Microsoft Security Intelligence Report

Volume 13

JANUARY-JUNE 2012

KEY FINDINGS

www.microsoft.com/sir

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.

Microsoft Security Intelligence Report, Volume 13

Volume 13 of the *Microsoft® Security Intelligence Report* (*SIRv13*) 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 first half of 2012.

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.

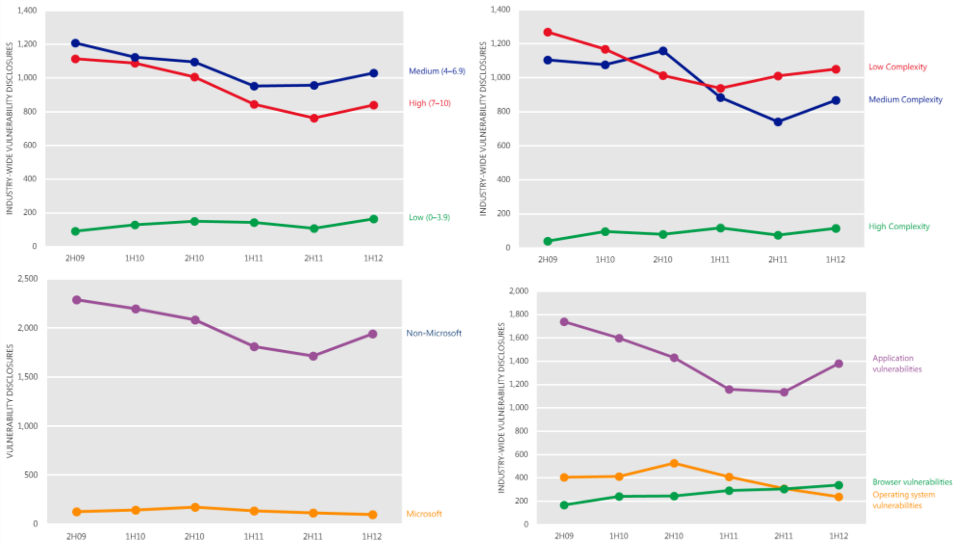
You can download the full report from www.microsoft.com/sir.

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, 2H09-1H12[1]



- Vulnerability disclosures across the industry in 1H12 were up 11.3 percent from 2H11, and 4.8 percent from 1H11.
- This increase reverses a trend of small declines in every six-month period from 2H09 to 2H11.The majority of the increase comes from application

[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, 2H09 represents the period covering the second half of 2009 (July 1 through December 31), and 1H12 represents the period covering the first half of 2012 (January 1 through June 30).

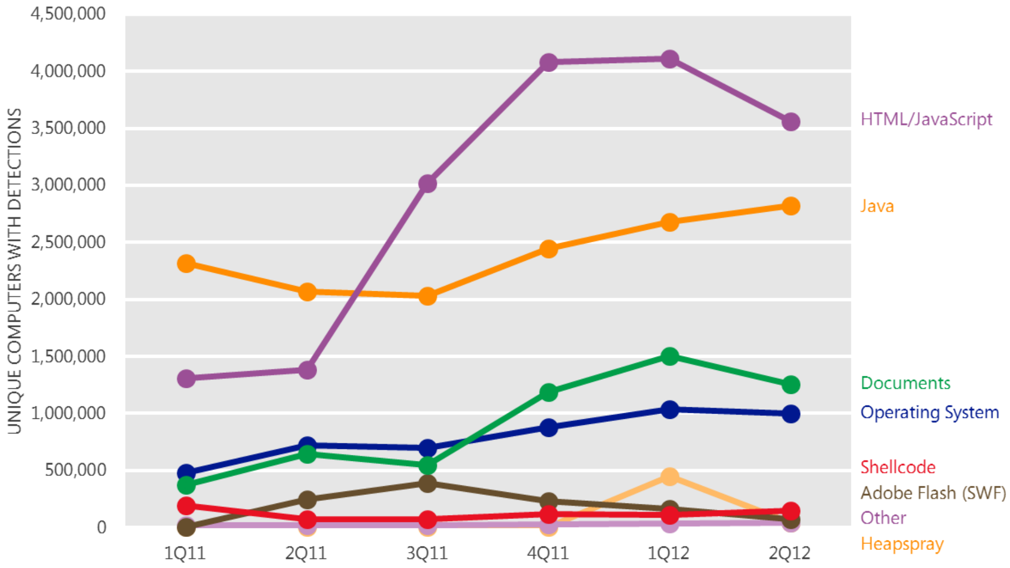
vulnerabilities, as operating system vulnerabilities continue a downward trend.

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 *SIRv13* at www.microsoft.com/sir.

Figure 2 shows the prevalence of different types of exploits detected by Microsoft antimalware products each quarter from 1Q11 to 2Q12, by number of unique computers affected.

Figure 2. Unique computers reporting different types of exploits, 1Q11-2Q12



- The number of computers reporting exploits delivered through HTML or JavaScript remained high during the first half of 2012, primarily driven by the continued prevalence of Blacole, the most commonly detected exploit family in 1H12.

- Java exploits, the second most common type of exploit detected in 1H12, increased throughout the period, driven by increased detection of exploits for CVE-2012-0507 and CVE-2011-3544.
- Exploits that target vulnerabilities in document readers and editors were the third most commonly detected type of exploit during 1H12, primarily because of detections of exploits that target older versions of Adobe Reader.

Exploit families

Figure 3 lists the exploit-related families detected most often during the first half of 2012.

Figure 3 Top exploit families detected by Microsoft antimalware products in 1H12, by number of unique computers with detections, shaded according to relative prevalence

Exploit Family	Platform or Technology	3Q11	4Q11	1Q12	2Q12
Blacole	HTML/JavaScript	1,054,045	2,535,171	3,154,826	2,793,451
CVE-2012-0507*	Java	–	–	205,613	1,494,074
Win32/Pdfjsc	Documents	491,036	921,325	1,430,448	1,217,348
Malicious IFrame	HTML/JavaScript	1,610,177	1,191,316	950,347	812,470
CVE-2010-0840*	Java	1,527,000	1,446,271	1,254,553	810,254
CVE-2011-3544	Java	–	331,231	1,358,266	803,053
CVE-2010-2568 (MS10-046)	Operating System	517,322	656,922	726,797	783,013
JS/Phoex	Java	–	–	274,811	232,773
CVE-2008-5353	Java	335,259	537,807	295,515	215,593
ShellCode	Shell code	71,729	112,399	105,479	145,352

* This vulnerability is also used by the Blacole kit; the totals given here for this vulnerability exclude Blacole detections.

- Blacole, a family of exploits used by the so-called “Blackhole” exploit kit to deliver malicious software through infected webpages, was the most commonly detected exploit family in the first half of 2012.Prospective attackers buy or rent the Blacole kit on hacker forums and through other illegitimate outlets. It consists of a collection of malicious webpages that contain exploits for vulnerabilities in versions of Adobe Flash Player, Adobe Reader, Microsoft Data Access Components (MDAC), the Oracle Java Runtime Environment (JRE), and other popular products and components. When the attacker installs the Blacole kit on a malicious or compromised web server, visitors who don’t have the appropriate security updates installed are at risk of infection through a drive-by download attack.

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 4 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 4. Infection rates by country/region in 2Q12, by CCM

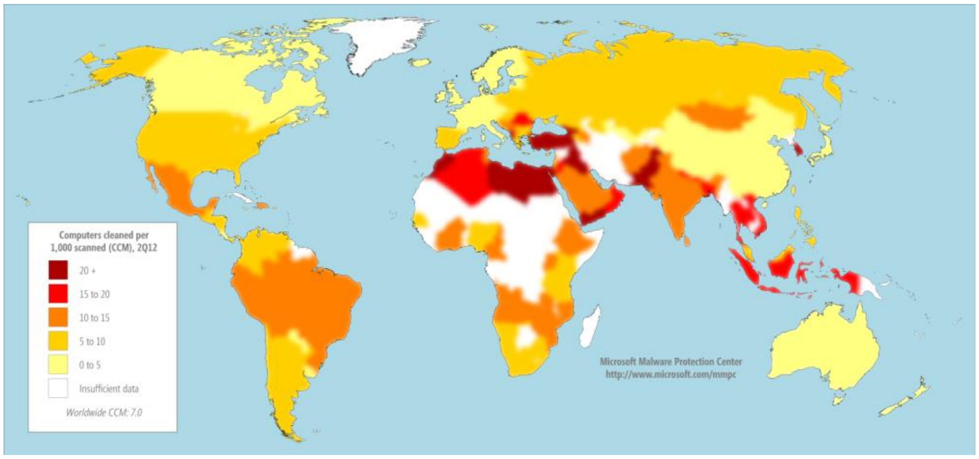
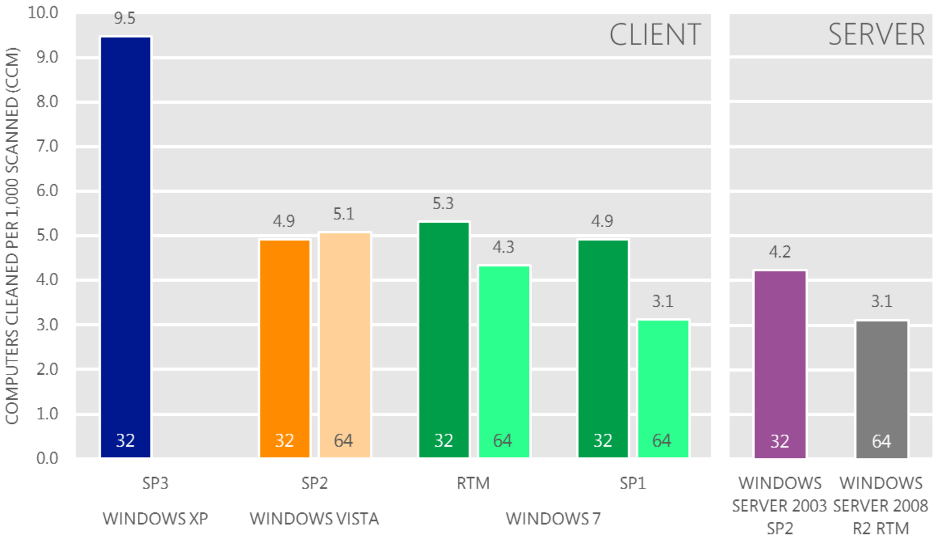

Computers cleaned per 1,000 scanned (CCM), 2Q12
20 +
15 to 20
10 to 15
5 to 10
0 to 5
Insufficient data
Worldwide CCM: 7.0
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Figure 5. Average infection rate (CCM) by operating system and service pack in 1H12

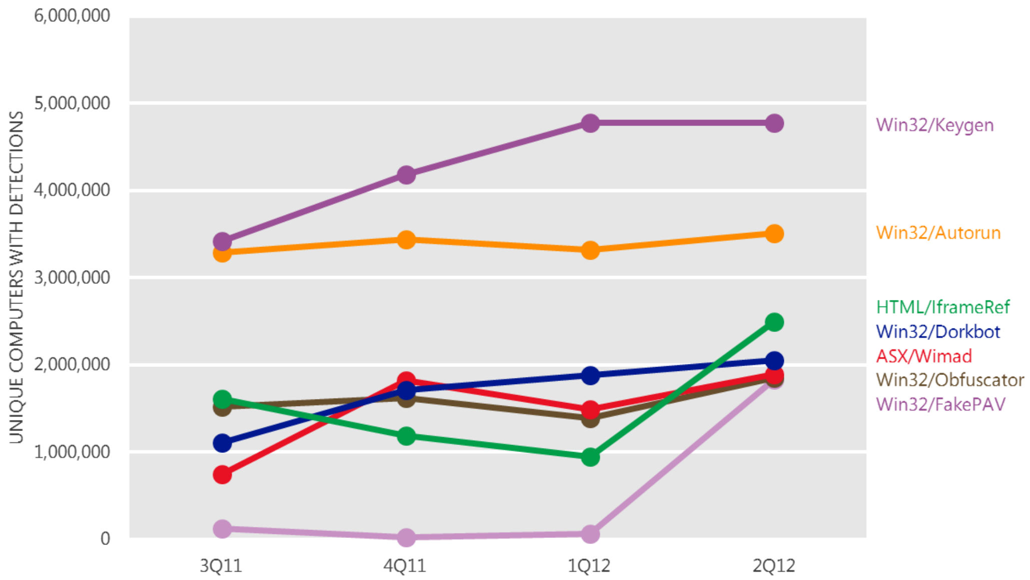


“32” = 32-bit edition; “64” = 64-bit edition. SP = Service Pack. RTM = release to manufacturing.
Operating systems with at least 0.1 percent of total MSRT executions in 2Q12 shown.

- 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 compared to 1,000 Windows 7 RTM computers).

Threat families

Figure 6. Detection trends for a number of notable families, 3Q11-2Q12



- A pair of generic detections, Win32/Keygen and Win32/Autorun, were the first and second most commonly detected families in 1H12. Keygen is a generic detection for tools that generate keys for illegally obtained versions of various software products.

  Autorun is a generic detection for worms that spread between mounted volumes using the Autorun feature of Windows. Recent changes to the feature in Windows XP and Windows Vista have made this technique less effective, but attackers continue to distribute malware that attempts to target it.
- Detections of the generic family JS/IframeRef more than doubled between 1Q12 and 2Q12 after several quarters of small declines. IframeRef is a generic detection for specially formed HTML inline frame (IFrame) tags that point to remote websites containing malicious content.

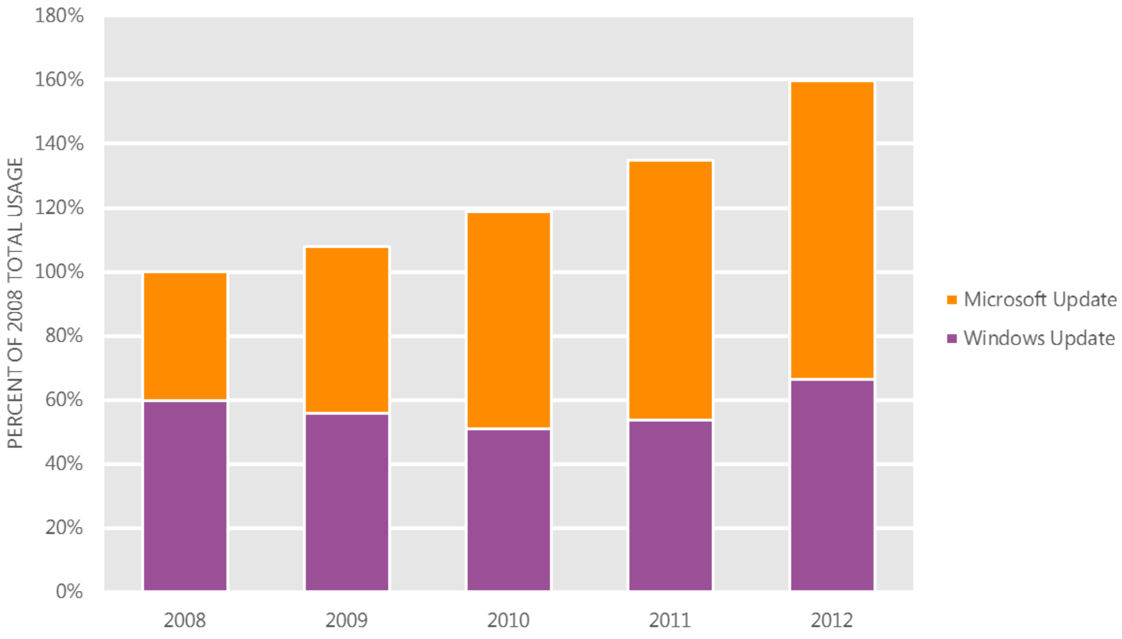
Home and enterprise threats

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 Blacole.
- Families that were significantly more prevalent on domain-joined computers during at least one quarter include the generic family JS/IframeRef and the worm family Win32/Conficker.
- Families that were significantly more prevalent on non-domain computers include Keygen and the adware families JS/Pornpop and Win32/Hotbar.

Windows Update and Microsoft Update usage

Figure 7. Windows computers updated by Windows Update and Microsoft Update, worldwide, 2008–2012



- Figure 7 shows the increase in the number of computers updated by Windows Update and Microsoft Update, worldwide over the last four years, indexed to the total usage for both services in 2008.
- Since 2008, worldwide usage of Windows Update and Microsoft Update has increased by 60 percent. Almost all of this growth is due to increased use of Microsoft Update, which went up 53 percentage points between 2008 and 2012, compared to 6 percentage points for Windows Update.
- **Windows Update** provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- **Microsoft Update** provides all of the updates offered through Windows Update and provides updates for other Microsoft software, such as the

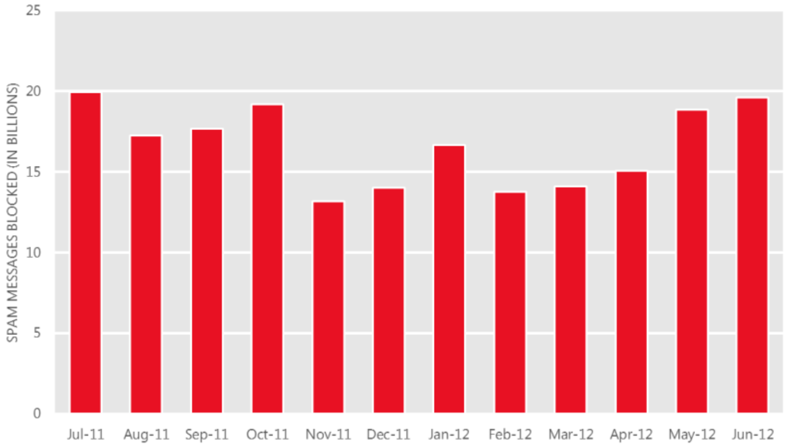
Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update website (update.microsoft.com/microsoftupdate). Microsoft recommends that users configure computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.

Email threats

Spam messages blocked

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

Figure 8. Messages blocked by Exchange Online Protection, July 2011-June 2012



- Blocked mail volumes in 1H12 were consistent with those of 2H11, and remain well below levels seen prior to the end of 2010. The dramatic decline in spam observed over the past year and a half has occurred in the wake of successful takedowns of a number of large spam-sending botnets, notably Cutwail (August 2010) and Rustock (March 2011).

Figure 9. Messages blocked by Exchange Online Protection each half-year period, 2H08–1H12

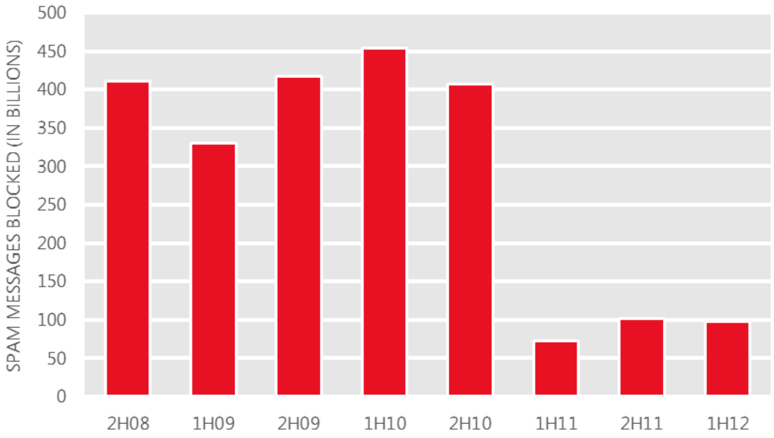
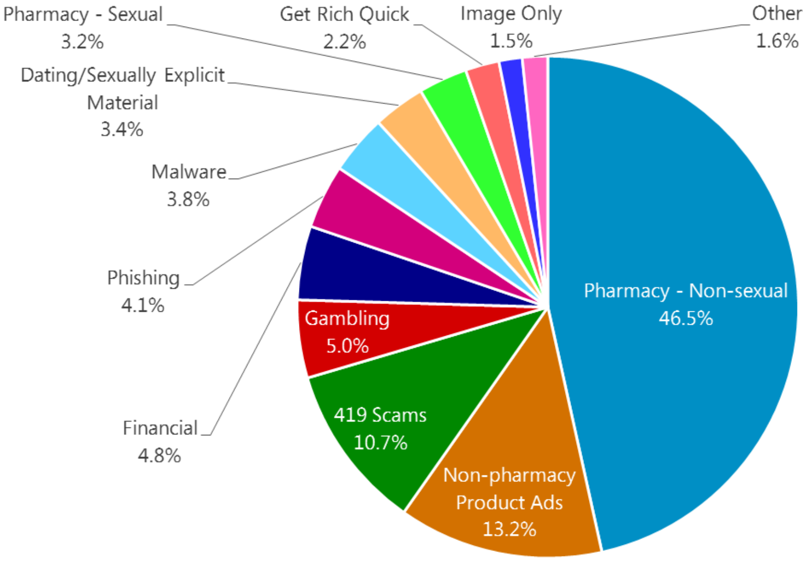


Figure 10. Inbound messages blocked by Exchange Online Protection filters in 1H12, by category

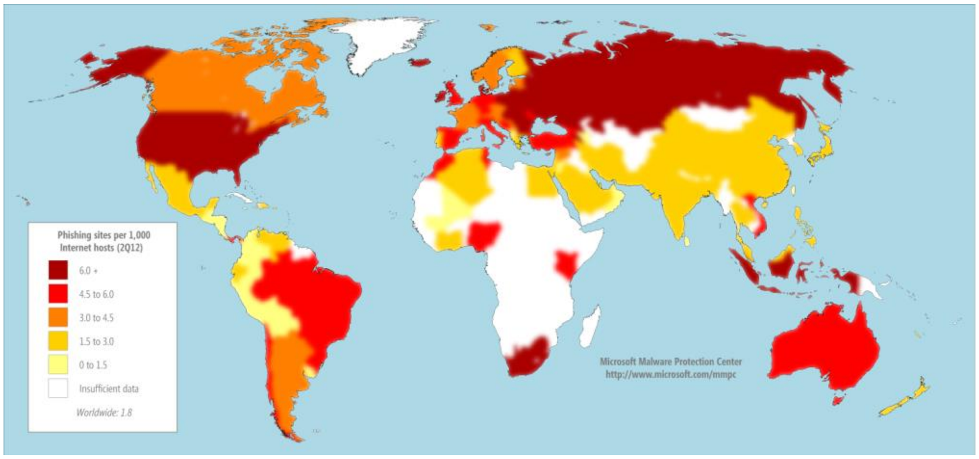


- The Exchange Online Protection content filters recognize several different common types of spam messages. Figure 10 shows the relative prevalence of the spam types that were detected in 1H12.

Malicious websites

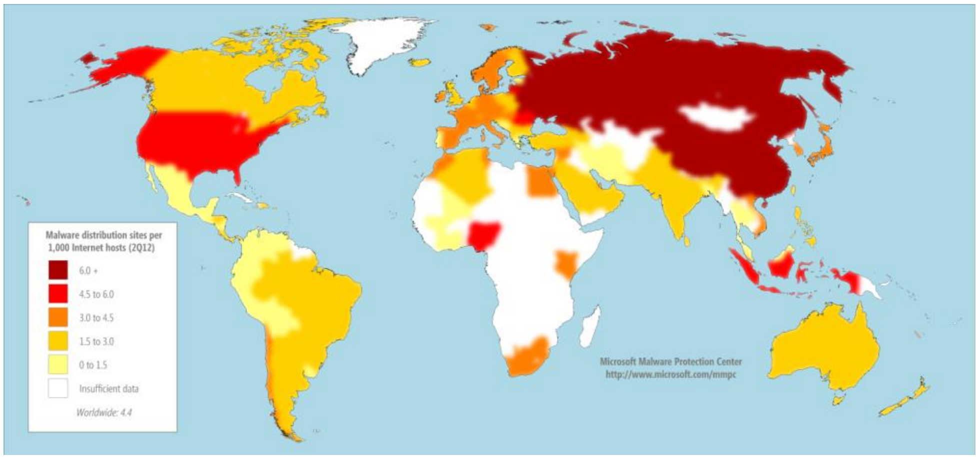
Phishing sites are hosted all over the world on free hosting sites, on compromised web servers, and in numerous other contexts.

Figure 11. Phishing sites per 1,000 Internet hosts for locations around the world in 2Q12


Phishing sites per 1,000 Internet hosts (2Q12)
6.0 +
4.5 to 6.0
3.0 to 4.5
1.5 to 3.0
0 to 1.5
Insufficient data
Worldwide: 1.8
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

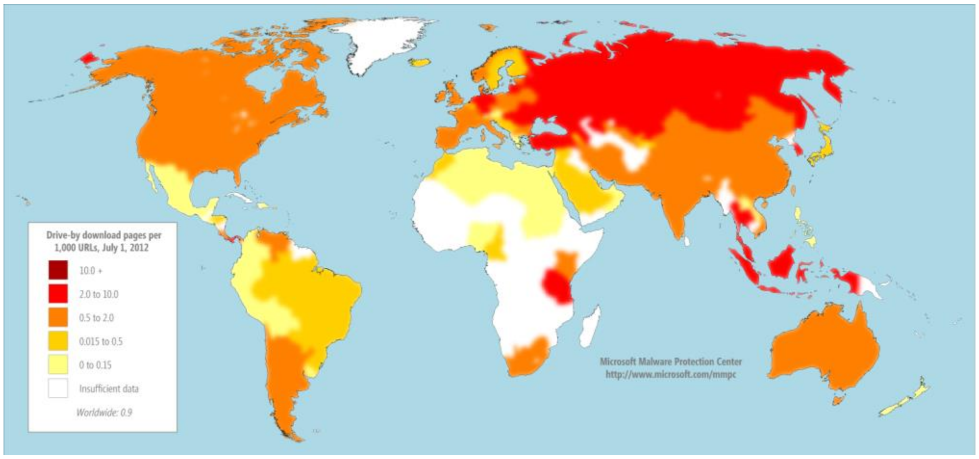
The United States, which has the largest number of hosts, also has a large number of phishing sites (2.9 per 1000 Internet hosts in 2Q12); China, with the second largest number of hosts, has a much lower concentration of phishing sites (0.6 per 1000 Internet hosts).

Figure 12. Malware distribution sites per 1,000 Internet hosts for locations around the world in 2Q12


Malware distribution sites per 1,000 Internet hosts (2Q12)
6.0 +
4.5 to 6.0
3.0 to 4.5
1.5 to 3.0
0 to 1.5
Insufficient data
Worldwide: 4.4
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

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 13. Drive-by download pages indexed by Bing.com at the end of 2Q12, per 1000 URLs in each country/region


Drive-by download pages per 1,000 URLs, July 1, 2012
10.0 +
2.0 to 10.0
0.5 to 2.0
0.015 to 0.5
0 to 0.15
Insufficient data
Worldwide: 0.9
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

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.

You can download the full report from www.microsoft.com/sir.

TwC Next

Microsoft

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

www.microsoft.com/twcnext