# Microsoft Security Intelligence Report

Volume 12

JULY-DECEMBER 2011

# KEY FINDINGS

www.microsoft.com/sir

# Microsoft Security Intelligence Report

# Microsoft Security Intelligence Report, Volume 12

Volume 12 of the *Microsoft® Security Intelligence Report* (*SIRv12*) provides in-depth perspectives on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in Microsoft and third-party software. Microsoft developed these perspectives based on detailed trend analyses over the past several years, with a focus on the second half of 2011.

This document summarizes the key findings of the report. The full report also includes deep analysis of trends found in more than 100 countries/regions around the world and offers suggestions to help manage risks to your organization, software, and people.

*SIRv12* includes the following two feature articles that provide insight into the malware threat Conficker and advanced persistent threats (APT), respectively.

## How Conficker continues to propagate

This article provides information about an analysis Microsoft conducted to better understand why Conficker remains a serious threat, especially for enterprises. The analysis uses information that was obtained since Conficker was discussed in *SIRv7*.

The article establishes that Conficker remains a threat, provides background information on why it is a serious threat, and what organizations can do to protect themselves. The full analysis can be downloaded from www.microsoft.com/sir.

## Determined adversaries and targeted attacks

Reports of targeted attacks against organizations, governments, and individuals have become more widespread in recent years. This article provides insight into such threats, also known as advanced persistent threats (APT).

The article discusses the threats posed by targeted attacks that are carried out by determined adversaries and outlines a defensive strategy of prevention, detection, containment, and recovery. The full analysis can be downloaded from www.microsoft.com/sir.

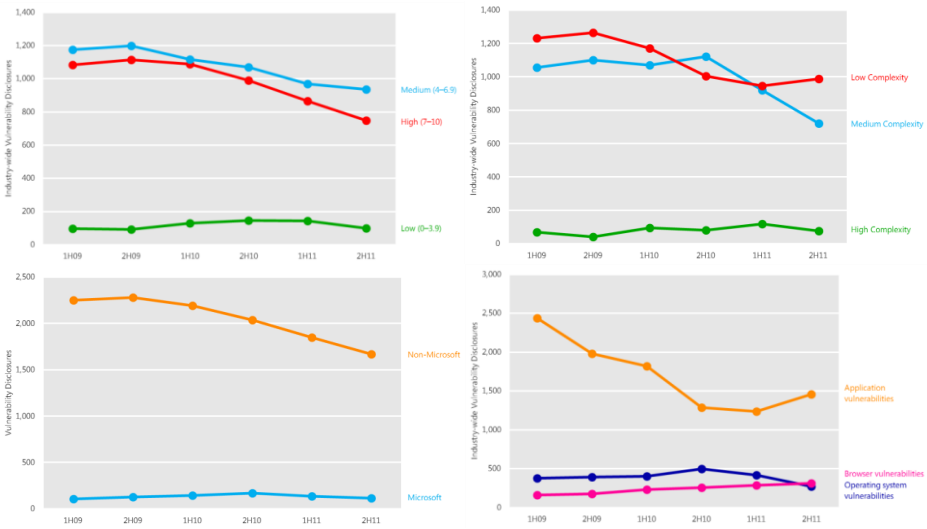
The full report, as well as previous volumes and related videos, can be downloaded from www.microsoft.com/sir.

# Worldwide threat assessment

## Vulnerabilities

*Vulnerabilities* are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of the software or the data it processes. Some of the worst vulnerabilities allow attackers to exploit the compromised system by causing it to run malicious code without the user's knowledge.

Figure 1. Trends for vulnerability (CVE) severity, vulnerability complexity, disclosures by vendor, and disclosures by type, across the entire software industry, 1H09-2H11[1]



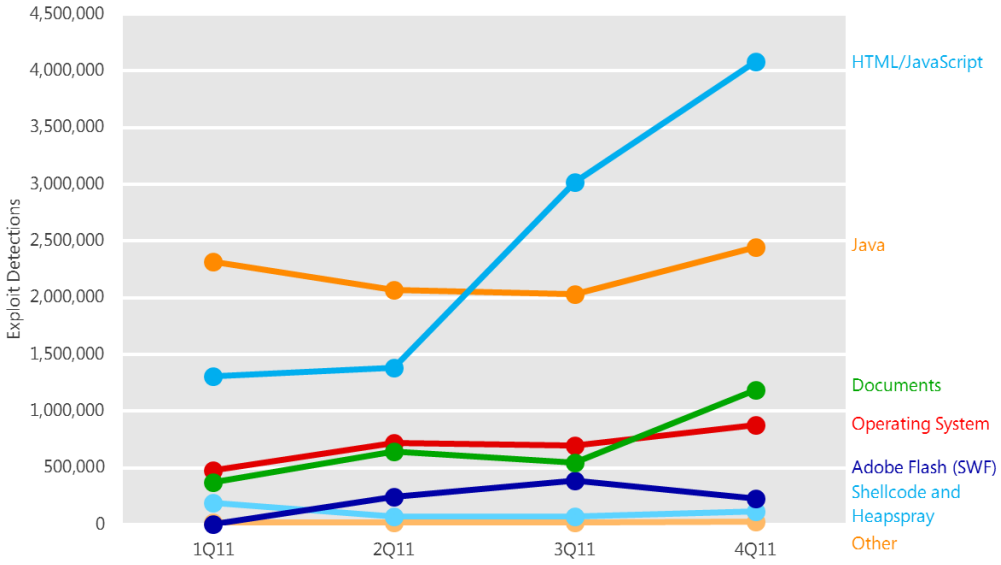

- The overall vulnerability severity trend has been a positive one. All three CVSS severity classifications decreased between 1H11 and 2H11, with the Medium and High severity classifications continuing a trend of declining disclosures in every period since 2H09.

[1] The nomenclature used throughout the report to refer to different reporting periods is nHYY, where nH refers to either the first (1) or second (2) half of the year, and YY denotes the year. For example, 1H09 represents the period covering the first half of 2009 (January 1 through June 30), and 2H11 represents the period covering the second half of 2011 (July 1 through December 31).

# Exploits

An *exploit* is malicious code that takes advantage of software vulnerabilities to infect, disrupt, or take control of a computer without the user's consent and usually without the user's knowledge. Exploits target vulnerabilities in operating systems, web browsers, applications, or software components that are installed on the computer. For more information, download the complete *SIRv12* at www.microsoft.com/sir.

Figure 2. Exploits detected and blocked by Microsoft antimalware products each quarter in 2011, by targeted platform or technology




- Detections of exploits that are delivered through HTML or JavaScript increased steeply in the second half of 2011, primarily because of the emergence of JS/Blacole, a family of exploits used by the so-called "Blackhole" exploit kit to deliver malicious software through infected webpages.
- Detections of exploits that target vulnerabilities in document readers and editors increased in 4Q11, making them the third most commonly detected type of exploit during the quarter, primarily because of an increase in exploits that target Adobe Reader.

# Malware and potentially unwanted software

Except where specified, the information in this section was compiled from telemetry data that was generated from more than 600 million computers worldwide and some of the busiest online services on the Internet. Infection rates are given in computers cleaned per mille (CCM), or thousand, and represent the number of reported computers cleaned in a quarter for every 1,000 executions of the Windows® Malicious Software Removal Tool, which is available through Microsoft Update and the Microsoft Safety & Security Center website.

For a perspective on infection patterns worldwide, Figure 3 shows the infection rates in locations around the world using CCM. Detections and removals in individual countries/regions can vary significantly from quarter to quarter.

Figure 3. Infection rates by country/region in 4Q11, by CCM

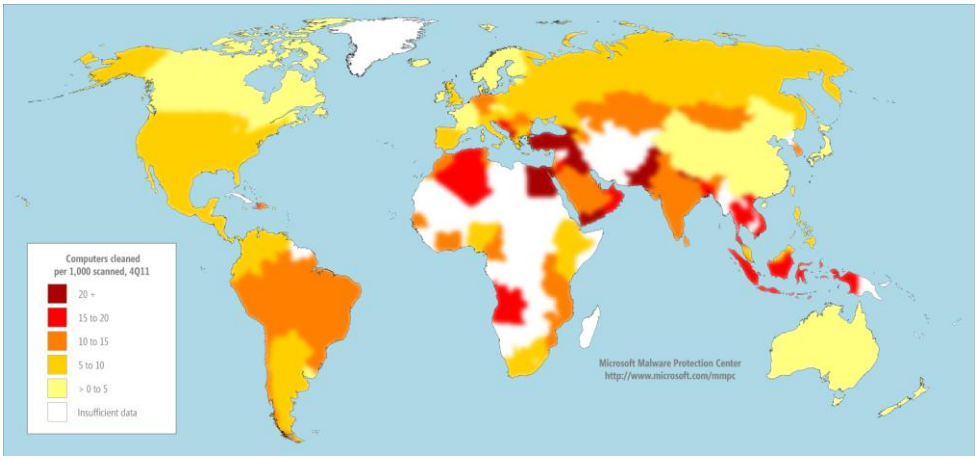
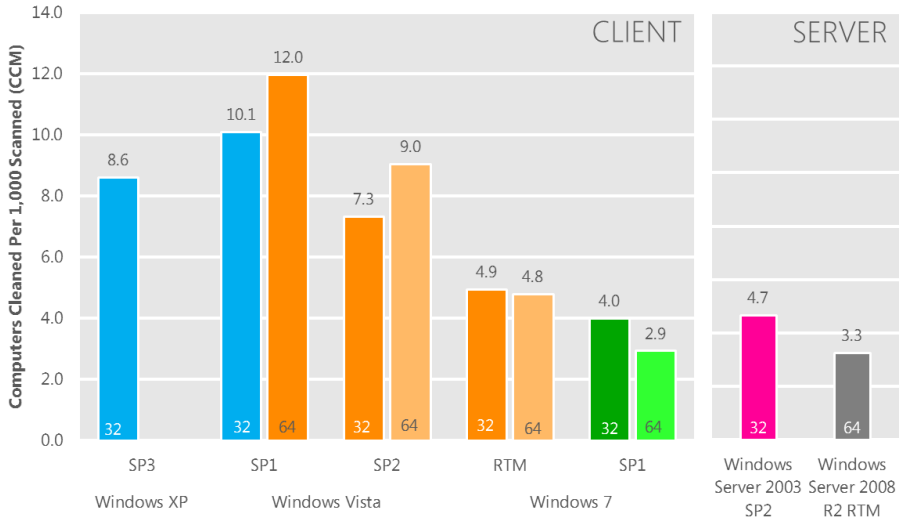


Figure 4. Infection rate (CCM) by operating system and service pack in 4Q11

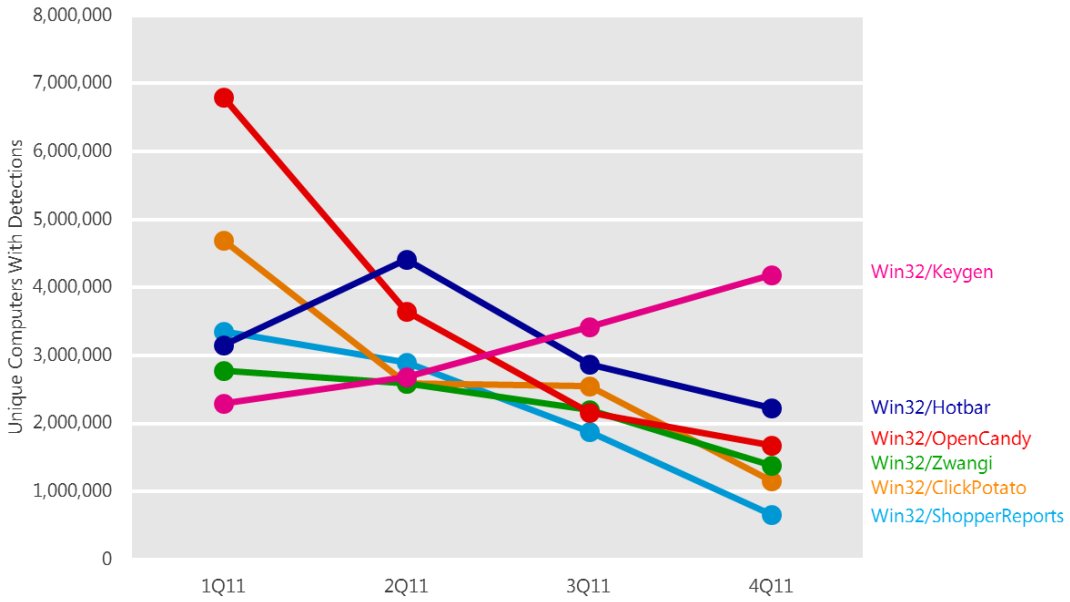



"32" = 32-bit edition. "64" = 64-bit edition. SP = Service Pack. RTM = released to manufacturing or no service pack.
Supported operating systems with at least 0.1 percent of total executions in 4Q11 shown.

- This data is normalized: the infection rate for each version of Windows is calculated by comparing an equal number of computers per version (for example, 1,000 Windows XP SP3 computers to 1,000 Windows 7 RTM computers).

## Threat families

Figure 5. Detection trends for a number of notable families in 2011




- Win32/Keygen was the most commonly detected family in 4Q11, and the only one of the top ten families with more detections in the fourth quarter of the year than in the first. Keygen is a generic detection for tools that generate keys for illegally obtained versions of various software products.
- Keygen, Win32/Autorun, and Win32/Sality were the only families in the top ten with more detections in 4Q11 than in 3Q11.

## Home and enterprise threats

Comparing the threats encountered by domain-joined computers and non-domain computers can provide insights into the different ways attackers target enterprise and home users, and also which threats are more likely to succeed in each environment.

- Five families are common to both lists, notably the generic families Win32/Keygen and Win32/Autorun and the exploit family JS/Blacole.

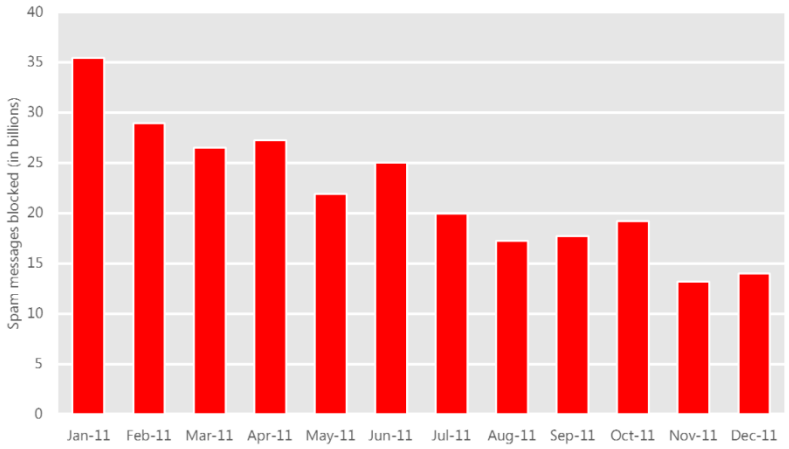
- Families that were significantly more prevalent on domain-joined computers include Conficker, the botnet family Win32/Zbot, and the potentially unwanted software program Win32/RealVNC.
- Families that were significantly more prevalent on non-domain computers include the adware families JS/Pornpop and Win32/Hotbar and the generic detection ASX/Wimad. Wimad is a detection for malicious files in the Advanced Stream Redirector (ASX) format used by Windows Media Player.

# Email threats

## Spam messages blocked

The information in this section of the *Microsoft Security Intelligence Report* is compiled from telemetry data provided by Microsoft Forefront® Online Protection for Exchange (FOPE), which provides spam, phishing, and malware filtering services for thousands of Microsoft enterprise customers who process tens of billions of messages each month.

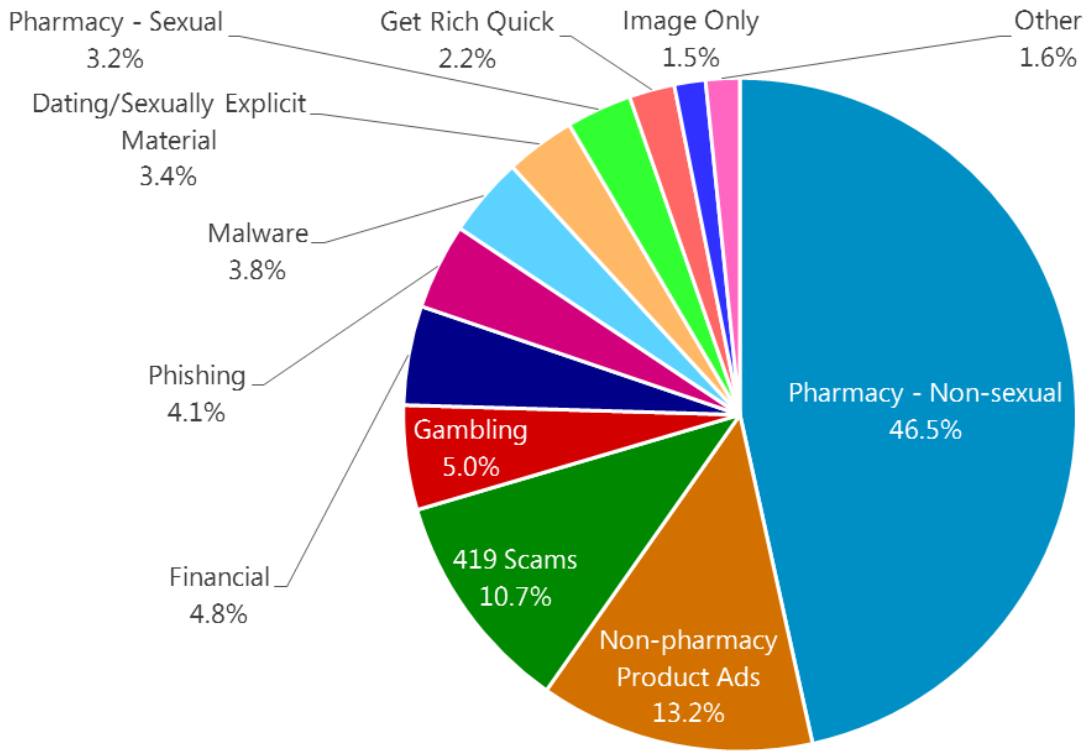
Figure 6. Messages blocked by FOPE each month in 2011




- FOPE blocked 14.0 billion messages in December 2011, less than half of the amount blocked in January. The significant decline in blocked messages seen throughout 2011 is likely attributable to takedown actions waged against a number of high-volume botnets, including the Rustock botnet in March and the Kelihos botnet in September. These actions, conducted by Microsoft in cooperation with other members of the software industry and law enforcement agencies, seem to have had a significant impact on the ability of spammers to distribute their messages to wide audiences.

- The FOPE content filters recognize several different common types of spam messages. The following figure shows the relative prevalence of these spam types in 2011.

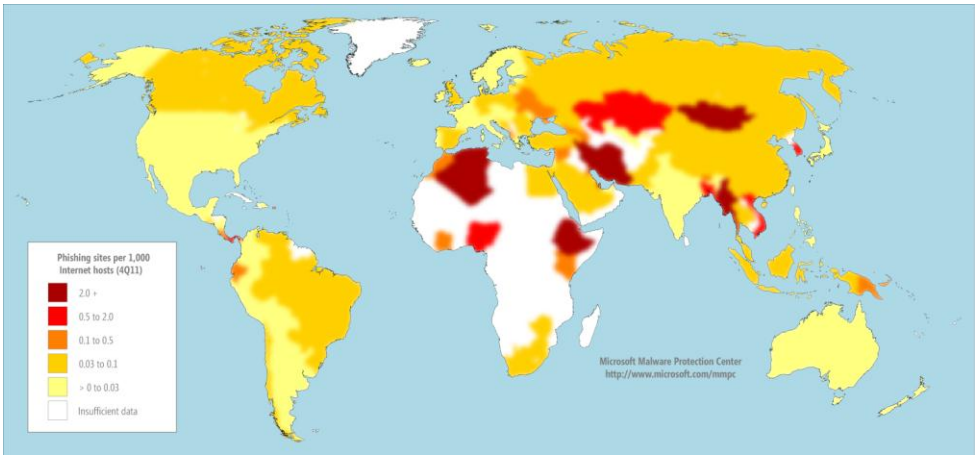
Figure 7. Inbound messages blocked by FOPE filters in 2H11, by category



## Malicious websites

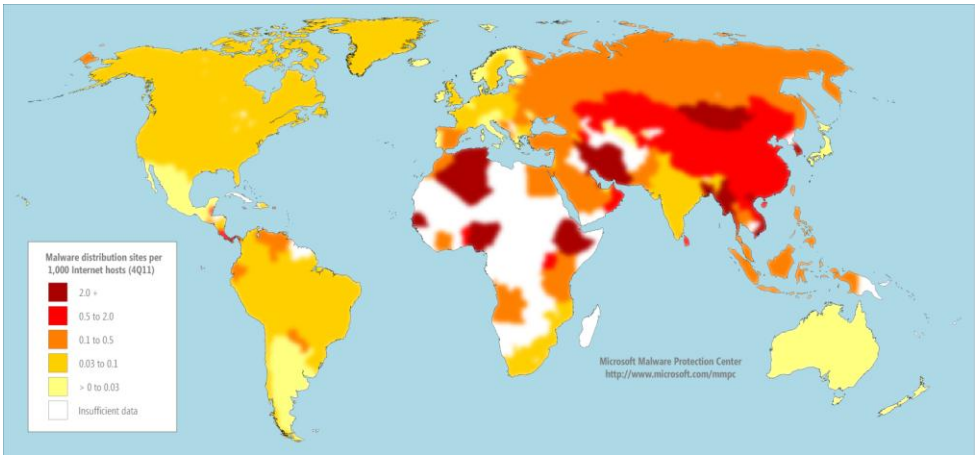
Phishing sites are hosted all over the world on free hosting sites, on compromised web servers, and in numerous other contexts.

Figure 8. Phishing sites per 1,000 Internet hosts for locations around the world in 2H11




Significant locations with unusually high concentrations of malware hosting sites include Iran, with 16.8 sites per 1,000 hosts, and Korea with 5.52.

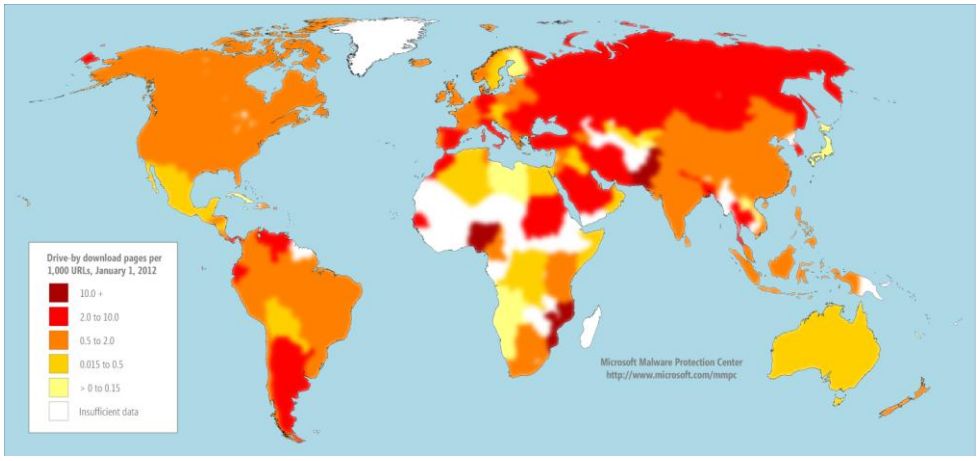
Figure 1. Malware distribution sites per 1,000 Internet hosts for locations around the world in 2H11




A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable

computers can be infected with malware simply by visiting such a website, even without attempting to download anything.

Figure 10. Drive-by download pages indexed by Bing.com at the end of 4Q11, per 1000 URLs in each country/region




Microsoft

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