |
| 4 | Win32/Taterf | 10.6% |
| 5 | Win32/IRCbot | 10.1% |
| 6 | Win32/Renos | 6.6% |
| 7 | Win32/Keygen | 6.2% |
| 8 | Win32/Frethog | 6.0% |
| 9 | JS/Pornpop | 5.9% |
| 10 | Win32/Conficker | 4.8% |

- The most common threat family in El Salvador in 4Q10 was Win32/Rimecud, which affected 19.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in El Salvador in 4Q10 was Win32/Autorun, which affected 18.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in El Salvador in 4Q10 was Win32/Vobfus, which affected 13.5 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in El Salvador in 4Q10 was Win32/Taterf, which affected 10.6 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Estonia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

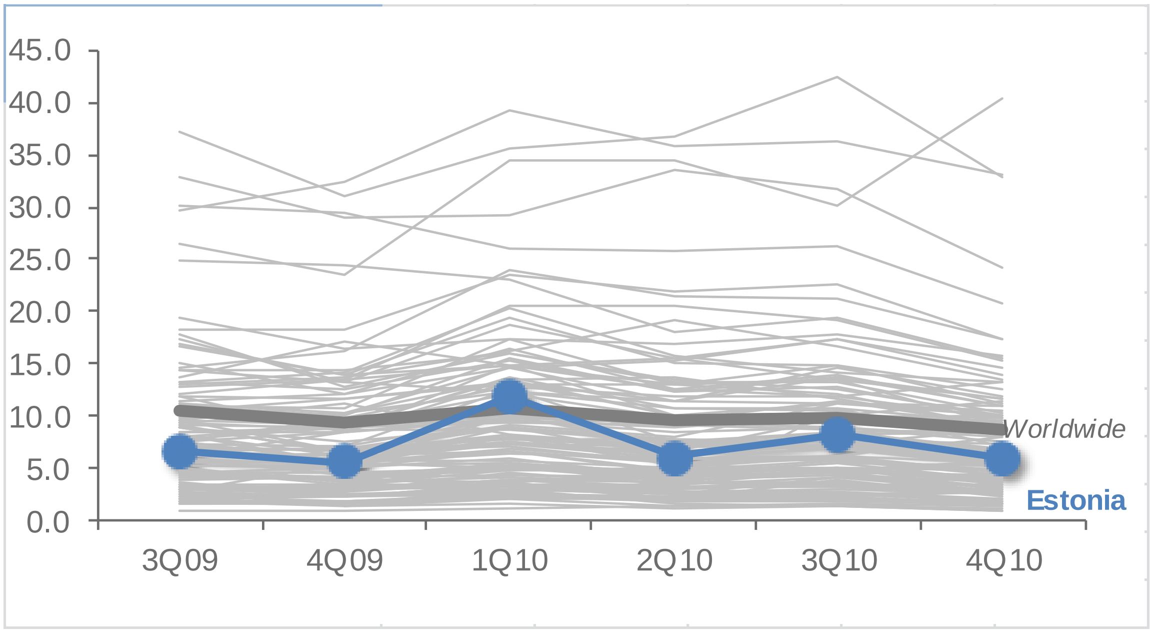
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Estonia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Estonia and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 11.9 | 6.0 | 8.1 | 5.9 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.15 | | 0.09 | |
| Malware hosting sites per 1000 hosts | 0.88 | | 0.18 | |
| Percentage of sites hosting drive-by downloads | 0.339% | 0.073% | 0.091% | |

## Infection Trends (CCM)

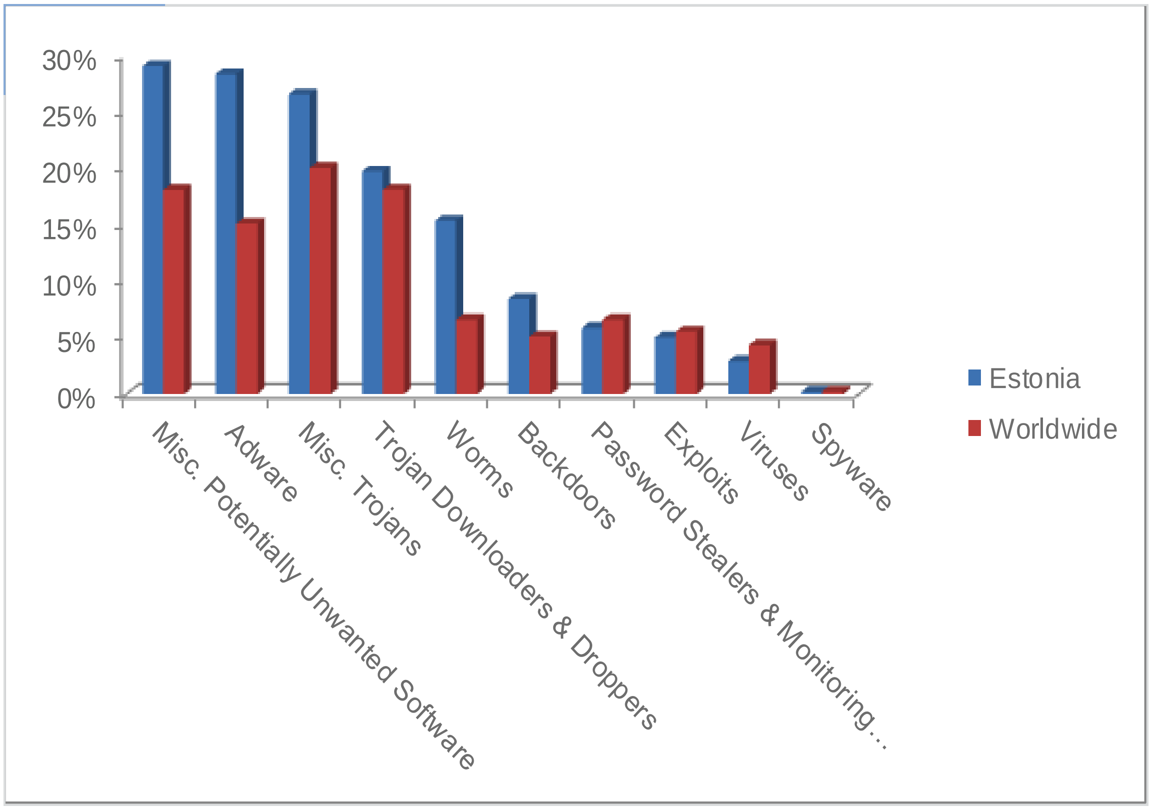
The MSRT detected malware on 5.9 of every 1,000 computers scanned in Estonia in 4Q10 (a CCM score of 5.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Estonia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Estonia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Estonia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Estonia in 4Q10 was Misc. Potentially Unwanted Software, which affected 29.0 percent of all cleaned computers, down from 33.6 percent in 3Q10.
- The second most common category in Estonia in 4Q10 was Adware, which affected 28.3 percent of all cleaned computers, up from 26.0 percent in 3Q10.
- The third most common category in Estonia in 4Q10 was Misc. Trojans, which affected 26.5 percent of all cleaned computers, up from 23.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Estonia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 14.7% |
| 2 | Win32/ClickPotato | 7.0% |
| 3 | Win32/Keygen | 6.8% |
| 4 | Win32/Renos | 6.7% |
| 5 | Win32/Zwangi | 5.7% |
| 6 | Win32/Conficker | 5.5% |
| 7 | Win32/Rimecud | 5.2% |
| 8 | Win32/IRCbot | 4.9% |
| 9 | Win32/Hotbar | 4.6% |
| 10 | Win32/Autorun | 4.1% |

- The most common threat family in Estonia in 4Q10 was JS/Pornpop, which affected 14.7 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Estonia in 4Q10 was Win32/ClickPotato, which affected 7.0 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Estonia in 4Q10 was Win32/Keygen, which affected 6.8 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.
- The fourth most common threat family in Estonia in 4Q10 was Win32/Renos, which affected 6.7 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.

# Finland

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

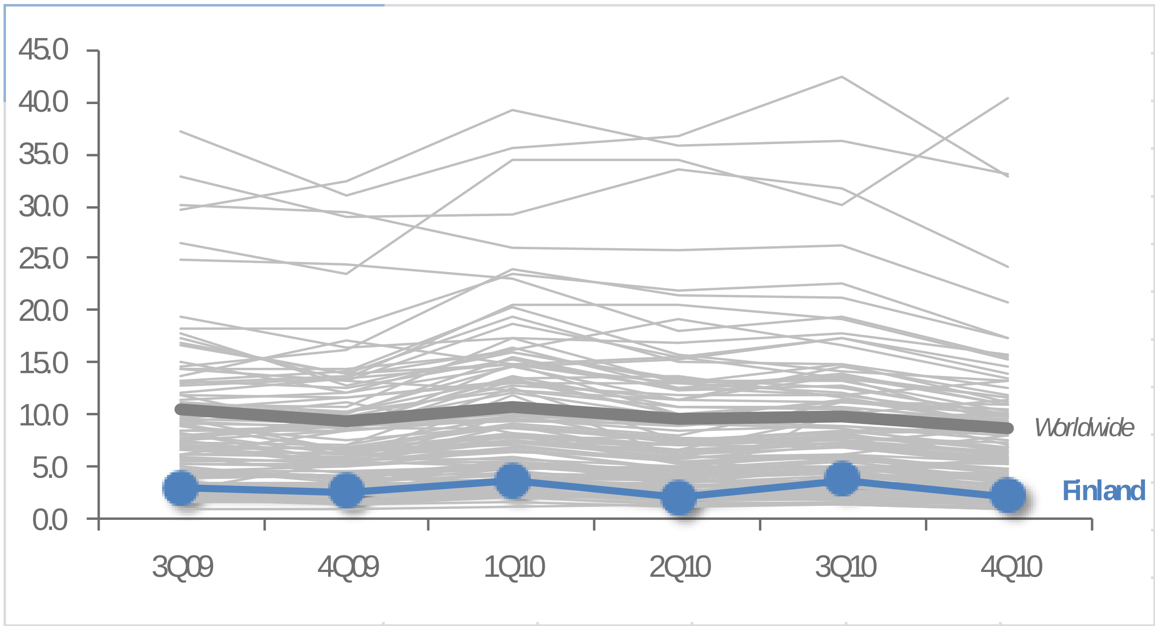
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Finland in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Finland and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">3.7</td><td colspan="3">2.1</td><td colspan="3">3.8</td><td colspan="3">2.3</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.21</td><td colspan="6">0.04</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.09</td><td colspan="6">0.03</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.238%</td><td colspan="4">0.012%</td><td colspan="4">0.015%</td></tr>
</table>

## Infection Trends (CCM)

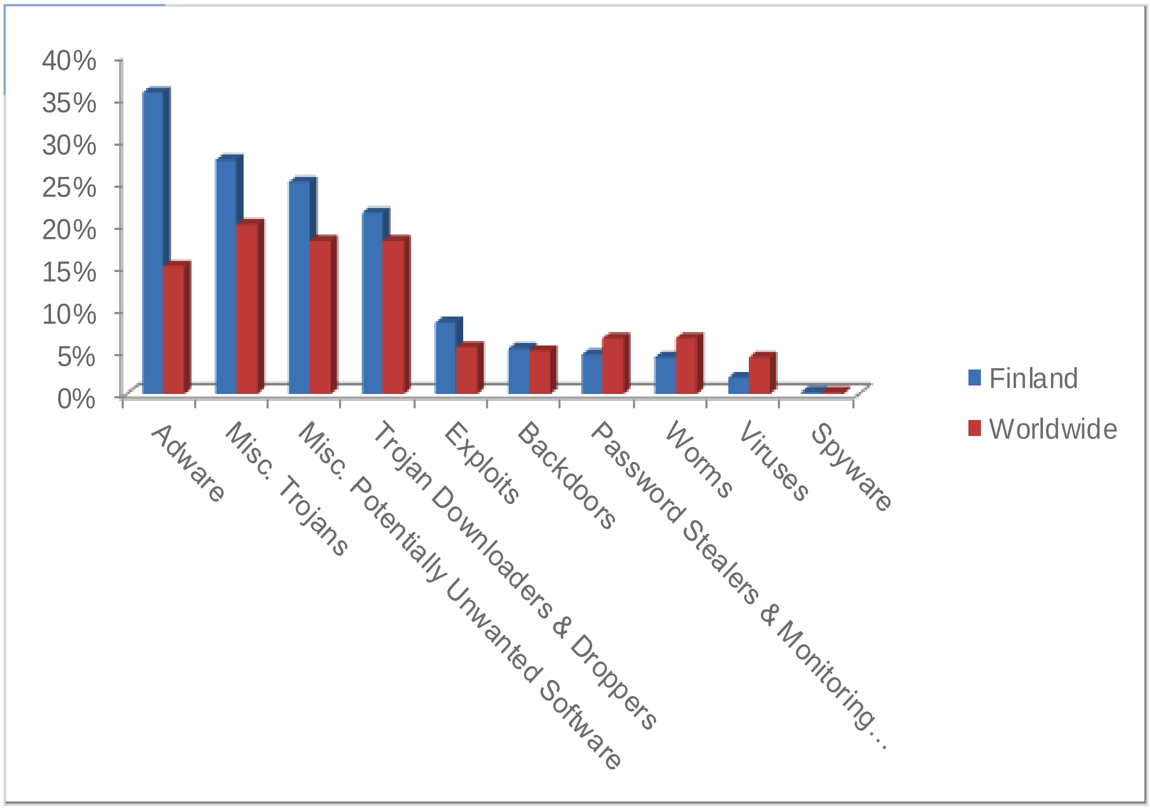
The MSRT detected malware on 2.3 of every 1,000 computers scanned in Finland in 4Q10 (a CCM score of 2.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Finland over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Finland and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Finland in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Finland in 4Q10 was Adware, which affected 35.5 percent of all cleaned computers, down from 36.0 percent in 3Q10.
- The second most common category in Finland in 4Q10 was Misc. Trojans, which affected 27.6 percent of all cleaned computers, up from 26.9 percent in 3Q10.
- The third most common category in Finland in 4Q10 was Misc. Potentially Unwanted Software, which affected 25.0 percent of all cleaned computers, down from 26.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Finland in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 21.4% |
| 2 | Win32/Renos | 6.9% |
| 3 | Win32/ClickPotato | 6.3% |
| 4 | Win32/Zwangi | 5.6% |
| 5 | Java/CVE-2008-5353 | 4.6% |
| 6 | Java/CVE-2009-3867 | 4.4% |
| 7 | Win32/Keygen | 4.1% |
| 8 | ASX/Wimad | 4.0% |
| 9 | Win32/Hotbar | 3.9% |
| 10 | Win32/Bubnix | 3.8% |

- The most common threat family in Finland in 4Q10 was JS/Pornpop, which affected 21.4 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Finland in 4Q10 was Win32/Renos, which affected 6.9 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.
- The third most common threat family in Finland in 4Q10 was Win32/ClickPotato, which affected 6.3 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The fourth most common threat family in Finland in 4Q10 was Win32/Zwangi, which affected 5.6 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# France

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

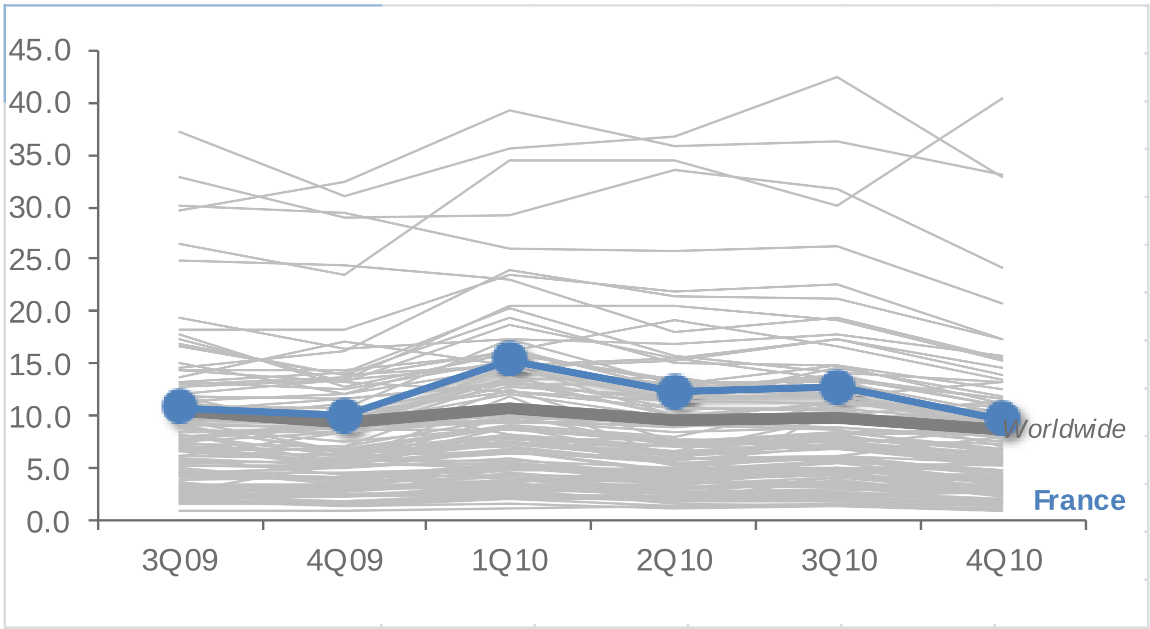
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in France in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in France and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">15.5</td><td colspan="3">12.4</td><td colspan="3">12.8</td><td colspan="3">9.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.41</td><td colspan="6">1.36</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.21</td><td colspan="6">0.95</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.151%</td><td colspan="4">0.026%</td><td colspan="4">0.033%</td></tr>
</table>

## Infection Trends (CCM)

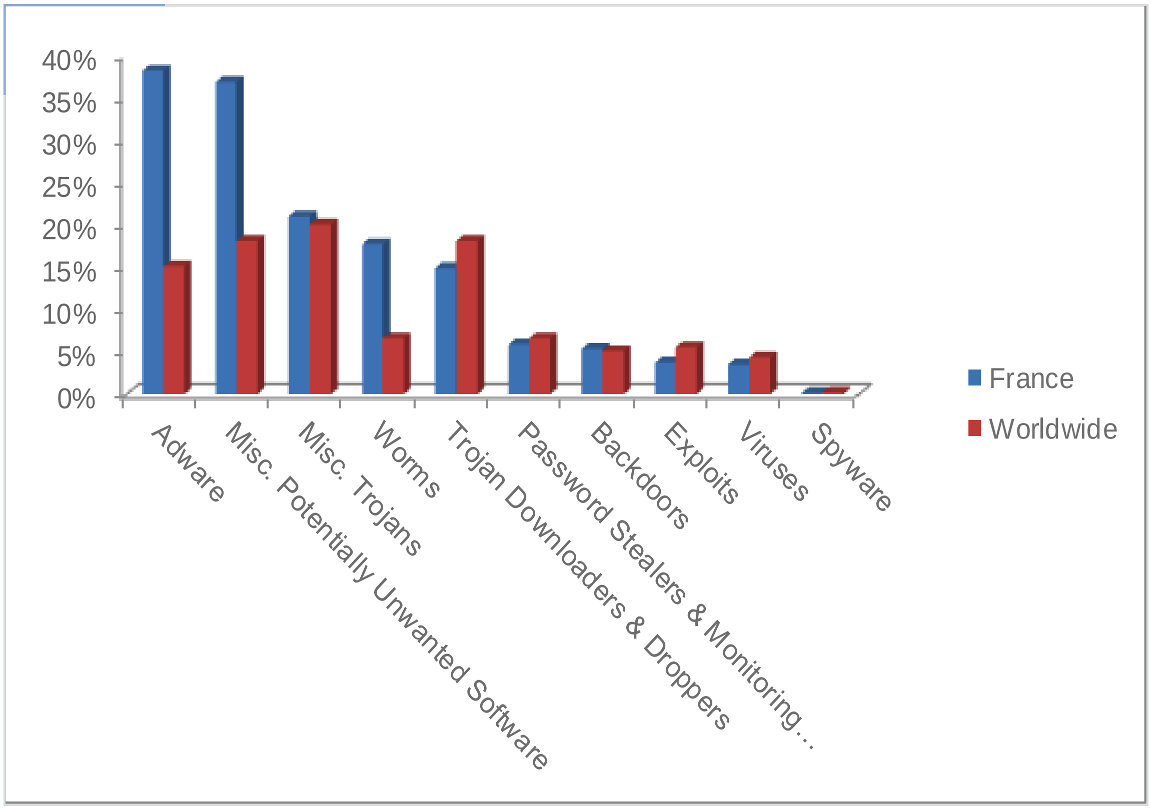
The MSRT detected malware on 9.8 of every 1,000 computers scanned in France in 4Q10 (a CCM score of 9.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for France over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in France and worldwide



## Threat Categories

Malware and potentially unwanted software categories in France in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in France in 4Q10 was Adware, which affected 38.2 percent of all cleaned computers, up from 25.9 percent in 3Q10.
- The second most common category in France in 4Q10 was Misc. Potentially Unwanted Software, which affected 36.8 percent of all cleaned computers, up from 25.7 percent in 3Q10.
- The third most common category in France in 4Q10 was Misc. Trojans, which affected 21.0 percent of all cleaned computers, down from 25.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in France in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/ClickPotato | 20.8% |
| 2 | Win32/Zwangi | 19.4% |
| 3 | Win32/Hotbar | 10.1% |
| 4 | JS/Pornpop | 6.9% |
| 5 | Win32/Autorun | 6.5% |
| 6 | Win32/Taterf | 4.6% |
| 7 | ASX/Wimad | 4.6% |
| 8 | Win32/Renos | 4.2% |
| 9 | Win32/Rimecud | 3.3% |
| 10 | Win32/Vobfus | 3.2% |

- The most common threat family in France in 4Q10 was Win32/ClickPotato, which affected 20.8 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The second most common threat family in France in 4Q10 was Win32/Zwangi, which affected 19.4 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The third most common threat family in France in 4Q10 was Win32/Hotbar, which affected 10.1 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.
- The fourth most common threat family in France in 4Q10 was JS/Pornpop, which affected 6.9 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Georgia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

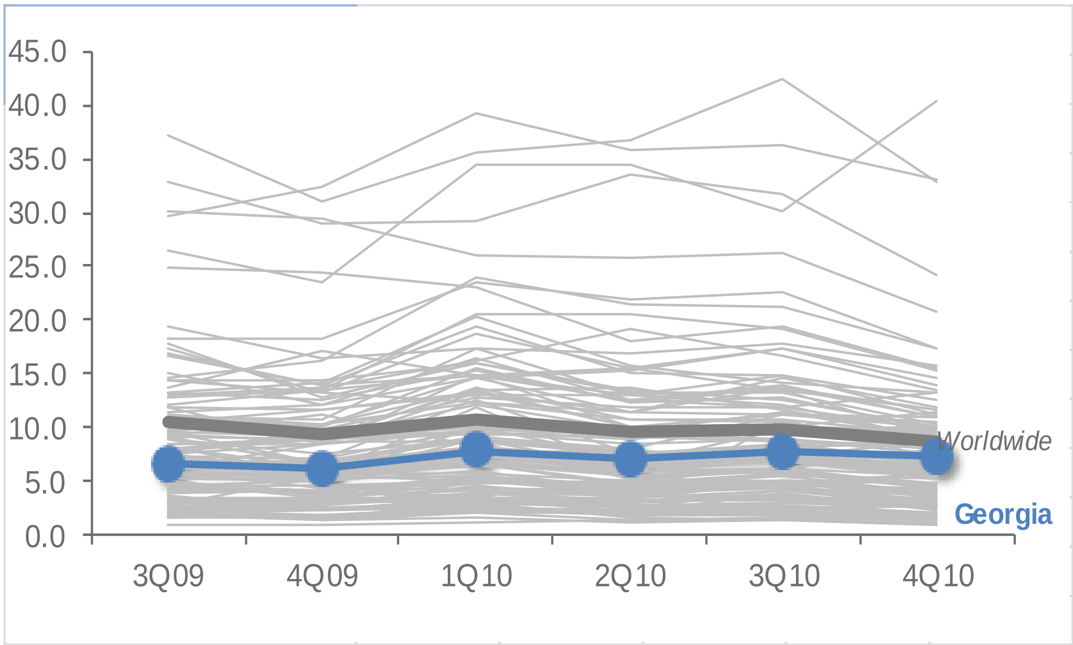
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Georgia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Georgia and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 7.9 | 7.1 | 7.7 | 7.3 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 14.69 | | 5.81 | |
| Malware hosting sites per 1000 hosts | 43.58 | | 29.92 | |
| Percentage of sites hosting drive-by downloads | 0.675% | 0.392% | 0.341% | |

## Infection Trends (CCM)

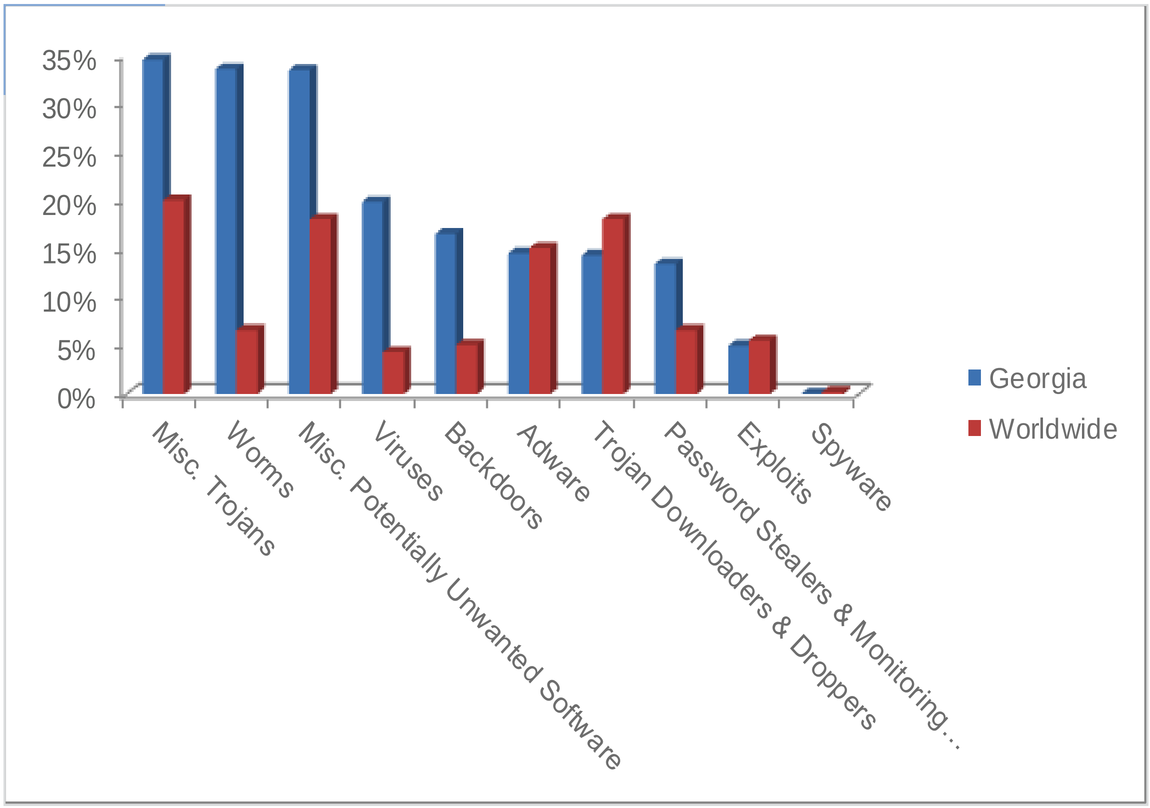
The MSRT detected malware on 7.3 of every 1,000 computers scanned in Georgia in 4Q10 (a CCM score of 7.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Georgia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Georgia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Georgia in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Georgia in 4Q10 was Misc. Trojans, which affected 34.5 percent of all cleaned computers, down from 40.0 percent in 3Q10.
- The second most common category in Georgia in 4Q10 was Worms, which affected 33.5 percent of all cleaned computers, down from 37.1 percent in 3Q10.
- The third most common category in Georgia in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.4 percent of all cleaned computers, up from 32.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Georgia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 21.4% |
| 2 | Win32/Rimecud | 13.5% |
| 3 | Win32/IRCbot | 11.8% |
| 4 | Win32/Taterf | 11.4% |
| 5 | Win32/Sality | 11.2% |
| 6 | JS/Pornpop | 10.9% |
| 7 | Win32/Frethog | 8.2% |
| 8 | Jeefo | 6.5% |
| 9 | Win32/Keygen | 6.2% |
| 10 | Win32/Conficker | 5.9% |

- The most common threat family in Georgia in 4Q10 was Win32/Autorun, which affected 21.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Georgia in 4Q10 was Win32/Rimecud, which affected 13.5 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Georgia in 4Q10 was Win32/IRCbot, which affected 11.8 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The fourth most common threat family in Georgia in 4Q10 was Win32/Taterf, which affected 11.4 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Germany

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

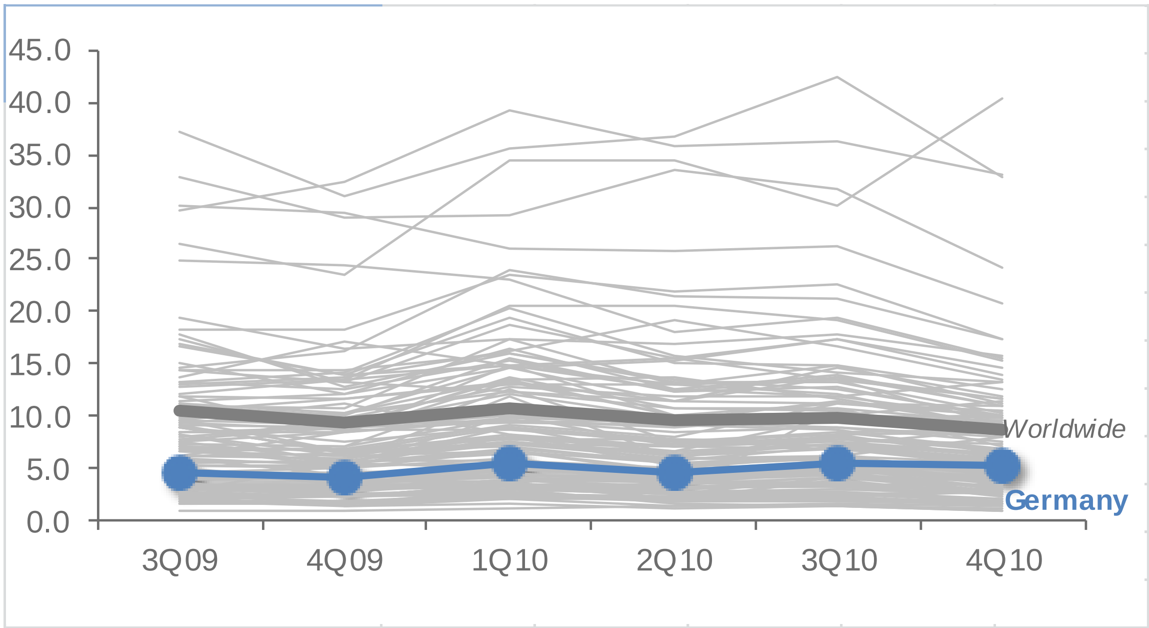
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Germany in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Germany and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">5.5</td><td colspan="3">4.6</td><td colspan="3">5.6</td><td colspan="3">5.3</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.44</td><td colspan="6">0.43</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.98</td><td colspan="6">4.98</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.109%</td><td colspan="4">0.019%</td><td colspan="4">0.026%</td></tr>
</table>

## Infection Trends (CCM)

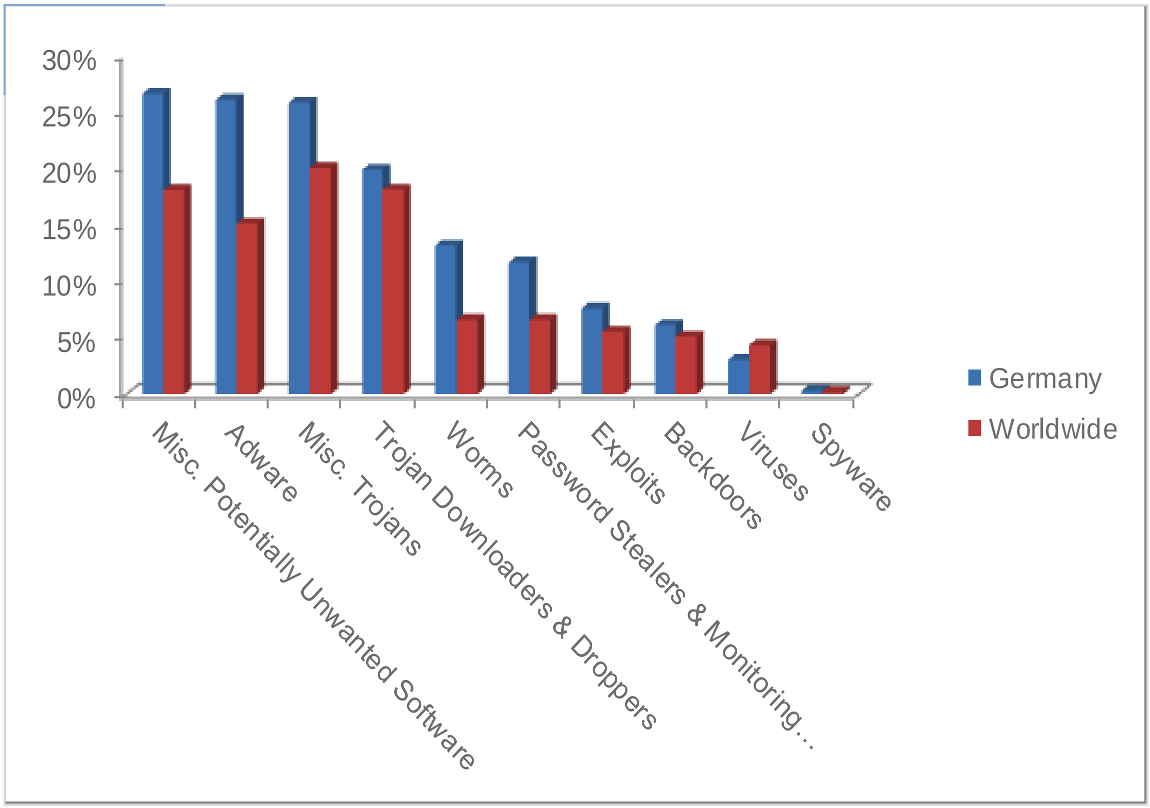
The MSRT detected malware on 5.3 of every 1,000 computers scanned in Germany in 4Q10 (a CCM score of 5.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Germany over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Germany and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Germany in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Germany in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.6 percent of all cleaned computers, down from 31.2 percent in 3Q10.
- The second most common category in Germany in 4Q10 was Adware, which affected 26.0 percent of all cleaned computers, down from 28.5 percent in 3Q10.
- The third most common category in Germany in 4Q10 was Misc. Trojans, which affected 25.8 percent of all cleaned computers, up from 22.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Germany in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 18.2% |
| 2 | Win32/Renos | 7.6% |
| 3 | Win32/Zbot | 6.9% |
| 4 | Win32/Conficker | 5.2% |
| 5 | Win32/Obfuscator | 4.8% |
| 6 | Win32/Keygen | 4.2% |
| 7 | Win32/Alureon | 4.1% |
| 8 | PossibleHostsFileHijack | 3.7% |
| 9 | Win32/Autorun | 3.5% |
| 10 | Win32/ClickPotato | 3.4% |

- The most common threat family in Germany in 4Q10 was JS/Pornpop, which affected 18.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Germany in 4Q10 was Win32/Renos, which affected 7.6 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.
- The third most common threat family in Germany in 4Q10 was Win32/Zbot, which affected 6.9 percent of cleaned computers. Win32/Zbot is a family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected machine.
- The fourth most common threat family in Germany in 4Q10 was Win32/Conficker, which affected 5.2 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

# Ghana

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

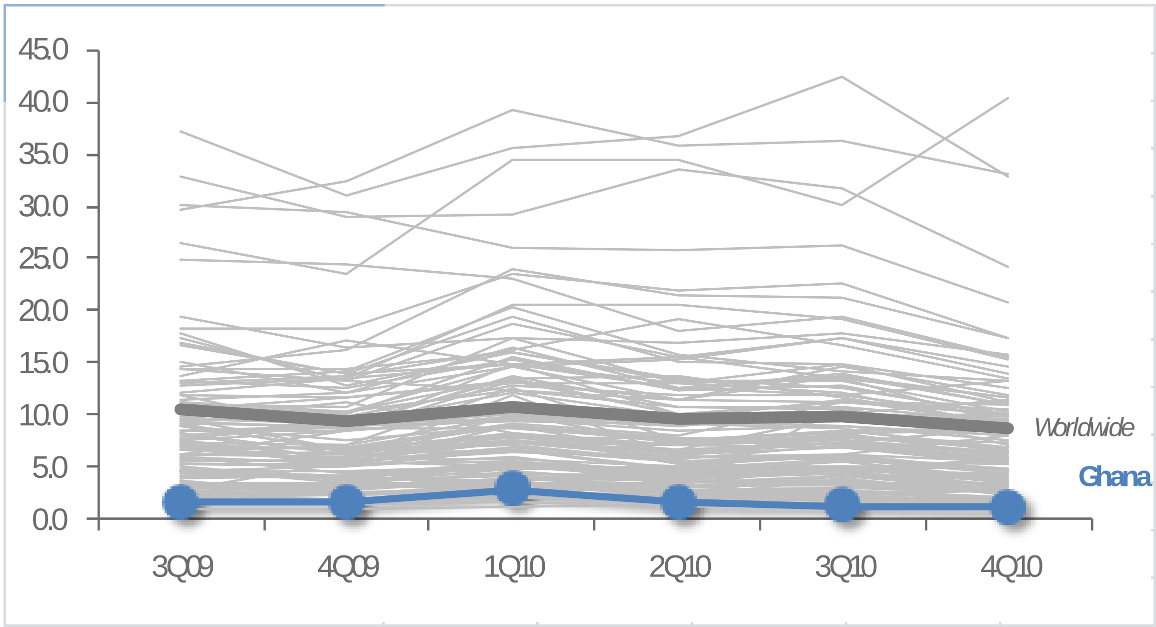
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Ghana in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Ghana and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 2.9 | 1.6 | 1.5 | 1.2 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.04 | | | |
| Malware hosting sites per 1000 hosts | 0.08 | | | |
| Percentage of sites hosting drive-by downloads | 8.755% | 0.122% | | |

## Infection Trends (CCM)

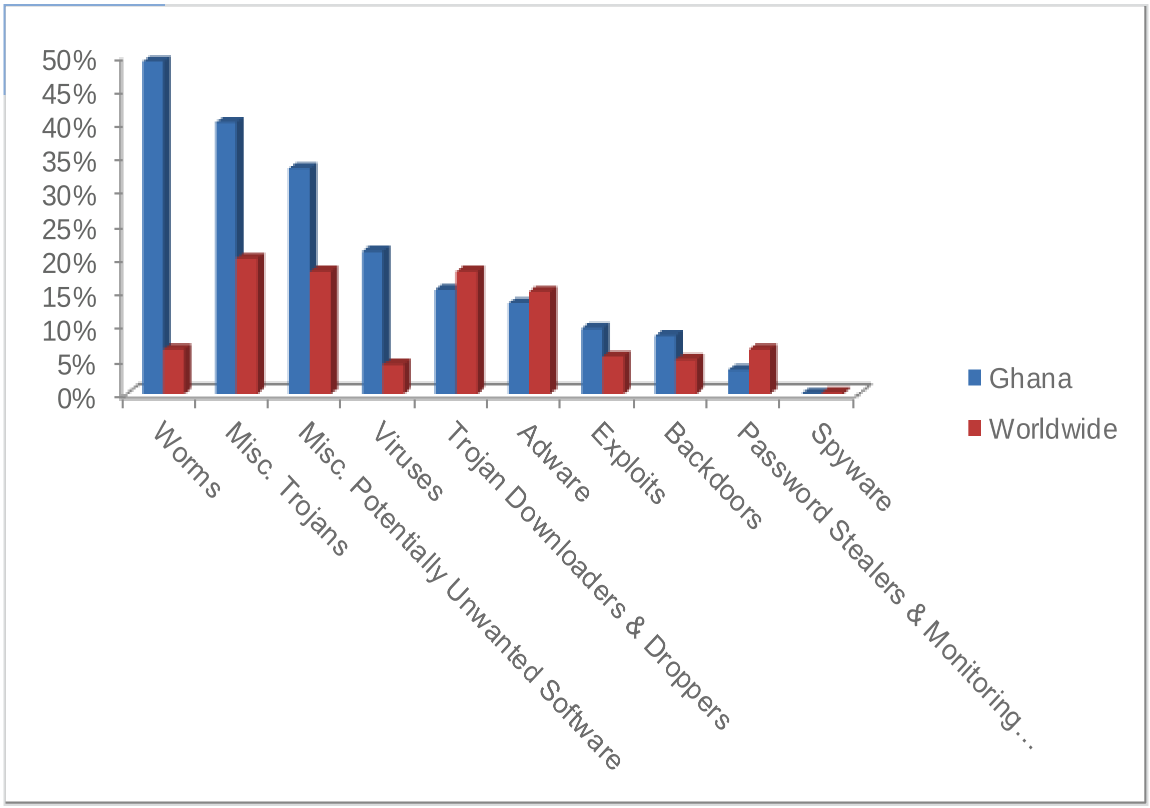
The MSRT detected malware on 1.2 of every 1,000 computers scanned in Ghana in 4Q10 (a CCM score of 1.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Ghana over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Ghana and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Ghana in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Ghana in 4Q10 was Worms, which affected 49.0 percent of all cleaned computers, down from 54.3 percent in 3Q10.
- The second most common category in Ghana in 4Q10 was Misc. Trojans, which affected 40.0 percent of all cleaned computers, down from 42.1 percent in 3Q10.
- The third most common category in Ghana in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.3 percent of all cleaned computers, up from 30.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Ghana in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 29.8% |
| 2 | Win32/Rimecud | 26.6% |
| 3 | Win32/Vobfus | 17.8% |
| 4 | Win32/Folstart | 15.2% |
| 5 | Win32/Sality | 10.5% |
| 6 | Win32/Mabezat | 8.1% |
| 7 | Win32/Virut | 7.9% |
| 8 | CplLnk | 7.6% |
| 9 | Win32/Nuqel | 5.8% |
| 10 | Win32/Renos | 5.6% |

- The most common threat family in Ghana in 4Q10 was Win32/Autorun, which affected 29.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Ghana in 4Q10 was Win32/Rimecud, which affected 26.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Ghana in 4Q10 was Win32/Vobfus, which affected 17.8 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Ghana in 4Q10 was Win32/Folstart, which affected 15.2 percent of cleaned computers. Win32/Folstart is

# Greece

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

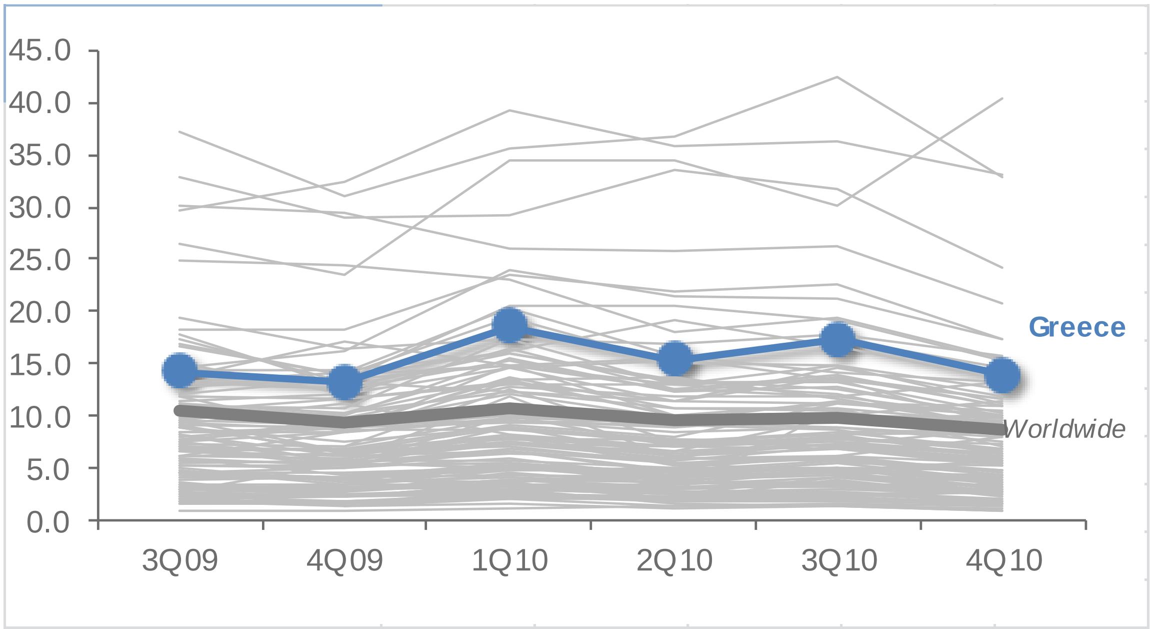
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Greece in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Greece and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 18.7 | 15.4 | 17.5 | 14.0 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.08 | | 0.03 | |
| Malware hosting sites per 1000 hosts | 0.33 | | 0.06 | |
| Percentage of sites hosting drive-by downloads | 0.275% | 0.076% | 0.068% | |

## Infection Trends (CCM)

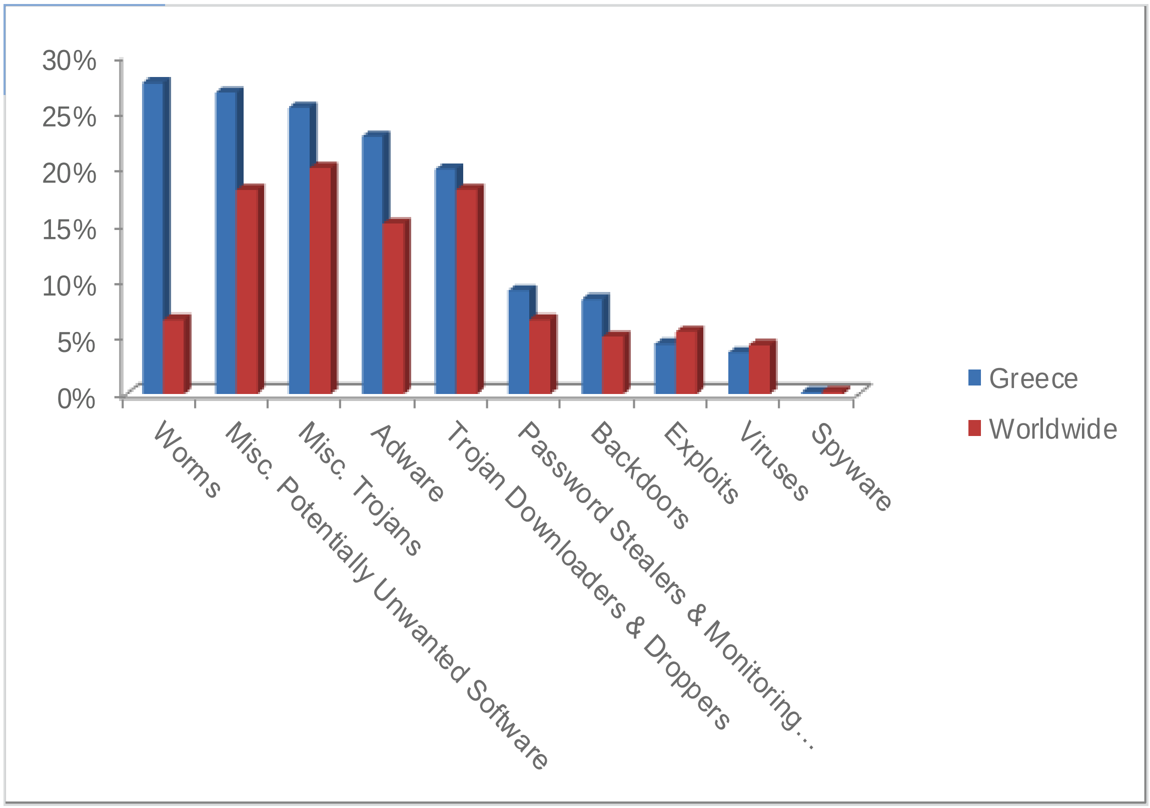
The MSRT detected malware on 14.0 of every 1,000 computers scanned in Greece in 4Q10 (a CCM score of 14.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Greece over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Greece and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Greece in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Greece in 4Q10 was Worms, which affected 27.5 percent of all cleaned computers, down from 30.9 percent in 3Q10.
- The second most common category in Greece in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.7 percent of all cleaned computers, down from 26.9 percent in 3Q10.
- The third most common category in Greece in 4Q10 was Misc. Trojans, which affected 25.3 percent of all cleaned computers, up from 23.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Greece in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 12.6% |
| 2 | Win32/Autorun | 9.7% |
| 3 | Win32/Taterf | 8.5% |
| 4 | Win32/Renos | 7.0% |
| 5 | Win32/Keygen | 6.3% |
| 6 | Win32/Zwangi | 5.4% |
| 7 | Win32/Frethog | 5.1% |
| 8 | Win32/Rimecud | 4.3% |
| 9 | Win32/ClickPotato | 4.1% |
| 10 | Win32/IRCbot | 4.1% |

- The most common threat family in Greece in 4Q10 was JS/Pornpop, which affected 12.6 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Greece in 4Q10 was Win32/Autorun, which affected 9.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Greece in 4Q10 was Win32/Taterf, which affected 8.5 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Greece in 4Q10 was Win32/Renos, which affected 7.0 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.

# Guadeloupe

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

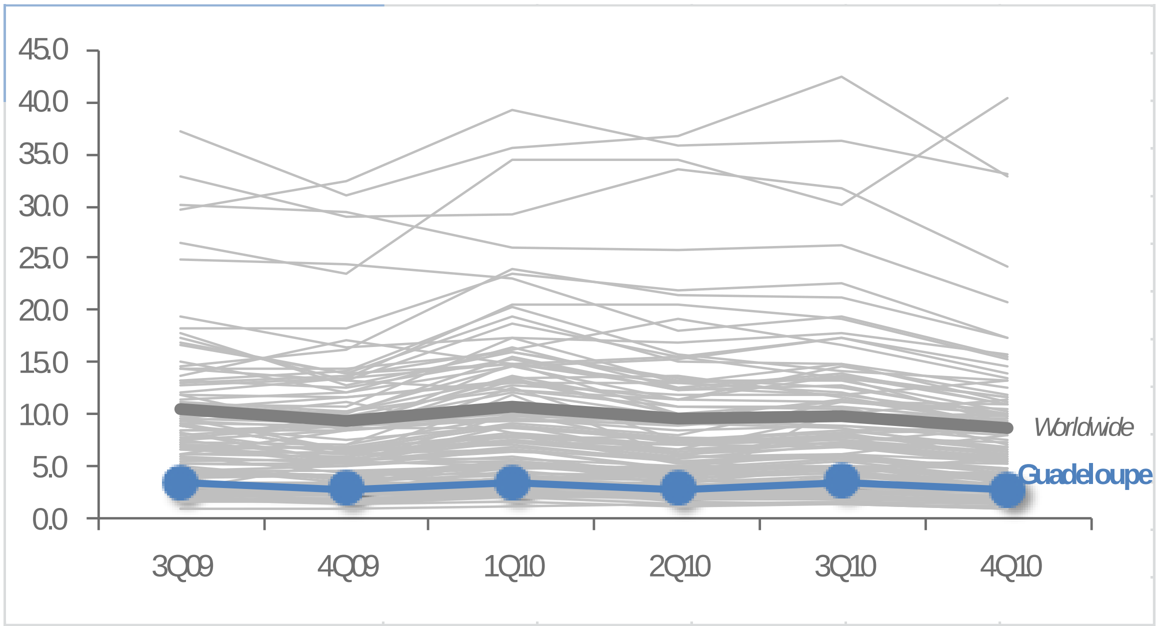
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Guadeloupe in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Guadeloupe and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.5 | 3.0 | 3.6 | 2.8 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | | | | |
| Malware hosting sites per 1000 hosts | | | | |
| Percentage of sites hosting drive-by downloads | 0.000% | | | 0.137% |

## Infection Trends (CCM)

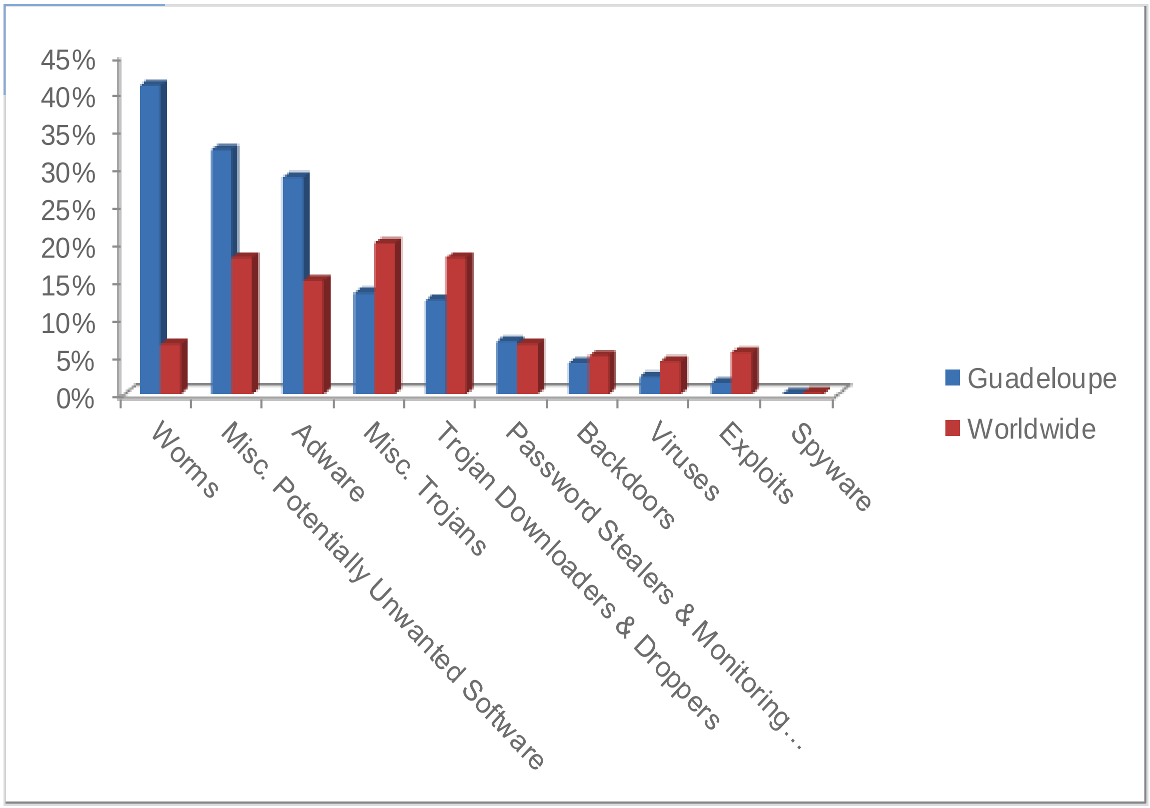
The MSRT detected malware on 2.8 of every 1,000 computers scanned in Guadeloupe in 4Q10 (a CCM score of 2.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Guadeloupe over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Guadeloupe and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Guadeloupe in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Guadeloupe in 4Q10 was Worms, which affected 40.9 percent of all cleaned computers, down from 43.6 percent in 3Q10.
- The second most common category in Guadeloupe in 4Q10 was Misc. Potentially Unwanted Software, which affected 32.4 percent of all cleaned computers, up from 23.3 percent in 3Q10.
- The third most common category in Guadeloupe in 4Q10 was Adware, which affected 28.7 percent of all cleaned computers, up from 22.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Guadeloupe in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Vobfus | 24.2% |
| 2 | Win32/Autorun | 14.8% |
| 3 | Win32/ClickPotato | 14.7% |
| 4 | Win32/Zwangi | 14.2% |
| 5 | Win32/Brontok | 8.0% |
| 6 | Win32/Hotbar | 7.9% |
| 7 | Win32/Taterf | 7.3% |
| 8 | Win32/Frethog | 4.4% |
| 9 | Win32/Renos | 4.3% |
| 10 | JS/Pornpop | 3.4% |

- The most common threat family in Guadeloupe in 4Q10 was Win32/Vobfus, which affected 24.2 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The second most common threat family in Guadeloupe in 4Q10 was Win32/Autorun, which affected 14.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Guadeloupe in 4Q10 was Win32/ClickPotato, which affected 14.7 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The fourth most common threat family in Guadeloupe in 4Q10 was Win32/Zwangi, which affected 14.2 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Guatemala

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

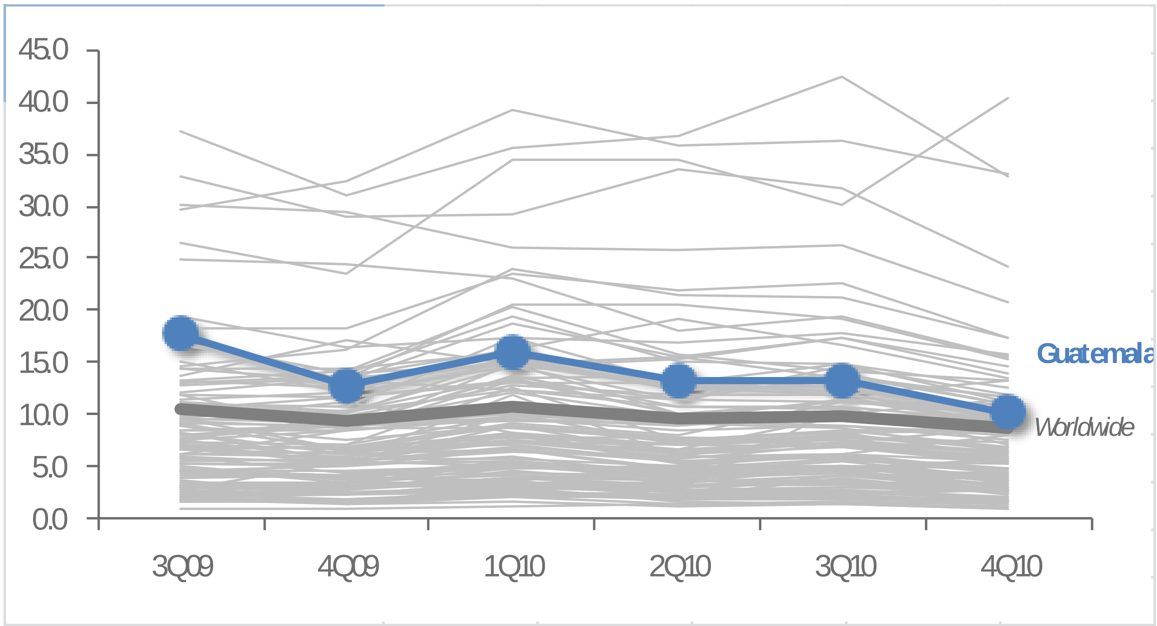
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Guatemala in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Guatemala and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">16.1</td><td colspan="3">13.3</td><td colspan="3">13.2</td><td colspan="3">10.2</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.02</td><td colspan="6">0.18</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.02</td><td colspan="6">0.16</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.122%</td><td colspan="4">0.143%</td><td colspan="4">0.092%</td></tr>
</table>

## Infection Trends (CCM)

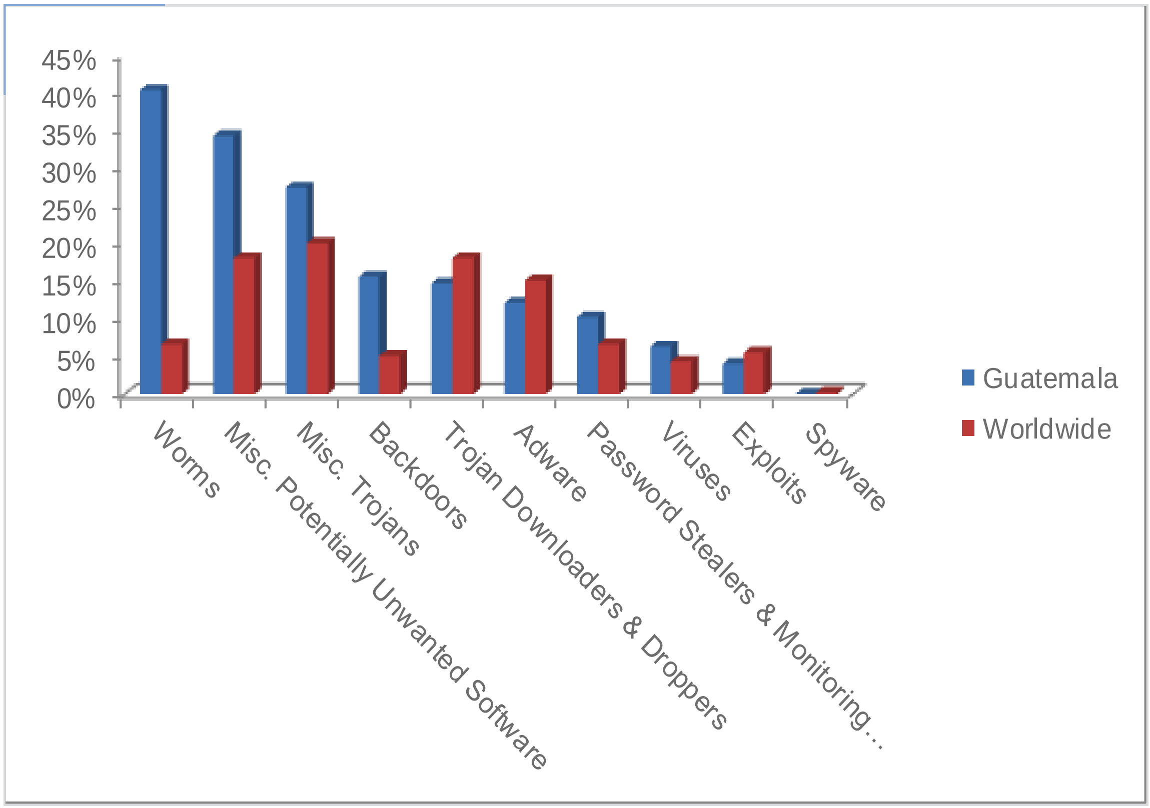
The MSRT detected malware on 10.2 of every 1,000 computers scanned in Guatemala in 4Q10 (a CCM score of 10.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Guatemala over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Guatemala and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Guatemala in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Guatemala in 4Q10 was Worms, which affected 40.3 percent of all cleaned computers, down from 48.6 percent in 3Q10.
- The second most common category in Guatemala in 4Q10 was Misc. Potentially Unwanted Software, which affected 34.3 percent of all cleaned computers, up from 32.5 percent in 3Q10.
- The third most common category in Guatemala in 4Q10 was Misc. Trojans, which affected 27.4 percent of all cleaned computers, up from 21.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Guatemala in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 19.0% |
| 2 | Win32/Autorun | 17.7% |
| 3 | Win32/Taterf | 13.3% |
| 4 | Win32/Vobfus | 11.3% |
| 5 | Win32/IRCbot | 10.6% |
| 6 | Win32/Frethog | 7.4% |
| 7 | Win32/Keygen | 6.3% |
| 8 | Win32/Sality | 5.4% |
| 9 | Win32/VBInject | 5.3% |
| 10 | JS/Pornpop | 4.8% |

- The most common threat family in Guatemala in 4Q10 was Win32/Rimecud, which affected 19.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Guatemala in 4Q10 was Win32/Autorun, which affected 17.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Guatemala in 4Q10 was Win32/Taterf, which affected 13.3 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Guatemala in 4Q10 was Win32/Vobfus, which affected 11.3 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

# Honduras

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

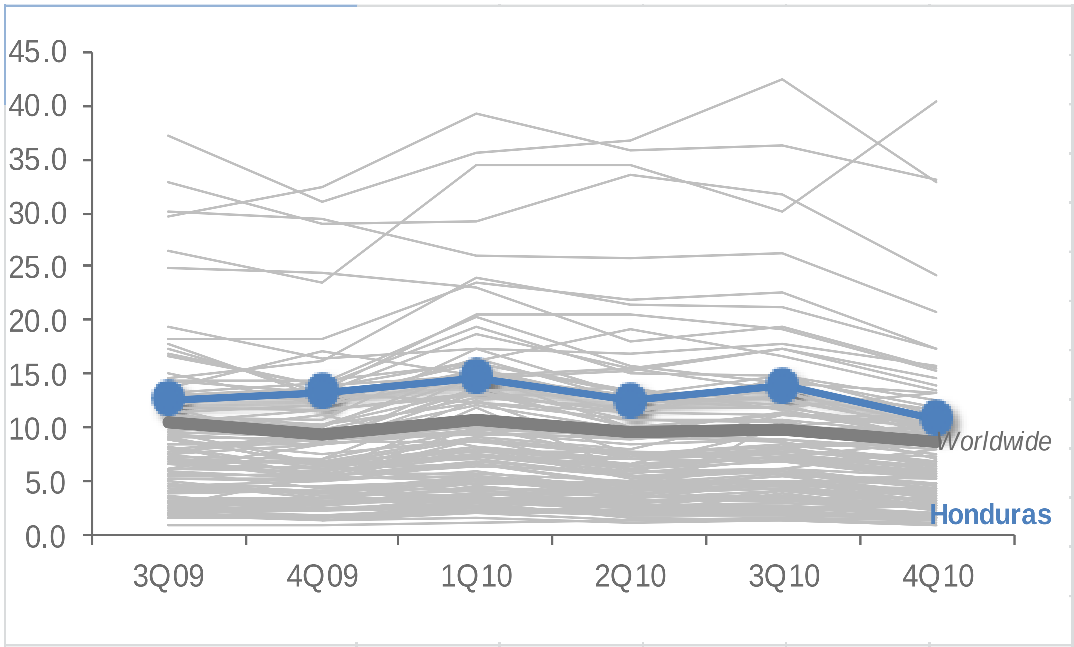
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Honduras in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Honduras and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 14.8 | 12.6 | 13.9 | 11.0 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.37 | | | |
| Malware hosting sites per 1000 hosts | 3.22 | | 2.84 | |
| Percentage of sites hosting drive-by downloads | 0.216% | | 0.058% | |

## Infection Trends (CCM)

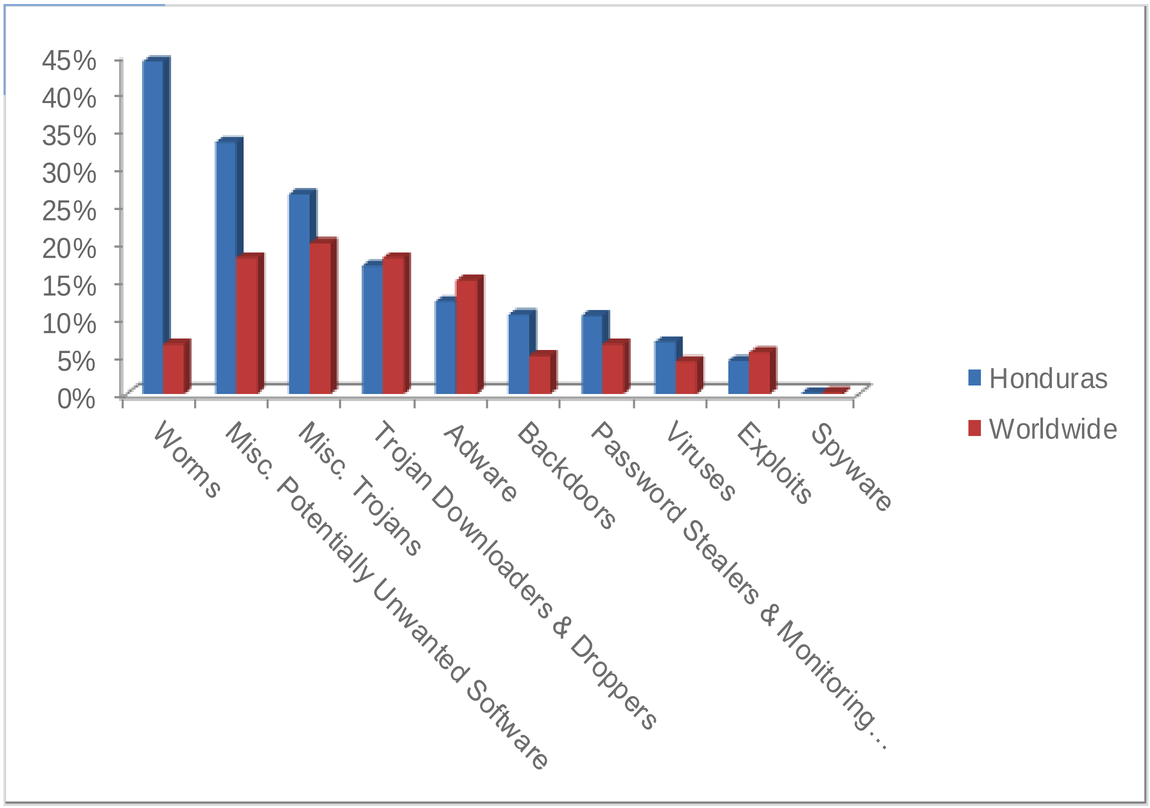
The MSRT detected malware on 11.0 of every 1,000 computers scanned in Honduras in 4Q10 (a CCM score of 11.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Honduras over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Honduras and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Honduras in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Honduras in 4Q10 was Worms, which affected 44.1 percent of all cleaned computers, down from 49.9 percent in 3Q10.
- The second most common category in Honduras in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.4 percent of all cleaned computers, up from 29.1 percent in 3Q10.
- The third most common category in Honduras in 4Q10 was Misc. Trojans, which affected 26.5 percent of all cleaned computers, up from 22.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Honduras in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Vobfus | 20.3% |
| 2 | Win32/Autorun | 20.2% |
| 3 | Win32/Rimecud | 16.6% |
| 4 | Win32/Taterf | 9.2% |
| 5 | Win32/Renos | 7.4% |
| 6 | Win32/Nuqel | 6.8% |
| 7 | Win32/Keygen | 6.3% |
| 8 | Win32/IRCbot | 6.0% |
| 9 | Win32/Frethog | 5.1% |
| 10 | Win32/Conficker | 5.0% |

- The most common threat family in Honduras in 4Q10 was Win32/Vobfus, which affected 20.3 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The second most common threat family in Honduras in 4Q10 was Win32/Autorun, which affected 20.2 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Honduras in 4Q10 was Win32/Rimecud, which affected 16.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Honduras in 4Q10 was Win32/Taterf, which affected 9.2 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Hong Kong

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

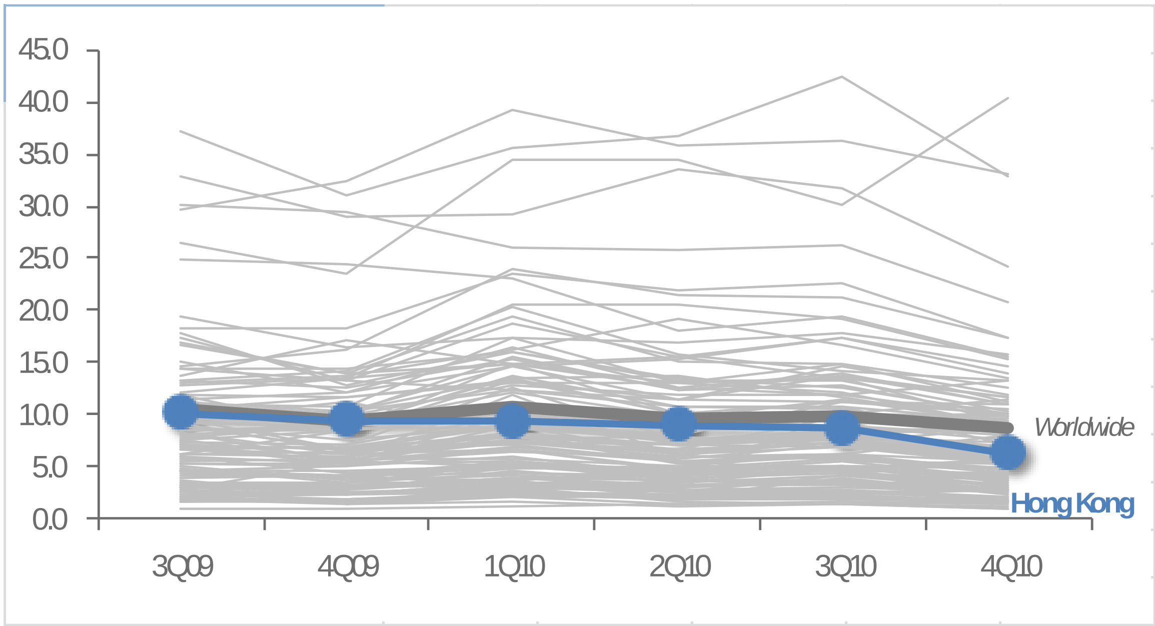
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Hong Kong in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Hong Kong and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">9.4</td><td colspan="3">9.1</td><td colspan="3">8.8</td><td colspan="3">6.3</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.95</td><td colspan="6">4.55</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">4.97</td><td colspan="6">46.28</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.228%</td><td colspan="4">0.091%</td><td colspan="4">0.135%</td></tr>
</table>

## Infection Trends (CCM)

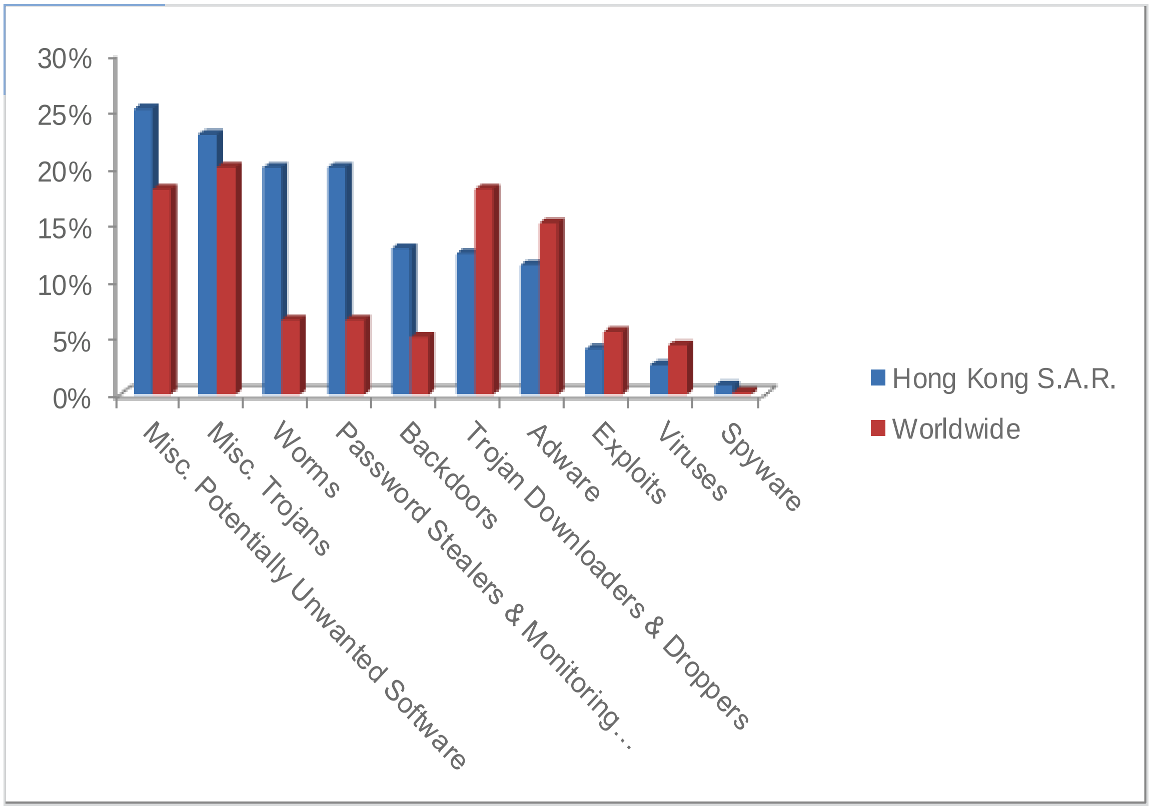
The MSRT detected malware on 6.3 of every 1,000 computers scanned in Hong Kong in 4Q10 (a CCM score of 6.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Hong Kong over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Hong Kong and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Hong Kong in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Hong Kong in 4Q10 was Misc. Potentially Unwanted Software, which affected 25.1 percent of all cleaned computers, down from 28.6 percent in 3Q10.
- The second most common category in Hong Kong in 4Q10 was Misc. Trojans, which affected 22.9 percent of all cleaned computers, down from 23.7 percent in 3Q10.
- The third most common category in Hong Kong in 4Q10 was Worms, which affected 20.0 percent of all cleaned computers, down from 22.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Hong Kong in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Frethog | 16.5% |
| 2 | Win32/Taterf | 9.8% |
| 3 | Win32/IRCbot | 8.4% |
| 4 | Win32/Autorun | 8.0% |
| 5 | JS/Pornpop | 5.4% |
| 6 | Win32/BaiduSobar | 4.1% |
| 7 | Win32/Keygen | 3.9% |
| 8 | Giframe | 3.7% |
| 9 | Win32/Renos | 3.2% |
| 10 | Win32/Rimecud | 3.1% |

- The most common threat family in Hong Kong in 4Q10 was Win32/Frethog, which affected 16.5 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.
- The second most common threat family in Hong Kong in 4Q10 was Win32/Taterf, which affected 9.8 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The third most common threat family in Hong Kong in 4Q10 was Win32/IRCbot, which affected 8.4 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The fourth most common threat family in Hong Kong in 4Q10 was Win32/Autorun, which affected 8.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

# Hungary

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

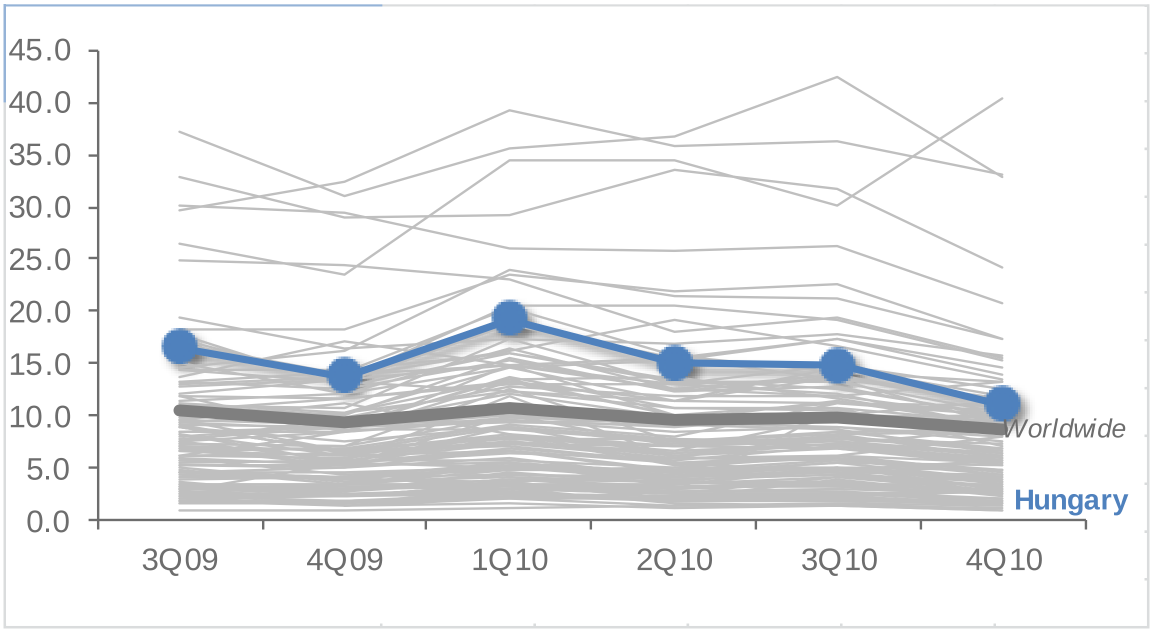
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Hungary in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Hungary and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">19.4</td><td colspan="3">15.2</td><td colspan="3">14.9</td><td colspan="3">11.1</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.48</td><td colspan="6">0.74</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.57</td><td colspan="6">2.05</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.238%</td><td colspan="4">0.142%</td><td colspan="4">0.099%</td></tr>
</table>

## Infection Trends (CCM)

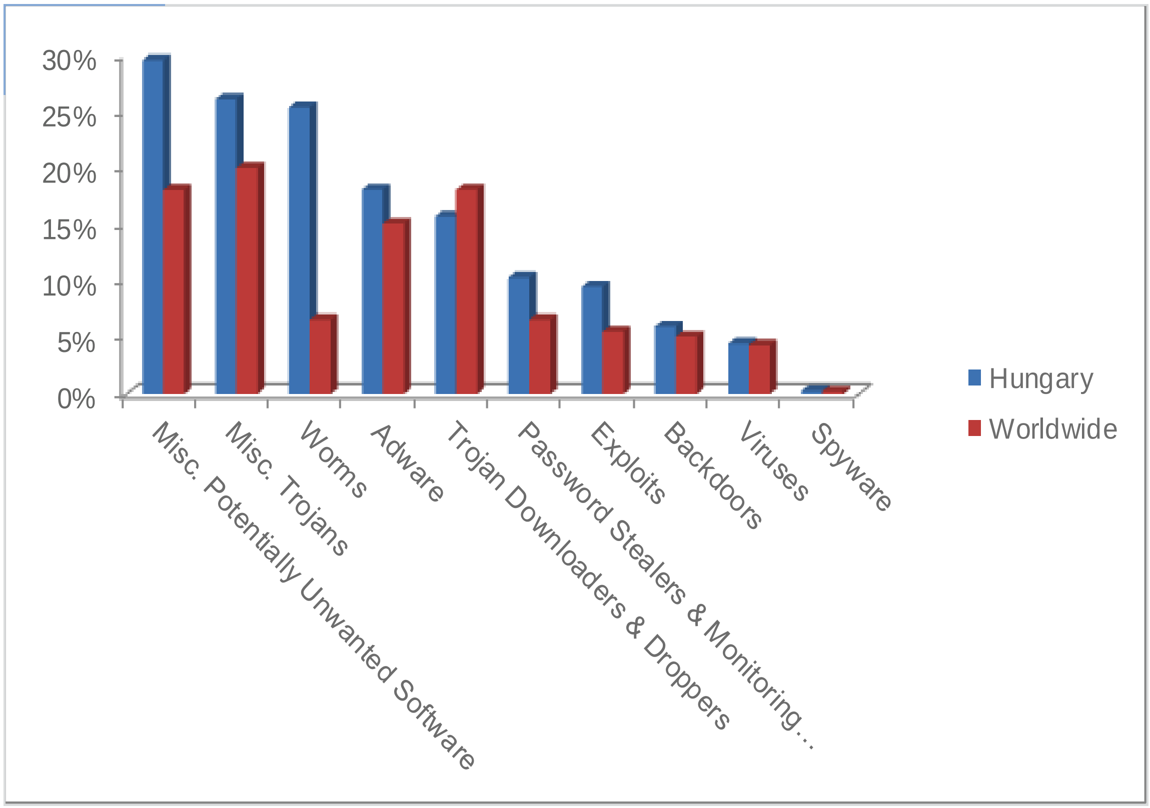
The MSRT detected malware on 11.1 of every 1,000 computers scanned in Hungary in 4Q10 (a CCM score of 11.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Hungary over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Hungary and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Hungary in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Hungary in 4Q10 was Misc. Potentially Unwanted Software, which affected 29.5 percent of all cleaned computers, down from 30.2 percent in 3Q10.
- The second most common category in Hungary in 4Q10 was Misc. Trojans, which affected 26.1 percent of all cleaned computers, down from 28.7 percent in 3Q10.
- The third most common category in Hungary in 4Q10 was Worms, which affected 25.3 percent of all cleaned computers, up from 24.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Hungary in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---:|
| 1 | JS/Pornpop | 11.8% |
| 2 | Win32/Autorun | 9.4% |
| 3 | Win32/Taterf | 7.9% |
| 4 | Win32/Keygen | 7.5% |
| 5 | HTML/IframeRef | 7.3% |
| 6 | Win32/Renos | 6.8% |
| 7 | Win32/Conficker | 6.3% |
| 8 | Win32/Frethog | 5.4% |
| 9 | Win32/Obfuscator | 3.8% |
| 10 | Win32/Rimecud | 3.4% |

- The most common threat family in Hungary in 4Q10 was JS/Pornpop, which affected 11.8 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Hungary in 4Q10 was Win32/Autorun, which affected 9.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Hungary in 4Q10 was Win32/Taterf, which affected 7.9 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Hungary in 4Q10 was Win32/Keygen, which affected 7.5 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.

# Iceland

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

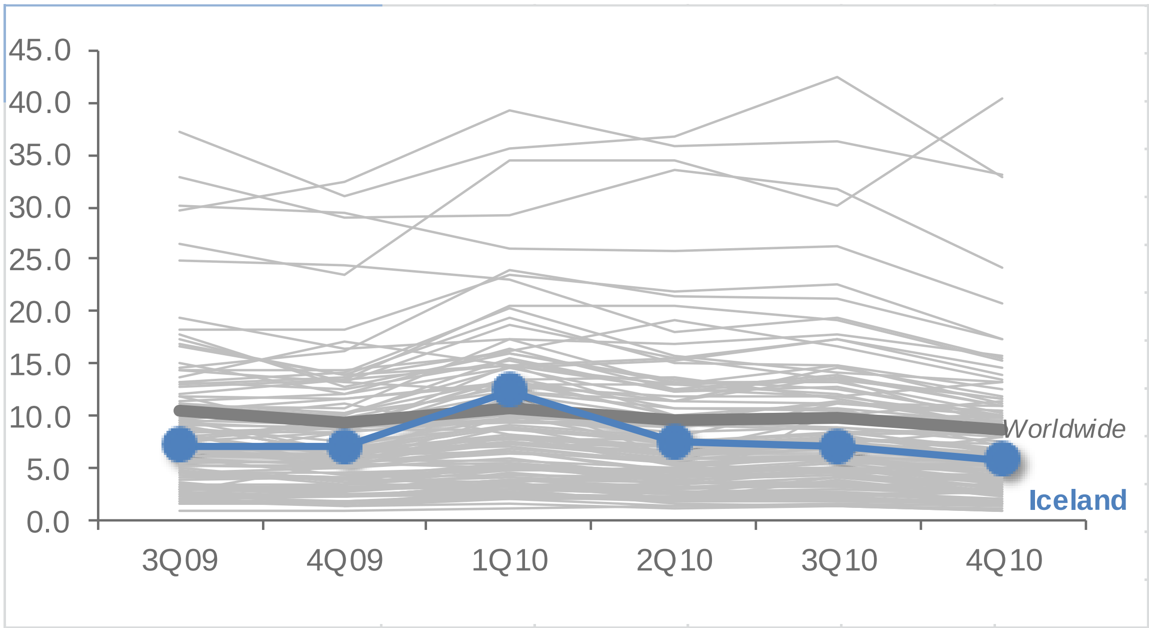
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Iceland in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Iceland and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">12.5</td><td colspan="3">7.7</td><td colspan="3">7.1</td><td colspan="3">5.9</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.08</td><td colspan="6">0.19</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.14</td><td colspan="6">0.12</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.198%</td><td colspan="4">0.032%</td><td colspan="4">0.041%</td></tr>
</table>

## Infection Trends (CCM)

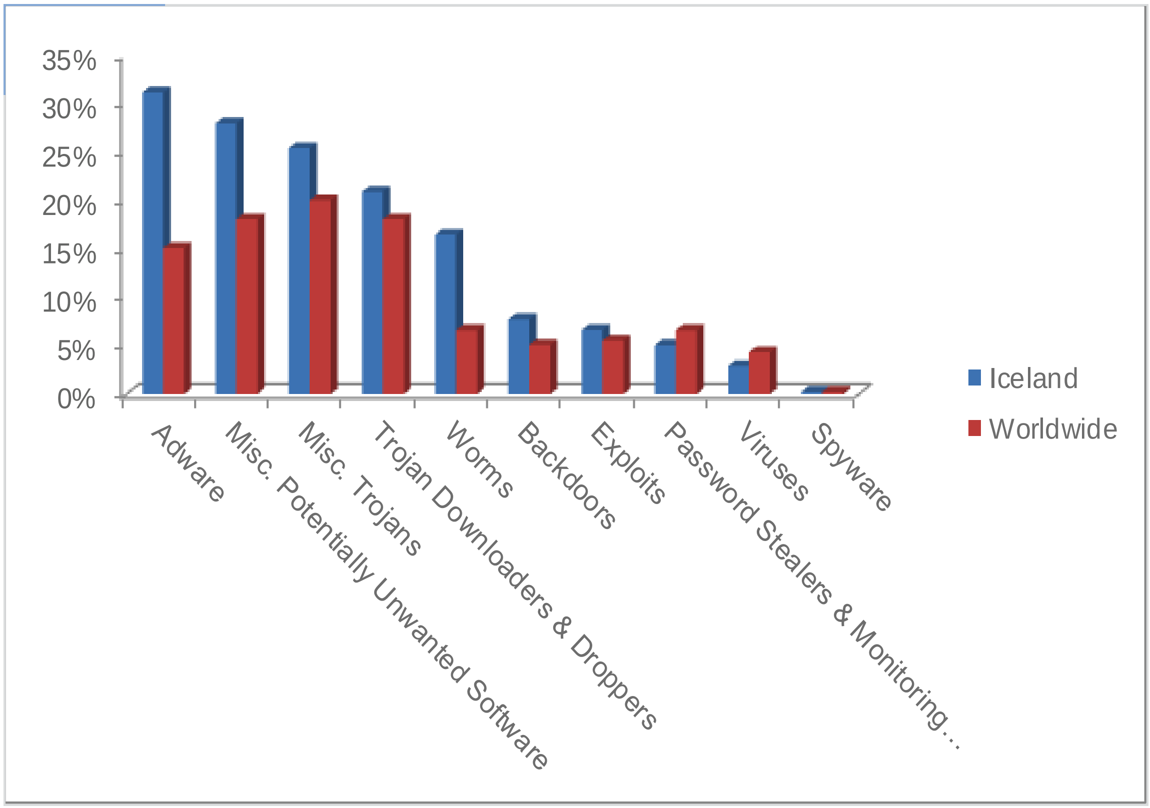
The MSRT detected malware on 5.9 of every 1,000 computers scanned in Iceland in 4Q10 (a CCM score of 5.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Iceland over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Iceland and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Iceland in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Iceland in 4Q10 was Adware, which affected 31.1 percent of all cleaned computers, up from 29.3 percent in 3Q10.
- The second most common category in Iceland in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.9 percent of all cleaned computers, up from 26.5 percent in 3Q10.
- The third most common category in Iceland in 4Q10 was Misc. Trojans, which affected 25.4 percent of all cleaned computers, down from 25.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Iceland in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 14.7% |
| 2 | Win32/ClickPotato | 9.4% |
| 3 | Win32/Renos | 7.5% |
| 4 | Win32/Zwangi | 7.5% |
| 5 | Win32/Rimecud | 6.4% |
| 6 | Win32/Hotbar | 5.9% |
| 7 | Win32/Keygen | 5.0% |
| 8 | Win32/Autorun | 4.4% |
| 9 | Win32/IRCbot | 4.0% |
| 10 | Win32/Conficker | 2.8% |

- The most common threat family in Iceland in 4Q10 was JS/Pornpop, which affected 14.7 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Iceland in 4Q10 was Win32/ClickPotato, which affected 9.4 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Iceland in 4Q10 was Win32/Renos, which affected 7.5 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.
- The fourth most common threat family in Iceland in 4Q10 was Win32/Zwangi, which affected 7.5 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# India

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

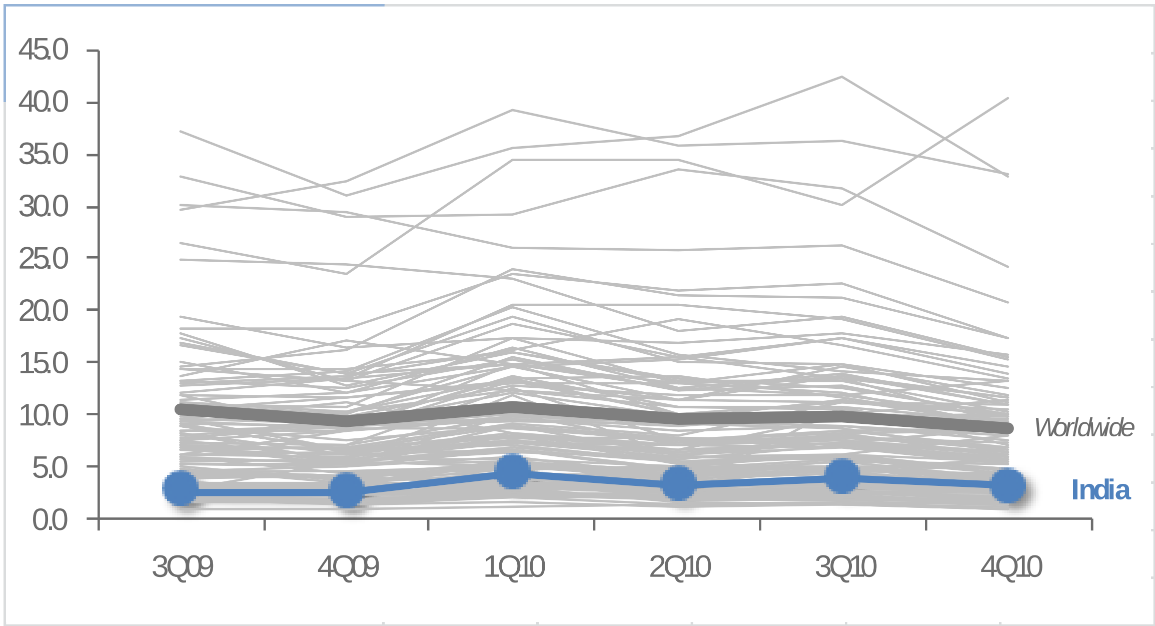
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in India in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in India and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 4.6 | 3.4 | 4.1 | 3.2 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.60 | | 0.14 | |
| Malware hosting sites per 1000 hosts | 0.69 | | 0.70 | |
| Percentage of sites hosting drive-by downloads | 0.267% | 0.210% | | 0.150% |

## Infection Trends (CCM)

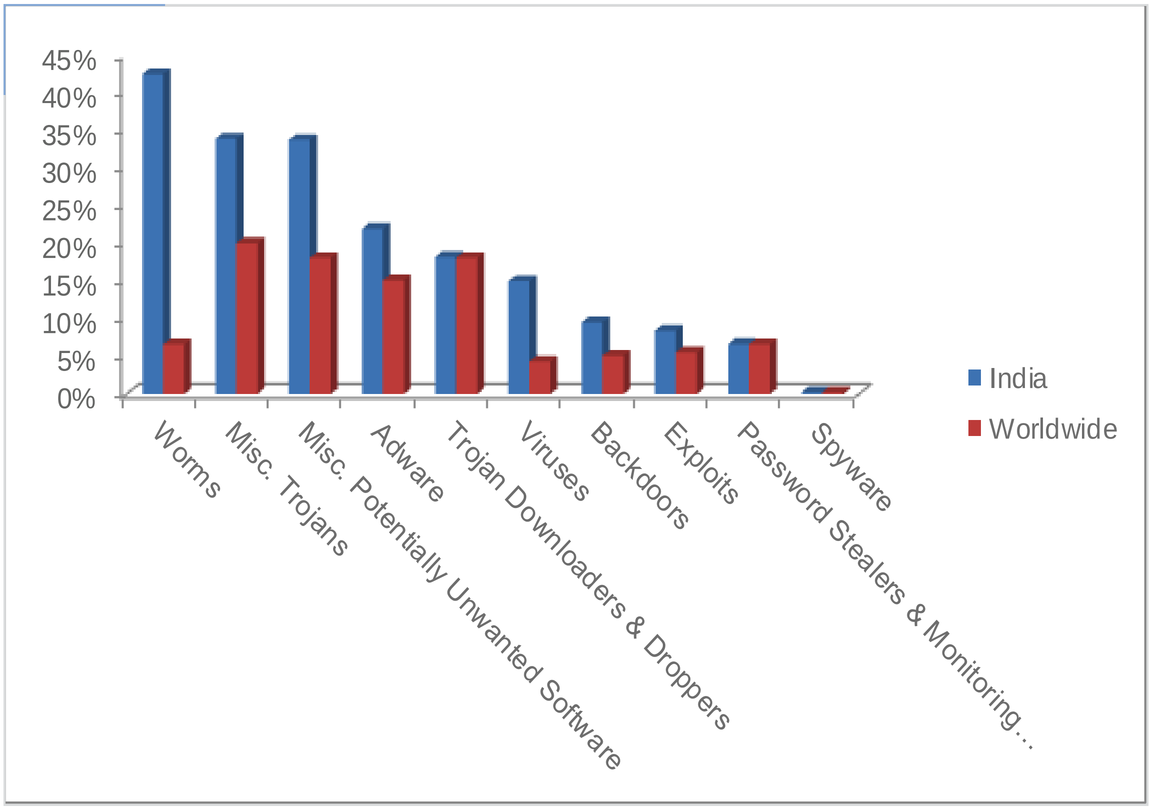
The MSRT detected malware on 3.2 of every 1,000 computers scanned in India in 4Q10 (a CCM score of 3.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for India over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in India and worldwide



## Threat Categories

Malware and potentially unwanted software categories in India in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in India in 4Q10 was Worms, which affected 42.5 percent of all cleaned computers, down from 45.4 percent in 3Q10.
- The second most common category in India in 4Q10 was Misc. Trojans, which affected 33.9 percent of all cleaned computers, down from 34.5 percent in 3Q10.
- The third most common category in India in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.7 percent of all cleaned computers, up from 31.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in India in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 28.4% |
| 2 | Win32/Rimecud | 23.0% |
| 3 | JS/Pornpop | 13.2% |
| 4 | Win32/Sality | 11.0% |
| 5 | Win32/Conficker | 6.8% |
| 6 | Win32/Nuqel | 6.6% |
| 7 | Win32/Vobfus | 6.5% |
| 8 | Win32/Renos | 6.4% |
| 9 | CplLnk | 4.8% |
| 10 | Win32/ClickPotato | 4.8% |

- The most common threat family in India in 4Q10 was Win32/Autorun, which affected 28.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in India in 4Q10 was Win32/Rimecud, which affected 23.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in India in 4Q10 was JS/Pornpop, which affected 13.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in India in 4Q10 was Win32/Sality, which affected 11.0 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Indonesia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

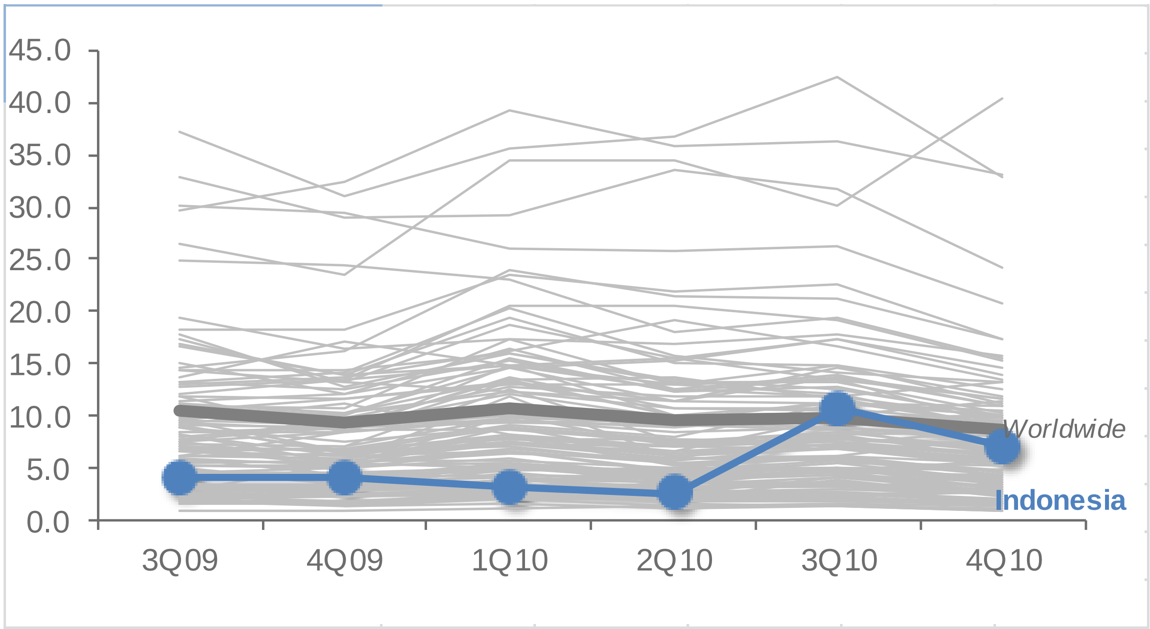
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Indonesia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Indonesia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">3.2</td><td colspan="3">2.7</td><td colspan="3">10.8</td><td colspan="3">7.1</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.65</td><td colspan="6">0.99</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.54</td><td colspan="6">0.43</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.485%</td><td colspan="4">0.146%</td><td colspan="4">0.091%</td></tr>
</table>

## Infection Trends (CCM)

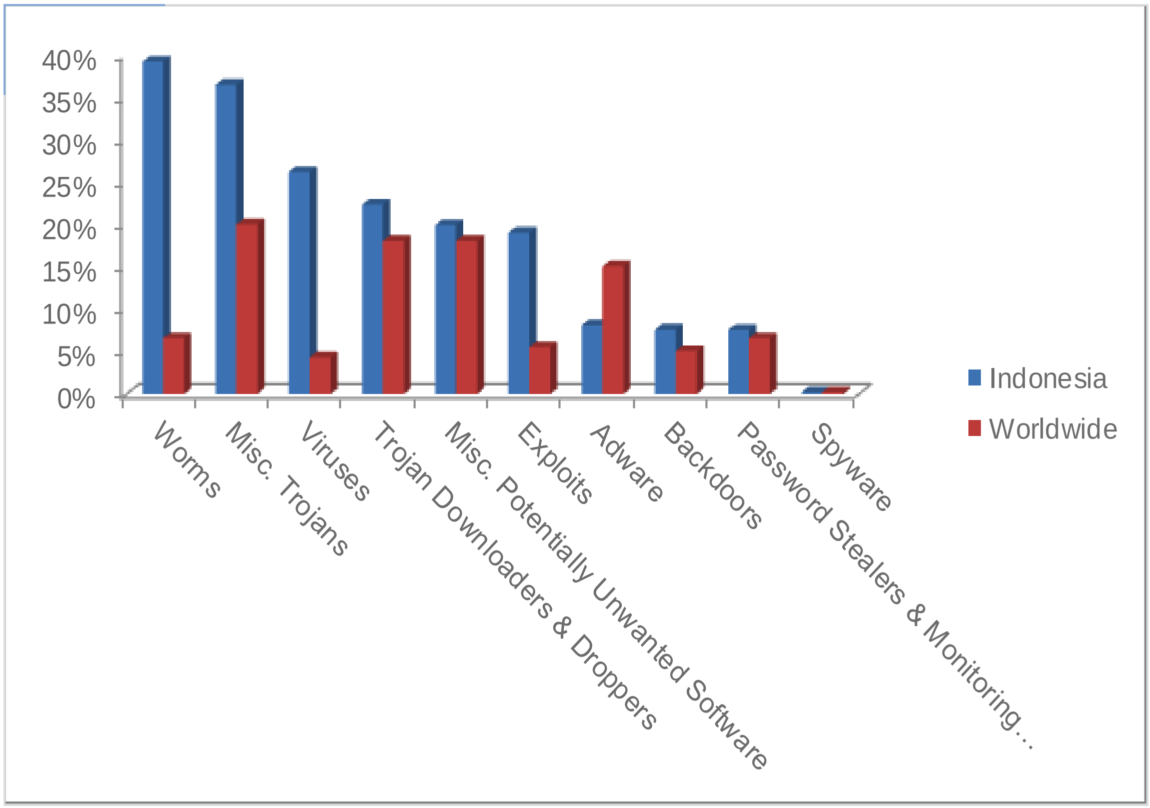
The MSRT detected malware on 7.1 of every 1,000 computers scanned in Indonesia in 4Q10 (a CCM score of 7.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Indonesia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Indonesia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Indonesia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Indonesia in 4Q10 was Worms, which affected 39.2 percent of all cleaned computers, down from 51.5 percent in 3Q10.
- The second most common category in Indonesia in 4Q10 was Misc. Trojans, which affected 36.5 percent of all cleaned computers, up from 30.8 percent in 3Q10.
- The third most common category in Indonesia in 4Q10 was Viruses, which affected 26.2 percent of all cleaned computers, up from 20.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Indonesia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Stuxnet | 22.1% |
| 2 | Win32/Vobfus | 18.1% |
| 3 | Win32/Sality | 17.0% |
| 4 | CplLnk | 16.9% |
| 5 | Win32/Conficker | 11.2% |
| 6 | Win32/Autorun | 10.5% |
| 7 | Win32/Virut | 9.4% |
| 8 | Win32/Renos | 5.8% |
| 9 | Cantix | 5.0% |
| 10 | Win32/Keygen | 4.9% |

- The most common threat family in Indonesia in 4Q10 was Win32/Stuxnet, which affected 22.1 percent of cleaned computers. Win32/Stuxnet is a multi-component family that spreads via removable volumes by exploiting the vulnerability addressed by Microsoft Security Bulletin MS10-046.
- The second most common threat family in Indonesia in 4Q10 was Win32/Vobfus, which affected 18.1 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The third most common threat family in Indonesia in 4Q10 was Win32/Sality, which affected 17.0 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Indonesia in 4Q10 was CplLnk, which affected 16.9 percent of cleaned computers. CplLnk is

# Iraq

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

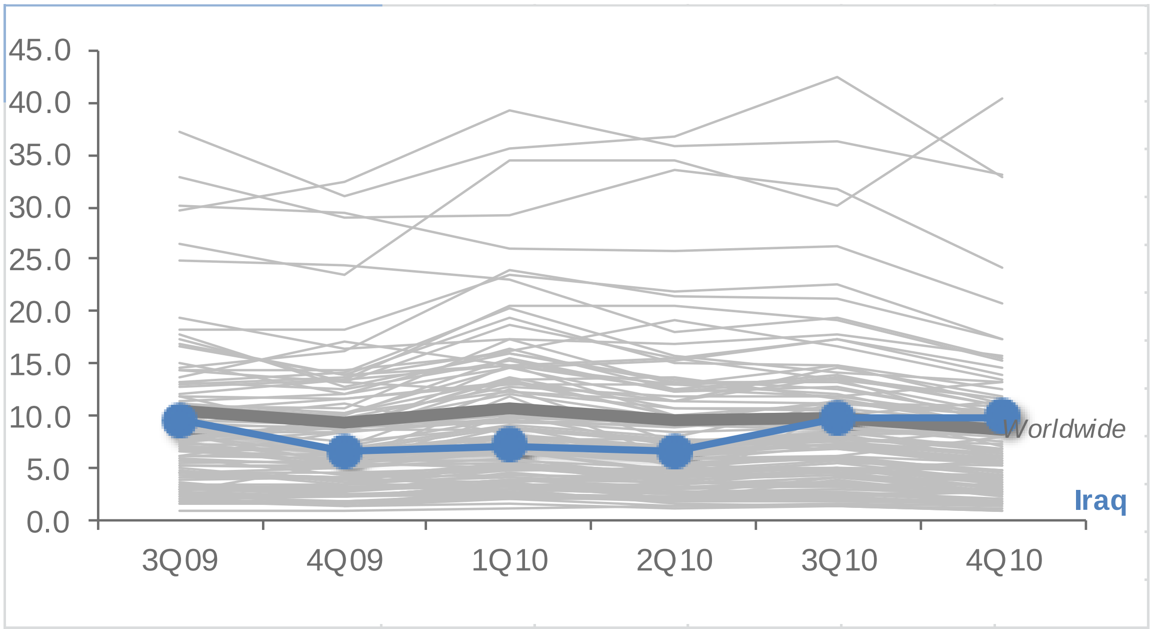
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Iraq in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Iraq and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 7.2 | 6.7 | 9.8 | 10.0 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 333.33 | | | |
| Malware hosting sites per 1000 hosts | 12666.67 | | 43666.67 | |
| Percentage of sites hosting drive-by downloads | 1.948% | 2.073% | | |

## Infection Trends (CCM)

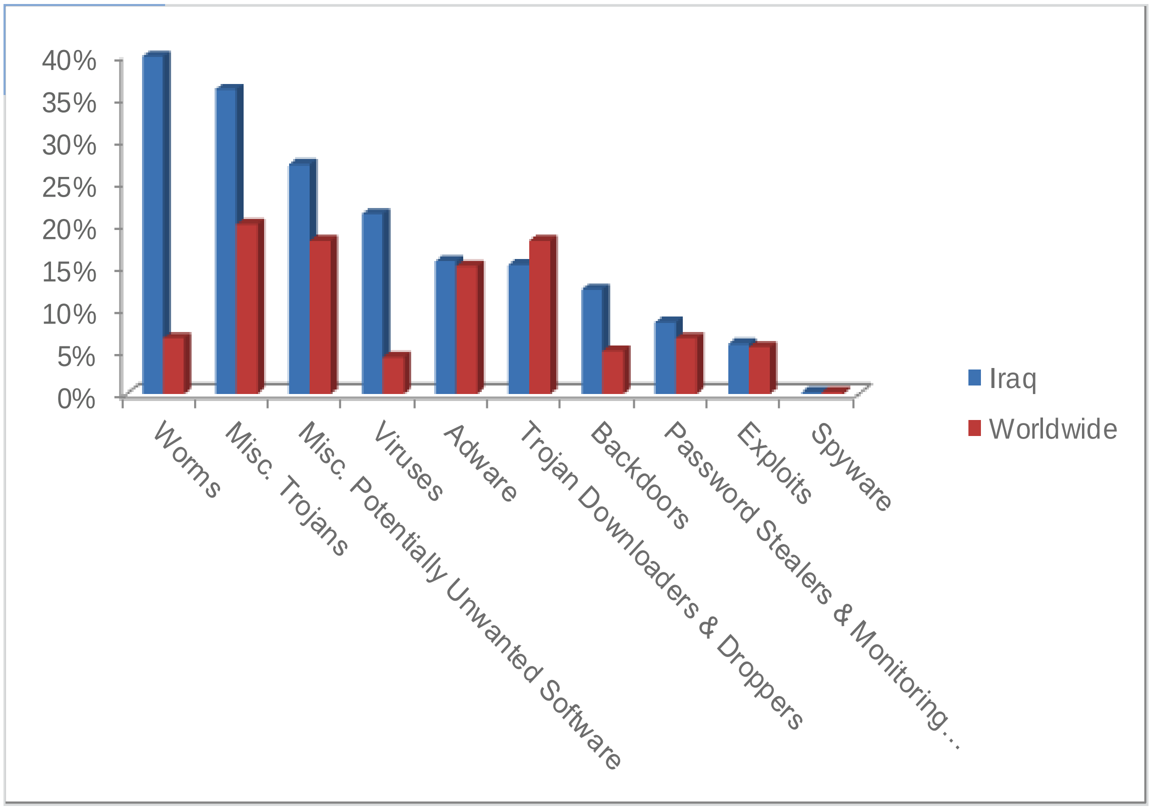
The MSRT detected malware on 10.0 of every 1,000 computers scanned in Iraq in 4Q10 (a CCM score of 10.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Iraq over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Iraq and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Iraq in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Iraq in 4Q10 was Worms, which affected 39.8 percent of all cleaned computers, up from 37.8 percent in 3Q10.
- The second most common category in Iraq in 4Q10 was Misc. Trojans, which affected 35.9 percent of all cleaned computers, up from 31.5 percent in 3Q10.
- The third most common category in Iraq in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.1 percent of all cleaned computers, up from 21.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Iraq in 4Q10.

|  | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Sality | 21.2% |
| 2 | Win32/Autorun | 18.6% |
| 3 | Win32/Vobfus | 10.3% |
| 4 | JS/Pornpop | 9.4% |
| 5 | Win32/Stuxnet | 8.6% |
| 6 | Win32/Agent | 8.4% |
| 7 | Win32/Taterf | 7.8% |
| 8 | Win32/Conficker | 6.9% |
| 9 | Win32/Rimecud | 6.5% |
| 10 | Win32/Keygen | 5.8% |

- The most common threat family in Iraq in 4Q10 was Win32/Sality, which affected 21.2 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family in Iraq in 4Q10 was Win32/Autorun, which affected 18.6 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Iraq in 4Q10 was Win32/Vobfus, which affected 10.3 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Iraq in 4Q10 was JS/Pornpop, which affected 9.4 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Ireland

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

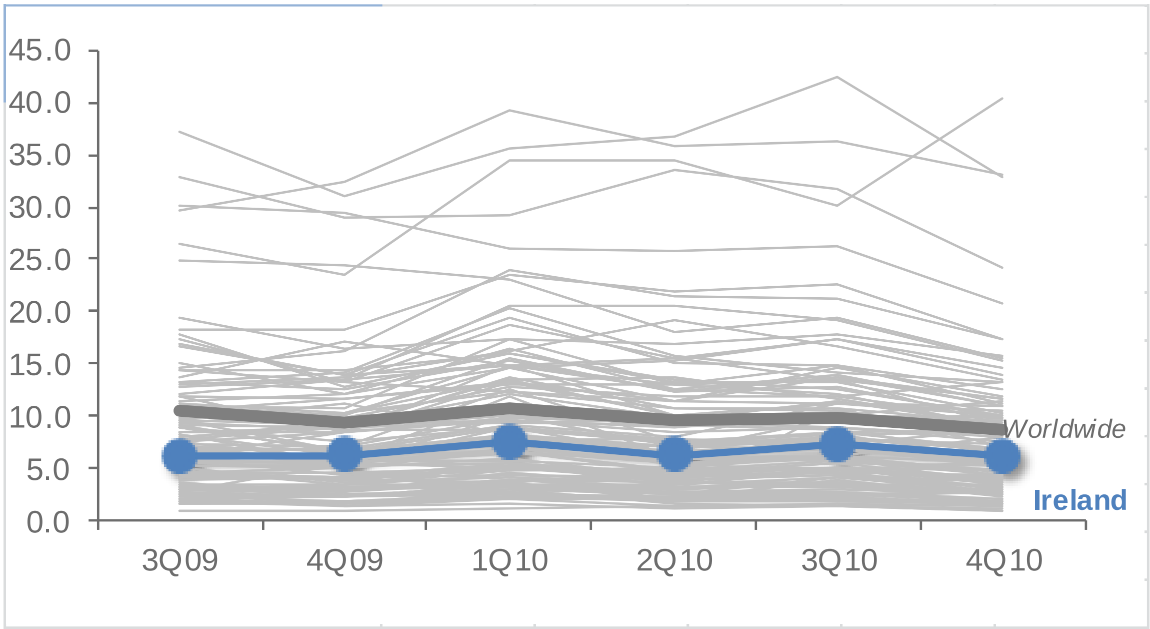
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Ireland in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Ireland and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">7.6</td><td colspan="3">6.4</td><td colspan="3">7.3</td><td colspan="3">6.2</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.05</td><td colspan="6">1.45</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.69</td><td colspan="6">2.71</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.134%</td><td colspan="4">0.066%</td><td colspan="4">0.082%</td></tr>
</table>

## Infection Trends (CCM)

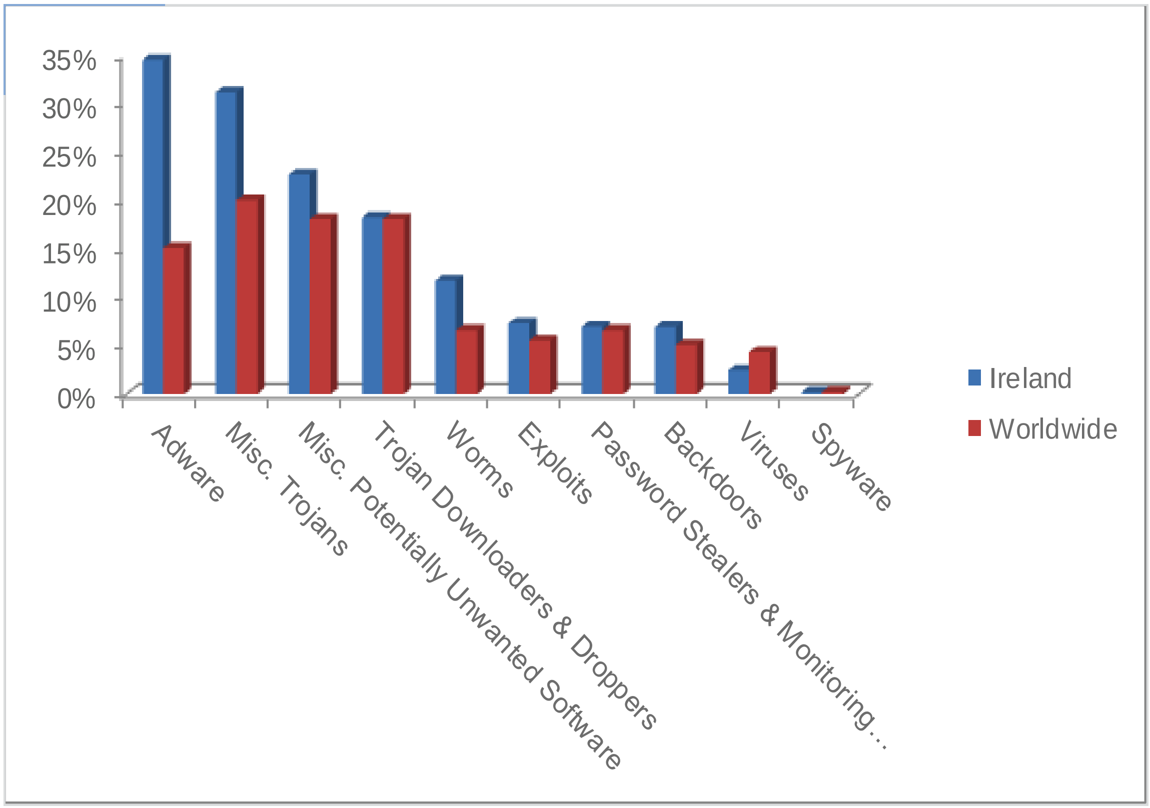
The MSRT detected malware on 6.2 of every 1,000 computers scanned in Ireland in 4Q10 (a CCM score of 6.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Ireland over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Ireland and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Ireland in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Ireland in 4Q10 was Adware, which affected 34.5 percent of all cleaned computers, down from 33.8 percent in 3Q10.
- The second most common category in Ireland in 4Q10 was Misc. Trojans, which affected 31.1 percent of all cleaned computers, up from 29.4 percent in 3Q10.
- The third most common category in Ireland in 4Q10 was Misc. Potentially Unwanted Software, which affected 22.6 percent of all cleaned computers, up from 22.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Ireland in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 14.8% |
| 2 | Win32/ClickPotato | 11.1% |
| 3 | Win32/Zwangi | 8.2% |
| 4 | Win32/Hotbar | 7.8% |
| 5 | Win32/Renos | 6.3% |
| 6 | Win32/Zbot | 4.4% |
| 7 | Win32/FakeSpypro | 4.2% |
| 8 | Win32/Autorun | 4.0% |
| 9 | Win32/Winwebsec | 3.7% |
| 10 | Java/CVE-2008-5353 | 3.5% |

- The most common threat family in Ireland in 4Q10 was JS/Pornpop, which affected 14.8 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Ireland in 4Q10 was Win32/ClickPotato, which affected 11.1 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Ireland in 4Q10 was Win32/Zwangi, which affected 8.2 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in Ireland in 4Q10 was Win32/Hotbar, which affected 7.8 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

# Israel

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

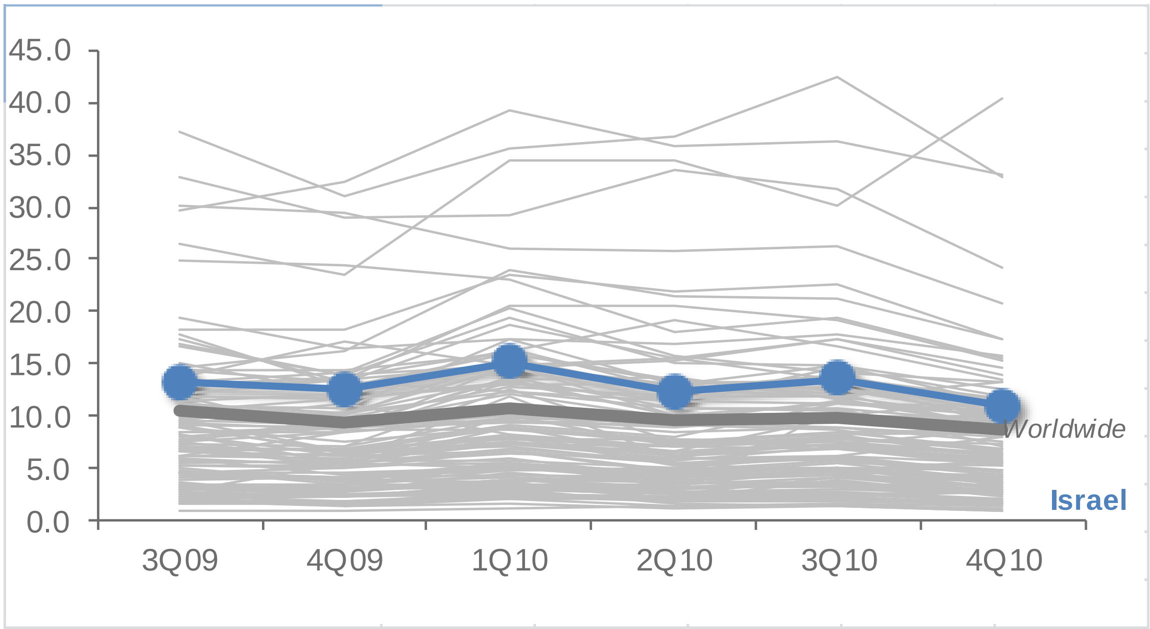
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Israel in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Israel and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">15.2</td><td colspan="3">12.2</td><td colspan="3">13.6</td><td colspan="3">11.0</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.39</td><td colspan="6">0.13</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">9.40</td><td colspan="6">43.70</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.242%</td><td colspan="4">0.097%</td><td colspan="4">0.081%</td></tr>
</table>

## Infection Trends (CCM)

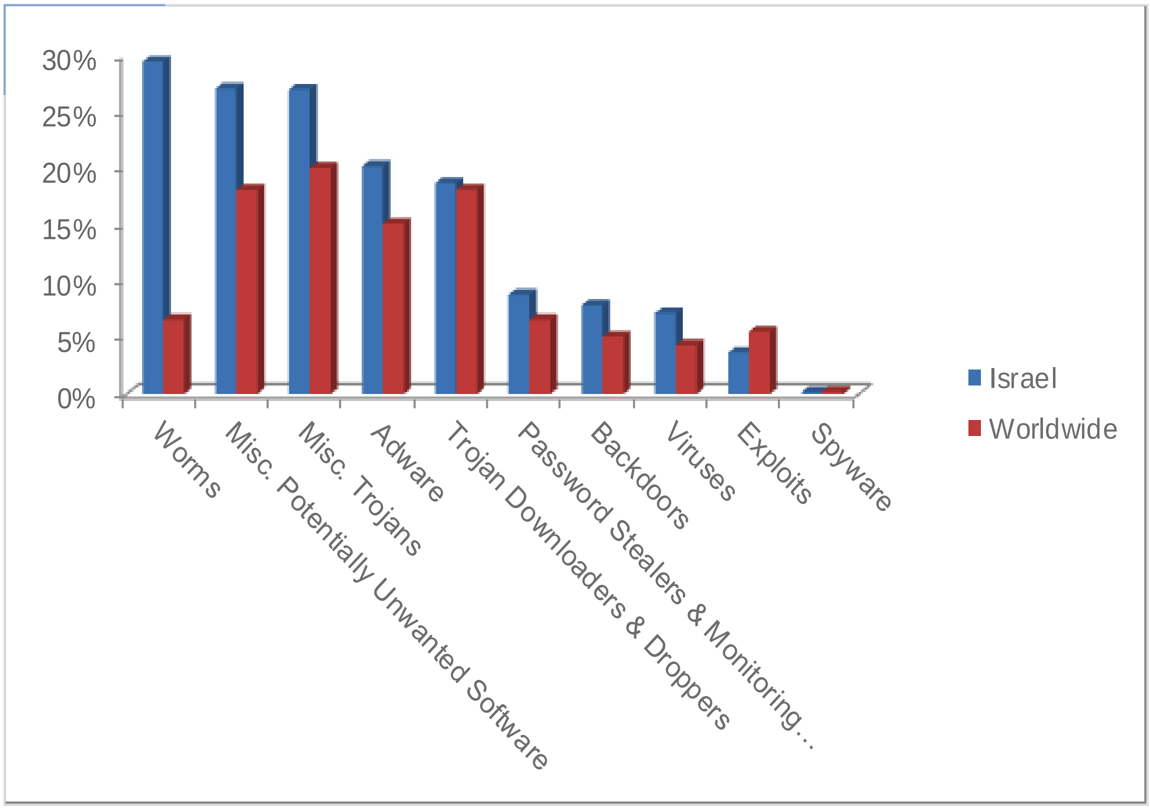
The MSRT detected malware on 11.0 of every 1,000 computers scanned in Israel in 4Q10 (a CCM score of 11.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Israel over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Israel and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Israel in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Israel in 4Q10 was Worms, which affected 29.4 percent of all cleaned computers, up from 26.2 percent in 3Q10.
- The second most common category in Israel in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.0 percent of all cleaned computers, up from 24.5 percent in 3Q10.
- The third most common category in Israel in 4Q10 was Misc. Trojans, which affected 26.9 percent of all cleaned computers, up from 19.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Israel in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 11.4% |
| 2 | JS/Pornpop | 10.6% |
| 3 | Win32/Rimecud | 6.6% |
| 4 | Win32/Renos | 6.2% |
| 5 | Win32/Taterf | 5.6% |
| 6 | ASX/Wimad | 5.2% |
| 7 | Win32/Keygen | 4.9% |
| 8 | Win32/Frethog | 4.0% |
| 9 | Win32/IRCbot | 3.9% |
| 10 | Win32/Brontok | 3.9% |

- The most common threat family in Israel in 4Q10 was Win32/Autorun, which affected 11.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Israel in 4Q10 was JS/Pornpop, which affected 10.6 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Israel in 4Q10 was Win32/Rimecud, which affected 6.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Israel in 4Q10 was Win32/Renos, which affected 6.2 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.

# Italy

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

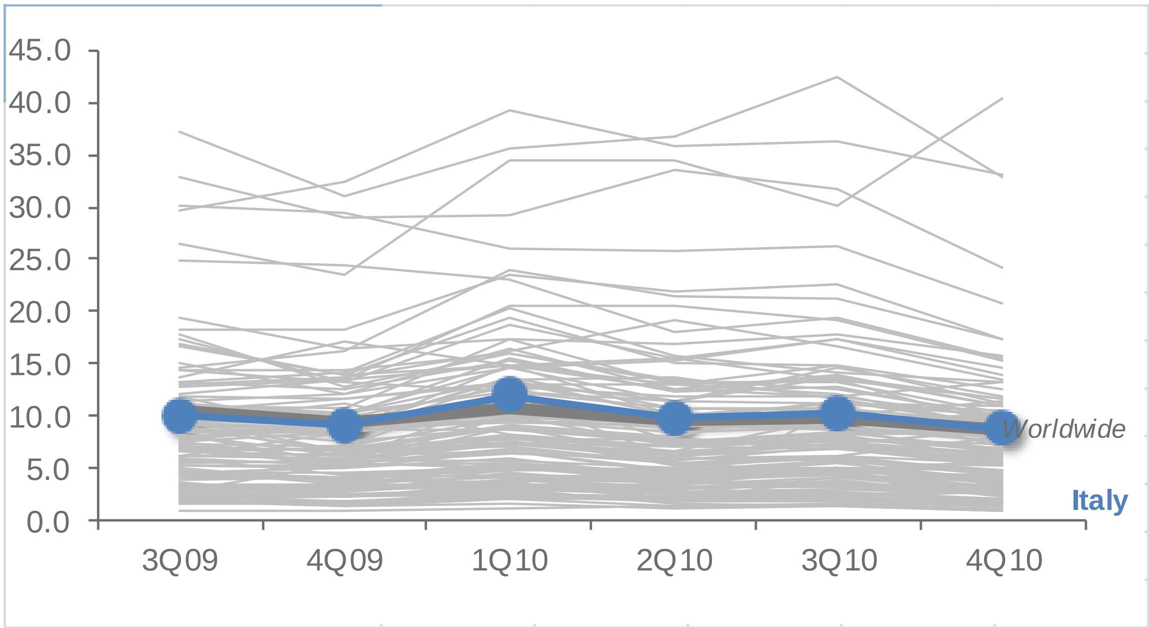
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Italy in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Italy and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">12.0</td><td colspan="3">9.7</td><td colspan="3">10.3</td><td colspan="3">8.9</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.33</td><td colspan="6">0.29</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.51</td><td colspan="6">0.25</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.173%</td><td colspan="4">0.037%</td><td colspan="4">0.211%</td></tr>
</table>

## Infection Trends (CCM)

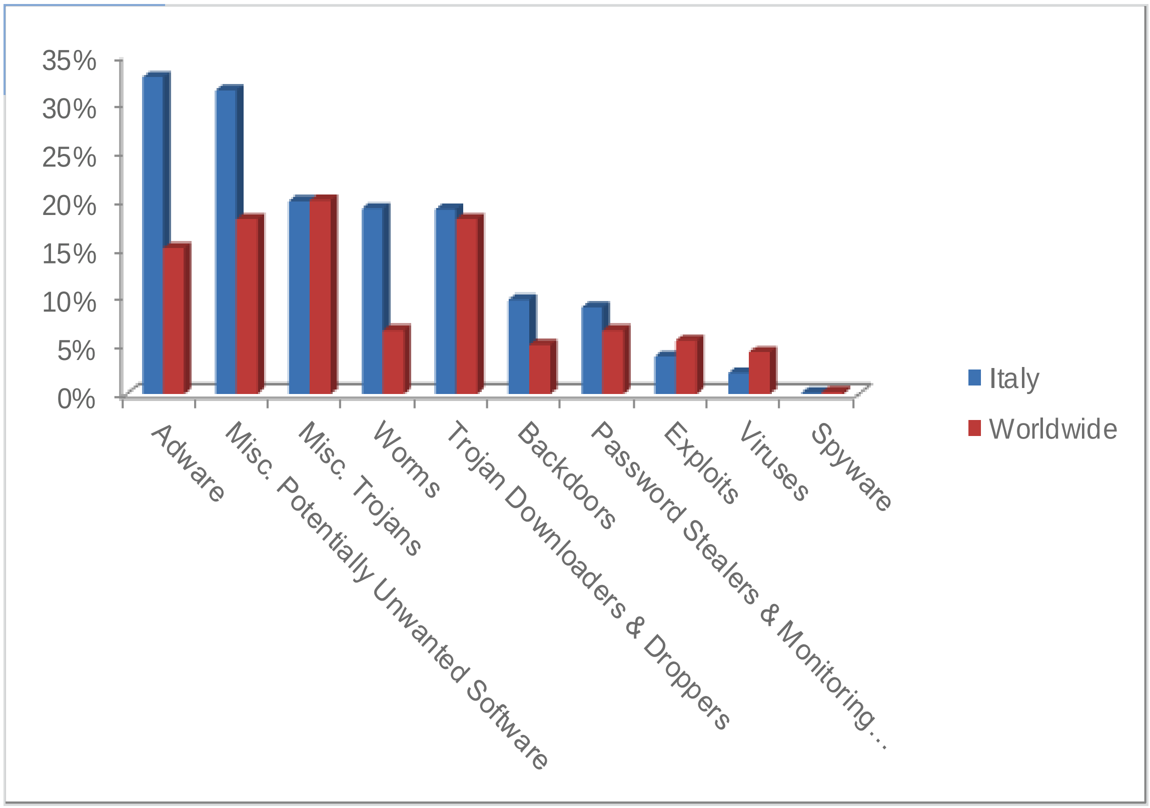
The MSRT detected malware on 8.9 of every 1,000 computers scanned in Italy in 4Q10 (a CCM score of 8.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Italy over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Italy and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Italy in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Italy in 4Q10 was Adware, which affected 32.7 percent of all cleaned computers, up from 29.3 percent in 3Q10.
- The second most common category in Italy in 4Q10 was Misc. Potentially Unwanted Software, which affected 31.4 percent of all cleaned computers, up from 23.9 percent in 3Q10.
- The third most common category in Italy in 4Q10 was Misc. Trojans, which affected 19.9 percent of all cleaned computers, down from 23.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Italy in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 16.1% |
| 2 | Win32/Hotbar | 11.3% |
| 3 | Win32/Zwangi | 9.8% |
| 4 | ASX/Wimad | 8.5% |
| 5 | Win32/IRCbot | 6.7% |
| 6 | Win32/Autorun | 6.5% |
| 7 | Win32/ClickPotato | 6.1% |
| 8 | Win32/Conficker | 6.0% |
| 9 | Win32/Renos | 5.7% |
| 10 | Win32/Taterf | 4.8% |

- The most common threat family in Italy in 4Q10 was JS/Pornpop, which affected 16.1 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Italy in 4Q10 was Win32/Hotbar, which affected 11.3 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.
- The third most common threat family in Italy in 4Q10 was Win32/Zwangi, which affected 9.8 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in Italy in 4Q10 was ASX/Wimad, which affected 8.5 percent of cleaned computers. ASX/Wimad is a detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.

# Jamaica

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

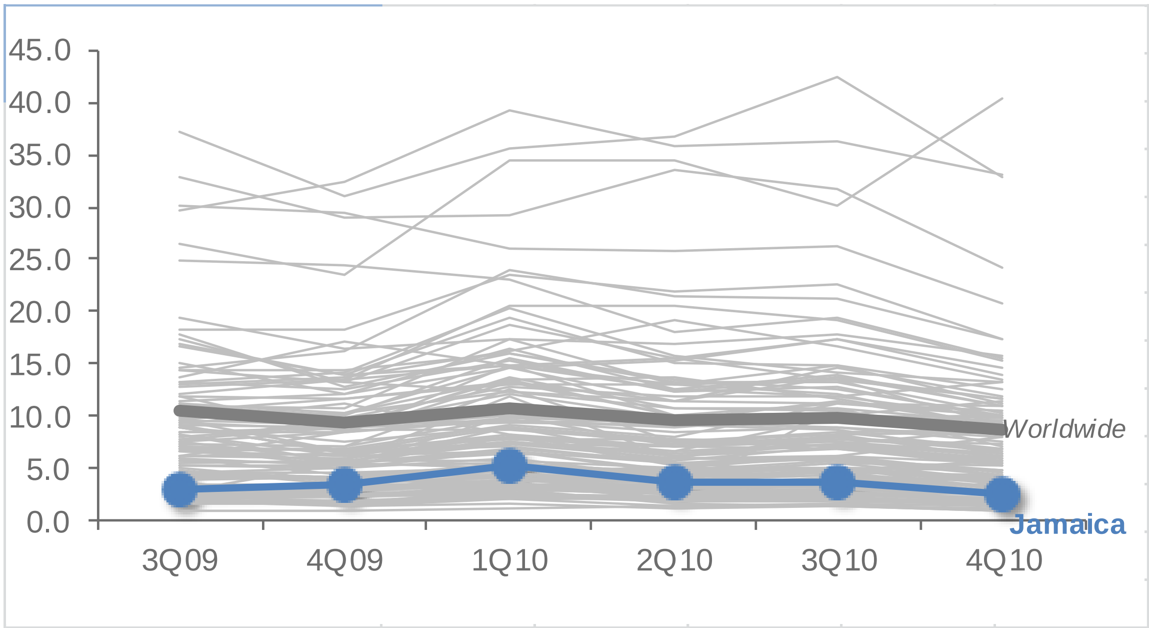
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Jamaica in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Jamaica and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 5.4 | 3.7 | 3.6 | 2.5 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 13.93 | | 2.32 | |
| Malware hosting sites per 1000 hosts | 1662.54 | | 24.77 | |
| Percentage of sites hosting drive-by downloads | 0.105% | 0.220% | 0.106% | |

## Infection Trends (CCM)

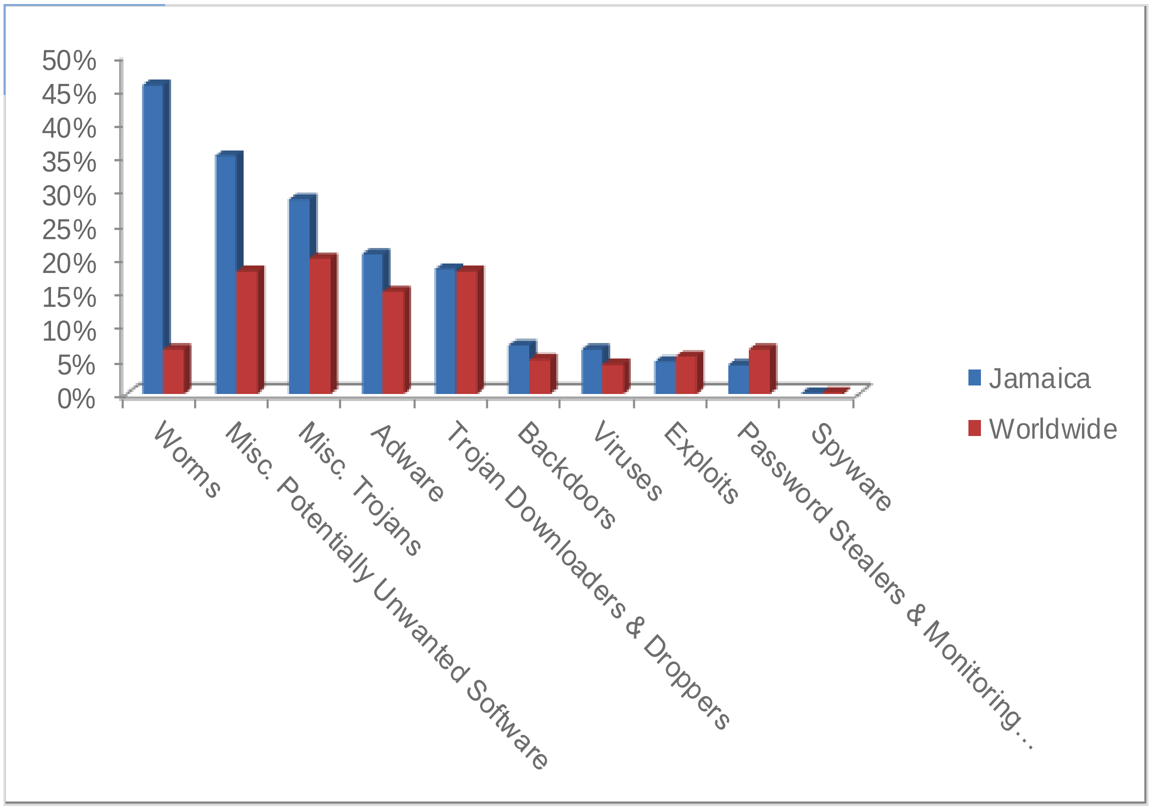
The MSRT detected malware on 2.5 of every 1,000 computers scanned in Jamaica in 4Q10 (a CCM score of 2.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Jamaica over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Jamaica and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Jamaica in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Jamaica in 4Q10 was Worms, which affected 45.5 percent of all cleaned computers, down from 52.7 percent in 3Q10.
- The second most common category in Jamaica in 4Q10 was Misc. Potentially Unwanted Software, which affected 35.1 percent of all cleaned computers, up from 30.4 percent in 3Q10.
- The third most common category in Jamaica in 4Q10 was Misc. Trojans, which affected 28.7 percent of all cleaned computers, up from 24.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Jamaica in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 25.8% |
| 2 | Win32/Rimecud | 22.6% |
| 3 | Win32/Vobfus | 14.1% |
| 4 | Win32/Hamweq | 12.5% |
| 5 | Win32/ClickPotato | 8.7% |
| 6 | Win32/Renos | 7.9% |
| 7 | Win32/Zwangi | 6.5% |
| 8 | JS/Pornpop | 5.7% |
| 9 | Win32/VBInject | 5.5% |
| 10 | Win32/Hotbar | 5.5% |

- The most common threat family in Jamaica in 4Q10 was Win32/Autorun, which affected 25.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Jamaica in 4Q10 was Win32/Rimecud, which affected 22.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Jamaica in 4Q10 was Win32/Vobfus, which affected 14.1 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Jamaica in 4Q10 was Win32/Hamweq, which affected 12.5 percent of cleaned computers. Win32/Hamweq is a worm that spreads through removable drives, such as USB memory sticks. It may contain an IRC-based backdoor that enables the computer to be controlled remotely by an attacker.

# Japan

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

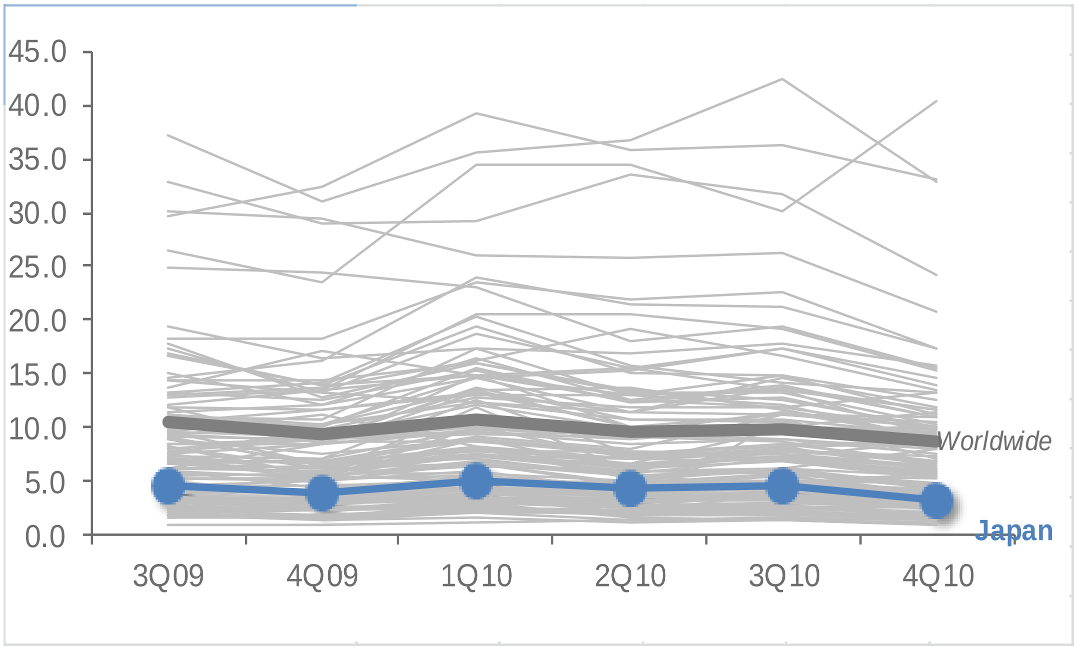
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Japan in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Japan and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">5.1</td><td colspan="3">4.4</td><td colspan="3">4.6</td><td colspan="3">3.3</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.06</td><td colspan="6">0.04</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.09</td><td colspan="6">0.09</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.136%</td><td colspan="4">0.022%</td><td colspan="4">0.032%</td></tr>
</table>

## Infection Trends (CCM)

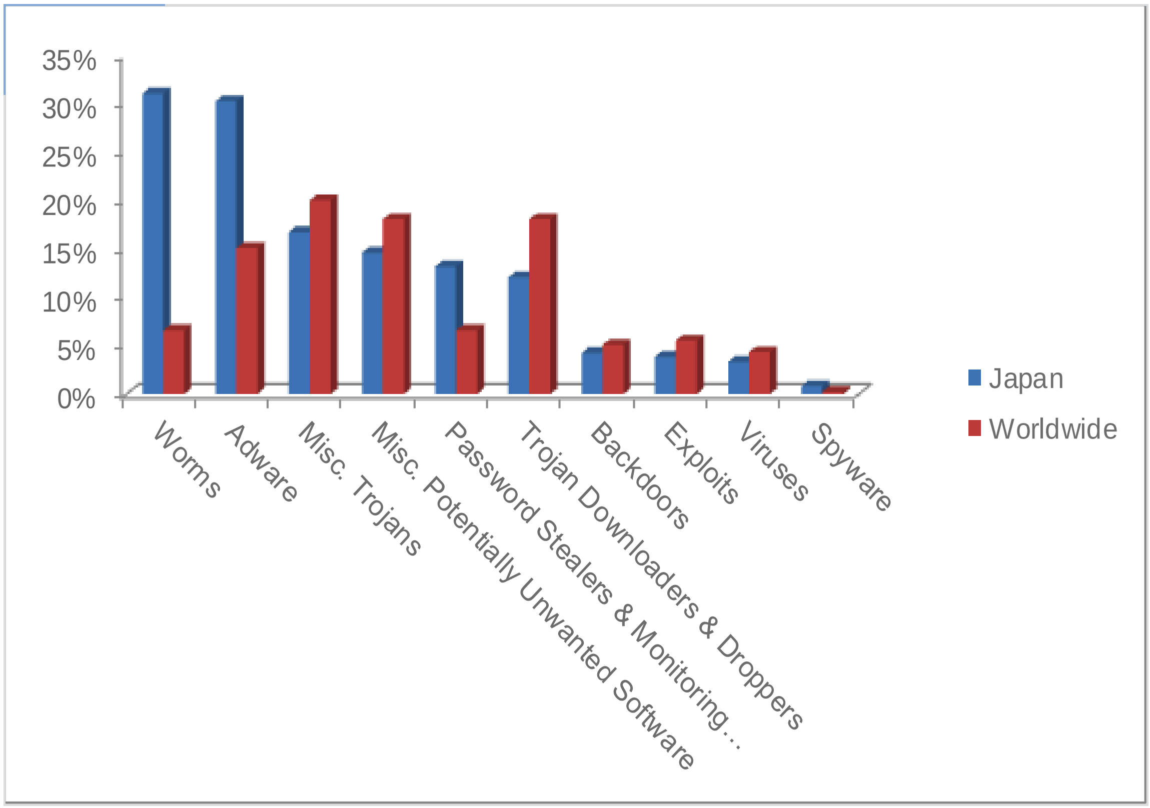
The MSRT detected malware on 3.3 of every 1,000 computers scanned in Japan in 4Q10 (a CCM score of 3.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Japan over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Japan and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Japan in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Japan in 4Q10 was Worms, which affected 31.0 percent of all cleaned computers, down from 36.3 percent in 3Q10.
- The second most common category in Japan in 4Q10 was Adware, which affected 30.2 percent of all cleaned computers, up from 20.8 percent in 3Q10.
- The third most common category in Japan in 4Q10 was Misc. Trojans, which affected 16.7 percent of all cleaned computers, down from 20.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Japan in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 24.5% |
| 2 | Win32/Taterf | 19.0% |
| 3 | Win32/Frethog | 9.9% |
| 4 | Win32/Autorun | 6.8% |
| 5 | Win32/Conficker | 4.3% |
| 6 | ASX/Wimad | 2.8% |
| 7 | Win32/Keygen | 2.6% |
| 8 | Doubled | 1.8% |
| 9 | Win32/Renos | 1.8% |
| 10 | Win32/Bubnix | 1.7% |

- The most common threat family in Japan in 4Q10 was JS/Pornpop, which affected 24.5 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Japan in 4Q10 was Win32/Taterf, which affected 19.0 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The third most common threat family in Japan in 4Q10 was Win32/Frethog, which affected 9.9 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.
- The fourth most common threat family in Japan in 4Q10 was Win32/Autorun, which affected 6.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

# Jordan

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

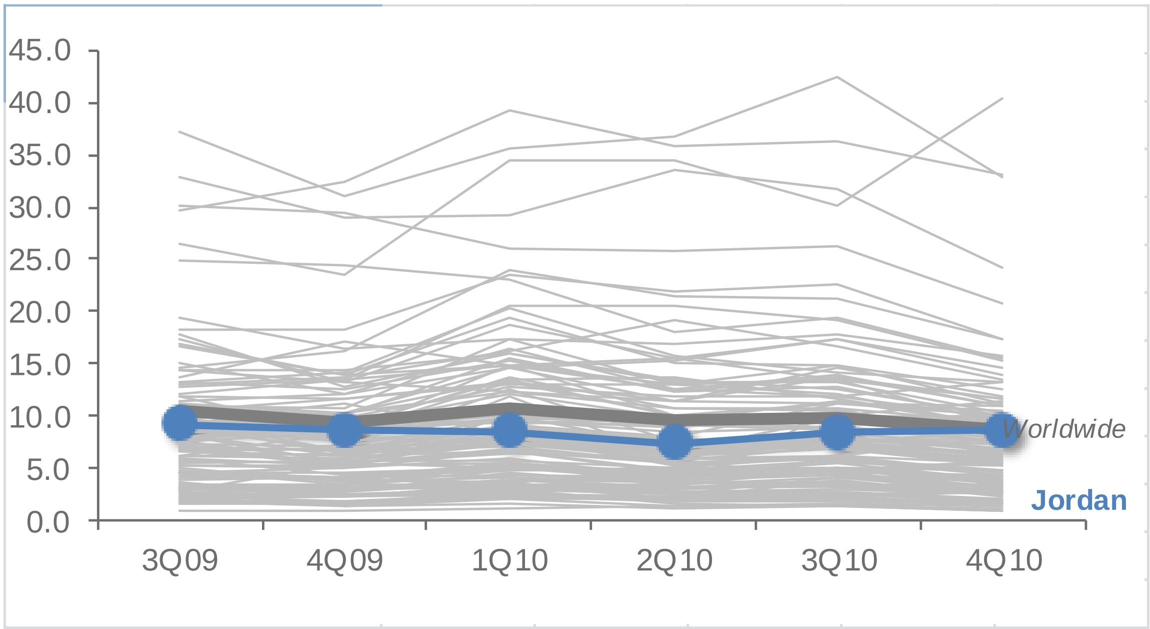
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Jordan in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Jordan and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">8.6</td><td colspan="3">7.4</td><td colspan="3">8.4</td><td colspan="3">8.7</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">2.41</td><td colspan="6">0.76</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">14.75</td><td colspan="6">18.30</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.542%</td><td colspan="4">0.208%</td><td colspan="4">0.246%</td></tr>
</table>

## Infection Trends (CCM)

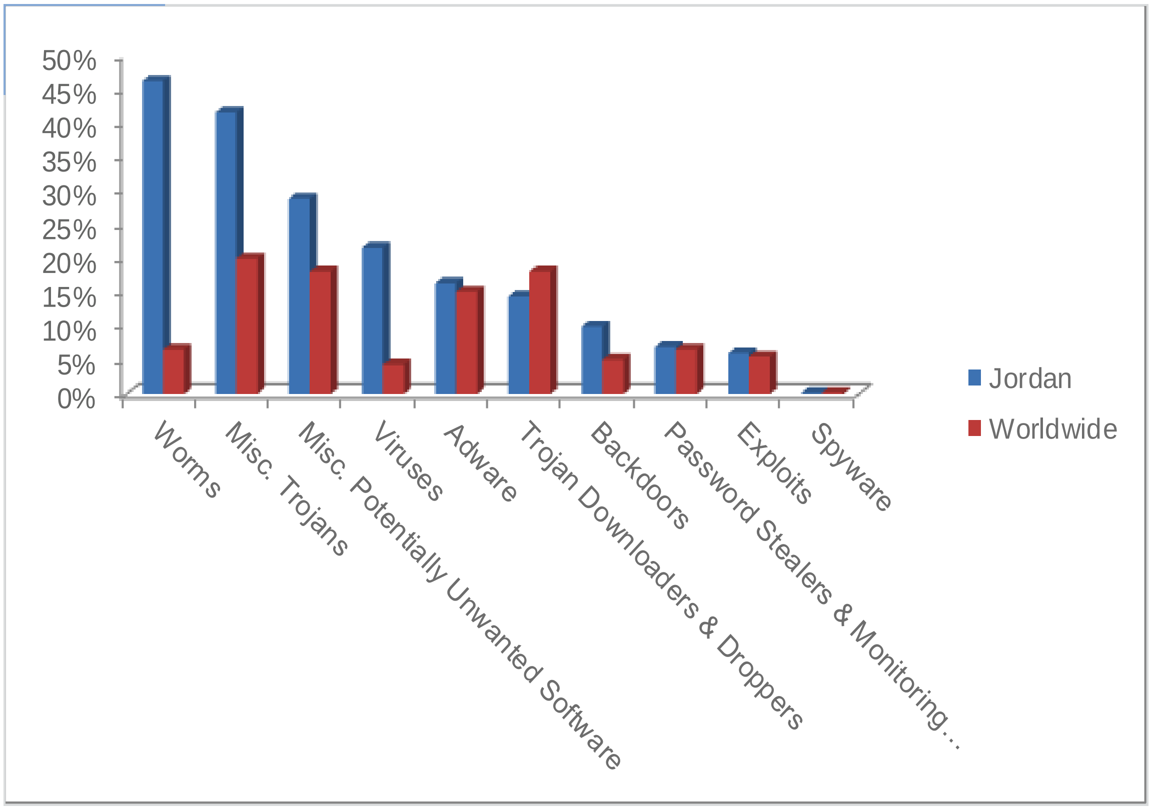
The MSRT detected malware on 8.7 of every 1,000 computers scanned in Jordan in 4Q10 (a CCM score of 8.7, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Jordan over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Jordan and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Jordan in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Jordan in 4Q10 was Worms, which affected 46.2 percent of all cleaned computers, down from 46.8 percent in 3Q10.
- The second most common category in Jordan in 4Q10 was Misc. Trojans, which affected 41.5 percent of all cleaned computers, up from 37.0 percent in 3Q10.
- The third most common category in Jordan in 4Q10 was Misc. Potentially Unwanted Software, which affected 28.8 percent of all cleaned computers, up from 25.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Jordan in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 29.9% |
| 2 | Win32/Sality | 18.6% |
| 3 | Win32/Agent | 13.9% |
| 4 | Win32/Rimecud | 12.6% |
| 5 | Win32/Conficker | 11.5% |
| 6 | JS/Pornpop | 11.1% |
| 7 | Win32/Mabezat | 5.4% |
| 8 | Win32/Taterf | 5.2% |
| 9 | Win32/Vobfus | 5.0% |
| 10 | Malagent | 4.8% |

- The most common threat family in Jordan in 4Q10 was Win32/Autorun, which affected 29.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Jordan in 4Q10 was Win32/Sality, which affected 18.6 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family in Jordan in 4Q10 was Win32/Agent, which affected 13.9 percent of cleaned computers. Win32/Agent is a generic detection for a number of trojans that may perform different malicious functions. The functionality exhibited by this family is highly variable.
- The fourth most common threat family in Jordan in 4Q10 was Win32/Rimecud, which affected 12.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Kazakhstan

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

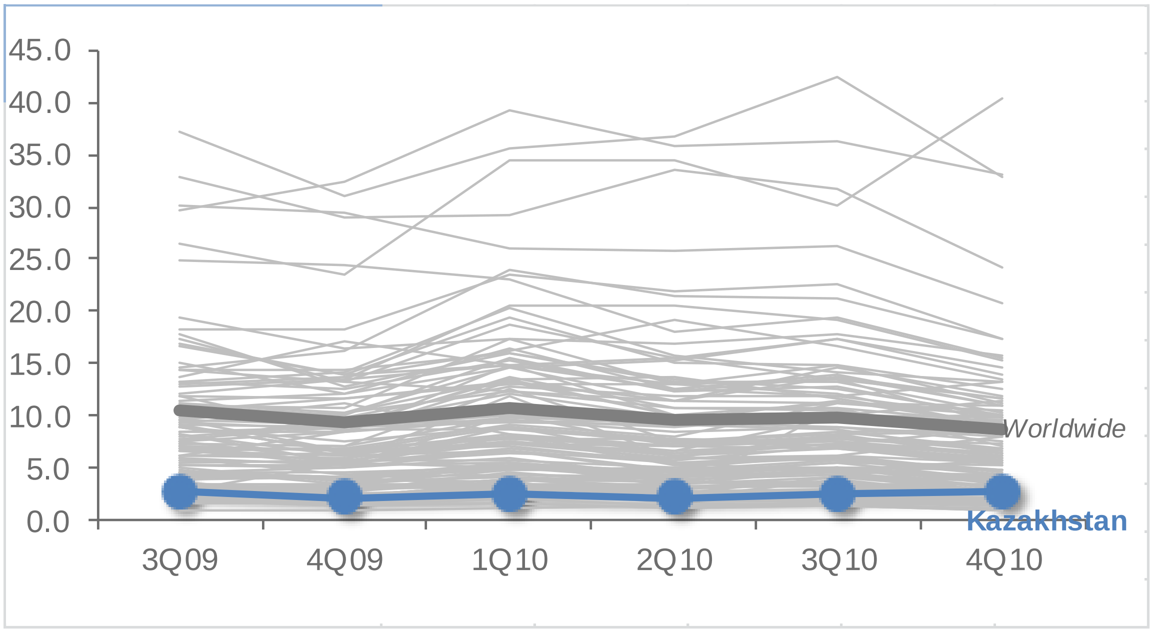
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Kazakhstan in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Kazakhstan and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">2.5</td><td colspan="3">2.2</td><td colspan="3">2.5</td><td colspan="3">2.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">8.73</td><td colspan="6">4.12</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">17.63</td><td colspan="6">69.67</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.206%</td><td colspan="4">0.086%</td><td colspan="4">0.100%</td></tr>
</table>

## Infection Trends (CCM)

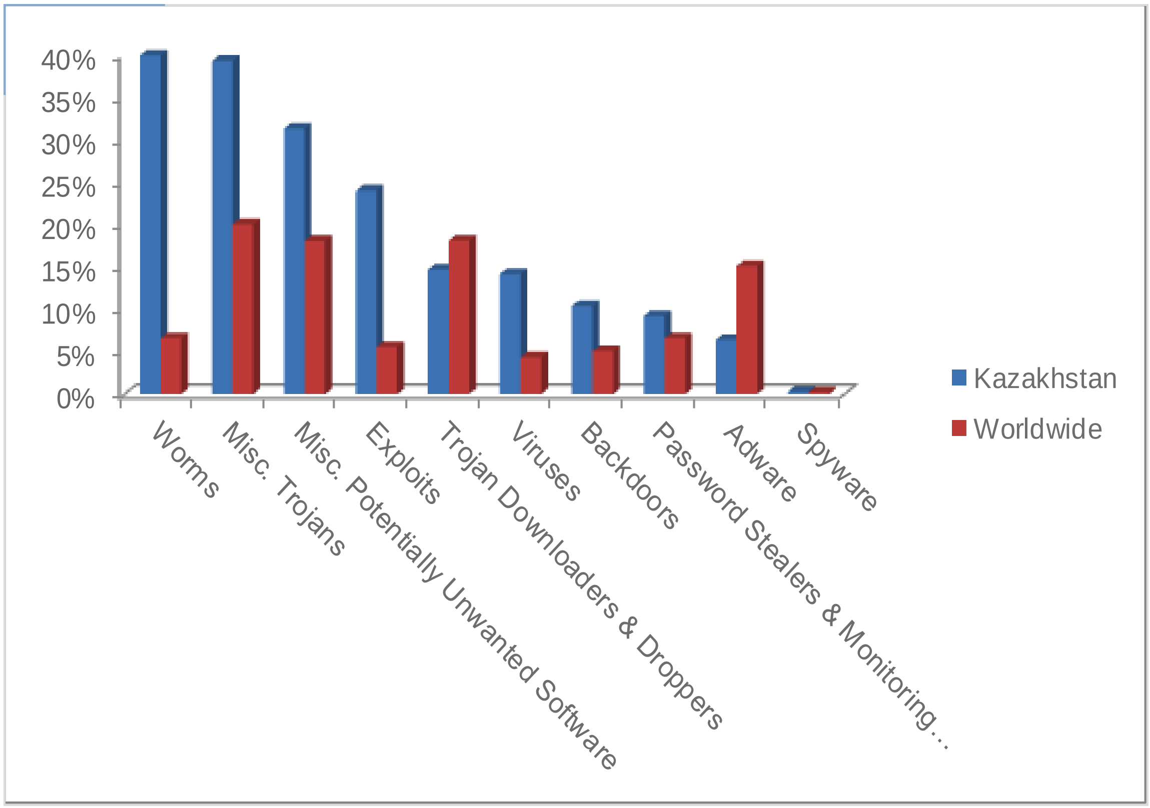
The MSRT detected malware on 2.8 of every 1,000 computers scanned in Kazakhstan in 4Q10 (a CCM score of 2.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Kazakhstan over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Kazakhstan and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Kazakhstan in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Kazakhstan in 4Q10 was Worms, which affected 39.9 percent of all cleaned computers, down from 48.2 percent in 3Q10.
- The second most common category in Kazakhstan in 4Q10 was Misc. Trojans, which affected 39.3 percent of all cleaned computers, up from 36.9 percent in 3Q10.
- The third most common category in Kazakhstan in 4Q10 was Misc. Potentially Unwanted Software, which affected 31.3 percent of all cleaned computers, up from 29.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Kazakhstan in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | CplLnk | 21.4% |
| 2 | Win32/Autorun | 20.0% |
| 3 | Win32/Rimecud | 18.0% |
| 4 | Win32/Vobfus | 12.0% |
| 5 | Meredrop | 8.0% |
| 6 | Win32/Sality | 7.5% |
| 7 | Win32/Stuxnet | 7.4% |
| 8 | Win32/Keygen | 6.9% |
| 9 | Win32/Conficker | 6.4% |
| 10 | Win32/Obfuscator | 5.2% |

- The most common threat family in Kazakhstan in 4Q10 was CplLnk, which affected 21.4 percent of cleaned computers. CplLnk is

- The second most common threat family in Kazakhstan in 4Q10 was Win32/Autorun, which affected 20.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

- The third most common threat family in Kazakhstan in 4Q10 was Win32/Rimecud, which affected 18.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

- The fourth most common threat family in Kazakhstan in 4Q10 was Win32/Vobfus, which affected 12.0 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

# Kenya

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

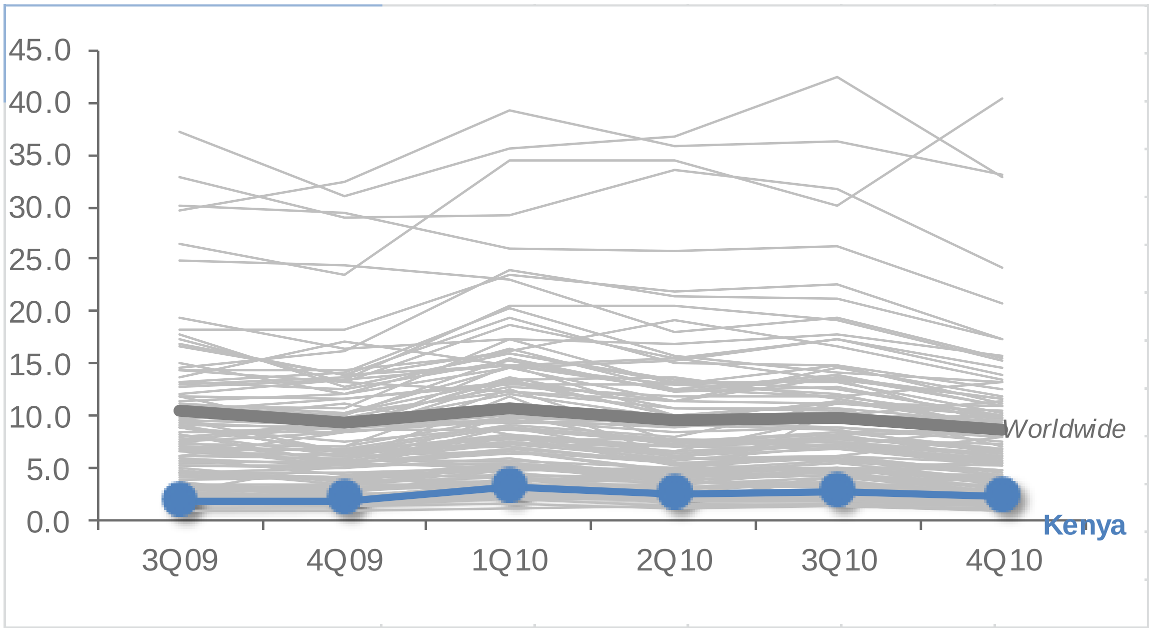
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Kenya in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Kenya and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.4 | 2.7 | 2.9 | 2.5 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 1.32 | | 0.29 | |
| Malware hosting sites per 1000 hosts | 0.26 | | 0.07 | |
| Percentage of sites hosting drive-by downloads | 0.220% | 0.245% | 0.226% | |

## Infection Trends (CCM)

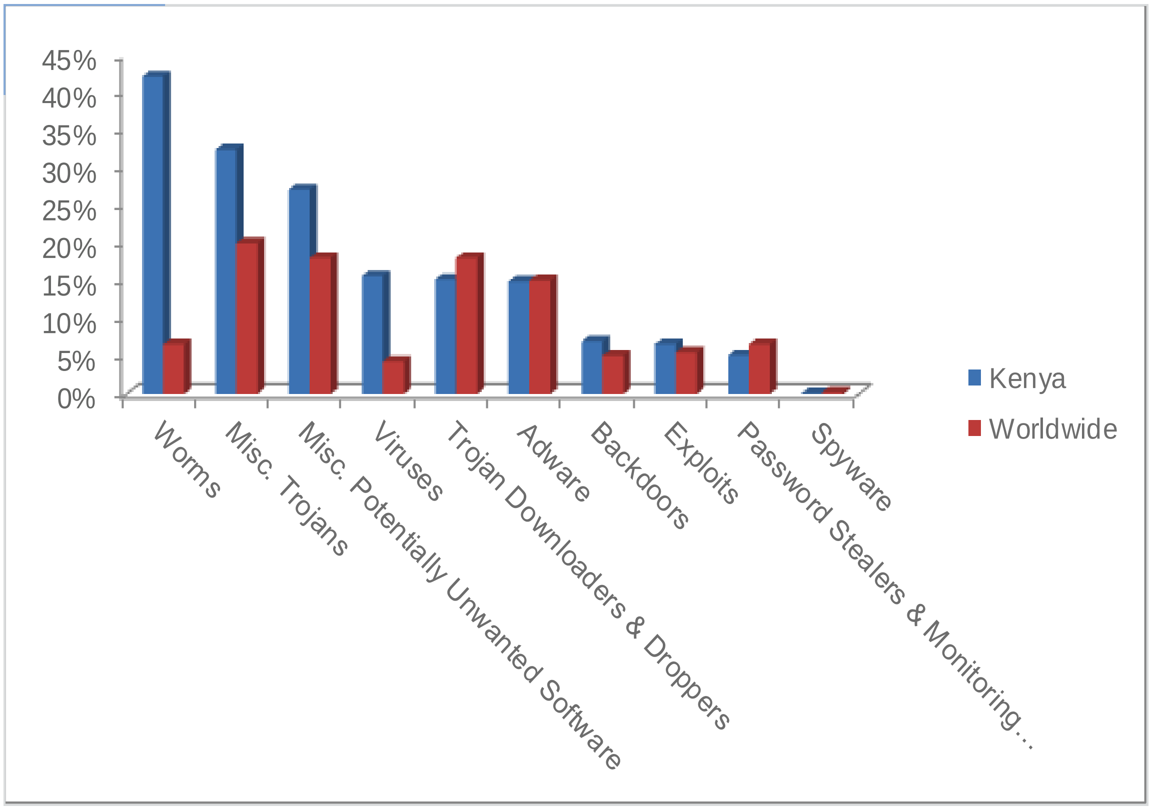
The MSRT detected malware on 2.5 of every 1,000 computers scanned in Kenya in 4Q10 (a CCM score of 2.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Kenya over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Kenya and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Kenya in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Kenya in 4Q10 was Worms, which affected 42.1 percent of all cleaned computers, down from 50.5 percent in 3Q10.
- The second most common category in Kenya in 4Q10 was Misc. Trojans, which affected 32.4 percent of all cleaned computers, up from 25.8 percent in 3Q10.
- The third most common category in Kenya in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.1 percent of all cleaned computers, up from 23.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Kenya in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 28.3% |
| 2 | Win32/Autorun | 19.8% |
| 3 | Win32/Sality | 12.2% |
| 4 | Win32/Vobfus | 9.9% |
| 5 | JS/Pornpop | 6.0% |
| 6 | Win32/Renos | 5.1% |
| 7 | Win32/ClickPotato | 4.7% |
| 8 | Win32/Conficker | 4.5% |
| 9 | Win32/Zwangi | 4.4% |
| 10 | Win32/Taterf | 4.3% |

- The most common threat family in Kenya in 4Q10 was Win32/Rimecud, which affected 28.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Kenya in 4Q10 was Win32/Autorun, which affected 19.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Kenya in 4Q10 was Win32/Sality, which affected 12.2 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Kenya in 4Q10 was Win32/Vobfus, which affected 9.9 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

# Korea

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

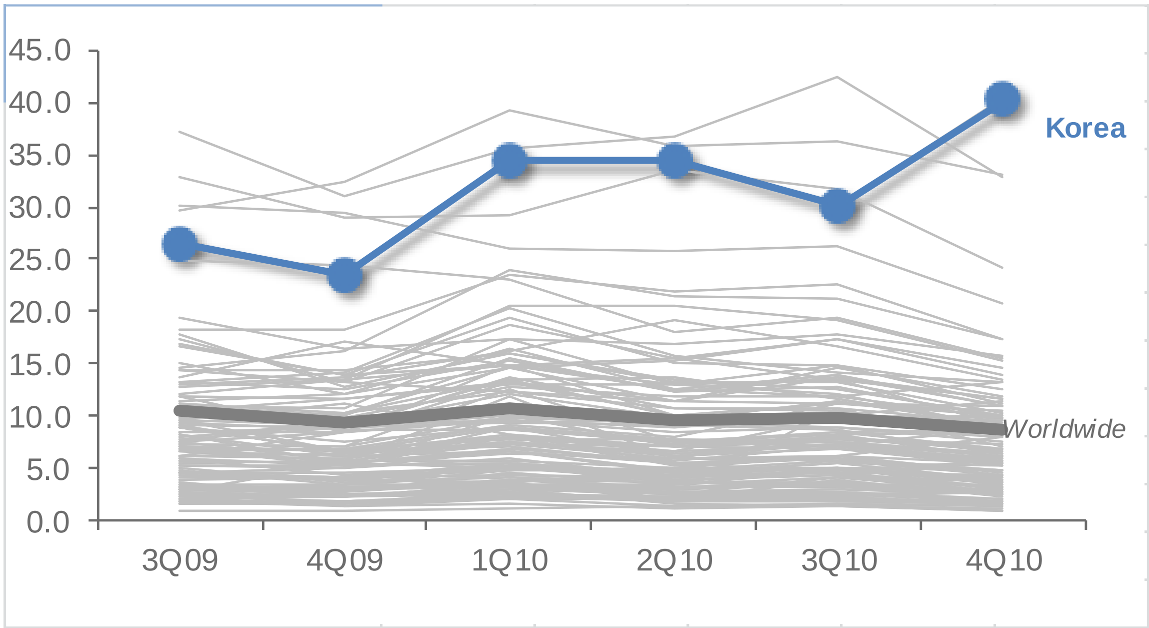
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Korea in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Korea and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 34.4 | 34.4 | 30.1 | 40.3 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 36.31 | | 14.77 | |
| Malware hosting sites per 1000 hosts | 154.47 | | 408.35 | |
| Percentage of sites hosting drive-by downloads | 0.361% | 0.271% | 0.377% | |

## Infection Trends (CCM)

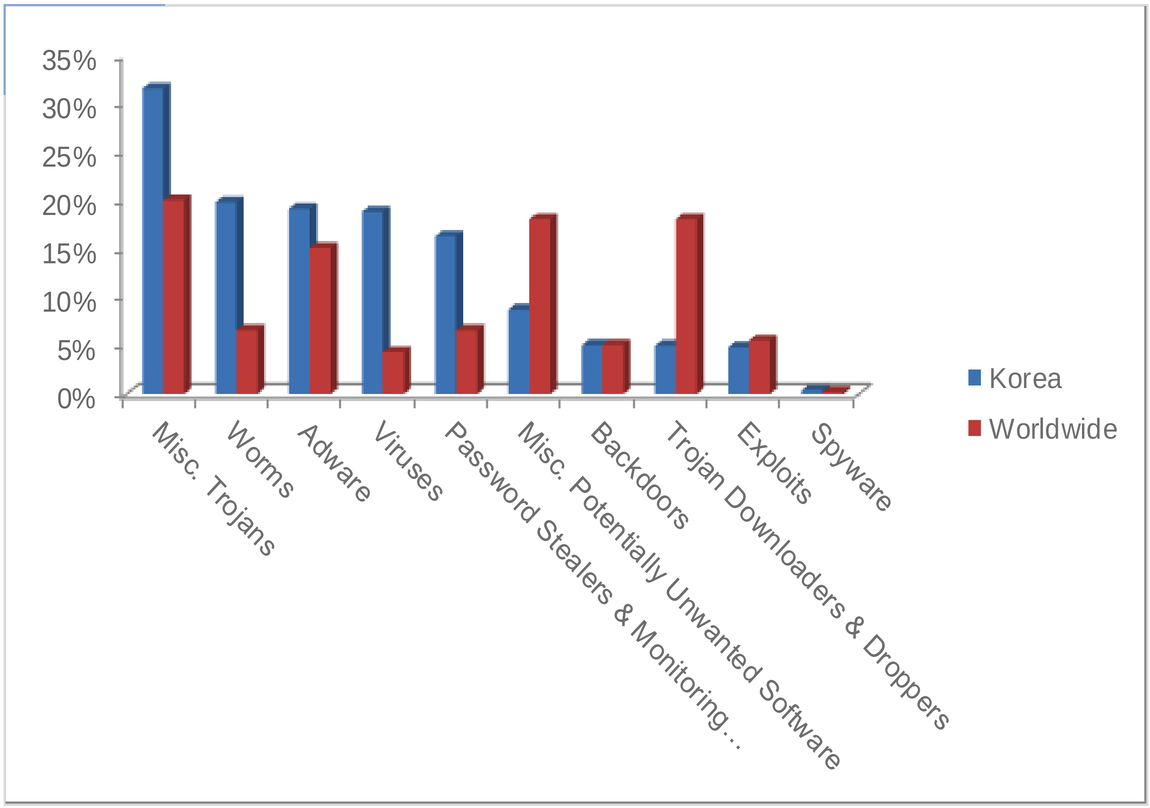
The MSRT detected malware on 40.3 of every 1,000 computers scanned in Korea in 4Q10 (a CCM score of 40.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Korea over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Korea and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Korea in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Korea in 4Q10 was Misc. Trojans, which affected 31.5 percent of all cleaned computers, down from 38.7 percent in 3Q10.
- The second most common category in Korea in 4Q10 was Worms, which affected 19.8 percent of all cleaned computers, up from 17.1 percent in 3Q10.
- The third most common category in Korea in 4Q10 was Adware, which affected 19.1 percent of all cleaned computers, up from 15.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Korea in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Onescan | 21.0% |
| 2 | Win32/Parite | 14.4% |
| 3 | Win32/Nbar | 12.9% |
| 4 | Win32/Rimecud | 11.1% |
| 5 | Win32/Frethog | 9.8% |
| 6 | Win32/Taterf | 6.8% |
| 7 | Win32/Magania | 6.4% |
| 8 | SideTab | 3.7% |
| 9 | Win32/Virut | 2.8% |
| 10 | Mult | 2.8% |

- The most common threat family in Korea in 4Q10 was Win32/Onescan, which affected 21.0 percent of cleaned computers. Win32/Onescan is a Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, My Vaccine, and others.
- The second most common threat family in Korea in 4Q10 was Win32/Parite, which affected 14.4 percent of cleaned computers. Win32/Parite is a family of viruses that infect .exe and .scr executable files on the local file system and on writeable network shares.
- The third most common threat family in Korea in 4Q10 was Win32/Nbar, which affected 12.9 percent of cleaned computers. Win32/Nbar is a program that may display advertisements and redirect user searches to a certain website. It may also download malicious or unwanted content into the system without user consent.
- The fourth most common threat family in Korea in 4Q10 was Win32/Rimecud, which affected 11.1 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Kuwait

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

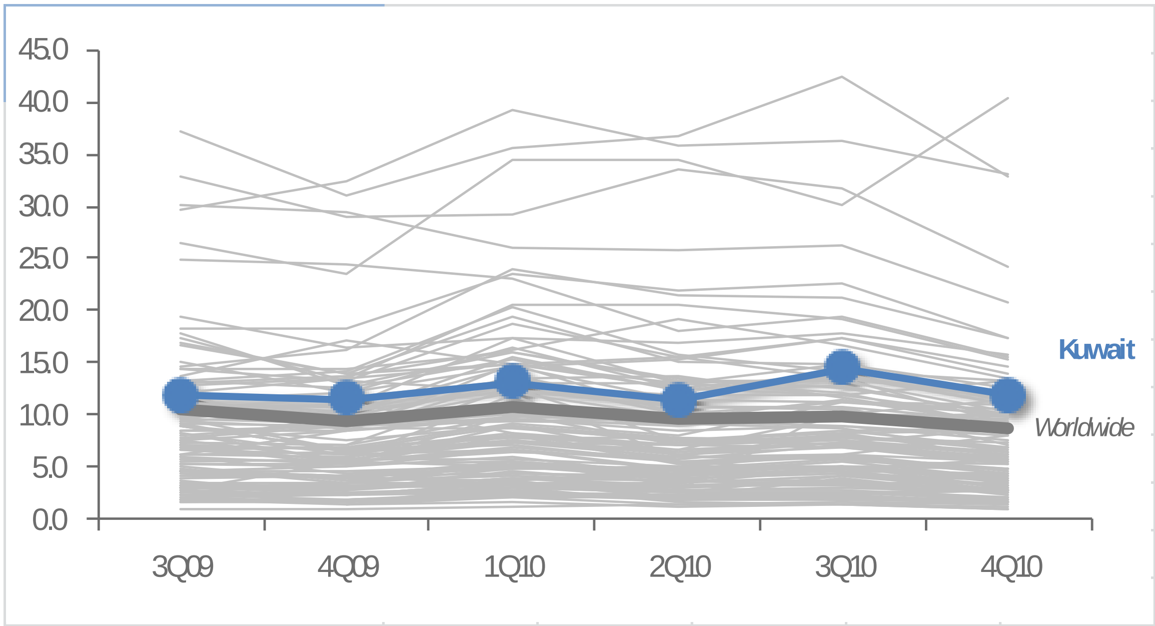
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Kuwait in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Kuwait and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 13.2 | 11.5 | 14.6 | 12.0 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 13.38 | | 17.03 | |
| Malware hosting sites per 1000 hosts | 20.67 | | 10.34 | |
| Percentage of sites hosting drive-by downloads | 0.341% | 0.353% | | |

## Infection Trends (CCM)

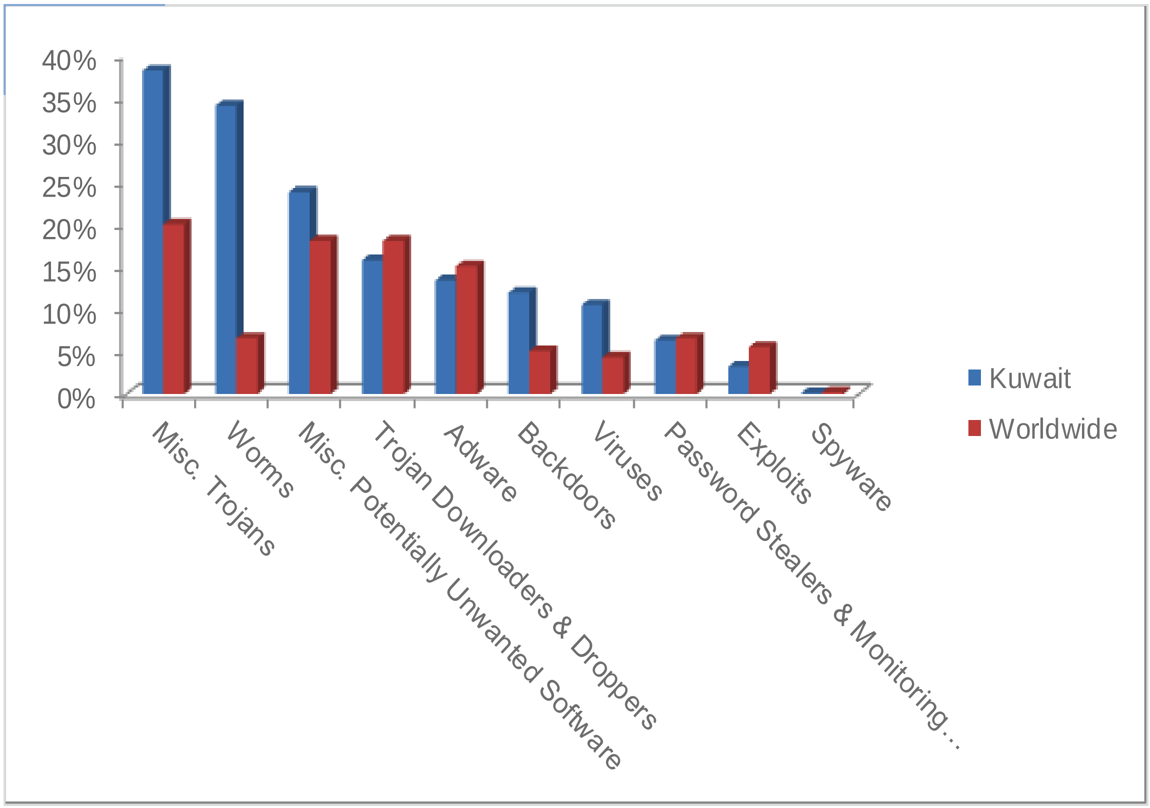
The MSRT detected malware on 12.0 of every 1,000 computers scanned in Kuwait in 4Q10 (a CCM score of 12.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Kuwait over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Kuwait and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Kuwait in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Kuwait in 4Q10 was Misc. Trojans, which affected 38.1 percent of all cleaned computers, down from 39.6 percent in 3Q10.
- The second most common category in Kuwait in 4Q10 was Worms, which affected 34.0 percent of all cleaned computers, up from 33.1 percent in 3Q10.
- The third most common category in Kuwait in 4Q10 was Misc. Potentially Unwanted Software, which affected 23.8 percent of all cleaned computers, up from 19.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Kuwait in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 19.0% |
| 2 | Win32/Autorun | 15.3% |
| 3 | Win32/Sality | 9.4% |
| 4 | Win32/Agent | 8.8% |
| 5 | Win32/Renos | 5.8% |
| 6 | Win32/Vobfus | 4.7% |
| 7 | Win32/Zwangi | 4.7% |
| 8 | Win32/IRCbot | 4.7% |
| 9 | Giframe | 4.4% |
| 10 | Win32/ClickPotato | 4.4% |

- The most common threat family in Kuwait in 4Q10 was Win32/Rimecud, which affected 19.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Kuwait in 4Q10 was Win32/Autorun, which affected 15.3 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Kuwait in 4Q10 was Win32/Sality, which affected 9.4 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Kuwait in 4Q10 was Win32/Agent, which affected 8.8 percent of cleaned computers. Win32/Agent is a generic detection for a number of trojans that may perform different malicious functions. The functionality exhibited by this family is highly variable.

# Latvia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

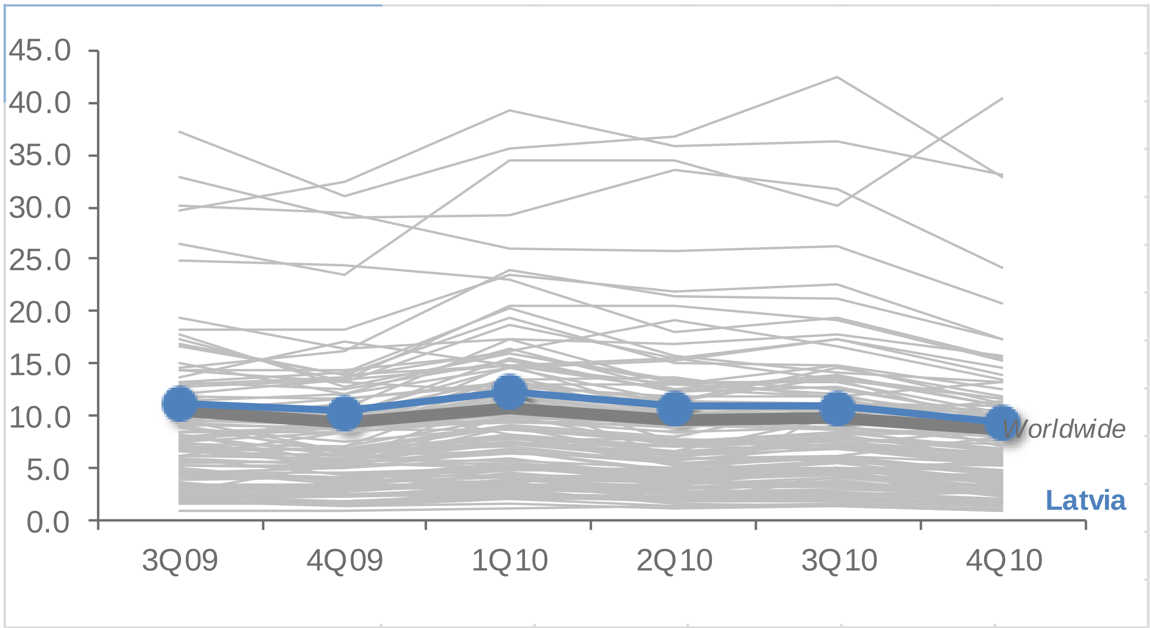
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Latvia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Latvia and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 12.4 | 10.8 | 10.8 | 9.4 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.44 | | 1.01 | |
| Malware hosting sites per 1000 hosts | 31.24 | | 27.22 | |
| Percentage of sites hosting drive-by downloads | 0.208% | 0.047% | 0.057% | |

## Infection Trends (CCM)

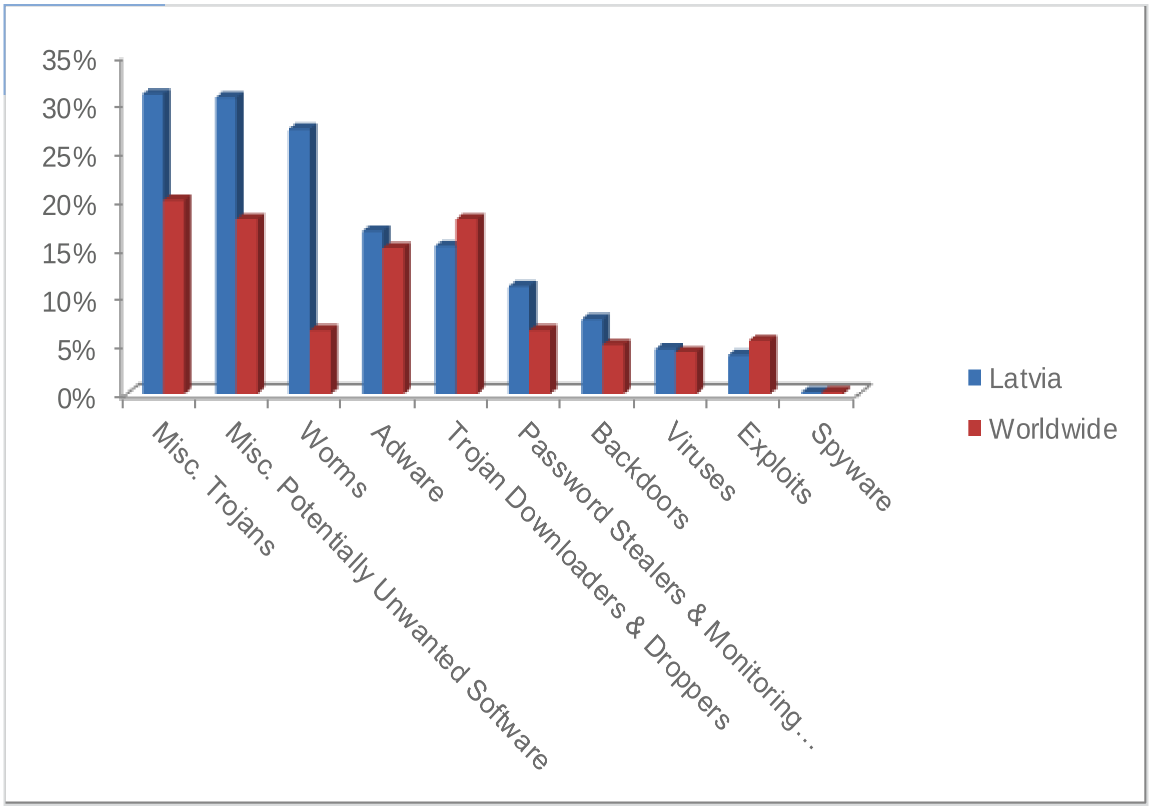
The MSRT detected malware on 9.4 of every 1,000 computers scanned in Latvia in 4Q10 (a CCM score of 9.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Latvia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Latvia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Latvia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Latvia in 4Q10 was Misc. Trojans, which affected 30.9 percent of all cleaned computers, down from 36.4 percent in 3Q10.
- The second most common category in Latvia in 4Q10 was Misc. Potentially Unwanted Software, which affected 30.6 percent of all cleaned computers, up from 27.9 percent in 3Q10.
- The third most common category in Latvia in 4Q10 was Worms, which affected 27.4 percent of all cleaned computers, down from 27.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Latvia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 13.9% |
| 2 | Win32/Rimecud | 12.5% |
| 3 | JS/Pornpop | 9.0% |
| 4 | Win32/Taterf | 8.1% |
| 5 | Win32/Keygen | 6.7% |
| 6 | Win32/Conficker | 6.6% |
| 7 | Win32/Renos | 6.0% |
| 8 | Win32/Frethog | 5.4% |
| 9 | Win32/IRCbot | 4.5% |
| 10 | Win32/ClickPotato | 3.9% |

- The most common threat family in Latvia in 4Q10 was Win32/Autorun, which affected 13.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Latvia in 4Q10 was Win32/Rimecud, which affected 12.5 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Latvia in 4Q10 was JS/Pornpop, which affected 9.0 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Latvia in 4Q10 was Win32/Taterf, which affected 8.1 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Lebanon

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

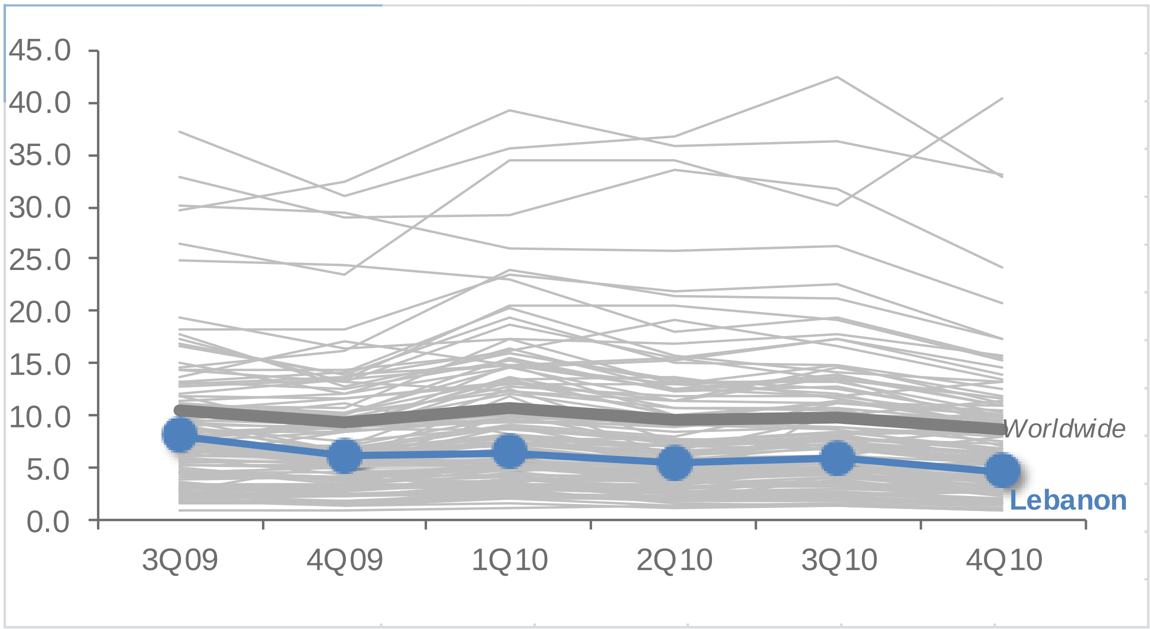
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Lebanon in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Lebanon and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 6.5 | 5.6 | 6.0 | 4.8 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 1.31 | | 0.19 | |
| Malware hosting sites per 1000 hosts | 0.05 | | 0.05 | |
| Percentage of sites hosting drive-by downloads | 0.324% | 0.118% | | |

## Infection Trends (CCM)

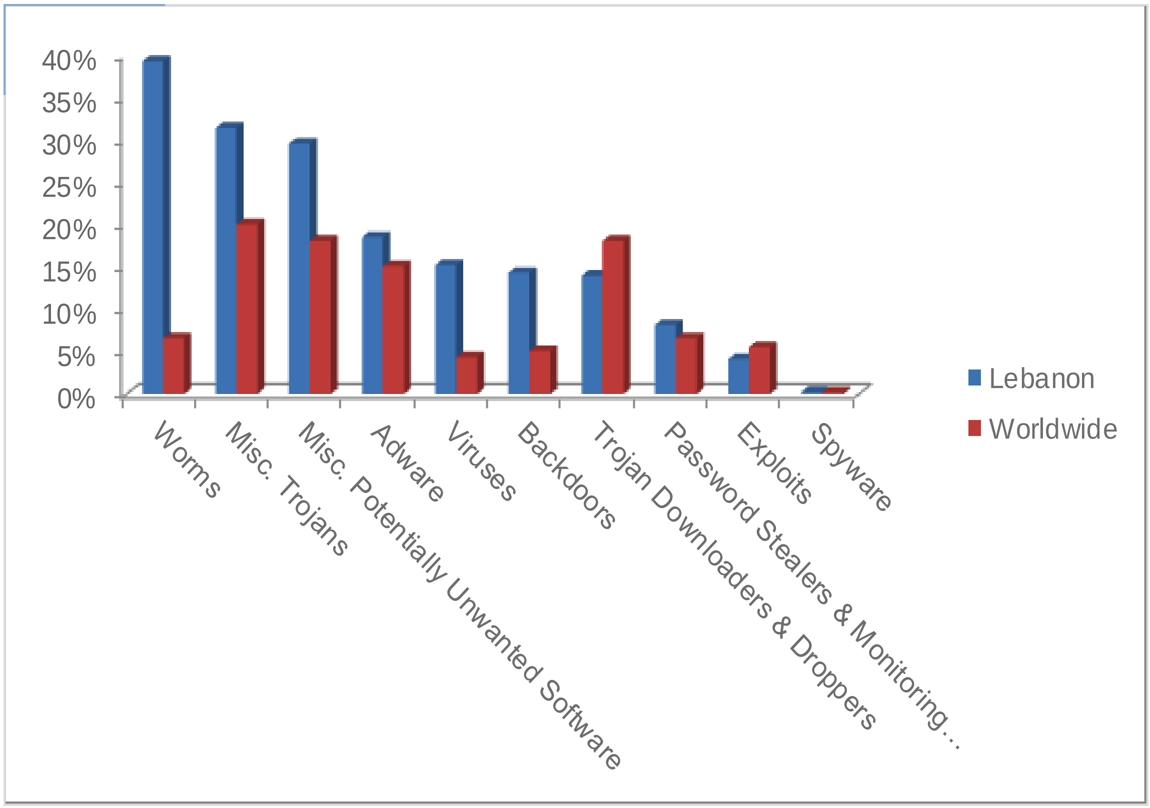
The MSRT detected malware on 4.8 of every 1,000 computers scanned in Lebanon in 4Q10 (a CCM score of 4.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Lebanon over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Lebanon and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Lebanon in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Lebanon in 4Q10 was Worms, which affected 39.2 percent of all cleaned computers, down from 42.0 percent in 3Q10.
- The second most common category in Lebanon in 4Q10 was Misc. Trojans, which affected 31.4 percent of all cleaned computers, up from 26.9 percent in 3Q10.
- The third most common category in Lebanon in 4Q10 was Misc. Potentially Unwanted Software, which affected 29.5 percent of all cleaned computers, up from 25.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Lebanon in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 19.7% |
| 2 | Win32/Rimecud | 16.0% |
| 3 | Win32/Sality | 13.1% |
| 4 | JS/Pornpop | 10.5% |
| 5 | Win32/Conficker | 8.0% |
| 6 | Win32/Taterf | 6.2% |
| 7 | Win32/FlyAgent | 6.2% |
| 8 | Win32/Keygen | 4.9% |
| 9 | Win32/Hamweq | 4.8% |
| 10 | Win32/Renos | 4.5% |

- The most common threat family in Lebanon in 4Q10 was Win32/Autorun, which affected 19.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Lebanon in 4Q10 was Win32/Rimecud, which affected 16.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Lebanon in 4Q10 was Win32/Sality, which affected 13.1 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Lebanon in 4Q10 was JS/Pornpop, which affected 10.5 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Libya

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

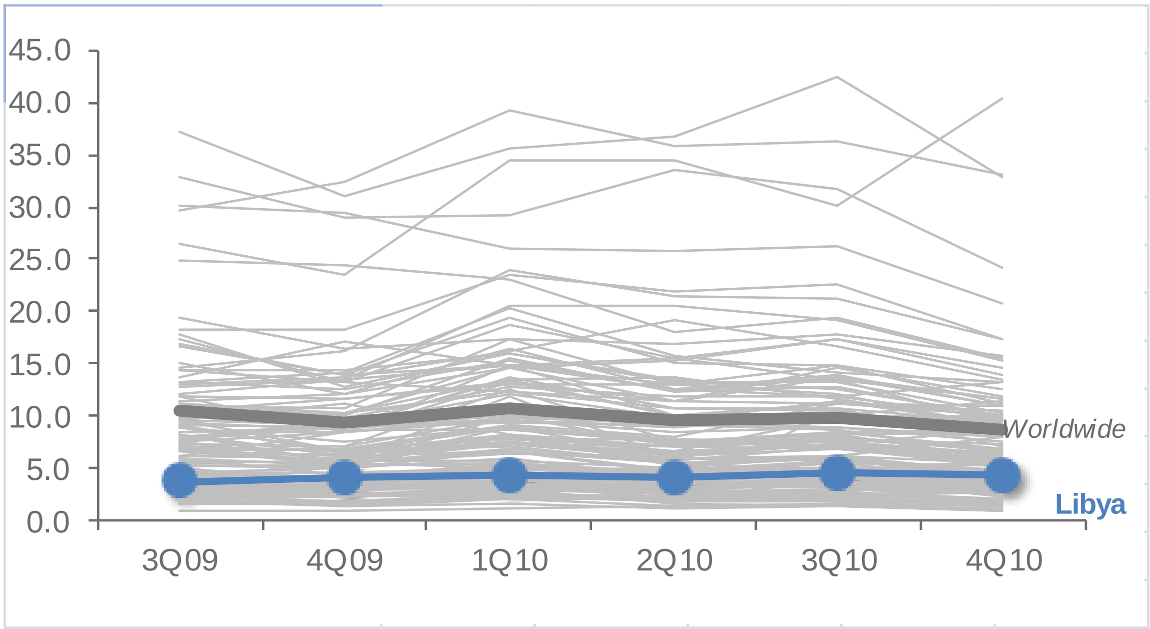
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Libya in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Libya and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 4.4 | 4.1 | 4.7 | 4.4 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | | | 32.26 | |
| Malware hosting sites per 1000 hosts | | | 64.52 | |
| Percentage of sites hosting drive-by downloads | 0.560% | 0.253% | 0.402% | |

## Infection Trends (CCM)

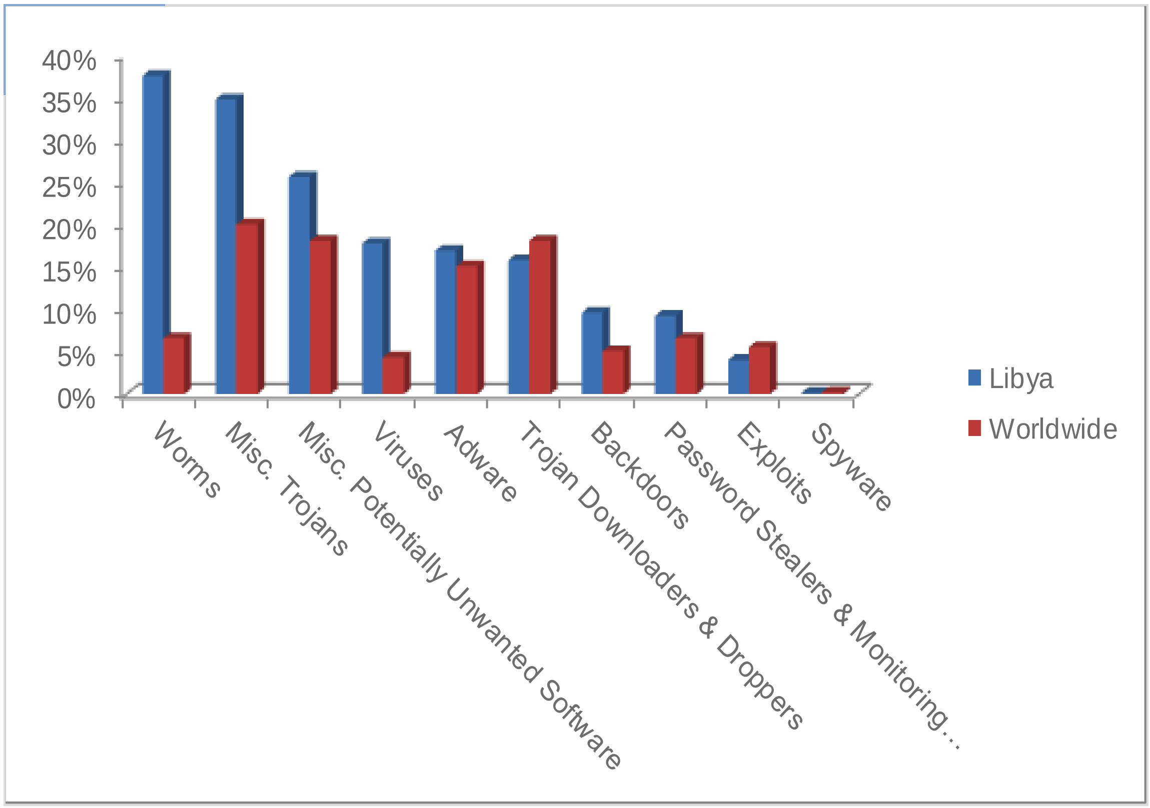
The MSRT detected malware on 4.4 of every 1,000 computers scanned in Libya in 4Q10 (a CCM score of 4.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Libya over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Libya and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Libya in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Libya in 4Q10 was Worms, which affected 37.5 percent of all cleaned computers, down from 38.1 percent in 3Q10.
- The second most common category in Libya in 4Q10 was Misc. Trojans, which affected 34.8 percent of all cleaned computers, up from 27.1 percent in 3Q10.
- The third most common category in Libya in 4Q10 was Misc. Potentially Unwanted Software, which affected 25.6 percent of all cleaned computers, up from 20.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Libya in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Sality | 17.0% |
| 2 | Win32/Autorun | 15.4% |
| 3 | Win32/Rimecud | 12.9% |
| 4 | Win32/Taterf | 9.4% |
| 5 | JS/Pornpop | 9.2% |
| 6 | Win32/Agent | 8.8% |
| 7 | Win32/Vobfus | 6.6% |
| 8 | Win32/Conficker | 5.6% |
| 9 | Win32/Renos | 5.3% |
| 10 | Win32/Frethog | 5.1% |

- The most common threat family in Libya in 4Q10 was Win32/Sality, which affected 17.0 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family in Libya in 4Q10 was Win32/Autorun, which affected 15.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Libya in 4Q10 was Win32/Rimecud, which affected 12.9 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Libya in 4Q10 was Win32/Taterf, which affected 9.4 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Lithuania

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

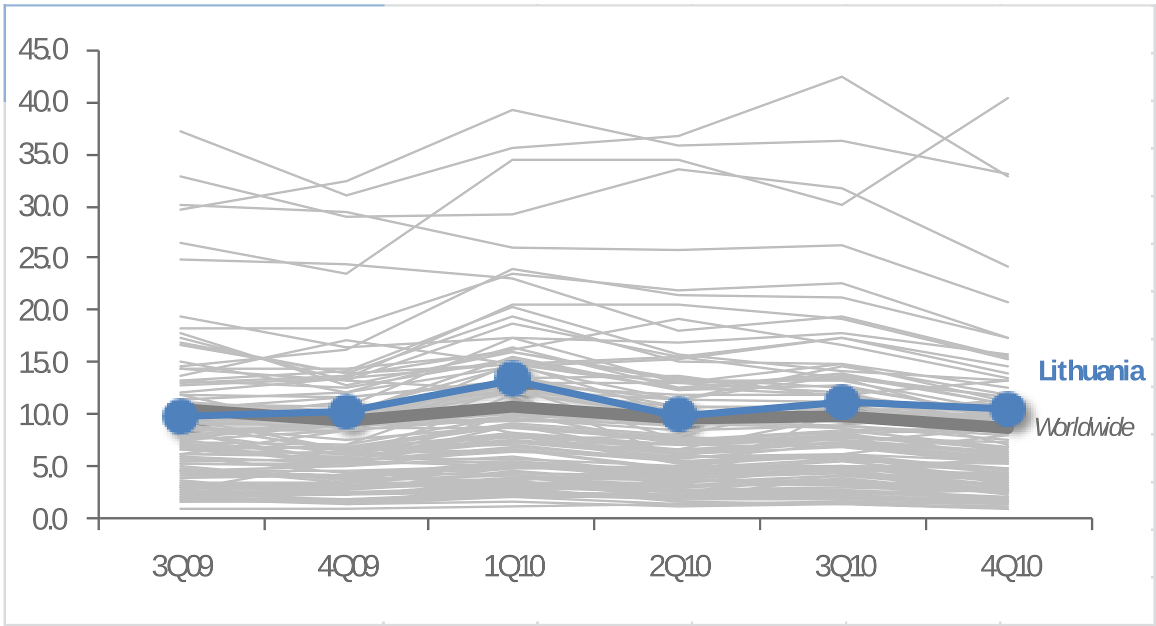
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Lithuania in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Lithuania and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 13.4 | 10.1 | 11.2 | 10.5 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.21 | | 0.28 | |
| Malware hosting sites per 1000 hosts | 1.54 | | 1.18 | |
| Percentage of sites hosting drive-by downloads | 0.205% | 0.095% | 0.074% | |

## Infection Trends (CCM)

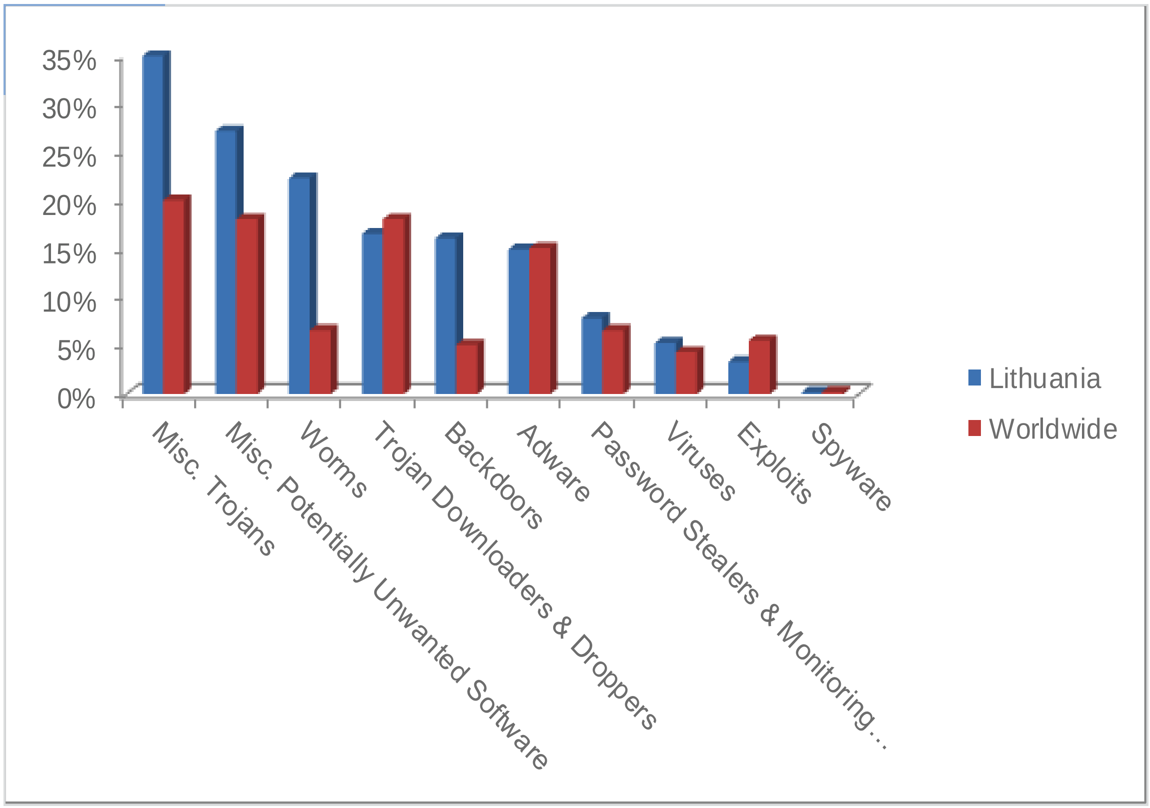
The MSRT detected malware on 10.5 of every 1,000 computers scanned in Lithuania in 4Q10 (a CCM score of 10.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Lithuania over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Lithuania and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Lithuania in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Lithuania in 4Q10 was Misc. Trojans, which affected 34.9 percent of all cleaned computers, up from 34.3 percent in 3Q10.
- The second most common category in Lithuania in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.1 percent of all cleaned computers, down from 29.3 percent in 3Q10.
- The third most common category in Lithuania in 4Q10 was Worms, which affected 22.3 percent of all cleaned computers, down from 26.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Lithuania in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/IRCbot | 12.7% |
| 2 | Win32/Rimecud | 12.1% |
| 3 | Win32/Autorun | 10.5% |
| 4 | JS/Pornpop | 9.1% |
| 5 | Win32/Renos | 6.8% |
| 6 | Win32/Keygen | 5.7% |
| 7 | Win32/Conficker | 4.9% |
| 8 | Giframe | 3.8% |
| 9 | Win32/Obfuscator | 3.8% |
| 10 | Killav | 3.7% |

- The most common threat family in Lithuania in 4Q10 was Win32/IRCbot, which affected 12.7 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The second most common threat family in Lithuania in 4Q10 was Win32/Rimecud, which affected 12.1 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Lithuania in 4Q10 was Win32/Autorun, which affected 10.5 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common threat family in Lithuania in 4Q10 was JS/Pornpop, which affected 9.1 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Luxembourg

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

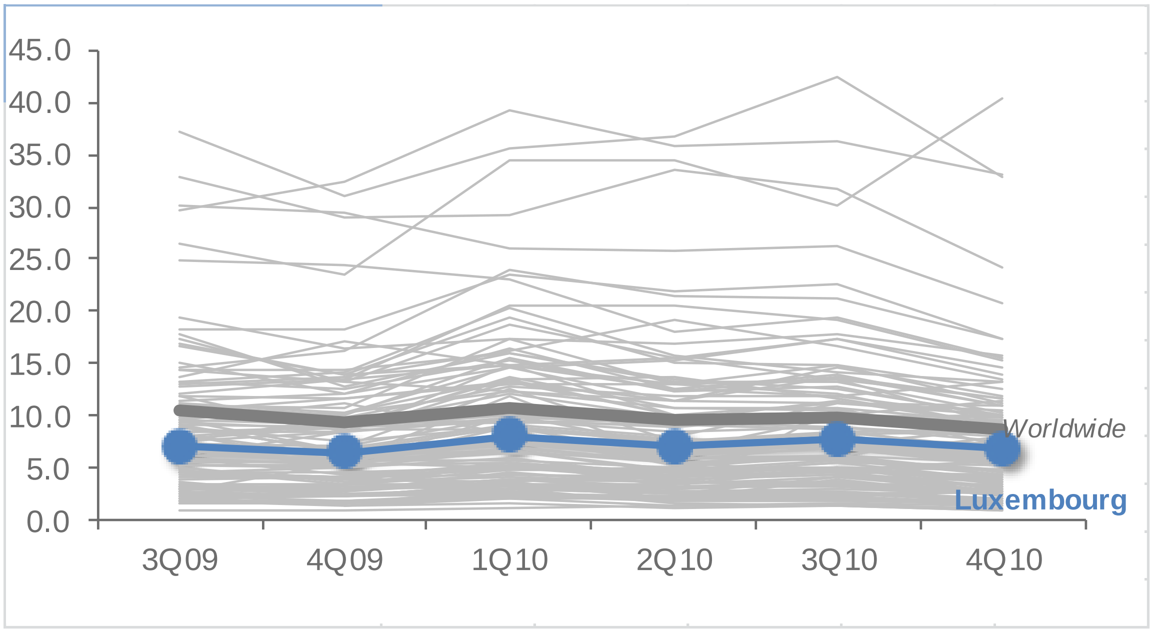
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Luxembourg in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Luxembourg and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">8.2</td><td colspan="3">7.1</td><td colspan="3">7.9</td><td colspan="3">6.9</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.60</td><td colspan="6">0.37</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">16.39</td><td colspan="6">6.30</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.081%</td><td colspan="4">0.019%</td><td colspan="4">0.014%</td></tr>
</table>

## Infection Trends (CCM)

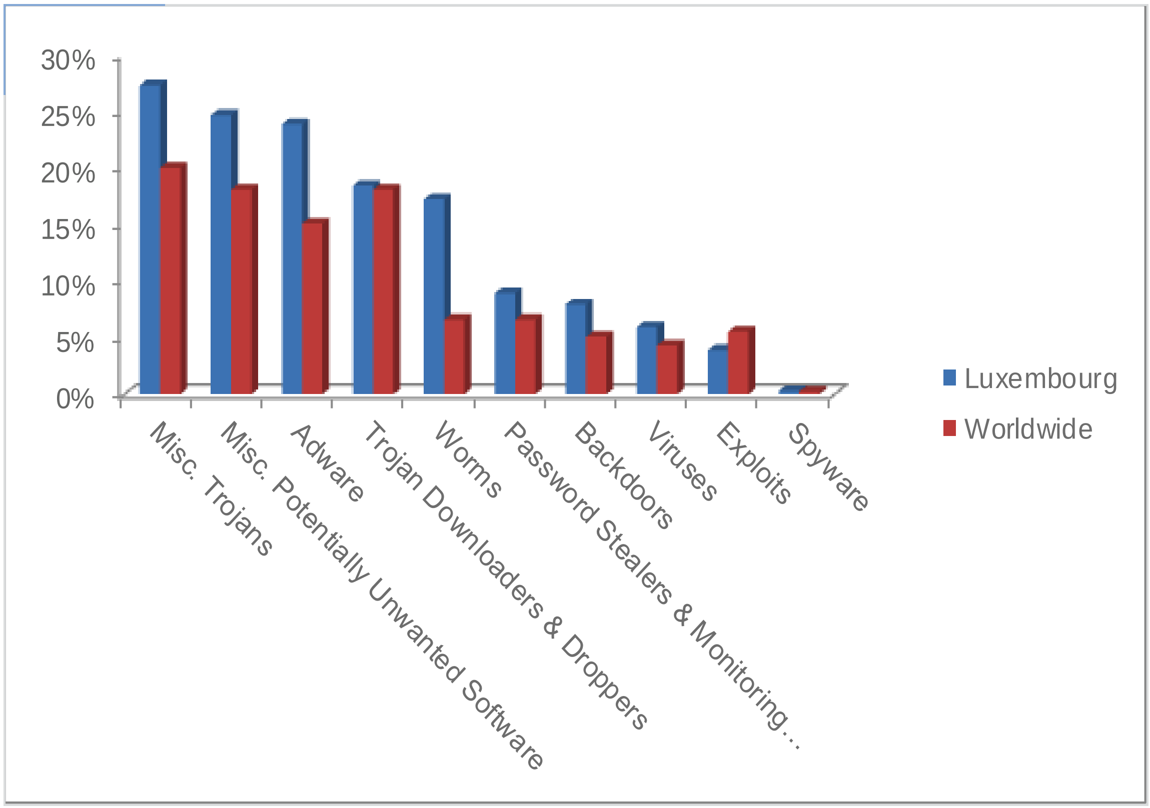
The MSRT detected malware on 6.9 of every 1,000 computers scanned in Luxembourg in 4Q10 (a CCM score of 6.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Luxembourg over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Luxembourg and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Luxembourg in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Luxembourg in 4Q10 was Misc. Trojans, which affected 27.3 percent of all cleaned computers, down from 30.4 percent in 3Q10.
- The second most common category in Luxembourg in 4Q10 was Misc. Potentially Unwanted Software, which affected 24.7 percent of all cleaned computers, up from 22.7 percent in 3Q10.
- The third most common category in Luxembourg in 4Q10 was Adware, which affected 23.8 percent of all cleaned computers, up from 20.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Luxembourg in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 9.9% |
| 2 | Win32/Zwangi | 7.2% |
| 3 | Win32/Renos | 6.1% |
| 4 | Win32/ClickPotato | 6.0% |
| 5 | Win32/Autorun | 5.3% |
| 6 | Win32/IRCbot | 5.0% |
| 7 | Win32/Hotbar | 4.8% |
| 8 | Win32/Sality | 4.4% |
| 9 | ASX/Wimad | 4.3% |
| 10 | Win32/Rimecud | 3.9% |

- The most common threat family in Luxembourg in 4Q10 was JS/Pornpop, which affected 9.9 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Luxembourg in 4Q10 was Win32/Zwangi, which affected 7.2 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The third most common threat family in Luxembourg in 4Q10 was Win32/Renos, which affected 6.1 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.
- The fourth most common threat family in Luxembourg in 4Q10 was Win32/ClickPotato, which affected 6.0 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user’s browsing habits.

# Macao S.A.R.

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

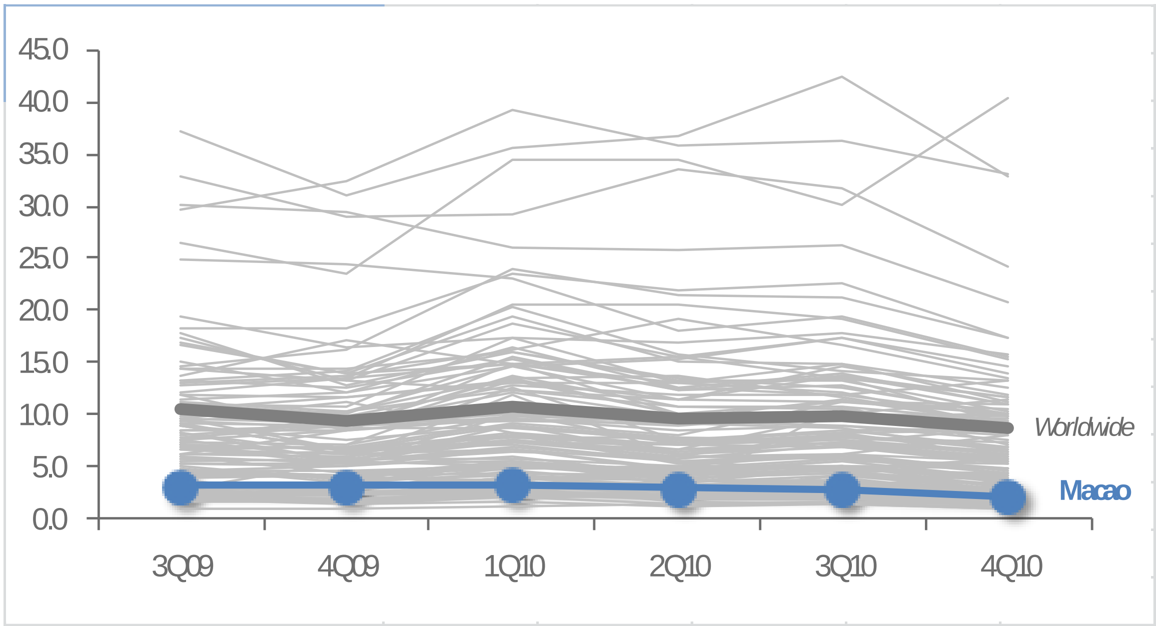
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Macao S.A.R. in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Macao S.A.R. and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">3.2</td><td colspan="3">2.8</td><td colspan="3">2.7</td><td colspan="3">2.1</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">3.80</td><td colspan="6">19.01</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">273.76</td><td colspan="6">72.24</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.265%</td><td colspan="4">0.238%</td><td colspan="4"></td></tr>
</table>

## Infection Trends (CCM)

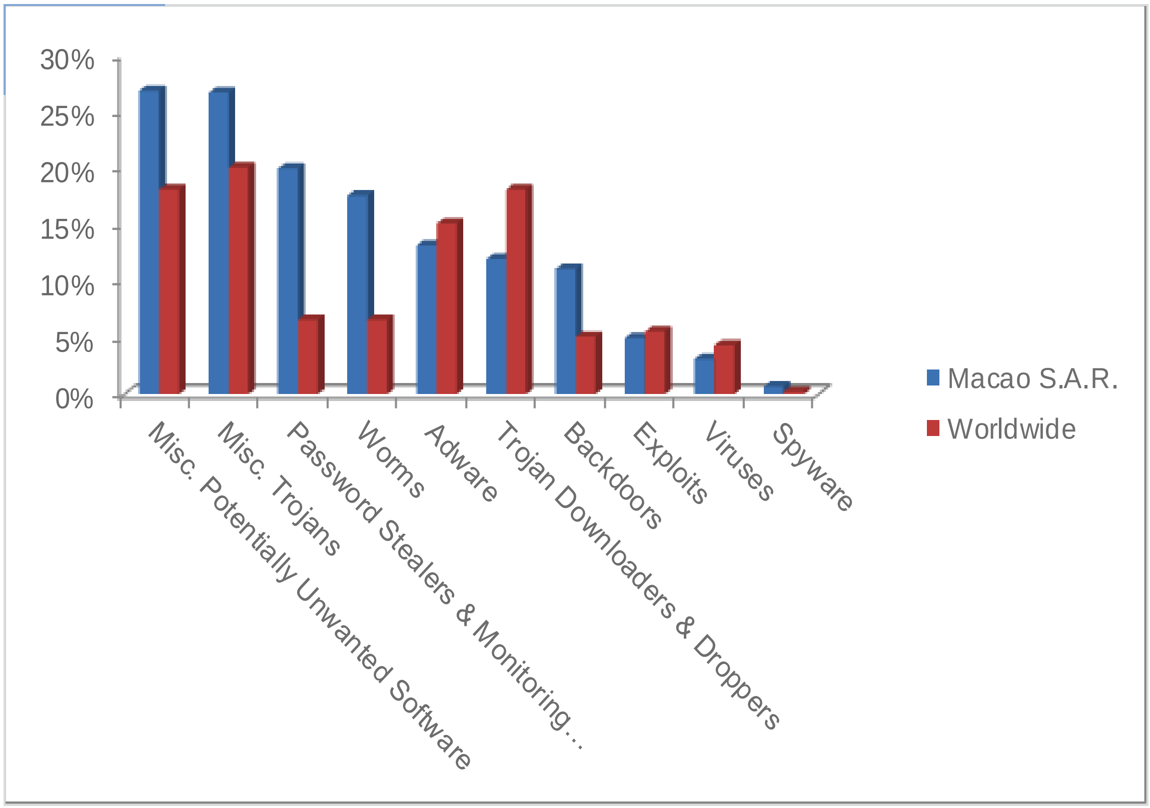
The MSRT detected malware on 2.1 of every 1,000 computers scanned in Macao S.A.R. in 4Q10 (a CCM score of 2.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Macao S.A.R. over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Macao S.A.R. and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Macao S.A.R. in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Macao S.A.R. in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.8 percent of all cleaned computers, down from 31.2 percent in 3Q10.
- The second most common category in Macao S.A.R. in 4Q10 was Misc. Trojans, which affected 26.6 percent of all cleaned computers, up from 23.7 percent in 3Q10.
- The third most common category in Macao S.A.R. in 4Q10 was Password Stealers & Monitoring Tools, which affected 19.9 percent of all cleaned computers, down from 22.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Macao S.A.R. in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Frethog | 15.5% |
| 2 | Win32/Autorun | 7.0% |
| 3 | Win32/Taterf | 6.9% |
| 4 | Win32/Vundo | 5.9% |
| 5 | JS/Pornpop | 5.4% |
| 6 | Win32/IRCbot | 5.0% |
| 7 | Win32/BaiduSobar | 4.5% |
| 8 | Win32/Conficker | 3.9% |
| 9 | Win32/Zwangi | 3.8% |
| 10 | Win32/Keygen | 3.4% |

- The most common threat family in Macao S.A.R. in 4Q10 was Win32/Frethog, which affected 15.5 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.
- The second most common threat family in Macao S.A.R. in 4Q10 was Win32/Autorun, which affected 7.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Macao S.A.R. in 4Q10 was Win32/Taterf, which affected 6.9 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Macao S.A.R. in 4Q10 was Win32/Vundo, which affected 5.9 percent of cleaned computers. Win32/Vundo is a multiple-component family of programs that deliver pop-up advertisements and may download and execute arbitrary files. Vundo is often installed as a browser helper object (BHO) without a user's consent.

# Malaysia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

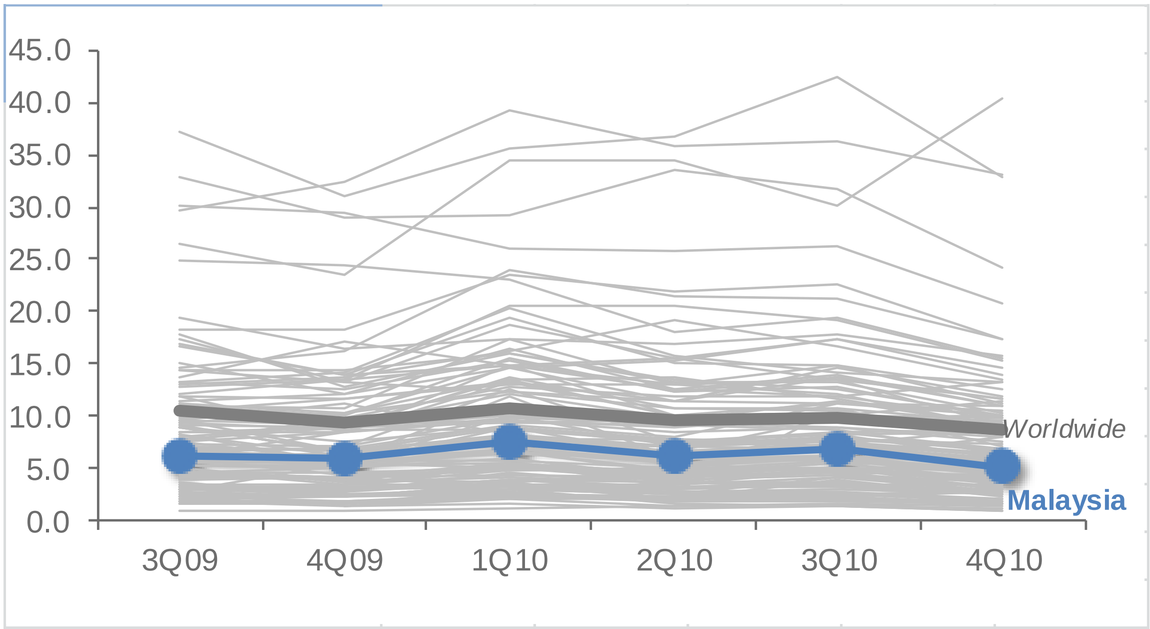
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Malaysia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Malaysia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">7.6</td><td colspan="3">6.2</td><td colspan="3">6.8</td><td colspan="3">5.1</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">2.95</td><td colspan="6">9.33</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">2.57</td><td colspan="6">1.63</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.514%</td><td colspan="4">0.117%</td><td colspan="4">0.110%</td></tr>
</table>

## Infection Trends (CCM)

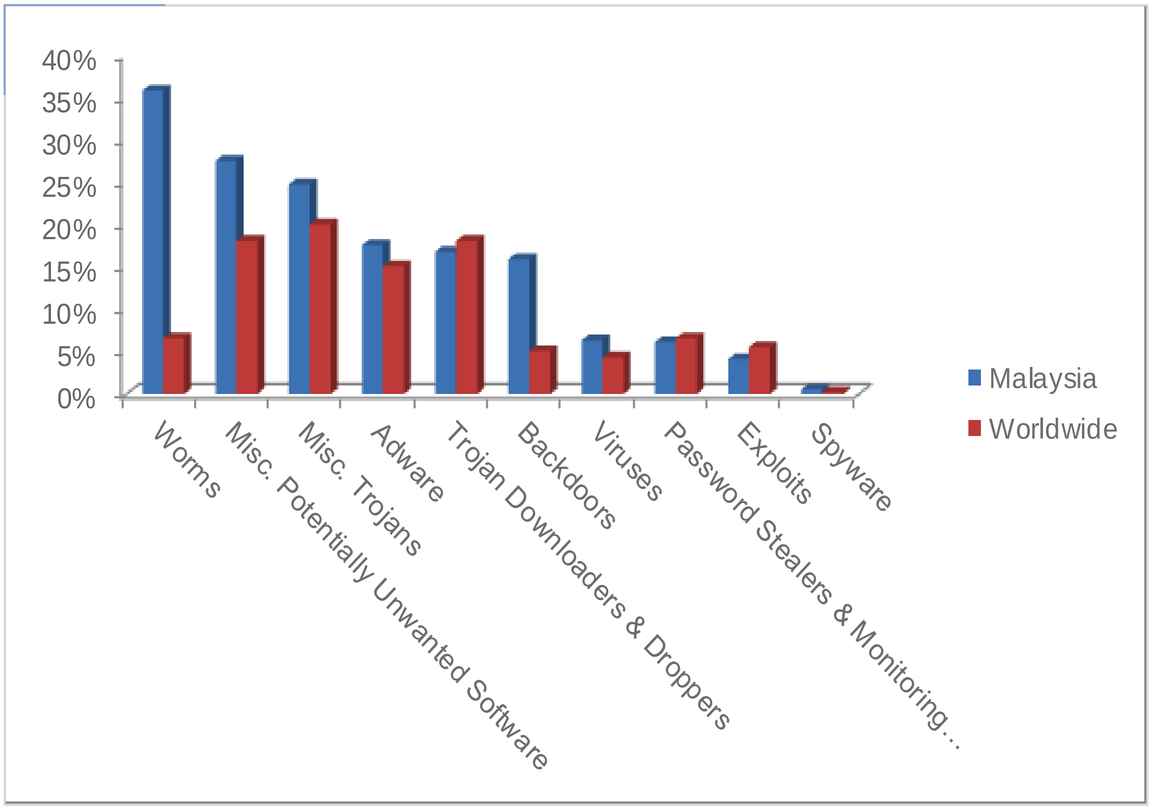
The MSRT detected malware on 5.1 of every 1,000 computers scanned in Malaysia in 4Q10 (a CCM score of 5.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Malaysia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Malaysia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Malaysia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Malaysia in 4Q10 was Worms, which affected 35.8 percent of all cleaned computers, down from 41.4 percent in 3Q10.
- The second most common category in Malaysia in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.5 percent of all cleaned computers, up from 25.4 percent in 3Q10.
- The third most common category in Malaysia in 4Q10 was Misc. Trojans, which affected 24.7 percent of all cleaned computers, up from 23.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Malaysia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 18.9% |
| 2 | Win32/Rimecud | 10.3% |
| 3 | Win32/Conficker | 9.0% |
| 4 | JS/Pornpop | 8.4% |
| 5 | Win32/Renos | 7.1% |
| 6 | Win32/Hupigon | 6.9% |
| 7 | Win32/IRCbot | 5.7% |
| 8 | Win32/Taterf | 5.2% |
| 9 | Win32/Vobfus | 4.8% |
| 10 | Win32/Sality | 4.5% |

- The most common threat family in Malaysia in 4Q10 was Win32/Autorun, which affected 18.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Malaysia in 4Q10 was Win32/Rimecud, which affected 10.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Malaysia in 4Q10 was Win32/Conficker, which affected 9.0 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The fourth most common threat family in Malaysia in 4Q10 was JS/Pornpop, which affected 8.4 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Malta

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

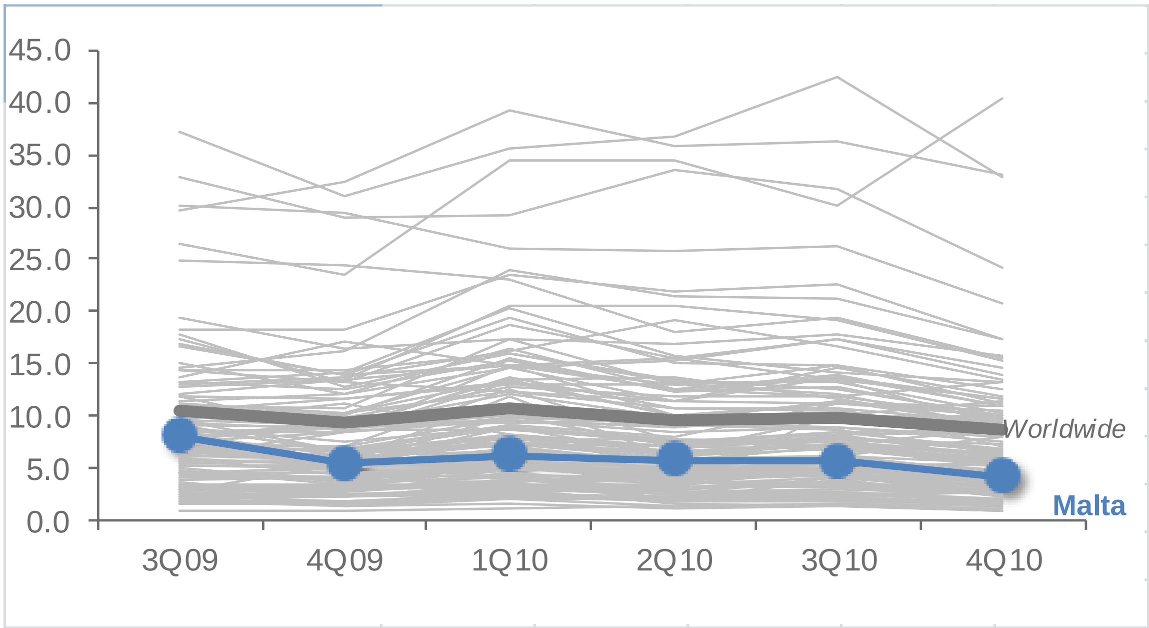
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Malta in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Malta and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">6.3</td><td colspan="3">5.9</td><td colspan="3">5.8</td><td colspan="3">4.3</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.89</td><td colspan="6">0.30</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">27.40</td><td colspan="6">0.42</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.332%</td><td colspan="4">0.199%</td><td colspan="4">0.075%</td></tr>
</table>

## Infection Trends (CCM)

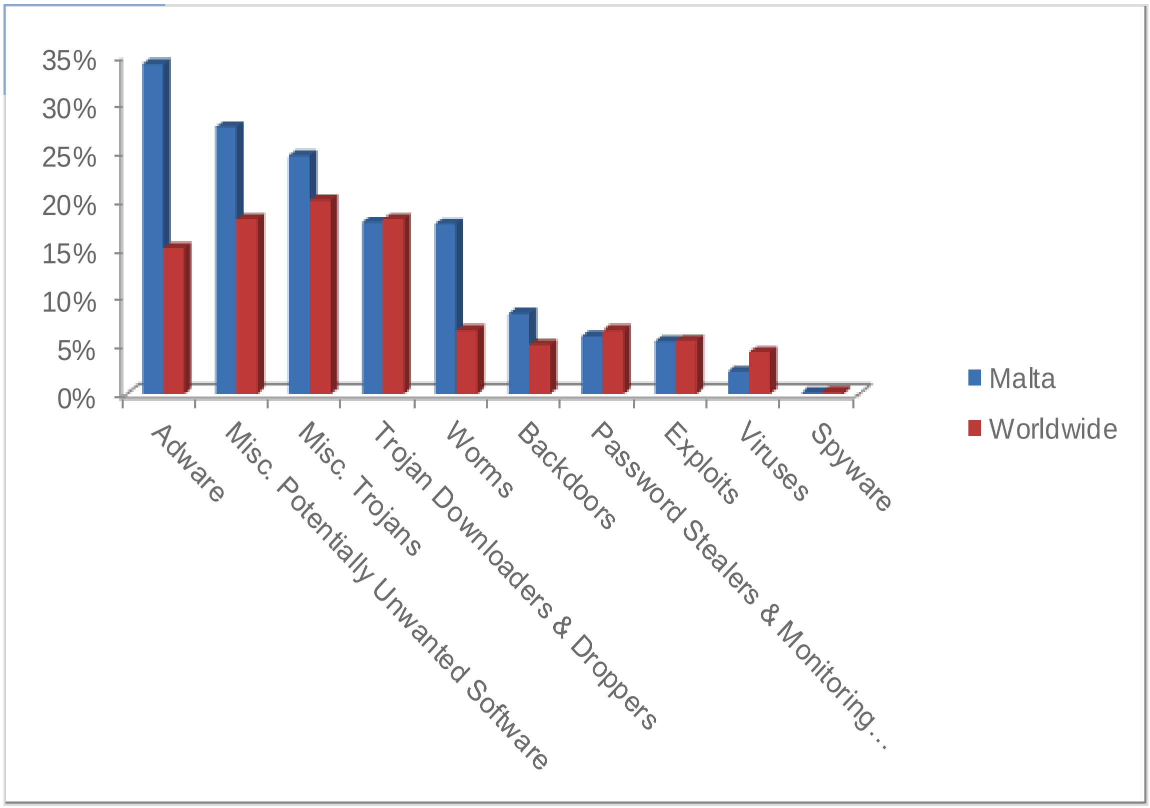
The MSRT detected malware on 4.3 of every 1,000 computers scanned in Malta in 4Q10 (a CCM score of 4.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Malta over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Malta and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Malta in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Malta in 4Q10 was Adware, which affected 34.1 percent of all cleaned computers, up from 32.6 percent in 3Q10.
- The second most common category in Malta in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.5 percent of all cleaned computers, up from 25.3 percent in 3Q10.
- The third most common category in Malta in 4Q10 was Misc. Trojans, which affected 24.6 percent of all cleaned computers, up from 24.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Malta in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/ClickPotato | 14.3% |
| 2 | Win32/Zwangi | 13.2% |
| 3 | JS/Pornpop | 9.6% |
| 4 | Win32/Hotbar | 7.7% |
| 5 | Win32/Rimecud | 6.6% |
| 6 | Win32/Renos | 6.4% |
| 7 | Win32/Autorun | 5.3% |
| 8 | Win32/IRCbot | 4.4% |
| 9 | Win32/Keygen | 3.2% |
| 10 | Win32/Conficker | 3.0% |

- The most common threat family in Malta in 4Q10 was Win32/ClickPotato, which affected 14.3 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The second most common threat family in Malta in 4Q10 was Win32/Zwangi, which affected 13.2 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The third most common threat family in Malta in 4Q10 was JS/Pornpop, which affected 9.6 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Malta in 4Q10 was Win32/Hotbar, which affected 7.7 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

# Martinique

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

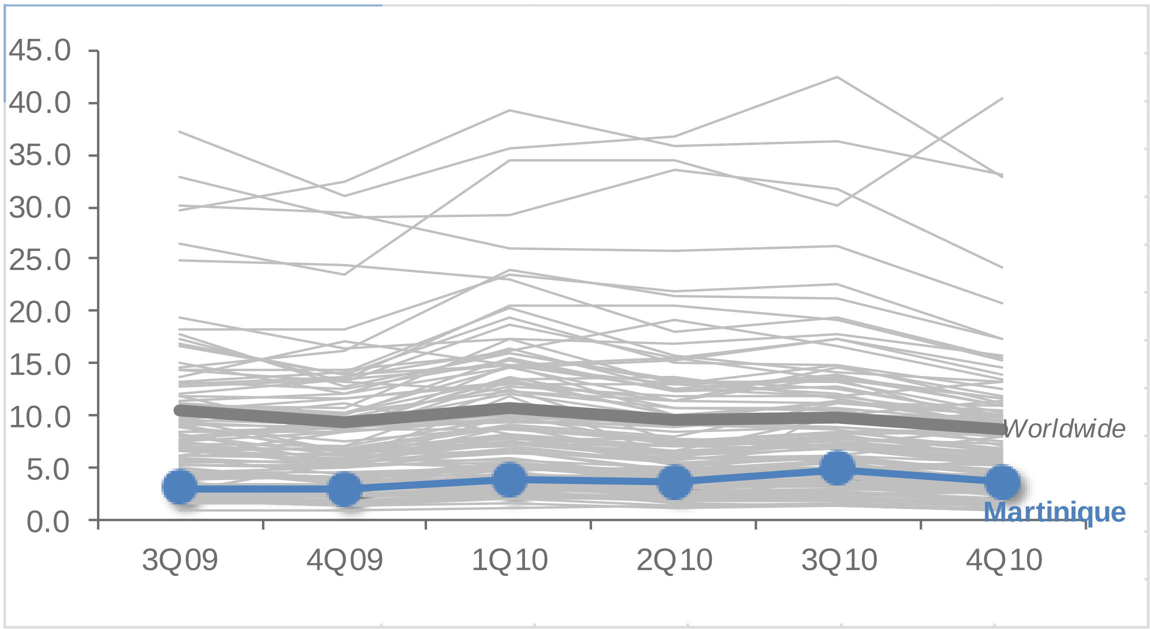
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Martinique in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Martinique and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.9 | 3.7 | 5.0 | 3.7 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | | | | |
| Malware hosting sites per 1000 hosts | | | | |
| Percentage of sites hosting drive-by downloads | 3.125% | | | |

## Infection Trends (CCM)

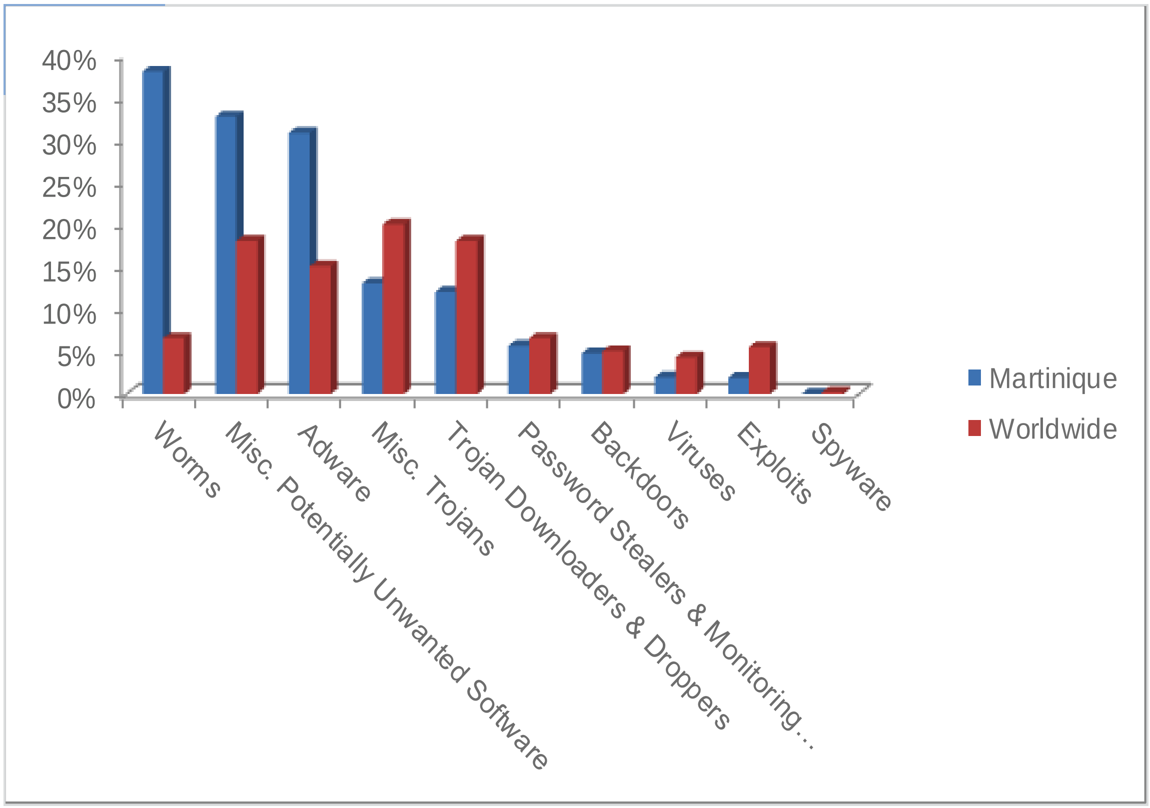
The MSRT detected malware on 3.7 of every 1,000 computers scanned in Martinique in 4Q10 (a CCM score of 3.7, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Martinique over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Martinique and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Martinique in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Martinique in 4Q10 was Worms, which affected 38.0 percent of all cleaned computers, down from 42.2 percent in 3Q10.
- The second most common category in Martinique in 4Q10 was Misc. Potentially Unwanted Software, which affected 32.7 percent of all cleaned computers, up from 24.2 percent in 3Q10.
- The third most common category in Martinique in 4Q10 was Adware, which affected 30.8 percent of all cleaned computers, up from 22.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Martinique in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Vobfus | 22.5% |
| 2 | Win32/ClickPotato | 16.4% |
| 3 | Win32/Autorun | 15.4% |
| 4 | Win32/Zwangi | 14.9% |
| 5 | Win32/Hotbar | 7.9% |
| 6 | Win32/Brontok | 6.6% |
| 7 | Win32/Taterf | 6.1% |
| 8 | Win32/Renos | 4.2% |
| 9 | ASX/Wimad | 3.6% |
| 10 | Win32/Frethog | 3.6% |

- ♦ The most common threat family in Martinique in 4Q10 was Win32/Vobfus, which affected 22.5 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

- ♦ The second most common threat family in Martinique in 4Q10 was Win32/ClickPotato, which affected 16.4 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.

- ♦ The third most common threat family in Martinique in 4Q10 was Win32/Autorun, which affected 15.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

- ♦ The fourth most common threat family in Martinique in 4Q10 was Win32/Zwangi, which affected 14.9 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Mauritius

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

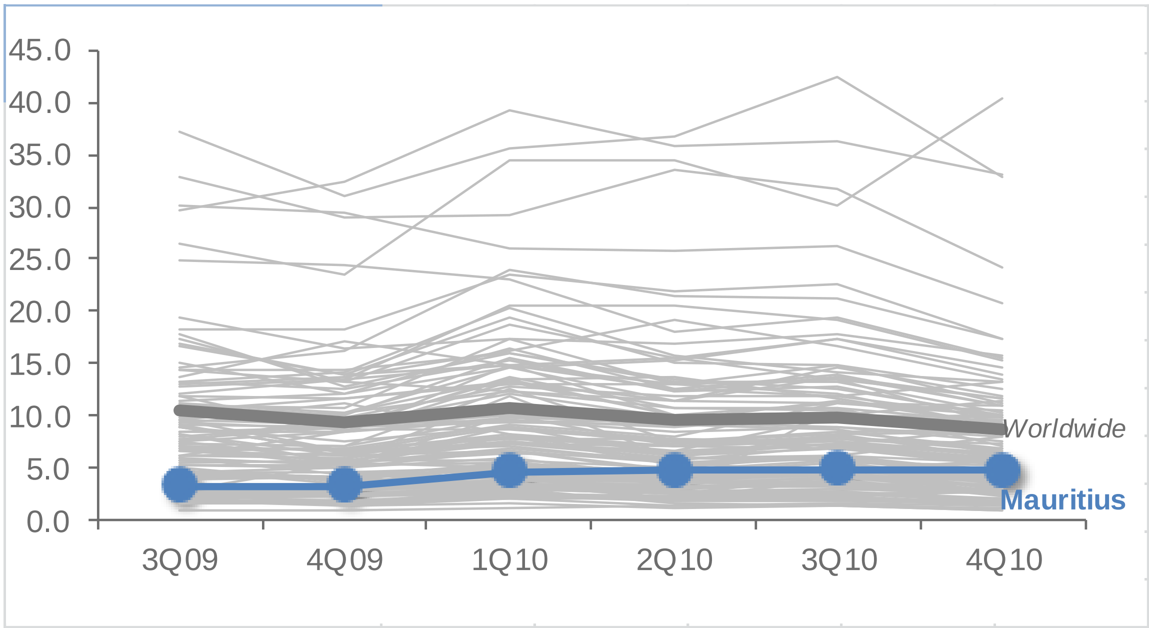
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Mauritius in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Mauritius and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">4.7</td><td colspan="3">4.8</td><td colspan="3">5.0</td><td colspan="3">4.9</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.73</td><td colspan="6">54.32</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.35</td><td colspan="6">30.91</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.136%</td><td colspan="4">0.244%</td><td colspan="4">0.106%</td></tr>
</table>

## Infection Trends (CCM)

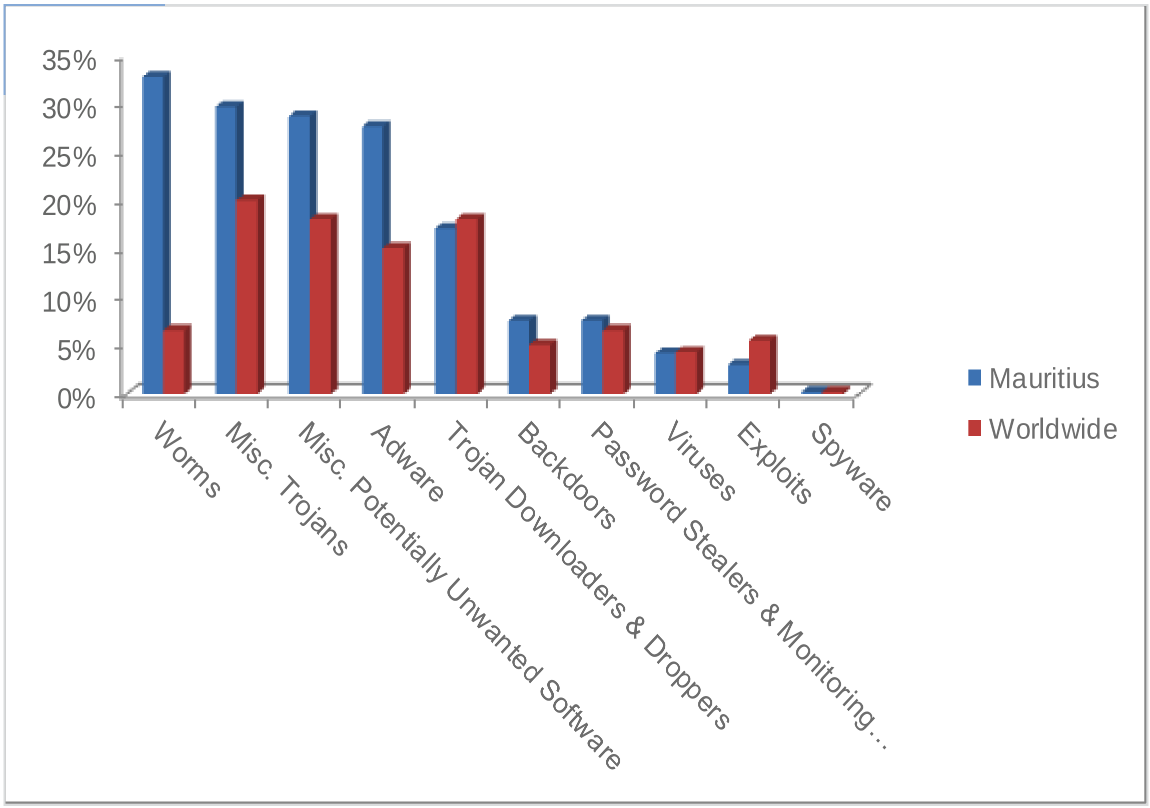
The MSRT detected malware on 4.9 of every 1,000 computers scanned in Mauritius in 4Q10 (a CCM score of 4.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Mauritius over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Mauritius and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Mauritius in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Mauritius in 4Q10 was Worms, which affected 32.7 percent of all cleaned computers, down from 42.0 percent in 3Q10.
- The second most common category in Mauritius in 4Q10 was Misc. Trojans, which affected 29.6 percent of all cleaned computers, up from 28.5 percent in 3Q10.
- The third most common category in Mauritius in 4Q10 was Misc. Potentially Unwanted Software, which affected 28.7 percent of all cleaned computers, up from 25.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Mauritius in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 16.8% |
| 2 | Win32/Autorun | 14.7% |
| 3 | Win32/ClickPotato | 11.2% |
| 4 | JS/Pornpop | 10.4% |
| 5 | Win32/Renos | 8.3% |
| 6 | Win32/Zwangi | 8.3% |
| 7 | Win32/Taterf | 5.8% |
| 8 | Win32/Hotbar | 5.8% |
| 9 | Win32/Vobfus | 4.8% |
| 10 | Win32/Conficker | 4.5% |

- The most common threat family in Mauritius in 4Q10 was Win32/Rimecud, which affected 16.8 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Mauritius in 4Q10 was Win32/Autorun, which affected 14.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Mauritius in 4Q10 was Win32/ClickPotato, which affected 11.2 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The fourth most common threat family in Mauritius in 4Q10 was JS/Pornpop, which affected 10.4 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Mexico

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

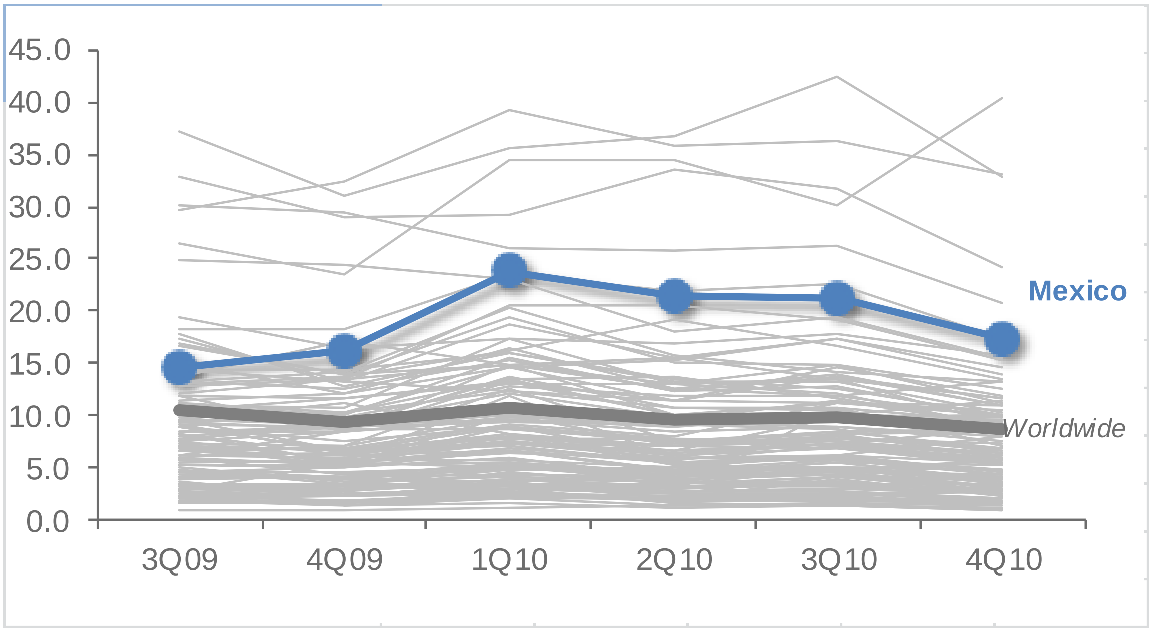
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Mexico in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Mexico and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 23.9 | 21.4 | 21.1 | 17.4 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.07 | | 0.01 | |
| Malware hosting sites per 1000 hosts | 0.03 | | 0.02 | |
| Percentage of sites hosting drive-by downloads | 0.224% | 0.071% | 0.067% | |

## Infection Trends (CCM)

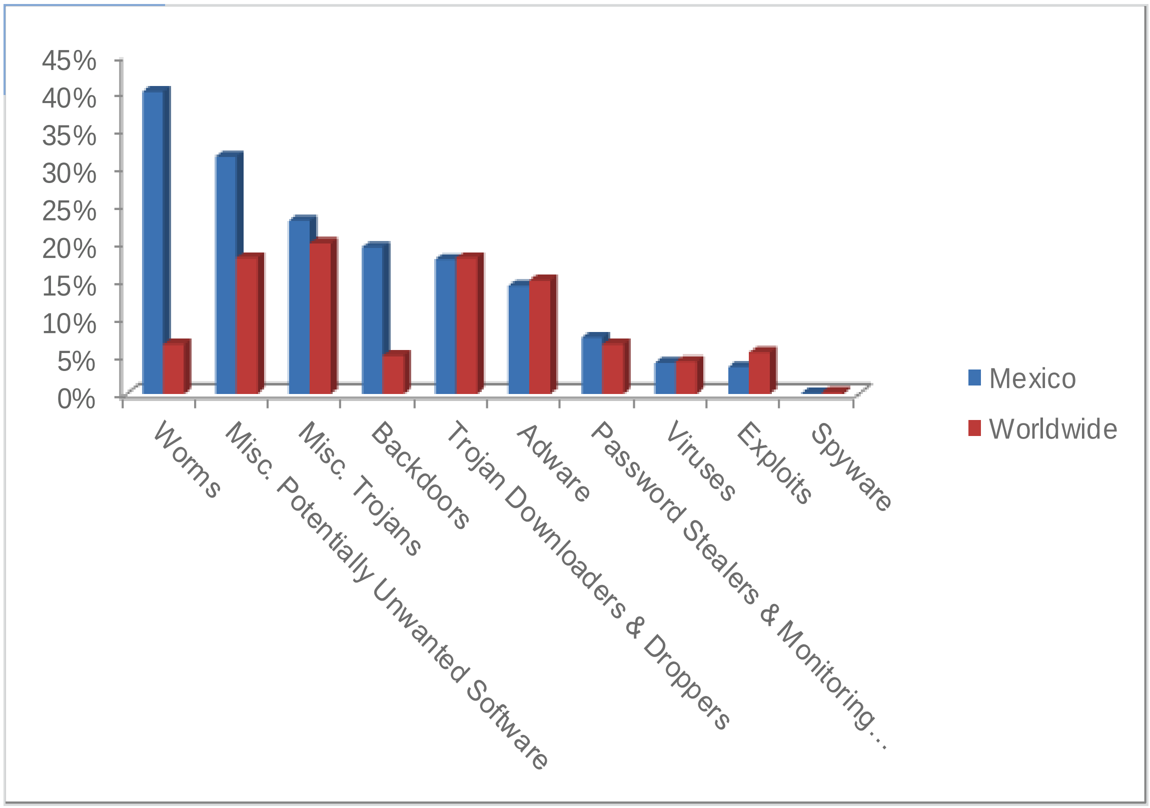
The MSRT detected malware on 17.4 of every 1,000 computers scanned in Mexico in 4Q10 (a CCM score of 17.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Mexico over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Mexico and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Mexico in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Mexico in 4Q10 was Worms, which affected 40.1 percent of all cleaned computers, down from 47.3 percent in 3Q10.
- The second most common category in Mexico in 4Q10 was Misc. Potentially Unwanted Software, which affected 31.5 percent of all cleaned computers, up from 30.5 percent in 3Q10.
- The third most common category in Mexico in 4Q10 was Misc. Trojans, which affected 23.0 percent of all cleaned computers, up from 22.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Mexico in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 17.0% |
| 2 | Win32/IRCbot | 14.8% |
| 3 | Win32/Rimecud | 13.2% |
| 4 | Win32/Vobfus | 10.5% |
| 5 | JS/Pornpop | 7.2% |
| 6 | Win32/Taterf | 6.8% |
| 7 | Win32/Renos | 6.7% |
| 8 | Win32/Conficker | 6.4% |
| 9 | Win32/VBInject | 5.5% |
| 10 | Win32/Pushbot | 5.1% |

- The most common threat family in Mexico in 4Q10 was Win32/Autorun, which affected 17.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Mexico in 4Q10 was Win32/IRCbot, which affected 14.8 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The third most common threat family in Mexico in 4Q10 was Win32/Rimecud, which affected 13.2 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Mexico in 4Q10 was Win32/Vobfus, which affected 10.5 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

# Moldova

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

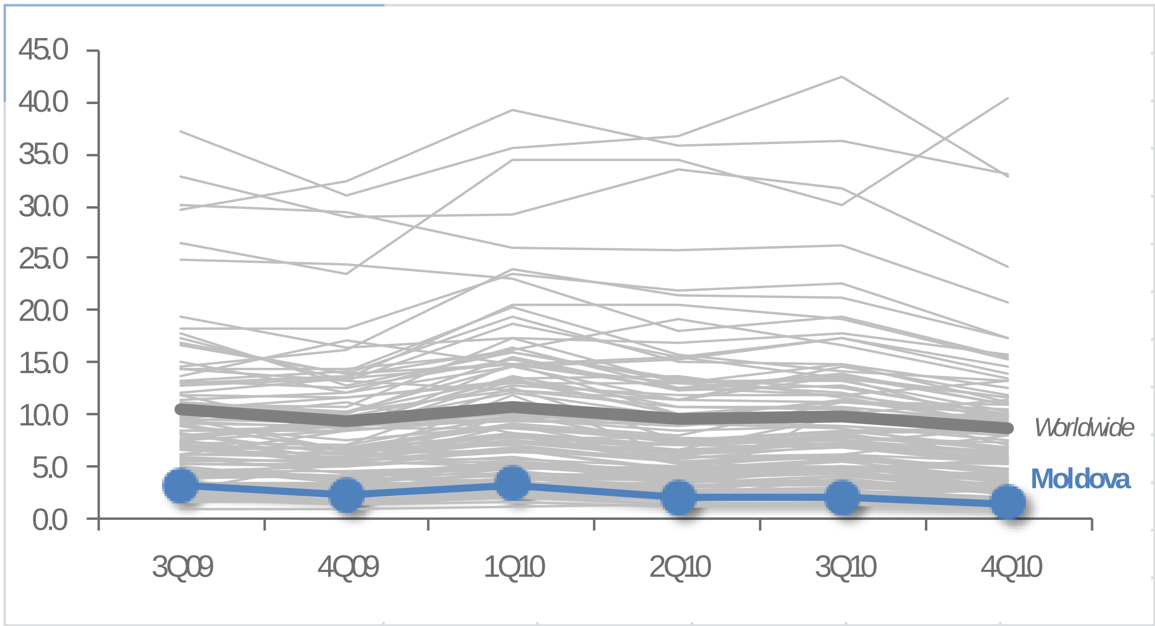
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Moldova in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Moldova and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.3 | 2.0 | 2.1 | 1.6 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.14 | | 0.03 | |
| Malware hosting sites per 1000 hosts | 45.70 | | 122.02 | |
| Percentage of sites hosting drive-by downloads | 0.269% | 0.075% | 0.071% | |

## Infection Trends (CCM)

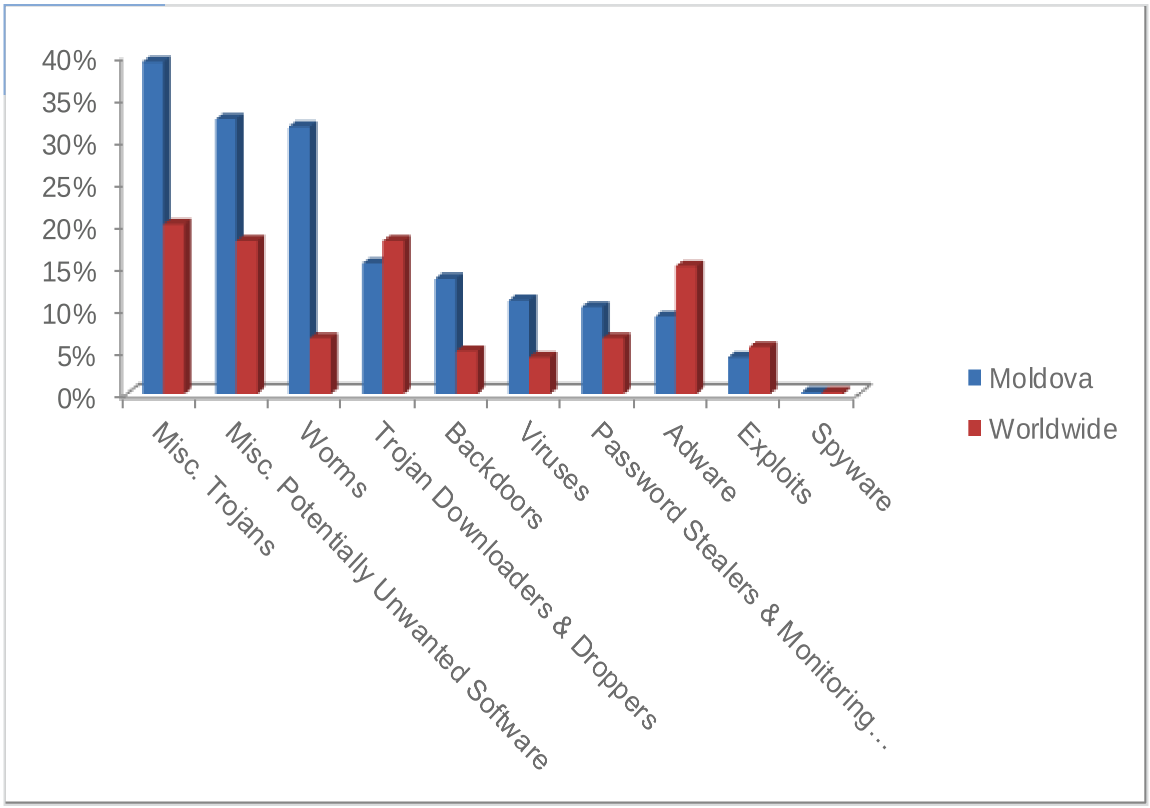
The MSRT detected malware on 1.6 of every 1,000 computers scanned in Moldova in 4Q10 (a CCM score of 1.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Moldova over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Moldova and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Moldova in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Moldova in 4Q10 was Misc. Trojans, which affected 39.2 percent of all cleaned computers, down from 41.4 percent in 3Q10.
- The second most common category in Moldova in 4Q10 was Misc. Potentially Unwanted Software, which affected 32.4 percent of all cleaned computers, down from 37.1 percent in 3Q10.
- The third most common category in Moldova in 4Q10 was Worms, which affected 31.5 percent of all cleaned computers, up from 29.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Moldova in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 21.2% |
| 2 | Win32/Autorun | 17.0% |
| 3 | Win32/IRCbot | 8.1% |
| 4 | Win32/Sality | 6.5% |
| 5 | Win32/Keygen | 6.4% |
| 6 | Win32/Obfuscator | 6.2% |
| 7 | Win32/Taterf | 6.1% |
| 8 | JS/Pornpop | 5.6% |
| 9 | Win32/Conficker | 5.2% |
| 10 | Win32/Renos | 4.8% |

- The most common threat family in Moldova in 4Q10 was Win32/Rimecud, which affected 21.2 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Moldova in 4Q10 was Win32/Autorun, which affected 17.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Moldova in 4Q10 was Win32/IRCbot, which affected 8.1 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The fourth most common threat family in Moldova in 4Q10 was Win32/Sality, which affected 6.5 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Mongolia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

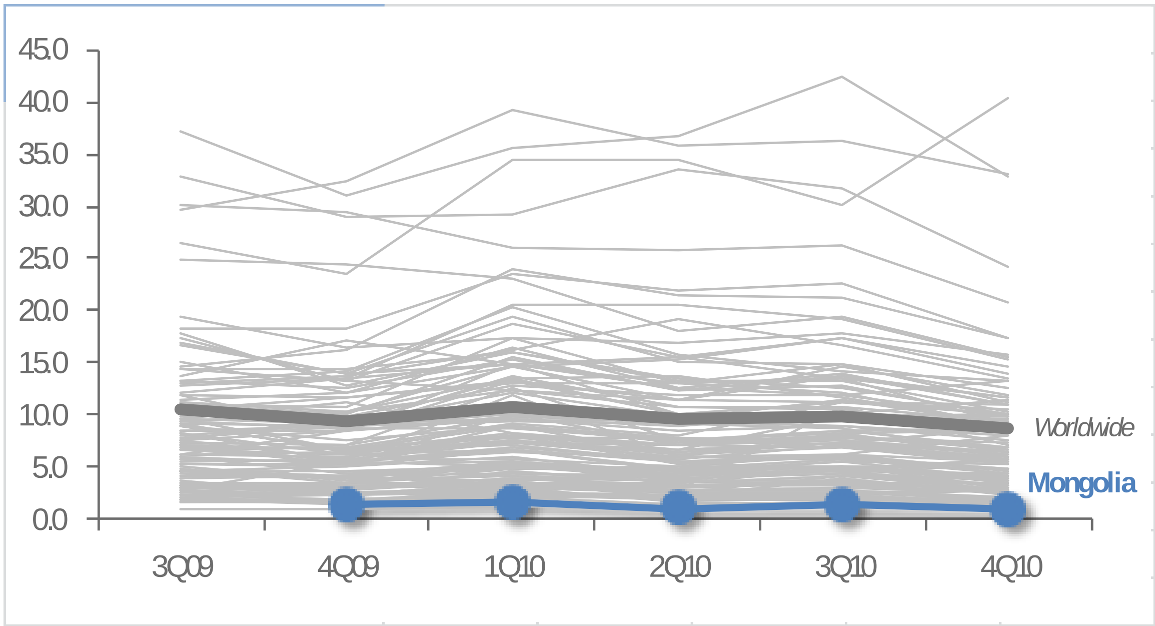
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Mongolia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Mongolia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">1.7</td><td colspan="3">1.1</td><td colspan="3">1.3</td><td colspan="3">1.0</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">244.38</td><td colspan="6">73.03</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">148.88</td><td colspan="6">250.00</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.130%</td><td colspan="4">0.145%</td><td colspan="4">0.131%</td></tr>
</table>

## Infection Trends (CCM)

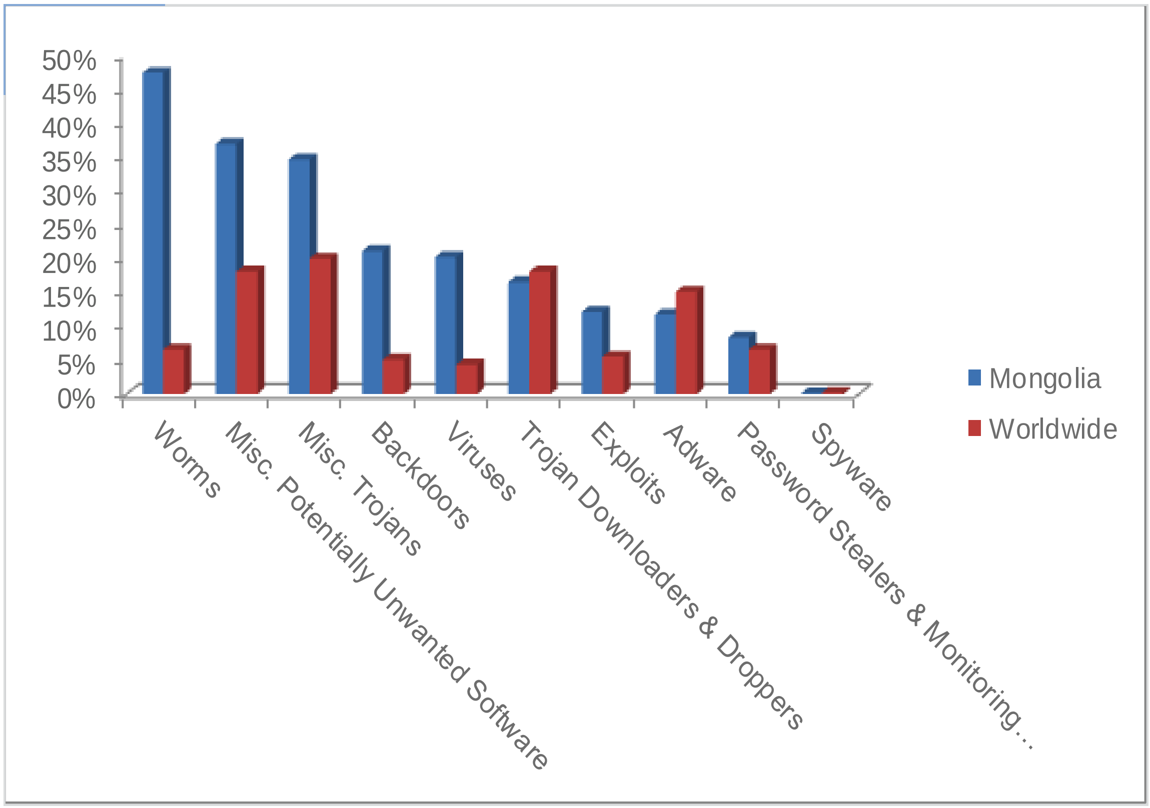
The MSRT detected malware on 1.0 of every 1,000 computers scanned in Mongolia in 4Q10 (a CCM score of 1.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Mongolia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Mongolia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Mongolia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Mongolia in 4Q10 was Worms, which affected 47.3 percent of all cleaned computers, up from 42.8 percent in 3Q10.
- The second most common category in Mongolia in 4Q10 was Misc. Potentially Unwanted Software, which affected 36.9 percent of all cleaned computers, up from 36.4 percent in 3Q10.
- The third most common category in Mongolia in 4Q10 was Misc. Trojans, which affected 34.6 percent of all cleaned computers, up from 32.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Mongolia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 29.4% |
| 2 | Win32/Rimecud | 21.5% |
| 3 | Win32/Sality | 15.5% |
| 4 | Win32/Conficker | 14.5% |
| 5 | Win32/Vobfus | 13.1% |
| 6 | Win32/IRCbot | 13.0% |
| 7 | Win32/Taterf | 11.0% |
| 8 | Win32/VB | 8.6% |
| 9 | CplLnk | 8.2% |
| 10 | Win32/Virut | 7.7% |

- The most common threat family in Mongolia in 4Q10 was Win32/Autorun, which affected 29.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Mongolia in 4Q10 was Win32/Rimecud, which affected 21.5 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Mongolia in 4Q10 was Win32/Sality, which affected 15.5 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Mongolia in 4Q10 was Win32/Conficker, which affected 14.5 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

# Morocco

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

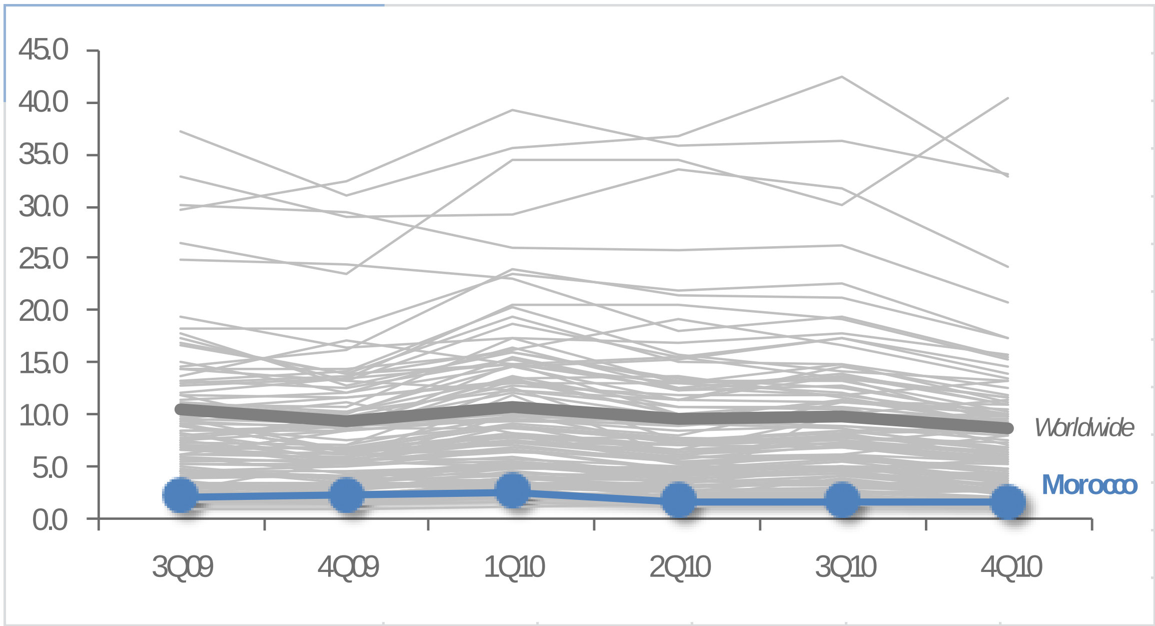
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Morocco in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Morocco and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 2.7 | 1.9 | 1.9 | 1.6 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 1.03 | | 0.11 | |
| Malware hosting sites per 1000 hosts | 1.27 | | 0.02 | |
| Percentage of sites hosting drive-by downloads | 0.329% | 0.174% | 0.091% | |

## Infection Trends (CCM)

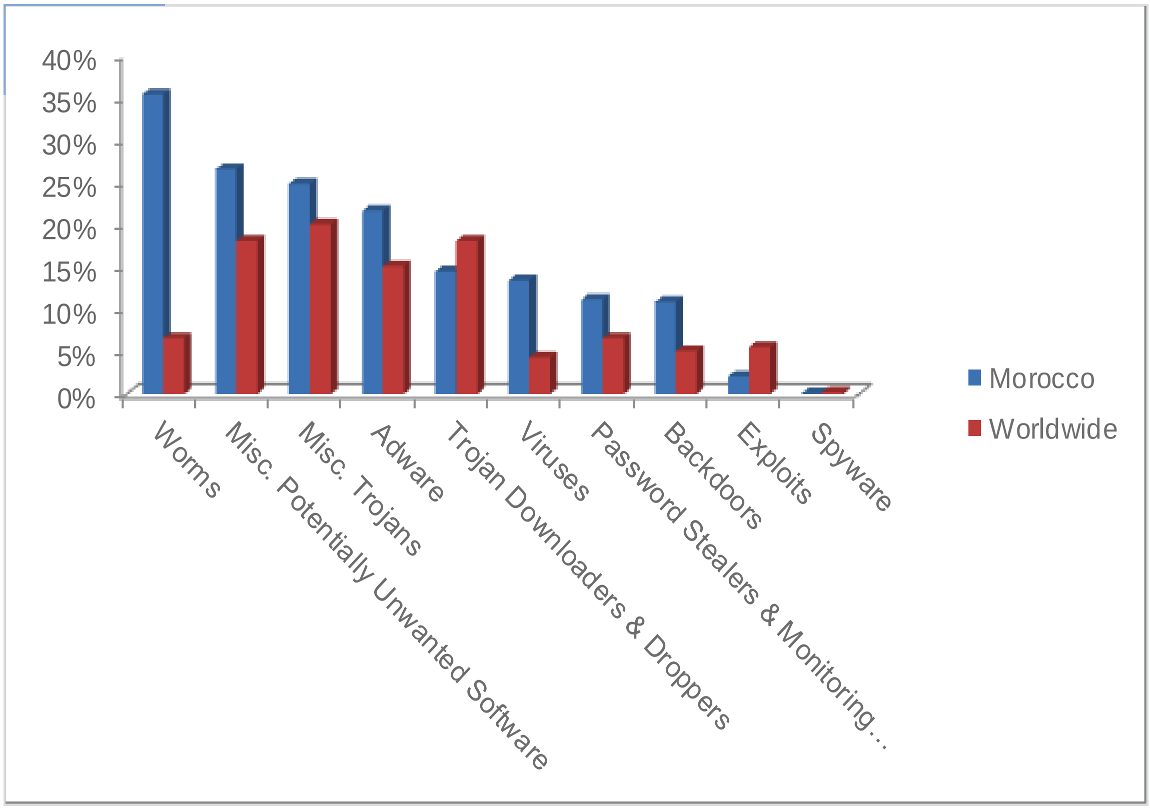
The MSRT detected malware on 1.6 of every 1,000 computers scanned in Morocco in 4Q10 (a CCM score of 1.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Morocco over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Morocco and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Morocco in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Morocco in 4Q10 was Worms, which affected 35.3 percent of all cleaned computers, down from 37.1 percent in 3Q10.
- The second most common category in Morocco in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.5 percent of all cleaned computers, up from 25.1 percent in 3Q10.
- The third most common category in Morocco in 4Q10 was Misc. Trojans, which affected 24.8 percent of all cleaned computers, up from 23.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Morocco in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 13.0% |
| 2 | Win32/Sality | 10.6% |
| 3 | Win32/Taterf | 10.0% |
| 4 | Win32/Zwangi | 9.7% |
| 5 | Win32/Rimecud | 9.4% |
| 6 | Win32/ClickPotato | 9.0% |
| 7 | Win32/Frethog | 7.2% |
| 8 | Win32/Renos | 5.9% |
| 9 | JS/Pornpop | 5.4% |
| 10 | Win32/IRCbot | 4.9% |

- The most common threat family in Morocco in 4Q10 was Win32/Autorun, which affected 13.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Morocco in 4Q10 was Win32/Sality, which affected 10.6 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family in Morocco in 4Q10 was Win32/Taterf, which affected 10.0 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Morocco in 4Q10 was Win32/Zwangi, which affected 9.7 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Nepal

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

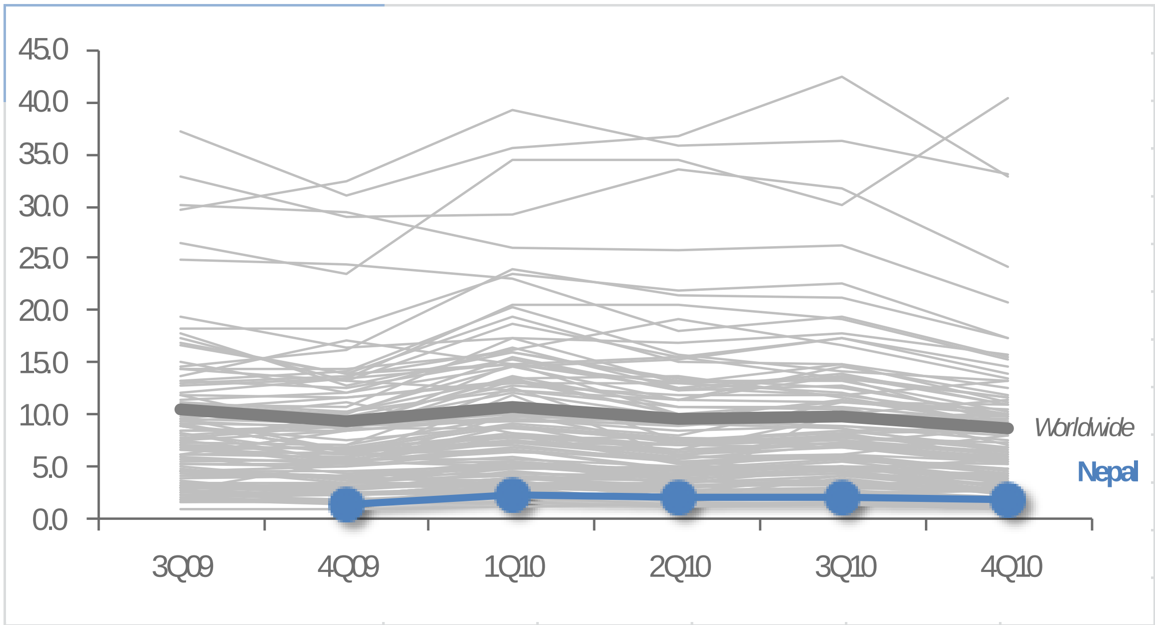
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Nepal in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Nepal and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">2.3</td><td colspan="3">2.0</td><td colspan="3">2.0</td><td colspan="3">1.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.99</td><td colspan="6">0.88</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.40</td><td colspan="6">0.62</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.355%</td><td colspan="4">0.360%</td><td colspan="4">0.286%</td></tr>
</table>

## Infection Trends (CCM)

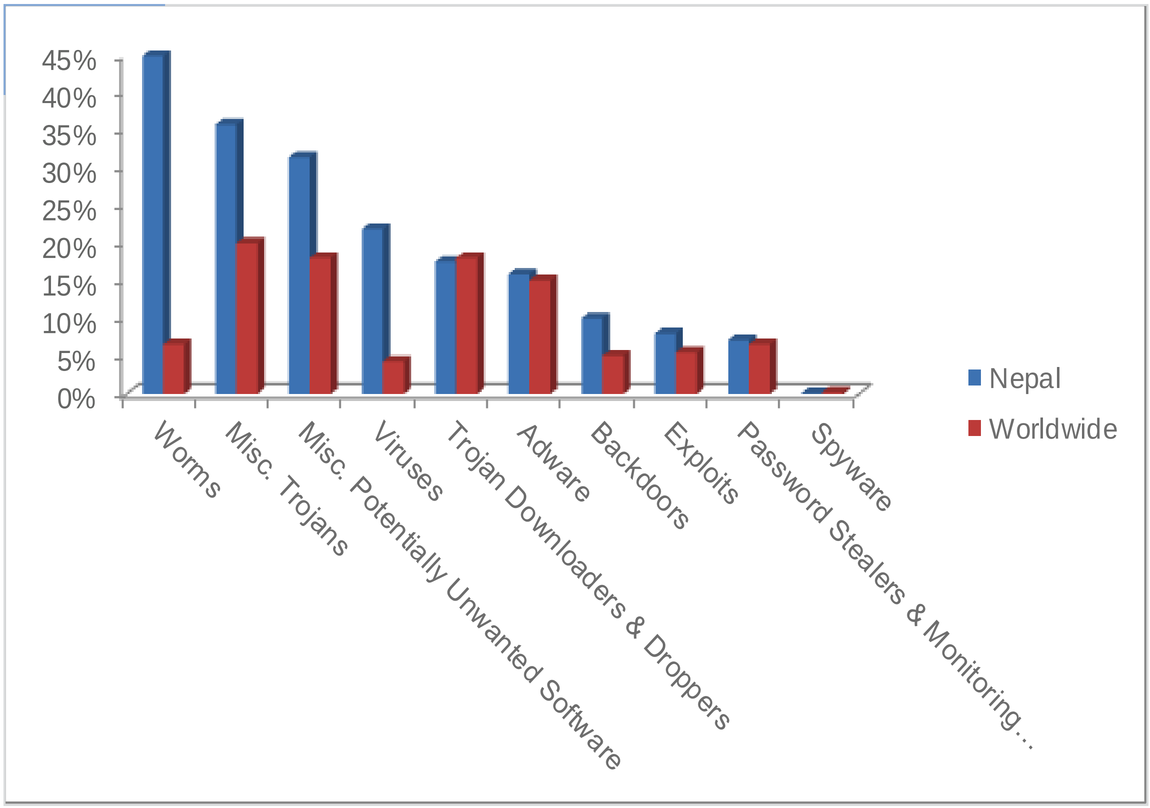
The MSRT detected malware on 1.8 of every 1,000 computers scanned in Nepal in 4Q10 (a CCM score of 1.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Nepal over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Nepal and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Nepal in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Nepal in 4Q10 was Worms, which affected 44.8 percent of all cleaned computers, down from 48.7 percent in 3Q10.
- The second most common category in Nepal in 4Q10 was Misc. Trojans, which affected 35.7 percent of all cleaned computers, up from 33.1 percent in 3Q10.
- The third most common category in Nepal in 4Q10 was Misc. Potentially Unwanted Software, which affected 31.4 percent of all cleaned computers, down from 32.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Nepal in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 29.8% |
| 2 | Win32/Rimecud | 23.7% |
| 3 | Win32/Sality | 19.2% |
| 4 | Win32/Conficker | 10.1% |
| 5 | JS/Pornpop | 9.4% |
| 6 | Win32/Taterf | 6.4% |
| 7 | Sohanad | 5.7% |
| 8 | Win32/Renos | 5.7% |
| 9 | Win32/Virut | 5.4% |
| 10 | Win32/Nuqel | 4.4% |

- The most common threat family in Nepal in 4Q10 was Win32/Autorun, which affected 29.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Nepal in 4Q10 was Win32/Rimecud, which affected 23.7 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Nepal in 4Q10 was Win32/Sality, which affected 19.2 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Nepal in 4Q10 was Win32/Conficker, which affected 10.1 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

# Netherlands

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

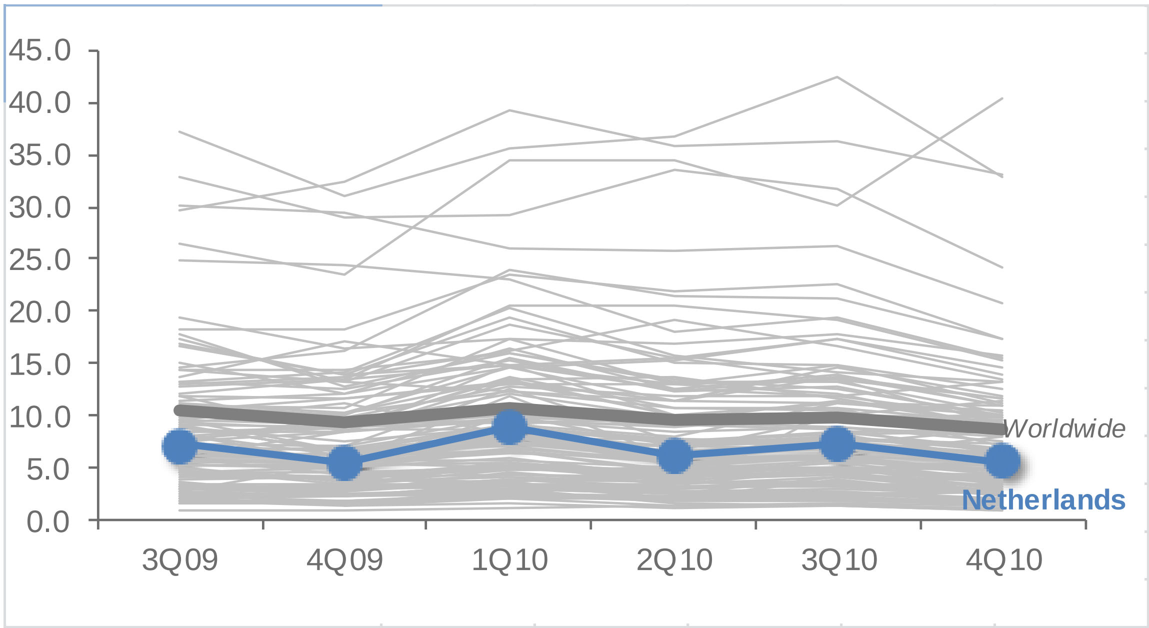
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Netherlands in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Netherlands and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">9.0</td><td colspan="3">6.1</td><td colspan="3">7.3</td><td colspan="3">5.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.69</td><td colspan="6">0.92</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">11.14</td><td colspan="6">3.17</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.088%</td><td colspan="4">0.029%</td><td colspan="4">0.047%</td></tr>
</table>

## Infection Trends (CCM)

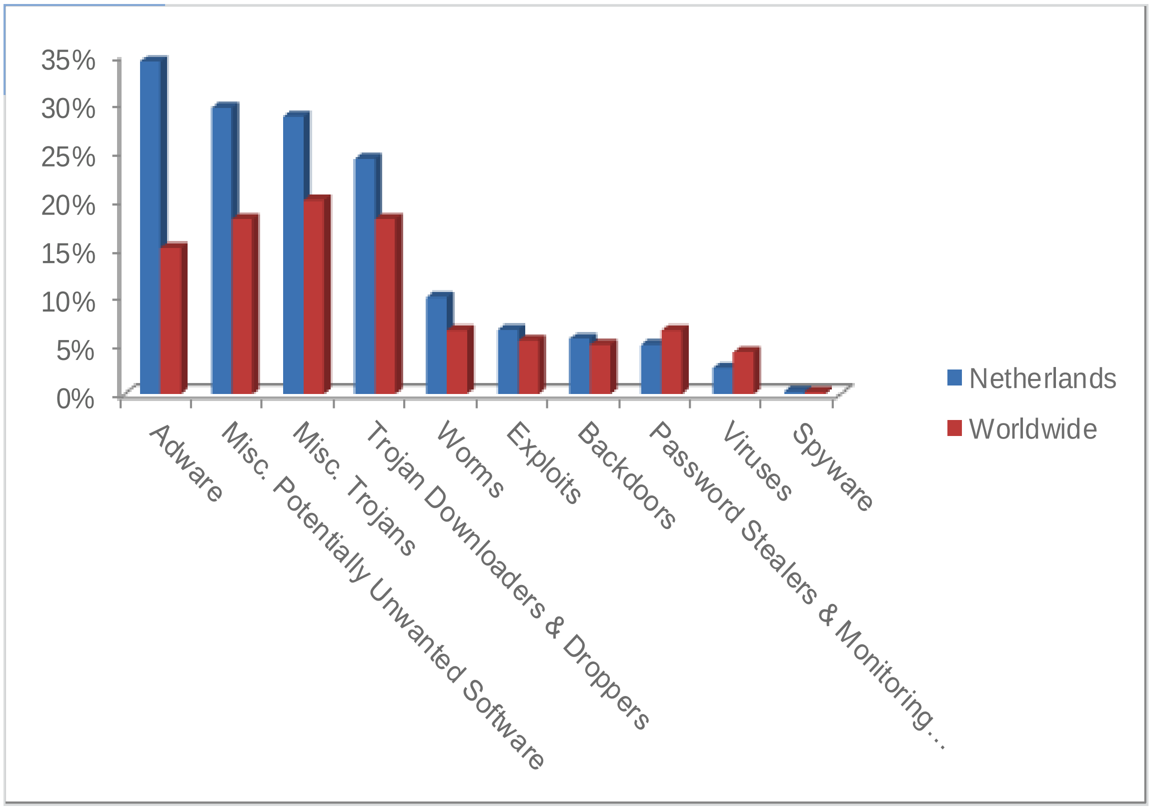
The MSRT detected malware on 5.8 of every 1,000 computers scanned in Netherlands in 4Q10 (a CCM score of 5.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Netherlands over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Netherlands and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Netherlands in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Netherlands in 4Q10 was Adware, which affected 34.3 percent of all cleaned computers, up from 32.3 percent in 3Q10.
- The second most common category in Netherlands in 4Q10 was Misc. Potentially Unwanted Software, which affected 29.5 percent of all cleaned computers, down from 29.5 percent in 3Q10.
- The third most common category in Netherlands in 4Q10 was Misc. Trojans, which affected 28.6 percent of all cleaned computers, up from 27.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Netherlands in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 17.5% |
| 2 | Win32/ClickPotato | 9.0% |
| 3 | Win32/Zwangi | 8.6% |
| 4 | Win32/Renos | 6.6% |
| 5 | Win32/Keygen | 5.9% |
| 6 | Win32/Alureon | 5.7% |
| 7 | ASX/Wimad | 5.7% |
| 8 | Win32/Hotbar | 5.7% |
| 9 | Java/CVE-2009-3867 | 3.2% |
| 10 | Win32/Autorun | 3.2% |

- The most common threat family in Netherlands in 4Q10 was JS/Pornpop, which affected 17.5 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Netherlands in 4Q10 was Win32/ClickPotato, which affected 9.0 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Netherlands in 4Q10 was Win32/Zwangi, which affected 8.6 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in Netherlands in 4Q10 was Win32/Renos, which affected 6.6 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.

# Netherlands Antilles

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

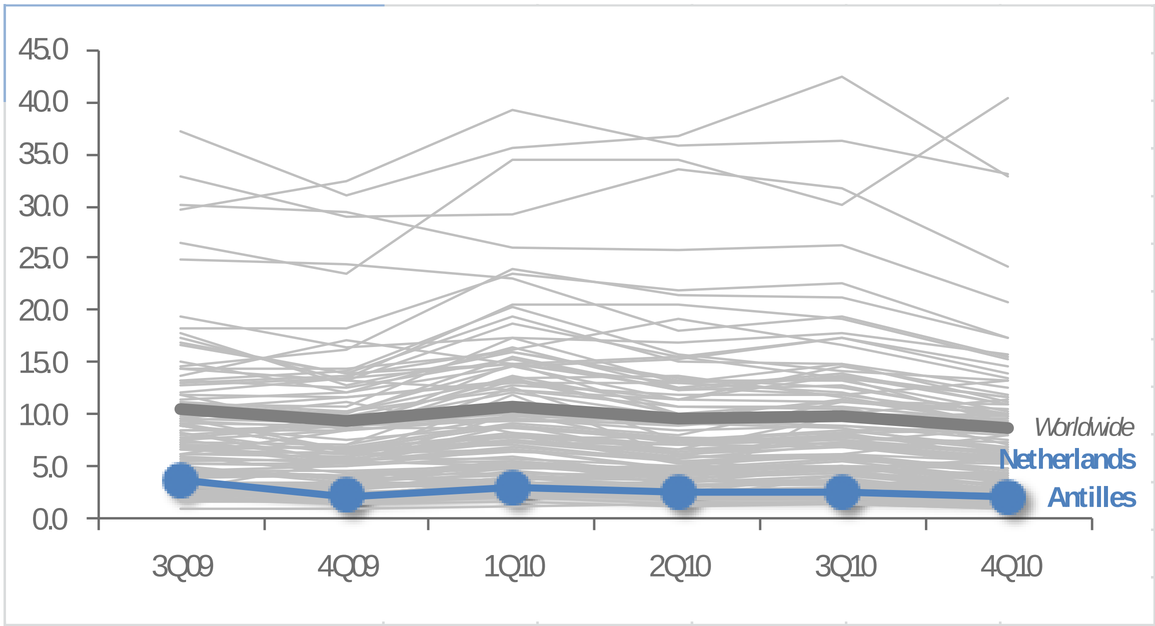
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Netherlands Antilles in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Netherlands Antilles and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.0 | 2.5 | 2.5 | 2.2 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | | | | |
| Malware hosting sites per 1000 hosts | 0.21 | | 0.11 | |
| Percentage of sites hosting drive-by downloads | 0.300% | | | |

## Infection Trends (CCM)

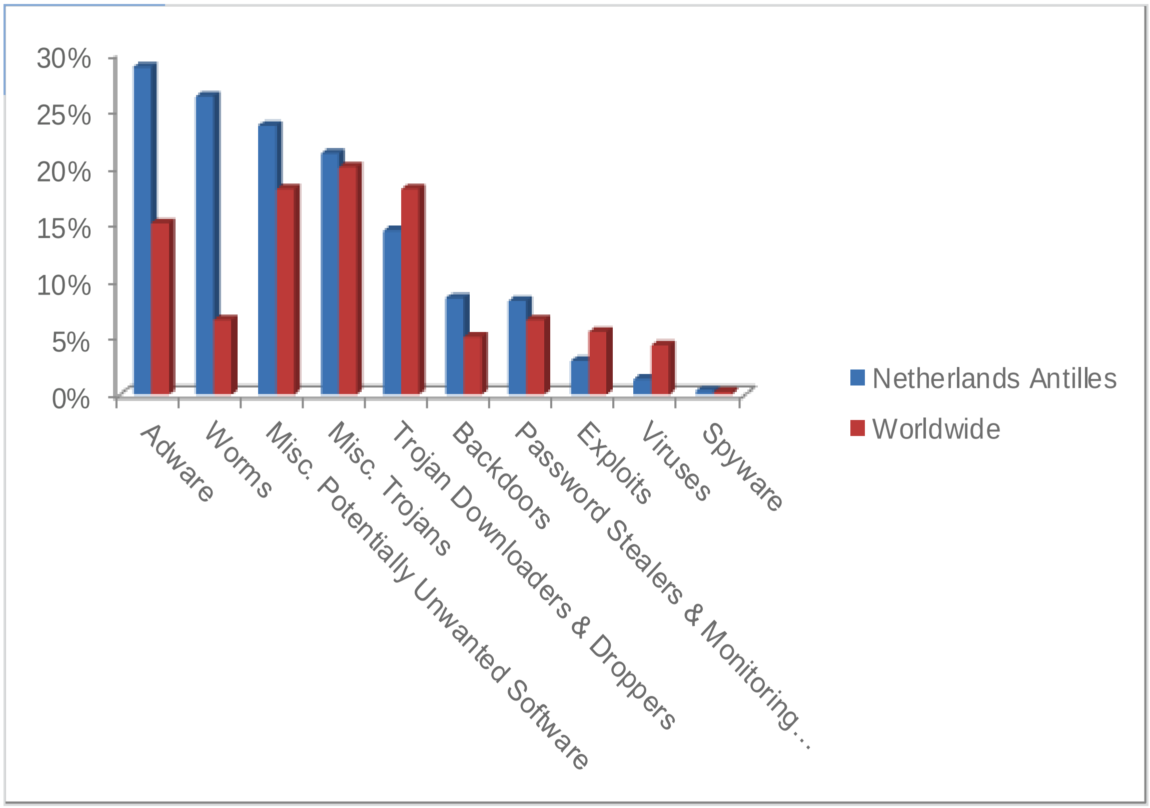
The MSRT detected malware on 2.2 of every 1,000 computers scanned in Netherlands Antilles in 4Q10 (a CCM score of 2.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Netherlands Antilles over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Netherlands Antilles and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Netherlands Antilles in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Netherlands Antilles in 4Q10 was Adware, which affected 28.8 percent of all cleaned computers, down from 30.9 percent in 3Q10.
- The second most common category in Netherlands Antilles in 4Q10 was Worms, which affected 26.2 percent of all cleaned computers, down from 26.3 percent in 3Q10.
- The third most common category in Netherlands Antilles in 4Q10 was Misc. Potentially Unwanted Software, which affected 23.6 percent of all cleaned computers, down from 25.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Netherlands Antilles in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Zwangi | 11.1% |
| 2 | Win32/ClickPotato | 10.3% |
| 3 | Win32/Hotbar | 8.0% |
| 4 | Win32/Autorun | 7.4% |
| 5 | Win32/Vobfus | 6.9% |
| 6 | Win32/Rimecud | 6.5% |
| 7 | JS/Pornpop | 6.5% |
| 8 | Win32/Renos | 5.5% |
| 9 | Win32/Taterf | 4.8% |
| 10 | Win32/IRCbot | 4.4% |

- The most common threat family in Netherlands Antilles in 4Q10 was Win32/Zwangi, which affected 11.1 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The second most common threat family in Netherlands Antilles in 4Q10 was Win32/ClickPotato, which affected 10.3 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Netherlands Antilles in 4Q10 was Win32/Hotbar, which affected 8.0 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.
- The fourth most common threat family in Netherlands Antilles in 4Q10 was Win32/Autorun, which affected 7.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

# New Zealand

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

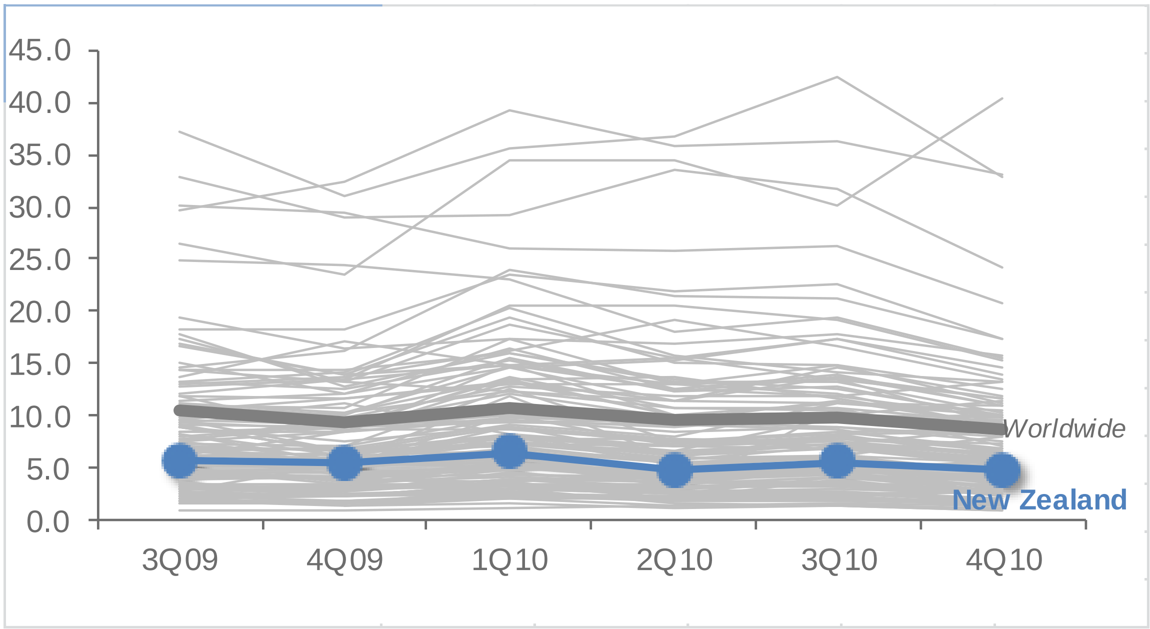
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in New Zealand in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in New Zealand and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">6.6</td><td colspan="3">4.9</td><td colspan="3">5.7</td><td colspan="3">4.9</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.30</td><td colspan="6">0.18</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.11</td><td colspan="6">0.11</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.267%</td><td colspan="4">0.025%</td><td colspan="4">0.032%</td></tr>
</table>

## Infection Trends (CCM)

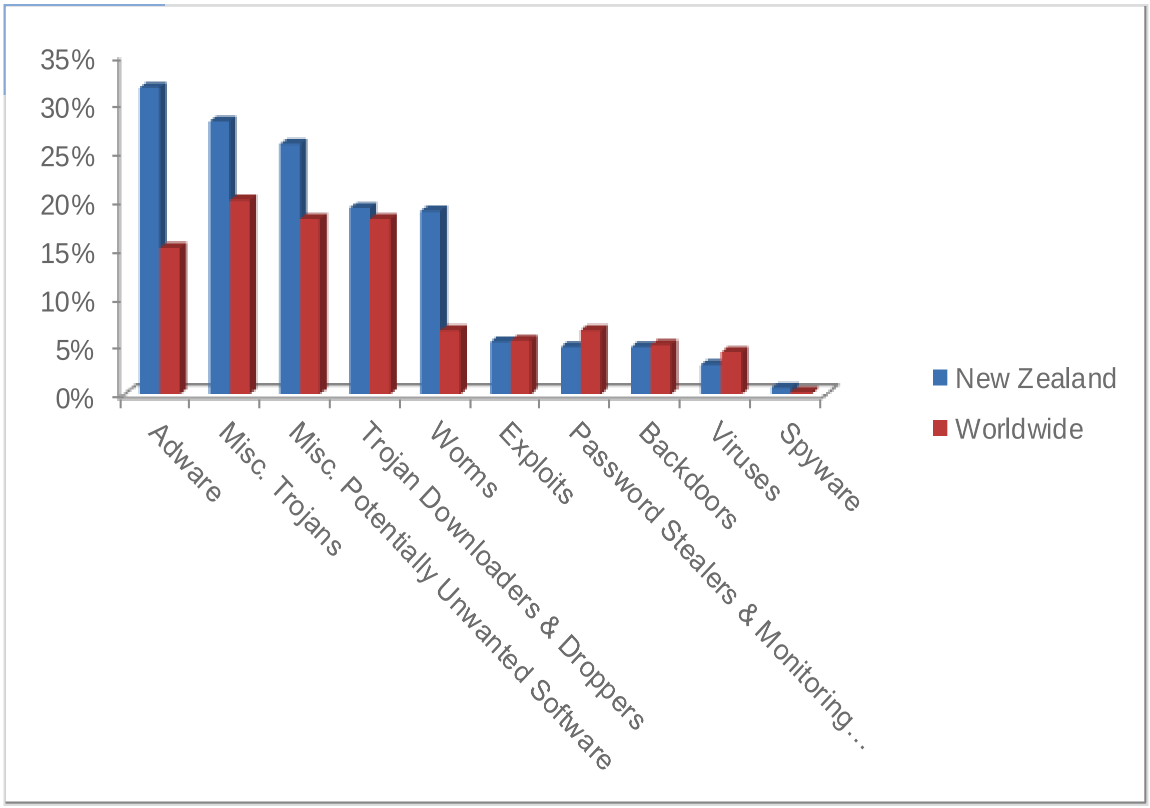
The MSRT detected malware on 4.9 of every 1,000 computers scanned in New Zealand in 4Q10 (a CCM score of 4.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for New Zealand over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in New Zealand and worldwide



## Threat Categories

Malware and potentially unwanted software categories in New Zealand in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in New Zealand in 4Q10 was Adware, which affected 31.6 percent of all cleaned computers, up from 28.1 percent in 3Q10.
- The second most common category in New Zealand in 4Q10 was Misc. Trojans, which affected 28.1 percent of all cleaned computers, up from 26.8 percent in 3Q10.
- The third most common category in New Zealand in 4Q10 was Misc. Potentially Unwanted Software, which affected 25.8 percent of all cleaned computers, down from 26.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in New Zealand in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 18.7% |
| 2 | Win32/Autorun | 6.8% |
| 3 | Win32/ClickPotato | 6.1% |
| 4 | Win32/Zwangi | 5.9% |
| 5 | Win32/Renos | 5.8% |
| 6 | Win32/Vobfus | 5.7% |
| 7 | ASX/Wimad | 5.0% |
| 8 | Win32/Hotbar | 4.9% |
| 9 | Win32/Winwebsec | 4.1% |
| 10 | PowerRegScheduler | 3.3% |

- The most common threat family in New Zealand in 4Q10 was JS/Pornpop, which affected 18.7 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in New Zealand in 4Q10 was Win32/Autorun, which affected 6.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in New Zealand in 4Q10 was Win32/ClickPotato, which affected 6.1 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The fourth most common threat family in New Zealand in 4Q10 was Win32/Zwangi, which affected 5.9 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Nicaragua

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

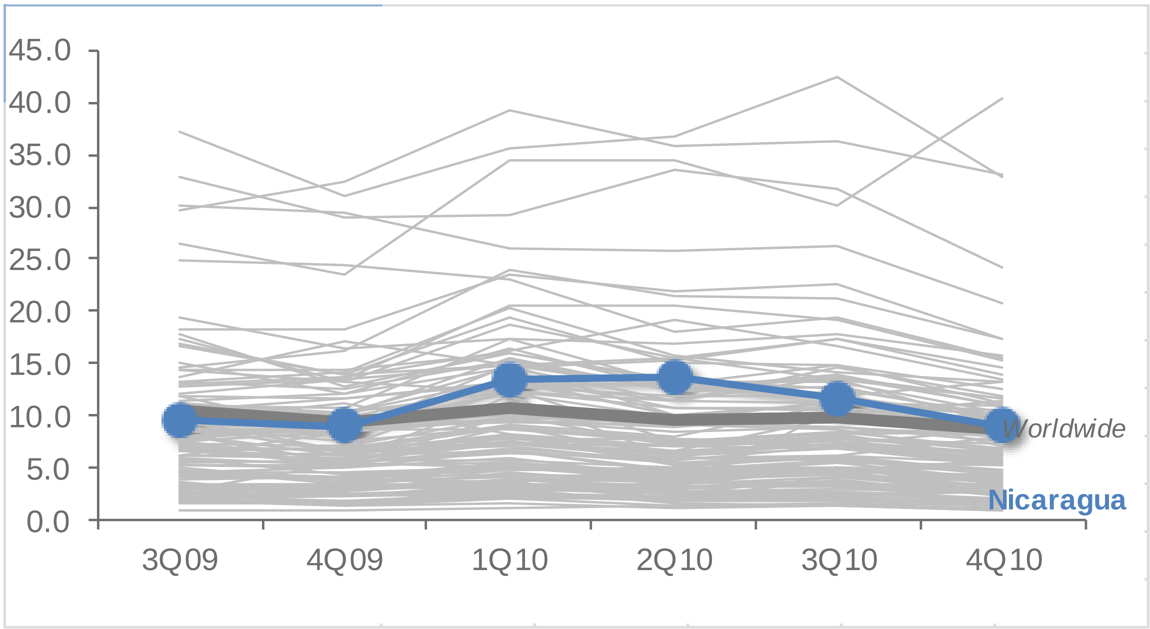
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Nicaragua in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Nicaragua and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 13.5 | 13.8 | 11.7 | 9.1 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | | | 0.57 | |
| Malware hosting sites per 1000 hosts | | | 0.05 | |
| Percentage of sites hosting drive-by downloads | 0.054% | | | |

## Infection Trends (CCM)

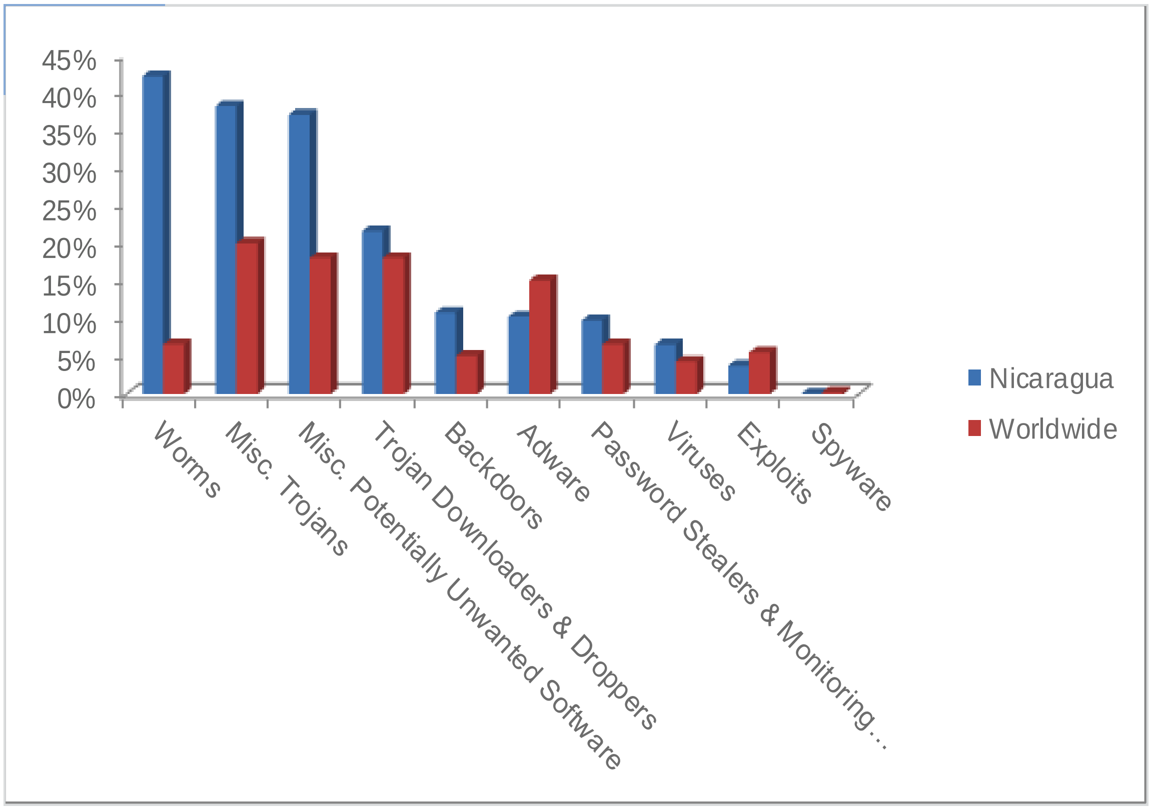
The MSRT detected malware on 9.1 of every 1,000 computers scanned in Nicaragua in 4Q10 (a CCM score of 9.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Nicaragua over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Nicaragua and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Nicaragua in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Nicaragua in 4Q10 was Worms, which affected 42.2 percent of all cleaned computers, down from 53.3 percent in 3Q10.
- The second most common category in Nicaragua in 4Q10 was Misc. Trojans, which affected 38.2 percent of all cleaned computers, up from 34.4 percent in 3Q10.
- The third most common category in Nicaragua in 4Q10 was Misc. Potentially Unwanted Software, which affected 37.1 percent of all cleaned computers, up from 26.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Nicaragua in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 31.1% |
| 2 | Win32/Autorun | 20.6% |
| 3 | Win32/Vobfus | 13.1% |
| 4 | Win32/Taterf | 12.1% |
| 5 | Win32/Keygen | 9.5% |
| 6 | Win32/Renos | 8.1% |
| 7 | Win32/Conficker | 6.9% |
| 8 | Win32/Frethog | 6.2% |
| 9 | Win32/Silly_P2P | 5.9% |
| 10 | Win32/FlyAgent | 5.1% |

- The most common threat family in Nicaragua in 4Q10 was Win32/Rimecud, which affected 31.1 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Nicaragua in 4Q10 was Win32/Autorun, which affected 20.6 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Nicaragua in 4Q10 was Win32/Vobfus, which affected 13.1 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Nicaragua in 4Q10 was Win32/Taterf, which affected 12.1 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Nigeria

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

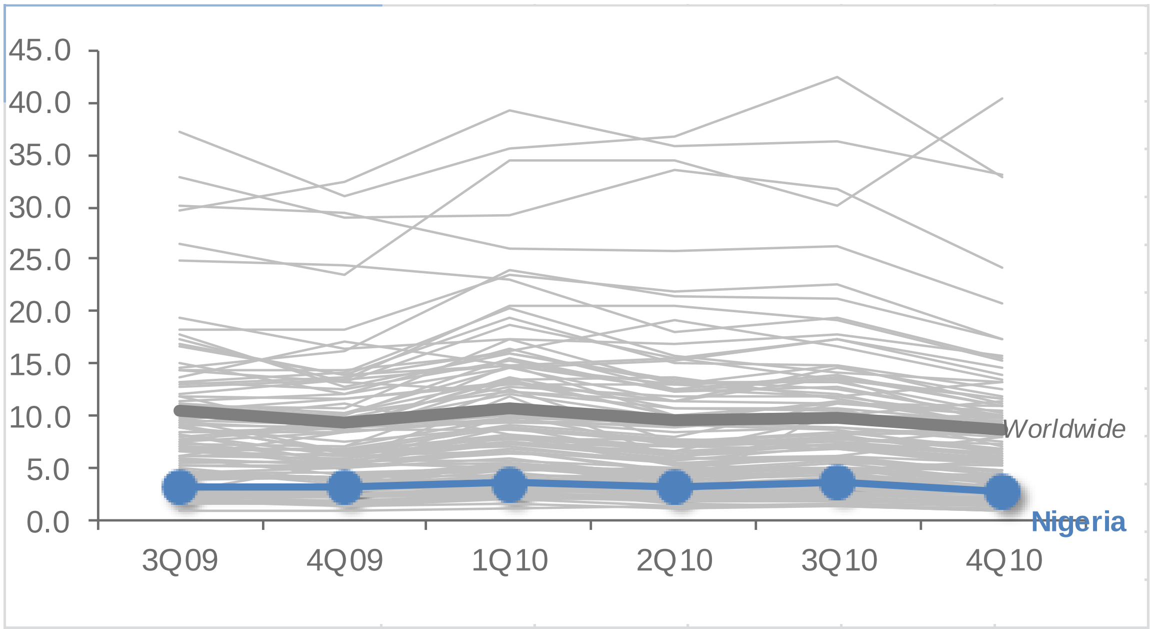
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Nigeria in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Nigeria and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.5 | 3.2 | 3.7 | 2.8 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | | | 0.95 | |
| Malware hosting sites per 1000 hosts | 29.58 | | 4.77 | |
| Percentage of sites hosting drive-by downloads | 0.291% | | | |

## Infection Trends (CCM)

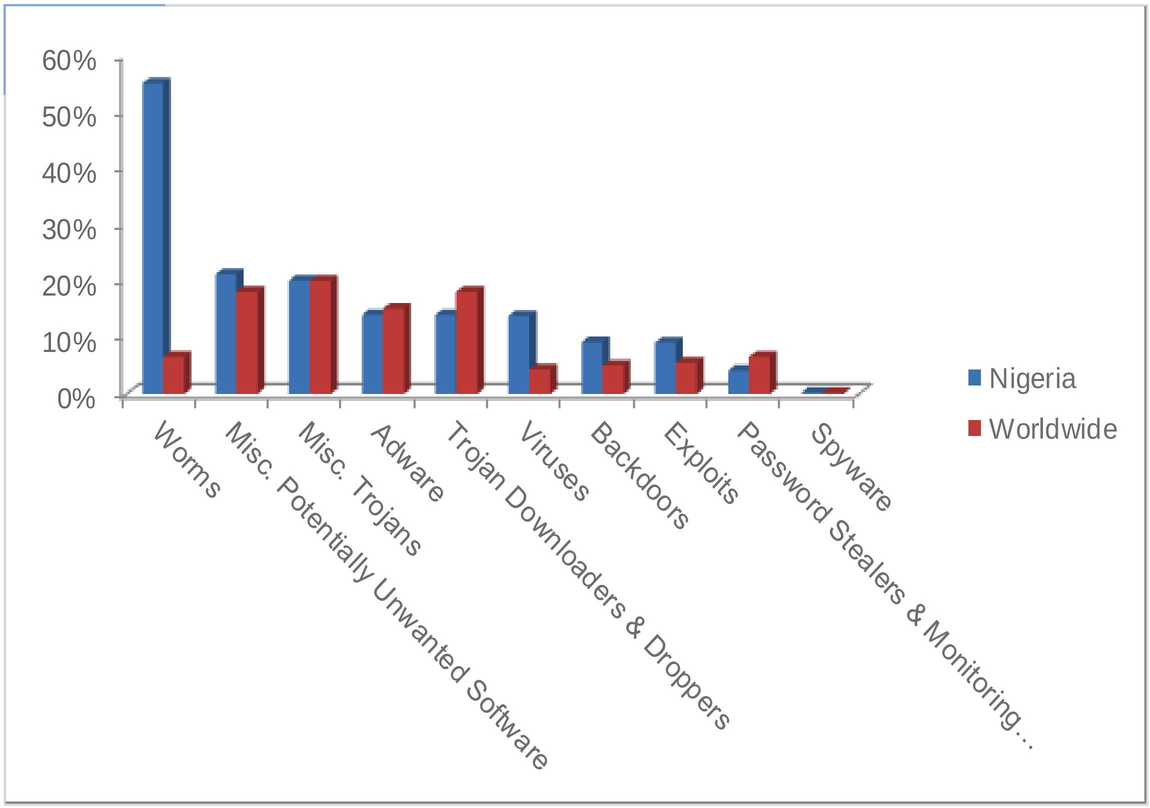
The MSRT detected malware on 2.8 of every 1,000 computers scanned in Nigeria in 4Q10 (a CCM score of 2.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Nigeria over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Nigeria and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Nigeria in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Nigeria in 4Q10 was Worms, which affected 55.0 percent of all cleaned computers, down from 59.2 percent in 3Q10.
- The second most common category in Nigeria in 4Q10 was Misc. Potentially Unwanted Software, which affected 21.2 percent of all cleaned computers, up from 19.3 percent in 3Q10.
- The third most common category in Nigeria in 4Q10 was Misc. Trojans, which affected 20.1 percent of all cleaned computers, up from 18.8 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Nigeria in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Vobfus | 22.6% |
| 2 | Win32/Rimecud | 22.4% |
| 3 | Win32/Autorun | 18.2% |
| 4 | Win32/Conficker | 10.3% |
| 5 | Win32/Sality | 8.8% |
| 6 | CplLnk | 6.8% |
| 7 | Win32/Virut | 6.1% |
| 8 | Win32/Zwangi | 5.4% |
| 9 | Win32/ClickPotato | 4.4% |
| 10 | Win32/Renos | 4.3% |

- The most common threat family in Nigeria in 4Q10 was Win32/Vobfus, which affected 22.6 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The second most common threat family in Nigeria in 4Q10 was Win32/Rimecud, which affected 22.4 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Nigeria in 4Q10 was Win32/Autorun, which affected 18.2 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common threat family in Nigeria in 4Q10 was Win32/Conficker, which affected 10.3 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

# Norway

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

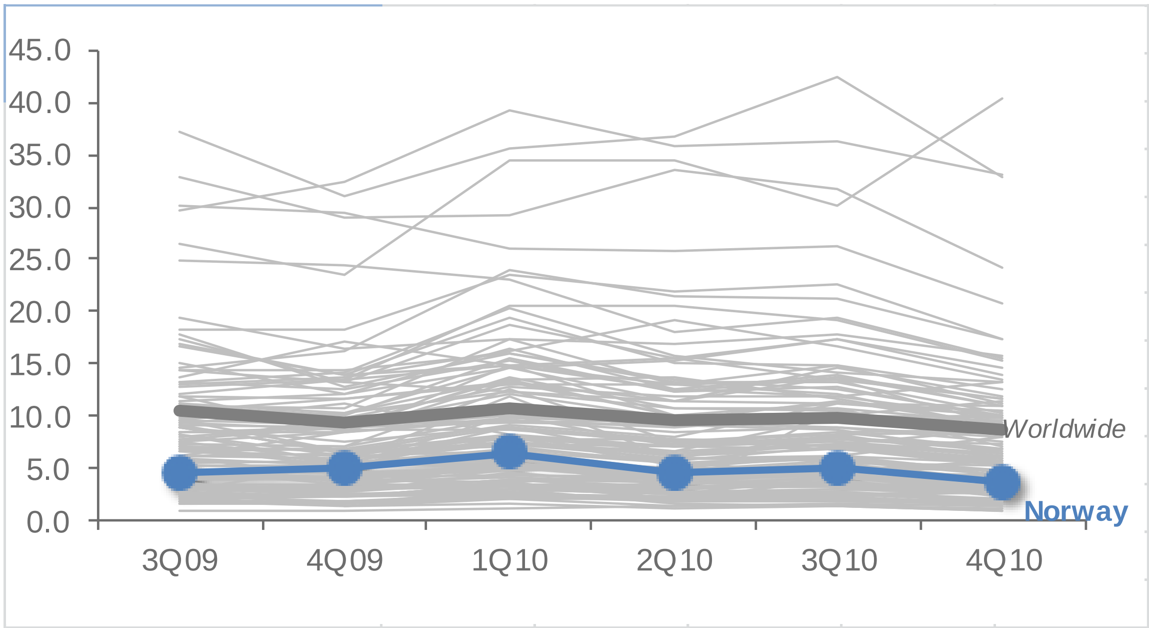
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Norway in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Norway and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 6.6 | 4.7 | 5.0 | 3.8 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.25 | | 0.22 | |
| Malware hosting sites per 1000 hosts | 0.34 | | 0.22 | |
| Percentage of sites hosting drive-by downloads | 0.185% | 0.044% | 0.049% | |

## Infection Trends (CCM)

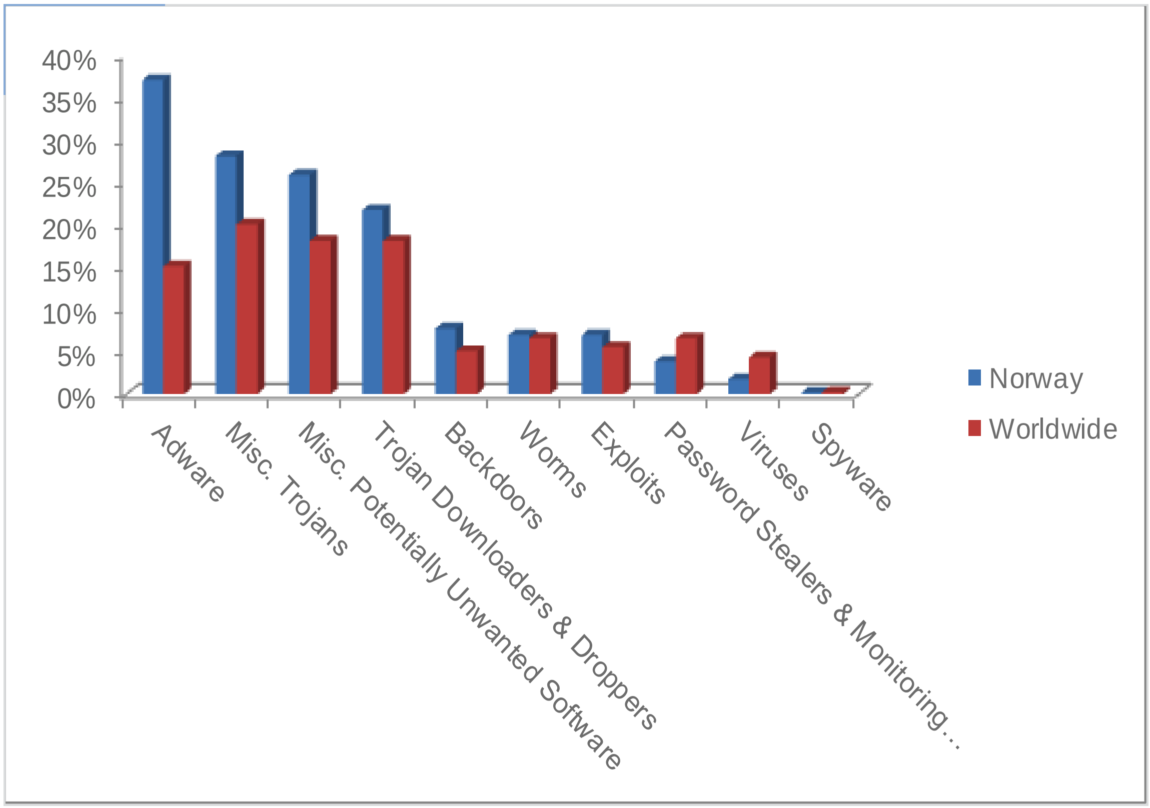
The MSRT detected malware on 3.8 of every 1,000 computers scanned in Norway in 4Q10 (a CCM score of 3.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Norway over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Norway and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Norway in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Norway in 4Q10 was Adware, which affected 37.0 percent of all cleaned computers, up from 30.7 percent in 3Q10.
- The second most common category in Norway in 4Q10 was Misc. Trojans, which affected 28.1 percent of all cleaned computers, down from 29.4 percent in 3Q10.
- The third most common category in Norway in 4Q10 was Misc. Potentially Unwanted Software, which affected 25.8 percent of all cleaned computers, down from 28.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Norway in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 19.2% |
| 2 | Win32/ClickPotato | 8.9% |
| 3 | Win32/Renos | 8.3% |
| 4 | Win32/Zwangi | 8.0% |
| 5 | Win32/Hotbar | 6.7% |
| 6 | Win32/FakeSpypro | 4.9% |
| 7 | ASX/Wimad | 4.5% |
| 8 | Win32/Keygen | 4.0% |
| 9 | Win32/IRCbot | 3.9% |
| 10 | Java/CVE-2009-3867 | 3.7% |

- The most common threat family in Norway in 4Q10 was JS/Pornpop, which affected 19.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Norway in 4Q10 was Win32/ClickPotato, which affected 8.9 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user’s browsing habits.
- The third most common threat family in Norway in 4Q10 was Win32/Renos, which affected 8.3 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.
- The fourth most common threat family in Norway in 4Q10 was Win32/Zwangi, which affected 8.0 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Oman

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

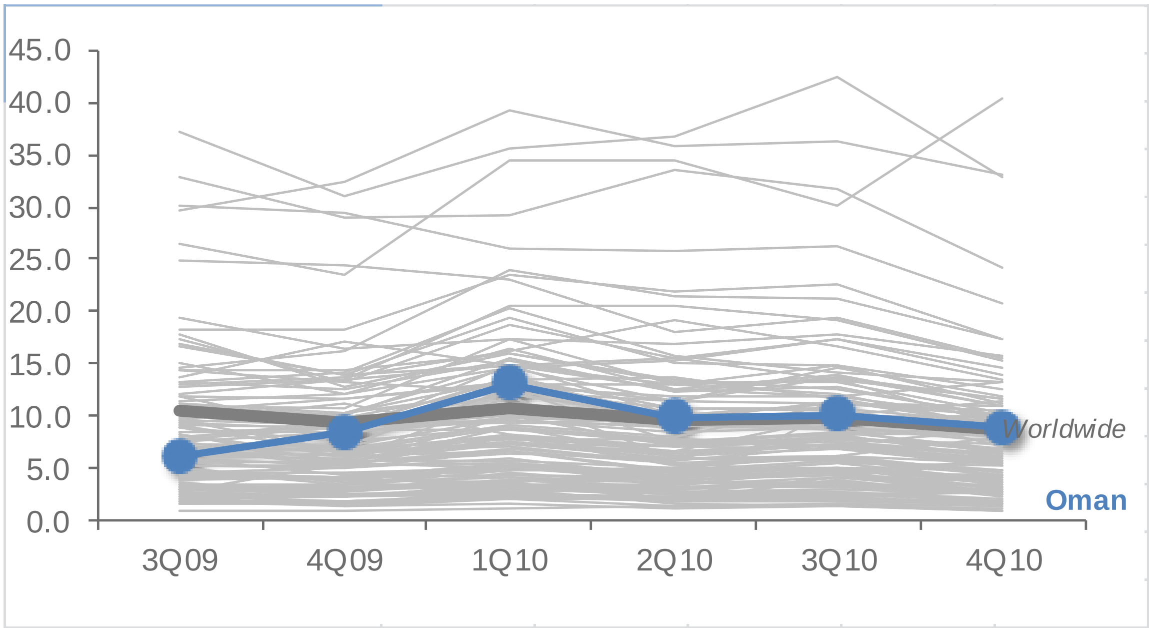
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Oman in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Oman and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 13.2 | 10.0 | 10.3 | 9.0 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.21 | | 0.84 | |
| Malware hosting sites per 1000 hosts | | | 0.42 | |
| Percentage of sites hosting drive-by downloads | 0.000% | | | |

## Infection Trends (CCM)

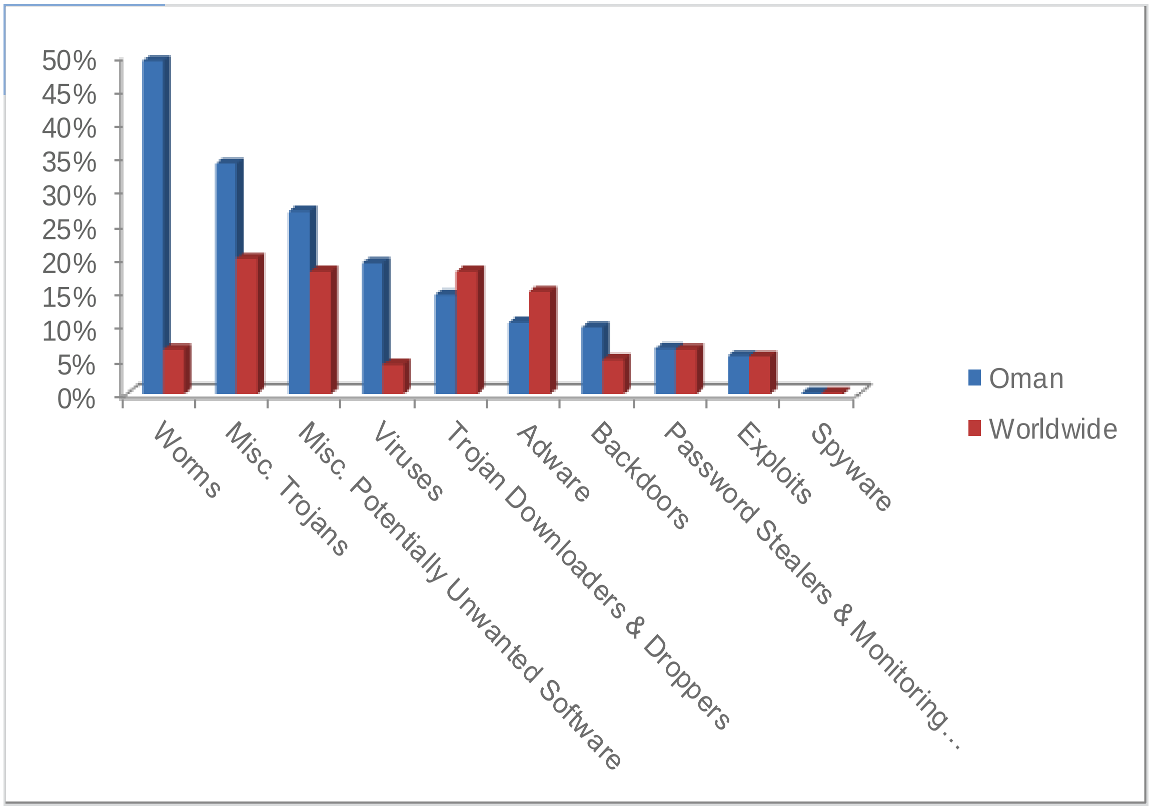
The MSRT detected malware on 9.0 of every 1,000 computers scanned in Oman in 4Q10 (a CCM score of 9.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Oman over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Oman and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Oman in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Oman in 4Q10 was Worms, which affected 49.1 percent of all cleaned computers, up from 45.3 percent in 3Q10.
- The second most common category in Oman in 4Q10 was Misc. Trojans, which affected 34.0 percent of all cleaned computers, up from 29.8 percent in 3Q10.
- The third most common category in Oman in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.0 percent of all cleaned computers, up from 22.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Oman in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 23.2% |
| 2 | Win32/Vobfus | 20.1% |
| 3 | Win32/Rimecud | 17.6% |
| 4 | Win32/Sality | 12.7% |
| 5 | Win32/Agent | 11.5% |
| 6 | Win32/Renos | 6.7% |
| 7 | Win32/Virut | 6.3% |
| 8 | Win32/Mabezat | 5.1% |
| 9 | Win32/Zwangi | 4.3% |
| 10 | Win32/Hamweq | 4.2% |

- The most common threat family in Oman in 4Q10 was Win32/Autorun, which affected 23.2 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Oman in 4Q10 was Win32/Vobfus, which affected 20.1 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The third most common threat family in Oman in 4Q10 was Win32/Rimecud, which affected 17.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Oman in 4Q10 was Win32/Sality, which affected 12.7 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Pakistan

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

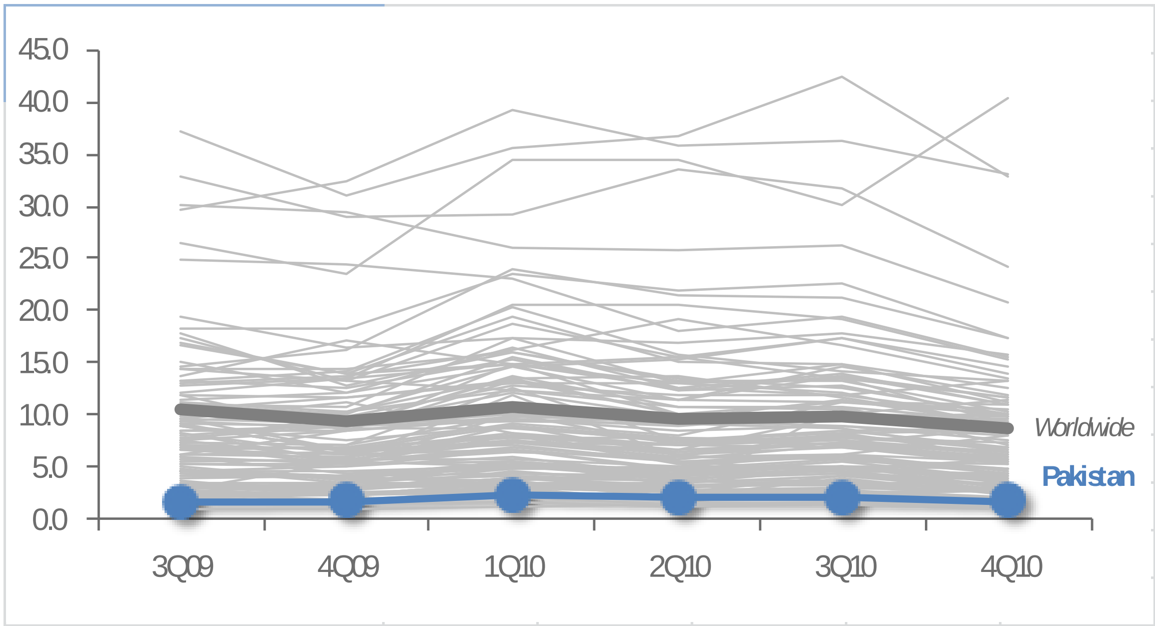
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Pakistan in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Pakistan and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">2.4</td><td colspan="3">2.1</td><td colspan="3">2.1</td><td colspan="3">1.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.54</td><td colspan="6">0.28</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">3.46</td><td colspan="6">1.86</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.415%</td><td colspan="4">0.341%</td><td colspan="4">0.335%</td></tr>
</table>

## Infection Trends (CCM)

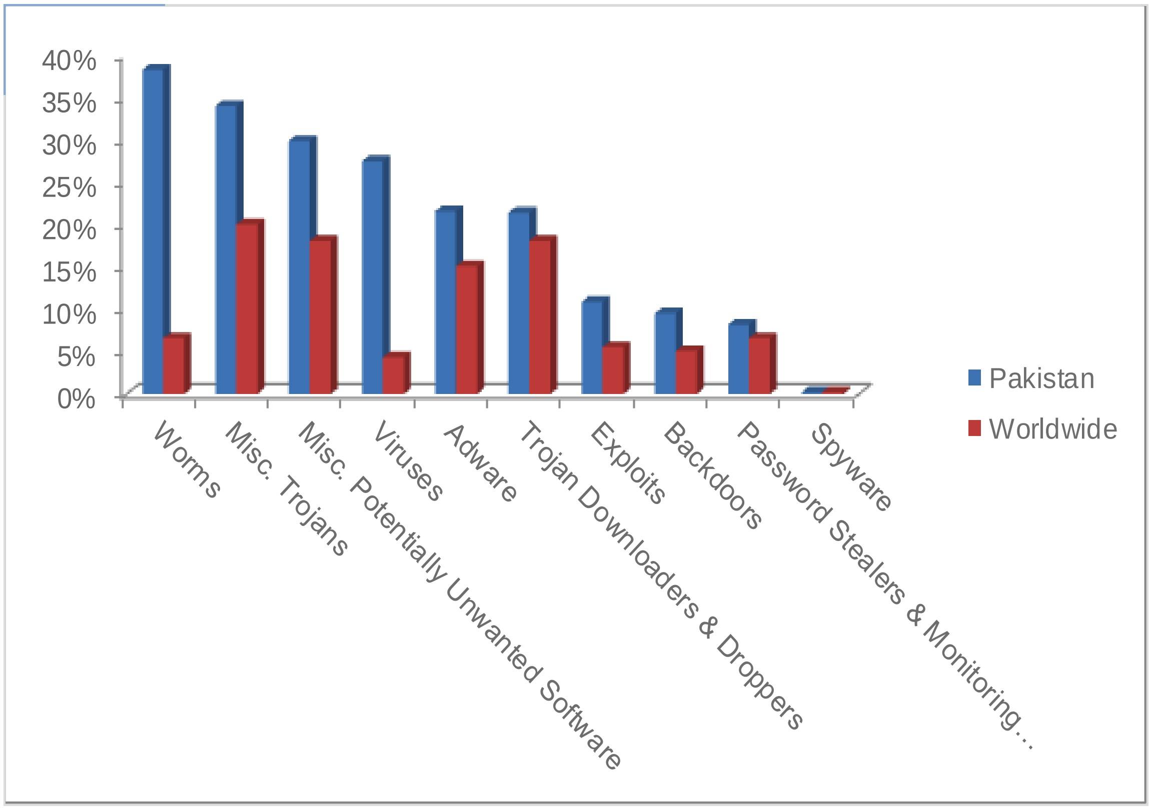
The MSRT detected malware on 1.8 of every 1,000 computers scanned in Pakistan in 4Q10 (a CCM score of 1.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Pakistan over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Pakistan and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Pakistan in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Pakistan in 4Q10 was Worms, which affected 38.3 percent of all cleaned computers, down from 41.4 percent in 3Q10.
- The second most common category in Pakistan in 4Q10 was Misc. Trojans, which affected 34.0 percent of all cleaned computers, up from 33.2 percent in 3Q10.
- The third most common category in Pakistan in 4Q10 was Misc. Potentially Unwanted Software, which affected 29.9 percent of all cleaned computers, up from 26.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Pakistan in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 22.5% |
| 2 | Win32/Rimecud | 16.6% |
| 3 | Win32/Sality | 12.5% |
| 4 | JS/Pornpop | 12.3% |
| 5 | Win32/Virut | 11.0% |
| 6 | Win32/Chir | 10.7% |
| 7 | Win32/Conficker | 10.2% |
| 8 | Win32/Renos | 7.2% |
| 9 | Win32/ClickPotato | 6.1% |
| 10 | CplLnk | 5.8% |

- The most common threat family in Pakistan in 4Q10 was Win32/Autorun, which affected 22.5 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Pakistan in 4Q10 was Win32/Rimecud, which affected 16.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Pakistan in 4Q10 was Win32/Sality, which affected 12.5 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Pakistan in 4Q10 was JS/Pornpop, which affected 12.3 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Palestinian Authority

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

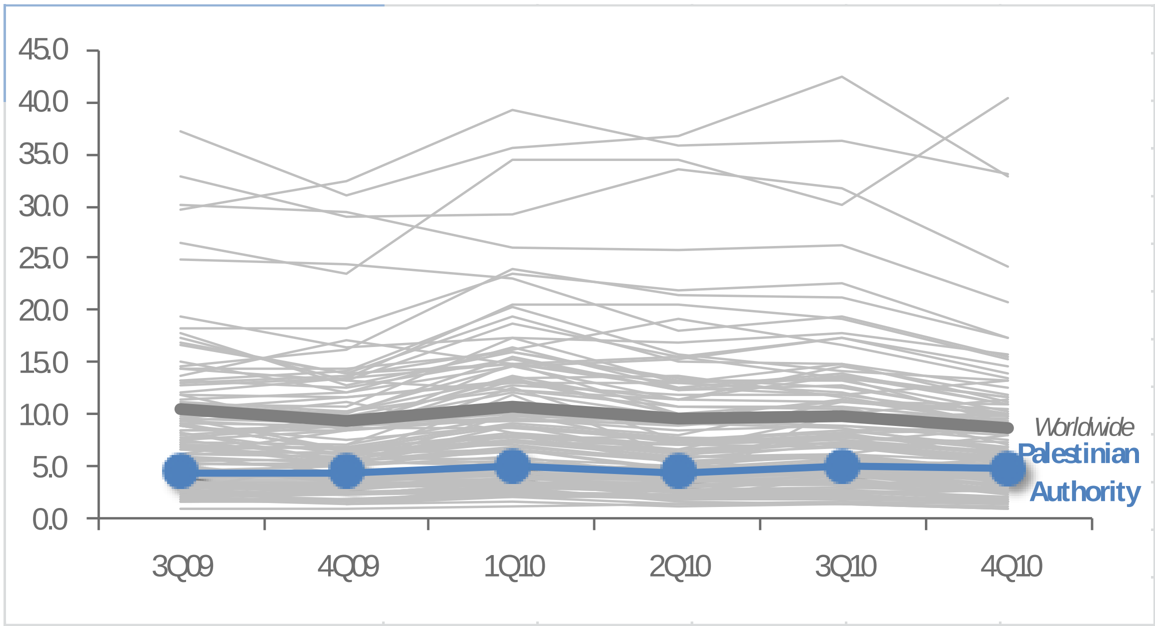
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Palestinian Authority in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Palestinian Authority and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">5.1</td><td colspan="3">4.5</td><td colspan="3">5.0</td><td colspan="3">4.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6"></td><td colspan="6"></td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6"></td><td colspan="6"></td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">1.437%</td><td colspan="4">0.694%</td><td colspan="4">0.678%</td></tr>
</table>

## Infection Trends (CCM)

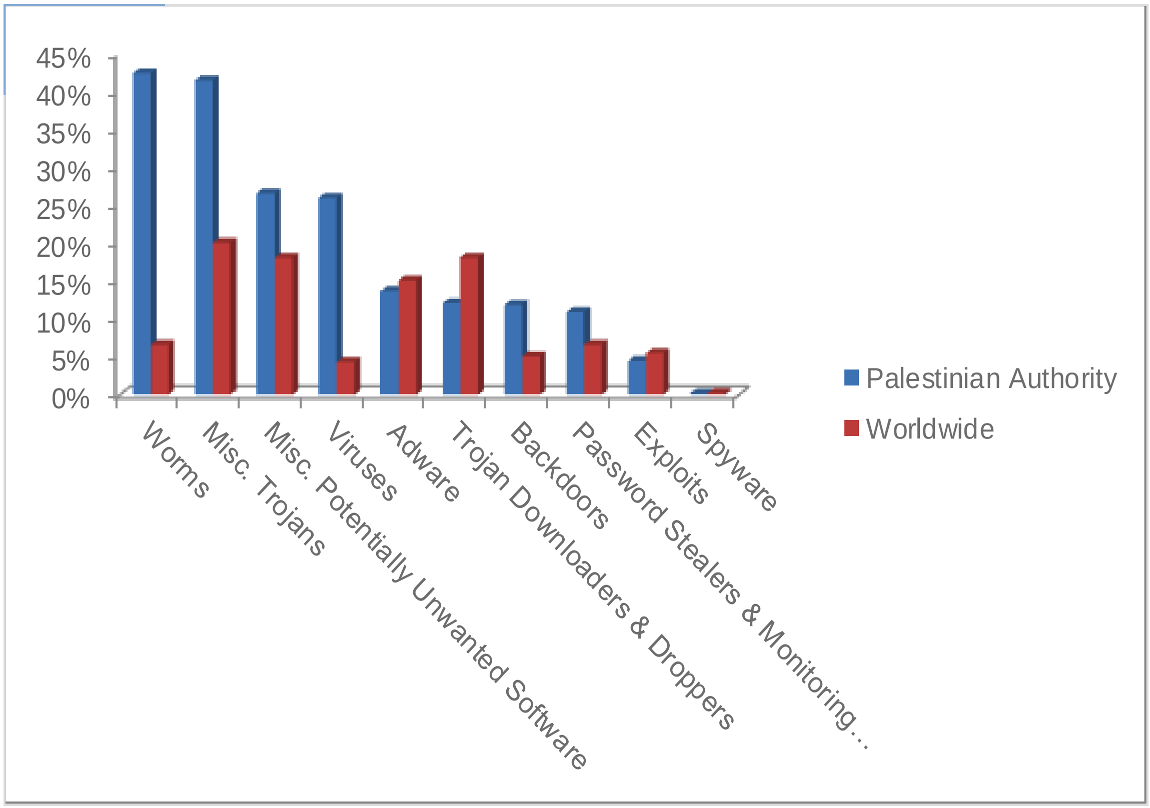
The MSRT detected malware on 4.8 of every 1,000 computers scanned in Palestinian Authority in 4Q10 (a CCM score of 4.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Palestinian Authority over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Palestinian Authority and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Palestinian Authority in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Palestinian Authority in 4Q10 was Worms, which affected 42.4 percent of all cleaned computers, down from 43.4 percent in 3Q10.
- The second most common category in Palestinian Authority in 4Q10 was Misc. Trojans, which affected 41.4 percent of all cleaned computers, up from 37.5 percent in 3Q10.
- The third most common category in Palestinian Authority in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.5 percent of all cleaned computers, up from 23.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Palestinian Authority in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Sality | 28.7% |
| 2 | Win32/Autorun | 20.5% |
| 3 | Win32/Rimecud | 14.3% |
| 4 | Win32/Taterf | 10.1% |
| 5 | Win32/Agent | 9.8% |
| 6 | JS/Pornpop | 9.5% |
| 7 | Win32/Frethog | 6.8% |
| 8 | Win32/Vobfus | 6.5% |
| 9 | Win32/FlyAgent | 6.2% |
| 10 | Win32/Conficker | 5.7% |

- The most common threat family in Palestinian Authority in 4Q10 was Win32/Sality, which affected 28.7 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

- The second most common threat family in Palestinian Authority in 4Q10 was Win32/Autorun, which affected 20.5 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

- The third most common threat family in Palestinian Authority in 4Q10 was Win32/Rimecud, which affected 14.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

- The fourth most common threat family in Palestinian Authority in 4Q10 was Win32/Taterf, which affected 10.1 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Panama

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

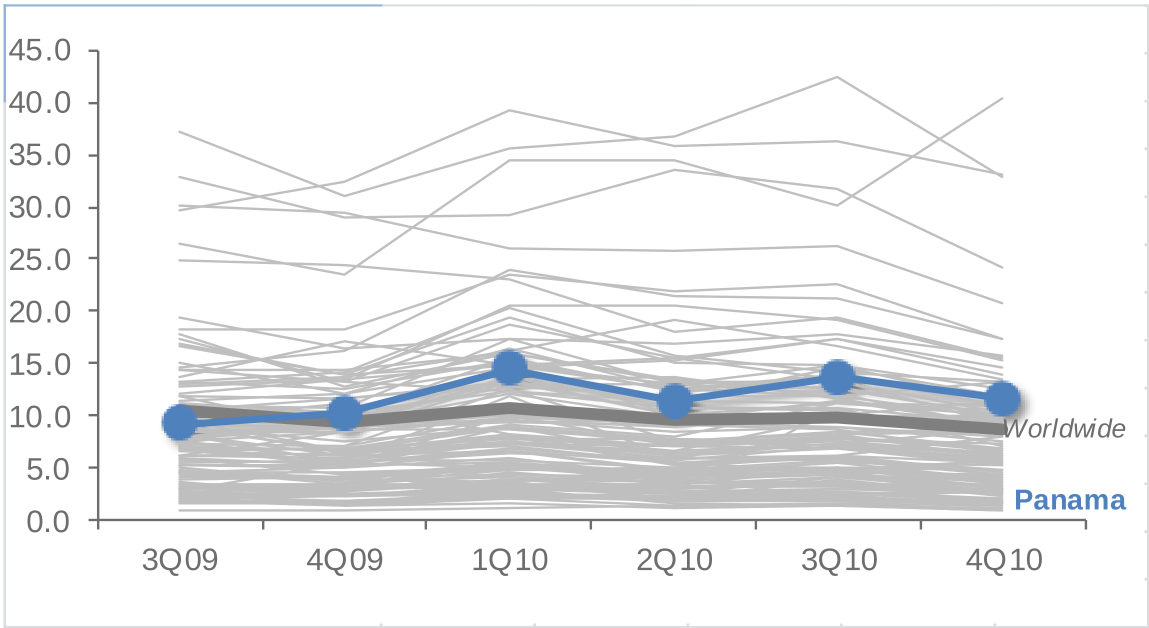
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Panama in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Panama and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">14.5</td><td colspan="3">11.5</td><td colspan="3">13.6</td><td colspan="3">11.7</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">16.67</td><td colspan="6">112.75</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">37.54</td><td colspan="6">41.61</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.000%</td><td colspan="4">0.154%</td><td colspan="4">0.187%</td></tr>
</table>

## Infection Trends (CCM)

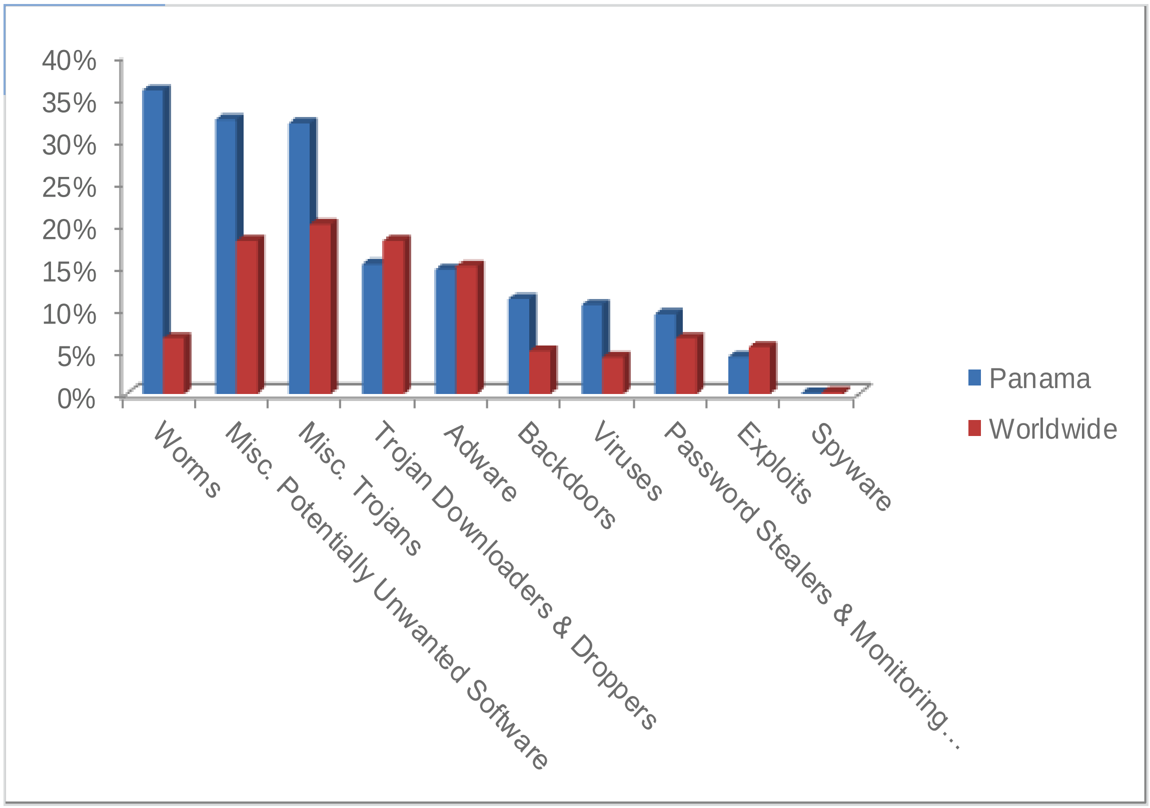
The MSRT detected malware on 11.7 of every 1,000 computers scanned in Panama in 4Q10 (a CCM score of 11.7, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Panama over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Panama and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Panama in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Panama in 4Q10 was Worms, which affected 35.8 percent of all cleaned computers, down from 44.5 percent in 3Q10.
- The second most common category in Panama in 4Q10 was Misc. Potentially Unwanted Software, which affected 32.4 percent of all cleaned computers, up from 29.6 percent in 3Q10.
- The third most common category in Panama in 4Q10 was Misc. Trojans, which affected 31.9 percent of all cleaned computers, up from 26.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Panama in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 19.8% |
| 2 | Win32/Autorun | 16.5% |
| 3 | Win32/Vobfus | 12.6% |
| 4 | Win32/Sality | 10.3% |
| 5 | Win32/IRCbot | 6.8% |
| 6 | Win32/Conficker | 6.5% |
| 7 | JS/Pornpop | 6.2% |
| 8 | Win32/Zwangi | 5.3% |
| 9 | Win32/Renos | 5.1% |
| 10 | Win32/VBInject | 4.4% |

- The most common threat family in Panama in 4Q10 was Win32/Rimecud, which affected 19.8 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Panama in 4Q10 was Win32/Autorun, which affected 16.5 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Panama in 4Q10 was Win32/Vobfus, which affected 12.6 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Panama in 4Q10 was Win32/Sality, which affected 10.3 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Paraguay

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

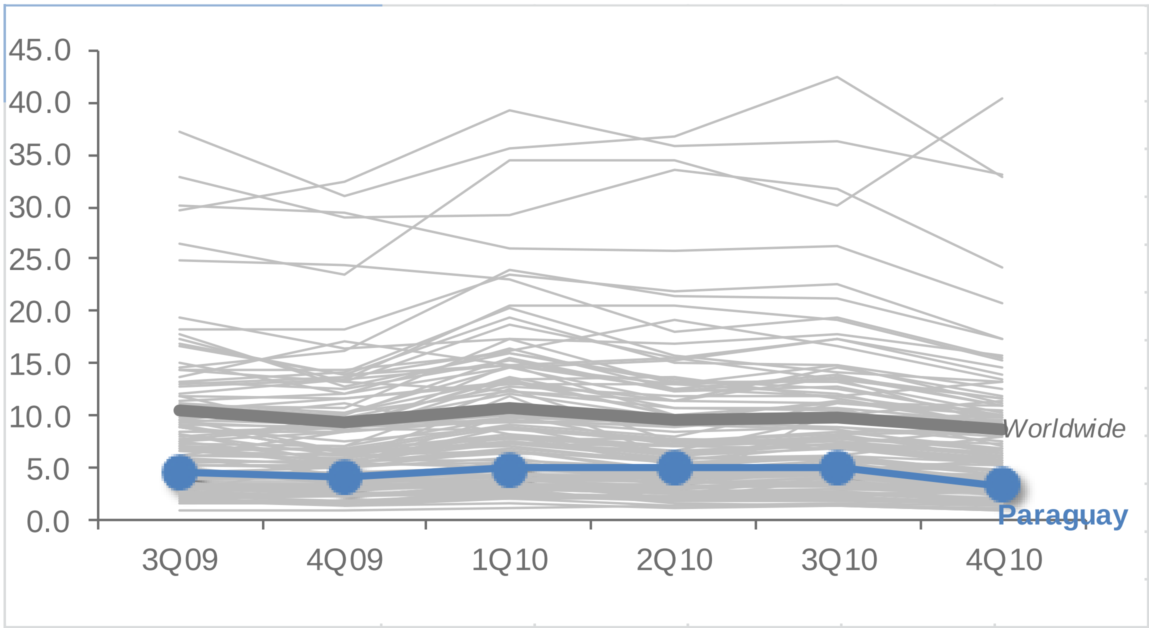
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Paraguay in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Paraguay and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">4.9</td><td colspan="3">5.1</td><td colspan="3">4.9</td><td colspan="3">3.4</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.07</td><td colspan="6">0.15</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">4.57</td><td colspan="6">4.11</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.073%</td><td colspan="4">0.036%</td><td colspan="4">0.119%</td></tr>
</table>

## Infection Trends (CCM)

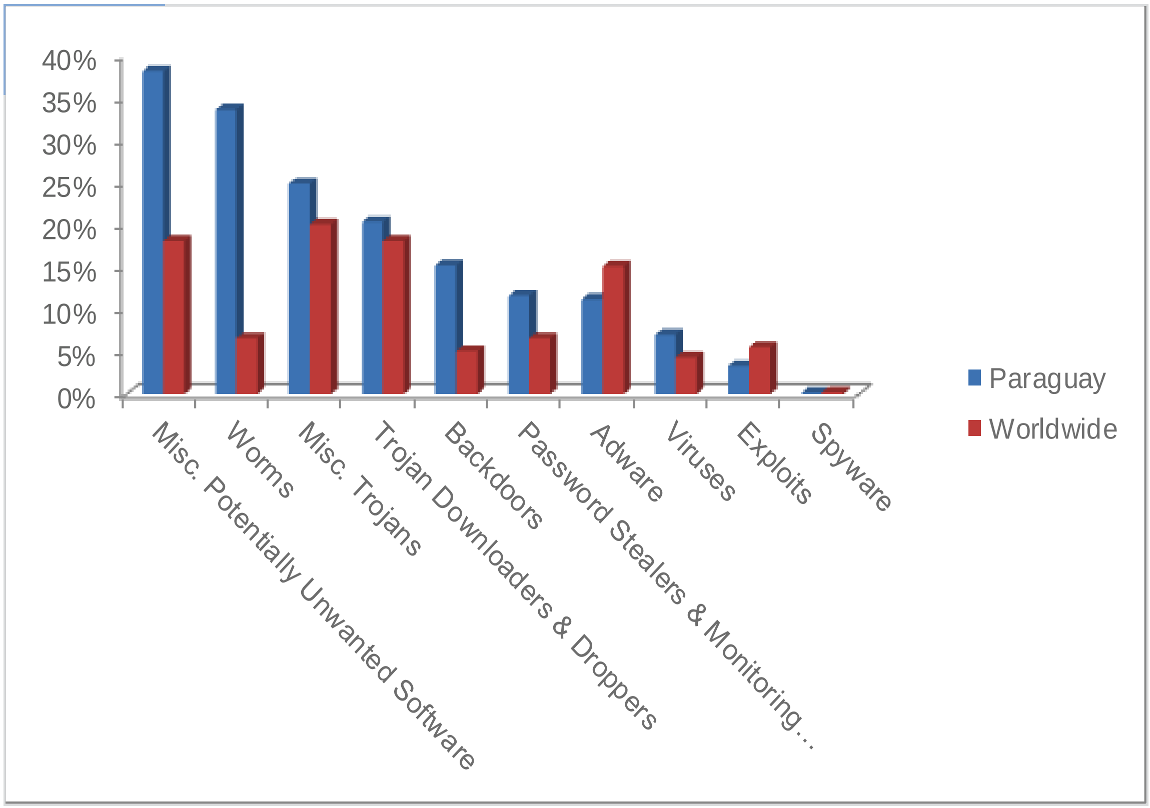
The MSRT detected malware on 3.4 of every 1,000 computers scanned in Paraguay in 4Q10 (a CCM score of 3.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Paraguay over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Paraguay and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Paraguay in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Paraguay in 4Q10 was Misc. Potentially Unwanted Software, which affected 38.1 percent of all cleaned computers, down from 41.8 percent in 3Q10.
- The second most common category in Paraguay in 4Q10 was Worms, which affected 33.5 percent of all cleaned computers, down from 38.7 percent in 3Q10.
- The third most common category in Paraguay in 4Q10 was Misc. Trojans, which affected 24.8 percent of all cleaned computers, up from 21.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Paraguay in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 21.5% |
| 2 | Win32/IRCbot | 11.0% |
| 3 | Win32/Rimecud | 10.0% |
| 4 | Win32/Keygen | 8.0% |
| 5 | Win32/Taterf | 7.9% |
| 6 | Win32/Silly_P2P | 6.7% |
| 7 | JS/Pornpop | 5.7% |
| 8 | Win32/Sality | 5.4% |
| 9 | Win32/Conficker | 4.8% |
| 10 | Win32/Frethog | 4.4% |

- The most common threat family in Paraguay in 4Q10 was Win32/Autorun, which affected 21.5 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Paraguay in 4Q10 was Win32/IRCbot, which affected 11.0 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The third most common threat family in Paraguay in 4Q10 was Win32/Rimecud, which affected 10.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Paraguay in 4Q10 was Win32/Keygen, which affected 8.0 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.

# Peru

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

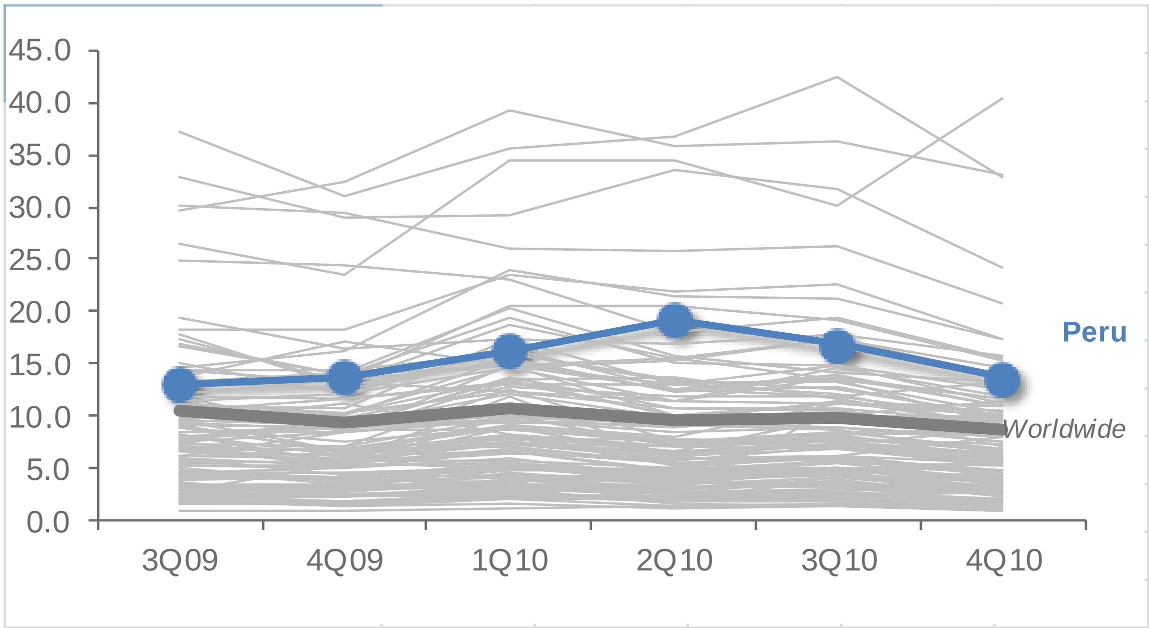
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Peru in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Peru and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">16.2</td><td colspan="3">19.2</td><td colspan="3">16.7</td><td colspan="3">13.5</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.38</td><td colspan="6">0.04</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.03</td><td colspan="6">0.10</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.179%</td><td colspan="4">0.089%</td><td colspan="4">0.119%</td></tr>
</table>

## Infection Trends (CCM)

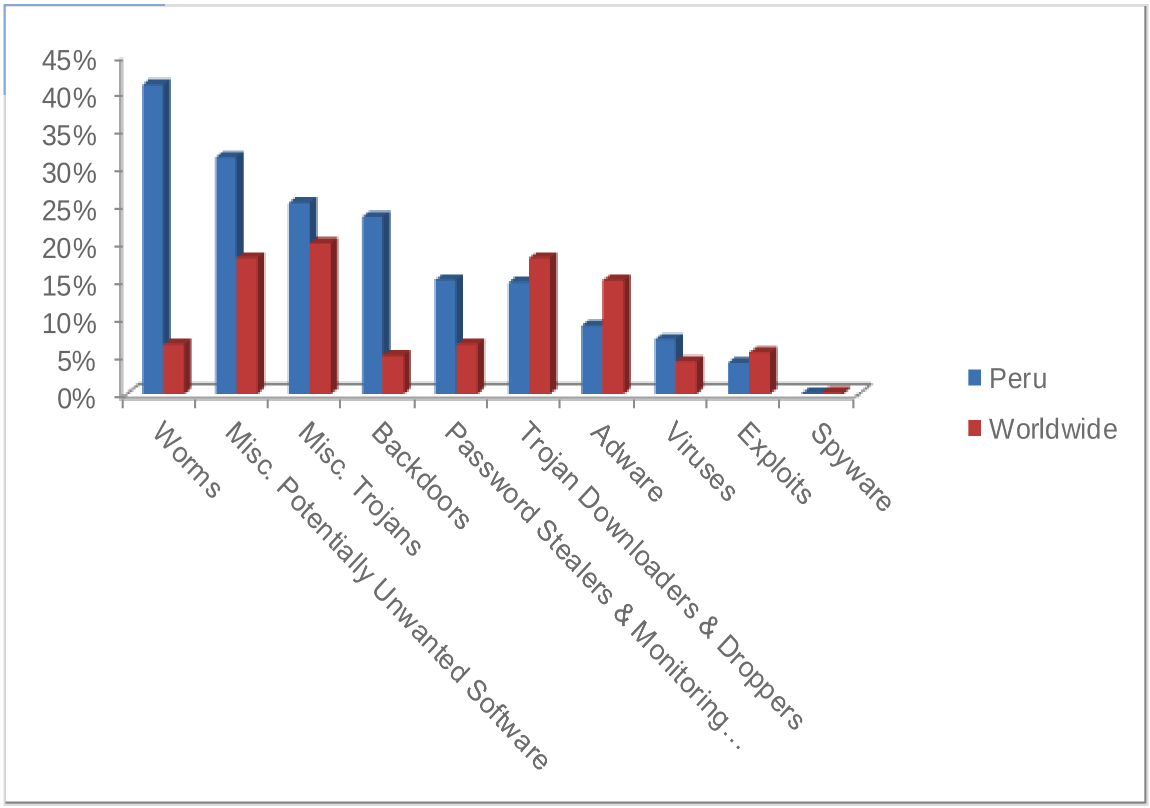
The MSRT detected malware on 13.5 of every 1,000 computers scanned in Peru in 4Q10 (a CCM score of 13.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Peru over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Peru and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Peru in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Peru in 4Q10 was Worms, which affected 41.1 percent of all cleaned computers, down from 53.0 percent in 3Q10.
- The second most common category in Peru in 4Q10 was Misc. Potentially Unwanted Software, which affected 31.4 percent of all cleaned computers, up from 29.1 percent in 3Q10.
- The third most common category in Peru in 4Q10 was Misc. Trojans, which affected 25.4 percent of all cleaned computers, up from 23.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Peru in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/IRCbot | 18.4% |
| 2 | Win32/Autorun | 17.8% |
| 3 | Win32/Taterf | 15.6% |
| 4 | Win32/Rimecud | 15.1% |
| 5 | Win32/Frethog | 10.2% |
| 6 | Win32/Conficker | 7.2% |
| 7 | Win32/Vobfus | 6.9% |
| 8 | Win32/Renos | 6.4% |
| 9 | Win32/Keygen | 5.9% |
| 10 | JS/Pornpop | 5.4% |

- The most common threat family in Peru in 4Q10 was Win32/IRCbot, which affected 18.4 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The second most common threat family in Peru in 4Q10 was Win32/Autorun, which affected 17.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Peru in 4Q10 was Win32/Taterf, which affected 15.6 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Peru in 4Q10 was Win32/Rimecud, which affected 15.1 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Philippines

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

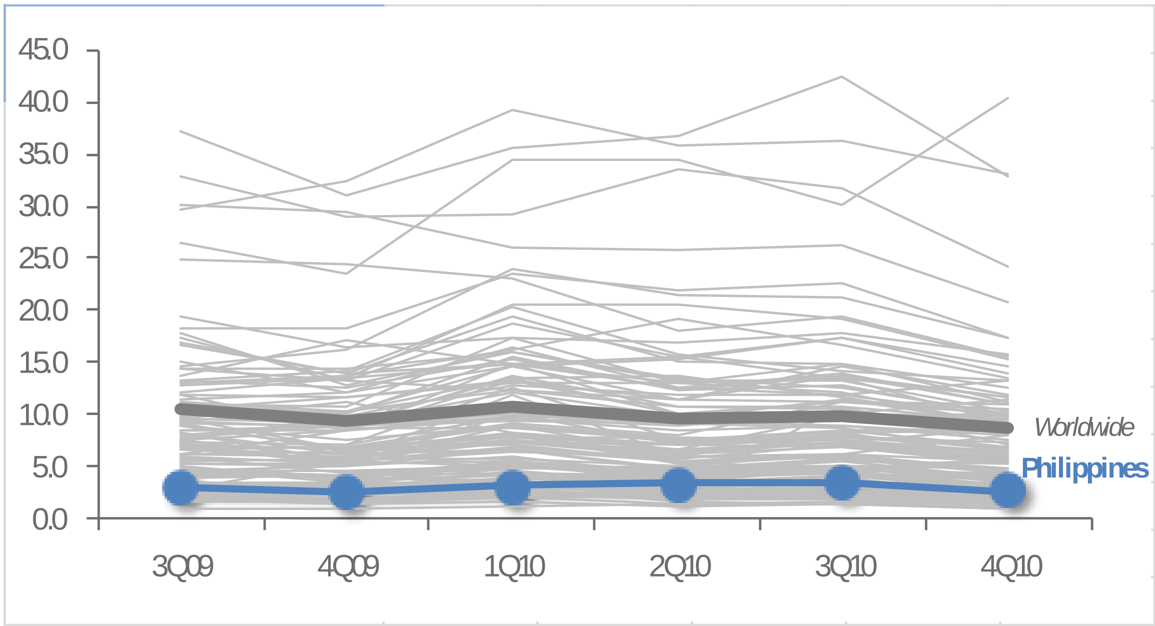
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Philippines in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Philippines and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.0 | 3.3 | 3.5 | 2.8 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 1.12 | | 0.31 | |
| Malware hosting sites per 1000 hosts | 2.92 | | 3.90 | |
| Percentage of sites hosting drive-by downloads | 0.141% | 0.055% | 0.041% | |

## Infection Trends (CCM)

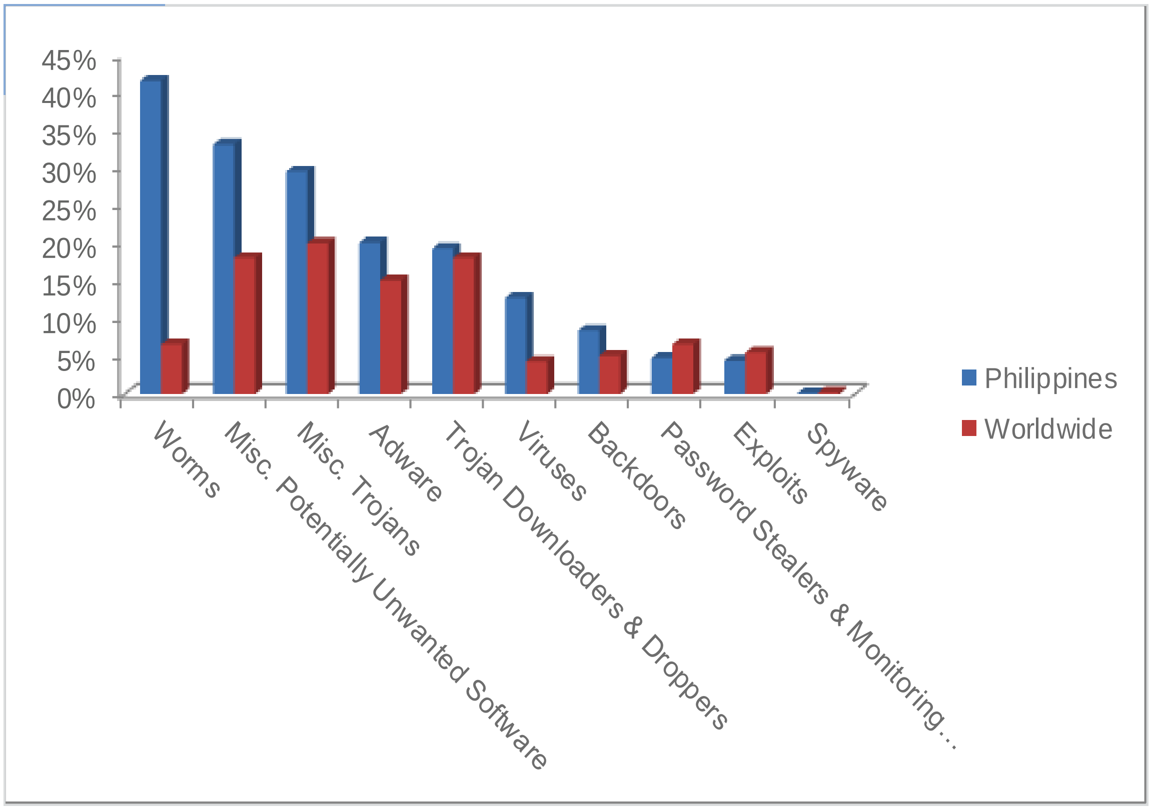
The MSRT detected malware on 2.8 of every 1,000 computers scanned in Philippines in 4Q10 (a CCM score of 2.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Philippines over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Philippines and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Philippines in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Philippines in 4Q10 was Worms, which affected 41.6 percent of all cleaned computers, down from 46.6 percent in 3Q10.
- The second most common category in Philippines in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.1 percent of all cleaned computers, up from 31.2 percent in 3Q10.
- The third most common category in Philippines in 4Q10 was Misc. Trojans, which affected 29.5 percent of all cleaned computers, up from 27.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Philippines in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 22.4% |
| 2 | Win32/Rimecud | 17.3% |
| 3 | Win32/Conficker | 12.6% |
| 4 | Win32/Sality | 10.4% |
| 5 | Win32/Zwangi | 7.3% |
| 6 | Win32/ClickPotato | 6.9% |
| 7 | Win32/Renos | 6.7% |
| 8 | JS/Pornpop | 6.1% |
| 9 | Win32/Nuqel | 6.1% |
| 10 | Win32/Hotbar | 6.0% |

- The most common threat family in Philippines in 4Q10 was Win32/Autorun, which affected 22.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Philippines in 4Q10 was Win32/Rimecud, which affected 17.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Philippines in 4Q10 was Win32/Conficker, which affected 12.6 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The fourth most common threat family in Philippines in 4Q10 was Win32/Sality, which affected 10.4 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Poland

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

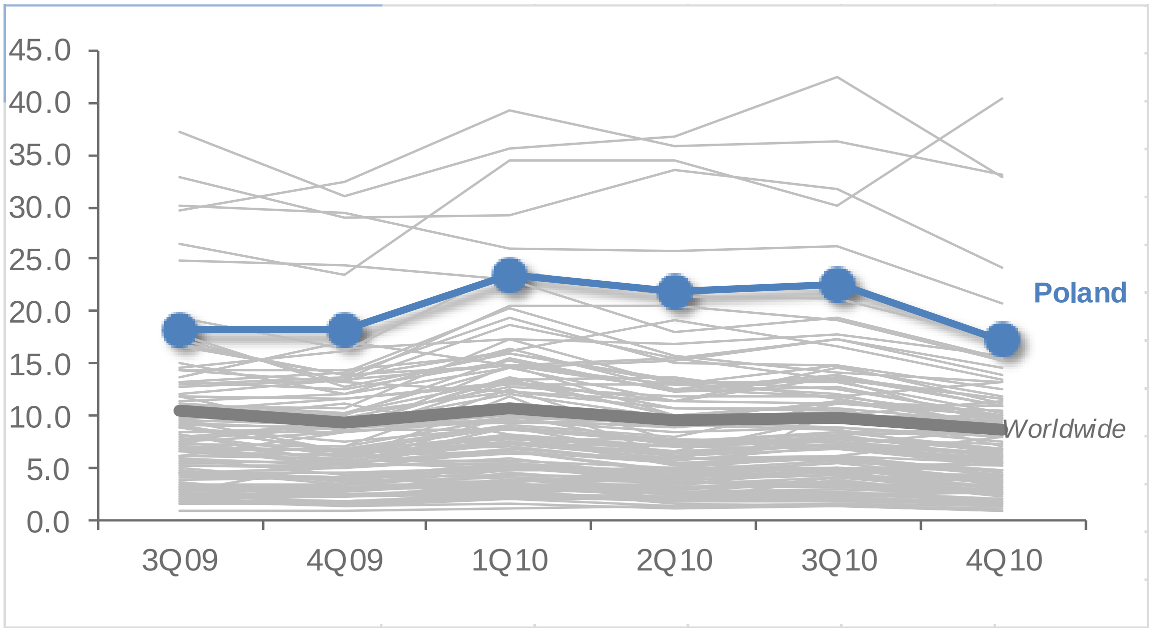
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Poland in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Poland and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 23.6 | 21.8 | 22.6 | 17.3 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.40 | | 0.25 | |
| Malware hosting sites per 1000 hosts | 7.07 | | 1.31 | |
| Percentage of sites hosting drive-by downloads | 0.163% | 0.088% | 0.082% | |

## Infection Trends (CCM)

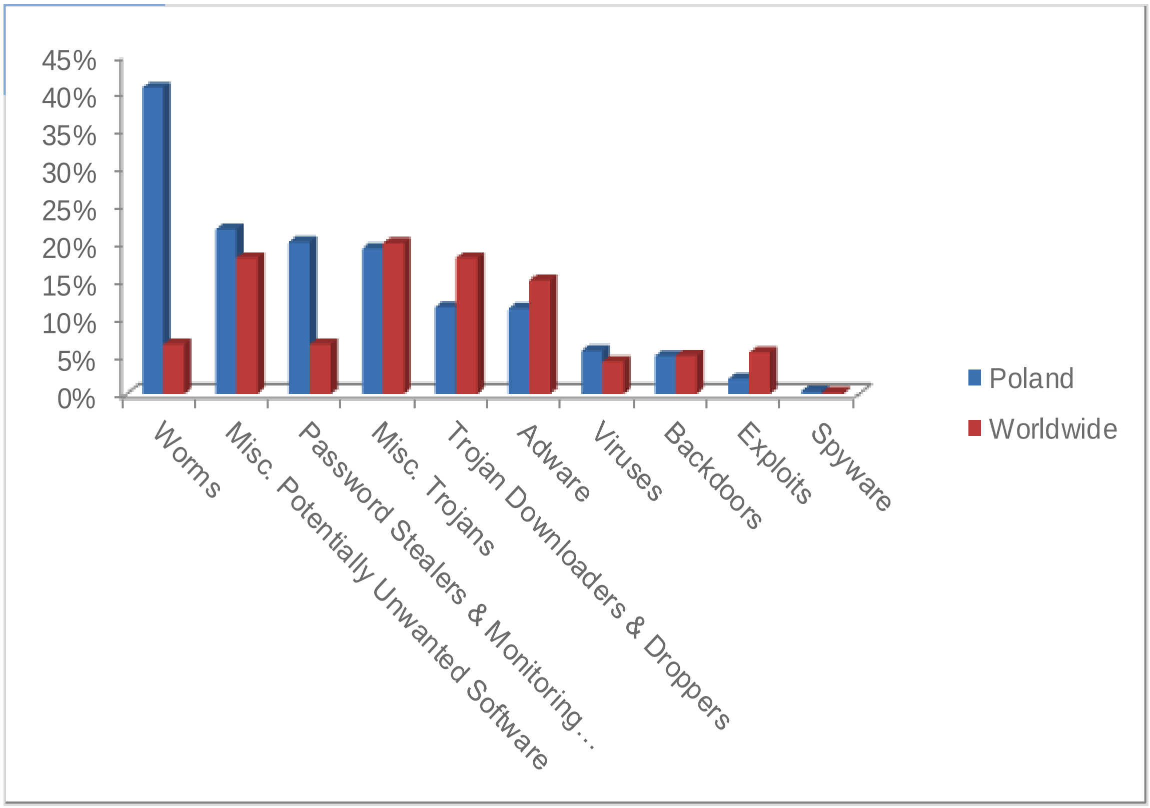
The MSRT detected malware on 17.3 of every 1,000 computers scanned in Poland in 4Q10 (a CCM score of 17.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Poland over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Poland and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Poland in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Poland in 4Q10 was Worms, which affected 40.6 percent of all cleaned computers, down from 46.2 percent in 3Q10.
- The second most common category in Poland in 4Q10 was Misc. Potentially Unwanted Software, which affected 21.8 percent of all cleaned computers, up from 19.6 percent in 3Q10.
- The third most common category in Poland in 4Q10 was Password Stealers & Monitoring Tools, which affected 20.2 percent of all cleaned computers, up from 18.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Poland in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Taterf | 23.9% |
| 2 | Win32/Frethog | 15.9% |
| 3 | Win32/Autorun | 8.8% |
| 4 | Win32/Rimecud | 5.3% |
| 5 | JS/Pornpop | 4.6% |
| 6 | Win32/Vobfus | 4.0% |
| 7 | Win32/Renos | 4.0% |
| 8 | Win32/Conficker | 3.5% |
| 9 | Win32/Sality | 3.5% |
| 10 | Win32/Keygen | 3.4% |

- The most common threat family in Poland in 4Q10 was Win32/Taterf, which affected 23.9 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The second most common threat family in Poland in 4Q10 was Win32/Frethog, which affected 15.9 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.
- The third most common threat family in Poland in 4Q10 was Win32/Autorun, which affected 8.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common threat family in Poland in 4Q10 was Win32/Rimecud, which affected 5.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Portugal

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

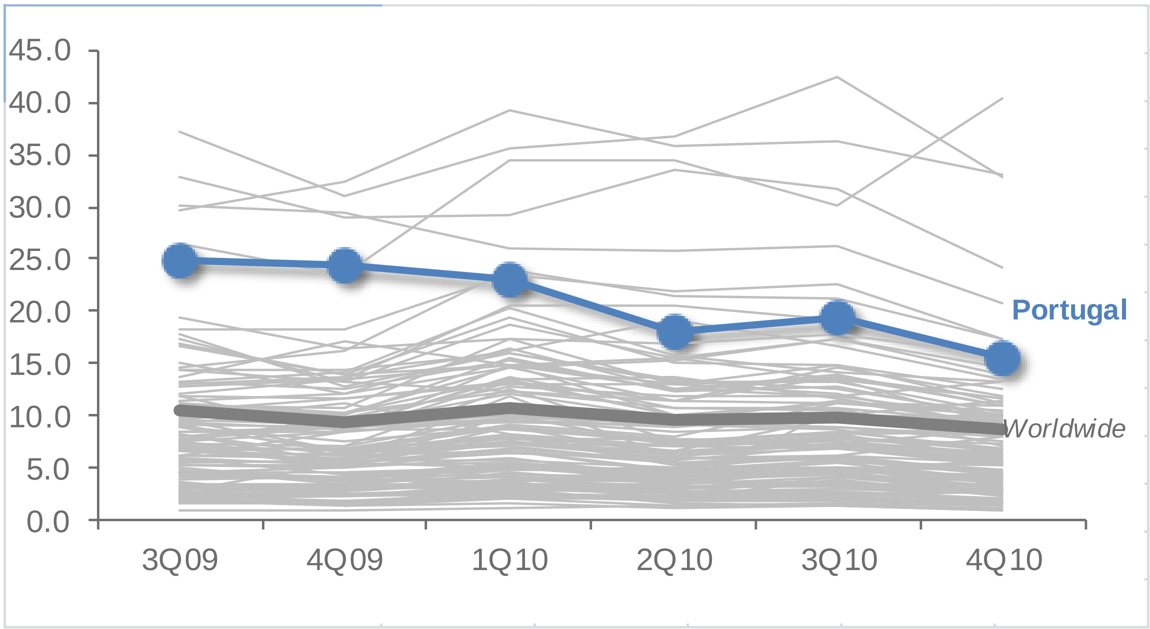
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Portugal in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Portugal and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">23.0</td><td colspan="3">18.1</td><td colspan="3">19.3</td><td colspan="3">15.6</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.23</td><td colspan="6">0.29</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.36</td><td colspan="6">0.25</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.172%</td><td colspan="4">0.080%</td><td colspan="4">0.078%</td></tr>
</table>

## Infection Trends (CCM)

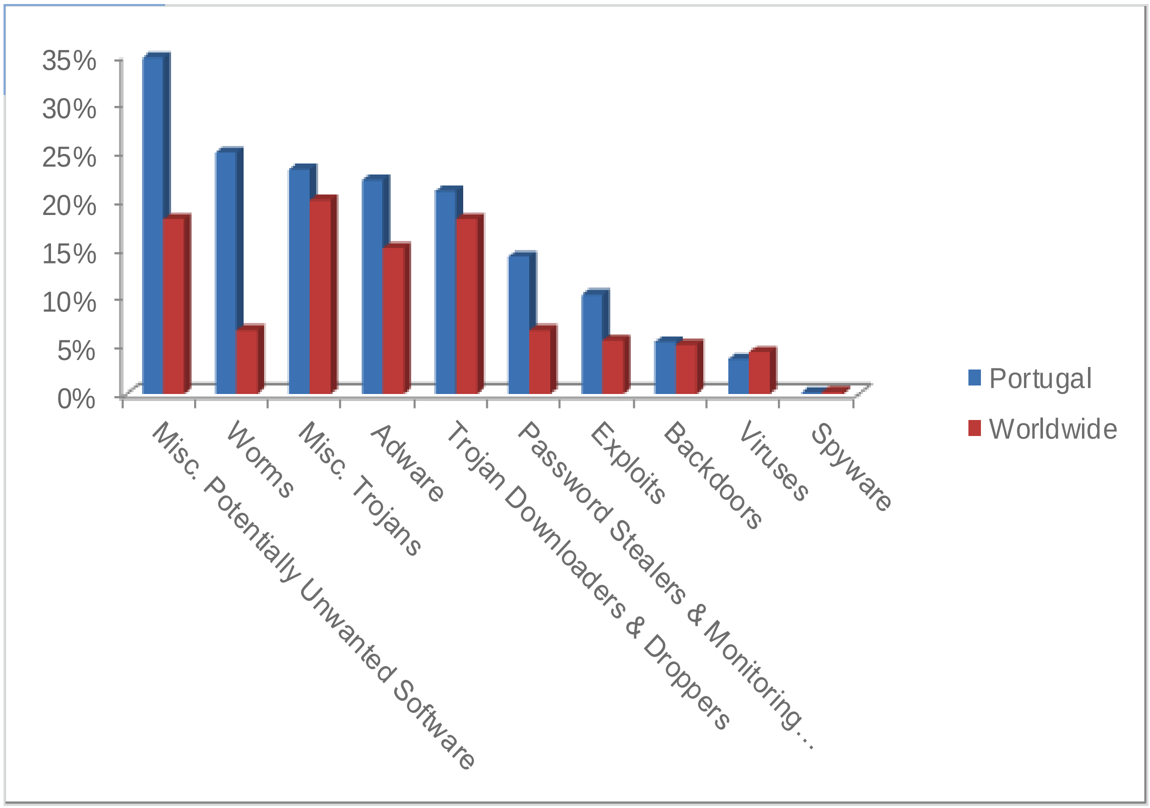
The MSRT detected malware on 15.6 of every 1,000 computers scanned in Portugal in 4Q10 (a CCM score of 15.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Portugal over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Portugal and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Portugal in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Portugal in 4Q10 was Misc. Potentially Unwanted Software, which affected 34.7 percent of all cleaned computers, up from 27.0 percent in 3Q10.
- The second most common category in Portugal in 4Q10 was Worms, which affected 24.9 percent of all cleaned computers, down from 25.5 percent in 3Q10.
- The third most common category in Portugal in 4Q10 was Misc. Trojans, which affected 23.2 percent of all cleaned computers, down from 23.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Portugal in 4Q10.

|  | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 13.9% |
| 2 | JS/Pornpop | 11.7% |
| 3 | Win32/Vobfus | 8.8% |
| 4 | Win32/Zwangi | 6.8% |
| 5 | Win32/Keygen | 6.7% |
| 6 | Win32/Bancos | 6.5% |
| 7 | Win32/ClickPotato | 5.9% |
| 8 | HTML/IframeRef | 5.8% |
| 9 | Win32/Renos | 5.5% |
| 10 | Win32/Banload | 4.3% |

- The most common threat family in Portugal in 4Q10 was Win32/Autorun, which affected 13.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Portugal in 4Q10 was JS/Pornpop, which affected 11.7 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Portugal in 4Q10 was Win32/Vobfus, which affected 8.8 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Portugal in 4Q10 was Win32/Zwangi, which affected 6.8 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Puerto Rico

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

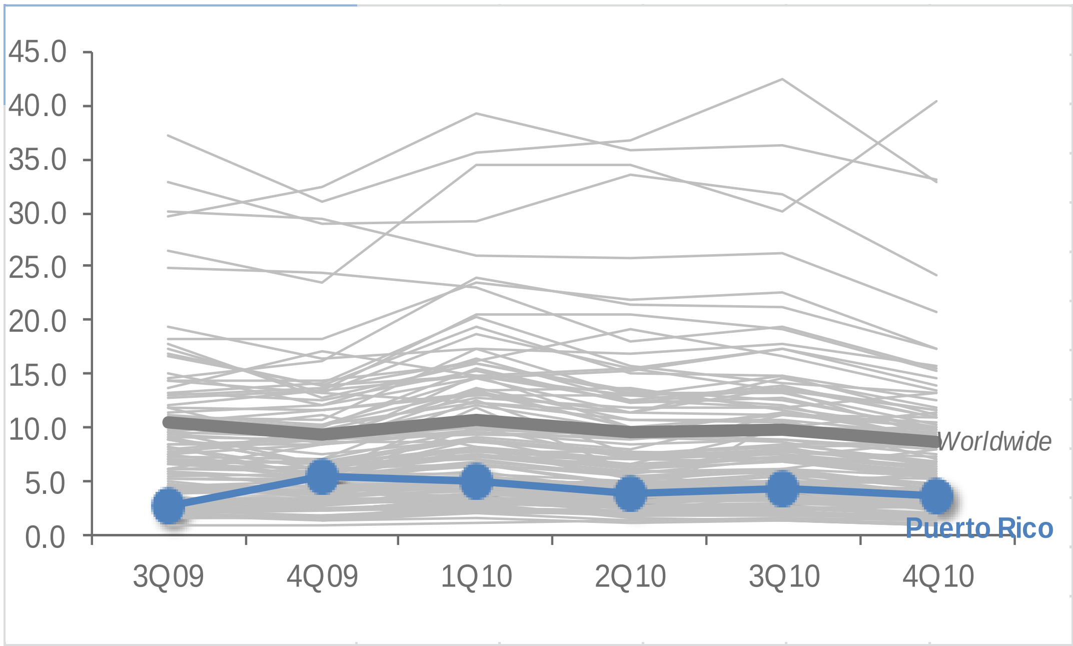
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Puerto Rico in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Puerto Rico and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 5.0 | 4.0 | 4.4 | 3.6 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 225.25 | | | |
| Malware hosting sites per 1000 hosts | 2252.48 | | 86.63 | |
| Percentage of sites hosting drive-by downloads | 0.000% | | | |

## Infection Trends (CCM)

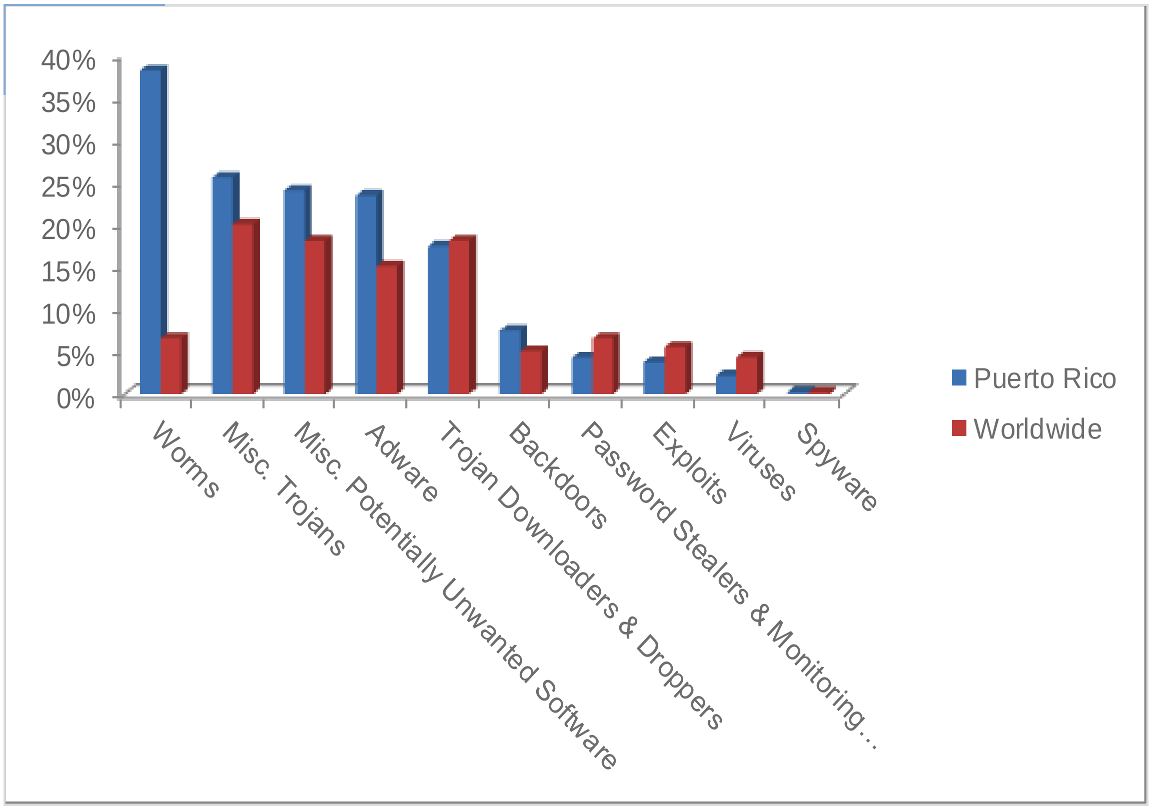
The MSRT detected malware on 3.6 of every 1,000 computers scanned in Puerto Rico in 4Q10 (a CCM score of 3.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Puerto Rico over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Puerto Rico and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Puerto Rico in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Puerto Rico in 4Q10 was Worms, which affected 38.1 percent of all cleaned computers, down from 43.0 percent in 3Q10.
- The second most common category in Puerto Rico in 4Q10 was Misc. Trojans, which affected 25.5 percent of all cleaned computers, up from 23.5 percent in 3Q10.
- The third most common category in Puerto Rico in 4Q10 was Misc. Potentially Unwanted Software, which affected 24.0 percent of all cleaned computers, up from 22.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Puerto Rico in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Vobfus | 17.4% |
| 2 | Win32/Autorun | 13.6% |
| 3 | Win32/Zwangi | 9.0% |
| 4 | Win32/Rimecud | 8.3% |
| 5 | Win32/Renos | 7.8% |
| 6 | JS/Pornpop | 6.5% |
| 7 | Win32/ClickPotato | 6.3% |
| 8 | Win32/Hotbar | 5.9% |
| 9 | Win32/Hamweq | 5.2% |
| 10 | Win32/IRCbot | 4.7% |

- The most common threat family in Puerto Rico in 4Q10 was Win32/Vobfus, which affected 17.4 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The second most common threat family in Puerto Rico in 4Q10 was Win32/Autorun, which affected 13.6 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Puerto Rico in 4Q10 was Win32/Zwangi, which affected 9.0 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in Puerto Rico in 4Q10 was Win32/Rimecud, which affected 8.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Qatar

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

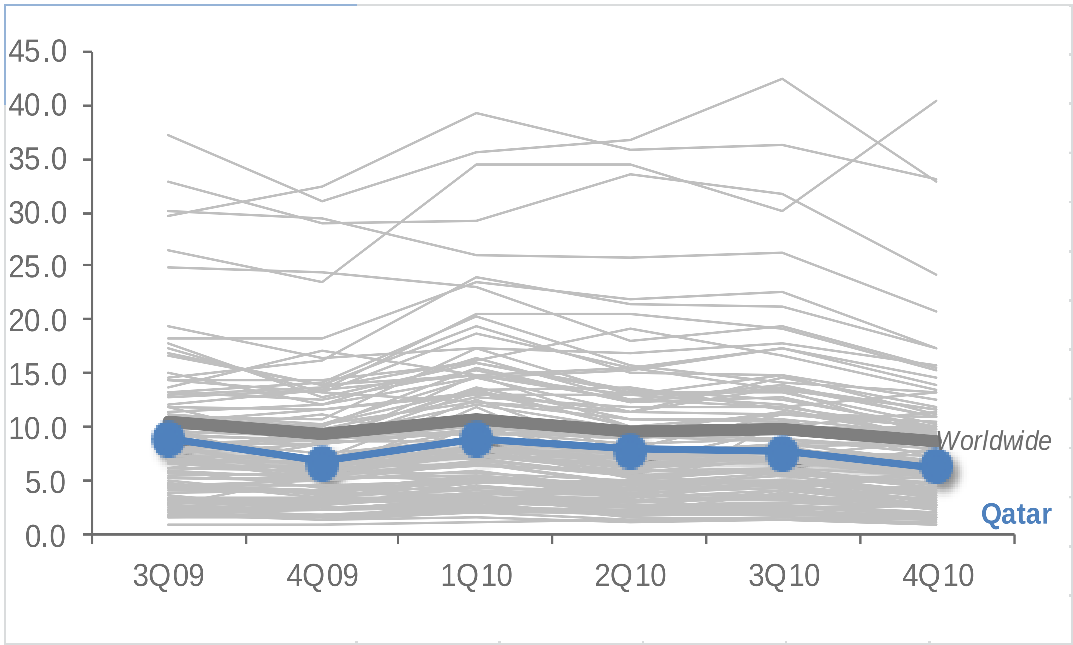
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Qatar in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Qatar and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 8.9 | 7.9 | 7.6 | 6.4 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 1.78 | | | |
| Malware hosting sites per 1000 hosts | 12.43 | | | |
| Percentage of sites hosting drive-by downloads | 0.212% | 0.114% | 0.109% | |

## Infection Trends (CCM)

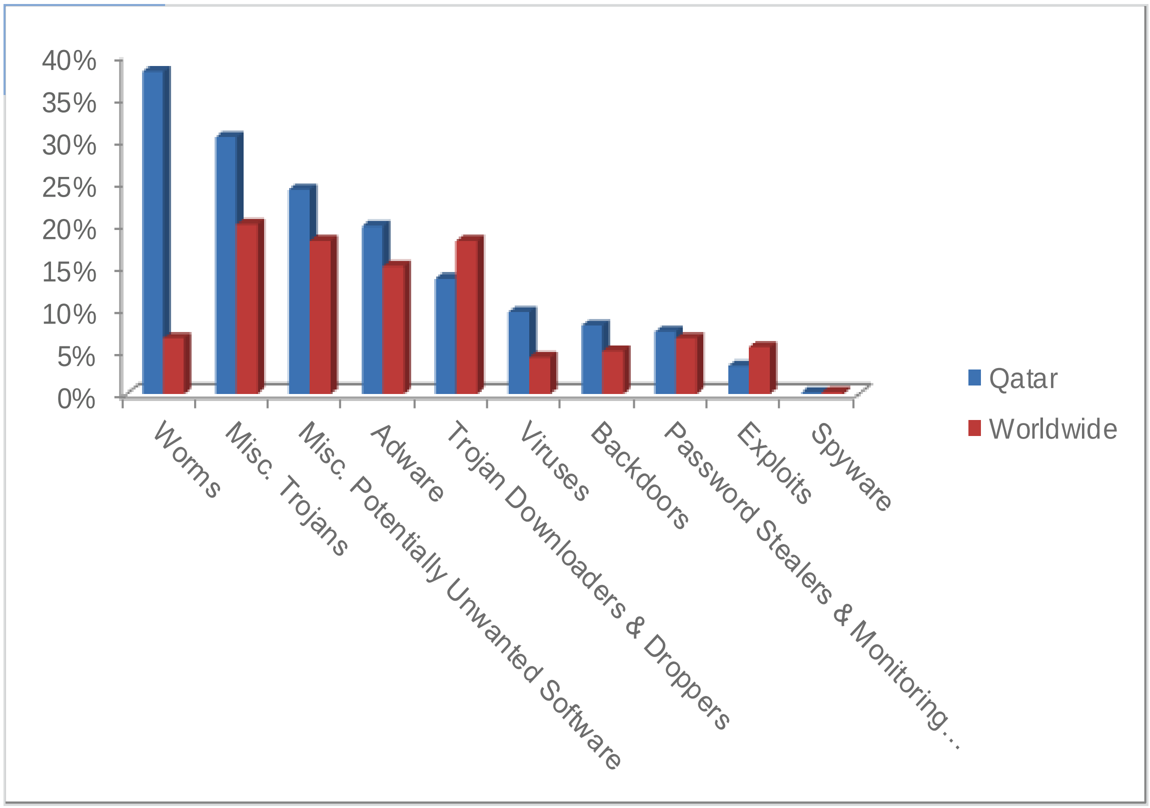
The MSRT detected malware on 6.4 of every 1,000 computers scanned in Qatar in 4Q10 (a CCM score of 6.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Qatar over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Qatar and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Qatar in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Qatar in 4Q10 was Worms, which affected 38.0 percent of all cleaned computers, down from 40.9 percent in 3Q10.
- The second most common category in Qatar in 4Q10 was Misc. Trojans, which affected 30.3 percent of all cleaned computers, up from 27.4 percent in 3Q10.
- The third most common category in Qatar in 4Q10 was Misc. Potentially Unwanted Software, which affected 24.1 percent of all cleaned computers, up from 20.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Qatar in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 14.6% |
| 2 | Win32/Autorun | 14.5% |
| 3 | Win32/ClickPotato | 8.8% |
| 4 | Win32/Zwangi | 8.0% |
| 5 | Win32/Conficker | 7.6% |
| 6 | Win32/Sality | 7.4% |
| 7 | Win32/Agent | 7.0% |
| 8 | Win32/Taterf | 6.0% |
| 9 | Win32/Renos | 5.5% |
| 10 | Win32/Hotbar | 5.1% |

- The most common threat family in Qatar in 4Q10 was Win32/Rimecud, which affected 14.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Qatar in 4Q10 was Win32/Autorun, which affected 14.5 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Qatar in 4Q10 was Win32/ClickPotato, which affected 8.8 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The fourth most common threat family in Qatar in 4Q10 was Win32/Zwangi, which affected 8.0 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Romania

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

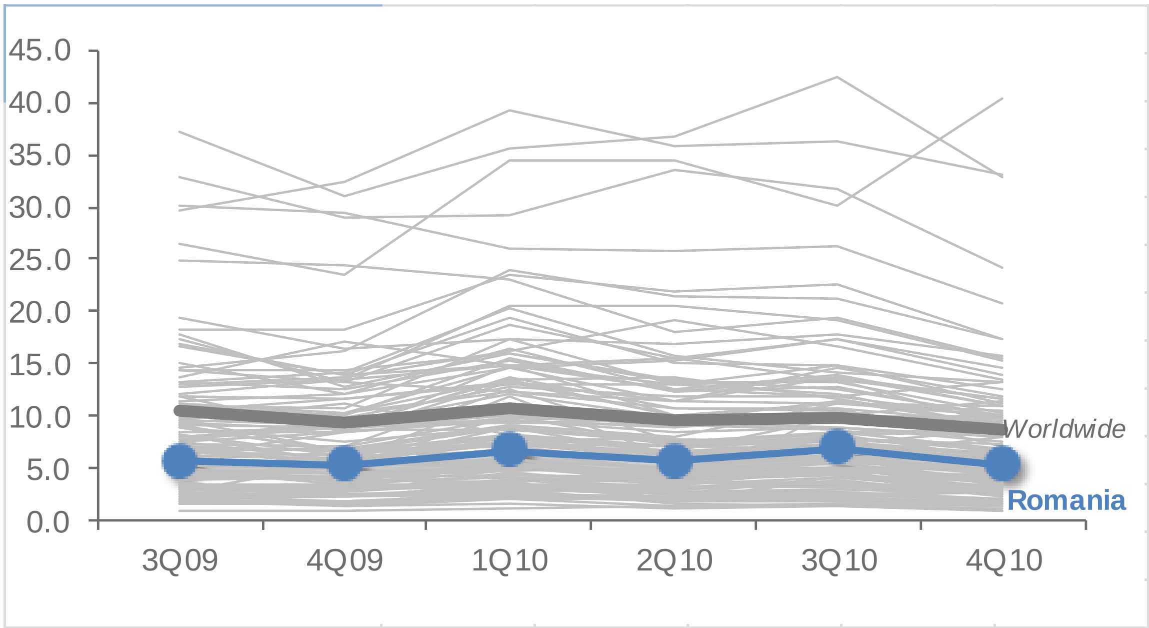
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Romania in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Romania and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">6.8</td><td colspan="3">5.7</td><td colspan="3">7.0</td><td colspan="3">5.4</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.73</td><td colspan="6">0.75</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">2.04</td><td colspan="6">4.92</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.190%</td><td colspan="4">0.124%</td><td colspan="4">0.122%</td></tr>
</table>

## Infection Trends (CCM)

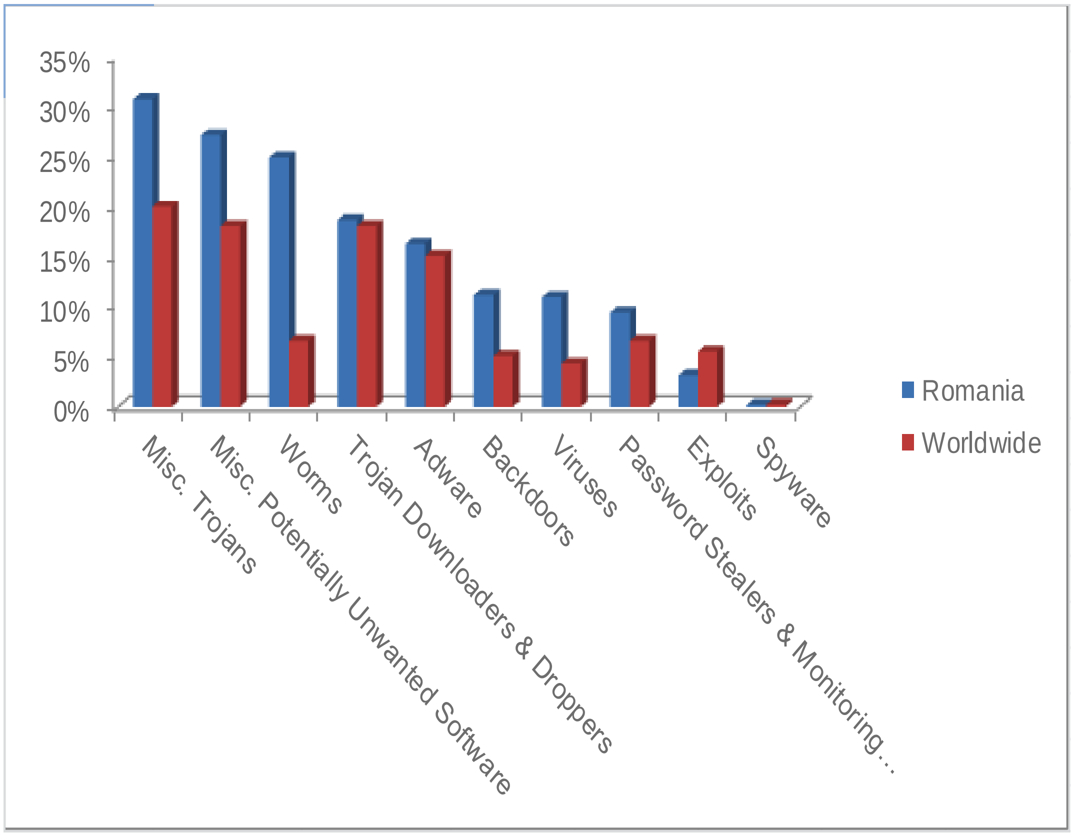
The MSRT detected malware on 5.4 of every 1,000 computers scanned in Romania in 4Q10 (a CCM score of 5.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Romania over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Romania and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Romania in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Romania in 4Q10 was Misc. Trojans, which affected 30.7 percent of all cleaned computers, down from 32.3 percent in 3Q10.
- The second most common category in Romania in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.1 percent of all cleaned computers, down from 30.8 percent in 3Q10.
- The third most common category in Romania in 4Q10 was Worms, which affected 24.9 percent of all cleaned computers, down from 24.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Romania in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 10.8% |
| 2 | Win32/Sality | 8.6% |
| 3 | Win32/Rimecud | 8.1% |
| 4 | JS/Pornpop | 7.8% |
| 5 | Win32/IRCbot | 7.5% |
| 6 | Win32/Conficker | 7.3% |
| 7 | Win32/Keygen | 6.6% |
| 8 | Win32/Renos | 6.2% |
| 9 | Win32/Taterf | 5.3% |
| 10 | Win32/Agent | 4.1% |

- The most common threat family in Romania in 4Q10 was Win32/Autorun, which affected 10.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Romania in 4Q10 was Win32/Sality, which affected 8.6 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family in Romania in 4Q10 was Win32/Rimecud, which affected 8.1 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The fourth most common threat family in Romania in 4Q10 was JS/Pornpop, which affected 7.8 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Russia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

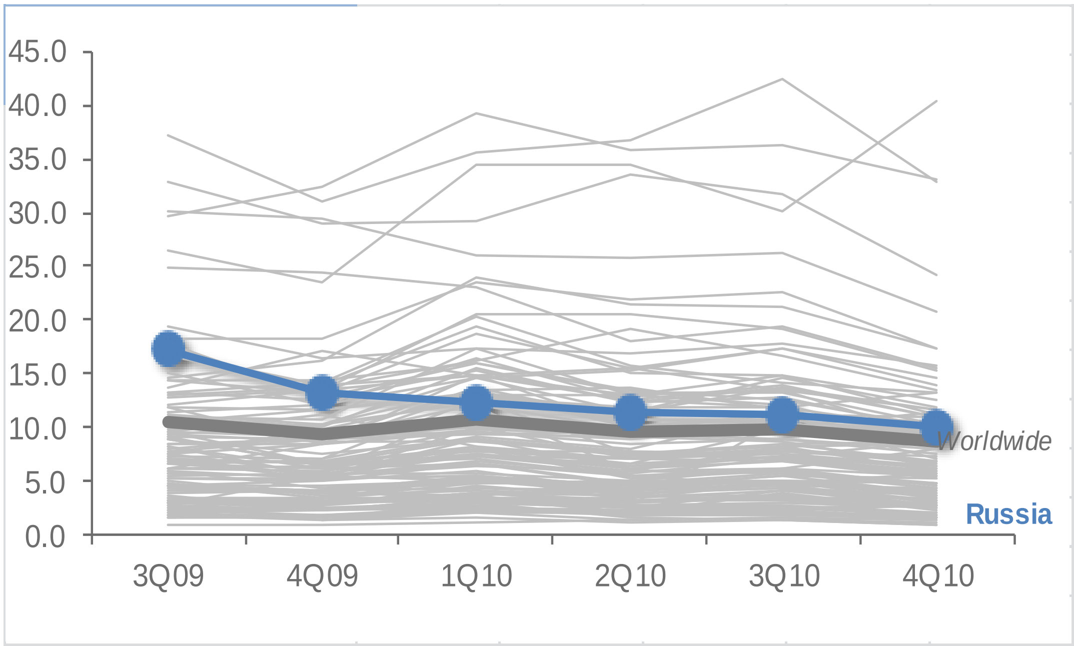
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Russia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Russia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">12.4</td><td colspan="3">11.5</td><td colspan="3">11.1</td><td colspan="3">10.1</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.55</td><td colspan="6">0.93</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">7.43</td><td colspan="6">4.55</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.228%</td><td colspan="4">0.125%</td><td colspan="4">0.127%</td></tr>
</table>

## Infection Trends (CCM)

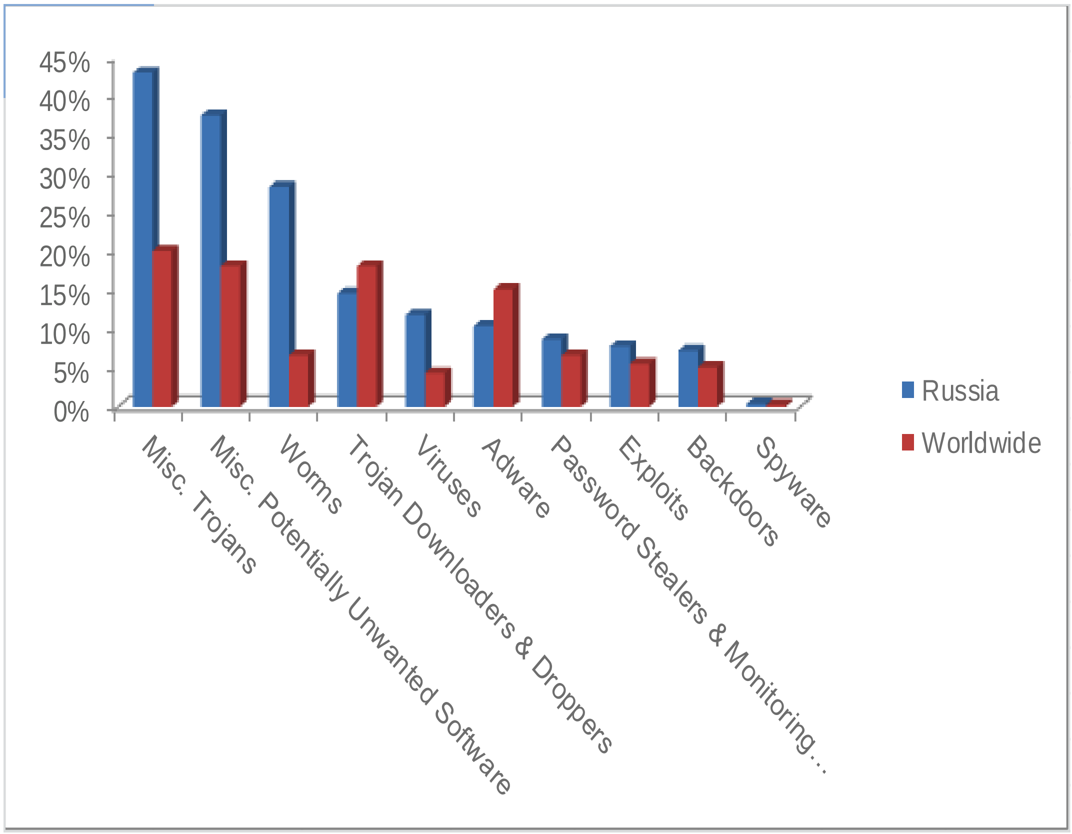
The MSRT detected malware on 10.1 of every 1,000 computers scanned in Russia in 4Q10 (a CCM score of 10.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Russia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Russia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Russia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Russia in 4Q10 was Misc. Trojans, which affected 42.9 percent of all cleaned computers, up from 42.0 percent in 3Q10.
- The second most common category in Russia in 4Q10 was Misc. Potentially Unwanted Software, which affected 37.5 percent of all cleaned computers, up from 35.2 percent in 3Q10.
- The third most common category in Russia in 4Q10 was Worms, which affected 28.3 percent of all cleaned computers, down from 32.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Russia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 15.4% |
| 2 | Win32/Rimecud | 10.6% |
| 3 | Win32/Obfuscator | 9.5% |
| 4 | Win32/Conficker | 9.4% |
| 5 | Win32/Keygen | 8.9% |
| 6 | JS/Pornpop | 5.4% |
| 7 | Bumat | 5.2% |
| 8 | Win32/Sality | 5.0% |
| 9 | Meredrop | 4.2% |
| 10 | Dynamer | 4.1% |

- The most common threat family in Russia in 4Q10 was Win32/Autorun, which affected 15.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Russia in 4Q10 was Win32/Rimecud, which affected 10.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Russia in 4Q10 was Win32/Obfuscator, which affected 9.5 percent of cleaned computers. Win32/Obfuscator is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by anti-virus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.
- The fourth most common threat family in Russia in 4Q10 was Win32/Conficker, which affected 9.4 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

# Saudi Arabia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

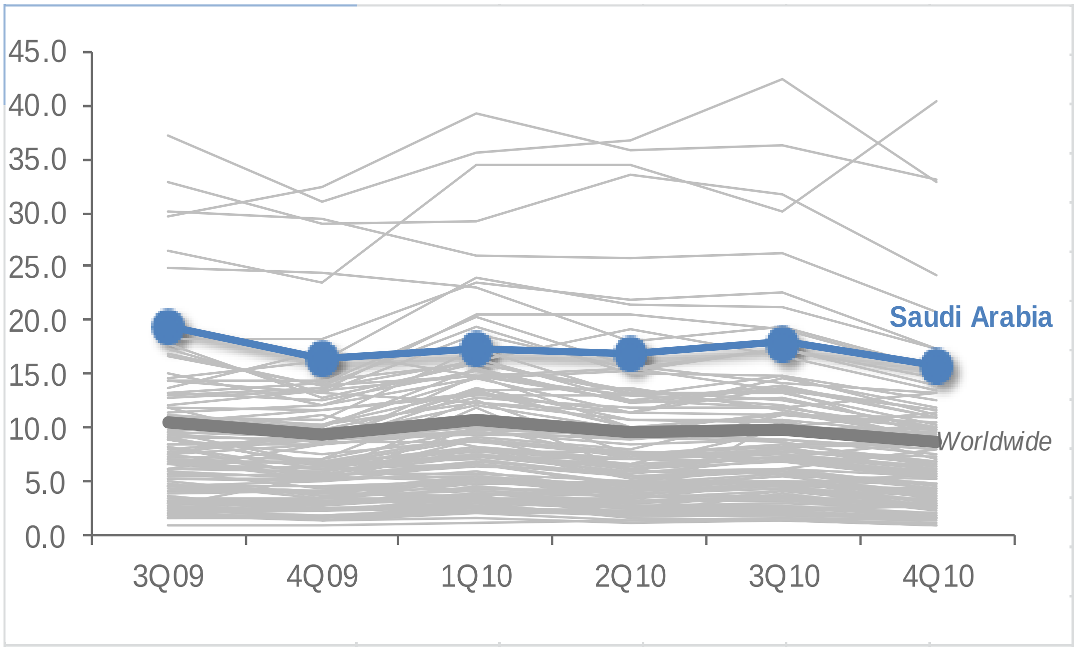
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Saudi Arabia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Saudi Arabia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">17.3</td><td colspan="3">16.8</td><td colspan="3">17.9</td><td colspan="3">15.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.62</td><td colspan="6">1.37</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.73</td><td colspan="6">1.98</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.479%</td><td colspan="4">0.307%</td><td colspan="4">0.347%</td></tr>
</table>

## Infection Trends (CCM)

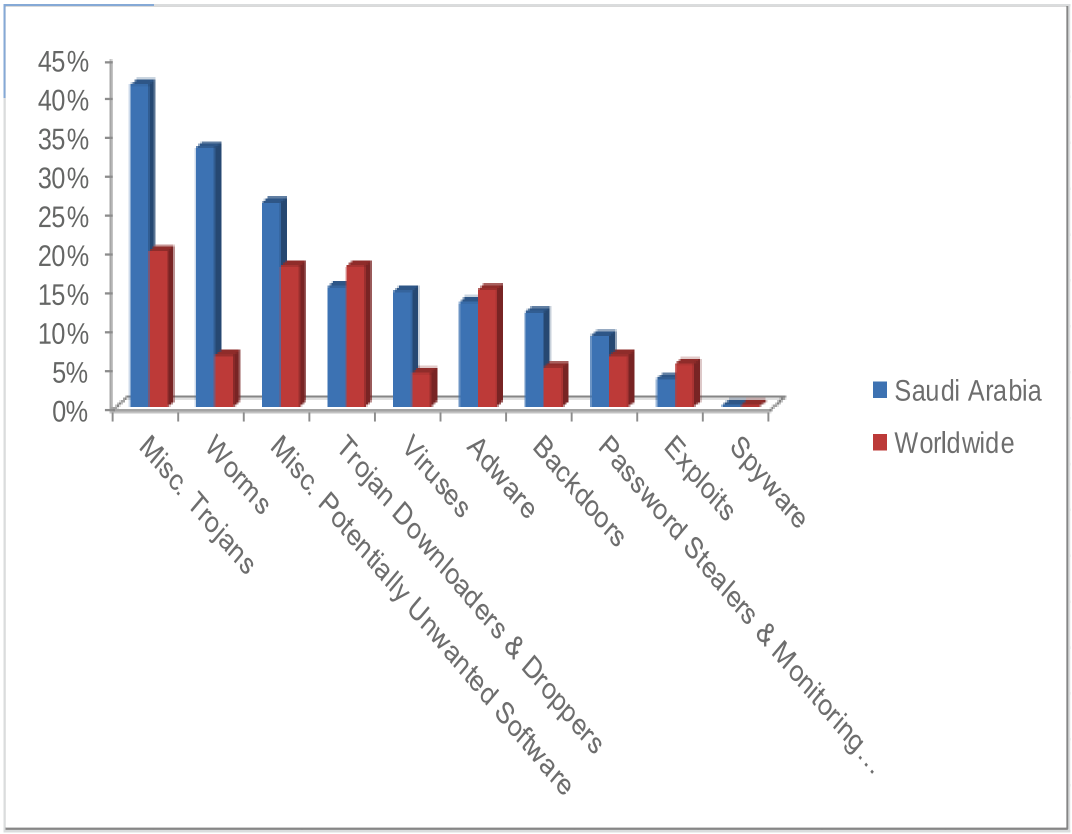
The MSRT detected malware on 15.8 of every 1,000 computers scanned in Saudi Arabia in 4Q10 (a CCM score of 15.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Saudi Arabia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Saudi Arabia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Saudi Arabia in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Saudi Arabia in 4Q10 was Misc. Trojans, which affected 41.3 percent of all cleaned computers, up from 38.4 percent in 3Q10.
- The second most common category in Saudi Arabia in 4Q10 was Worms, which affected 33.3 percent of all cleaned computers, down from 35.9 percent in 3Q10.
- The third most common category in Saudi Arabia in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.2 percent of all cleaned computers, up from 22.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Saudi Arabia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Agent | 17.0% |
| 2 | Win32/Autorun | 13.8% |
| 3 | Win32/Sality | 12.3% |
| 4 | Win32/Rimecud | 9.2% |
| 5 | Win32/Taterf | 7.7% |
| 6 | JS/Pornpop | 5.9% |
| 7 | Giframe | 5.5% |
| 8 | Win32/Conficker | 5.4% |
| 9 | Win32/Renos | 5.0% |
| 10 | Win32/Frethog | 4.9% |

- The most common threat family in Saudi Arabia in 4Q10 was Win32/Agent, which affected 17.0 percent of cleaned computers. Win32/Agent is a generic detection for a number of trojans that may perform different malicious functions. The functionality exhibited by this family is highly variable.
- The second most common threat family in Saudi Arabia in 4Q10 was Win32/Autorun, which affected 13.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Saudi Arabia in 4Q10 was Win32/Sality, which affected 12.3 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Saudi Arabia in 4Q10 was Win32/Rimecud, which affected 9.2 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Senegal

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

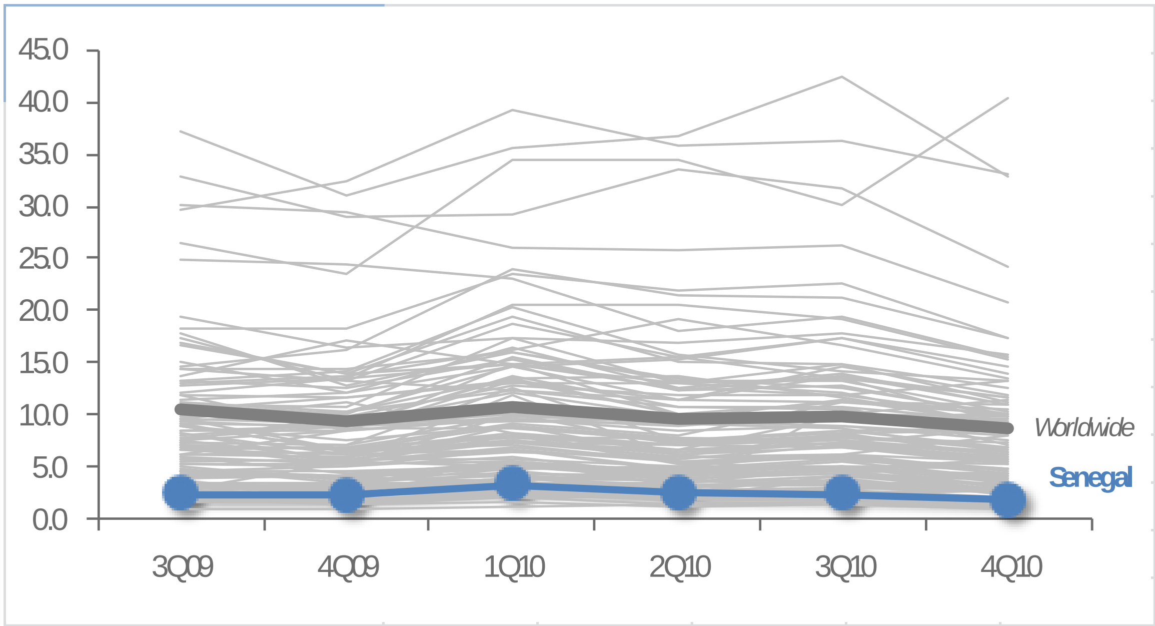
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Senegal in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Senegal and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.4 | 2.6 | 2.4 | 1.9 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 46.08 | | | |
| Malware hosting sites per 1000 hosts | 4.61 | | 4.61 | |
| Percentage of sites hosting drive-by downloads | 0.881% | 0.580% | 0.268% | |

## Infection Trends (CCM)

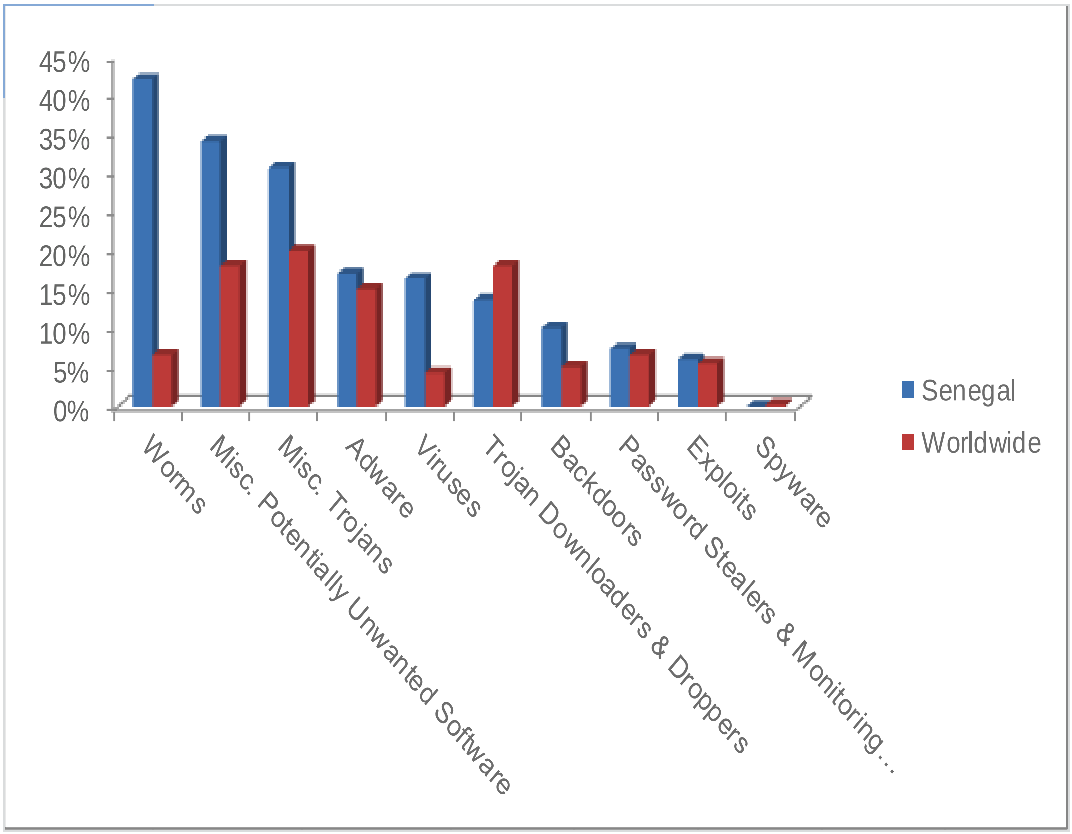
The MSRT detected malware on 1.9 of every 1,000 computers scanned in Senegal in 4Q10 (a CCM score of 1.9, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Senegal over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Senegal and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Senegal in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Senegal in 4Q10 was Worms, which affected 42.0 percent of all cleaned computers, down from 47.2 percent in 3Q10.
- The second most common category in Senegal in 4Q10 was Misc. Potentially Unwanted Software, which affected 34.1 percent of all cleaned computers, up from 32.9 percent in 3Q10.
- The third most common category in Senegal in 4Q10 was Misc. Trojans, which affected 30.7 percent of all cleaned computers, up from 25.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Senegal in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 23.1% |
| 2 | Win32/Rimecud | 20.4% |
| 3 | Win32/Sality | 12.3% |
| 4 | Win32/Taterf | 10.2% |
| 5 | Win32/Vobfus | 9.5% |
| 6 | Win32/Zwangi | 7.7% |
| 7 | Win32/ClickPotato | 7.1% |
| 8 | VBS/Slogod | 5.2% |
| 9 | Win32/Mabezat | 5.0% |
| 10 | Win32/Delf | 5.0% |

- The most common threat family in Senegal in 4Q10 was Win32/Autorun, which affected 23.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Senegal in 4Q10 was Win32/Rimecud, which affected 20.4 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Senegal in 4Q10 was Win32/Sality, which affected 12.3 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Senegal in 4Q10 was Win32/Taterf, which affected 10.2 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Singapore

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

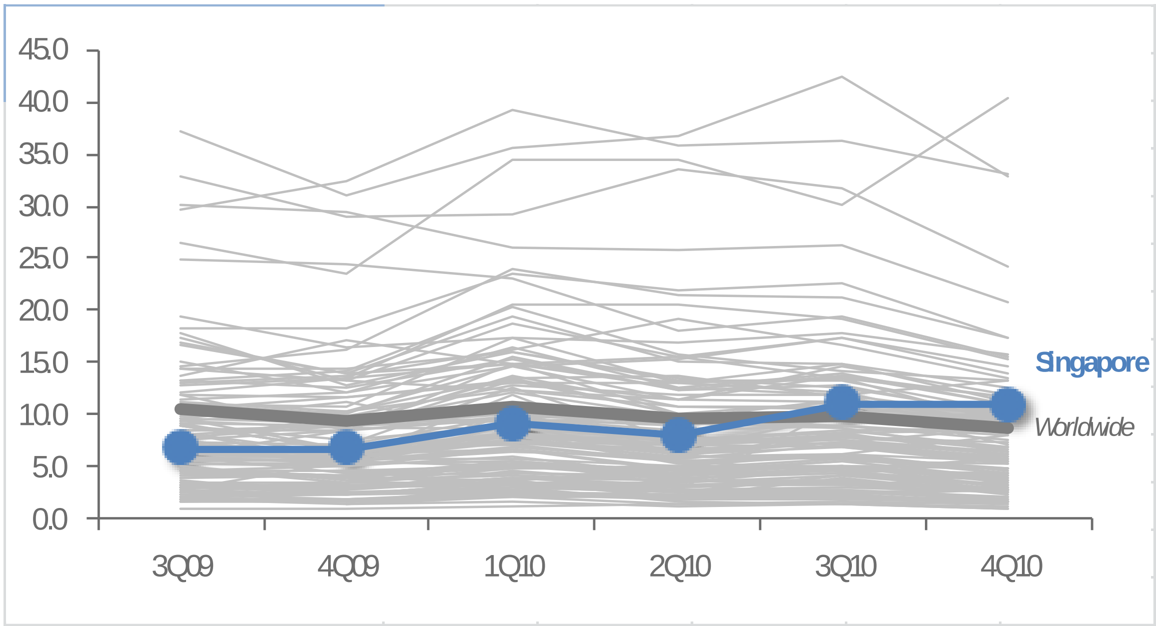
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Singapore in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Singapore and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">9.2</td><td colspan="3">8.0</td><td colspan="3">11.1</td><td colspan="3">11.0</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.62</td><td colspan="6">1.12</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.44</td><td colspan="6">0.28</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.225%</td><td colspan="4">0.089%</td><td colspan="4">0.083%</td></tr>
</table>

## Infection Trends (CCM)

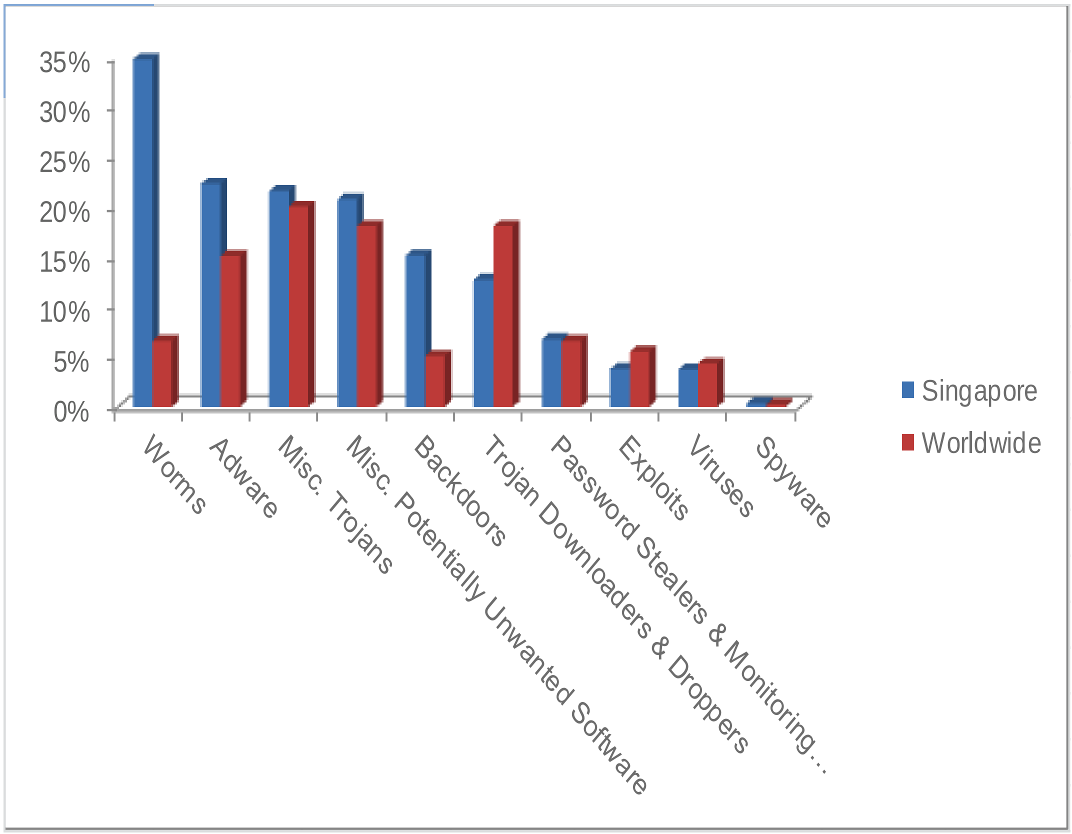
The MSRT detected malware on 11.0 of every 1,000 computers scanned in Singapore in 4Q10 (a CCM score of 11.0, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Singapore over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Singapore and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Singapore in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Singapore in 4Q10 was Worms, which affected 34.7 percent of all cleaned computers, up from 33.1 percent in 3Q10.
- The second most common category in Singapore in 4Q10 was Adware, which affected 22.3 percent of all cleaned computers, down from 22.0 percent in 3Q10.
- The third most common category in Singapore in 4Q10 was Misc. Trojans, which affected 21.6 percent of all cleaned computers, up from 20.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Singapore in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Vobfus | 12.6% |
| 2 | Win32/Autorun | 11.1% |
| 3 | JS/Pornpop | 9.8% |
| 4 | Win32/Hupigon | 9.0% |
| 5 | Win32/Rimecud | 8.7% |
| 6 | Win32/ClickPotato | 7.1% |
| 7 | Win32/Taterf | 7.1% |
| 8 | Win32/Zwangi | 5.6% |
| 9 | Win32/Hotbar | 4.2% |
| 10 | Win32/Renos | 3.8% |

- The most common threat family in Singapore in 4Q10 was Win32/Vobfus, which affected 12.6 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The second most common threat family in Singapore in 4Q10 was Win32/Autorun, which affected 11.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Singapore in 4Q10 was JS/Pornpop, which affected 9.8 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Singapore in 4Q10 was Win32/Hupigon, which affected 9.0 percent of cleaned computers. Win32/Hupigon is a family of trojans that uses a dropper to install one or more backdoor files, and installs sometimes a password stealer or other malicious programs.

# Slovakia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

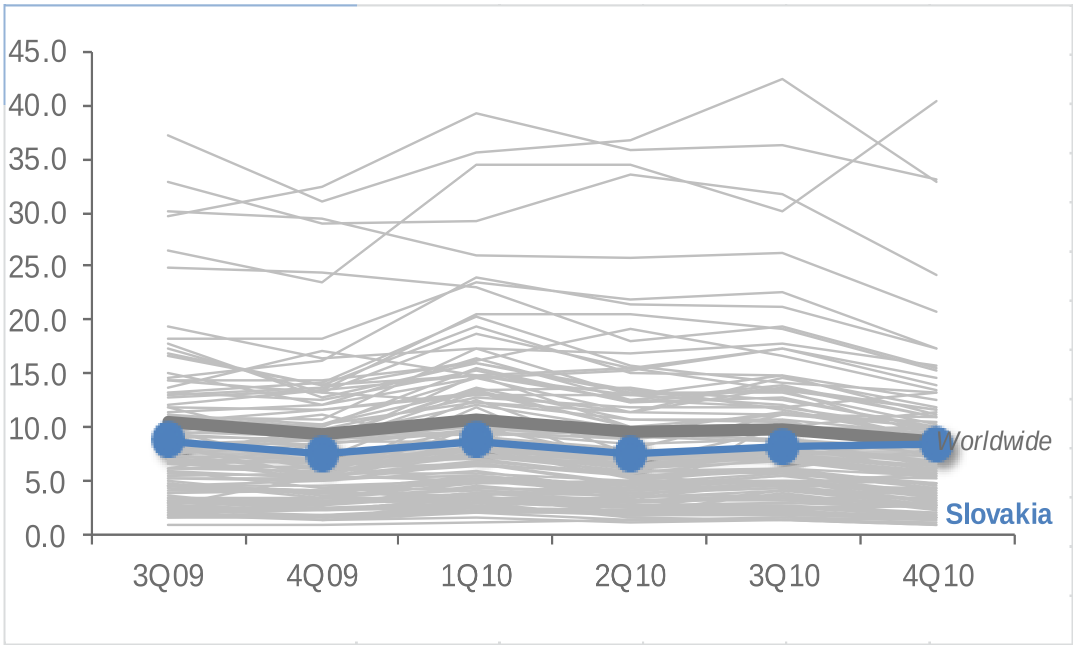
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Slovakia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Slovakia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">8.8</td><td colspan="3">7.6</td><td colspan="3">8.3</td><td colspan="3">8.5</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.79</td><td colspan="6">0.39</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">4.35</td><td colspan="6">1.06</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.206%</td><td colspan="4">0.110%</td><td colspan="4">0.069%</td></tr>
</table>

## Infection Trends (CCM)

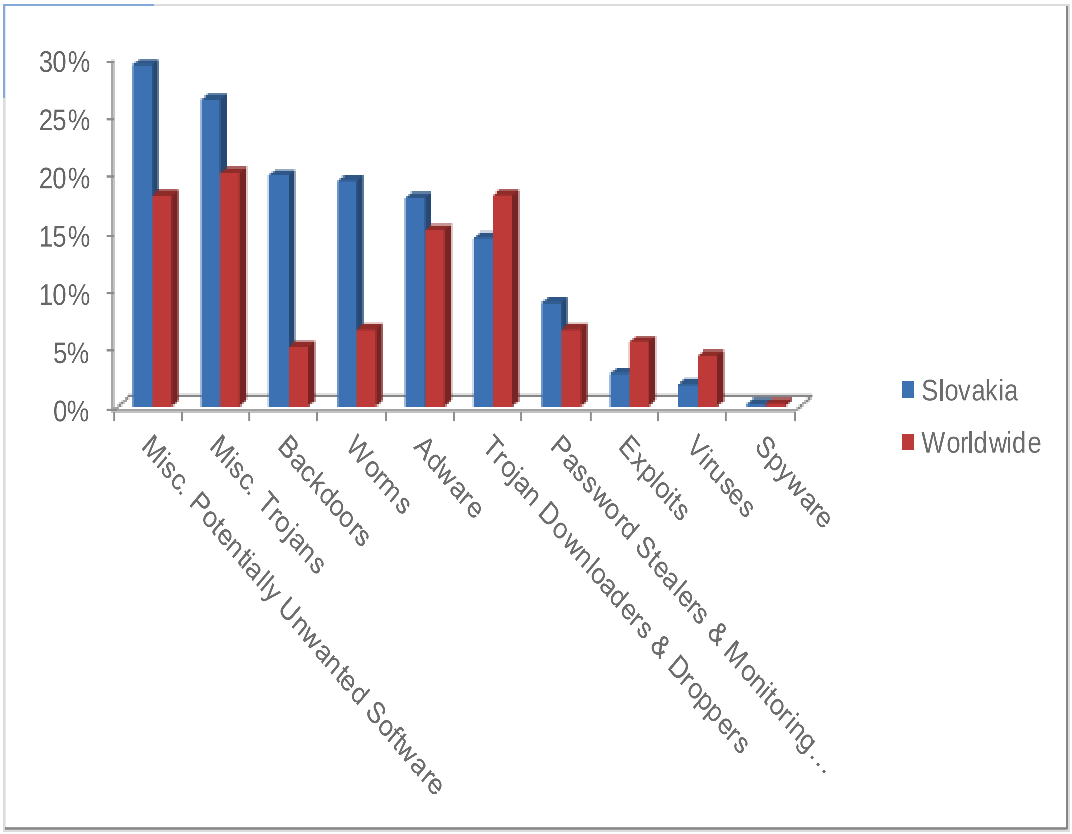
The MSRT detected malware on 8.5 of every 1,000 computers scanned in Slovakia in 4Q10 (a CCM score of 8.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Slovakia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Slovakia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Slovakia in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Slovakia in 4Q10 was Misc. Potentially Unwanted Software, which affected 29.2 percent of all cleaned computers, down from 30.1 percent in 3Q10.
- The second most common category in Slovakia in 4Q10 was Misc. Trojans, which affected 26.3 percent of all cleaned computers, down from 25.7 percent in 3Q10.
- The third most common category in Slovakia in 4Q10 was Backdoors, which affected 19.8 percent of all cleaned computers, down from 24.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Slovakia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/IRCbot | 16.7% |
| 2 | Win32/Autorun | 11.1% |
| 3 | JS/Pornpop | 10.8% |
| 4 | Win32/Rimecud | 7.3% |
| 5 | Win32/Taterf | 7.3% |
| 6 | Win32/Renos | 6.4% |
| 7 | Win32/Keygen | 6.1% |
| 8 | Win32/Frethog | 4.6% |
| 9 | Win32/Obfuscator | 4.2% |
| 10 | Win32/Winwebsec | 3.4% |

- The most common threat family in Slovakia in 4Q10 was Win32/IRCbot, which affected 16.7 percent of cleaned computers. Win32/IRCbot is a large family of backdoor trojans that drops other malicious software and connects to IRC servers to receive commands from attackers.
- The second most common threat family in Slovakia in 4Q10 was Win32/Autorun, which affected 11.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Slovakia in 4Q10 was JS/Pornpop, which affected 10.8 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in Slovakia in 4Q10 was Win32/Rimecud, which affected 7.3 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Slovenia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

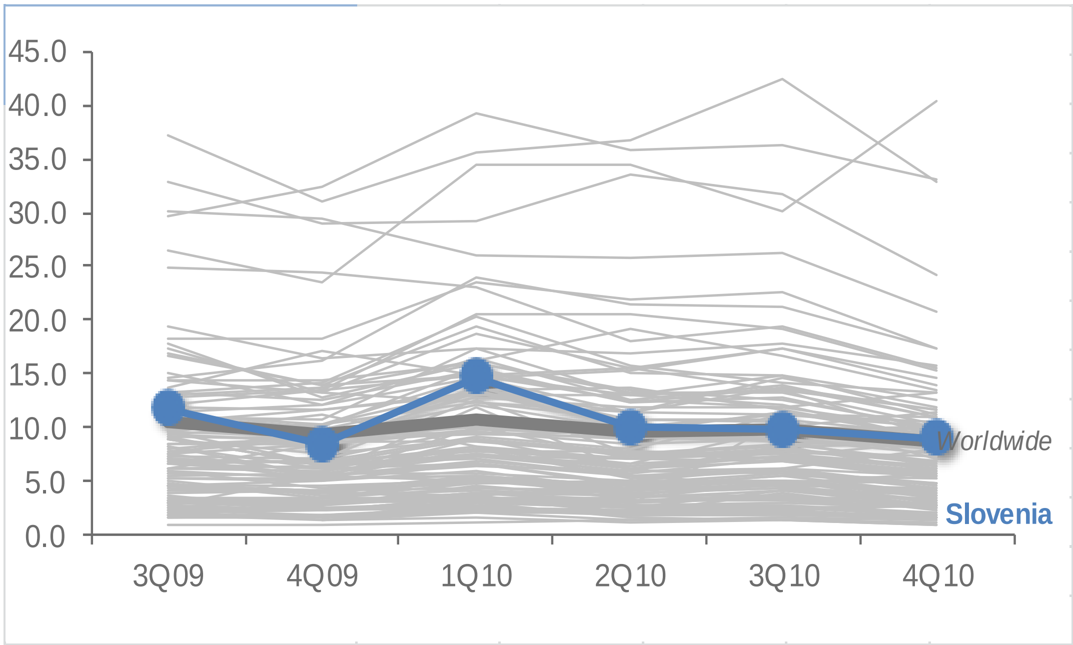
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Slovenia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Slovenia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">14.8</td><td colspan="3">10.0</td><td colspan="3">9.8</td><td colspan="3">9.1</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.41</td><td colspan="6">1.22</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.76</td><td colspan="6">2.00</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.176%</td><td colspan="4">0.048%</td><td colspan="4">0.048%</td></tr>
</table>

## Infection Trends (CCM)

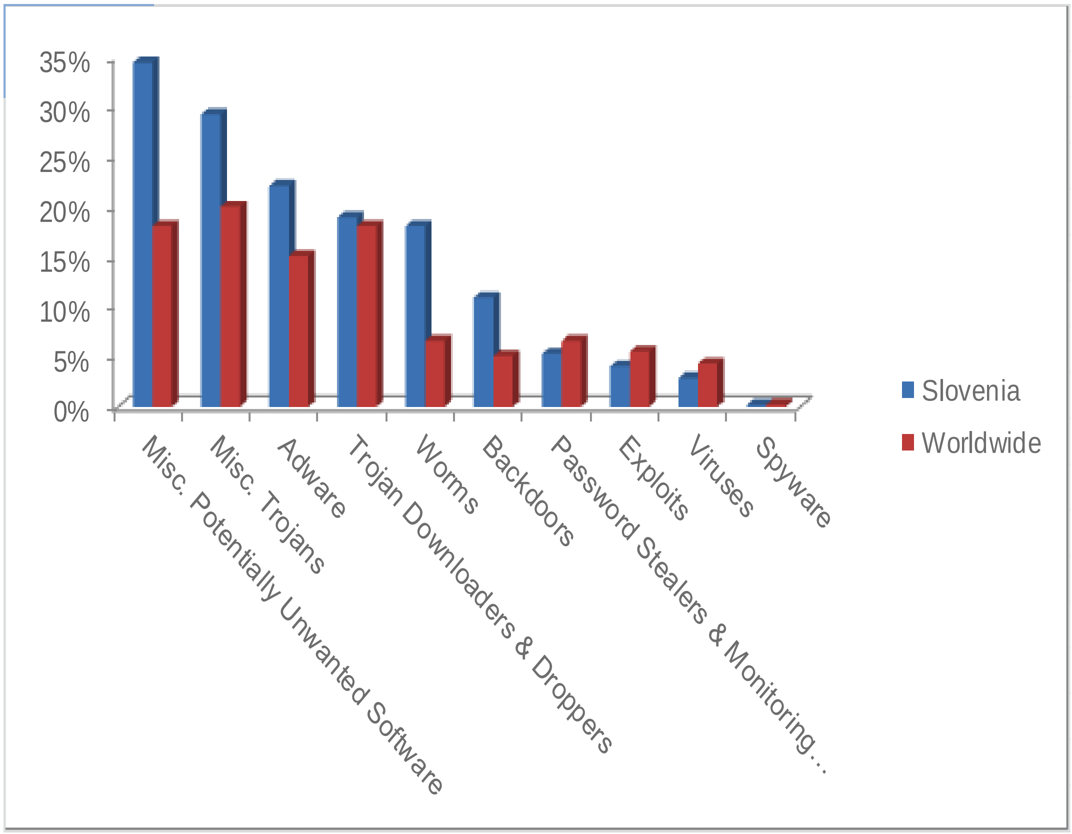
The MSRT detected malware on 9.1 of every 1,000 computers scanned in Slovenia in 4Q10 (a CCM score of 9.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Slovenia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Slovenia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Slovenia in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Slovenia in 4Q10 was Misc. Potentially Unwanted Software, which affected 34.4 percent of all cleaned computers, up from 32.9 percent in 3Q10.
- The second most common category in Slovenia in 4Q10 was Misc. Trojans, which affected 29.2 percent of all cleaned computers, down from 31.0 percent in 3Q10.
- The third most common category in Slovenia in 4Q10 was Adware, which affected 22.1 percent of all cleaned computers, down from 24.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Slovenia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 13.2% |
| 2 | Win32/Rimecud | 10.4% |
| 3 | Win32/Autorun | 9.7% |
| 4 | Win32/Keygen | 8.7% |
| 5 | Win32/Renos | 6.2% |
| 6 | Win32/IRCbot | 6.0% |
| 7 | Win32/Conficker | 5.2% |
| 8 | Win32/Obfuscator | 4.3% |
| 9 | Win32/Zwangi | 4.2% |
| 10 | ASX/Wimad | 4.2% |

- The most common threat family in Slovenia in 4Q10 was JS/Pornpop, which affected 13.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Slovenia in 4Q10 was Win32/Rimecud, which affected 10.4 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Slovenia in 4Q10 was Win32/Autorun, which affected 9.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common threat family in Slovenia in 4Q10 was Win32/Keygen, which affected 8.7 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.

# South Africa

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

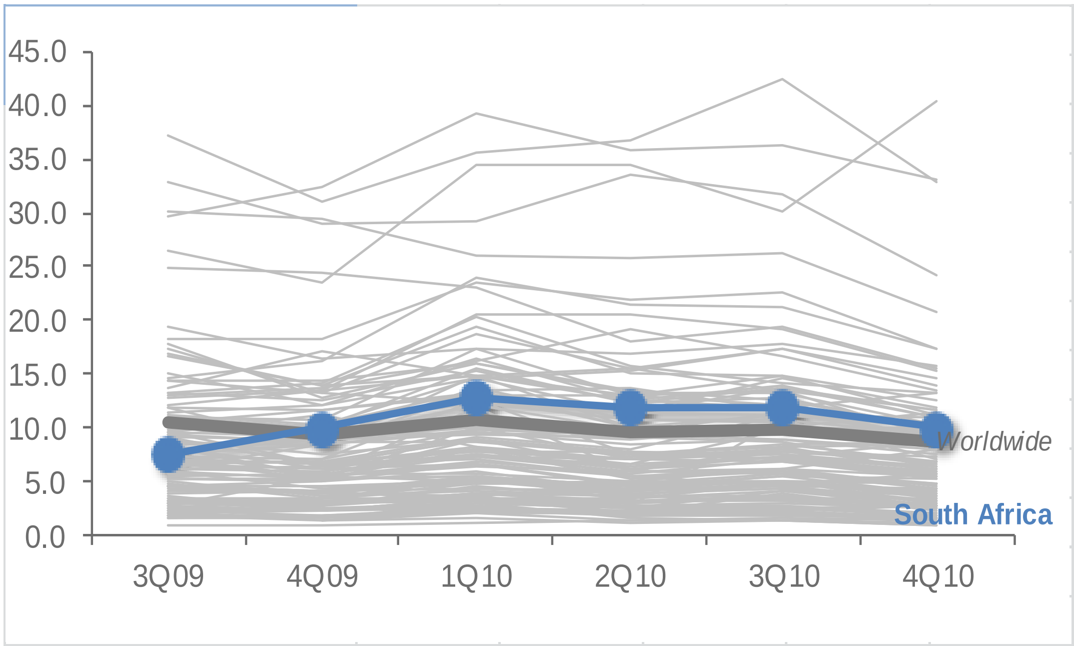
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in South Africa in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in South Africa and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 12.8 | 11.9 | 11.8 | 9.8 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.25 | | 0.11 | |
| Malware hosting sites per 1000 hosts | 0.12 | | 0.10 | |
| Percentage of sites hosting drive-by downloads | 0.116% | 0.056% | 0.042% | |

## Infection Trends (CCM)

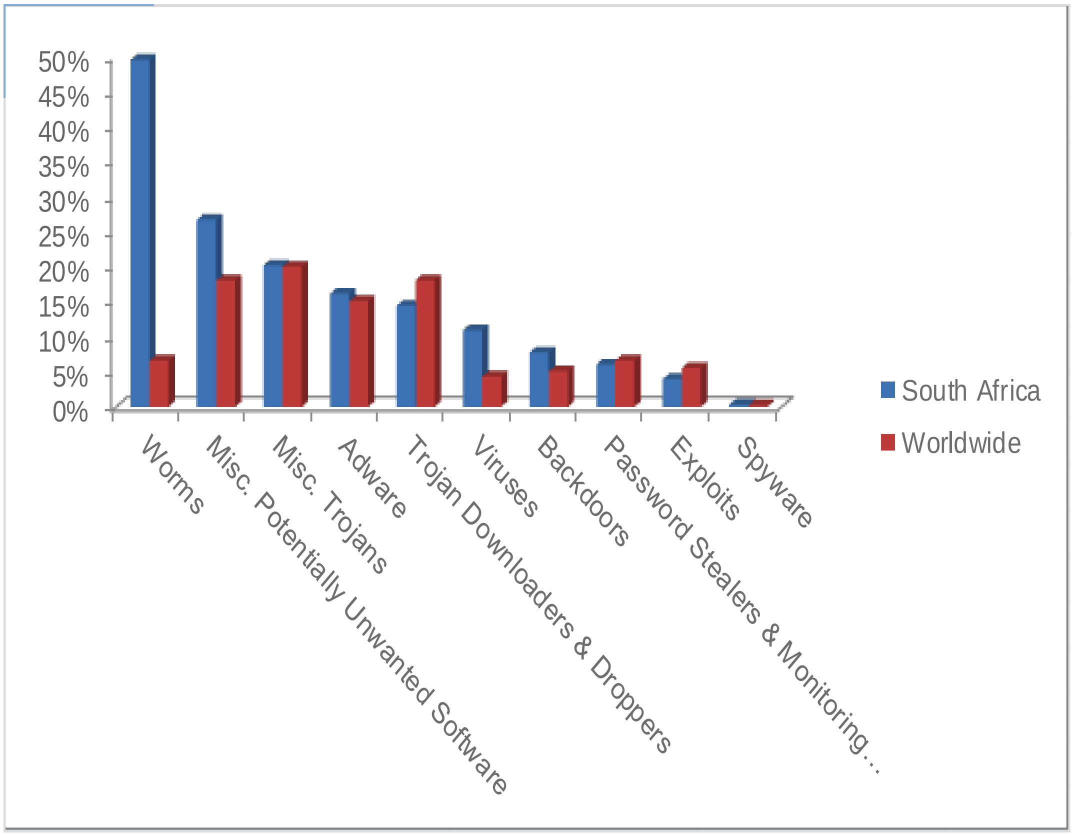
The MSRT detected malware on 9.8 of every 1,000 computers scanned in South Africa in 4Q10 (a CCM score of 9.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for South Africa over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in South Africa and worldwide



## Threat Categories

Malware and potentially unwanted software categories in South Africa in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in South Africa in 4Q10 was Worms, which affected 49.5 percent of all cleaned computers, down from 53.1 percent in 3Q10.
- The second most common category in South Africa in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.7 percent of all cleaned computers, up from 25.2 percent in 3Q10.
- The third most common category in South Africa in 4Q10 was Misc. Trojans, which affected 20.2 percent of all cleaned computers, down from 21.2 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in South Africa in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 18.9% |
| 2 | Win32/Rimecud | 18.6% |
| 3 | JS/Pornpop | 11.1% |
| 4 | Win32/Vobfus | 10.1% |
| 5 | Win32/Conficker | 8.3% |
| 6 | Win32/Hamweq | 5.4% |
| 7 | Win32/Renos | 5.4% |
| 8 | Win32/Virut | 4.6% |
| 9 | Win32/Mabezat | 3.9% |
| 10 | Win32/VBInject | 3.1% |

- The most common threat family in South Africa in 4Q10 was Win32/Autorun, which affected 18.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in South Africa in 4Q10 was Win32/Rimecud, which affected 18.6 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in South Africa in 4Q10 was JS/Pornpop, which affected 11.1 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The fourth most common threat family in South Africa in 4Q10 was Win32/Vobfus, which affected 10.1 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

# Spain

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

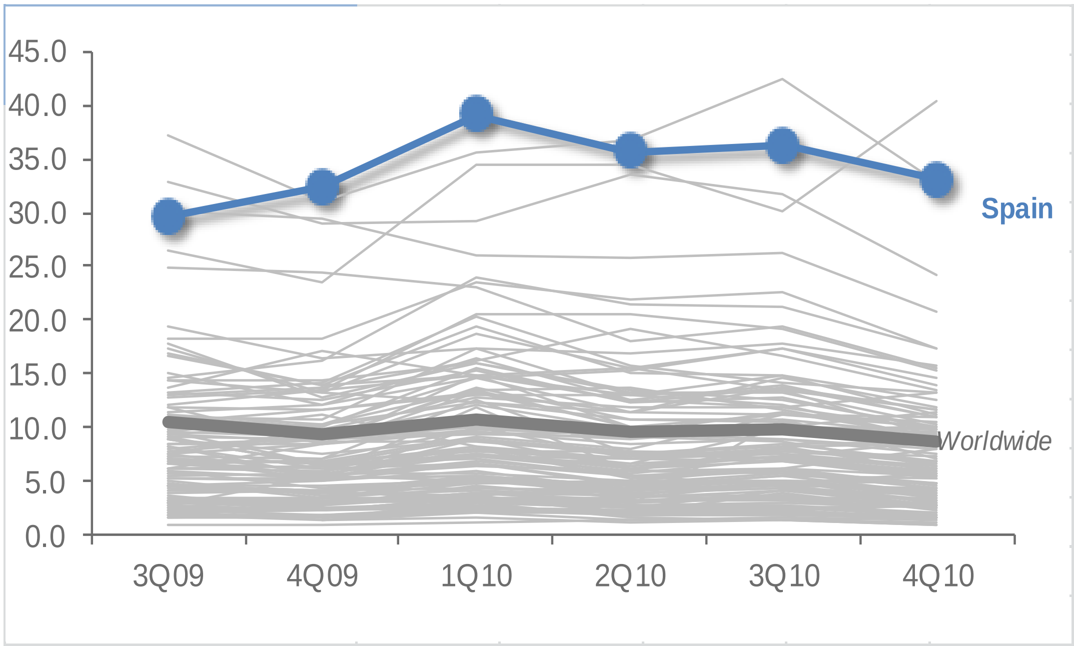
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Spain in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Spain and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">39.2</td><td colspan="3">35.7</td><td colspan="3">36.3</td><td colspan="3">33.2</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.46</td><td colspan="6">0.56</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">3.01</td><td colspan="6">1.83</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.200%</td><td colspan="4">0.041%</td><td colspan="4">0.051%</td></tr>
</table>

## Infection Trends (CCM)

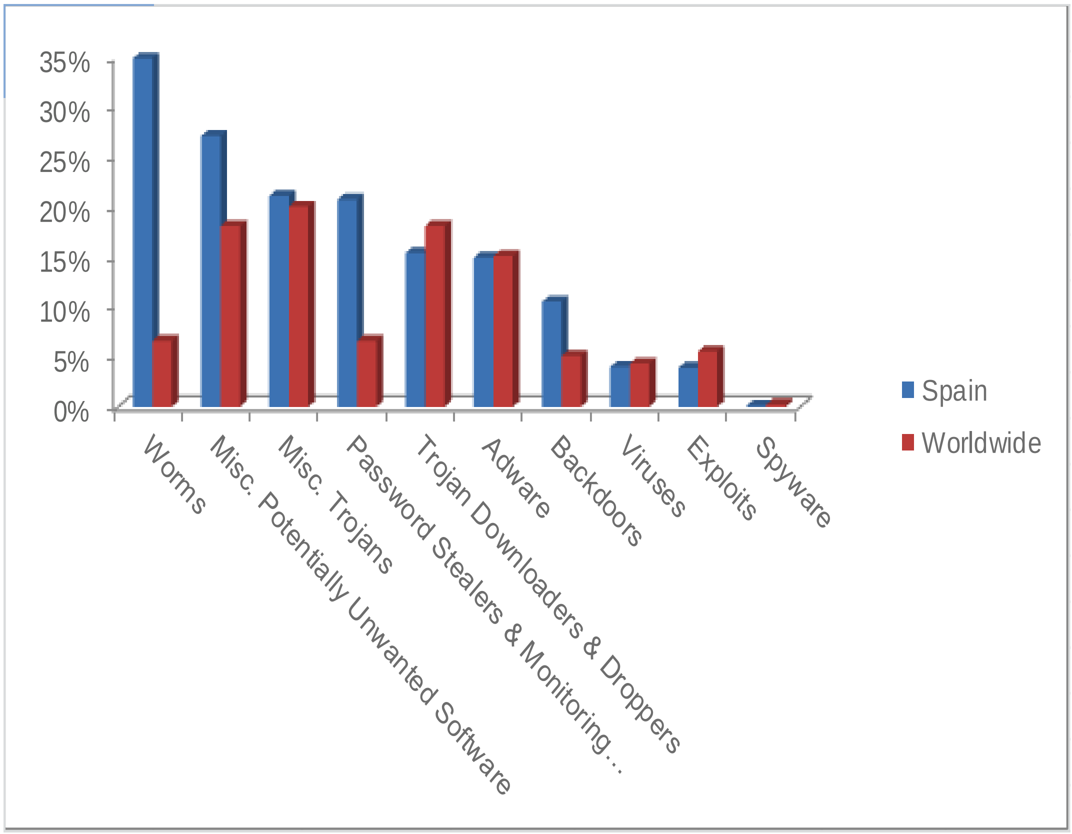
The MSRT detected malware on 33.2 of every 1,000 computers scanned in Spain in 4Q10 (a CCM score of 33.2, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Spain over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Spain and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Spain in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Spain in 4Q10 was Worms, which affected 34.8 percent of all cleaned computers, down from 40.7 percent in 3Q10.
- The second most common category in Spain in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.1 percent of all cleaned computers, up from 26.2 percent in 3Q10.
- The third most common category in Spain in 4Q10 was Misc. Trojans, which affected 21.1 percent of all cleaned computers, up from 20.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Spain in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Taterf | 12.7% |
| 2 | Win32/Autorun | 10.9% |
| 3 | Win32/Zbot | 9.0% |
| 4 | Win32/Frethog | 8.1% |
| 5 | Win32/Rimecud | 7.2% |
| 6 | Win32/IRCbot | 5.9% |
| 7 | Win32/Conficker | 5.8% |
| 8 | JS/Pornpop | 5.7% |
| 9 | Win32/Zwangi | 5.4% |
| 10 | Win32/Renos | 4.7% |

- The most common threat family in Spain in 4Q10 was Win32/Taterf, which affected 12.7 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The second most common threat family in Spain in 4Q10 was Win32/Autorun, which affected 10.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Spain in 4Q10 was Win32/Zbot, which affected 9.0 percent of cleaned computers. Win32/Zbot is a family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected machine.
- The fourth most common threat family in Spain in 4Q10 was Win32/Frethog, which affected 8.1 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

# Sri Lanka

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

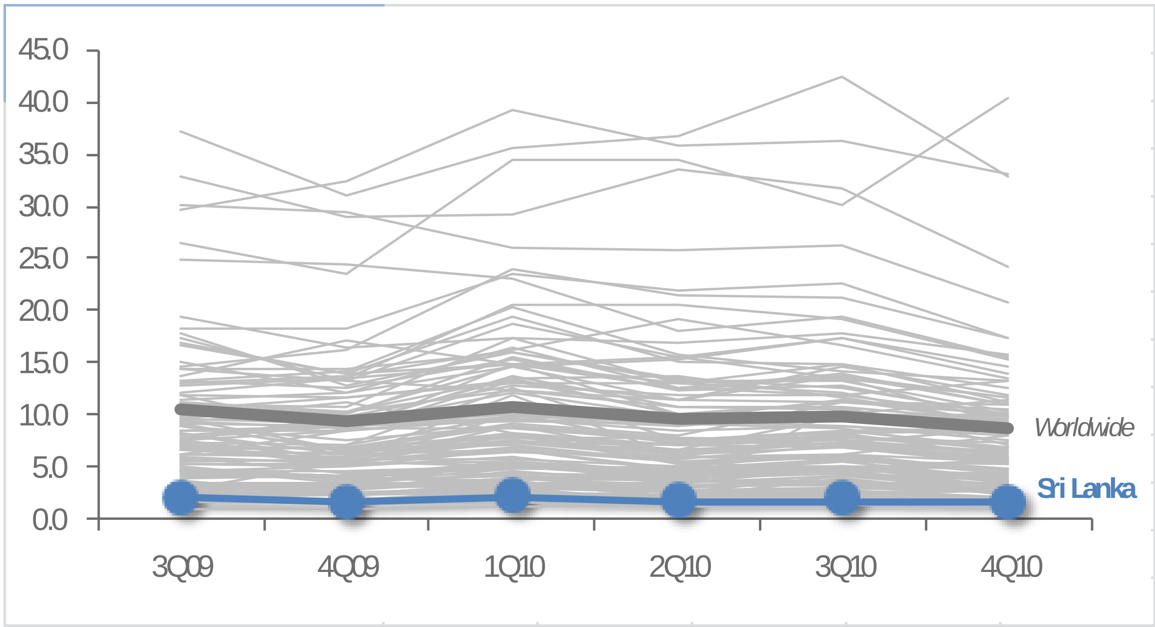
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Sri Lanka in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Sri Lanka and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">2.3</td><td colspan="3">1.8</td><td colspan="3">2.0</td><td colspan="3">1.7</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">14.57</td><td colspan="6">1.42</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">27.94</td><td colspan="6">6.48</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.200%</td><td colspan="4">0.066%</td><td colspan="4">0.062%</td></tr>
</table>

## Infection Trends (CCM)

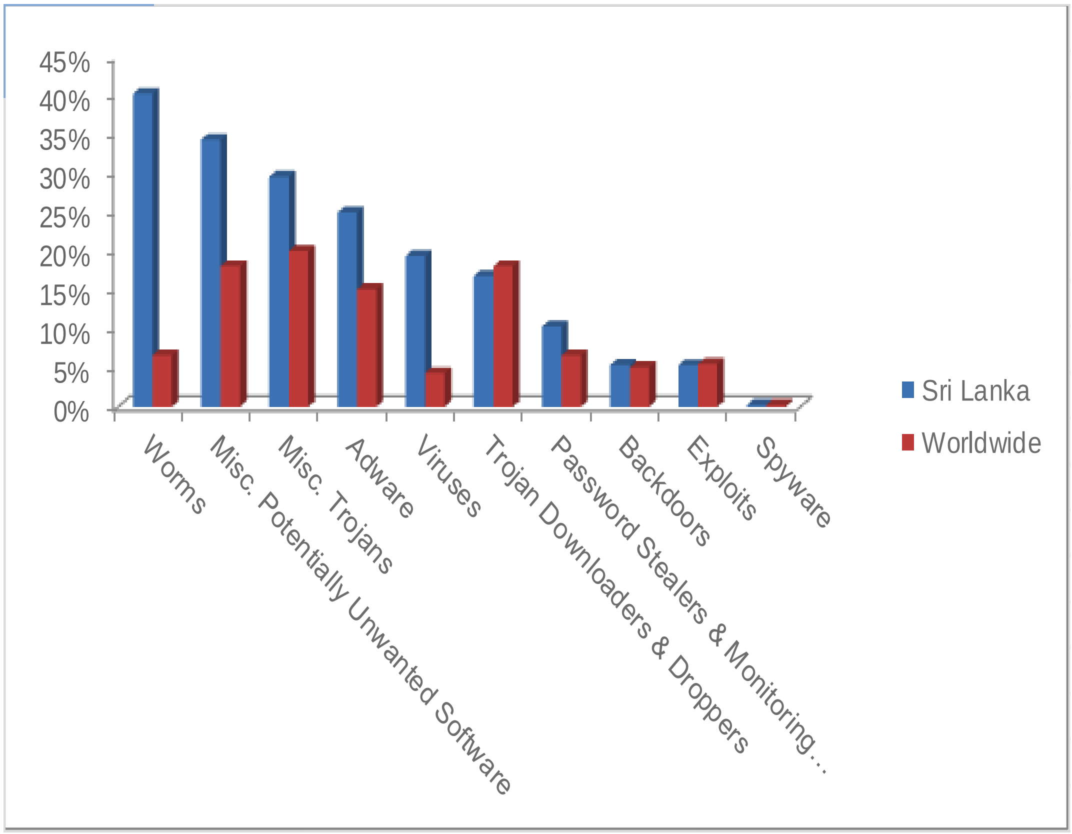
The MSRT detected malware on 1.7 of every 1,000 computers scanned in Sri Lanka in 4Q10 (a CCM score of 1.7, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Sri Lanka over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Sri Lanka and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Sri Lanka in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Sri Lanka in 4Q10 was Worms, which affected 40.2 percent of all cleaned computers, down from 43.0 percent in 3Q10.
- The second most common category in Sri Lanka in 4Q10 was Misc. Potentially Unwanted Software, which affected 34.3 percent of all cleaned computers, up from 30.2 percent in 3Q10.
- The third most common category in Sri Lanka in 4Q10 was Misc. Trojans, which affected 29.6 percent of all cleaned computers, up from 28.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Sri Lanka in 4Q10.

|  | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 28.7% |
| 2 | Win32/Rimecud | 14.5% |
| 3 | Win32/Sality | 13.4% |
| 4 | JS/Pornpop | 12.7% |
| 5 | Delicium | 8.0% |
| 6 | Win32/Renos | 7.9% |
| 7 | Win32/Taterf | 7.8% |
| 8 | Win32/Nuqel | 7.2% |
| 9 | Win32/Conficker | 6.1% |
| 10 | Win32/ClickPotato | 6.0% |

- The most common threat family in Sri Lanka in 4Q10 was Win32/Autorun, which affected 28.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Sri Lanka in 4Q10 was Win32/Rimecud, which affected 14.5 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Sri Lanka in 4Q10 was Win32/Sality, which affected 13.4 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Sri Lanka in 4Q10 was JS/Pornpop, which affected 12.7 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

# Sweden

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

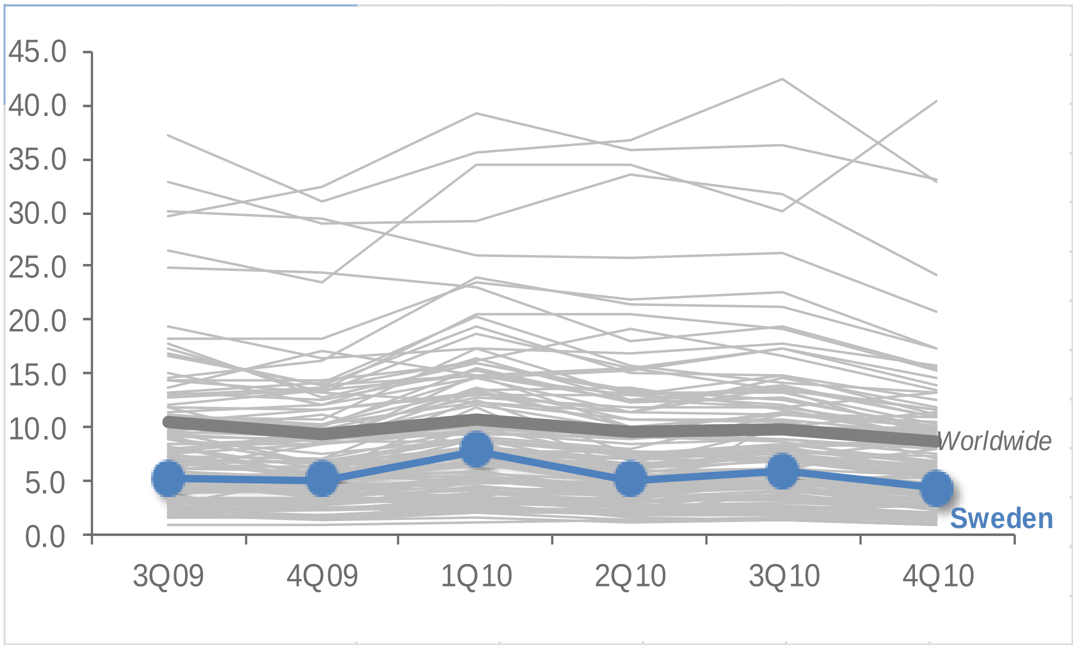
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Sweden in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Sweden and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">8.0</td><td colspan="3">5.2</td><td colspan="3">5.9</td><td colspan="3">4.4</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.25</td><td colspan="6">0.30</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">2.20</td><td colspan="6">6.14</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.093%</td><td colspan="4">0.033%</td><td colspan="4">0.034%</td></tr>
</table>

## Infection Trends (CCM)

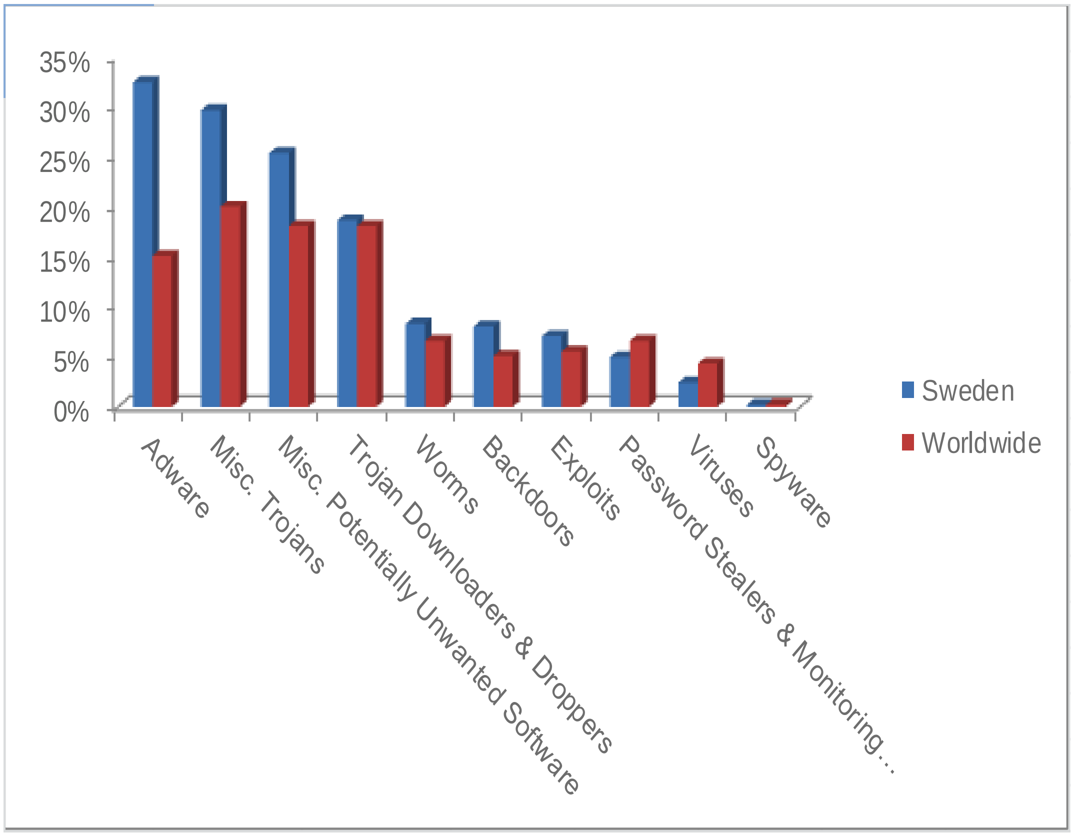
The MSRT detected malware on 4.4 of every 1,000 computers scanned in Sweden in 4Q10 (a CCM score of 4.4, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Sweden over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Sweden and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Sweden in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Sweden in 4Q10 was Adware, which affected 32.4 percent of all cleaned computers, down from 35.5 percent in 3Q10.
- The second most common category in Sweden in 4Q10 was Misc. Trojans, which affected 29.6 percent of all cleaned computers, up from 25.6 percent in 3Q10.
- The third most common category in Sweden in 4Q10 was Misc. Potentially Unwanted Software, which affected 25.3 percent of all cleaned computers, up from 24.3 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Sweden in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 17.2% |
| 2 | Win32/ClickPotato | 8.2% |
| 3 | Win32/Renos | 7.9% |
| 4 | Win32/Zwangi | 6.7% |
| 5 | Win32/Hotbar | 4.8% |
| 6 | Win32/Keygen | 4.6% |
| 7 | Win32/IRCbot | 4.6% |
| 8 | Win32/Vundo | 4.5% |
| 9 | Java/CVE-2009-3867 | 4.1% |
| 10 | Java/CVE-2008-5353 | 3.7% |

- The most common threat family in Sweden in 4Q10 was JS/Pornpop, which affected 17.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Sweden in 4Q10 was Win32/ClickPotato, which affected 8.2 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Sweden in 4Q10 was Win32/Renos, which affected 7.9 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.
- The fourth most common threat family in Sweden in 4Q10 was Win32/Zwangi, which affected 6.7 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Switzerland

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

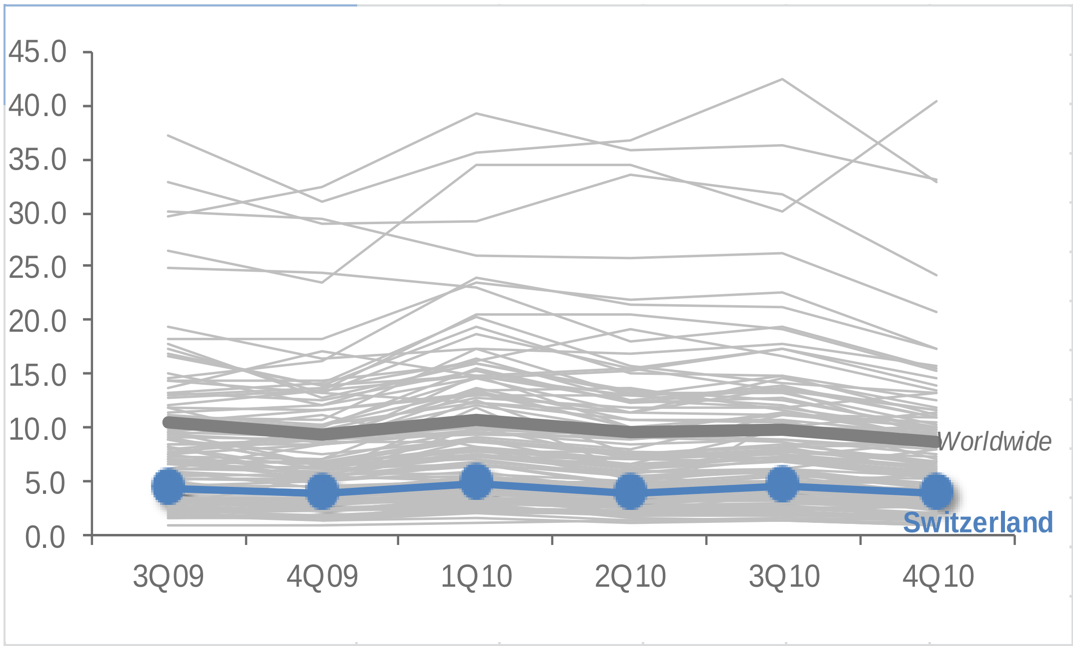
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Switzerland in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Switzerland and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">5.0</td><td colspan="3">4.0</td><td colspan="3">4.7</td><td colspan="3">4.1</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.32</td><td colspan="6">0.20</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.29</td><td colspan="6">0.35</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.188%</td><td colspan="4">0.030%</td><td colspan="4">0.034%</td></tr>
</table>

## Infection Trends (CCM)

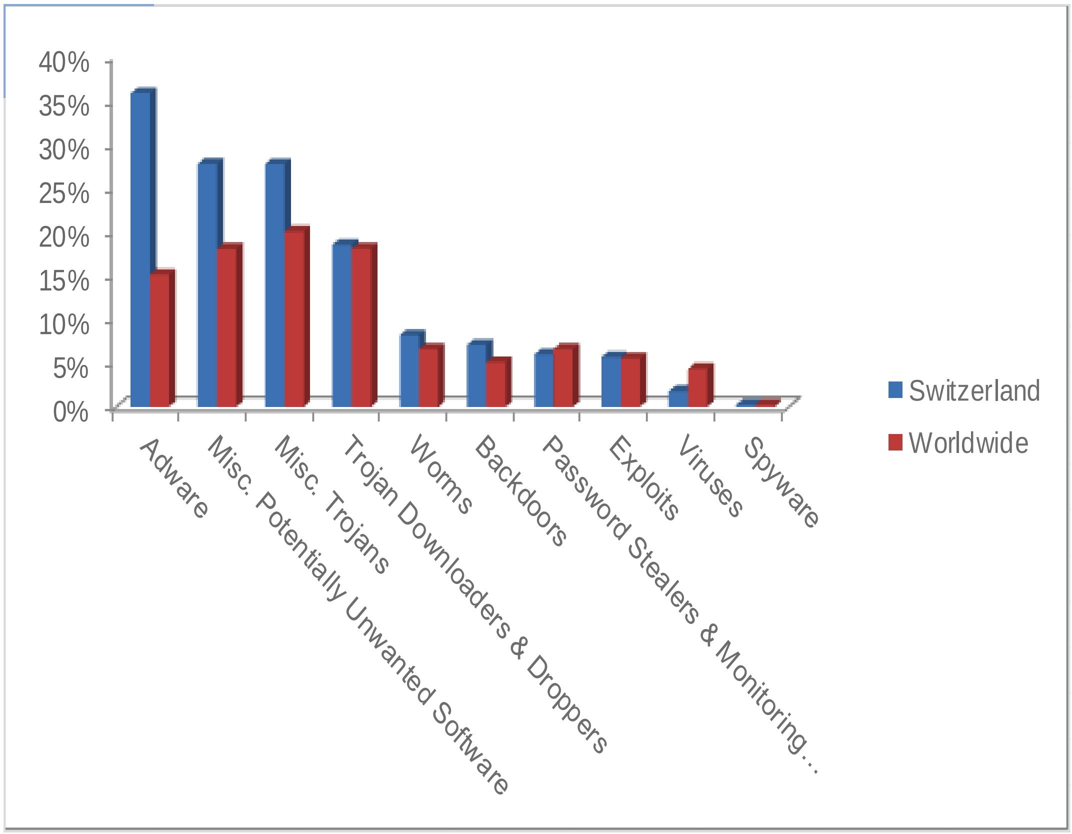
The MSRT detected malware on 4.1 of every 1,000 computers scanned in Switzerland in 4Q10 (a CCM score of 4.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Switzerland over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Switzerland and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Switzerland in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Switzerland in 4Q10 was Adware, which affected 35.8 percent of all cleaned computers, up from 28.4 percent in 3Q10.
- The second most common category in Switzerland in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.7 percent of all cleaned computers, up from 25.5 percent in 3Q10.
- The third most common category in Switzerland in 4Q10 was Misc. Trojans, which affected 27.7 percent of all cleaned computers, up from 24.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Switzerland in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 18.2% |
| 2 | Win32/ClickPotato | 9.9% |
| 3 | Win32/Zwangi | 9.4% |
| 4 | Win32/Renos | 6.3% |
| 5 | Win32/FakeSpypro | 5.9% |
| 6 | Win32/Hotbar | 5.8% |
| 7 | Win32/IRCbot | 4.6% |
| 8 | ASX/Wimad | 4.3% |
| 9 | Win32/Keygen | 3.5% |
| 10 | Win32/Winwebsec | 3.0% |

- The most common threat family in Switzerland in 4Q10 was JS/Pornpop, which affected 18.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Switzerland in 4Q10 was Win32/ClickPotato, which affected 9.9 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Switzerland in 4Q10 was Win32/Zwangi, which affected 9.4 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in Switzerland in 4Q10 was Win32/Renos, which affected 6.3 percent of cleaned computers. Win32/Renos is a family of trojan downloaders that install rogue security software.

# Syria

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

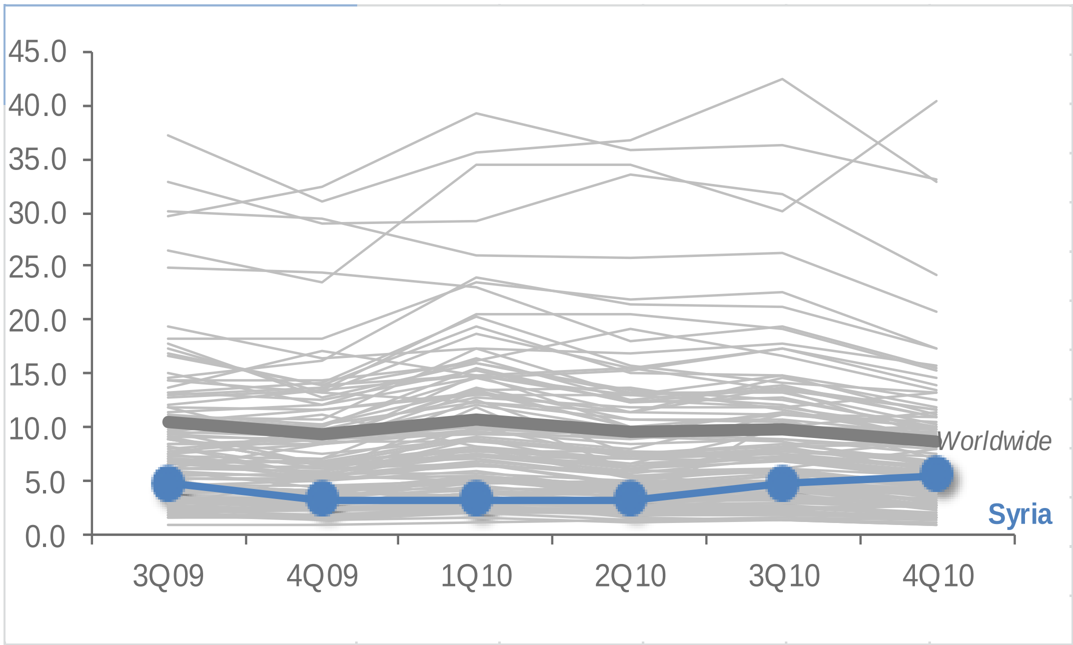
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Syria in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Syria and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.5 | 3.5 | 4.9 | 5.6 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.25 | | 0.89 | |
| Malware hosting sites per 1000 hosts | 0.76 | | | |
| Percentage of sites hosting drive-by downloads | 0.336% | 0.272% | 0.128% | |

## Infection Trends (CCM)

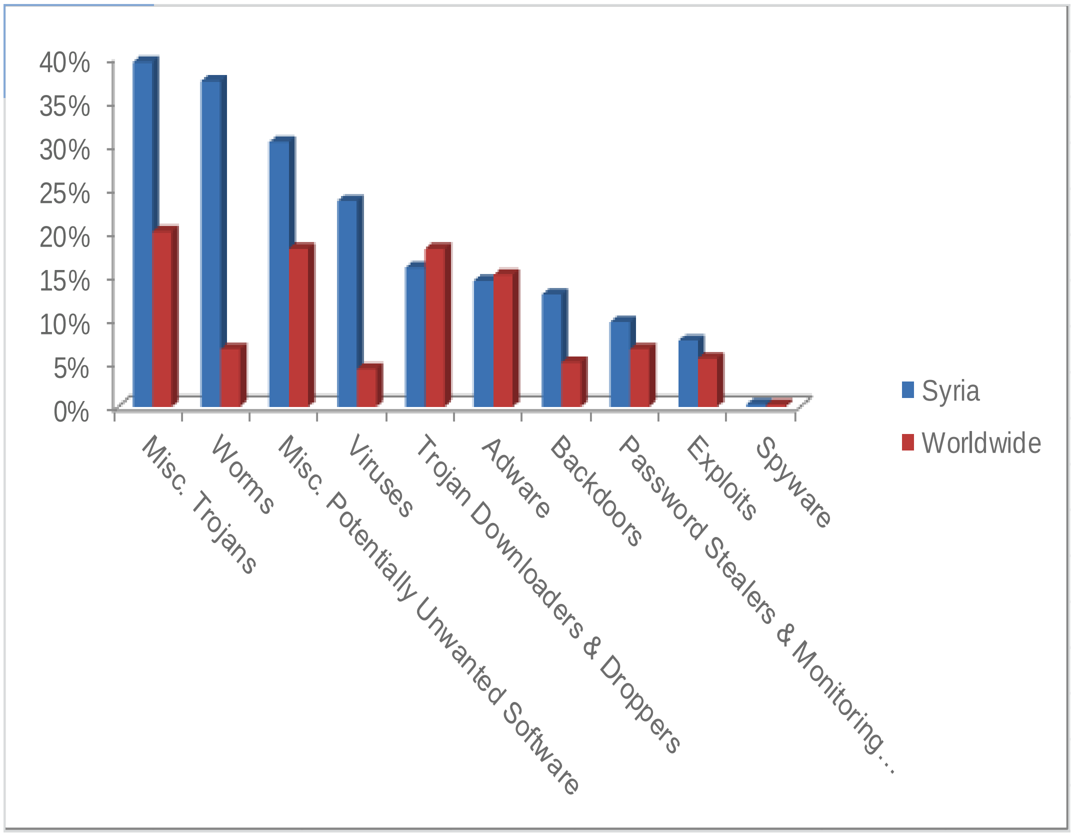
The MSRT detected malware on 5.6 of every 1,000 computers scanned in Syria in 4Q10 (a CCM score of 5.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Syria over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Syria and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Syria in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Syria in 4Q10 was Misc. Trojans, which affected 39.4 percent of all cleaned computers, up from 33.2 percent in 3Q10.
- The second most common category in Syria in 4Q10 was Worms, which affected 37.2 percent of all cleaned computers, up from 32.5 percent in 3Q10.
- The third most common category in Syria in 4Q10 was Misc. Potentially Unwanted Software, which affected 30.2 percent of all cleaned computers, up from 23.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Syria in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Sality | 22.9% |
| 2 | Win32/Autorun | 21.1% |
| 3 | Win32/Stuxnet | 10.3% |
| 4 | Win32/Agent | 9.6% |
| 5 | JS/Pornpop | 9.2% |
| 6 | Win32/Rimecud | 8.9% |
| 7 | Win32/Keygen | 7.5% |
| 8 | Win32/Conficker | 6.8% |
| 9 | Win32/Taterf | 6.6% |
| 10 | CplLnk | 6.0% |

- The most common threat family in Syria in 4Q10 was Win32/Sality, which affected 22.9 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The second most common threat family in Syria in 4Q10 was Win32/Autorun, which affected 21.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Syria in 4Q10 was Win32/Stuxnet, which affected 10.3 percent of cleaned computers. Win32/Stuxnet is a multi-component family that spreads via removable volumes by exploiting the vulnerability addressed by Microsoft Security Bulletin MS10-046.
- The fourth most common threat family in Syria in 4Q10 was Win32/Agent, which affected 9.6 percent of cleaned computers. Win32/Agent is a generic detection for a number of trojans that may perform different malicious functions. The functionality exhibited by this family is highly variable.

# Taiwan

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

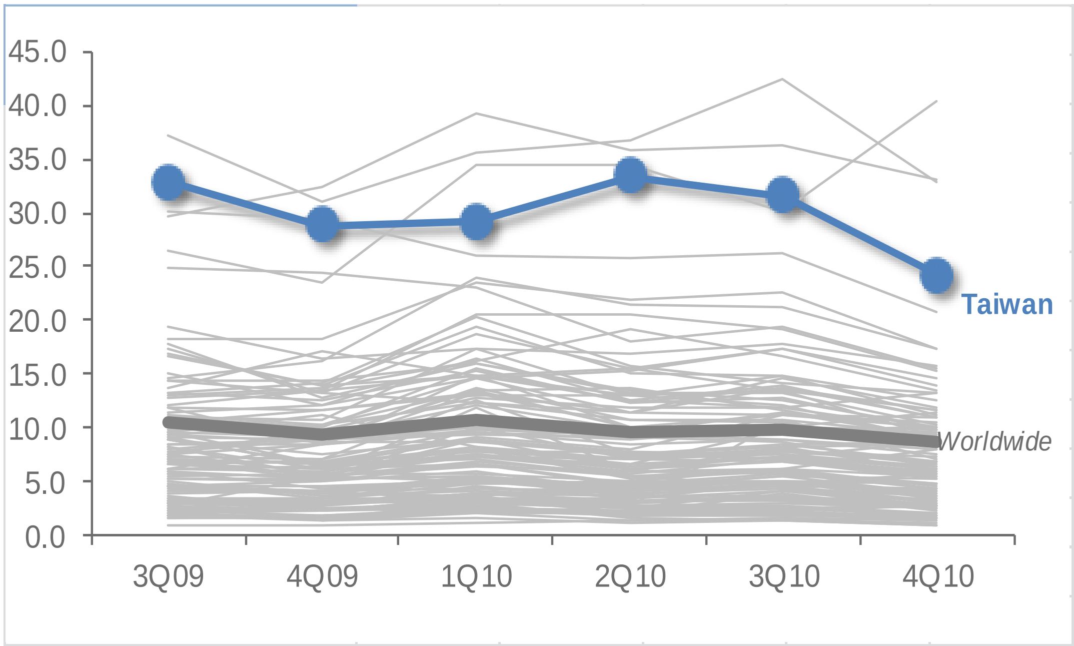
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Taiwan in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Taiwan and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">29.3</td><td colspan="3">33.5</td><td colspan="3">31.7</td><td colspan="3">24.3</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.79</td><td colspan="6">0.33</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.01</td><td colspan="6">1.74</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.266%</td><td colspan="4">0.143%</td><td colspan="4">0.138%</td></tr>
</table>

## Infection Trends (CCM)

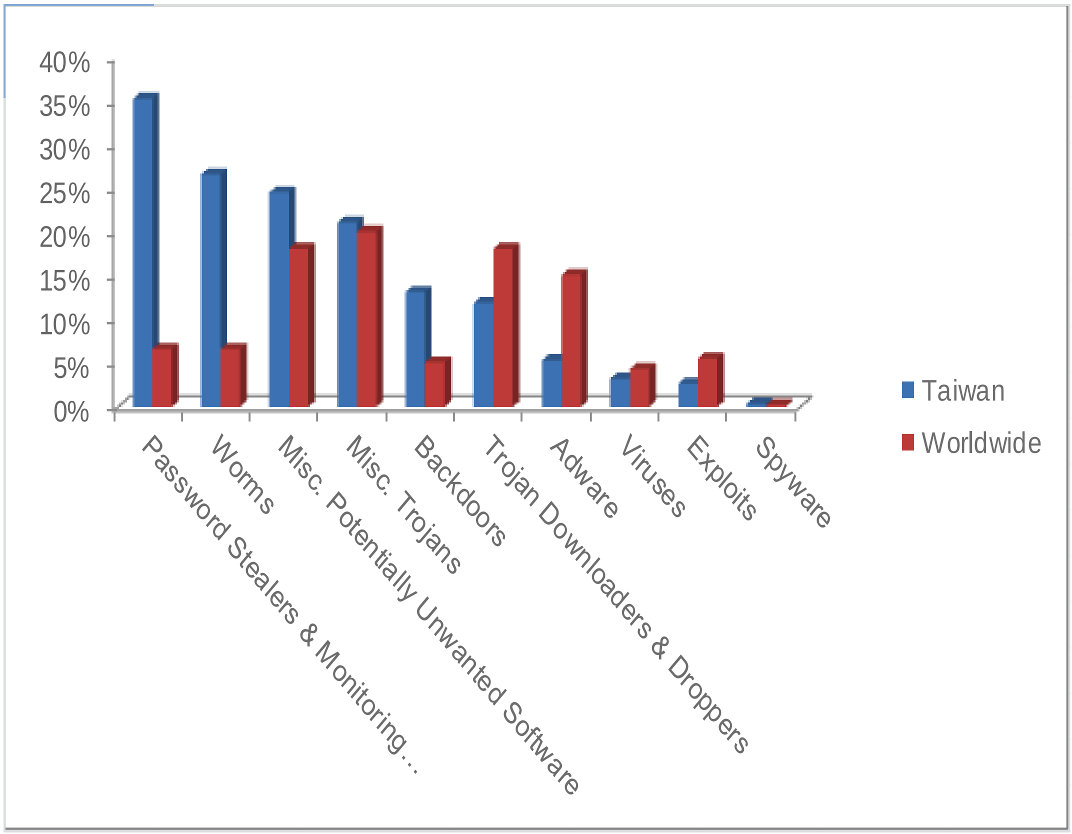
The MSRT detected malware on 24.3 of every 1,000 computers scanned in Taiwan in 4Q10 (a CCM score of 24.3, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Taiwan over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Taiwan and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Taiwan in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Taiwan in 4Q10 was Password Stealers & Monitoring Tools, which affected 35.2 percent of all cleaned computers, down from 41.7 percent in 3Q10.
- The second most common category in Taiwan in 4Q10 was Worms, which affected 26.5 percent of all cleaned computers, down from 34.7 percent in 3Q10.
- The third most common category in Taiwan in 4Q10 was Misc. Potentially Unwanted Software, which affected 24.5 percent of all cleaned computers, up from 20.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Taiwan in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Frethog | 28.2% |
| 2 | Win32/Taterf | 16.2% |
| 3 | Win32/Autorun | 12.2% |
| 4 | Win32/Rimecud | 9.0% |
| 5 | Win32/Magania | 6.3% |
| 6 | Win32/Hupigon | 5.2% |
| 7 | Win32/Conficker | 4.9% |
| 8 | Win32/Keygen | 4.5% |
| 9 | Win32/IRCbot | 3.9% |
| 10 | Win32/Agent | 3.7% |

- The most common threat family in Taiwan in 4Q10 was Win32/Frethog, which affected 28.2 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.
- The second most common threat family in Taiwan in 4Q10 was Win32/Taterf, which affected 16.2 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The third most common threat family in Taiwan in 4Q10 was Win32/Autorun, which affected 12.2 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common threat family in Taiwan in 4Q10 was Win32/Rimecud, which affected 9.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Tanzania

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

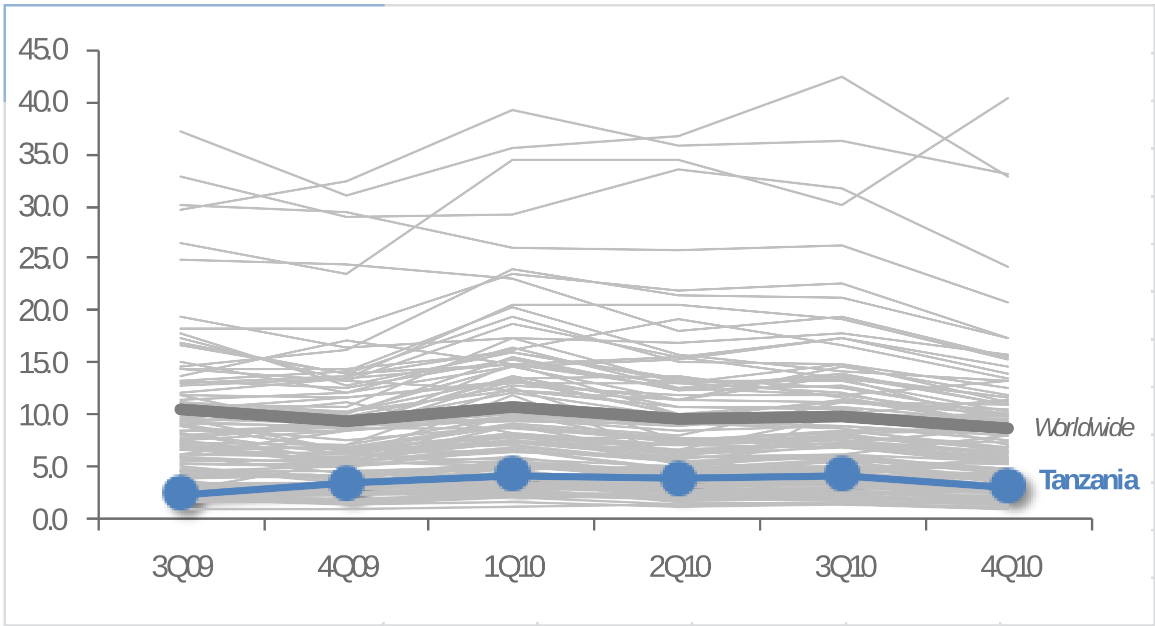
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Tanzania in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Tanzania and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 4.3 | 3.9 | 4.3 | 3.1 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.04 | | | |
| Malware hosting sites per 1000 hosts | 0.33 | | | |
| Percentage of sites hosting drive-by downloads | 5.540% | 0.432% | 0.190% | |

## Infection Trends (CCM)

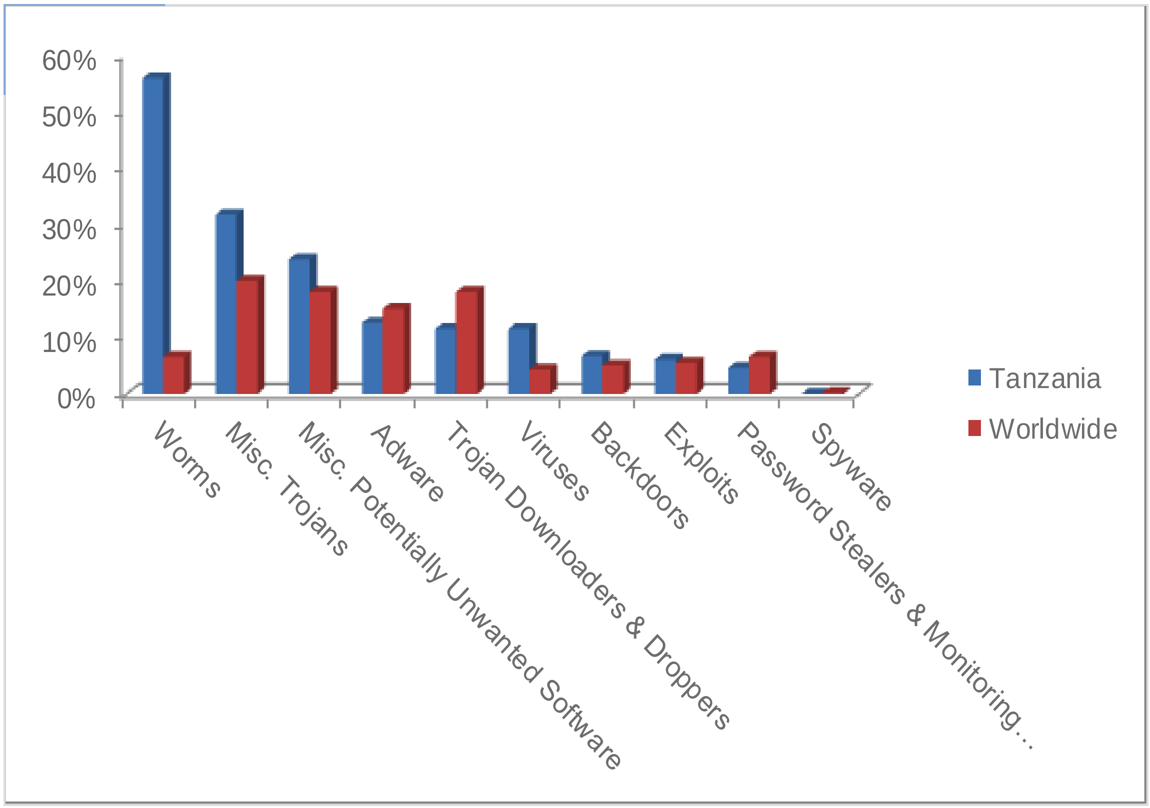
The MSRT detected malware on 3.1 of every 1,000 computers scanned in Tanzania in 4Q10 (a CCM score of 3.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Tanzania over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Tanzania and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Tanzania in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Tanzania in 4Q10 was Worms, which affected 55.9 percent of all cleaned computers, down from 64.6 percent in 3Q10.
- The second most common category in Tanzania in 4Q10 was Misc. Trojans, which affected 31.7 percent of all cleaned computers, up from 24.6 percent in 3Q10.
- The third most common category in Tanzania in 4Q10 was Misc. Potentially Unwanted Software, which affected 23.8 percent of all cleaned computers, up from 22.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Tanzania in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 43.1% |
| 2 | Win32/Autorun | 20.5% |
| 3 | Win32/Vobfus | 10.2% |
| 4 | Win32/Virut | 6.6% |
| 5 | Win32/Folstart | 6.3% |
| 6 | JS/Pornpop | 5.7% |
| 7 | Win32/Sality | 5.2% |
| 8 | Win32/Taterf | 5.1% |
| 9 | Win32/Hamweq | 5.1% |
| 10 | CplLnk | 4.3% |

- The most common threat family in Tanzania in 4Q10 was Win32/Rimecud, which affected 43.1 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Tanzania in 4Q10 was Win32/Autorun, which affected 20.5 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Tanzania in 4Q10 was Win32/Vobfus, which affected 10.2 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Tanzania in 4Q10 was Win32/Virut, which affected 6.6 percent of cleaned computers. Win32/Virut is a family of file-infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server.

# Thailand

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

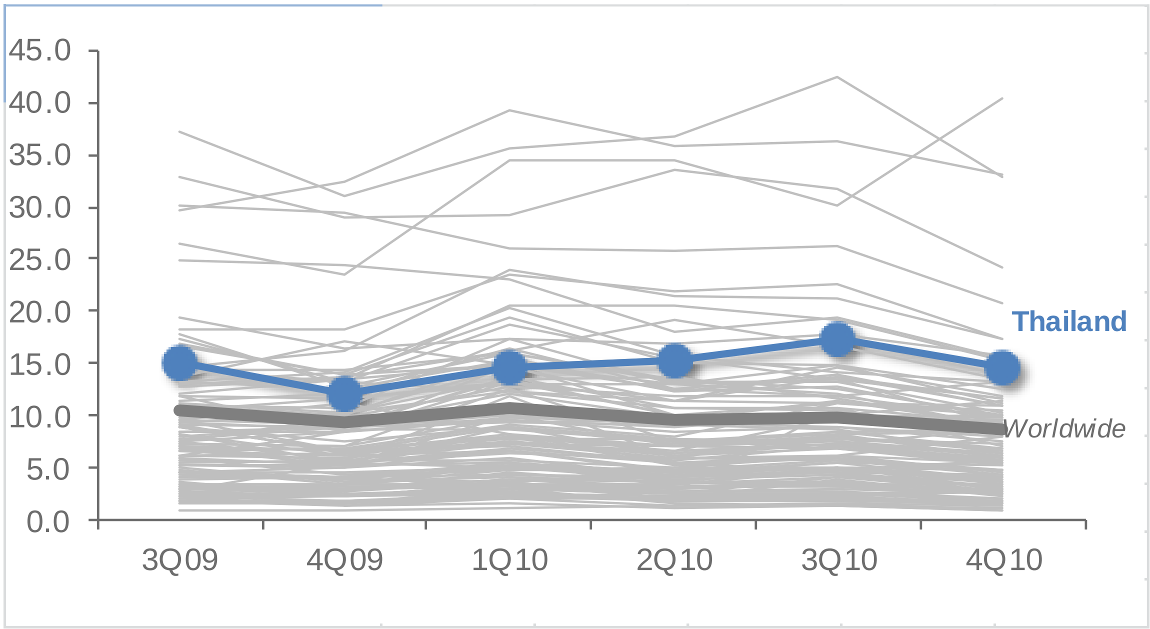
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Thailand in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Thailand and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">14.6</td><td colspan="3">15.3</td><td colspan="3">17.4</td><td colspan="3">14.5</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.96</td><td colspan="6">1.08</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.52</td><td colspan="6">1.64</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">1.024%</td><td colspan="4">0.679%</td><td colspan="4">0.517%</td></tr>
</table>

## Infection Trends (CCM)

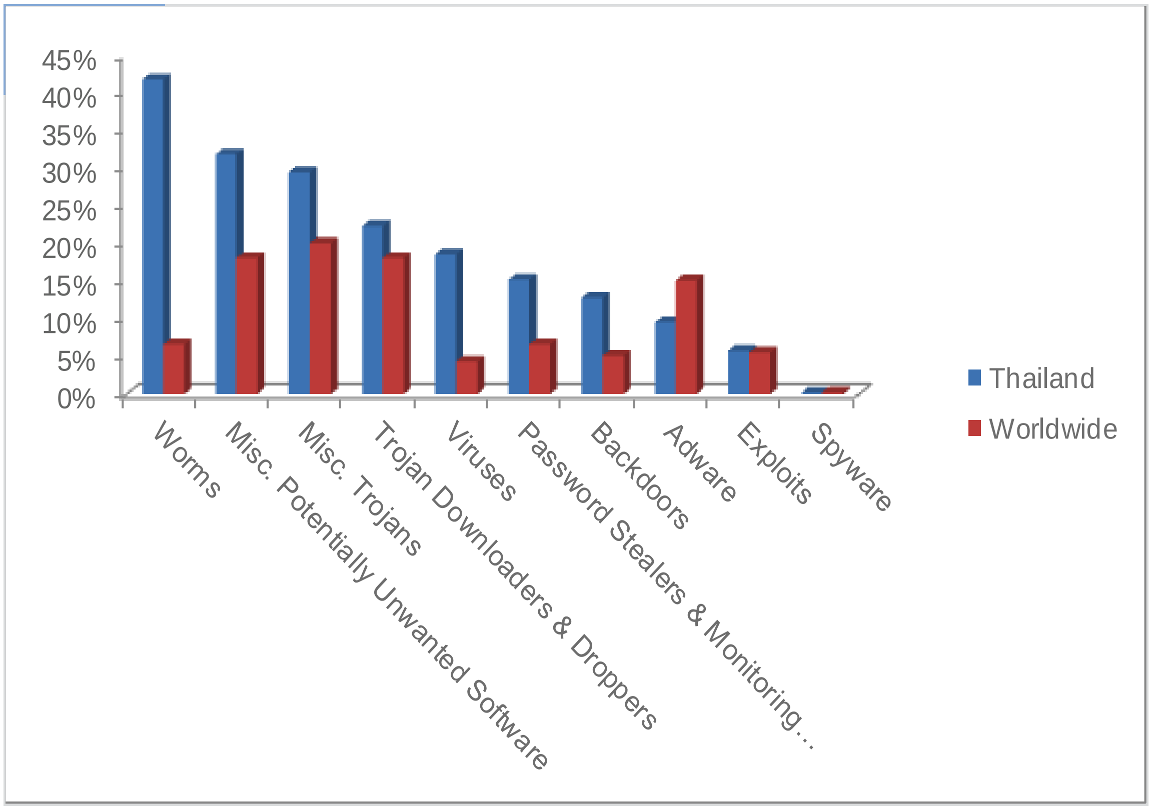
The MSRT detected malware on 14.5 of every 1,000 computers scanned in Thailand in 4Q10 (a CCM score of 14.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Thailand over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Thailand and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Thailand in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Thailand in 4Q10 was Worms, which affected 41.8 percent of all cleaned computers, down from 49.5 percent in 3Q10.
- The second most common category in Thailand in 4Q10 was Misc. Potentially Unwanted Software, which affected 31.8 percent of all cleaned computers, down from 31.9 percent in 3Q10.
- The third most common category in Thailand in 4Q10 was Misc. Trojans, which affected 29.4 percent of all cleaned computers, down from 30.1 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Thailand in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 19.9% |
| 2 | Win32/Sality | 17.4% |
| 3 | Win32/Taterf | 15.7% |
| 4 | Win32/Frethog | 11.1% |
| 5 | Win32/Conficker | 9.9% |
| 6 | Win32/Keygen | 8.1% |
| 7 | JS/Pornpop | 7.7% |
| 8 | Win32/Rimecud | 7.2% |
| 9 | Win32/Agent | 5.5% |
| 10 | Win32/FlyAgent | 5.2% |

- The most common threat family in Thailand in 4Q10 was Win32/Autorun, which affected 19.9 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Thailand in 4Q10 was Win32/Sality, which affected 17.4 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family in Thailand in 4Q10 was Win32/Taterf, which affected 15.7 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.
- The fourth most common threat family in Thailand in 4Q10 was Win32/Frethog, which affected 11.1 percent of cleaned computers. Win32/Frethog is a large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

# Trinidad and Tobago

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

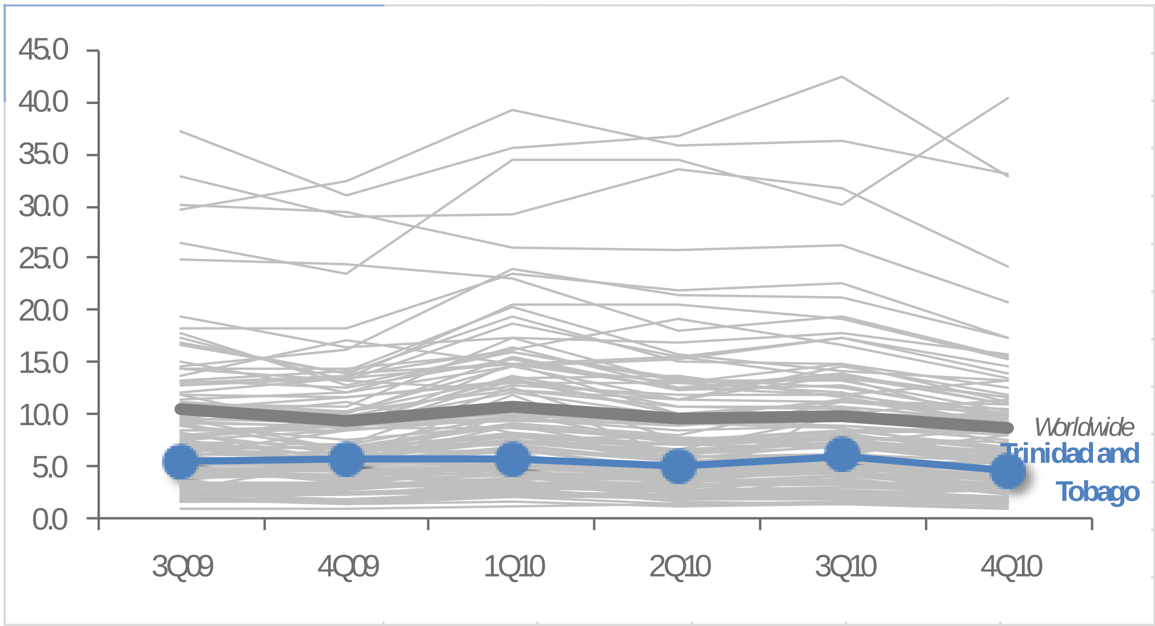
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Trinidad and Tobago in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Trinidad and Tobago and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">5.6</td><td colspan="3">5.1</td><td colspan="3">6.1</td><td colspan="3">4.6</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.47</td><td colspan="6"></td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.44</td><td colspan="6">0.82</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.072%</td><td colspan="4">0.044%</td><td colspan="4">0.074%</td></tr>
</table>

## Infection Trends (CCM)

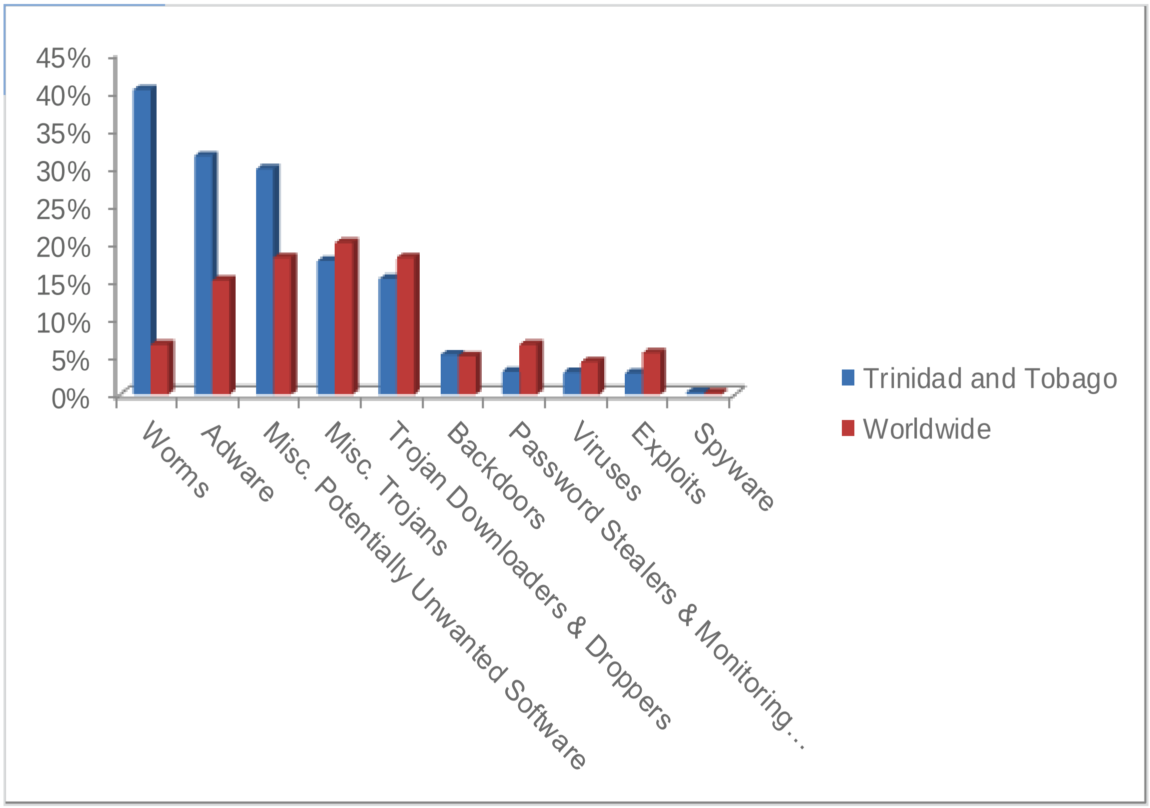
The MSRT detected malware on 4.6 of every 1,000 computers scanned in Trinidad and Tobago in 4Q10 (a CCM score of 4.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Trinidad and Tobago over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Trinidad and Tobago and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Trinidad and Tobago in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Trinidad and Tobago in 4Q10 was Worms, which affected 40.2 percent of all cleaned computers, down from 43.8 percent in 3Q10.
- The second most common category in Trinidad and Tobago in 4Q10 was Adware, which affected 31.5 percent of all cleaned computers, up from 27.7 percent in 3Q10.
- The third most common category in Trinidad and Tobago in 4Q10 was Misc. Potentially Unwanted Software, which affected 29.7 percent of all cleaned computers, up from 24.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Trinidad and Tobago in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 19.1% |
| 2 | Win32/Vobfus | 14.6% |
| 3 | Win32/ClickPotato | 12.2% |
| 4 | Win32/Zwangi | 11.1% |
| 5 | JS/Pornpop | 9.4% |
| 6 | Win32/Hotbar | 8.7% |
| 7 | Win32/Hamweq | 6.8% |
| 8 | Win32/Renos | 5.6% |
| 9 | Win32/Rimecud | 4.3% |
| 10 | Win32/VBInject | 3.2% |

- The most common threat family in Trinidad and Tobago in 4Q10 was Win32/Autorun, which affected 19.1 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Trinidad and Tobago in 4Q10 was Win32/Vobfus, which affected 14.6 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The third most common threat family in Trinidad and Tobago in 4Q10 was Win32/ClickPotato, which affected 12.2 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user’s browsing habits.
- The fourth most common threat family in Trinidad and Tobago in 4Q10 was Win32/Zwangi, which affected 11.1 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.

# Tunisia

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

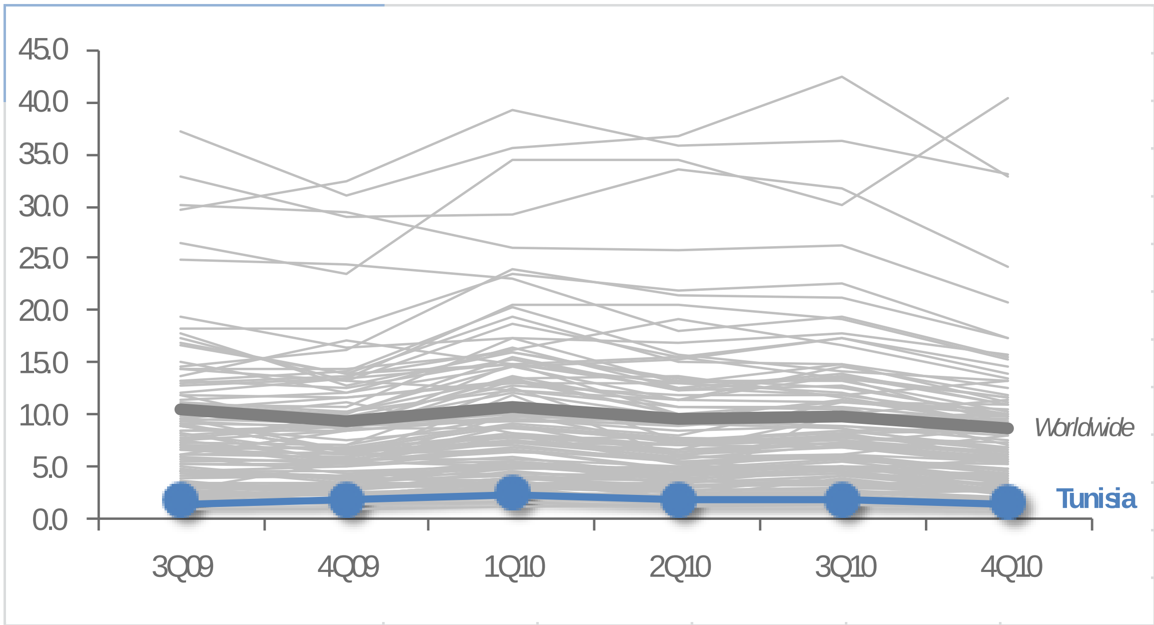
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Tunisia in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Tunisia and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">2.5</td><td colspan="3">1.8</td><td colspan="3">1.9</td><td colspan="3">1.6</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">13.30</td><td colspan="6"></td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">87.77</td><td colspan="6">7.98</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.238%</td><td colspan="4">0.139%</td><td colspan="4">0.130%</td></tr>
</table>

## Infection Trends (CCM)

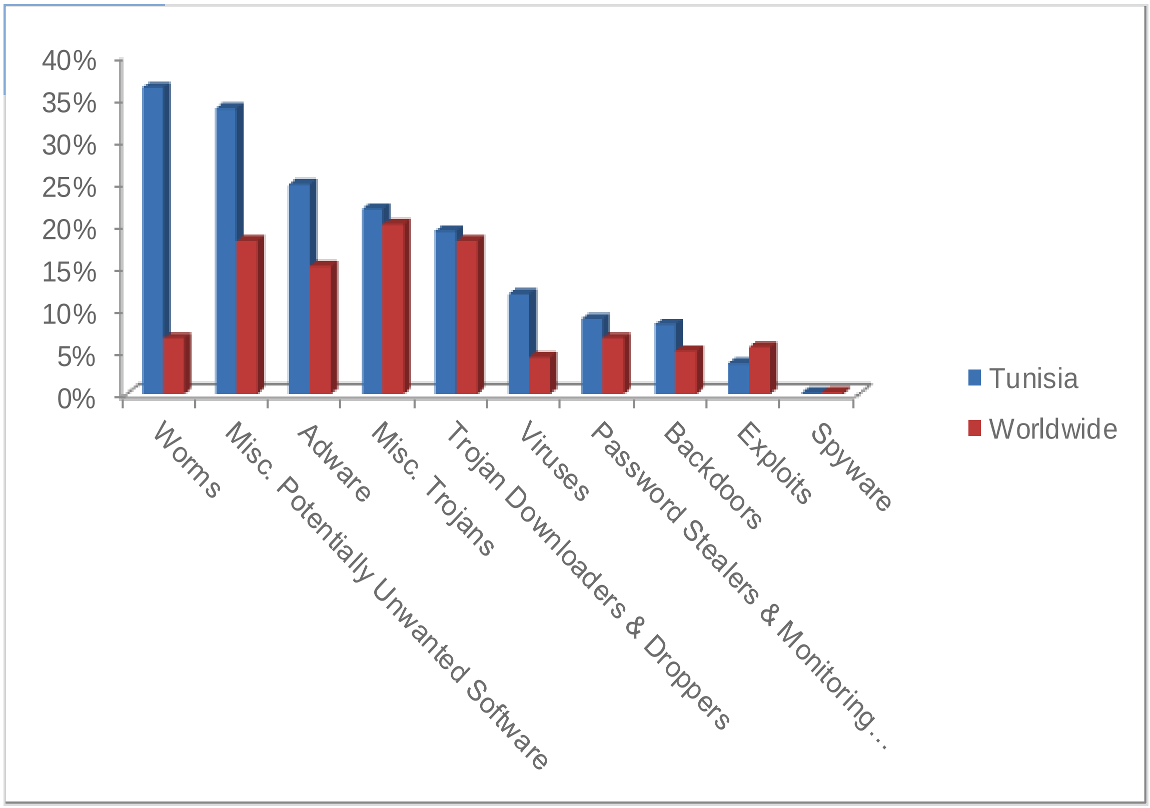
The MSRT detected malware on 1.6 of every 1,000 computers scanned in Tunisia in 4Q10 (a CCM score of 1.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Tunisia over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Tunisia and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Tunisia in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Tunisia in 4Q10 was Worms, which affected 36.1 percent of all cleaned computers, up from 35.2 percent in 3Q10.
- The second most common category in Tunisia in 4Q10 was Misc. Potentially Unwanted Software, which affected 33.7 percent of all cleaned computers, up from 25.8 percent in 3Q10.
- The third most common category in Tunisia in 4Q10 was Adware, which affected 24.7 percent of all cleaned computers, up from 23.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Tunisia in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 14.8% |
| 2 | Win32/ClickPotato | 13.6% |
| 3 | Win32/Zwangi | 13.5% |
| 4 | Win32/Vobfus | 12.7% |
| 5 | Win32/Renos | 9.4% |
| 6 | Win32/Taterf | 7.7% |
| 7 | Win32/Mabezat | 7.3% |
| 8 | Win32/Hotbar | 7.2% |
| 9 | Win32/Rimecud | 5.8% |
| 10 | Win32/Sality | 5.0% |

- The most common threat family in Tunisia in 4Q10 was Win32/Autorun, which affected 14.8 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Tunisia in 4Q10 was Win32/ClickPotato, which affected 13.6 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in Tunisia in 4Q10 was Win32/Zwangi, which affected 13.5 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in Tunisia in 4Q10 was Win32/Vobfus, which affected 12.7 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.

# Turkey

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

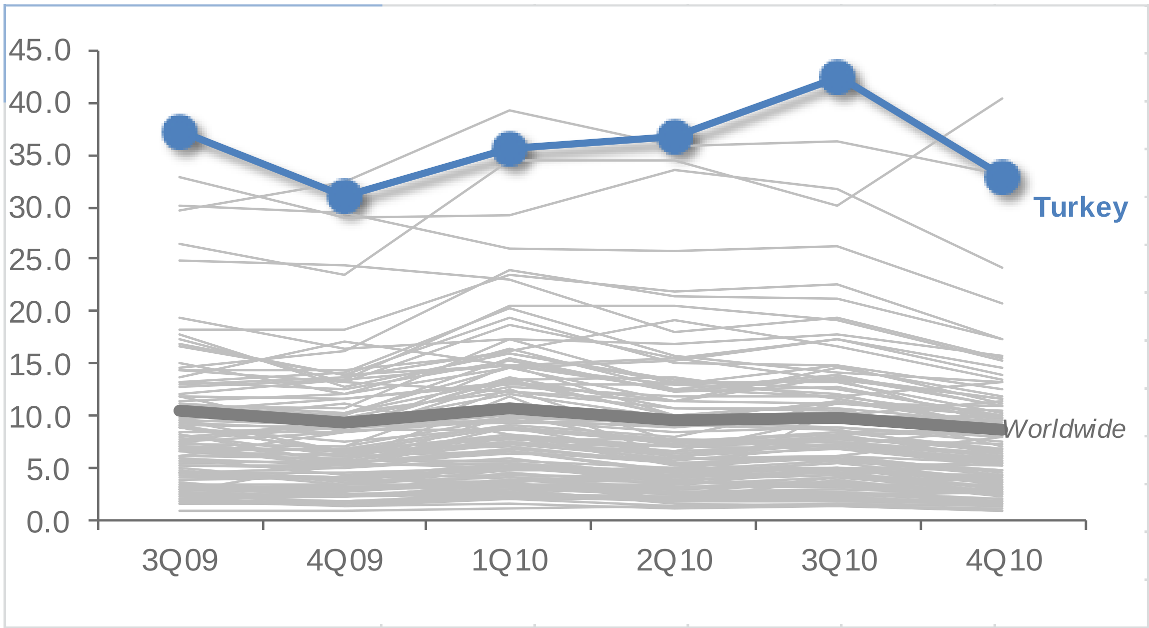
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Turkey in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Turkey and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">35.5</td><td colspan="3">36.6</td><td colspan="3">42.4</td><td colspan="3">32.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.42</td><td colspan="6">0.27</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">3.73</td><td colspan="6">3.35</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.419%</td><td colspan="4">0.312%</td><td colspan="4">0.231%</td></tr>
</table>

## Infection Trends (CCM)

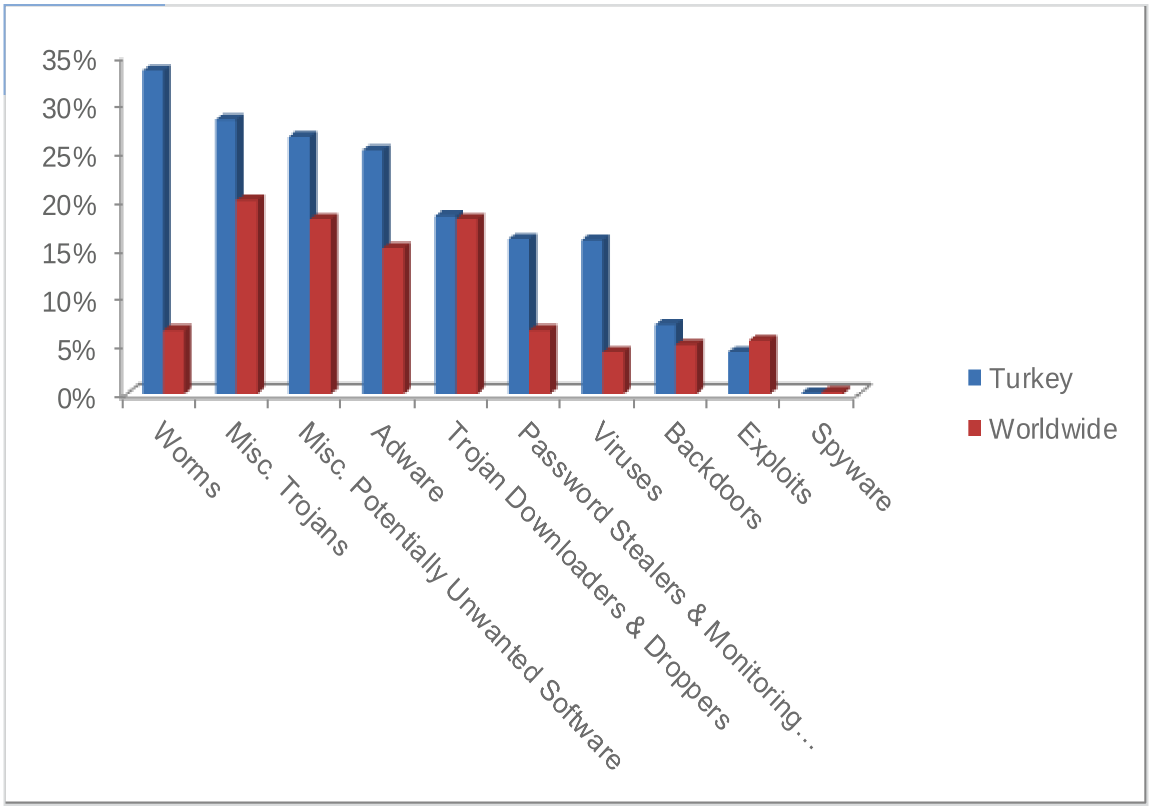
The MSRT detected malware on 32.8 of every 1,000 computers scanned in Turkey in 4Q10 (a CCM score of 32.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Turkey over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Turkey and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Turkey in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Turkey in 4Q10 was Worms, which affected 33.4 percent of all cleaned computers, down from 34.2 percent in 3Q10.
- The second most common category in Turkey in 4Q10 was Misc. Trojans, which affected 28.3 percent of all cleaned computers, down from 32.9 percent in 3Q10.
- The third most common category in Turkey in 4Q10 was Misc. Potentially Unwanted Software, which affected 26.6 percent of all cleaned computers, up from 24.8 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Turkey in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 21.8% |
| 2 | Win32/Sality | 15.9% |
| 3 | Win32/Autorun | 14.2% |
| 4 | Win32/Taterf | 13.1% |
| 5 | Win32/Frethog | 9.3% |
| 6 | Win32/Conficker | 5.5% |
| 7 | Win32/Rimecud | 5.1% |
| 8 | Win32/Keygen | 4.3% |
| 9 | Win32/Brontok | 3.5% |
| 10 | Win32/Renos | 3.0% |

- The most common threat family in Turkey in 4Q10 was JS/Pornpop, which affected 21.8 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in Turkey in 4Q10 was Win32/Sality, which affected 15.9 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The third most common threat family in Turkey in 4Q10 was Win32/Autorun, which affected 14.2 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The fourth most common threat family in Turkey in 4Q10 was Win32/Taterf, which affected 13.1 percent of cleaned computers. Win32/Taterf is a family of worms that spread through mapped drives to steal login and account details for popular online games.

# Uganda

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

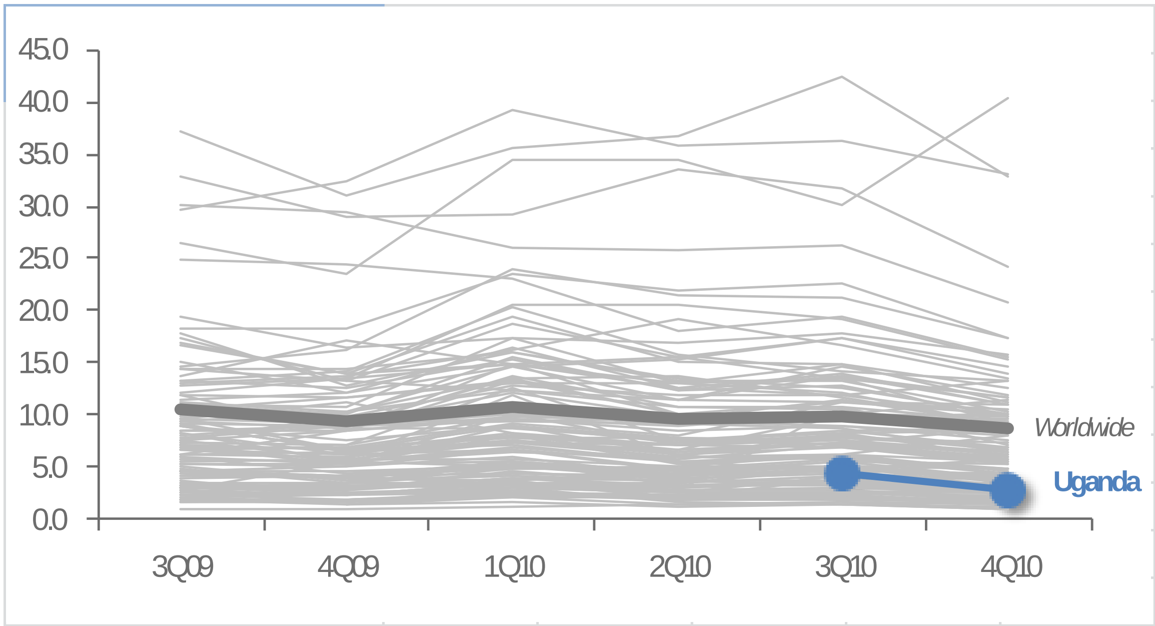
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Uganda in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Uganda and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3"></td><td colspan="3"></td><td colspan="3">4.4</td><td colspan="3">2.8</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">4.59</td><td colspan="6"></td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.83</td><td colspan="6"></td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.420%</td><td colspan="4">0.269%</td><td colspan="4">0.124%</td></tr>
</table>

## Infection Trends (CCM)

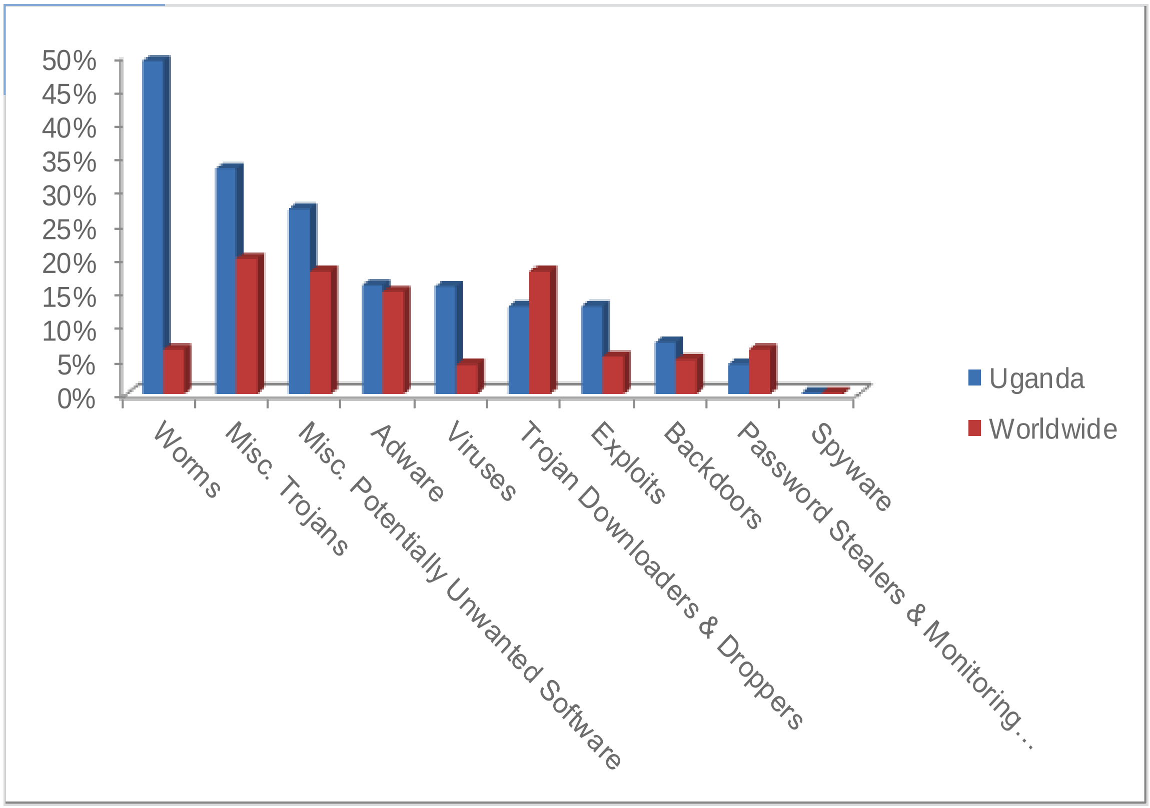
The MSRT detected malware on 2.8 of every 1,000 computers scanned in Uganda in 4Q10 (a CCM score of 2.8, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Uganda over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Uganda and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Uganda in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Uganda in 4Q10 was Worms, which affected 49.1 percent of all cleaned computers, down from 58.7 percent in 3Q10.
- The second most common category in Uganda in 4Q10 was Misc. Trojans, which affected 33.2 percent of all cleaned computers, up from 30.3 percent in 3Q10.
- The third most common category in Uganda in 4Q10 was Misc. Potentially Unwanted Software, which affected 27.3 percent of all cleaned computers, up from 24.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Uganda in 4Q10.

|  | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Rimecud | 36.5% |
| 2 | Win32/Autorun | 20.7% |
| 3 | Win32/Vobfus | 15.2% |
| 4 | Win32/Sality | 10.4% |
| 5 | CplLnk | 10.0% |
| 6 | JS/Pornpop | 7.5% |
| 7 | Win32/Folstart | 6.7% |
| 8 | Win32/Virut | 6.0% |
| 9 | Win32/ClickPotato | 4.6% |
| 10 | Win32/Zwangi | 4.3% |

- The most common threat family in Uganda in 4Q10 was Win32/Rimecud, which affected 36.5 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The second most common threat family in Uganda in 4Q10 was Win32/Autorun, which affected 20.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The third most common threat family in Uganda in 4Q10 was Win32/Vobfus, which affected 15.2 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in Uganda in 4Q10 was Win32/Sality, which affected 10.4 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# Ukraine

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

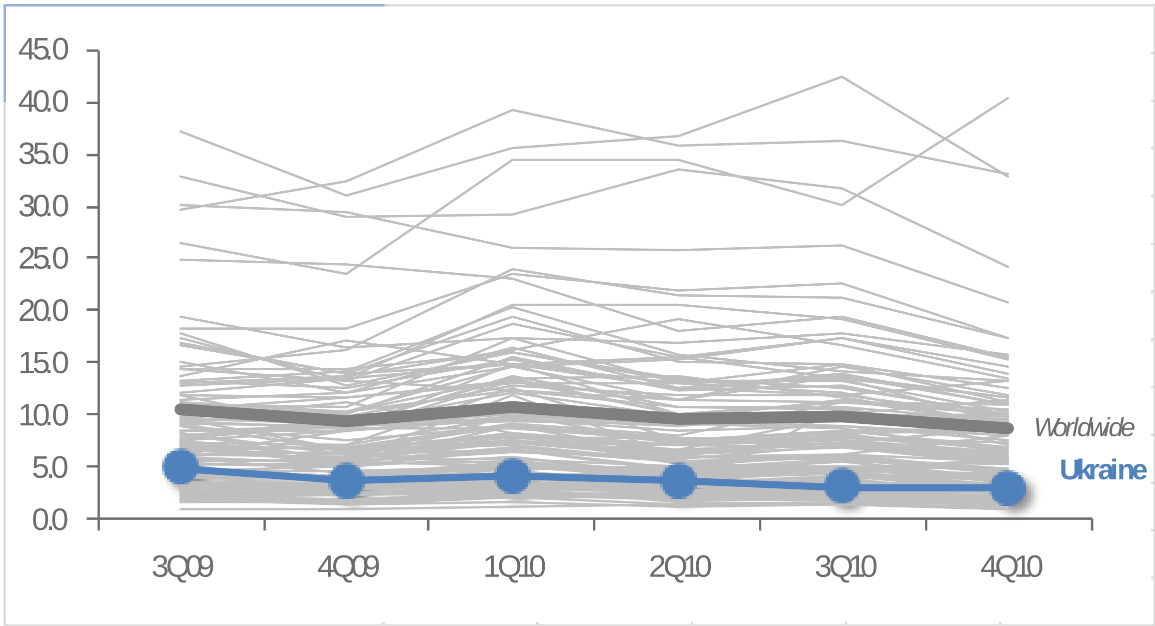
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Ukraine in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Ukraine and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">4.0</td><td colspan="3">3.6</td><td colspan="3">3.3</td><td colspan="3">3.1</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.46</td><td colspan="6">2.20</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">14.40</td><td colspan="6">37.38</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.288%</td><td colspan="4">0.100%</td><td colspan="4">0.094%</td></tr>
</table>

## Infection Trends (CCM)

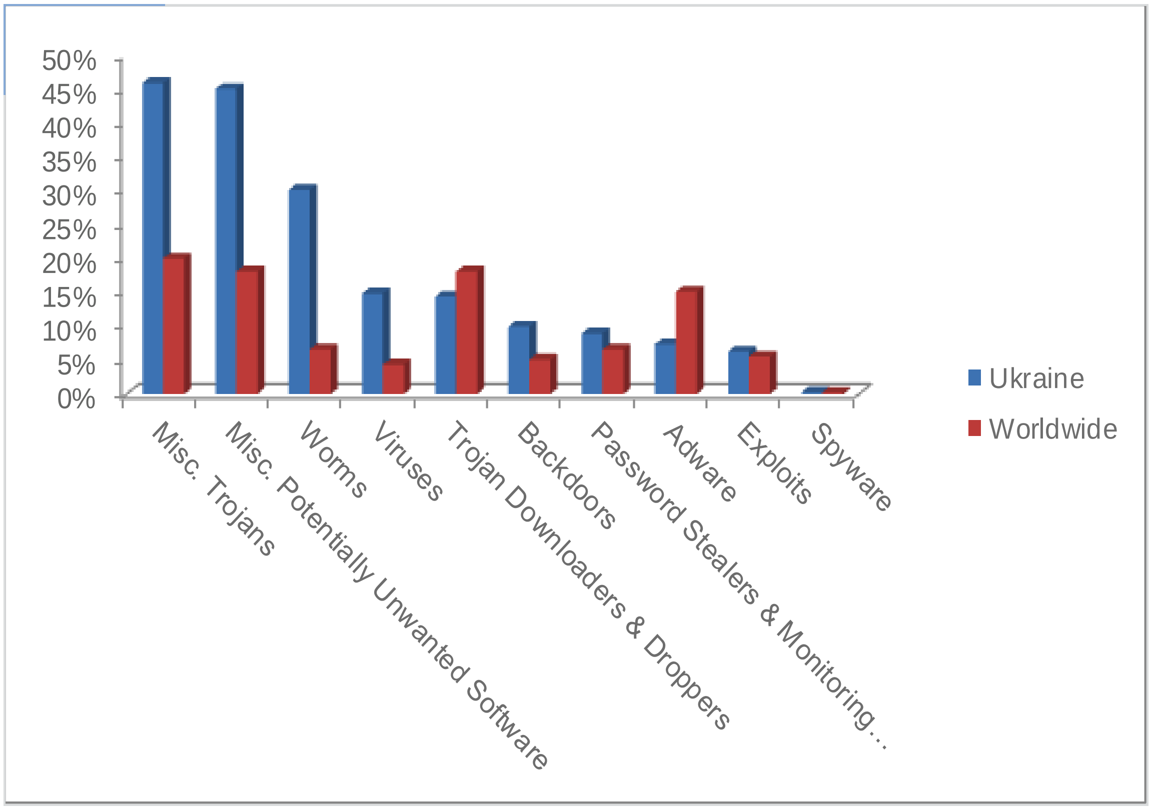
The MSRT detected malware on 3.1 of every 1,000 computers scanned in Ukraine in 4Q10 (a CCM score of 3.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Ukraine over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Ukraine and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Ukraine in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in Ukraine in 4Q10 was Misc. Trojans, which affected 45.9 percent of all cleaned computers, up from 42.3 percent in 3Q10.
- The second most common category in Ukraine in 4Q10 was Misc. Potentially Unwanted Software, which affected 45.0 percent of all cleaned computers, up from 40.3 percent in 3Q10.
- The third most common category in Ukraine in 4Q10 was Worms, which affected 30.1 percent of all cleaned computers, down from 35.6 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Ukraine in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 19.7% |
| 2 | Win32/Rimecud | 19.4% |
| 3 | Win32/Keygen | 11.9% |
| 4 | Win32/Obfuscator | 10.8% |
| 5 | Win32/Conficker | 9.5% |
| 6 | Win32/Sality | 6.8% |
| 7 | Bumat | 6.0% |
| 8 | Dynamer | 5.1% |
| 9 | Qhost | 4.3% |
| 10 | Orsam | 4.3% |

- The most common threat family in Ukraine in 4Q10 was Win32/Autorun, which affected 19.7 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Ukraine in 4Q10 was Win32/Rimecud, which affected 19.4 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in Ukraine in 4Q10 was Win32/Keygen, which affected 11.9 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.
- The fourth most common threat family in Ukraine in 4Q10 was Win32/Obfuscator, which affected 10.8 percent of cleaned computers. Win32/Obfuscator is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by anti-virus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

# United Arab Emirates

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

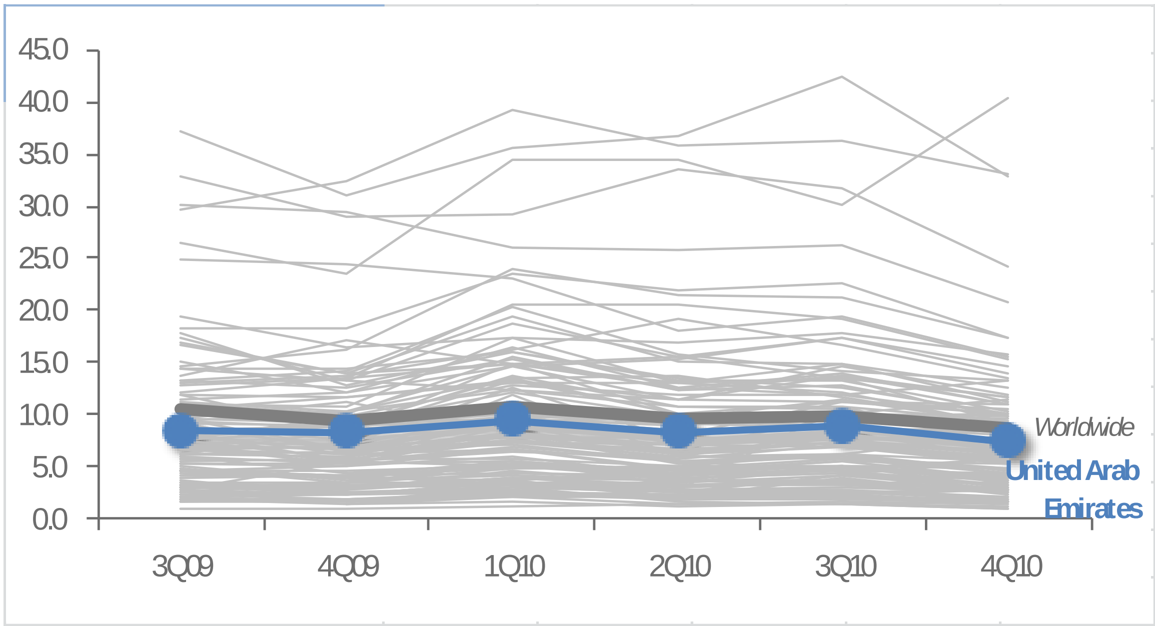
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in United Arab Emirates in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in United Arab Emirates and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 9.5 | 8.4 | 9.0 | 7.5 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.05 | | 0.10 | |
| Malware hosting sites per 1000 hosts | 0.19 | | 0.18 | |
| Percentage of sites hosting drive-by downloads | 1.020% | 0.132% | 0.119% | |

## Infection Trends (CCM)

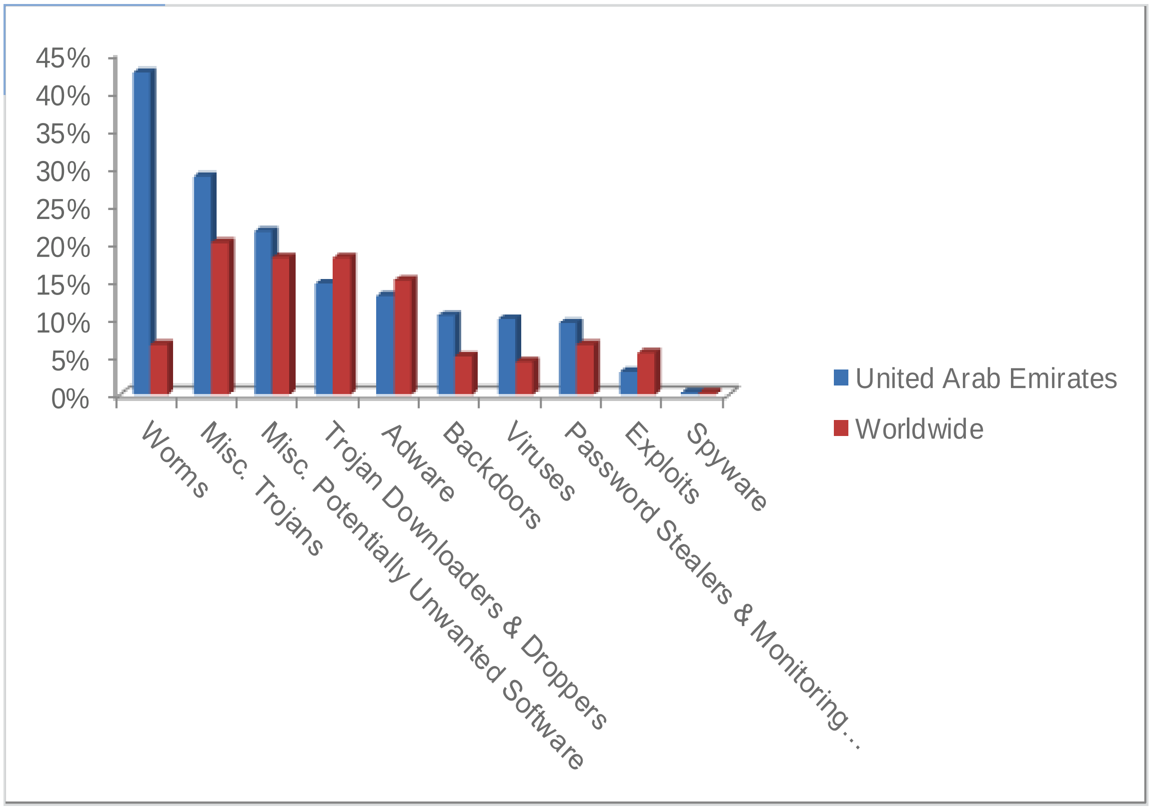
The MSRT detected malware on 7.5 of every 1,000 computers scanned in United Arab Emirates in 4Q10 (a CCM score of 7.5, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for United Arab Emirates over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in United Arab Emirates and worldwide



## Threat Categories

Malware and potentially unwanted software categories in United Arab Emirates in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in United Arab Emirates in 4Q10 was Worms, which affected 42.4 percent of all cleaned computers, down from 43.7 percent in 3Q10.
- The second most common category in United Arab Emirates in 4Q10 was Misc. Trojans, which affected 28.8 percent of all cleaned computers, up from 25.9 percent in 3Q10.
- The third most common category in United Arab Emirates in 4Q10 was Misc. Potentially Unwanted Software, which affected 21.5 percent of all cleaned computers, up from 18.5 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in United Arab Emirates in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 15.0% |
| 2 | Win32/Rimecud | 13.8% |
| 3 | Win32/Vobfus | 9.3% |
| 4 | Win32/Sality | 8.2% |
| 5 | Win32/Taterf | 7.4% |
| 6 | Win32/Renos | 5.4% |
| 7 | Win32/Conficker | 4.9% |
| 8 | Win32/IRCbot | 4.9% |
| 9 | Win32/Agent | 4.7% |
| 10 | Win32/Frethog | 4.6% |

- The most common threat family in United Arab Emirates in 4Q10 was Win32/Autorun, which affected 15.0 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in United Arab Emirates in 4Q10 was Win32/Rimecud, which affected 13.8 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.
- The third most common threat family in United Arab Emirates in 4Q10 was Win32/Vobfus, which affected 9.3 percent of cleaned computers. Win32/Vobfus is a family of worms that spreads via network drives and removable drives and download/executes arbitrary files. Downloaded files may include additional malware.
- The fourth most common threat family in United Arab Emirates in 4Q10 was Win32/Sality, which affected 8.2 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

# United Kingdom

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

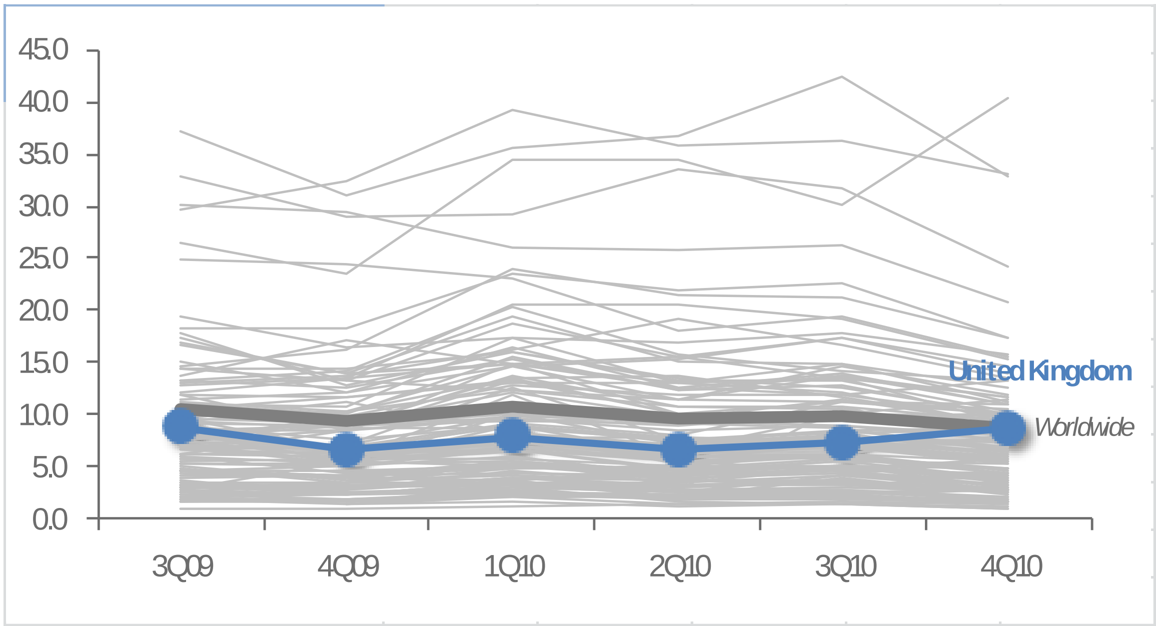
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in United Kingdom in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in United Kingdom and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">7.9</td><td colspan="3">6.7</td><td colspan="3">7.4</td><td colspan="3">8.7</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">1.52</td><td colspan="6">1.46</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">2.22</td><td colspan="6">1.58</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.133%</td><td colspan="4">0.034%</td><td colspan="4">0.049%</td></tr>
</table>

## Infection Trends (CCM)

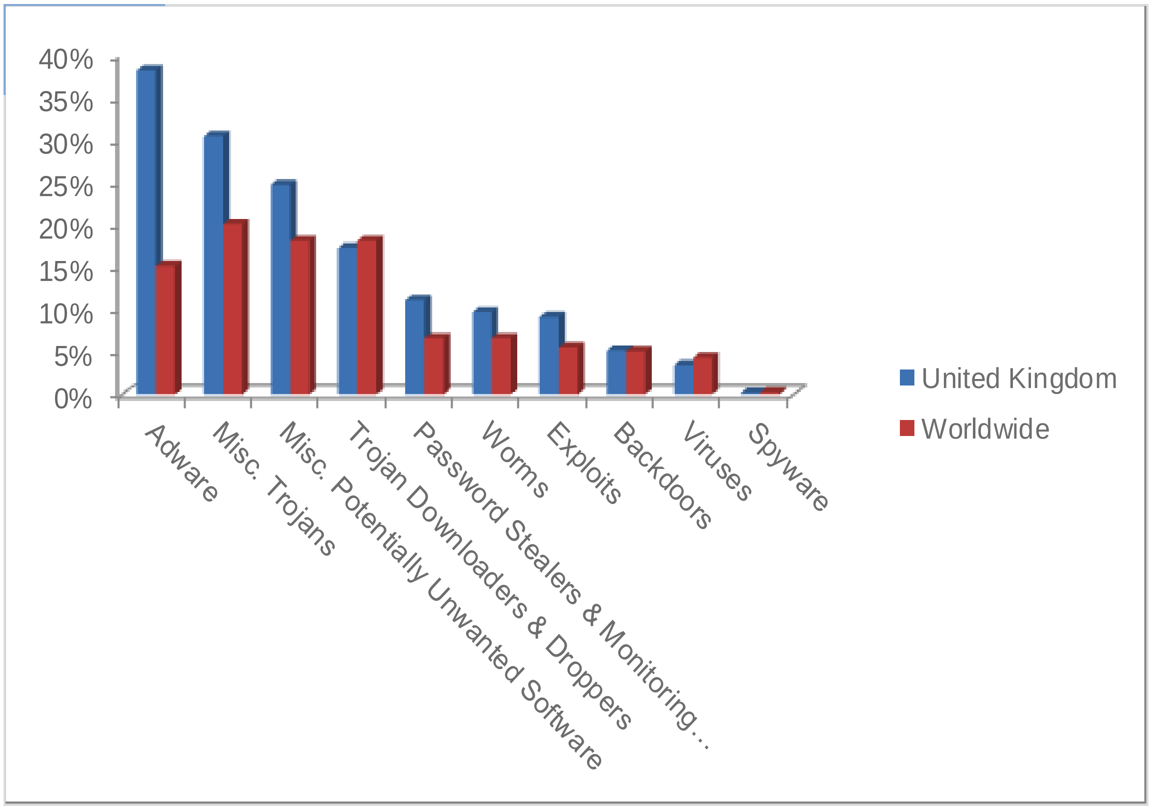
The MSRT detected malware on 8.7 of every 1,000 computers scanned in United Kingdom in 4Q10 (a CCM score of 8.7, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for United Kingdom over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in United Kingdom and worldwide



## Threat Categories

Malware and potentially unwanted software categories in United Kingdom in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in United Kingdom in 4Q10 was Adware, which affected 38.1 percent of all cleaned computers, down from 38.2 percent in 3Q10.
- The second most common category in United Kingdom in 4Q10 was Misc. Trojans, which affected 30.4 percent of all cleaned computers, down from 30.1 percent in 3Q10.
- The third most common category in United Kingdom in 4Q10 was Misc. Potentially Unwanted Software, which affected 24.6 percent of all cleaned computers, up from 23.9 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in United Kingdom in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 14.7% |
| 2 | Win32/ClickPotato | 13.4% |
| 3 | Win32/Zwangi | 11.4% |
| 4 | Win32/Hotbar | 11.4% |
| 5 | Win32/Zbot | 8.6% |
| 6 | Win32/Renos | 4.5% |
| 7 | Java/CVE-2008-5353 | 4.2% |
| 8 | Java/CVE-2009-3867 | 4.0% |
| 9 | Win32/FakeSpypro | 3.8% |
| 10 | Win32/Hiloti | 3.8% |

- The most common threat family in United Kingdom in 4Q10 was JS/Pornpop, which affected 14.7 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in United Kingdom in 4Q10 was Win32/ClickPotato, which affected 13.4 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in United Kingdom in 4Q10 was Win32/Zwangi, which affected 11.4 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in United Kingdom in 4Q10 was Win32/Hotbar, which affected 11.4 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

# United States

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

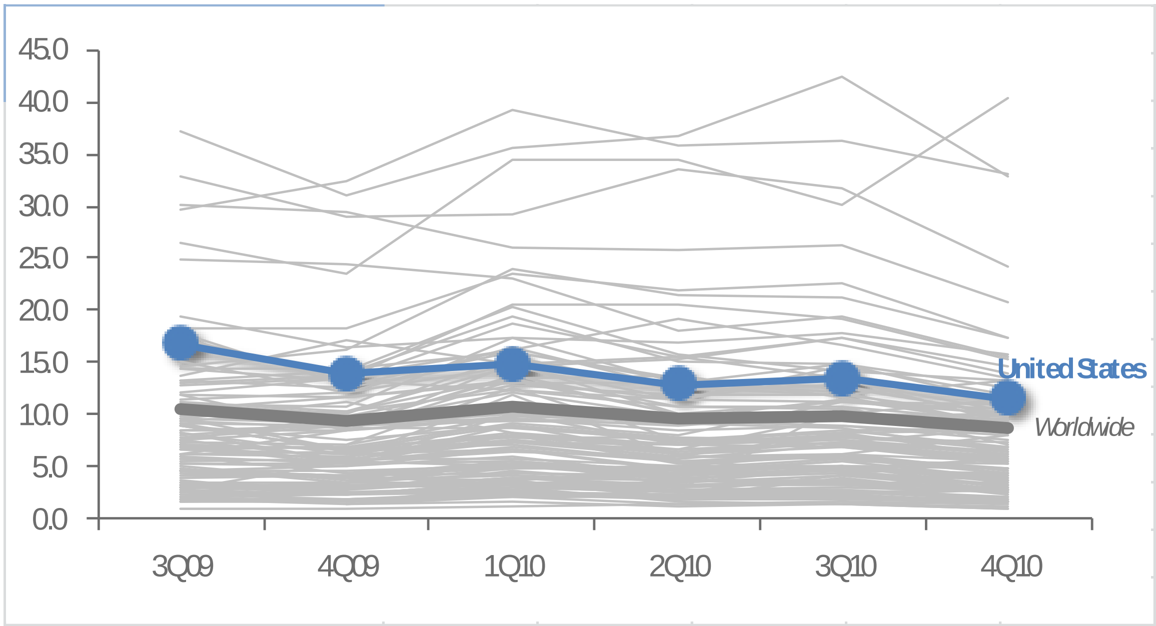
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in United States in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in United States and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">14.8</td><td colspan="3">12.9</td><td colspan="3">13.5</td><td colspan="3">11.6</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.45</td><td colspan="6">0.56</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">1.27</td><td colspan="6">2.38</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.122%</td><td colspan="4">0.032%</td><td colspan="4">0.007%</td></tr>
</table>

## Infection Trends (CCM)

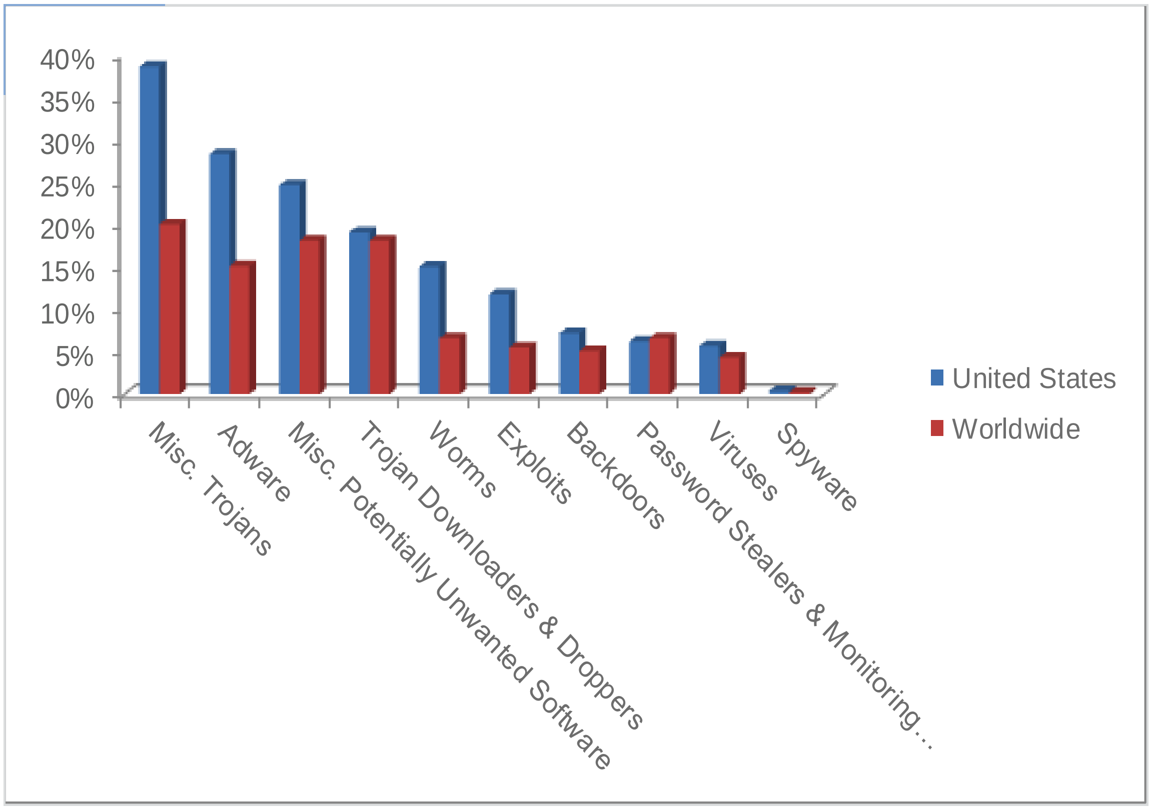
The MSRT detected malware on 11.6 of every 1,000 computers scanned in United States in 4Q10 (a CCM score of 11.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for United States over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in United States and worldwide



## Threat Categories

Malware and potentially unwanted software categories in United States in 4Q10, by percentage of cleaned computers affected



*Totals exceed 100 percent because some computers are affected by more than one kind of threat.*

- The most common category in United States in 4Q10 was Misc. Trojans, which affected 38.6 percent of all cleaned computers, down from 43.8 percent in 3Q10.
- The second most common category in United States in 4Q10 was Adware, which affected 28.3 percent of all cleaned computers, up from 23.0 percent in 3Q10.
- The third most common category in United States in 4Q10 was Misc. Potentially Unwanted Software, which affected 24.6 percent of all cleaned computers, up from 22.8 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in United States in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | JS/Pornpop | 11.5% |
| 2 | Win32/ClickPotato | 7.7% |
| 3 | Win32/Zwangi | 7.6% |
| 4 | Win32/Hotbar | 6.4% |
| 5 | Win32/Autorun | 6.3% |
| 6 | Win32/FakeSpypro | 5.4% |
| 7 | Win32/Renos | 5.1% |
| 8 | Java/CVE-2008-5353 | 4.8% |
| 9 | Win32/FakePAV | 4.4% |
| 10 | Java/CVE-2009-3867 | 4.2% |

- The most common threat family in United States in 4Q10 was JS/Pornpop, which affected 11.5 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The second most common threat family in United States in 4Q10 was Win32/ClickPotato, which affected 7.7 percent of cleaned computers. Win32/ClickPotato is a program that displays popup and notification-style advertisements based on the user's browsing habits.
- The third most common threat family in United States in 4Q10 was Win32/Zwangi, which affected 7.6 percent of cleaned computers. Win32/Zwangi is a program that runs as a service in the background and modifies Web browser settings to visit a particular website.
- The fourth most common threat family in United States in 4Q10 was Win32/Hotbar, which affected 6.4 percent of cleaned computers. Win32/Hotbar is adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.

# Uruguay

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

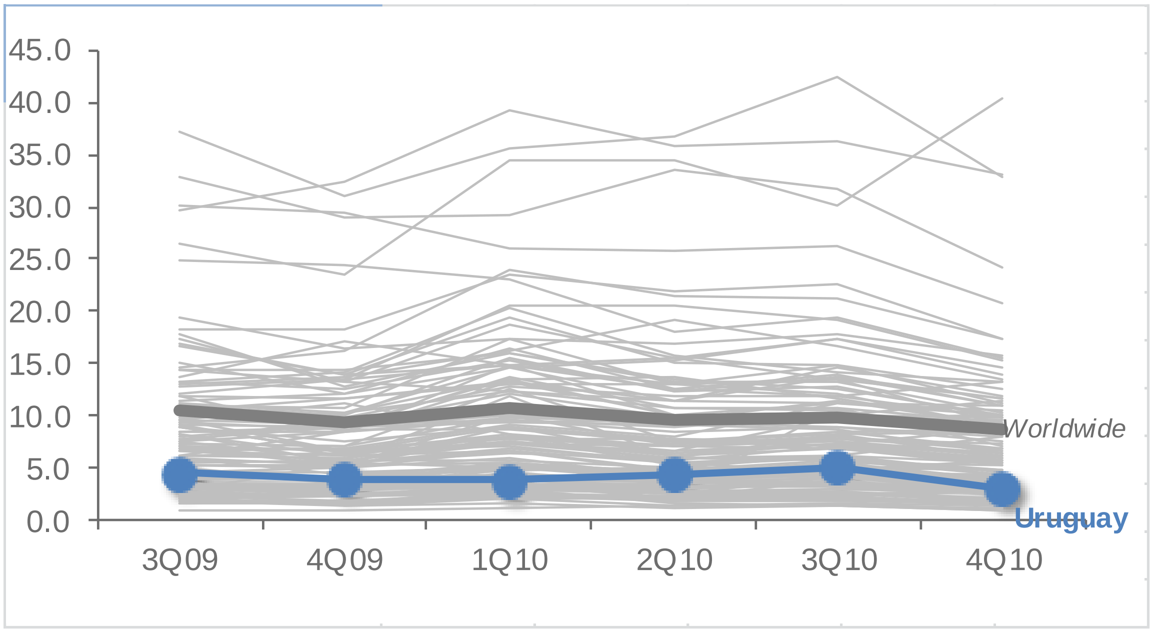
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Uruguay in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Uruguay and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 3.7 | 4.4 | 5.1 | 3.1 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 0.16 | | 0.06 | |
| Malware hosting sites per 1000 hosts | 0.06 | | 0.14 | |
| Percentage of sites hosting drive-by downloads | 0.095% | 0.051% | 0.061% | |

## Infection Trends (CCM)

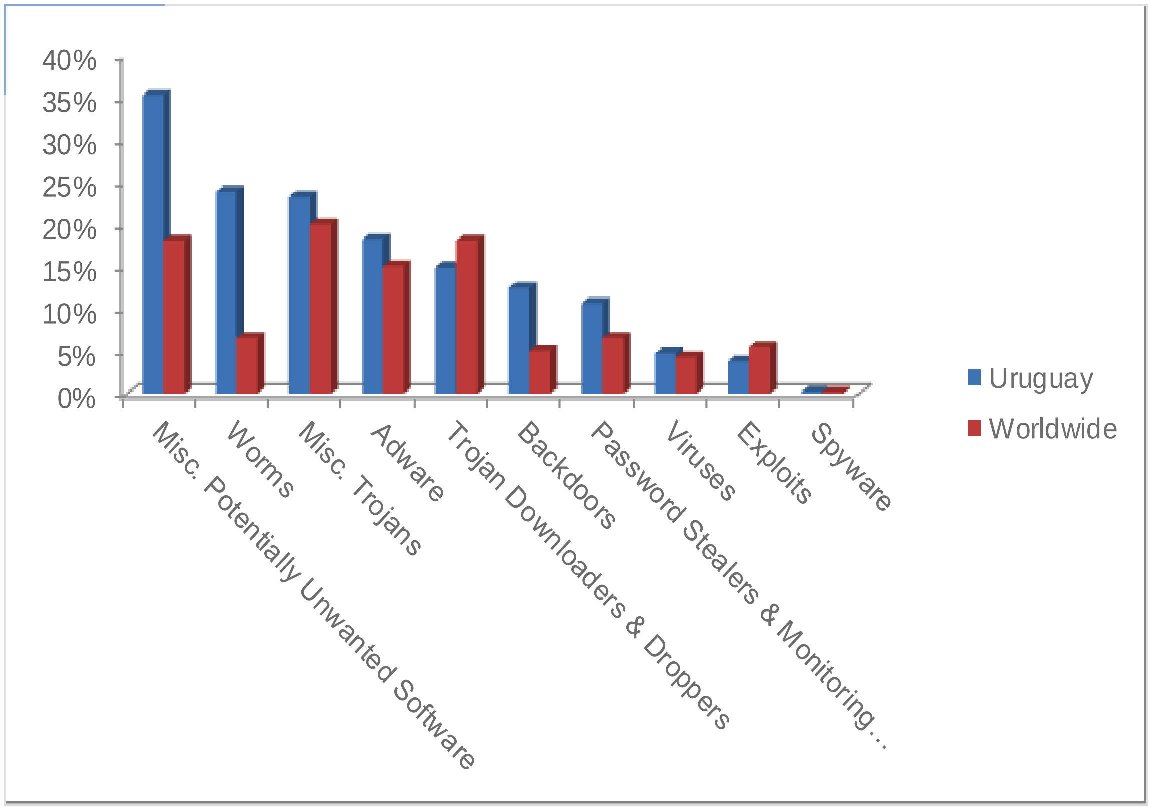
The MSRT detected malware on 3.1 of every 1,000 computers scanned in Uruguay in 4Q10 (a CCM score of 3.1, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Uruguay over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Uruguay and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Uruguay in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Uruguay in 4Q10 was Misc. Potentially Unwanted Software, which affected 35.2 percent of all cleaned computers, up from 34.1 percent in 3Q10.
- The second most common category in Uruguay in 4Q10 was Worms, which affected 23.8 percent of all cleaned computers, down from 28.5 percent in 3Q10.
- The third most common category in Uruguay in 4Q10 was Misc. Trojans, which affected 23.2 percent of all cleaned computers, up from 22.0 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Uruguay in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 12.4% |
| 2 | JS/Pornpop | 7.4% |
| 3 | Win32/Conficker | 7.1% |
| 4 | Win32/Keygen | 6.8% |
| 5 | Win32/IRCbot | 6.3% |
| 6 | Win32/Zwangi | 6.1% |
| 7 | Win32/Taterf | 5.4% |
| 8 | Win/Gabpath | 4.3% |
| 9 | Win32/Renos | 4.2% |
| 10 | Sdbot | 3.6% |

- The most common threat family in Uruguay in 4Q10 was Win32/Autorun, which affected 12.4 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Uruguay in 4Q10 was JS/Pornpop, which affected 7.4 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Uruguay in 4Q10 was Win32/Conficker, which affected 7.1 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The fourth most common threat family in Uruguay in 4Q10 was Win32/Keygen, which affected 6.8 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.

# Venezuela

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

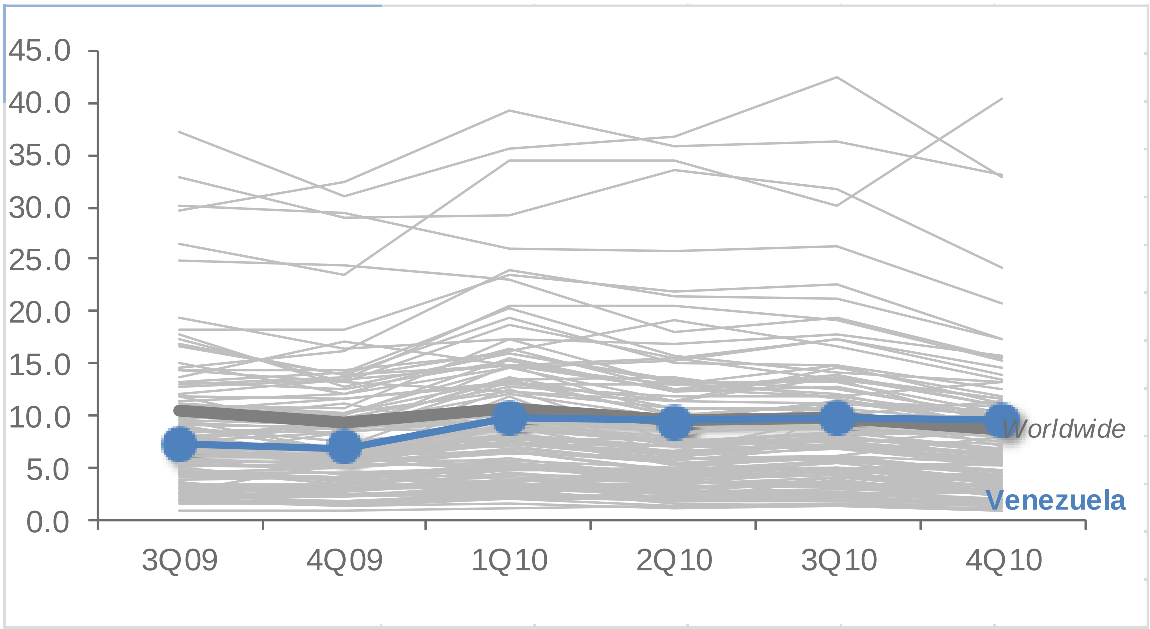
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Venezuela in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Venezuela and around the world.

<table>
<tr><th>Metric</th><th colspan="3">1Q10</th><th colspan="3">2Q10</th><th colspan="3">3Q10</th><th colspan="3">4Q10</th></tr>
<tr><td>Host infection rate (CCM)</td><td colspan="3">9.9</td><td colspan="3">9.5</td><td colspan="3">9.8</td><td colspan="3">9.7</td></tr>
<tr><td>CCM Worldwide</td><td colspan="3">10.8</td><td colspan="3">9.6</td><td colspan="3">9.9</td><td colspan="3">8.7</td></tr>
<tr><td>Phishing sites per 1000 hosts</td><td colspan="6">0.51</td><td colspan="6">1.04</td></tr>
<tr><td>Malware hosting sites per 1000 hosts</td><td colspan="6">0.48</td><td colspan="6">0.48</td></tr>
<tr><td>Percentage of sites hosting drive-by downloads</td><td colspan="4">0.110%</td><td colspan="4">0.110%</td><td colspan="4">0.112%</td></tr>
</table>

## Infection Trends (CCM)

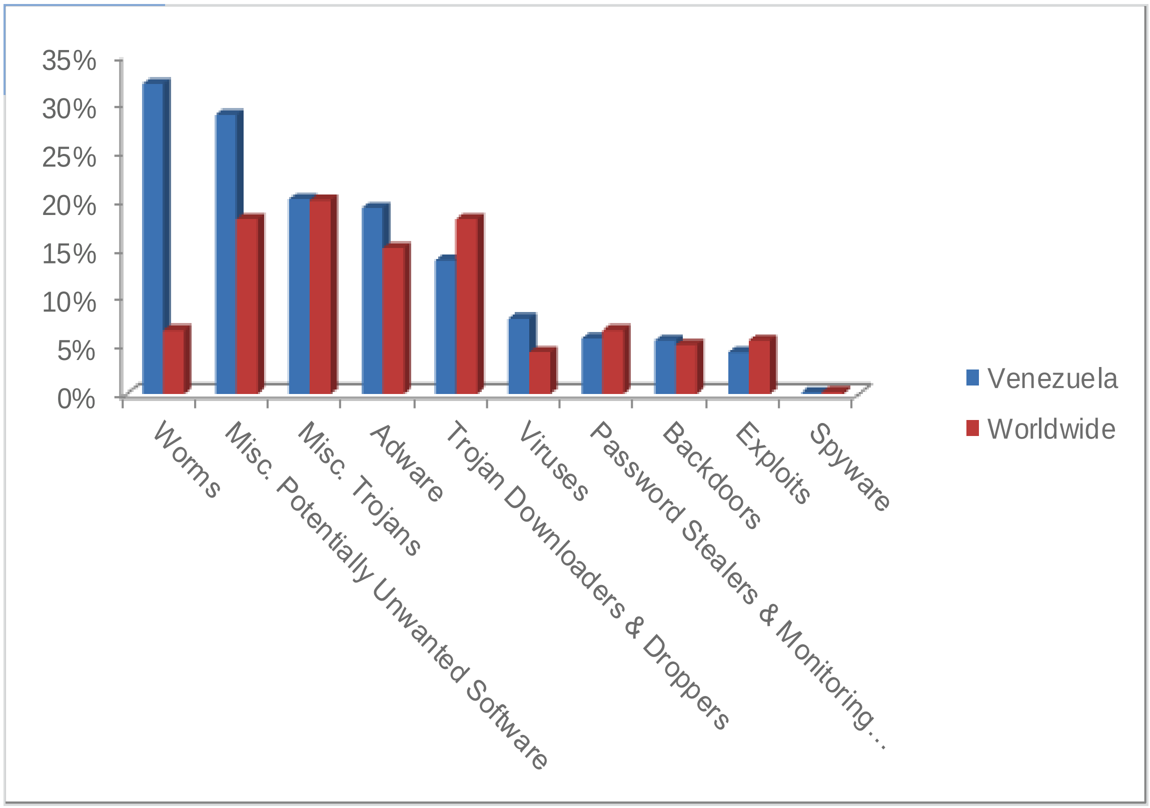
The MSRT detected malware on 9.7 of every 1,000 computers scanned in Venezuela in 4Q10 (a CCM score of 9.7, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Venezuela over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Venezuela and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Venezuela in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Venezuela in 4Q10 was Worms, which affected 32.0 percent of all cleaned computers, down from 50.9 percent in 3Q10.
- The second most common category in Venezuela in 4Q10 was Misc. Potentially Unwanted Software, which affected 28.8 percent of all cleaned computers, down from 36.6 percent in 3Q10.
- The third most common category in Venezuela in 4Q10 was Misc. Trojans, which affected 20.1 percent of all cleaned computers, down from 20.7 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Venezuela in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 15.3% |
| 2 | JS/Pornpop | 12.2% |
| 3 | Win32/Conficker | 11.3% |
| 4 | Win32/Rimecud | 7.0% |
| 5 | Win32/Zwangi | 4.9% |
| 6 | Win32/Sality | 4.8% |
| 7 | Win32/Taterf | 4.5% |
| 8 | Win32/Keygen | 4.1% |
| 9 | Win32/Silly_P2P | 3.6% |
| 10 | Win32/Vobfus | 3.2% |

- The most common threat family in Venezuela in 4Q10 was Win32/Autorun, which affected 15.3 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Venezuela in 4Q10 was JS/Pornpop, which affected 12.2 percent of cleaned computers. JS/Pornpop is a generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
- The third most common threat family in Venezuela in 4Q10 was Win32/Conficker, which affected 11.3 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The fourth most common threat family in Venezuela in 4Q10 was Win32/Rimecud, which affected 7.0 percent of cleaned computers. Win32/Rimecud is a family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

# Vietnam

The global threat landscape is evolving. Malware and potentially unwanted software has become more regional, and different locations around the world exhibit different threat patterns.

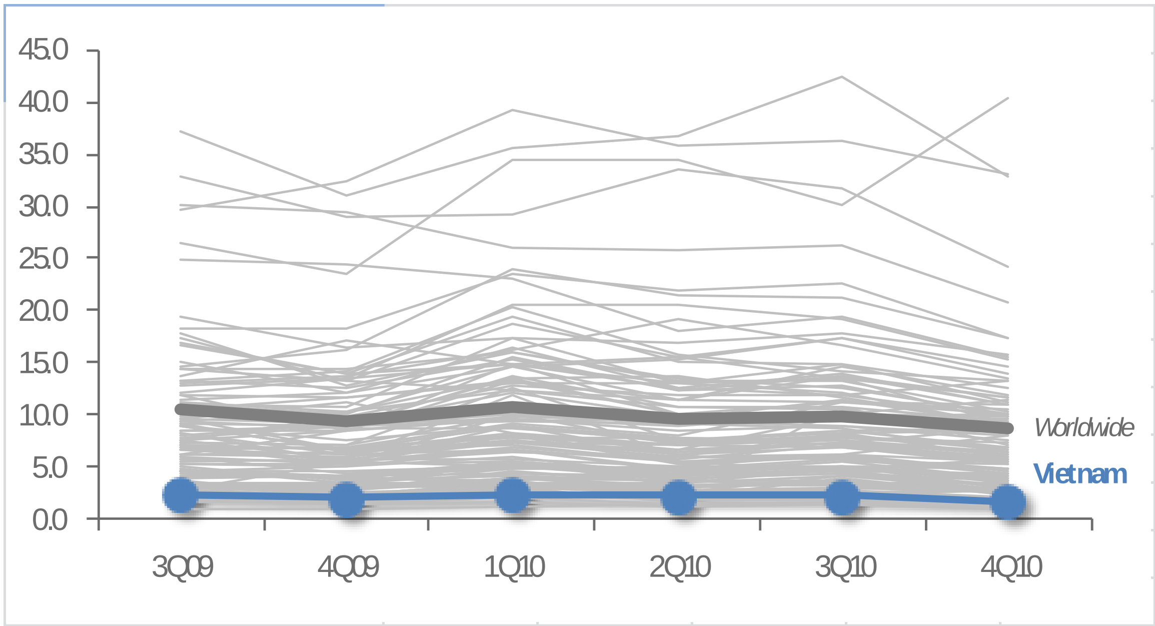
The statistics presented here are generated from telemetric data produced by Microsoft security programs and services running on computers in Vietnam in 4Q10 and previous quarters. See the *Security Intelligence Report* website at http://www.microsoft.com/sir for more information about threats in Vietnam and around the world.

| Metric | 1Q10 | 2Q10 | 3Q10 | 4Q10 |
|---|---|---|---|---|
| Host infection rate (CCM) | 2.2 | 2.1 | 2.1 | 1.6 |
| CCM Worldwide | 10.8 | 9.6 | 9.9 | 8.7 |
| Phishing sites per 1000 hosts | 10.80 | | 10.33 | |
| Malware hosting sites per 1000 hosts | 16.62 | | 30.78 | |
| Percentage of sites hosting drive-by downloads | 0.294% | 0.202% | 0.220% | |

## Infection Trends (CCM)

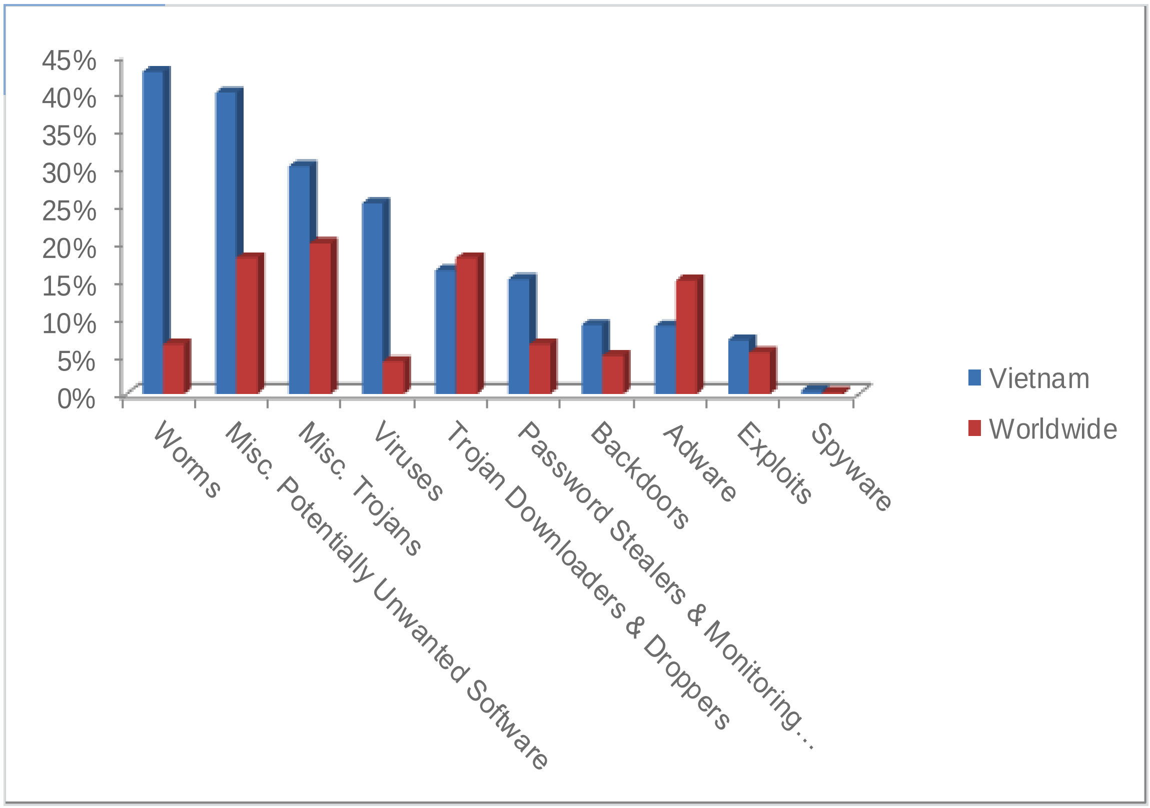
The MSRT detected malware on 1.6 of every 1,000 computers scanned in Vietnam in 4Q10 (a CCM score of 1.6, compared to the 4Q10 average worldwide CCM of 8.7). The figure below shows the CCM trend for Vietnam over the last 6 quarters, compared to 117 other countries and regions and to the world as a whole.

CCM infection trends in Vietnam and worldwide



## Threat Categories

Malware and potentially unwanted software categories in Vietnam in 4Q10, by percentage of cleaned computers affected



Totals exceed 100 percent because some computers are affected by more than one kind of threat.

- The most common category in Vietnam in 4Q10 was Worms, which affected 42.7 percent of all cleaned computers, up from 41.6 percent in 3Q10.
- The second most common category in Vietnam in 4Q10 was Misc. Potentially Unwanted Software, which affected 40.0 percent of all cleaned computers, up from 32.7 percent in 3Q10.
- The third most common category in Vietnam in 4Q10 was Misc. Trojans, which affected 30.2 percent of all cleaned computers, up from 28.4 percent in 3Q10.

## Threat Families

The top 10 malware and potentially unwanted software families in Vietnam in 4Q10.

| | Family | Percent of Computers Affected |
|---|---|---|
| 1 | Win32/Autorun | 27.3% |
| 2 | Win32/Conficker | 18.8% |
| 3 | Win32/Sality | 14.9% |
| 4 | Win32/Keygen | 11.6% |
| 5 | Win32/VB | 10.1% |
| 6 | Win32/Virut | 7.6% |
| 7 | PerfectKeylogger | 7.4% |
| 8 | Win32/Rimecud | 6.2% |
| 9 | Win32/Renos | 5.2% |
| 10 | Meredrop | 5.0% |

- The most common threat family in Vietnam in 4Q10 was Win32/Autorun, which affected 27.3 percent of cleaned computers. Win32/Autorun is a family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
- The second most common threat family in Vietnam in 4Q10 was Win32/Conficker, which affected 18.8 percent of cleaned computers. Win32/Conficker is a worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.
- The third most common threat family in Vietnam in 4Q10 was Win32/Sality, which affected 14.9 percent of cleaned computers. Win32/Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
- The fourth most common threat family in Vietnam in 4Q10 was Win32/Keygen, which affected 11.6 percent of cleaned computers. Win32/Keygen is a generic detection for tools that generate product keys for illegally obtained versions of various software products.

Microsoft®

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security