Microsoft

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

Microsoft Security Intelligence Report

Volume 15

January through June, 2013

KEY FINDINGS SUMMARY

Microsoft Security Intelligence Report

Microsoft Security Intelligence Report, Volume 15

Volume 15 of the *Microsoft® Security Intelligence Report (SIRv15)* provides in-depth perspectives on software vulnerabilities in Microsoft and third-party software, exploits, malicious code threats, and potentially unwanted software. Microsoft developed these perspectives based on detailed trend analyses over the past several years, with a focus on the first half of 2013.

This document summarizes the key findings of the report.

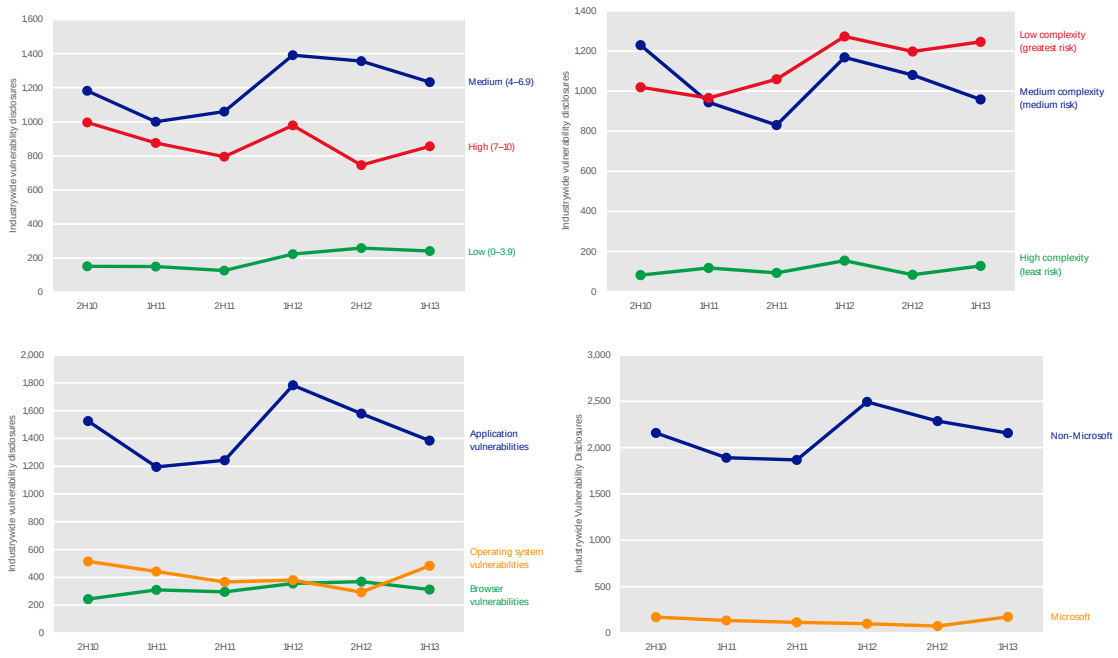
The SIR website also includes deep analysis of trends found in more than 100 countries/regions around the world and offers suggestions to help manage risks to your organization, software, and people.

You can download *SIRv15* from www.microsoft.com/sir.

Vulnerabilities

Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of the software or the data that 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 type, and disclosures for Microsoft and non-Microsoft products, across the entire software industry, 2H10-1H13[1]



- Vulnerability disclosures across the industry decreased 1.3 percent from 2H12, and 10.1 percent from 1H12. An increase in operating system vulnerability disclosures in 1H13 largely offset a corresponding decrease in application vulnerability disclosures during the same period, resulting in little overall change. Overall, however, vulnerability disclosures remain significantly lower than they were prior to 2009, when totals of 3,500 disclosures or more per half-year period were not uncommon.

[1] Throughout the report, half-yearly and quarterly time periods are referenced using the nHyy or nQyy formats, where yy indicates the calendar year and n indicates the half or quarter. For example, 1H13 represents the first half of 2013 (January 1 through June 30), and 4Q12 represents the fourth quarter of 2012 (October 1 through December 31).

Encounter rate: Introducing a new metric for analyzing malware prevalence

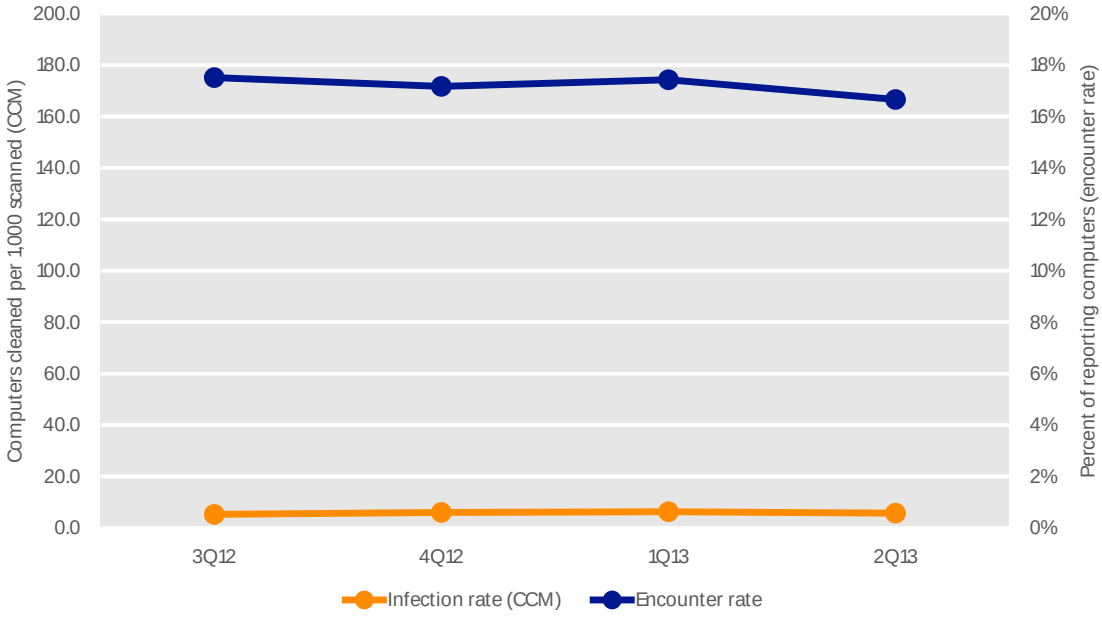
For several years the *Microsoft Security Intelligence Report* has reported infection rates using a metric called *computers cleaned per mille (CCM)*. CCM represents the number of computers cleaned for every 1,000 executions of the Malicious Software Removal Tool (MSRT). The MSRT gives perspective on the scope of widespread infections of specific families of malware. The tool's global reach, large installed base, and regularly scheduled release facilitate a consistent comparison of relative infection rates between different populations of computers.

To better describe the totality of what the users encounter in the malware ecosystem, Microsoft is introducing a new metric called the *encounter rate*. This metric is the percentage of computers running Microsoft real-time security products that encounter malware during a specified period of time, such as a quarter year. Note that a computer encountering malware will not necessarily be compromised by the threat; the real-time security product may detect the threat and prevent it executing. This detection would count towards the encounter rate, but not the infection rate for that computer.

Together, infection rates and encounter rates can assemble a broader picture of the malware landscape. The different perspectives that these two metrics can provide a clearer picture of malware prevalence and its potential effect in a global landscape.

Figure 2 shows the worldwide infection rate relative to the encounter rate for each quarter from 3Q12 to 2Q13, with the scales equalized for comparison purposes (100 per thousand is equivalent to 10 percent).

Figure 2. Worldwide encounter and infection rates, 3Q12–2Q13, by quarter



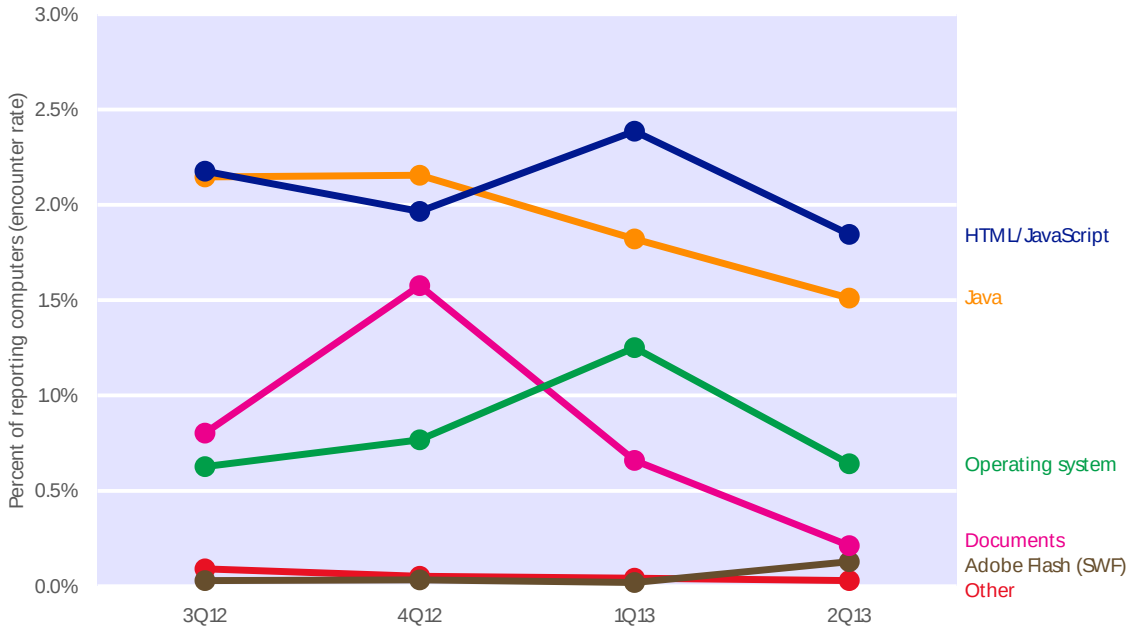
As Figure 2 shows, and as one would expect, malware encounters are much more common than malware infections. On average, about 17.0 percent of computers worldwide encountered malware each quarter in 1H12, as reported by Microsoft security products. At the same time, the MSRT detected and removed malware from about six out of every 1,000 computers (0.6 percent).

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 typically without their knowledge. Exploits target vulnerabilities in operating systems, web browsers, applications, or software components that are installed on the computer. For more information, download *SIRv15* at www.microsoft.com/sir.

Figure 13 shows the prevalence of different types of exploits detected by Microsoft antimalware products in each quarter from 3Q12 to 2Q13, by number of unique computers with encounters.

Figure 1. Unique computers reporting different types of exploit attempts, 3Q12–2Q13



- Detections of individual exploits often increase and decrease significantly from quarter to quarter as exploit kit distributors add and remove different exploits from their kits. This variation can also have an effect on the relative prevalence of different exploit types, as shown in Figure 13.
- Web-based (HTML/JavaScript) threats continued to be the most commonly encountered type of exploit encountered in 2Q13, followed by Java exploits and operating system exploits. The encounter rate for HTML/JavaScript exploits peaked in 1Q13, primarily driven by the multiplatform exploit family Blacole, which was encountered by 1.12

percent of computers worldwide during that quarter. (More information about Blacole is provided in the next section.)

Exploit families

Figure 4 lists the exploit-related families that were detected most often during the first half of 2013.

Figure 4. Quarterly encounter rate trends for the top exploit families detected by Microsoft antimalware products in 1H13, shaded according to relative prevalence

Exploit	Platform or technology	3Q12	4Q12	1Q13	2Q13
HTML/IframeRef*	HTML/JavaScript	0.37%	0.58%	0.98%	1.08%
Blacole	HTML/JavaScript	1.60%	1.34%	1.12%	0.62%
CVE-2012-1723	Java	0.84%	1.32%	0.89%	0.61%
CVE-2010-2568 (MS10-046)	Operating system	0.51%	0.57%	0.57%	0.53%
CVE-2012-0507	Java	0.91%	0.53%	0.49%	0.31%
CVE-2013-0422	Java	–	–	0.38%	0.33%
CVE-2011-3402 (MS12-034)	Operating system	–	0.11%	0.62%	0.04%
Pdfjsc	Document	0.77%	1.56%	0.53%	0.12%
CVE-2013-0431	Java	–	–	0.10%	0.32%
CVE-2010-0840	Java	0.31%	0.17%	0.18%	0.21%

Totals do not include exploits that were detected as part of exploit kits.
*Totals include only IframeRef variants categorized as exploits.

- HTML/IframeRef, the most commonly encountered exploit in 1H13, is a generic detection for specially formed HTML inline frame (IFrame) tags that redirect to remote websites that contain malicious content. More properly considered exploit downloaders than true exploits, these malicious pages use a variety of techniques to exploit vulnerabilities in browsers and plug-ins; the only commonality is that the attacker uses an inline frame to deliver the exploits to users. The exact exploit delivered and detected by one of these signatures may be changed frequently.

  Two highly prevalent IframeRef variants were reclassified as JS/Seedabutor variants in 1Q13, but the encounter rate for IframeRef remained high that quarter after detection signatures for the variant Trojan:JS/IframeRef.K were added to Microsoft antimalware products in response to the so-called "Darkleech" attacks, which add malicious inline frames to webpages hosted on compromised Apache web servers.

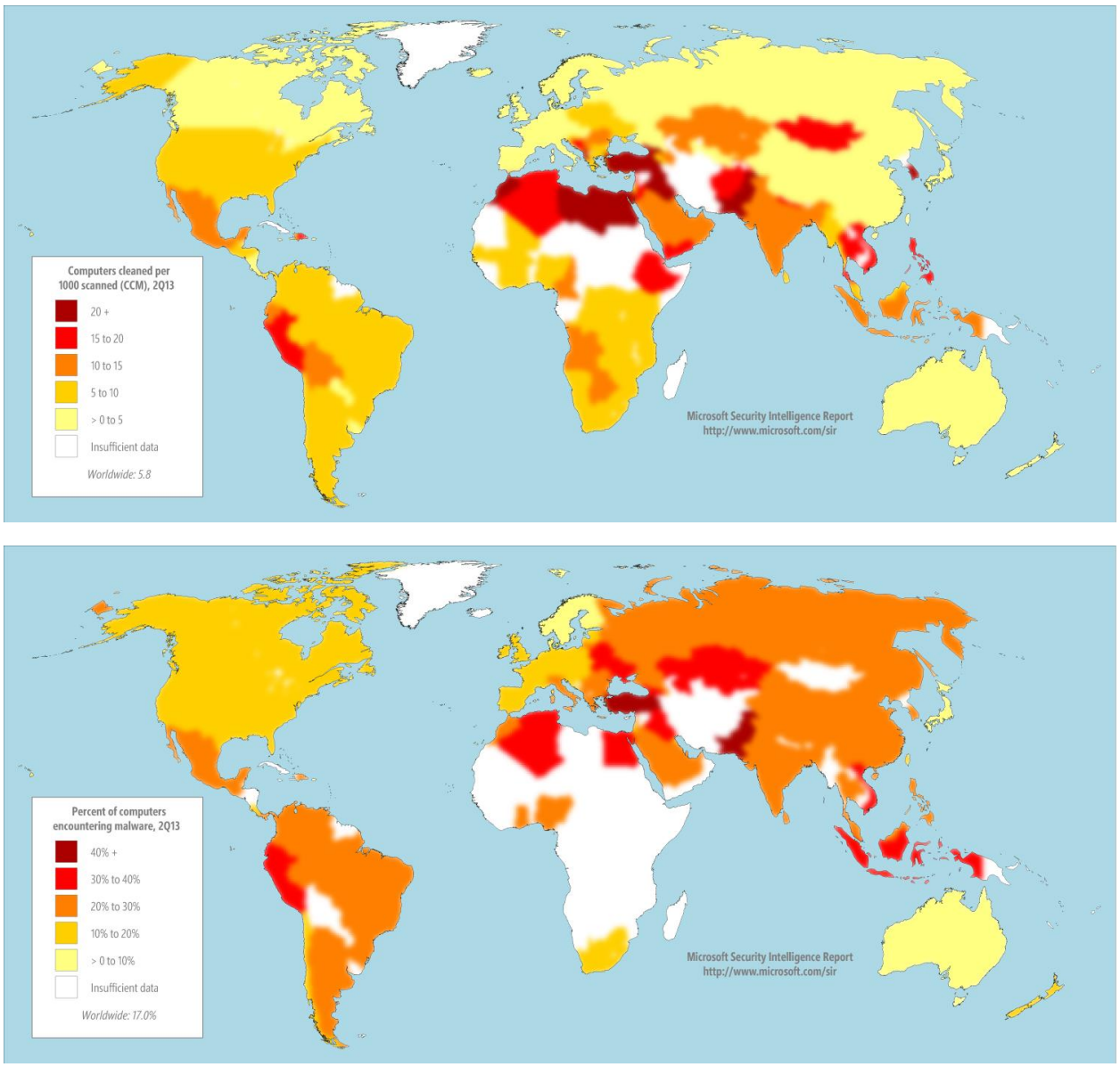
Malware

The information in this section was compiled from telemetry data generated from multiple sources, including more than a billion computers worldwide and some of the busiest services on the Internet.

This volume of the *Microsoft Security Intelligence Report* includes a new mechanism for measuring malware prevalence called *encounter rate*. Several of the charts in this section, along with their accompanying analysis, present encounter rate data alongside infection rate data, as measured using the established CCM metric.

For a perspective on threat patterns worldwide, Figure 5 shows the infection and encounter rates in locations around the world in the second quarter of 2013.

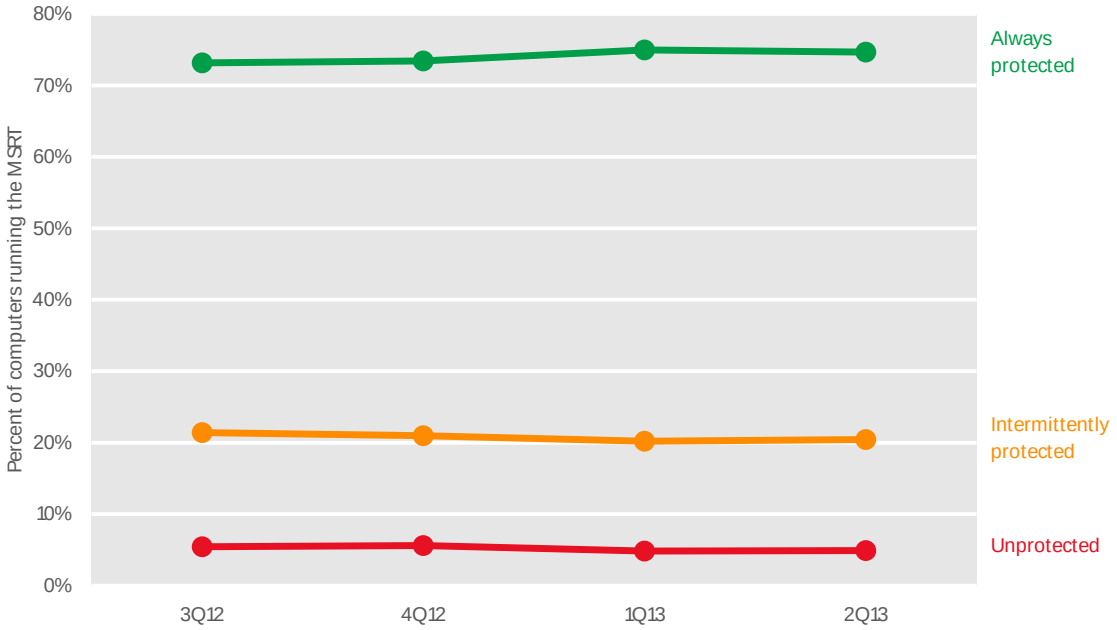
Figure 5. Infection rates (top) and encounter rates (bottom) by country/region in 2Q13



Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on the computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry makes it possible to analyze security software usage patterns around the world and correlate them with infection rates. Figure6 shows the percentage of computers worldwide that the MSRT found to be protected or unprotected by real-time security software each quarter from 3Q12 to 2Q13.

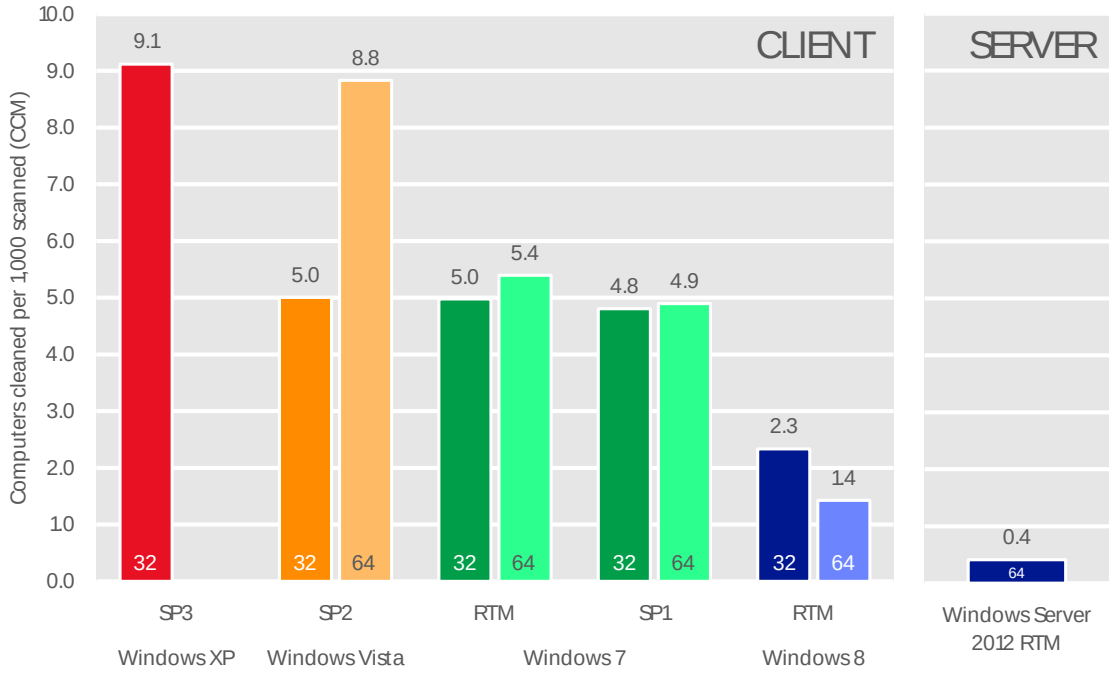
Figure 6. Percentage of computers worldwide protected by real-time security software, 3Q12–2Q13



Infection and encounter rates by operating system

The features and updates that are available with different versions of the Windows operating system and the differences in the way people and organizations use each version affect the infection rates for the different versions and service packs. Figure 7 shows the infection rate for each currently supported Windows operating system/service pack combination that accounted for at least 0.1 percent of total MSRT executions in 2Q13.

Figure 7. Infection rate (CCM) by operating system and service pack in 2Q13

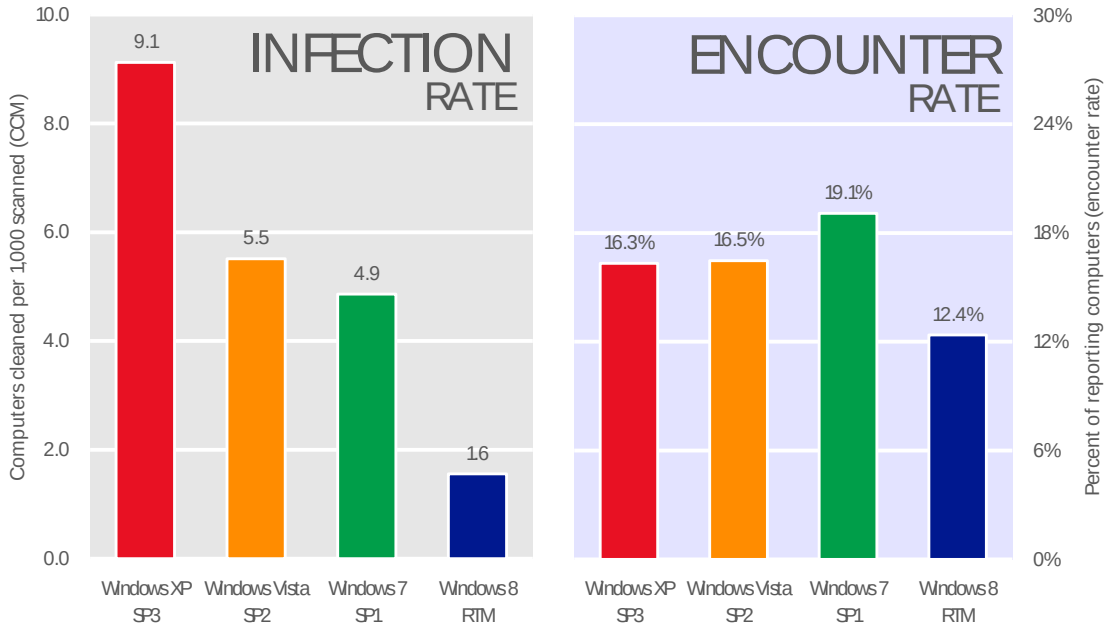


"32" = 32-bit edition; "64" = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.1 percent of total MSRT executions in 2Q13 shown.

- This data is normalized; that is, 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 8 RTM computers).

Figure 8 shows the difference between infection and encounter rates for supported Windows client operating systems in 2Q13 (32-bit and 64-bit editions combined).

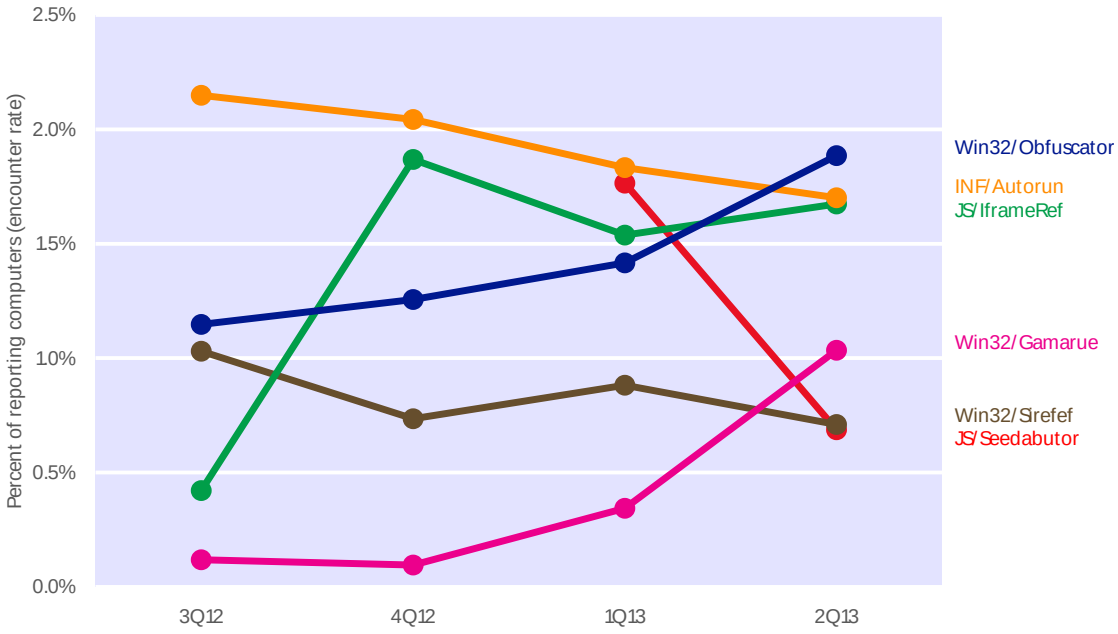
Figure 8. Infection and encounter rates for supported Windows client operating systems, 2Q13



Threat families

Figure 9 shows the detection trends for a number of families that increased or decreased significantly over the past four quarters.

Figure 9. Detection trends for a number of notable malware families, 3Q12–2Q13



- The generic detections Win32/Obfuscator, INF/Autorun, and HTML/IframeRef were the three most commonly encountered threats in

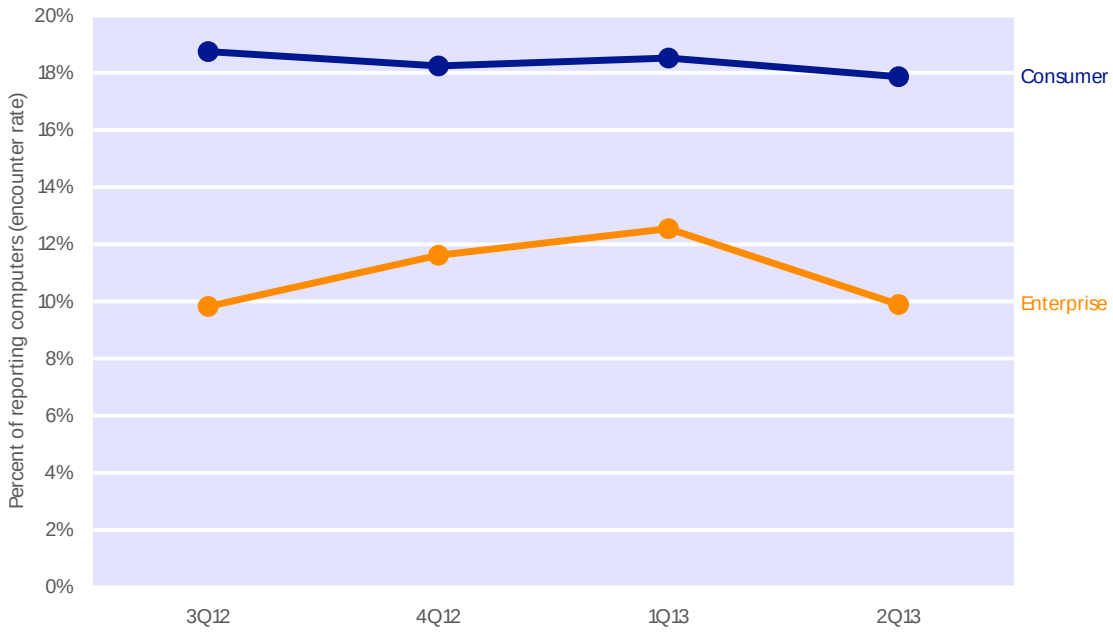
1H13. Autorun, the most commonly encountered threat worldwide during the period, is a generic detection for worms that spread between mounted volumes using the AutoRun feature of Windows. Changes to the feature in Windows XP and Windows Vista have made this technique less effective over time, but attackers continue to distribute malware that attempts to target it and Microsoft antimalware products detect and block these attempts even when they would not be successful.

- Detections of Obfuscator increased from fourth in 1Q13 to first in 2Q13, making it the second most commonly encountered threat worldwide for the half-year overall. Obfuscator is a generic detection for programs that have been modified by malware obfuscation tools. These tools typically use a combination of methods, including encryption, compression, and anti-debugging or anti-emulation techniques, to alter malware programs in an effort to hinder analysis or detection by security products. The output is usually another program that keeps the same functionality as the original program but with different code, data, and geometry.

Home and enterprise threats

The usage patterns of home users and enterprise users tend to be very different. Analyzing these differences can provide insights into the different ways attackers target enterprise and home users and which threats are more likely to succeed in each environment.

Figure 10. Malware encounter rates for consumer and enterprise computers, 3Q12–2Q13



- Enterprise environments typically implement defense-in-depth measures, such as enterprise firewalls that prevent a certain amount of malware from reaching users' computers. Consequently, enterprise computers tend to encounter malware at a lower rate than consumer computers. The encounter rate for consumer consumers was 1.5 times as high as that of enterprise computers in 1Q13, with the relative difference increasing to 1.8 in 2Q13.

Figure 11 and Figure 12 list the top 10 families detected by enterprise and consumer security products, respectively, in 1H13.

Figure 11. Quarterly trends for the top 10 families detected by Microsoft enterprise security products in 1H13, by percentage of computers encountering each family

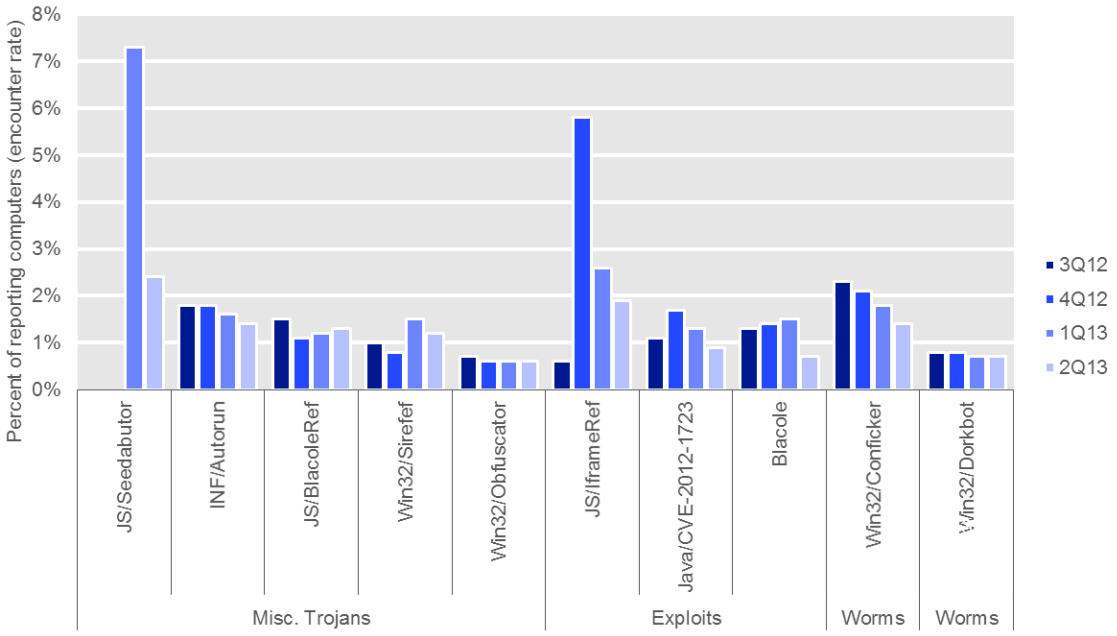
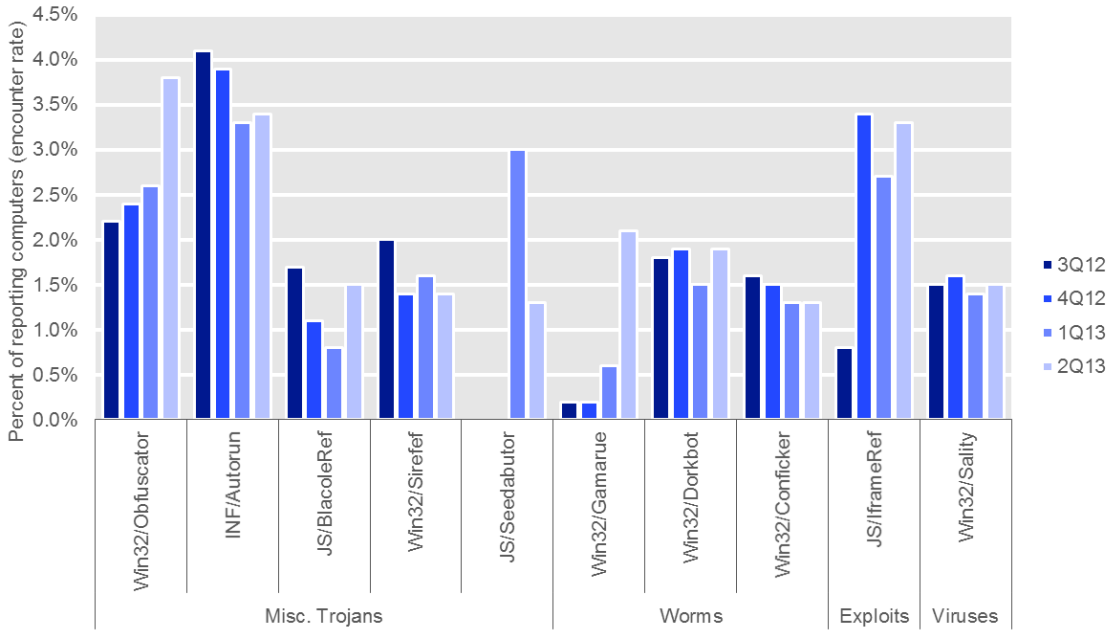


Figure 12. Quarterly trends for the top 10 families detected by Microsoft consumer security products in 1H13, by percentage of computers encountering each family



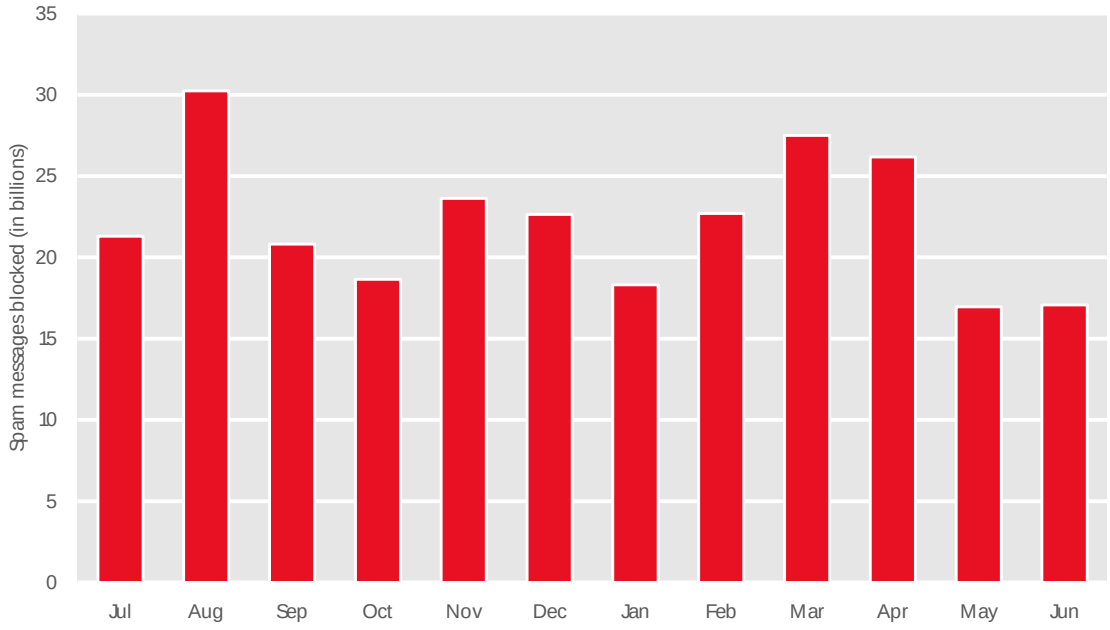
- Eight families are common to both lists. Of these, only Win32/Conficker and JS/Seedabutor were more prevalent on consumer computers than on enterprise computers. Two exploit families, Java/CVE-2012-1723 and Blacole, were among the top 10 threats for enterprises but not consumers. The worm family Win32/Gamarue and the virus family Win32/Sality were among the top 10 threats for consumers but not enterprises.
- The generic detections Win32/Obfuscator and INF/Autorun, the first and second most commonly encountered threats on consumer computers, were encountered much less frequently on enterprise computers. Obfuscator was encountered more than six times as often on enterprise computers in 2Q13 (an encounter rate of 3.8 percent) than on consumer computers (an encounter rate of 0.6 percent). Autorun was encountered more than twice as often on enterprise computers (an encounter rate of 3.4 percent) than on consumer computers (an encounter rate of 1.4 percent).

Email threats

Spam messages blocked

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

Figure 13. Messages blocked by Exchange Online Protection, July 2012–June 2013



- Blocked mail volumes in 1H13 were up slightly from 2H12, but remain well below levels seen prior to the end of 2010. The dramatic decline in spam observed since 2010 has occurred in the wake of successful takedowns of a number of large spam-sending botnets, notably Cutwail (August 2010) and Rustock (March 2011).[2] In 1H13, Exchange Online Protection determined that about 1 in 4 email messages did not require blocking or filtering, compared to just 1 in 33 messages in 2010.

[2] For more information about the Cutwail takedown, see *Microsoft Security Intelligence Report, Volume 10 (July-December 2010)*. For more information about the Rustock takedown, see "Battling the Rustock Threat," available from the Microsoft Download Center.

Figure 14. Messages blocked by Exchange Online Protection each half-year period, 2H09–1H13

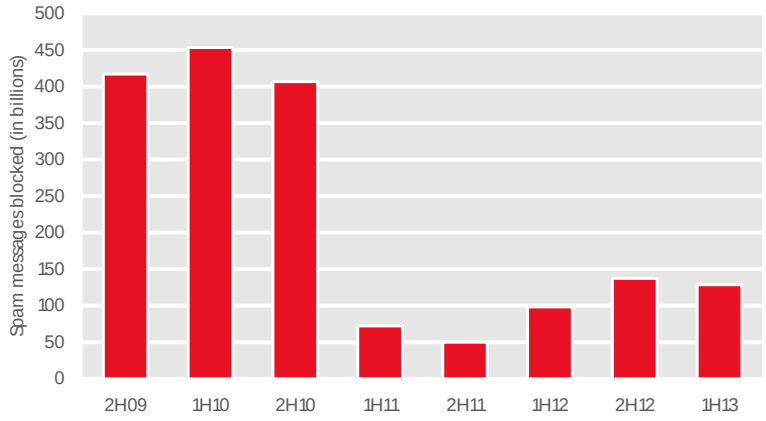
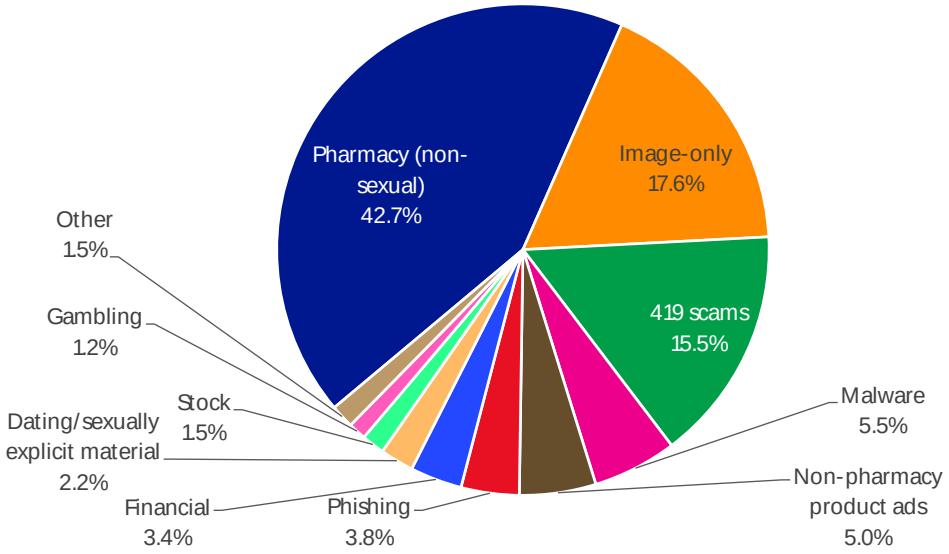


Figure 15. Inbound messages blocked by Exchange Online Protection filters in 1H13, by category



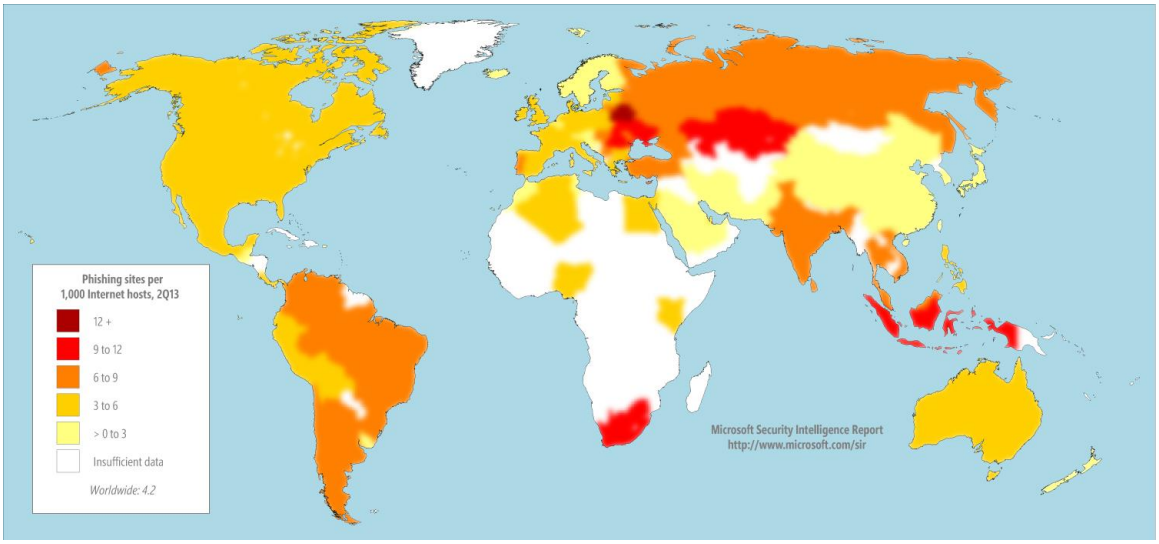
- The Exchange Online Protection content filters recognize several different common types of spam messages. Figure 15 shows the relative prevalence of the spam types that were detected in 1H13.

Malicious websites

Phishing sites

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

Figure 16. Phishing sites per 1,000 Internet hosts for locations around the world in 2Q13

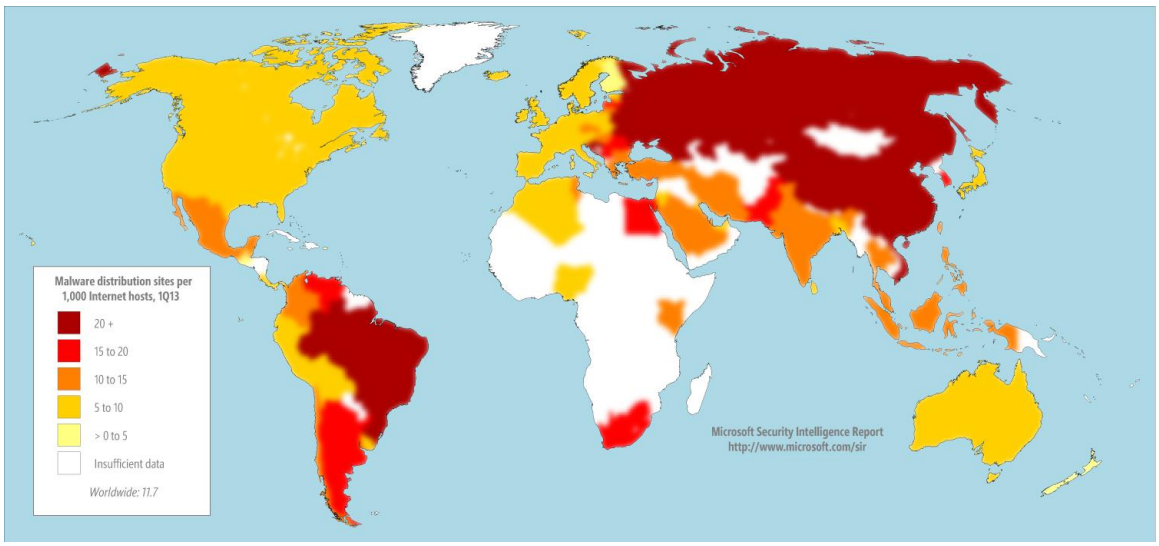


- SmartScreen Filter detected 4.2 phishing sites per 1,000 Internet hosts worldwide in 2Q13.
- Locations with higher than average concentrations of phishing sites include Indonesia (11.6 per 1,000 Internet hosts in 2Q13), Ukraine (10.9), and Russia (8.5). Locations with low concentrations of phishing sites include Taiwan (1.2), Japan (1.3), and Korea (1.9).

Malware hosting sites

SmartScreen Filter in Internet Explorer helps provide protection against sites that are known to host malware, in addition to phishing sites. SmartScreen Filter uses file and URL reputation data and Microsoft antimalware technologies to determine whether sites distribute unsafe content. As with phishing sites, Microsoft collects anonymized data regarding how many people visit each malware hosting site and uses the information to improve SmartScreen Filter and to better combat malware distribution.

Figure 17. Malware distribution sites per 1,000 Internet hosts for locations around the world in 2Q13

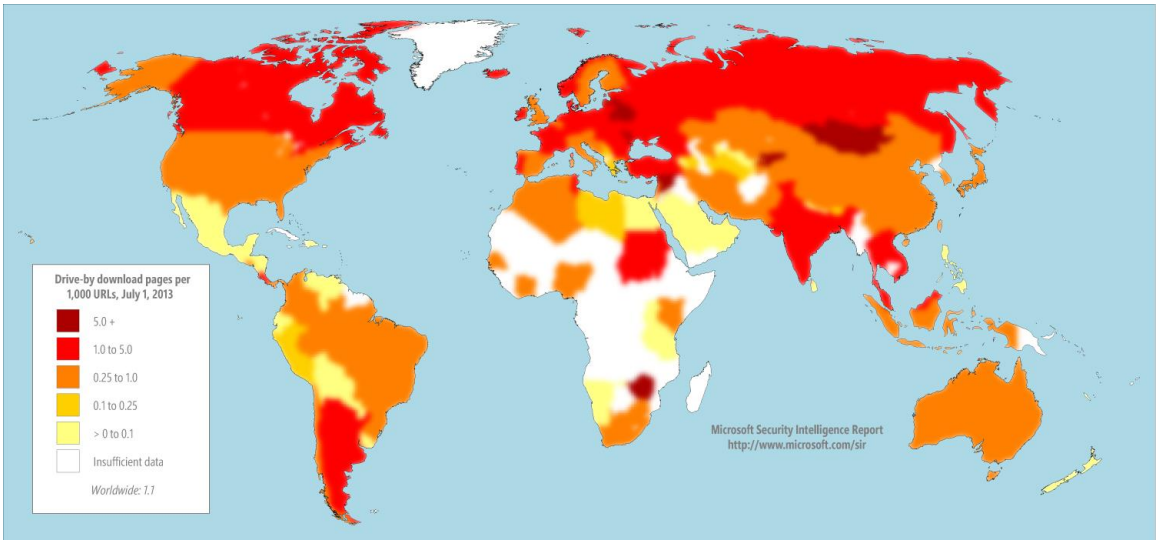


- Sites that host malware were significantly more common than phishing sites in 1H13. SmartScreen Filter detected 11.7 malware hosting sites per 1000 Internet hosts worldwide in 1Q13, and 17.7 per 1000 in 2Q13.
- China, which had a lower than average concentration of phishing sites (2.3 phishing sites per 1000 Internet hosts in 2Q13), also had a very high concentration of malware hosting sites (37.7 malware hosting sites per 1000 hosts in 2Q13). Other locations with large concentrations of malware hosting sites included Ukraine (71.2), Russia (43.6), and Brazil (33.6). Locations with low concentrations of malware hosting sites included Finland (6.1), Denmark (7.0), and Japan (7.0).

Drive-by download sites

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 18. Drive-by download pages indexed by Bing at the end of 2Q13 (bottom), per 1000 URLs in each country/region



This document summarizes the key findings of the report. The *SIR* website 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 *SIRv15* from www.microsoft.com/sir.

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