Microsoft

An in-depth perspective on software vulnerabilities and exploits, malware, potentially unwanted software, and malicious websites

Microsoft Security Intelligence Report

Volume 14

July through December, 2012

Hong Kong S.A.R.

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

The statistics presented here are generated by Microsoft security programs and services running on computers in Hong Kong S.A.R. in 4Q12 and previous quarters. This data is provided from administrators or users who choose to opt in to provide data to Microsoft, using IP address geolocation to determine country or region.

Infection rate statistics for Hong Kong S.A.R.

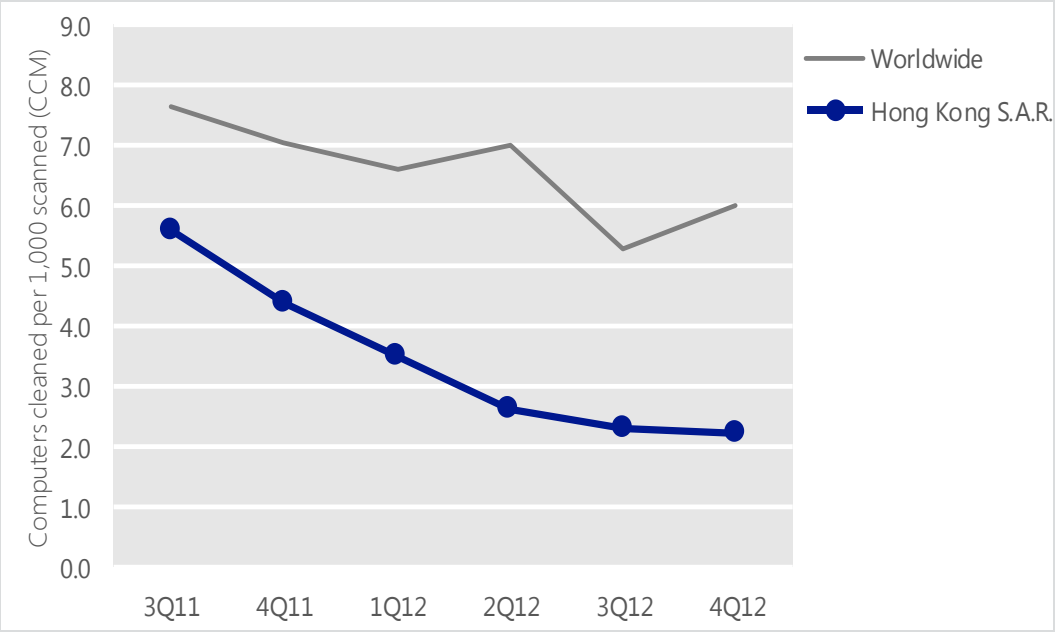
Metric	1Q12	2Q12	3Q12	4Q12
Computers cleaned per 1,000 MSRT executions (CCM)	3.5	2.6	2.3	2.2
Worldwide average CCM	6.6	7.0	5.3	6.0

See the Security Intelligence Report website at www.microsoft.com/sir for more information about threats in Hong Kong S.A.R. and around the world, and for explanations of the methods and terms used here.

Infection trends (CCM)

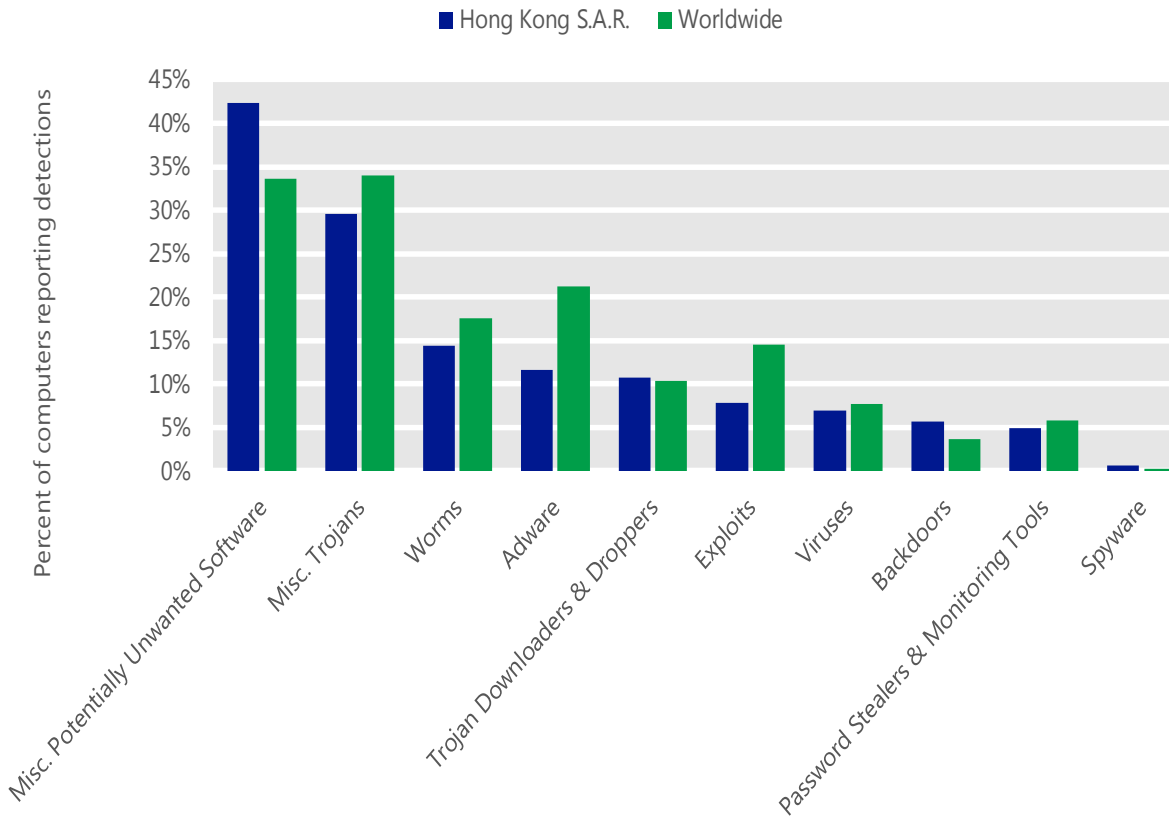
The MSRT detected malware on 2.2 of every 1,000 computers scanned in Hong Kong S.A.R. in 4Q12 (a CCM score of 2.2, compared to the 4Q12 worldwide average CCM of 6.0). The following figure shows the CCM trend for Hong Kong S.A.R. over the last six quarters, compared to the world as a whole.

CCM infection trends in Hong Kong S.A.R. and worldwide



Threat categories

Malware and potentially unwanted software categories in Hong Kong S.A.R. in 4Q12, by percentage of computers reporting detections



- The most common category in Hong Kong S.A.R. in 4Q12 was Miscellaneous Potentially Unwanted Software. It affected 42.3 percent of all computers with detections there, up from 34.2 percent in 3Q12.
- The second most common category in Hong Kong S.A.R. in 4Q12 was Miscellaneous Trojans. It affected 29.5 percent of all computers with detections there, up from 26.9 percent in 3Q12.
- The third most common category in Hong Kong S.A.R. in 4Q12 was Worms, which affected 14.4 percent of all computers with detections there, down from 14.5 percent in 3Q12.

Threat families

The top 10 malware and potentially unwanted software families in Hong Kong S.A.R. in 4Q12

	Family	Most significant category	% of computers with detections
1	Win32/Keygen	Misc. Potentially Unwanted Software	19.5%
2	JS/IframeRef	Misc. Trojans	6.9%
3	INF/Autorun	Misc. Potentially Unwanted Software	6.8%
4	Win32/Obfuscator	Misc. Potentially Unwanted Software	5.8%
5	ASX/Wimad	Trojan Downloaders & Droppers	3.3%
6	Win32/DealPly	Adware	3.0%
7	Win32/Injector	Misc. Potentially Unwanted Software	3.0%
8	Win32/OpenCandy	Adware	2.9%
9	Win32/Taterf	Worms	2.7%
10	Win32/Conficker	Worms	2.7%

- The most common threat family in Hong Kong S.A.R. in 4Q12 was Win32/Keygen, which affected 19.5 percent of computers with detections in Hong Kong S.A.R.. Win32/Keygen is a generic detection for tools that generate product keys for various software products.
- The second most common threat family in Hong Kong S.A.R. in 4Q12 was JS/IframeRef, which affected 6.9 percent of computers with detections in Hong Kong S.A.R.. JS/IframeRef is a generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.
- The third most common threat family in Hong Kong S.A.R. in 4Q12 was INF/Autorun, which affected 6.8 percent of computers with detections in Hong Kong S.A.R.. INF/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 Hong Kong S.A.R. in 4Q12 was Win32/Obfuscator, which affected 5.8 percent of computers with detections in Hong Kong S.A.R.. Win32/Obfuscator is a generic detection for programs that have had their purpose disguised to hinder analysis or detection by antivirus scanners. Such programs commonly employ a combination of methods, including encryption, compression, anti-debugging and anti-emulation techniques.

Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. In many cases, these sites are legitimate websites that have been compromised by malware, SQL injection, or other techniques, in an effort by attackers to take advantage of the trust users have invested in them. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

Web browsers such as Windows Internet Explorer and search engines such as Bing use lists of known phishing and malware hosting websites to warn users about malicious websites before they can do any harm. The information presented in this section has been generated from telemetry data produced by Internet Explorer and Bing. See the *Microsoft Security Intelligence Report* website for more information about these protections and how the data is collected.

To provide a more accurate perspective on the phishing and malware landscape, the methodology used to calculate the number of Internet hosts in each country or region has been revised. For this reason, the statistics presented here should not be directly compared to findings in previous volumes.

Malicious website statistics for Hong Kong S.A.R.

Metric	3Q12	4Q12
Phishing sites per 1,000 hosts *(Worldwide)*	6.01 *(5.41)*	6.23 *(5.10)*
Malware hosting sites per 1,000 hosts *(Worldwide)*	10.70 *(9.46)*	12.22 *(10.85)*
Drive-by download per 1,000 URLs *(Worldwide)*	0.28 *(0.56)*	0.11 *(0.33)*

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security