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

Microsoft Security Intelligence Report

Authors

Dennis Batchelder
Microsoft Malware Protection Center (MMPC)

Joe Blackbird
MMPC

David Felstead
Bing

Paul Henry
Wadeware LLC

Ben Hope
MMPC

Jeff Jones
Microsoft Trustworthy Computing

Aneesh Kulkarni
Windows Services Safety Platform

Marc Lauricella
Microsoft Trustworthy Computing

Russ McRee
Online Services Security & Compliance

Chad Mills
Windows Services Safety Platform

Nam Ng
Microsoft Trustworthy Computing

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Anthony Penta
Windows Services Safety Platform

Tim Rains
Microsoft Trustworthy Computing

Vidya Sekhar
MMPC

Holly Stewart
MMPC

Matt Thomlinson
Microsoft Trustworthy Computing

Todd Thompson
Microsoft IT Information Security and Risk Management

Terry Zink
Microsoft Exchange Online Protection

Contributors

Danielle Alyias
Microsoft Trustworthy Computing

Joe Faulhaber
MMPC

Methuselah Cebrian Ferrer
MMPC

Peter Ferrie
MMPC

Tanmay Ganacharya
MMPC

Kathryn Gillespie
Microsoft IT Information Security and Risk Management

Enrique Gonzalez
MMPC

Jonathan Green
MMPC

Angela Gunn
Microsoft Trustworthy Computing

Joe Gura
Microsoft Trustworthy Computing

Chris Hale
Microsoft Trustworthy Computing

Satomi Hayakawa
CSS Japan Security Response Team

Aaron Hulett
MMPC

Jimmy Kuo
MMPC

Hilda Larina Ragragio
MMPC

Jenn LeMond
Microsoft IT Information Security and Risk Management

Ken Malcolmson
Microsoft Trustworthy Computing

Marianne Mallen
MMPC

Scott Molenkamp
MMPC

Daric Morton
Microsoft Services

Yurika Muraki
CSS Japan Security Response Team

Takumi Onodera
Microsoft Premier Field Engineering, Japan

Bill Pfeifer
MMPC

Cynthia Sandvick
Microsoft Trustworthy Computing

Richard Saunders
Microsoft Trustworthy Computing

Jasmine Sesso
MMPC

Frank Simorjay
Microsoft Trustworthy Computing

Francis Tan Seng
MMPC

Henk van Roest
CSS Security EMEA

Steve Wacker
Wadeware LLC

Shawn Wang
MMPC

Bob White
Microsoft IT Information Security and Risk Management

Iaan Wiltshire
MMPC

Dan Wolff
MMPC

Table of contents

About this report

The *Microsoft Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, and malicious and potentially unwanted software. 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

This volume of the *Microsoft Security Intelligence Report* focuses on the first and second quarters of 2013, with trend data for the last several quarters presented on a quarterly basis. Because vulnerability disclosures can be highly inconsistent from quarter to quarter and often occur disproportionately at certain times of the year, statistics about vulnerability disclosures are presented on a half-yearly basis.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, in which *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). To avoid confusion, please note 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 "Appendix A: Threat naming conventions" on page 123. In this report, any threat or group of threats that share a common unique base name is considered a family for the sake of presentation. This consideration includes threats that may not otherwise be considered families according to common industry practices, such as adware programs and generic detections. For the purposes of this report, a "threat" is defined as a malware or potentially unwanted software family or variant that is detected by the Microsoft Malware Protection Engine.

Trustworthy Computing: Security engineering at Microsoft

Amid the increasing complexity of today's computing threat landscape and the growing sophistication of criminal attacks, enterprise organizations and governments are more focused than ever on protecting their computing environments so that they and their constituents are safer online. With more than a billion systems using its products and services worldwide, Microsoft collaborates with partners, industry, and governments to help create a safer, more trusted Internet.

The Microsoft Trustworthy Computing organization focuses on creating and delivering secure, private, and reliable computing experiences based on sound business practices. Most of the intelligence provided in this report comes from Trustworthy Computing security centers—the Microsoft Malware Protection Center (MMPC), Microsoft Security Response Center (MSRC), and Microsoft Security Engineering Center (MSEC)—which deliver in-depth threat intelligence, threat response, and security science. Additional information comes from product groups across Microsoft and from Microsoft IT, the group that manages global IT services for Microsoft. The report is designed to give Microsoft customers, partners, and the software industry a well-rounded understanding of the threat landscape so that they will be in a better position to protect themselves and their assets from criminal activity.

Cloud security: Conflict and cooperation

As one of the largest and fastest growing operators of cloud services in the world, Microsoft makes cloud security a top priority. Incidents are handled by multiple teams throughout the company, and many business groups have their own incident response teams with specific focus areas and authority. Despite this decentralized structure, all Microsoft cloud incident response teams face certain intrinsic challenges. For example, the infrastructure required to serve hundreds of millions of customer accounts on every continent generates an astronomical amount of data in the form of logs, alerts, and other telemetry. Over the course of one recent month, the domain controller logs for servers that manage primary Microsoft production environment domains generated 57.1 billion Windows security events. Add in network data (including NetFlow telemetry), firewall events, and intrusion prevention system (IPS) events, and event counts easily reach the trillions. And that's primarily from non-virtual systems!

Even at this scale, the Microsoft cloud infrastructure faces many of the same security challenges and attack patterns that affect much smaller computing environments. The scale may be vastly different, but many of the challenges that Microsoft cloud services administrators and security response teams face are similar or identical in nature to issues faced by every IT administrator reading this report. For example, administrators who manage monthly security updates from Microsoft might find it interesting to consider that the Microsoft cloud team deploys the same set of updates to a server base numbering in the hundreds of thousands. Automation plays an invaluable role, but system administration in massive, distributed cloud infrastructures is still a significant undertaking.

Similarly, some of the high-profile attack vectors that have been deeply problematic for system administrators around the world in recent times have not gone unnoticed by Microsoft cloud security teams. This section of the *Microsoft Security Intelligence Report* examines two of these attack vectors from the perspective of Microsoft cloud services and incident response teams.

Domain Name System (DNS) attacks

Attacks on the global Domain Name System (DNS) are some of the most serious and potentially damaging attacks affecting the Internet today. A group of malicious hackers calling itself the "Syrian Electronic Army" made headlines in mid-2013 when it successfully compromised a registrar that manages DNS

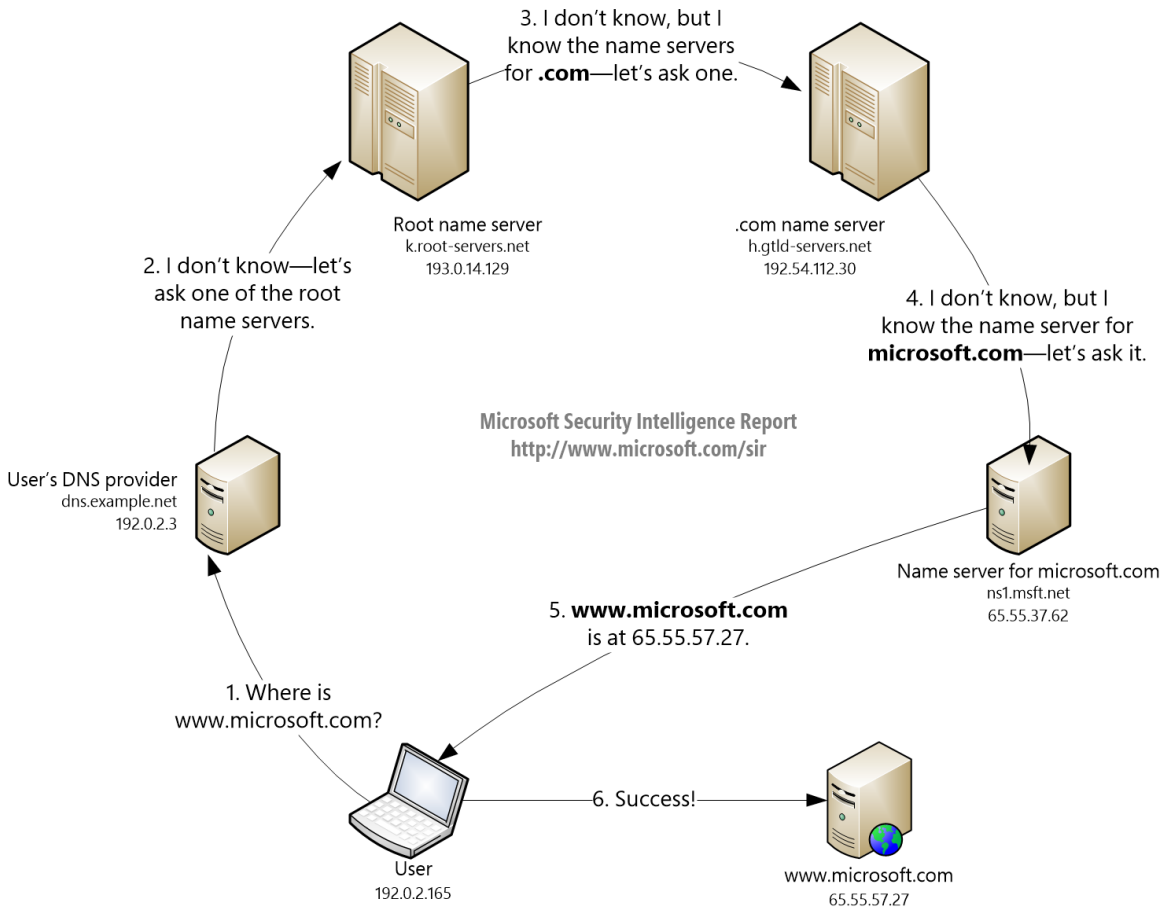
records for *The New York Times* and Twitter.[1] Over the last few years, Microsoft has experienced similar attacks, some of which were politically motivated, against registries managing its DNS records in specific markets. This malicious manipulation of DNS records has an adverse impact not only on Microsoft but on the global online community as well, including Microsoft industry peers, partners, and customers.

When a computer user requests a domain-based URL from a web browser, the computer usually must query at least one DNS name server to resolve the alphanumeric domain string into an IP address that can be used to locate and retrieve the desired web page. In a typical case, visiting a URL such as *www.microsoft.com* might require querying at least four different name servers:[2]

[1] Timothy B. Lee, "The New York Times Web site was taken down by DNS hijacking. Here's what that means," *The Washington Post*, August 27, 2013, www.washingtonpost.com/blogs/the-switch/wp/2013/08/27/the-new-york-times-web-site-was-taken-down-by-dns-hijacking-heres-what-that-means/.

[2] In practice, techniques such as DNS caching and hosts file lookups usually eliminate one or more of these steps for most queries.

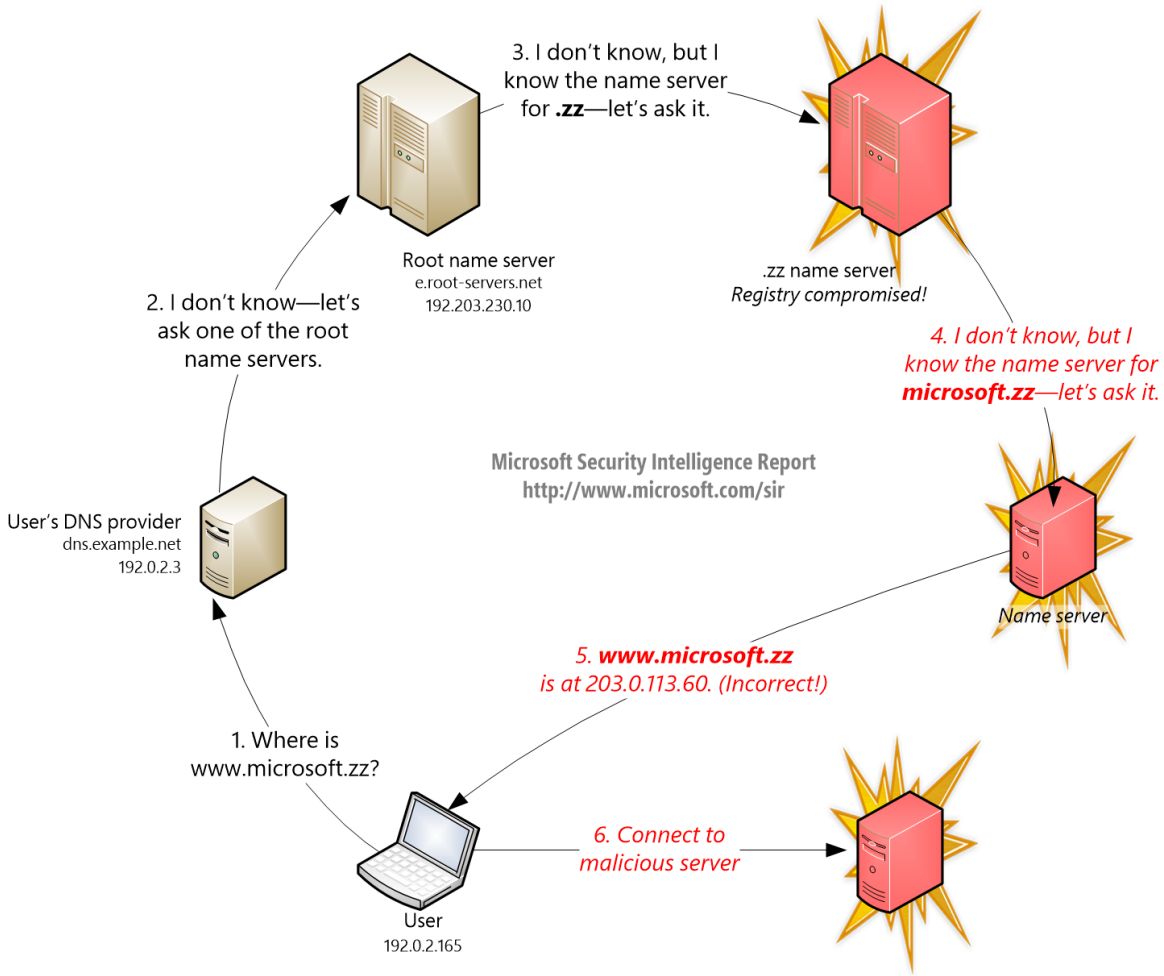
Figure 1. A simplified diagram of the DNS address resolution process



1. The computer queries the recursive DNS server for the network connection being used. A recursive DNS server handles DNS queries for its clients by locating and querying other DNS servers (called authoritative name servers), which are designated to provide authoritative address lookups for specific individual domains.
2. If the recursive name server doesn't have the answer, it queries one of the 13 root name servers (which correspond to hundreds of physical servers located around the world).
3. The root name server maintains a record of the authoritative name servers for the *.com* top-level domain (TLD) and queries one of them.
4. The *.com* name server maintains a record of the authoritative name server for the *microsoft.com* domain, and queries that server.
5. The *microsoft.com* name server maintains a record of the IP address for the *www* subdomain, and returns the IP address.

If attackers successfully compromise one of the name servers or registries in this chain, they can redirect DNS queries to a malicious name server. For example, a compromise of the authoritative name server for microsoft.com could result in requests for *www.microsoft.com* being redirected to an IP address of the attacker's choosing, which may serve malware or contain a maliciously altered version of the Microsoft website. The potential for greater damage increases as one travels up the DNS hierarchy; a hypothetical compromise of one of the root name servers could conceivably put every domain on the Internet in jeopardy.

Figure 2. A compromised registry can result in malicious responses being issued to DNS queries

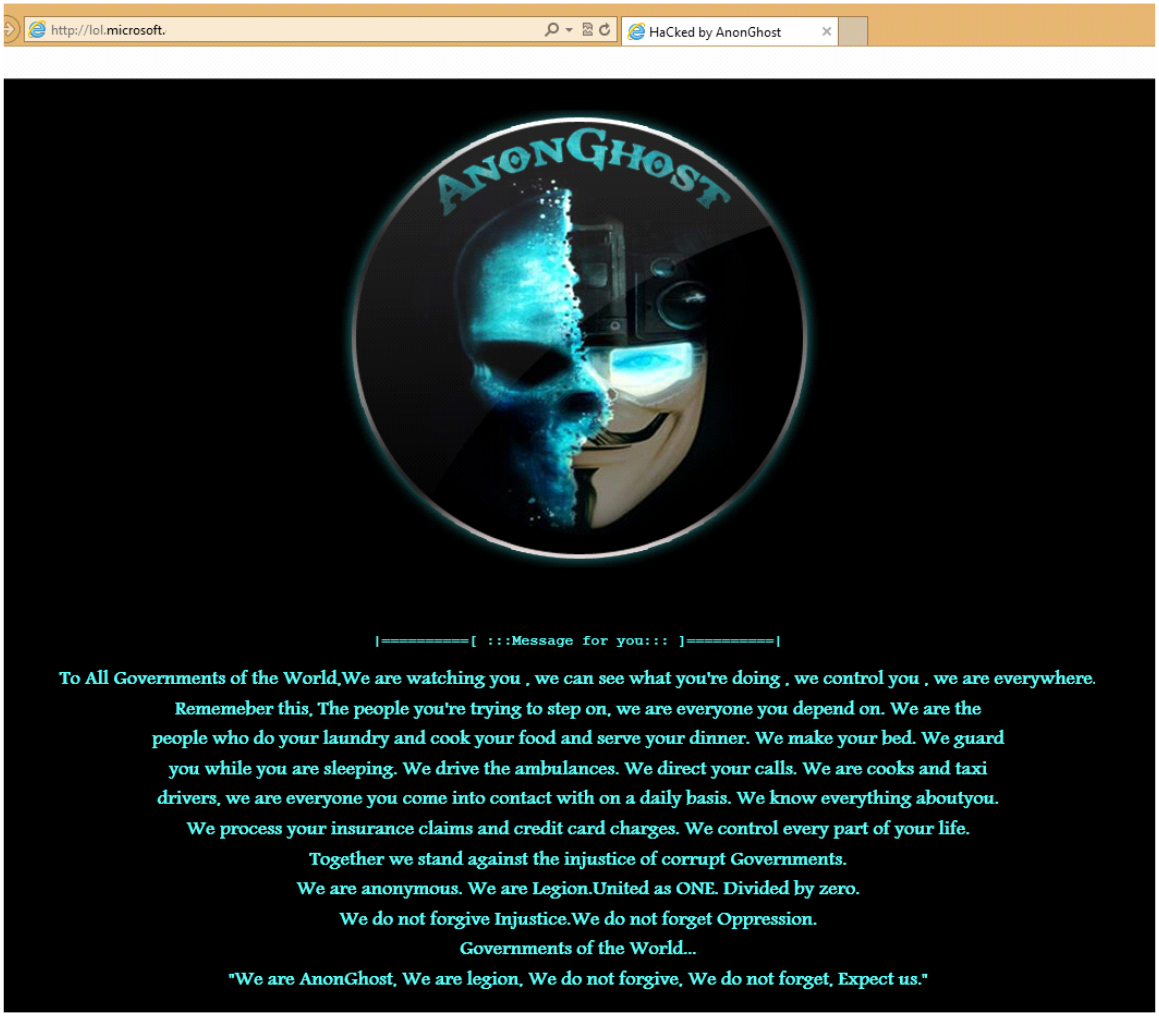


The exploitation of vulnerabilities that are specific to country-code top-level domain (ccTLD) registries has become increasingly common, especially in relatively small markets. A ccTLD is a top-level domain that is generally used or reserved for a country or region, such as .ca for Canada. There are currently

more than 300 ccTLD name registries responsible for servicing hundreds of millions of domain names worldwide. Domains registered under ccTLDs are typically websites or other resources that cater to the associated country or region for those who wish a web presence in their country of origin, or for companies that seek to grow their presence and market share in such countries. For example, Microsoft maintains registered domains under a number of different ccTLDs for its regional subsidiaries, such as microsoft.ca for Microsoft Canada and microsoft.co.jp for Microsoft Japan. Domains that are registered under ccTLDs help create positive Internet experiences for users in different communities by providing locally targeted resources at familiar and predictable domain names. Unfortunately, the name servers run by some ccTLD registrars are vulnerable to attack, which can negatively affect individuals, nonprofits, and government organizations as well small companies and large corporations such as Microsoft. Between May 2012 and July 2013, 17 ccTLDs that manage DNS records for Microsoft (and many other organizations) in specific countries and regions were compromised, often through a combination of Structured Query Language (SQL) injection exploits and social engineering.

When computer users attempt to reach a website whose DNS record has been hijacked, they are typically redirected to a server controlled by an attacker. This server may contain web browser exploit kits or malware, or may display malicious or inappropriate content. For example, in May 2013 a group of malicious hackers calling itself "AnonGhost" redirected queries for a Microsoft regional website to a server it controlled, as shown in Figure 3.

Figure 3. The appearance of a website defacement resulting from a compromised DNS record



To the computer user it appears as though the website itself has been compromised, even though the owner of the targeted website usually has no control over the ccTLD and is not responsible for the incident. Users typically can't differentiate between a problem with the ccTLD or the organization that runs the website they wish to browse, and even advanced users may have considerable trouble distinguishing between a website problem and a DNS problem. This type of DNS hijacking diminishes public confidence in the victimized organizations and adversely affects their reputations.

Although security best practices, reviews, training, and awareness can help prevent these types of attacks, the frequency and impact of such attacks have prompted Microsoft to offer help to registries. Microsoft now offers the ccTLD Registry Security Assessment Service, which helps registry operators find and fix

vulnerabilities at no charge before they are exploited.[3] Microsoft believes that close collaboration in this effort between industry peers, partners, and industry groups such as ICANN can help increase awareness for ccTLDs and reduce the unfortunate impact of DNS records manipulation.

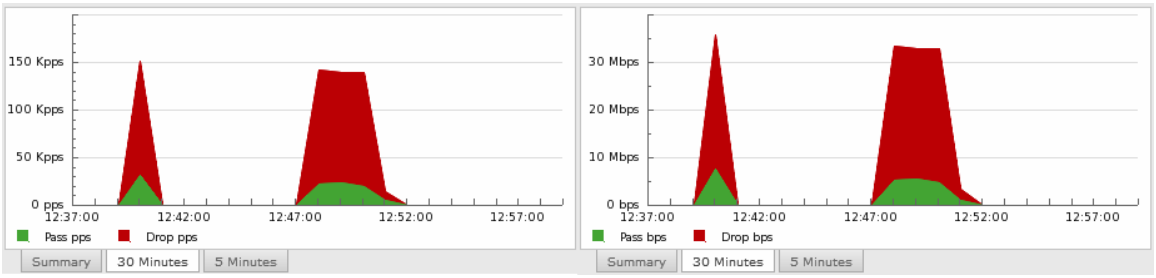
Distributed Denial of Service (DDoS) attacks

Another common attack vector that has been used to attempt to adversely affect cloud and online services at Microsoft is Distributed Denial of Service (DDoS), including attacks that result from *DNS amplification* (a technique that involves using publicly accessible open DNS servers to flood the target system with DNS traffic). DNS amplification made headlines in March 2013, when attackers used the technique to attack the Spamhaus spam prevention service with as much as 300 gigabits per second (Gbps) of traffic.[4]

On a daily basis, Microsoft's DDoS protective measures apply mitigations to prevent impact from DoS and DDoS attacks to ensure uptime and availability for services and customers. Common types of attack include SYN floods, DNS amplification, malformed packets (TCP and UDP), and application layer abuses specific to HTTP and DNS. One common attack technique used by a number of freely available DDoS toolkits involves using fragmented IP packets with a fixed payload, as described below.

A DDoS attack in progress quickly shows up on monitoring telemetry as a significant elevation of both packets-per-second and bits-per-second traffic, as seen in Figure 4. The 30Mbps attack shown here is nominal, but if left unchecked could impact the availability of the service.

Figure 4. Flow monitoring telemetry during a DDoS attack



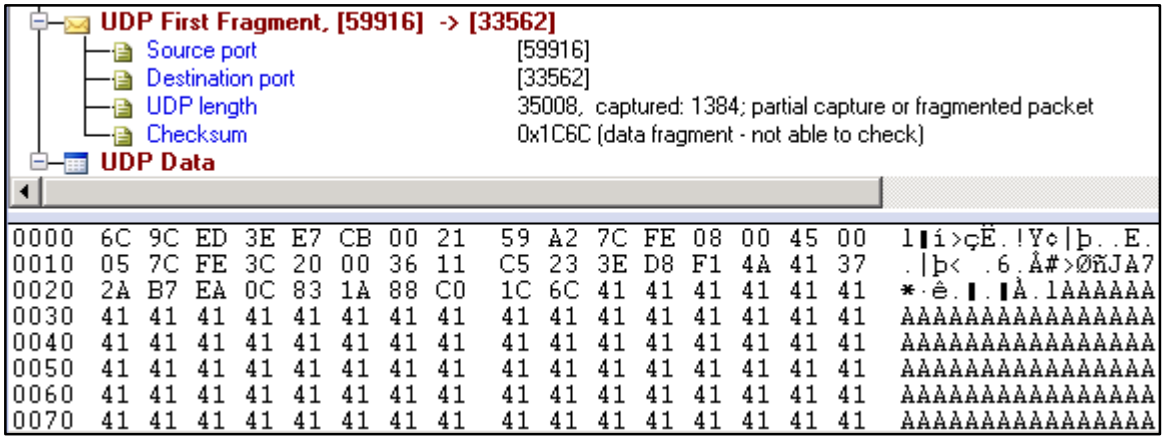
[3] For more information, see the entry "Microsoft Offers Security Assessment Service for Country-Code Top-Level Domain Registries (ccTLD)" (February 26, 2013) on the Microsoft Security Blog at blogs.technet.com/security.

[4] Michael McNally, "What is a DNS Amplification Attack?", *ISC Knowledge Base*, April 1, 2013, https://deepthought.isc.org/article/AA-00897/0/What-is-a-DNS-Amplification-Attack.html.

A typical attack involving IP fragments might consist of a padded payload consisting of a single ASCII letter, such as A (0x41 in hexadecimal), repeated many times, and transmitted using multiple communications protocols, including User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), KRYPTOLAN, Versatile Message Transaction Protocol (VMTP), Internet Protocol version 6 (IPv6), Extensible Name Service (XNS), and others. Packets often include full 1,518-byte payloads, and the UDP fragments are directed to multiple destination ports.

Figure 5 represents a UDP fragment that was captured during an attack.

Figure 5. A UDP fragment from a DDoS attack



During one 60-second window, Microsoft detected more than 8,985 unique IP addresses sending fragmented traffic during the attack. As the service was forced to drop incoming packets during the attacks, it is believed that the actual volume of the attack may have been considerably greater than what Microsoft was able to analyze.

An investigation of a host known to have participated in a recent attack, acquired via appropriate legal means by the Microsoft Digital Crimes Unit (DCU), revealed a common attack tool (currently detected as Backdoor:Perl/IRCbot.E) that was used for UDP flooding.

Figure 6. Perl code from a UDP flooding trojan

```
##############
if ($funcarg =~ /^udp2\s+(.*)\s+(\d+)\s+(\d+)/) {
        sendraw($IRC_cur_socket, "PRIVMSG $printl :┐└4,1 [UDP-2 DDOS]┐ └9,1Attacking └12".$1." └9,1with └12".$2." └9,1Kb Packets for └12".$3."
        └9,1seconds. └");
        my ($dtime, %pacotes) = udpflooder("$1", "$2", "$3");
        $dtime = 1 if $dtime == 0;
        my %bytes;
        $bytes{igmp} = $2 * $pacotes{igmp};
        $bytes{icmp} = $2 * $pacotes{icmp};
        $bytes{o} = $2 * $pacotes{o};
        $bytes{udp} = $2 * $pacotes{udp};
        $bytes{tcp} = $2 * $pacotes{tcp};
        sendraw($IRC_cur_socket, "PRIVMSG $printl :┐└4,1 [UDP-2 DDOS]┐ └9,1Results └12".int(($bytes{icmp}+$bytes{igmp}+$bytes{udp} + $bytes{o}
        /1024)." └9,1Kb in └12".$dtime." └9,1seconds to └12".$1."└9,1. └");
}
```

Tools such as this IRCbot provide even the most unsophisticated attackers a platform from which to launch potentially damaging attacks on cloud services. Although the defensive measures and tactics employed by Microsoft help mitigate such attacks, it can nonetheless be burdensome and resource intensive to do so.

Guidance: Preventing and mitigating DNS and DDoS attacks

For owners of websites in vulnerable ccTLDs, preventing DNS attacks at the TLD level can be very difficult or impossible. Website owners should urge their ccTLD registrars to visit www.microsoft.com/cctldregsec and take advantage of the Microsoft ccTLD Registry Security Assessment Service to find and mitigate any vulnerabilities that may leave domains open to attack.

Because attackers also target individual domains for DNS hijacking directly, website owners should act to ensure that their designated authoritative name servers cannot be changed without their approval. Many domain name registrars offer domain locking services that can help prevent DNS records from being changed without the domain owner's approval. Website owners should take advantage of any locking services offered by their registrars, and should urge registrars to offer such services if they do not. Site owners should also take general precautions to secure their domain names against unauthorized changes, such as carefully protecting the usernames and passwords they use to access their domain registry accounts, and only using SSL connections to review their accounts or make changes.

Because DDoS attacks are so difficult to mitigate, it's important that DNS administrators everywhere be willing to cooperate with each other to prevent attacks from happening in the first place. The United States Computer Emergency Readiness Team (US-CERT) has provided some suggestions to help

administrators stop attackers from taking advantage of their DNS servers to launch attacks.[5]

- Most DNS amplification attacks take advantage of open DNS name servers, which resolve DNS queries submitted to them by any computer on the Internet. System administrators should configure their DNS servers to ignore queries they receive from hosts outside their domain. A number of tools are available for helping administrators detect misconfigured DNS servers within their networks, including:
  - The Open Resolver Project (openresolverproject.org) maintains a list of open DNS resolvers and provides an interface for searching an IP range for open resolvers.
  - The Measurement Factory (dns.measurement-factory.com) also maintains a list of open resolvers and offers a free tool to test a single server to determine if it allows open recursion.
  - DNSInspect (dnsinspect.com) is another free tool for testing DNS resolvers, and it can also test an entire DNS zone for other possible configuration and security issues.
- Administrators of DNS resolvers can take a number of steps to prevent their resources from being used in attacks, including:
  - *Source IP verification*. Even well-configured DNS resolvers can be exploited by attackers who use source IP address spoofing to issue DNS queries. The Internet Engineering Task Force has released two Best Current Practice documents (tools.ietf.org/html/bcp38, tools.ietf.org/html/bcp84) that can help system administrators perform network ingress filtering, which rejects packets that appear to originate from addresses that cannot be reached via the paths the packets actually take.
  - *Disabling recursion on authoritative name servers*. An authoritative name server is one that provides public name resolution for a specified domain (such as *microsoft.com*) and optionally one or more subdomains (such as *www.microsoft.com*). Because authoritative name servers must be publicly accessible, they should be configured to reject recursive queries from clients. For help disabling recursion in Windows Server, see

[5] See https://www.us-cert.gov/ncas/alerts/TA13-088A for the full alert from US-CERT.

"Disable Recursion on the DNS Server" at Microsoft Technet (technet.microsoft.com).

- *Limiting recursion to authorized clients*. DNS servers that are deployed within an organization or Internet service provider (ISP) should be configured to perform recursive queries on behalf of authorized clients only, preferably restricted to clients within the organization's network.

Although attacks on popular cloud services tend to make the most headlines, DDoS attacks can—and do—happen to anyone. In fact, well-run cloud services tend to be much better prepared to deal with DDoS attacks than most enterprise IT infrastructures, because successfully overwhelming a large cloud service requires a level of coordination that few prospective attackers are likely to achieve. Organizations that have struggled with DDoS attacks on their websites or other vital parts of their network infrastructures should consider moving some resources to the cloud to take advantage of the security and operations benefits that cloud services provide.

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 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.

Industry-wide vulnerability disclosures

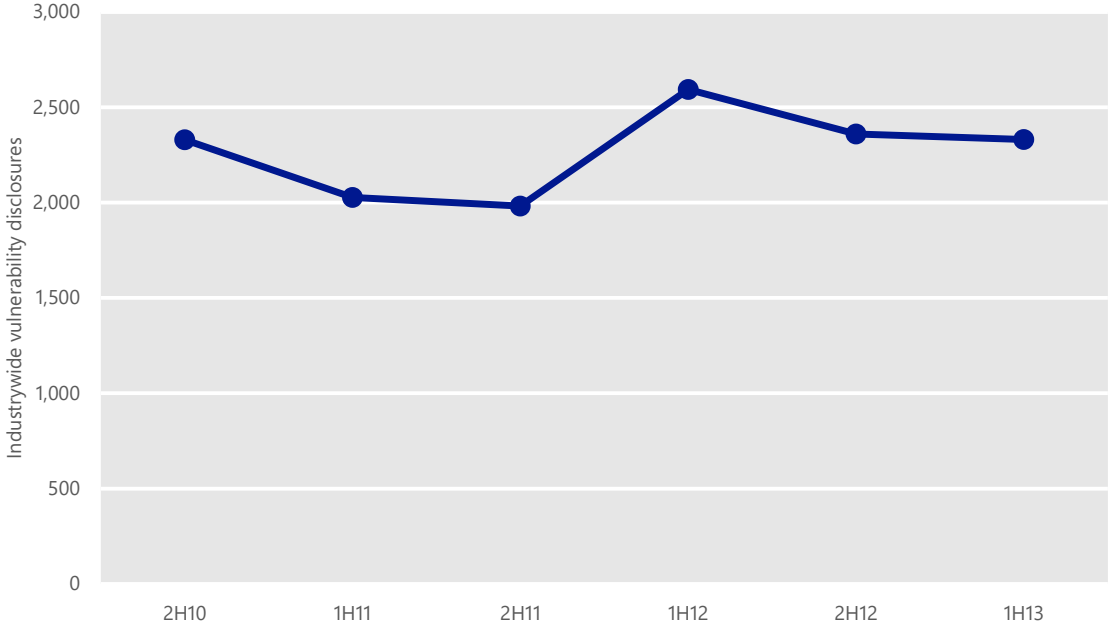
A *disclosure*, as the term is used in the *Microsoft Security Intelligence Report*, is the revelation of a software vulnerability to the public at large. Disclosures can come from a variety of sources, including publishers of the affected software, security software vendors, independent security researchers, and even malware creators.

The information in this section is compiled from vulnerability disclosure data that is published in the National Vulnerability Database (NVD), the US government's repository of standards-based vulnerability management data at nvd.nist.gov. The NVD represents all disclosures that have a published CVE (Common Vulnerabilities and Exposures) identifier.[6]

Figure 7 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 2H10. (See "About this report" on page v for an explanation of the reporting period nomenclature used in this report.)

[6] CVE entries are subject to ongoing revision as software vendors and security researchers publish more information about vulnerabilities. For this reason, the statistics presented here may differ slightly from comparable statistics published in previous volumes of the *Microsoft Security Intelligence Report*.

Figure 7. Industrywide vulnerability disclosures, 2H10–1H13



- 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. (See "Operating system, browser, and application vulnerabilities" on page 21 for more information.)
- An increase in application vulnerability disclosures in 1H12 interrupted a trend of consistent period-over-period decreases dating back to 2H09. It remains to be seen whether the decrease in 2H12 marks a return to this trend. 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.

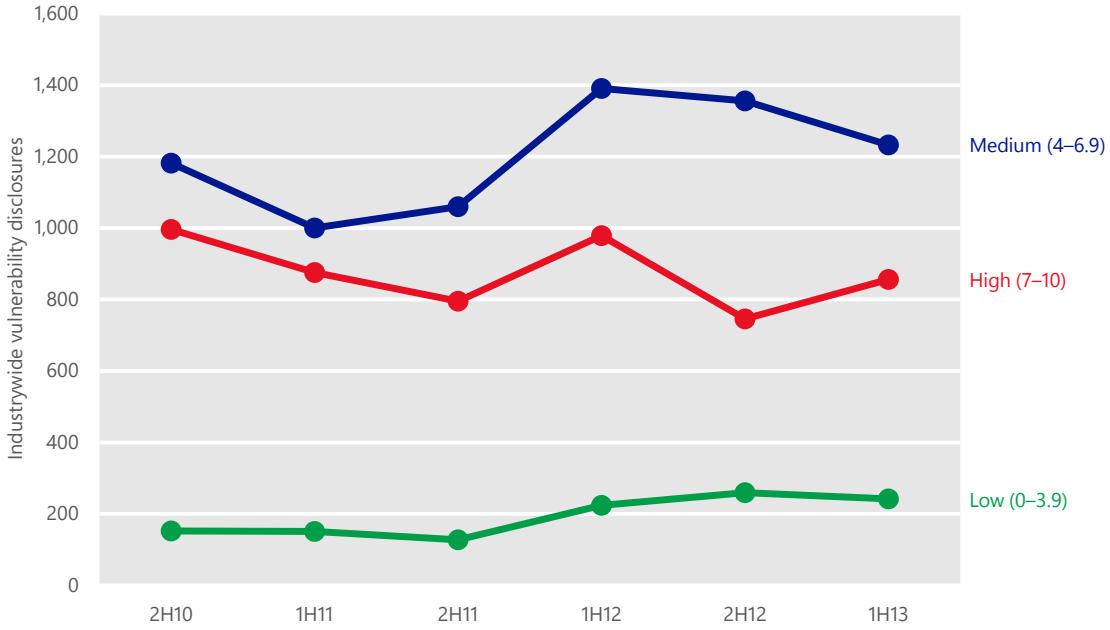
  For a ten-year view of the industry vulnerability disclosure trend, see the entry "Trustworthy Computing: Learning About Threats for Over 10 Years–Part 4" (March 15, 2012) at the Microsoft Security Blog at blogs.technet.com/security.

Vulnerability severity

The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities. The CVSS base metric

assigns a numeric value between 0 and 10 to vulnerabilities according to severity, with higher scores representing greater severity. (See Vulnerability Severity at the *Microsoft Security Intelligence Report* website (www.microsoft.com/sir) for more information.)

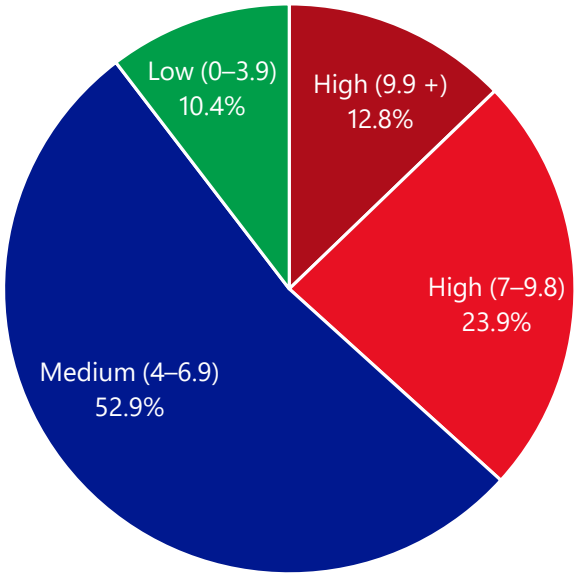
Figure 8. Industrywide vulnerability disclosures by severity, 2H10–1H13



- High-severity vulnerability disclosures increased 12.9 percent industrywide in 1H13, after decreasing by 31.2 percent from 1H12 to 2H12. High-severity vulnerabilities accounted for 36.7 percent of total disclosures in 1H13, compared to 31.6 percent in the previous period.
- Medium-severity vulnerability disclosures decreased 10.0 percent from 2H12, and accounted for 52.9 percent of total disclosures in 2H12.
- Low-severity vulnerability disclosures decreased 7.0 percent from 2H12. They remained relatively low in 1H13, and accounted for 10.4 percent of total disclosures.
- Mitigating the most severe vulnerabilities first is a security best practice. Vulnerabilities that scored 9.9 or greater represent 12.8 percent of all vulnerabilities disclosed in 1H13, as Figure 9 illustrates. These figures are an increase from 2H12, when vulnerabilities that scored 9.9 or greater accounted for 11.2 percent of all vulnerabilities. Vulnerabilities that scored

between 7.0 and 9.8 increased to 23.9 percent in 1H13 from 20.4 percent in 2H12.

Figure 9. Industrywide vulnerability disclosures in 1H13, by severity

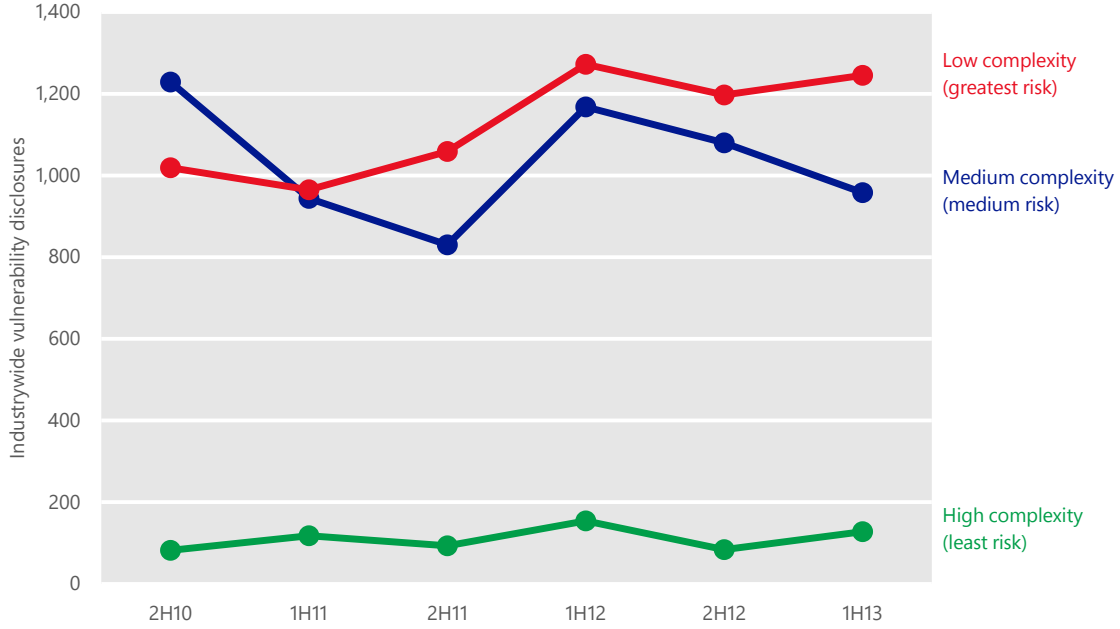


Vulnerability complexity

Some vulnerabilities are easier to exploit than others, and vulnerability complexity is an important factor to consider in determining the magnitude of the threat that a vulnerability poses. A high-severity vulnerability that can only be exploited under very specific and rare circumstances might require less immediate attention than a lower-severity vulnerability that can be exploited more easily.

The CVSS assigns each vulnerability a complexity ranking of Low, Medium, or High. (See Vulnerability Complexity on the *Microsoft Security Intelligence Report* website for more information about the CVSS complexity ranking system.) Figure 10 shows complexity trends for vulnerabilities disclosed since 2H10. Note that Low complexity in Figure 10 indicates greater risk, just as High severity indicates greater risk in Figure 8.

Figure 10. Industrywide vulnerability disclosures by access complexity, 2H10–1H13



- Disclosures of Low-complexity vulnerabilities—those that are the easiest to exploit—accounted for 53.4 percent of all disclosures in 1H13, an increase from 50.7 percent in 2H12.
- Disclosures of Medium-complexity vulnerabilities accounted for 41.1 percent of all disclosures in 1H13, a decrease from 45.7 percent in 2H12.
- Disclosures of High-complexity vulnerabilities increased to 5.5 percent of all disclosures in 2H12, an increase from 3.6 percent in 1H12.

Operating system, browser, and application vulnerabilities

Comparing operating system vulnerabilities to non-operating system vulnerabilities that affect other components requires determining whether a particular program or component should be considered part of an operating system. This determination is not always simple and straightforward, given the componentized nature of modern operating systems. Some programs (media players, for example) ship by default with some operating system software but can also be downloaded from the software vendor's website and installed individually. Linux distributions, in particular, are often assembled from

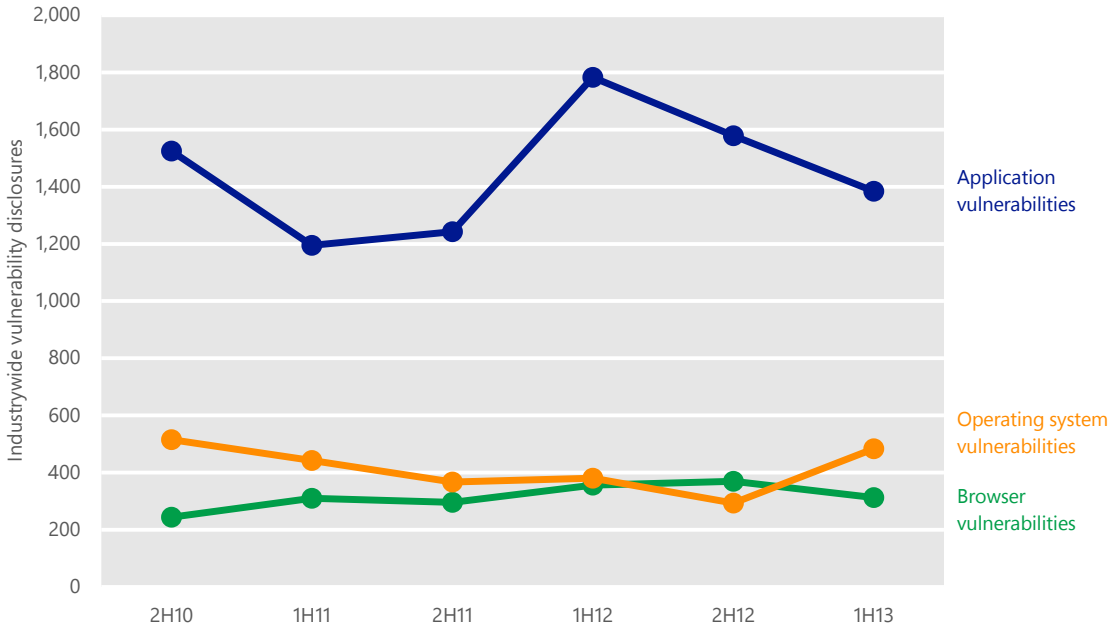
components developed by different teams, many of which provide crucial operating functions such as a graphical user interface (GUI) or Internet browsing.

To facilitate analysis of operating system and browser vulnerabilities, the *Microsoft Security Intelligence Report* distinguishes among three different kinds of vulnerabilities:

- *Operating system vulnerabilities* are those that affect the Linux kernel, or that affect components that ship with an operating system produced by Microsoft, Apple, or a proprietary Unix vendor, and are defined as part of the operating system by the vendor, except as described in the next paragraph.
- *Browser vulnerabilities* are those that affect components defined as part of a web browser, including web browsers such as Internet Explorer and Apple's Safari that ship with operating systems, along with third-party browsers such as Mozilla Firefox and Google Chrome.
- *Application vulnerabilities* are those that affect all other components, including executable files, services, and other components published by operating system vendors and other vendors. Vulnerabilities in open-source components that may ship with Linux distributions (such as the X Window System, the GNOME desktop environment, the GNU Image Manipulation Program (GIMP), and others) are considered application vulnerabilities.

Figure 11 shows industry-wide vulnerabilities for operating systems, browsers, and applications since 2H10.

Figure 11. Industrywide operating system, browser, and application vulnerabilities, 2H10–1H13

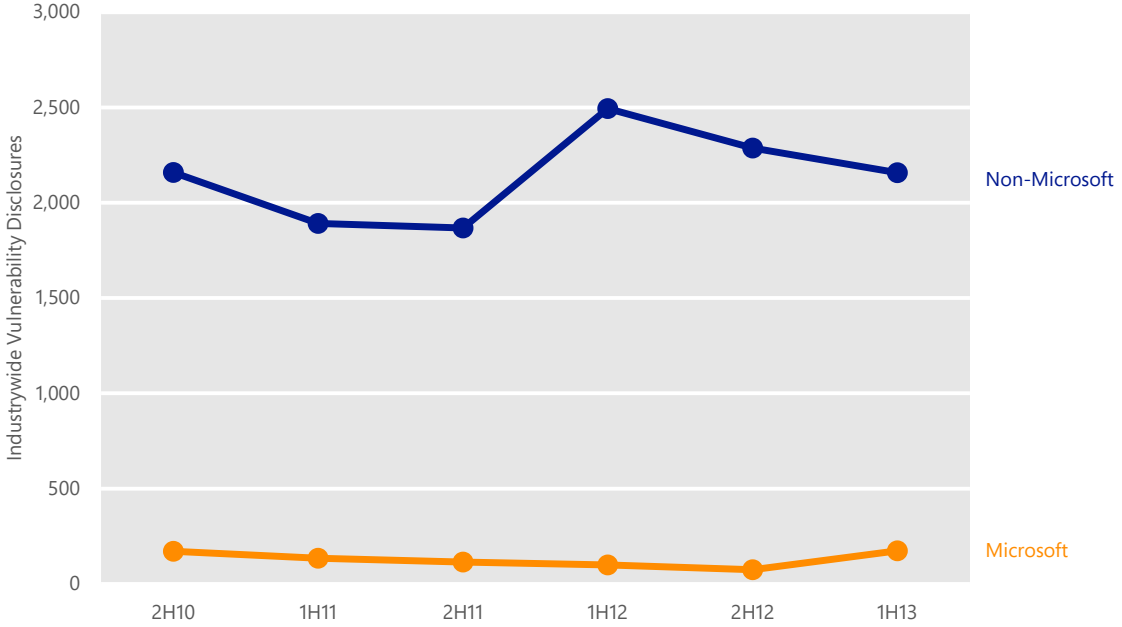


- Application vulnerability disclosures decreased 12.9 percent in 1H13 and accounted for 63.5 percent of total disclosures for the period.
- After several periods of decline, operating system vulnerability disclosures increased 39.3 percent in 1H13, outnumbering browser vulnerabilities. Overall, operating system vulnerabilities accounted for 22.2 percent of total disclosures for the period.
- Browser vulnerability disclosures decreased 18.3 percent in 1H13 and accounted for 14.3 percent of total disclosures for the period.

Microsoft vulnerability disclosures

Figure 12 shows vulnerability disclosures for Microsoft and non-Microsoft products since 2H10.

Figure 12. Vulnerability disclosures for Microsoft and non-Microsoft products, 2H10–1H13



- After several periods of decline, disclosures of vulnerabilities in Microsoft products increased to 7.4 percent of all disclosures across the industry, an increase from 3.1 percent in 2H12.

Guidance: Developing secure software

The Security Development Lifecycle (SDL) (www.microsoft.com/sdl) is a free software development methodology that incorporates security and privacy best practices throughout all phases of the development process with the goal of protecting software users. Using such a methodology can help reduce the number and severity of vulnerabilities in software and help manage vulnerabilities that might be found after deployment. See "State of Application Security: Immature Practices Fuel Inefficiencies, but Positive ROI Is Attainable - A Forrester Consulting Thought Leadership Paper Commissioned by Microsoft" to learn how companies are putting SDL techniques to work for them, and "Secure Software Development Trends in the Oil & Gas Sectors" for an example of how the SDL has helped one critical industry. Both papers are available from the Microsoft Download Center (www.microsoft.com/download).

For more in-depth information about the SDL and other techniques developers can use to secure their software, see Protecting Your Software in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website.

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[7] (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 understand the totality of what 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.

Used in combination, these two perspectives provide Microsoft with an improved overall assessment of malware impact and risk.

- The MSRT detects and removes a chosen set of highly prevalent or serious threats (203 malware families as of the June 2013 release). Specific families are selected on the basis of prevalence worldwide, on various platforms, and other similar criteria to ensure that adding detection signatures for a family would remove infections from a significantly large population of computers worldwide. By contrast, Microsoft real-time security products include detection signatures for all of the threat families in the Microsoft Malware Protection Engine database, which amounts to tens of thousands of families. The encounter rate therefore encompasses a much larger group of families than the infection rate as measured by CCM.

[7] See "Appendix B: Data sources" on page 126 for more information about the MSRT and the other products that provide data for this report.

- As "Regional Threat Assessment" on the *Microsoft Security Intelligence Report* website illustrates, the malware landscape has become significantly more regionally focused in recent years, and one country or region can display a significantly different mix of prevalent threats than another. The most prevalent malware family in one country might be all but unknown in the rest of the world, and may never be selected for the MSRT. Assessing threats that affect different populations demands an understanding of infection rates in the context of the overall prevalence of malware—which is measured with the encounter rate.
- The MSRT runs on computers that are protected by security software published by many different vendors, using a variety of detection signatures and mechanisms, as well as on computers that are not protected by real-time security software at all. The infection rate data produced by the MSRT therefore comes from a wider and more varied population of computers and devices than does encounter rate data, which comes exclusively from computers that are protected by Microsoft real-time security products.

For an accurate understanding of the threats that affect computers today, it's important to consider infection attempts that are blocked as well as the infections that are removed—data that can only be provided by real-time security products, measured by encounter rates.

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

Understanding infection and encounter rates

The encounter rate is the percentage of computers running Microsoft real-time security products that report a malware encounter. For example, the encounter rate for the worm family Win32/Gamarue in Poland in 2Q13 was 1.0 percent. This statistic means that, of the computers in Poland that were running Microsoft real-time security software, 1 percent reported encountering the Gamarue family and 99 percent did not. (Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[8])

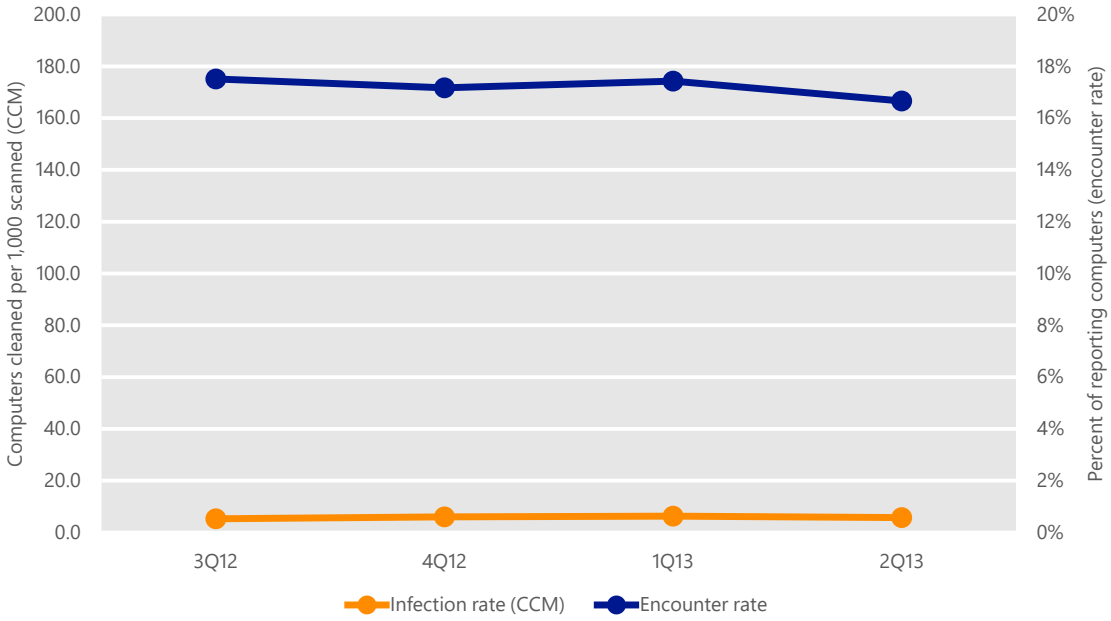
[8] For privacy statements and other information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 126.

Encounter rates do not equate to infections; some computers do get infected and cleaned, but more often, malware encounters represent blocked infection attempts.

To calculate infection rates by CCM, Microsoft measures the number of computers cleaned for every 1,000 executions of the MSRT. For example, if the tool has 50,000 executions in a particular location in 2Q13 and removes infections from 200 computers, the CCM infection rate for that location in 2Q13 is 4.0 (200 ÷ 50,000 × 1,000).

Figure 13 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 13. Worldwide encounter and infection rates, 3Q12–2Q13, by quarter



As Figure 13 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) on which it ran each quarter. In other words, for every computer the MSRT disinfected, about 28 computers encountered malware. As explained earlier, the magnitude of the difference between the two measurements is affected by a

number of factors, such as the fact that the MSRT only removes a specific subset of the malware families that Microsoft real-time security products detect. It's also important to remember that just because a computer has encountered malware does not mean the computer has faced any danger from it. The average computer running real-time security software is far more likely to encounter malware that gets blocked before it can do any harm than it is to be infected. Running a real-time antimalware product from a reputable vendor and ensuring that its detection signatures are updated regularly remains one of the most important steps an individual or organization can take to help guard against malware infection.[9]

Encounter rates around the world

The broader perspective achieved with both CCM and encounter rate metrics is again seen in Figure 14 and Figure 15. Figure 14 show the infection and encounter rate trend in Pakistan, which reported some of the highest rates of both infections and malware encounters in the world in 1H13; Figure 15 shows the infection and encounter rate trends in Denmark, which reported some of the lowest. Both metrics offer useful perspectives on the threat landscape, in different ways. In this report, charts that use encounter rate data are indicated by a light blue background to help distinguish them from similar charts that use infection rate data.

[9] For more information, see "Running unprotected: Measuring the benefits of real-time security software" on page 1 of *Microsoft Security Intelligence Report, Volume 14 (July–December 2012)*.

Figure 14. Infection and encounter rates in Pakistan, 3Q12–2Q13, by quarter

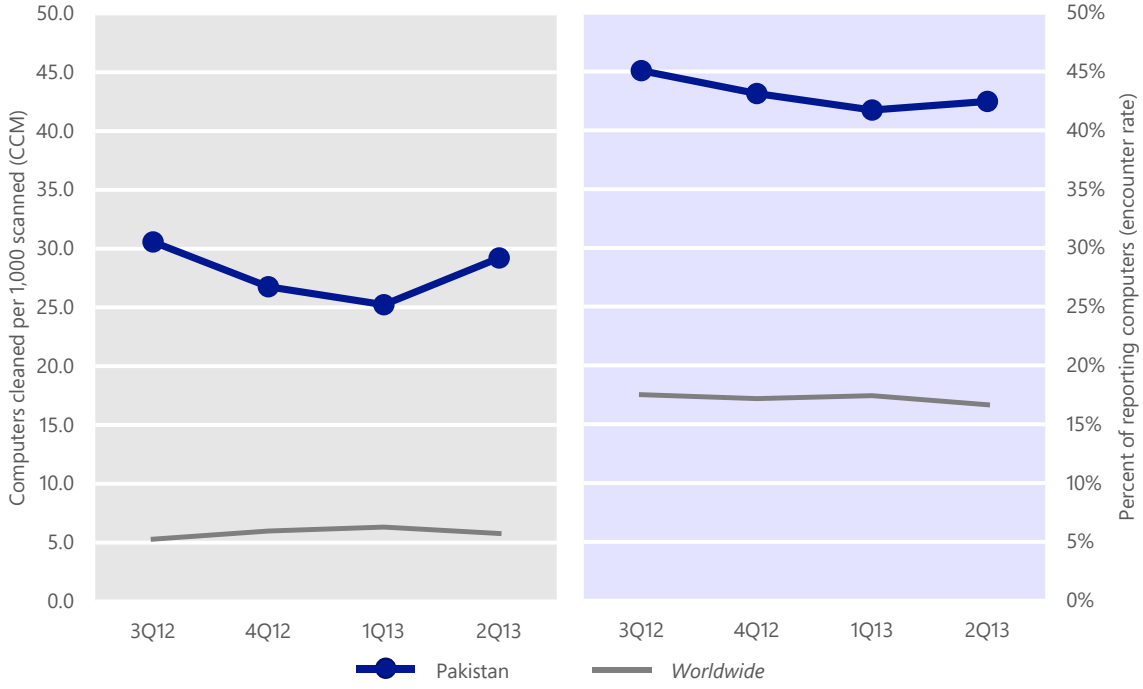
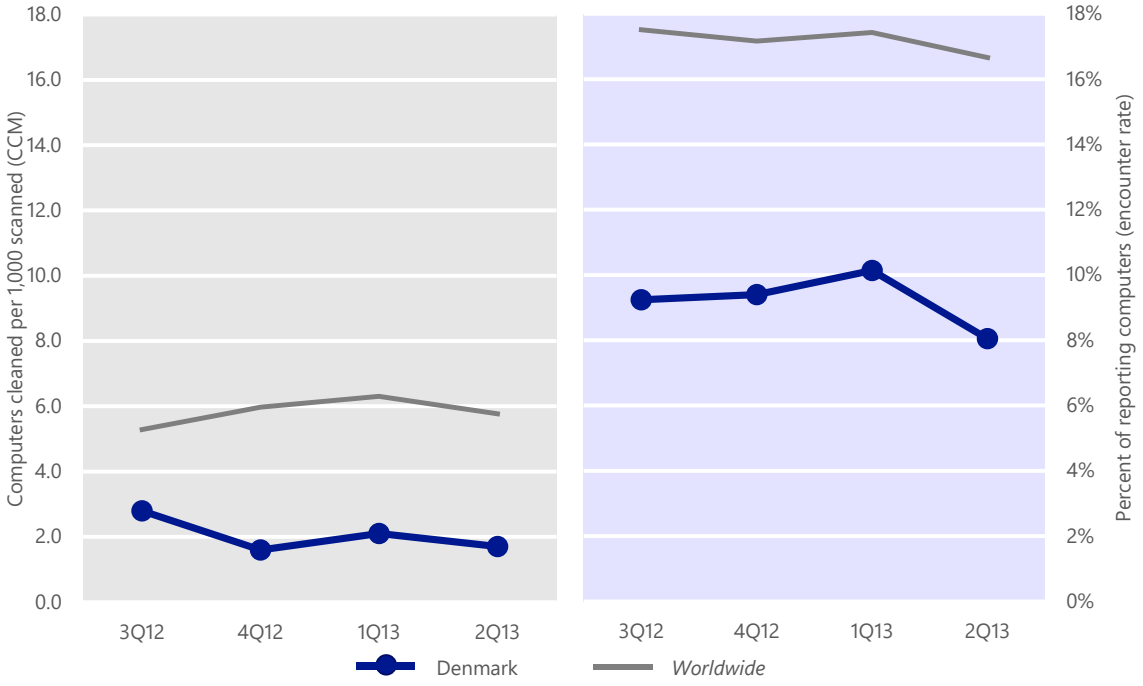


Figure 15. Infection and encounter rates in Denmark, 3Q12–2Q13, by quarter



- In Figure 14 and Figure 15, as in the remainder of the charts in this section, the infection rate scale on the left is magnified by a factor of 10 compared to

the encounter rate scale on the right, to make the infection rate trends easier to see. For example, in Figure 15 the infection rate axis on the left tops out at a CCM of 18.0, which is equal to 1.8 percent, or one-tenth of the encounter rate axis on the right.

- The MSRT data, which is used to produce the CCM charts on the right, provides important information about how computers are actually being infected in both locations, but only for the malware families that are addressed by the tool. Families that are prevalent in a location but which have not been selected for the MSRT would not be represented in the infection rate for that location. (For example, only one of the 10 most commonly encountered malware families in Denmark in 2Q13 is addressed by the MSRT, as opposed to six of the top 10 in Pakistan.) The additional encounter rate data provides additional perspective when considering how significant infection rates may actually be in the broader context.
- Infection rates and encounter rates don't always rise and fall together. In Denmark, the infection rate decreased by 75 percent between 3Q12 and 4Q12, while the encounter rate actually increased slightly. And in both locations, the infection rate was higher in 2Q13 than in 4Q12 but the encounter rate was lower.
- Denmark also had a much higher rate of real-time security software usage than Pakistan in 1H13, which probably contributed substantially to the difference in infection rates. Only 59.9 percent of computers in Pakistan were found to be running real-time security software in 1H13 on average, compared to 82.1 percent in Denmark. (See "Security software use" on page 54 for more information about real-time security software usage trends.)

To provide another example of how the encounter rate provides for a more comprehensive look at the malware landscape, Figure 16 and Figure 17 show trends for the top five threat families in France in 1H13, as measured by CCM and by the encounter rate:

Figure 16. The top five malware families infecting computers in France, 3Q12–2Q13, as measured by the MSRT

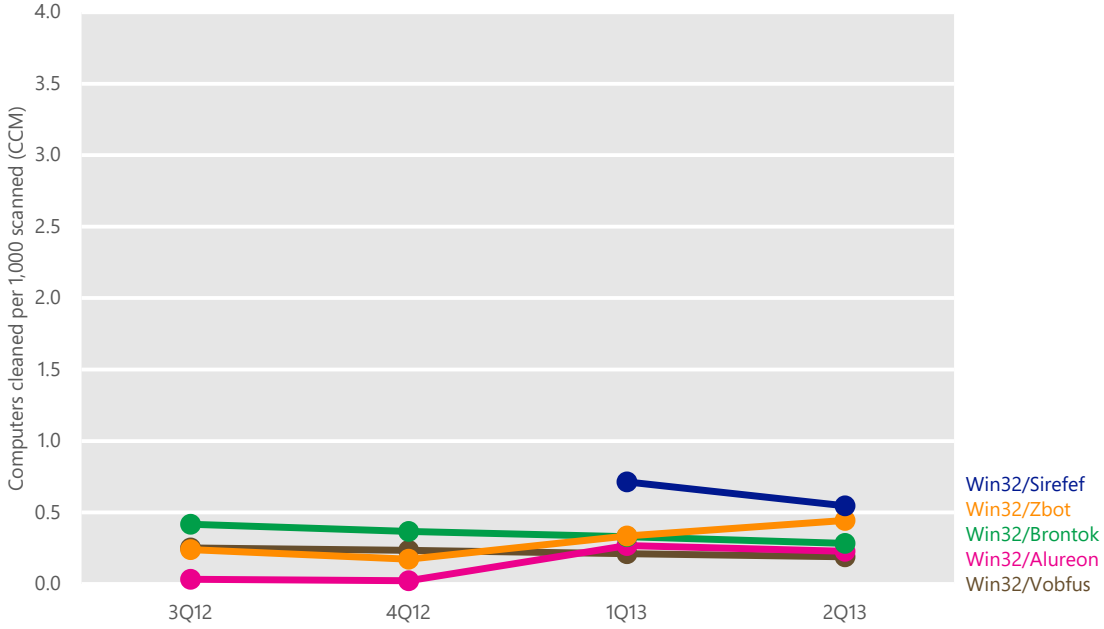
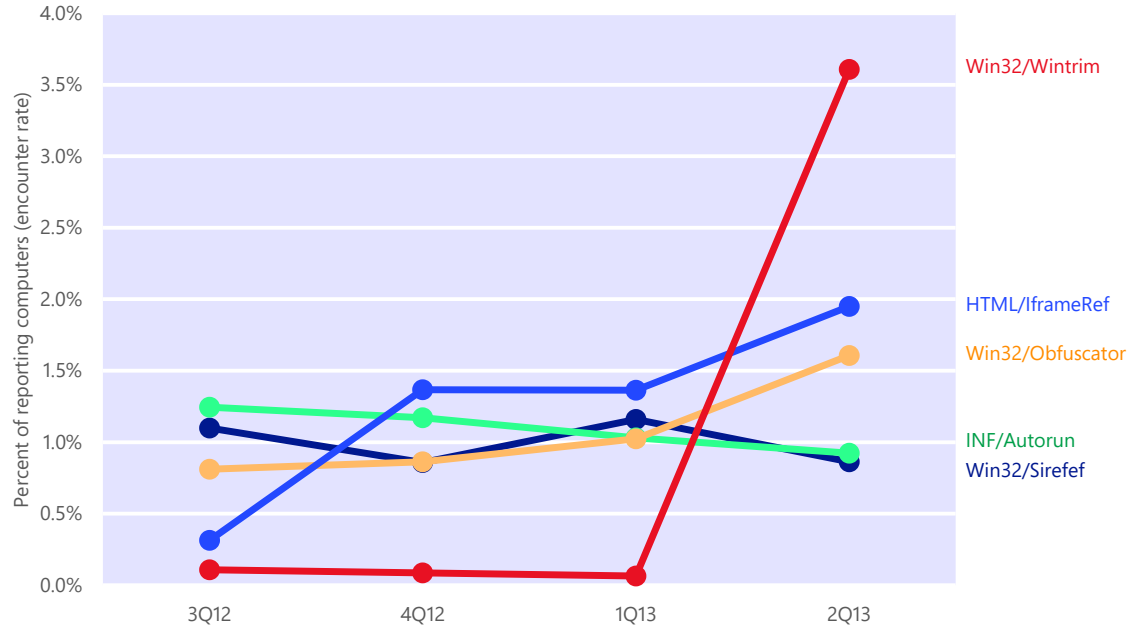


Figure 17. The top five families encountered on computers in France, 3Q12–2Q13



The lists of the top families produced by the infection rate and encounter rate metrics can be quite different. In the case of France, only one of the top five most commonly encountered threat families (Win32/Sirefef) is addressed by the MSRT. Because worldwide and platform prevalence are factors for family

inclusion in MSRT, only Sirefef had the prevalence to indicate that cleaning that family would remove it from a significant population of computers globally. Therefore, the other families do not appear as top infections for France.

Encounter rate data shows a different perspective on the current threat landscape. Sirefef was the family most commonly removed from computers in France by the MSRT in both 1Q13 and 2Q13 after detection signatures for the family were added to the tool in February 2013. By encounter rate, however, Sirefef was encountered less frequently than a number of others not addressed by the MSRT, including the generic detections HTML/IframeRef and Win32/Obfuscator, and the trojan family Win32/Wintrim. (Of course, computers that run real-time security software—as 79.3 percent of computers in France did in 1H13 on average, a higher percentage than the world overall—face substantially diminished risk from these and other malware families, regardless of whether they are addressed by the MSRT.)

The broader perspective given by the combination of CCM and encounter rate data demonstrates the necessity of protecting networks with a real-time antimalware protection and putting adequate security mechanisms in place in organizations. IT professionals can use the encounter rate to understand the infection rate in that context to assess risk, implement security processes, and select investments to manage that level of risk appropriately.

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. In some scenarios, targeted components are add-ons that are pre-installed by the computer manufacturer before the computer is sold. A user may not even use the vulnerable add-on or be aware that it is installed. In addition, some software has no facility for updating itself, so even if the software vendor publishes an update that fixes the vulnerability, the user may not know that the update is available or how to obtain it and therefore remains vulnerable to attack.[10]

Software vulnerabilities are enumerated and documented in the Common Vulnerabilities and Exposures (CVE) list (cve.mitre.org), a standardized repository of vulnerability information. Here and throughout this report, exploits are labeled with the CVE identifier that pertains to the affected vulnerability, if applicable. In addition, exploits that affect vulnerabilities in Microsoft software are labeled with the Microsoft Security Bulletin number that pertains to the vulnerability, if applicable.[11]

Microsoft security products can detect and block attempts to exploit known vulnerabilities whether the computer is affected by the vulnerabilities or not. (For example, the CVE-2010-2568 CplLnk vulnerability has never affected Windows 8, but if a Windows 8 user receives a malicious file that attempts to exploit that vulnerability, Windows Defender should detect and block it anyway.) Encounter data provides important information about which products and vulnerabilities are being targeted by attackers, and by what means. However, the statistics presented in this report should not be interpreted as evidence of successful exploit attempts, or of the relative vulnerability of computers to different exploits.

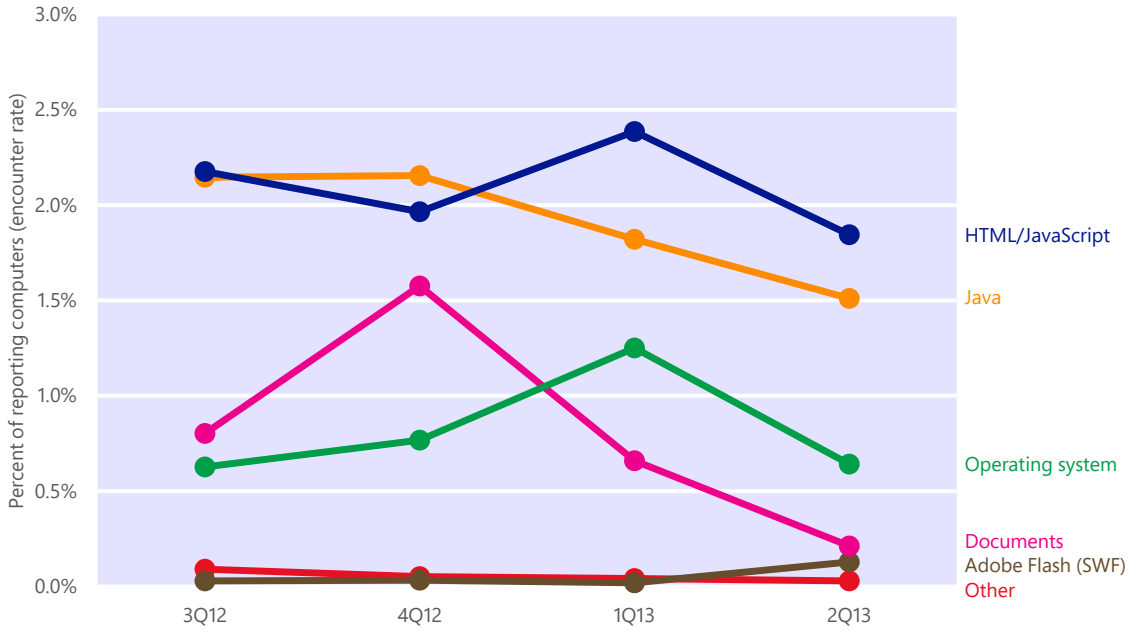
Figure 18 shows the prevalence of different types of exploits detected by Microsoft antimalware products in each quarter from 3Q12 to 2Q13, by number

[10] See the Microsoft Security Update Guide at www.microsoft.com/security/msrc/whatwedo/securityguide.aspx for guidance to help protect your IT infrastructure while creating a safer, more secure computing and Internet environment.

[11] See technet.microsoft.com/security/bulletin to search and read Microsoft Security Bulletins.

of unique computers with encounters. (See "Appendix B: Data sources" on page 125 for more information about the products and services that provided data for this report.)

Figure 18. Unique computers reporting different types of exploit attempts, 3Q12–2Q13



- Computers that report more than one type of exploit are counted for each type detected.
- 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 18.
- 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.)
- The encounter rate for Adobe Flash exploits increased slightly in the second quarter, from 0.01 percent of computers worldwide in 1Q13 to 0.12 percent in 2Q13. An increase in the exploitation of a number of older Flash

vulnerabilities was mostly responsible for the increase; Adobe has published security updates to address these vulnerabilities, but the updates had not been applied to the affected computers, which remained vulnerable.

Exploit families

Figure 19 lists the exploit-related families that were detected most often during the first half of 2013.

Figure 19. 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.

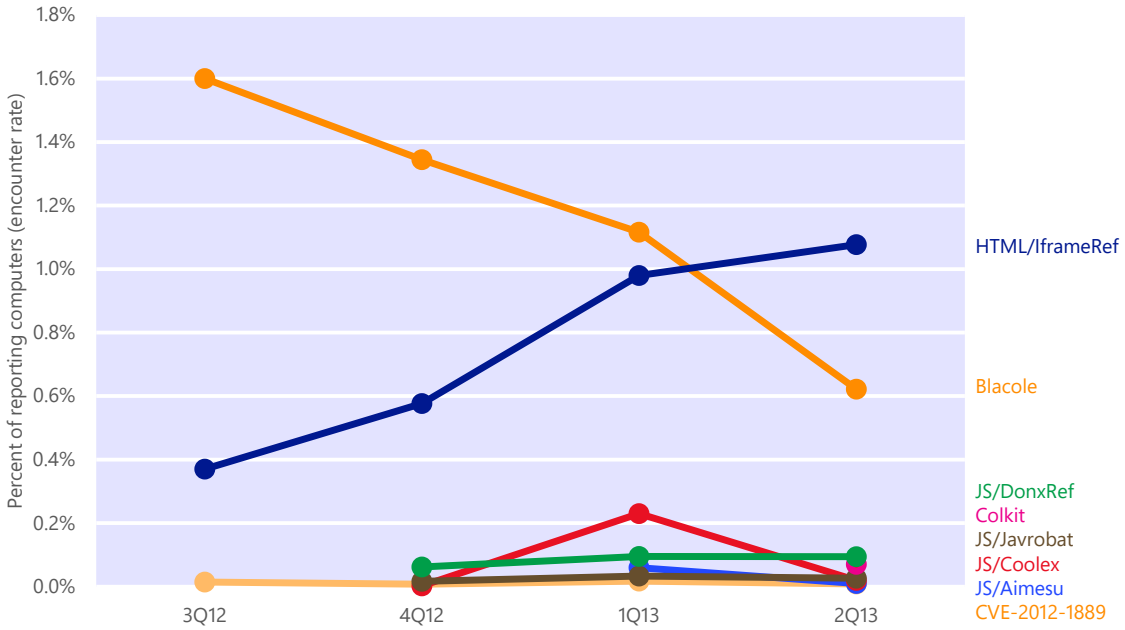
  Two highly prevalent IframeRef variants were reclassified as JS/Seedabutor variants in 1Q13, but the encounter rate for IframeRef remained high that quarter after detection signatures for the variant Trojan:JS/IframeRef.K were added to Microsoft antimalware products in response to the so-called "Darkleech"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

- Blacole, the second most commonly encountered exploit in 1H13, is the Microsoft detection name for components of the so-called "Blackhole" exploit kit, which delivers malicious software through infected webpages. 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 loads 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. (See page 106 for more information about drive-by download attacks.) Blacole was the most commonly encountered exploit family for six consecutive quarters before the encounter rate decreased by nearly half in 2Q12.
- The encounter rate for exploits that target CVE-2012-1723, a type-confusion vulnerability in the Java Runtime Environment (JRE), fell in 1H13 after they were replaced in the Blacole kit by exploits targeting a newer Java vulnerability, CVE-2013-0422. See "Java exploits" on page 38 for more information about these exploits.
- The encounter rate for Win32/Pdfjsc, a detection for specially crafted PDF files that exploit vulnerabilities in Adobe Reader and Adobe Acrobat, decreased significantly in 1H13 after Pdfjsc exploits were removed from the Blacole kit. See page 42 for more information about Pdfjsc.

HTML and JavaScript exploits

Figure 20 shows the prevalence of different types of HTML and JavaScript exploits during each of the four most recent quarters.

Figure 20. Trends for the top HTML and JavaScript exploits detected and blocked by Microsoft antimalware products in 1H13



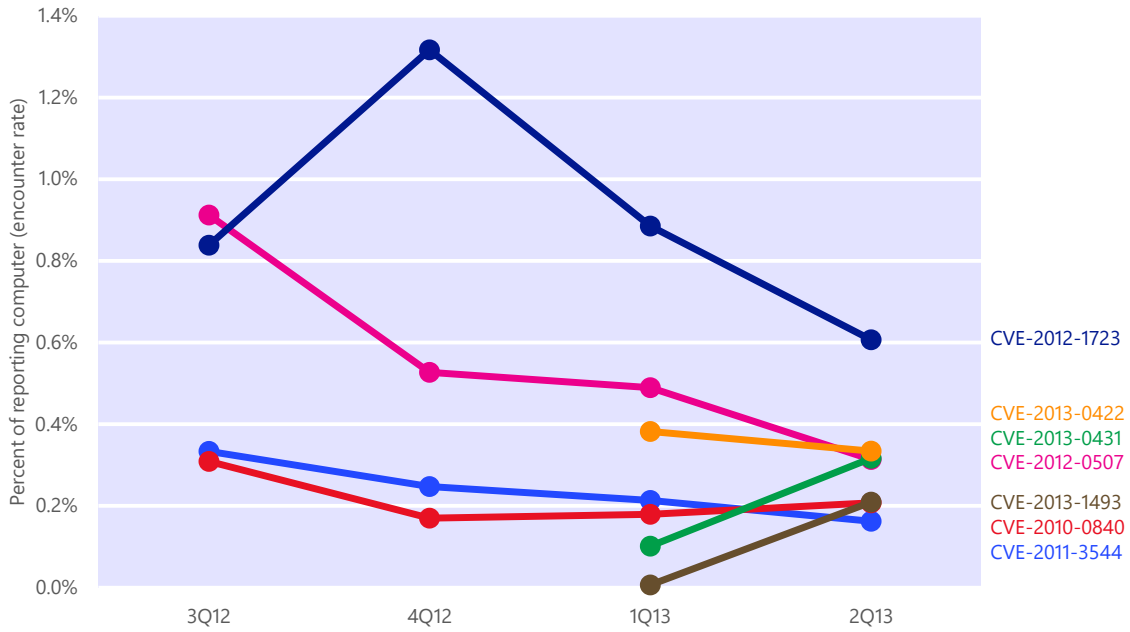
- JS/Coolex is the Microsoft detection name for the so-called Cool exploit kit, which first appeared in October 2012 and is often used in ransomware schemes in which an attacker locks a victim's computer or encrypts the user's data and demands money to make it available again. In its most recent version, Coolex includes exploits that target 19 different vulnerabilities in the Java JRE, Adobe Reader and Flash Player, Windows kernel-mode drivers, and other products and components. Coolex can be hosted on malicious websites or used to inject malicious code into legitimate websites. As with Blacole, computer users who visit a Coolex-infected website and don't have the appropriate security updates installed are at risk of infection through drive-by download attacks. Coolex encounters increased slightly in 1Q13 but then decreased in 2Q13, a sequence that appears to be correlated with the removal from the kit of exploits that target Java vulnerability CVE-2012-1723. (See the following "Java exploits" section for more information about this vulnerability.)

  For more information about the Coolex kit, see the entry "CVE-2012-1876: Recent update to the Cool Exploit Kit landing page" (May 7, 2013) in the Microsoft Malware Protection Center (MMPC) blog at blogs.technet.com/mmpc.

Java exploits

Figure 21 shows the prevalence of different Java exploits by quarter.

Figure 21. Trends for the top Java exploits detected and blocked by Microsoft antimalware products in 1H13



Totals do not include exploits that were detected as part of exploit kits.

- Several new Java exploits (notably CVE-2013-0431 and CVE-2013-1493) were first detected in 1Q13 and quickly became more prominent during the next quarter as they began to be included in various exploit kits. A number of older exploits from 2010 and 2011 also remained prevalent in 2Q13.
- CVE-2012-1723 accounted for most of the Java exploits detected and blocked in 4Q12. CVE-2012-1723 is a type-confusion vulnerability in the Java Runtime Environment (JRE), which is exploited by tricking the JRE into treating one type of variable like another type. Oracle confirmed the existence of the vulnerability in June 2012 and published a security update to address it the same month. The vulnerability was observed being exploited in the wild beginning in early July 2012, and exploits for the vulnerability were added to the Blacole exploit kit shortly thereafter. CVE-2012-1723 exploits were removed from the Blacole kit in 1H13, contributing to the decline in its encounter rate.

For more information about this exploit, see the entry "The rise of a new Java vulnerability - CVE-2012-1723" (August 1, 2012) in the MMPC blog at blogs.technet.com/mmpc.

- CVE-2013-0422 first appeared in January 2013 as a zero-day vulnerability, and became the second most targeted Java exploit in 2Q13 as detections of exploits that target CVE-2012-0507 declined. CVE-2013-0422 is a package access check vulnerability that allows an untrusted Java applet to access code in a trusted class, which then loads the attacker's own class with elevated privileges. Oracle published a security update to address the vulnerability on January 13, 2013.

  For more information about CVE-2013-0422, see the entry "A technical analysis of a new Java vulnerability (CVE-2013-0422)" (January 20, 2013) in the MMPC blog at blogs.technet.com/mmpc.

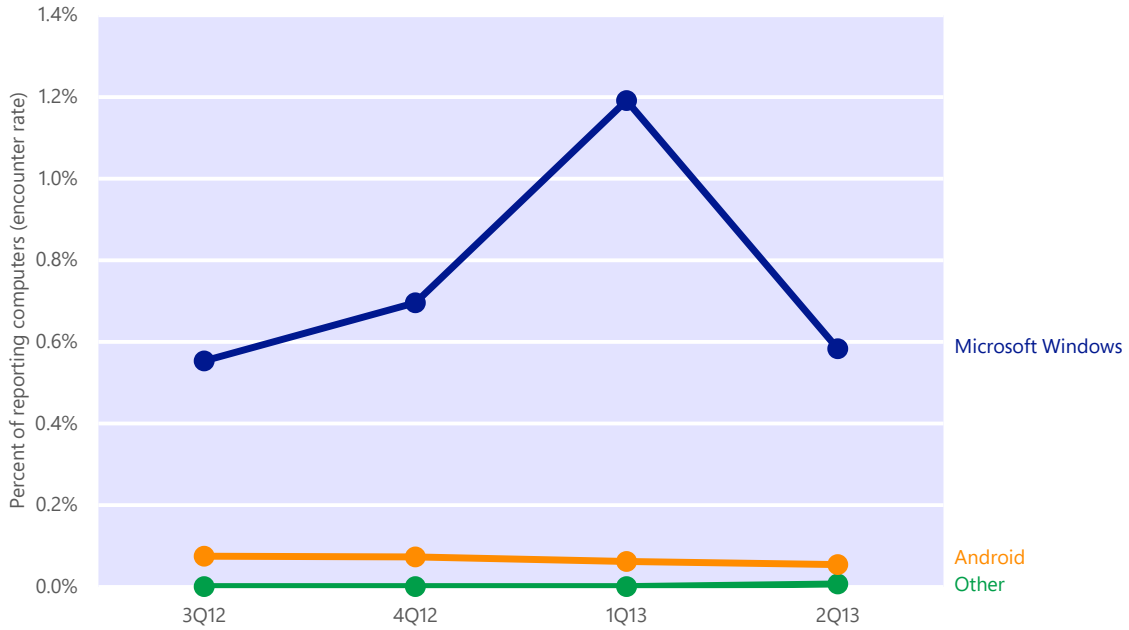
- The encounter rate for CVE-2012-0507 exploits continued its multi-quarter decline since 3Q12, when exploits that target the vulnerability were removed from the Blacole kit. (These exploits have been restored to the kit in its most recent versions.) CVE-2012-0507 allows an unsigned Java applet to gain elevated permissions and potentially have unrestricted access to a host system outside its sandbox environment. The vulnerability is a logic error that allows attackers to run code with the privileges of the current user, which means that an attacker can use it to perform reliable exploitation on other platforms that support the JRE, including Apple Mac OS X, Linux, VMWare, and others. Oracle released a security update in February 2012 to address the issue.

  For more information about CVE-2012-0507, see the entry "An interesting case of JRE sandbox breach (CVE-2012-0507)" (March 20, 2012) in the MMPC blog.

Operating system exploits

Although most operating system exploits detected by Microsoft security products are designed to affect the platforms on which the security products run, computer users sometimes download malicious or infected files that affect other operating systems. Figure 22 shows the prevalence of different exploits against operating system vulnerabilities that were detected and removed by Microsoft antimalware products during each of the past six quarters.

Figure 22. Exploits against operating system vulnerabilities detected and blocked by Microsoft antimalware products, 3Q12–2Q13

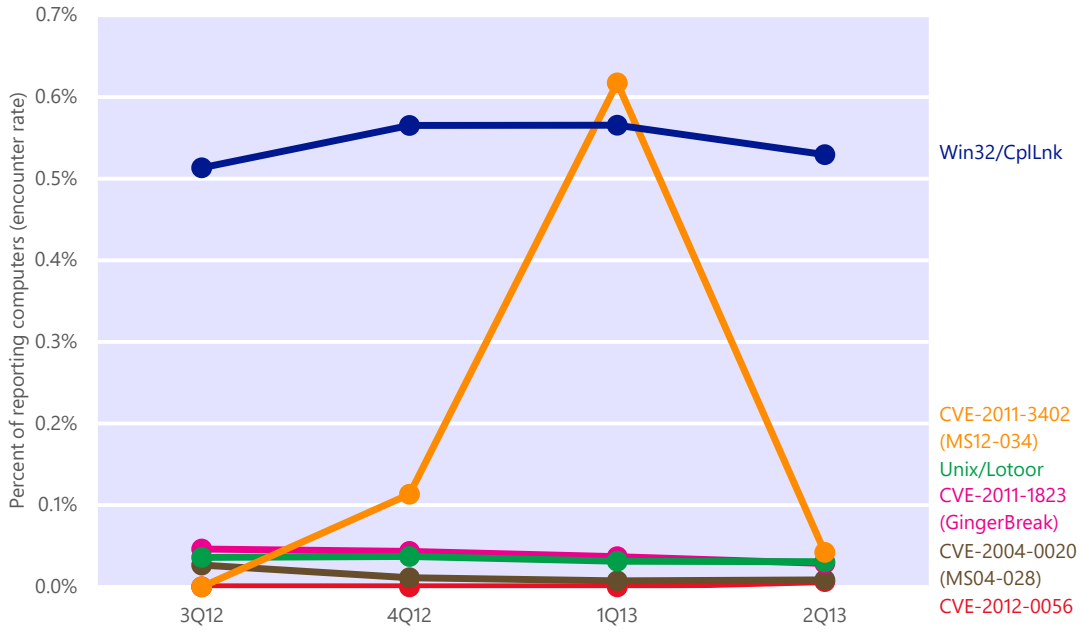


- Detections of exploits that affect Windows-based computers increased significantly in 1Q13, and then declined significantly in 2Q13. The increase in 1Q13 was mostly caused by the discovery of a new exploit family that targets CVE-2011-3402, and by a slight increase in detections of exploits that target CVE-2010-2568. See Figure 23 for more information about these exploits. Microsoft issued security updates for these vulnerabilities in December 2011 and August 2010, respectively.

  Detections of exploits that affect the Android mobile operating system published by Google and the Open Handset Alliance accounted for a small share of operating system exploit detections in 1H13. Microsoft security products detect these threats when Android devices or storage cards are connected to computers running Windows, or when Android users knowingly or unknowingly download infected or malicious programs to their computers before transferring the software to their devices. See page 42 for more information about these exploits.

For another perspective on these exploits and others, Figure 23 shows trends for the individual exploits most commonly detected and blocked or removed during each of the past six quarters.

Figure 23. Individual operating system exploits detected and blocked by Microsoft antimalware products, 3Q12–2Q13



- Win32/CplLnk, an exploit that targets a vulnerability in Windows Shell, remained the most commonly encountered operating system exploit in 1H13. An attacker exploits the vulnerability (CVE-2010-2568) by creating a malformed shortcut file that forces a vulnerable computer to load a malicious file when the shortcut icon is displayed in Windows Explorer. Microsoft released Security Bulletin MS10-046 in August 2010 to address this issue.

  The vulnerability was first discovered being used by the malware family Win32/Stuxnet in mid-2010. It has since been exploited by a number of other malware families, many of which predated the disclosure of the vulnerability and were subsequently adapted to attempt to exploit it.

- CVE-2011-3402 is a vulnerability in the way the Windows kernel processes TrueType font files. An attacker exploits the vulnerability by deceiving a user into opening a specially crafted document or visit a malicious webpage that embeds TrueType font files, which enables the attacker to run arbitrary code in kernel mode. Microsoft released Security Bulletin MS11-087 in December 2011 to address this issue.

- Detections of exploits that target CVE-2011-3402 briefly accounted for the largest share of operating system exploit encounters in 1Q13 following the discovery of Win64/Anogre, which exploits the vulnerability using a new

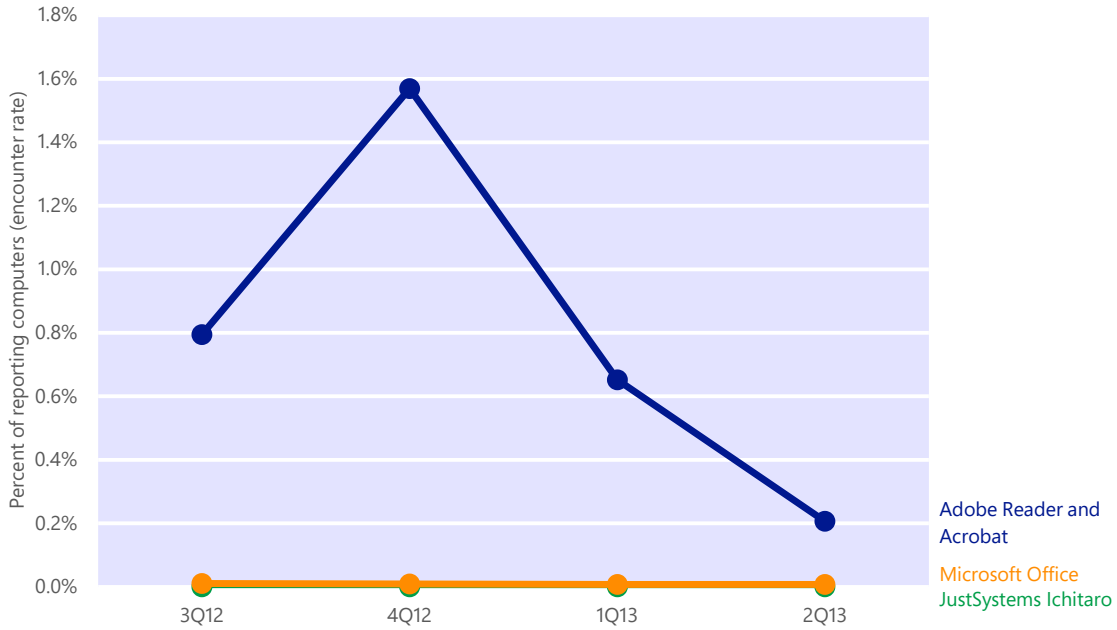
attack method that involves putting the malicious TrueType files into a container file that cannot be extracted. The large decline in encounters between the first and second quarters suggests that attackers may be abandoning the exploit as security software vendors update their signature databases to detect the new attack method.

- Most detections that affected Android involve a pair of exploits that enable an attacker or other user to obtain root privileges on vulnerable Android devices. Device owners sometimes use such exploits intentionally to gain access to additional functionality (a practice often called *rooting* or *jailbreaking*), but these exploits can also be used by attackers to infect devices with malware that bypasses many typical security systems.
    - CVE-2011-1823 is sometimes called the GingerBreak vulnerability because of its use by a popular rooting application of that name. It is also used by AndroidOS/GingerMaster, a malicious program that can allow a remote attacker to gain access to the mobile device. GingerMaster may be bundled with clean applications, and includes an exploit for the CVE-2011-1823 vulnerability disguised as an image file. Google published a source code update in May 2011 that addressed the vulnerability.
    - Unix/Lotoor is an exploit family that exploits vulnerabilities in the Android operating system to gain root privileges on a mobile device. Google published a source code update in March 2011 that addressed the vulnerability.

Document exploits

Document exploits are exploits that target vulnerabilities in the way a document editing or viewing application processes, or parses, a particular file format. Figure 24 shows the prevalence of different types of document exploits during each of the four most recent quarters.

Figure 24. Types of document exploits detected and blocked by Microsoft antimalware products, 3Q12–2Q13

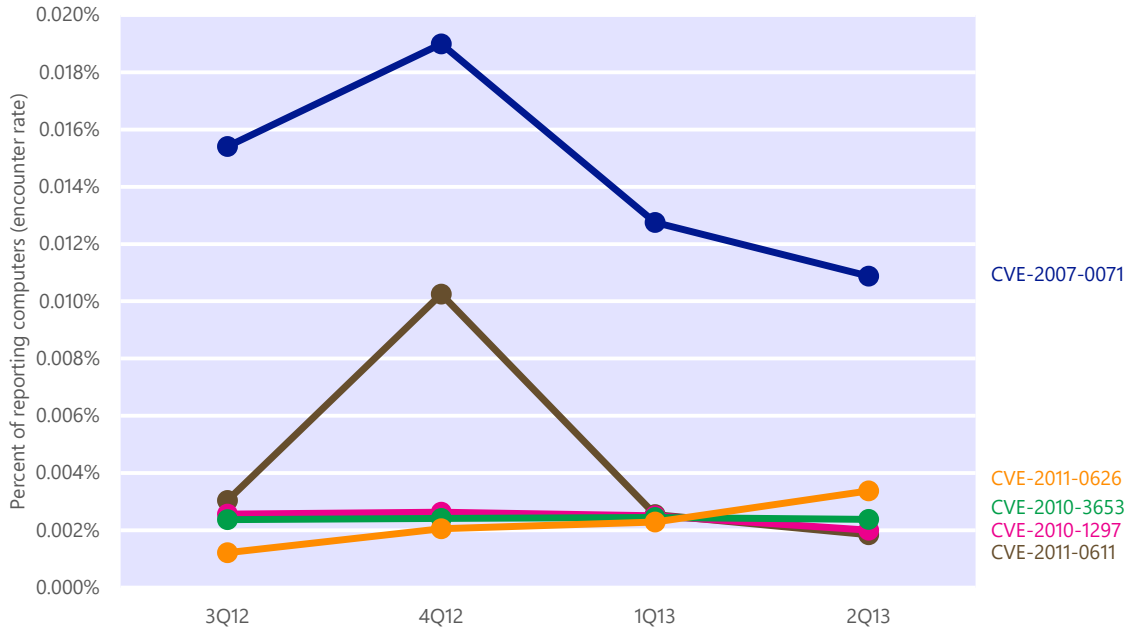


- Detections of exploits that affect Adobe Reader and Adobe Acrobat declined considerably from 4Q12 to 1Q13 and again from 1Q13 to 2Q13, possibly due to increased installations of security updates. Some exploit kits are known to scan a target computer for vulnerabilities and only use exploits that the computer is vulnerable to, so installing security updates can affect encounters as well as infections.
- Exploits that affect Microsoft Office and Ichitaro, a Japanese-language word processing application published by JustSystems, accounted for less than 0.1 percent of exploits detected during the period.

Adobe Flash Player exploits

Figure 25 shows the prevalence of different Adobe Flash Player exploits by quarter.

Figure 25. Adobe Flash Player exploits detected and blocked by Microsoft antimalware products, 3Q12–2Q13



- Attempts to exploit CVE-2007-0071 decreased significantly in 1H13, but it remained the most commonly encountered exploit in both quarters. CVE-2007-0071 is an invalid pointer vulnerability in some releases of Adobe Flash Player versions 8 and 9. Adobe released Security Bulletin APSB08-11 on April 8, 2008 to address the issue. Increased adoption of the security bulletin and of newer versions of Flash Player that are not vulnerable to the exploit probably contributed to its decline by making the exploit less effective.
- Exploit attempts that target CVE-2011-0626, the fifth most commonly encountered Adobe Flash Player exploit in 1Q13, increased to second place in 2Q13. CVE-2011-0626 is a bounds-checking vulnerability in some versions of Adobe Flash Player versions 10 and earlier. Adobe released Security Bulletin APSB11-12 on May 12, 2011 to address the issue.
- CVE-2011-0611, which accounted for the second largest number of Adobe Flash Player exploitation attempts detected in 2H12, declined to about a fifth of its peak level in 1Q13 and 2Q13. CVE-2011-0611 was discovered in April 2011 when it was observed being exploited in the wild; Adobe released Security Bulletin APSB11-07 on April 15 and Security Bulletin APSB11-08 on April 21 to address the issue.

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. (See "Appendix B: Data sources" on page 125 for more information about the telemetry used in this report.)

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. See "Encounter rate: Introducing a new metric for analyzing malware prevalence" on page 25 for more information about the CCM and encounter rate metrics.

In addition, statistics on potentially unwanted software have been moved to their own section in this volume of the report. See "Potentially unwanted software" on page 79 for more information.

Malware prevalence worldwide

The telemetry data generated by Microsoft security products from computers whose administrators or users choose to opt in to provide data to Microsoft includes information about the location of the computer, as determined by IP geolocation. This data makes it possible to compare infection and encounter rates, patterns, and trends in different locations around the world.[12]

[12] For more information about this process, see the entry "Determining the Geolocation of Systems Infected with Malware" (November 15, 2011) in the Microsoft Security Blog (blogs.technet.com/security).

Figure 26. Encounter rate trends for the locations with the most computers reporting malware detections in 1H13

	Country/Region	3Q12	4Q12	1Q13	2Q13	Chg. 2H–1H
1	United States	13.80%	13.36%	14.10%	11.51%	-5.72% ▼
2	Brazil	28.80%	26.28%	25.57%	26.75%	-5.00% ▼
3	Russia	26.61%	27.29%	28.61%	29.70%	8.18% ▲
4	Turkey	39.33%	38.95%	41.25%	47.35%	13.20% ▲
5	India	32.61%	29.67%	29.31%	29.44%	-5.88% ▼
6	Mexico	28.16%	26.41%	24.52%	29.18%	-1.61% ▼
7	Germany	13.97%	12.51%	13.21%	11.06%	-8.37% ▼
8	France	14.18%	14.89%	14.53%	15.57%	3.52% ▲
9	China	35.81%	31.81%	28.85%	25.88%	-19.06% ▼
10	United Kingdom	14.17%	13.47%	13.53%	12.32%	-6.48% ▼

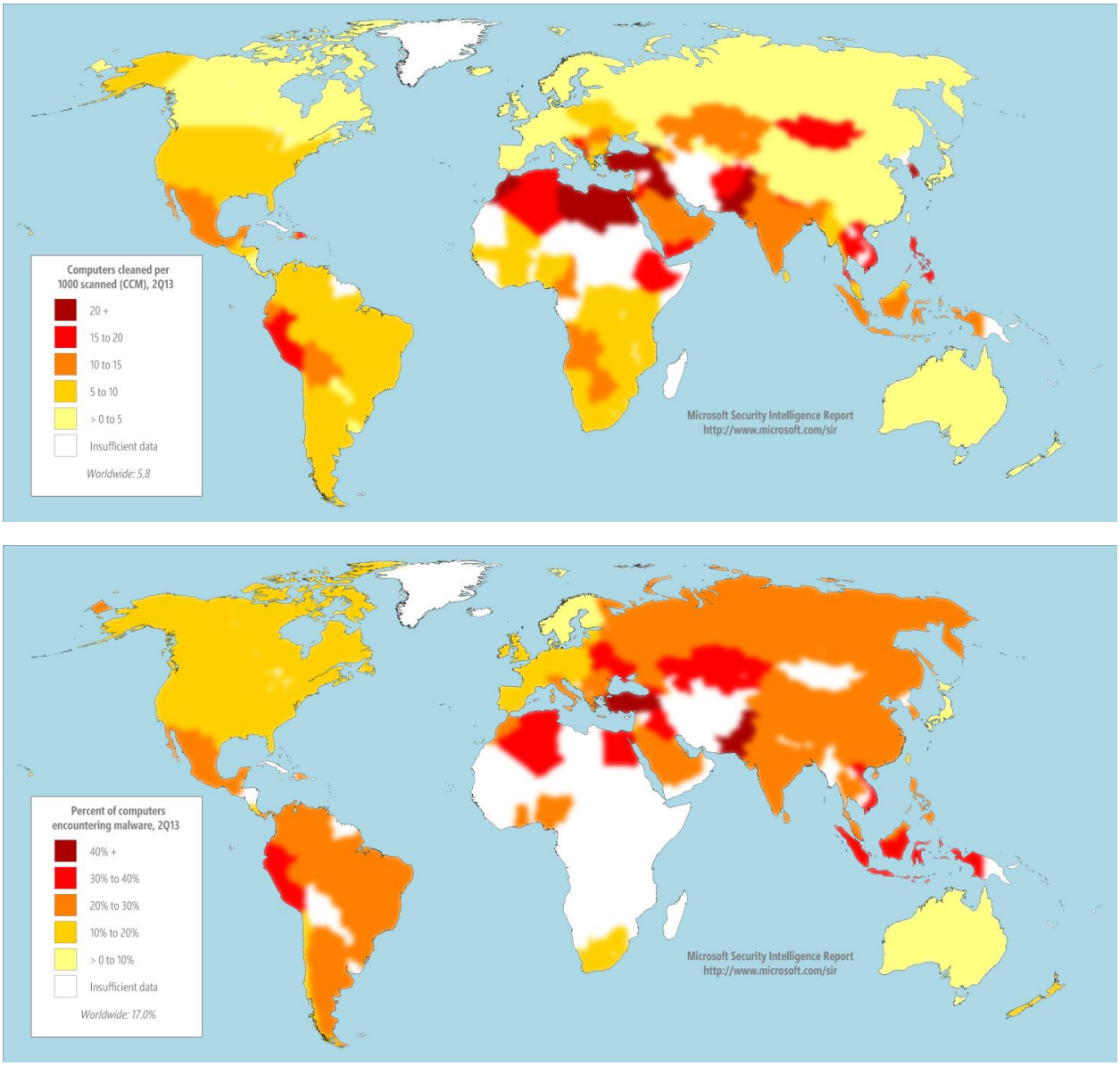
- Most of the largest countries and regions experienced encounter rate declines of between 5 and 10 percent from 2H12 to 1H13.
- The encounter rate in the United States decreased from 14.10 percent in the first quarter to 11.51 percent in the second, for an average of 12.81 in 1H13. The generic detection HTML/IframeRef (encountered by 1.6 percent of computers in the US in 2Q13) was the most commonly encountered threat in the US, followed by the trojan family Win32/Sirefef (encountered by 1.5 percent). (See "Threat families" on page 64 for more information about these and other threats.)
- The encounter rate in Brazil increased from 25.57 percent in 1Q13 to 26.75 percent in 2Q13, but was generally down overall from the second half of 2012. The generic detection INF/Autorun (encountered by 3.1 percent of computers in Brazil in 2Q13) and the trojan downloader Win32/Banload (encountered by 2.7 percent) were the most commonly encountered threats. Banload is usually associated with Win32/Banker, a data-stealing trojan that usually targets customers of Brazilian banks using Portuguese-language social engineering.
- The encounter rate in Russia increased from 28.61 percent in 1Q13 to 29.70 percent in 2Q13, and was up overall from 2H12. The generic detections Win32/Obfuscator (encountered by 6.4 percent of computers in Russia in

2Q13) and BAT/Qhost (encountered by 4.2 percent) were the most commonly encountered threats.

- Turkey had the highest encounter rate of any of the top 10 locations, ranging from 41.25 percent in 1Q13 to 47.35 percent in 2Q13. The worm family Win32/Gamarue (encountered by 1.3 percent of computers in Turkey in 2Q13) and the generic detections Obfuscator (7.1 percent) and Autorun (6.3 percent) were among the most commonly encountered threats. (See page 66 for more information about Gamarue.) The risk created by Turkey's high encounter rate was compounded by the high percentage of computers there without active real-time security software protection—an average of 38.2 percent in 1H13, compared to 25.1 percent for the world as a whole. (See "Security software use" on page 54 for more information about real-time security software usage trends.)
- In India, the encounter rate increased slightly from 29.31 percent in 1Q13 to 29.44 percent in 2Q13, but overall the rate decreased slightly from 2H12. Autorun (encountered by 7.6 percent of computers in India in 2Q13), Gamarue (4.7 percent), and the virus family Win32/Sality (4.4 percent) were among the most commonly encountered threats.

For a different perspective on threat patterns worldwide, Figure 27 shows the infection and encounter rates in locations around the world in the second quarter of 2013.

Figure 27. Infection rates (top) and encounter rates (bottom) by country/region in 2Q13



Infection and encounter rates in individual countries/regions can vary significantly from quarter to quarter. In particular, encounter rate increases can be caused not only by increased prevalence of malware in that location, but also by increased deployment of Microsoft antimalware solutions, and by enhancements to the ability of Microsoft antimalware solutions to detect malware.

The next several figures illustrate trends for specific locations around the world with particularly high or low incidences of threat detection. Figure 28 and Figure

29 show trends for the locations with the highest rates of detection as determined by CCM and encounter rate, respectively.

Figure 28. Trends for the five locations with the highest malware infection rates in 1H13, by CCM (100,000 MSRT executions minimum)

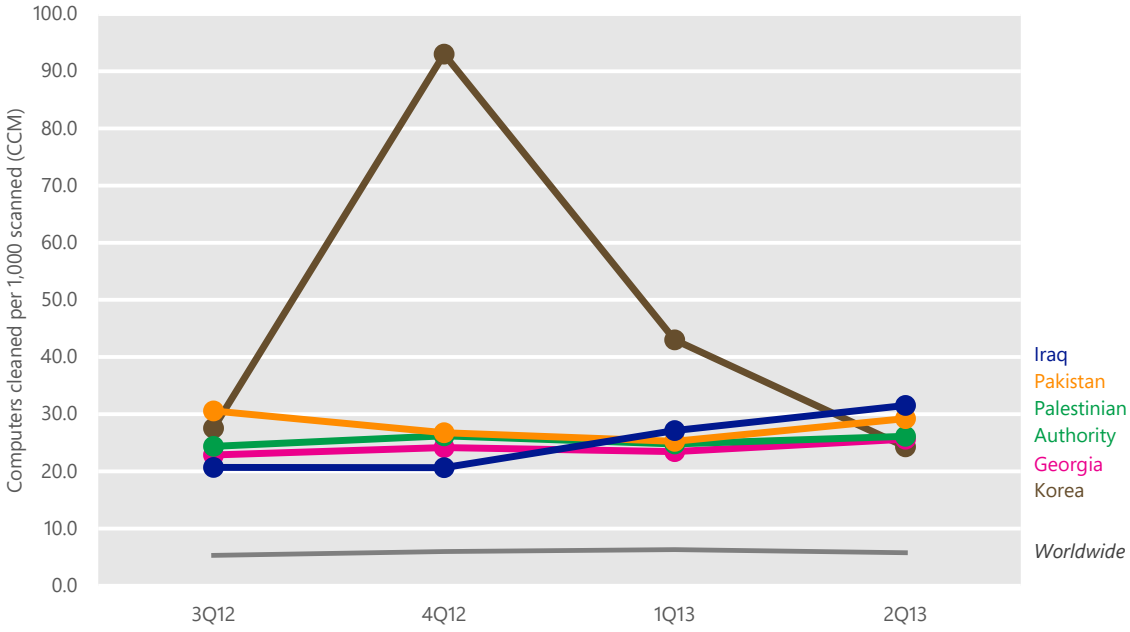
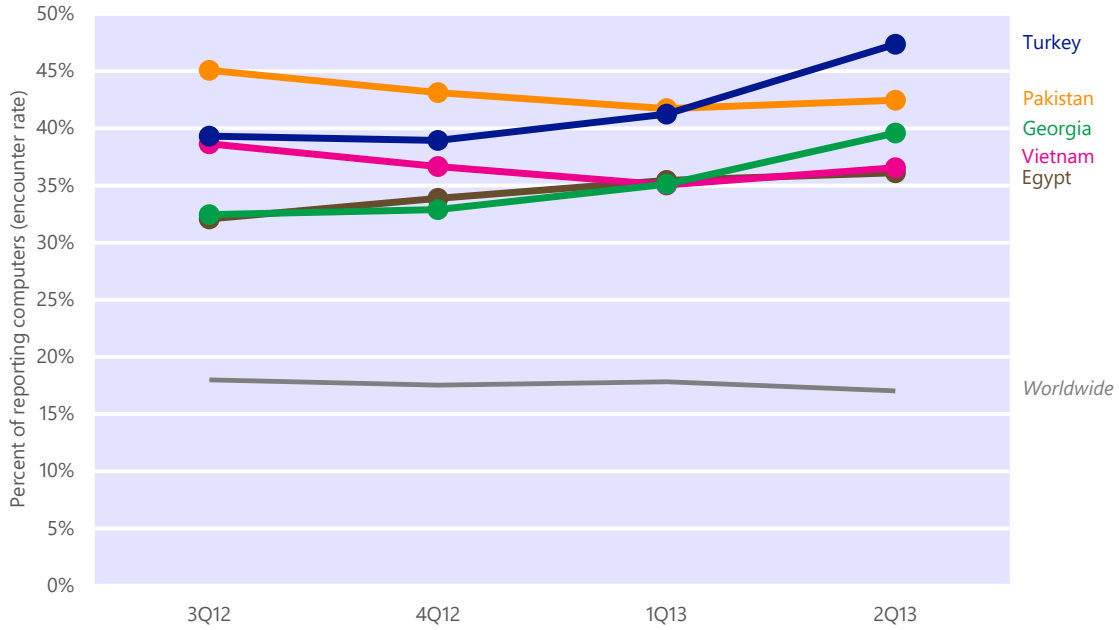


Figure 29. Trends for the five locations with the highest malware encounter rates in 1H13



- In this case, the two metrics produce significantly different lists of locations. Pakistan and Georgia are the only locations that rank among the top five by both encounter rate and infection rate.
- The locations with the highest infection rates in 1H13 as measured by CCM (which includes disinfections only) were Iraq, Pakistan, the Palestinian territories, Korea, and Georgia. Infection rates for these locations were between four and six times as high as the worldwide infection rate in 2Q13.
    - Korea had the highest infection rate in 1H13 with a CCM of 43.0 in the first quarter, significantly higher than any other location. Detection signatures for the Korean-language rogue security software program Win32/Onescan were added to the MSRT in October 2012, which led to a sharp increase in the CCM in Korea in 4Q12 as the MSRT detected and removed millions of Onescan infections that may have been present for many months or longer. The CCM in Korea remained much higher than normal in 1H13, as subsequent releases of the MSRT continued to deal with the backlog of older Onescan infections and clean computers that may have become reinfected between MSRT executions. By 2Q13, when most computers had already downloaded at least one release of the MSRT that contained Onescan detection signatures, Korea dropped to fifth place.
    - Infection rates in Iraq, Pakistan, and the Palestinian territories increased from 1Q13 to 2Q13, with the virus family Win32/Sality being the most commonly detected family by the MSRT in all three locations.
    - In Iraq the infection rate increased by more than half in 1H13, from a CCM of 20.6 in 4Q12 to 31.5 in 2Q13. A significant part of the increase was because of the worm family Win32/Wecykler, detection signatures for which were added to the MSRT in March 2013. Wecykler was the second most commonly detected family by the MSRT in Iraq in 2Q13.
    - In Pakistan, the worm family Win32/Gamarue was the second most commonly detected malware family by the MSRT in 1H13. The virus families Win32/Virut and Win32/Chir and the trojan family Win32/Ramnit round out the top five in Pakistan.
    - In the Palestinian territories, the trojan family Win32/Pramro was the second most commonly detected family by the MSRT in 1H13, followed by Ramnit and the worm family Win32/Vobfus.

- When measured by encounter rate (which includes both blocks and disinfections), Turkey, Pakistan, Georgia, Vietnam, and Egypt were the locations with the greatest percentages of computers that encountered malware in 1H13. Encounter rates for these locations were between two and three times as high as the worldwide encounter rate in the second quarter of the year.
    - In addition to Gamarue, the generic detections INF/Autorun and Win32/Obfuscator, the worm family Win32/Ramnit, and the virus family Win32/Sality played major roles in each of the locations with the highest encounter rates. Increased Gamarue encounters were the most significant factor contributing to the 2Q13 encounter rate increases seen in Turkey and Georgia, and to a lesser extent in the other locations.
    - The encounter rate in Turkey increased steadily throughout 1H13, reaching 47.4 percent in 2Q13. Turkey's encounter rate was likely influenced by its above average proportion of unprotected computers. Detections of Gamarue, Obfuscator, and Autorun were particularly high in Turkey.
    - The encounter rate in Vietnam increased from 35.1 percent in 1Q13 to 36.6 percent in 2Q13, but ended the second quarter slightly down from the end of 2012. Ramnit (encountered by 9.6 percent of computers in Vietnam in 2Q12) was the most commonly detected threat, followed by Gamarue (9.1 percent) and the exploit family Win32/CplLnk (9.1 percent).
    - The encounter rate in Egypt increased slightly during each of the past four quarters, with 41.2 percent of computers in Egypt encountering malware in 2Q13. Autorun (encountered by 10.4 percent of computers in Egypt in 2Q12), Sality (8.9 percent), and Obfuscator (6.3 percent) were the most commonly detected threats.

Figure 30. Trends for locations with low malware infection rates in 1H13, by CCM (100,000 reporting computers minimum)

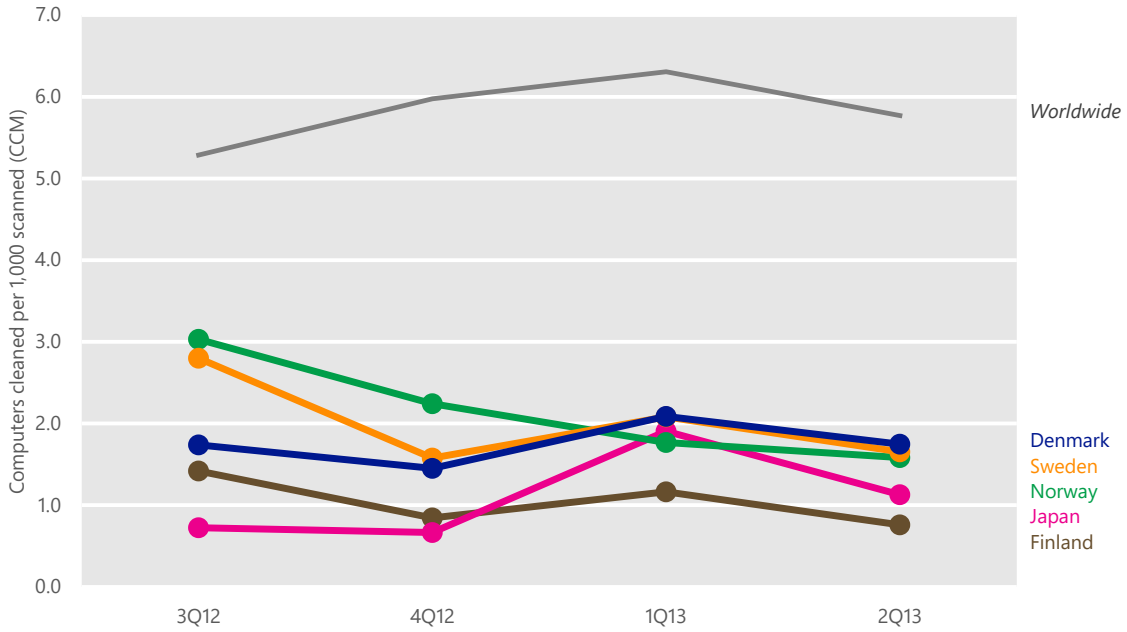
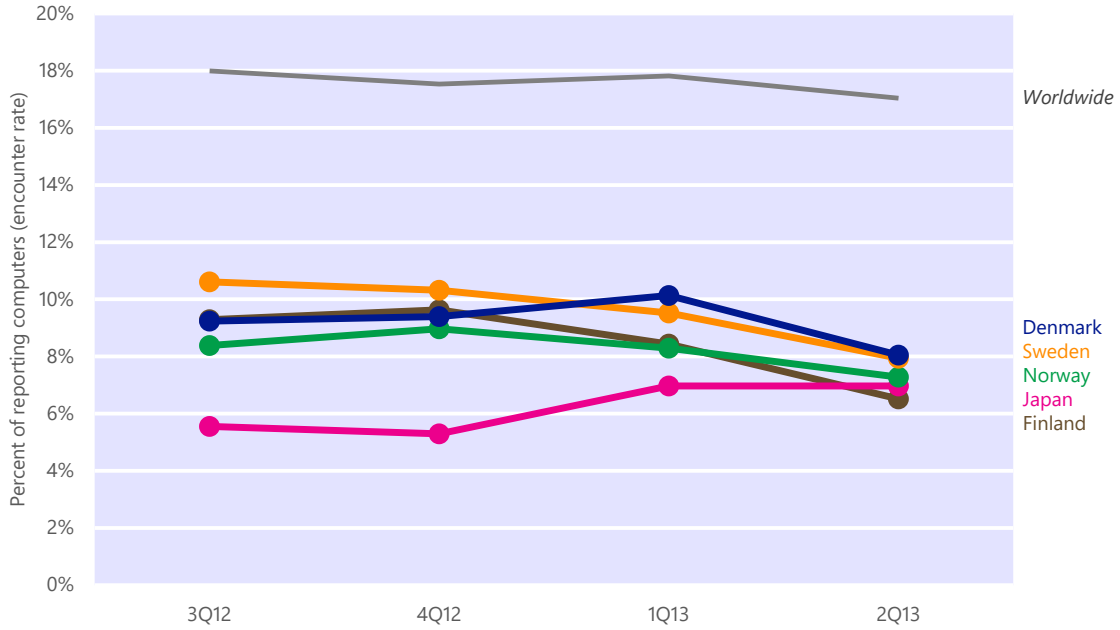


Figure 31. Trends for locations with low malware encounter rates in 1H13

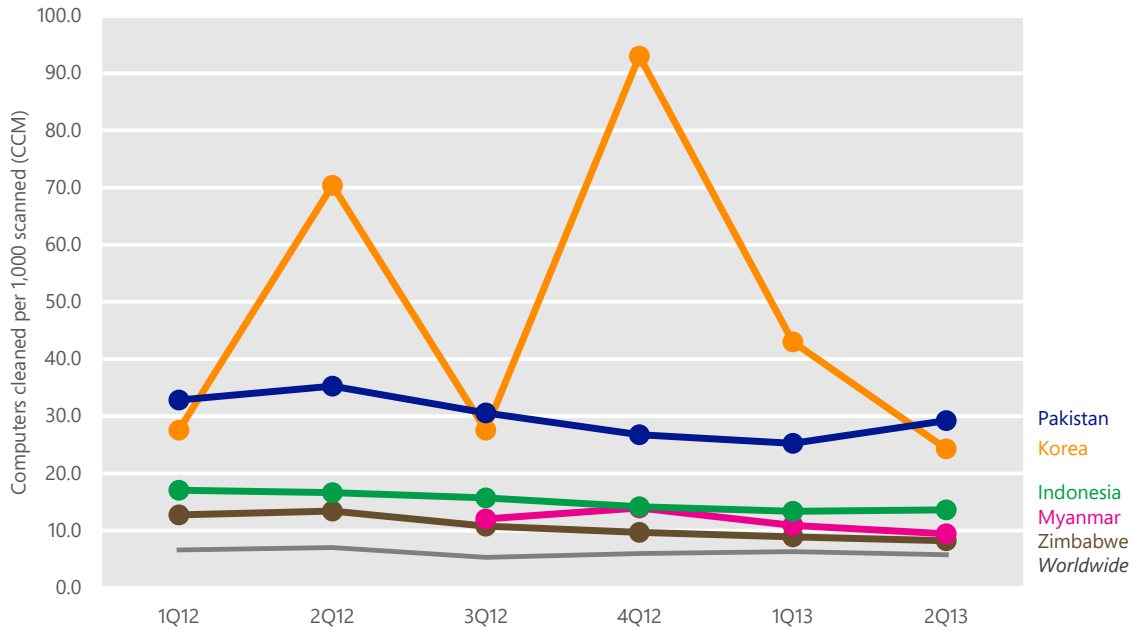


- In contrast to Figure 28 and Figure 29, the five locations with the lowest infection rates are also the locations with the lowest encounter rates, as shown in Figure 30 and Figure 31. The Nordic countries, including Norway, Sweden, Finland, and Denmark, have perennially been among the healthiest

locations in the world with regard to malware exposure, as has Japan. In 1H13, these locations had infection rates about a quarter as high as the world overall, and their encounter rates were typically between one-third and one-half of the worldwide average.[13]

- The generic detections INF/Autorun and Win32/Obfuscator were among the most commonly encountered threats in these five locations in 1H13 (as they were worldwide), although the risk that computers in these locations faced was lessened by their relatively high rate of usage of real-time security software.
- All five locations had higher rates of real-time security software usage in 1H13 than the world overall. Between 78.3 and 86.8 percent of computers in each location were found to be running security software in 1H13 on average, compared to 74.8 percent for the world overall. (See "Security software use" on page 54 for more information about real-time security software usage trends.)

Figure 32. Trends for the five locations with the most significant infection rate improvements from 1H12 to 1H13, by CCM (100,000 MSRT executions minimum per quarter)



- The infection rate in Korea dropped dramatically during the first half of the year, from a CCM of 93.0 in 4Q12 down to 24.3 in 2Q13. The large spike in

[13] For information and insights about fighting malware in Japan, see the entry "Microsoft Security Intelligence Report volume 14 on the Road: Japan" (May 6, 2013) at the MMPC blog at blogs.technet.com/mmpc.

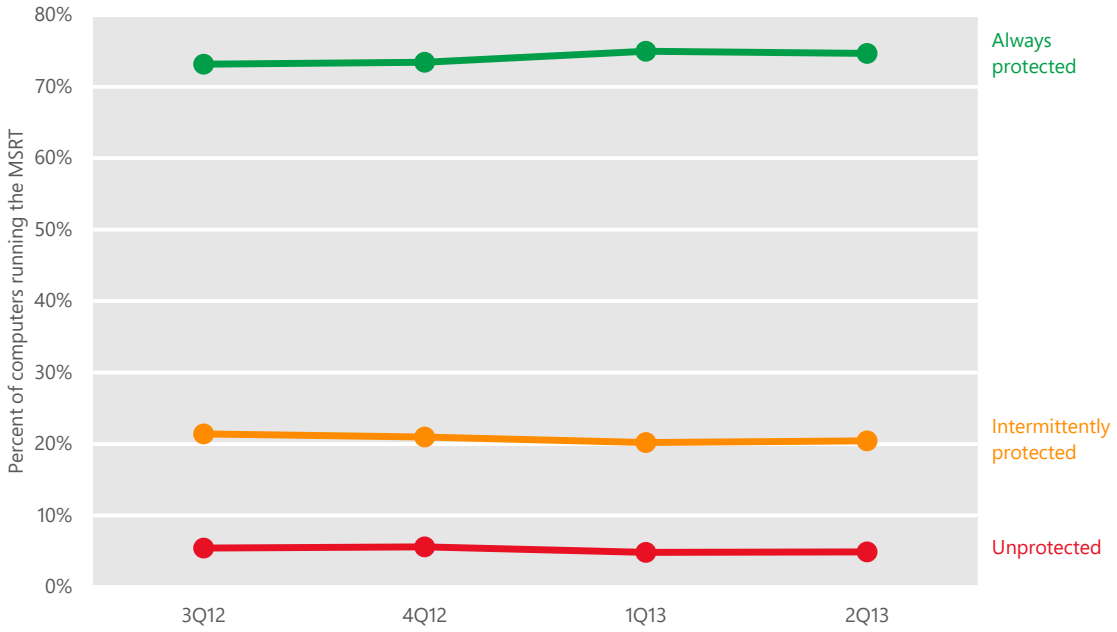
infections seen in 4Q12 was an artifact caused by the addition of detection signatures for Win32/Onescan to the MSRT in October 2012 (see page 50), after which the infection rate in Korea returned to more typical levels. Detections and removals of Win32/Pluzoks, another largely Korea-specific threat, also declined considerably in the first half of the year.

- Computers in Myanmar reported a steady decrease in infections that involve the trojan family Win32/Ramnit, which contributed to the improvement seen there. Infections that involve the virus families Win32/Sality and Win32/Virut also decreased during the first half of 2013, which decreased Myanmar's CCM from 13.9 in 4Q12 to 9.4 in 2Q13.
- Zimbabwe's CCM decreased from 10.7 in 3Q12 to 8.2 in 2Q13, influenced by a decrease in the prevalence of the worm family Win32/Vobfus, the most commonly detected threat family in Zimbabwe in 1H13.
- Although Pakistan remained one of the locations with the highest infection rates worldwide, the infection rate there decreased from a CCM of 35.3 in 2Q12 to a low of 25.2 in 1Q13, before increasing again to 29.2 in 2Q13. A decrease in infections involving Sality, Ramnit, and the trojan family Win32/Pramro contributed to the decline.
- Indonesia's CCM decreased from 15.7 in 3Q12 to 13.6 in 2Q13, which likely resulted from fewer infections from Ramnit and Sality.

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. Figure 33 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.

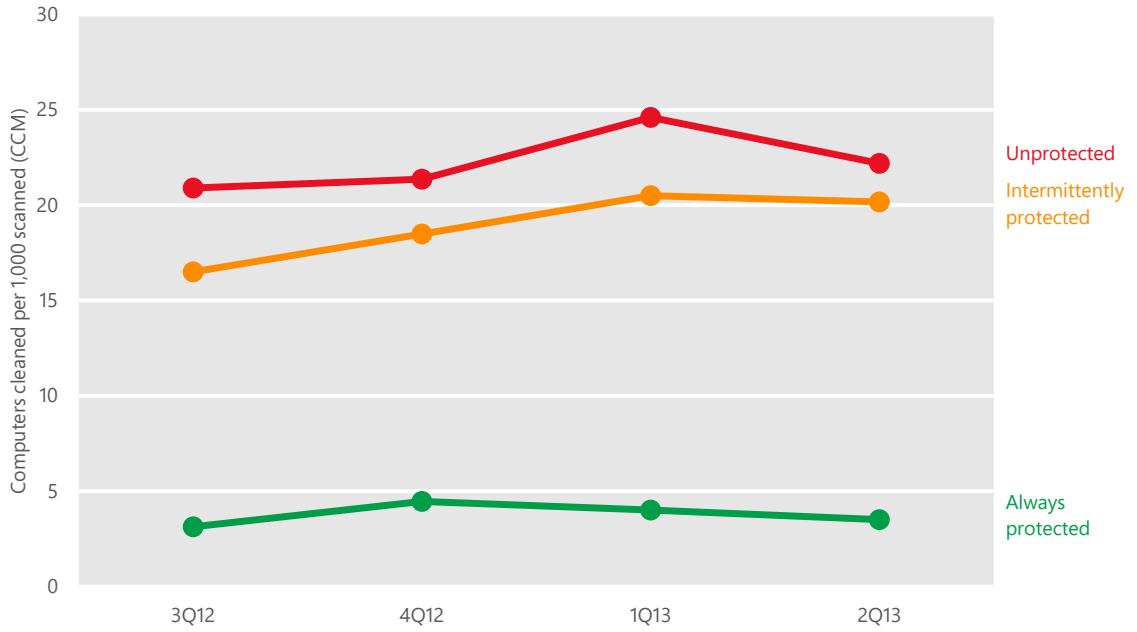
Figure 33. Percentage of computers worldwide protected by real-time security software, 3Q12–2Q13



- A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In Figure 33, "Always protected" represents computers that had real-time security software active and up to date all three times the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or two MSRT executions, but not all three; and "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.
- Overall, almost three-quarters of computers worldwide were found to be always protected every monthly MSRT execution in each of the past four quarters. The trend increased slightly over the four quarters, from 73.1 percent in 3Q12 to 74.7 percent in 2Q13.
- Of the computers that did not always have active protection, most were found to be running real-time security software during at least one of their three monthly MSRT executions. Intermittently protected computers accounted for between 20.2 and 21.4 percent of computers worldwide each quarter, and computers that never reported running security software accounted for between 4.8 and 5.6 percent of computers each quarter.

Computers that do not run real-time security software are at significantly greater risk of malware infection than computers that do. Figure 34 compares infection rates with protection levels worldwide for each of the last four quarters.

Figure 34. Infection rates for protected and unprotected computers, 3Q12–2Q13



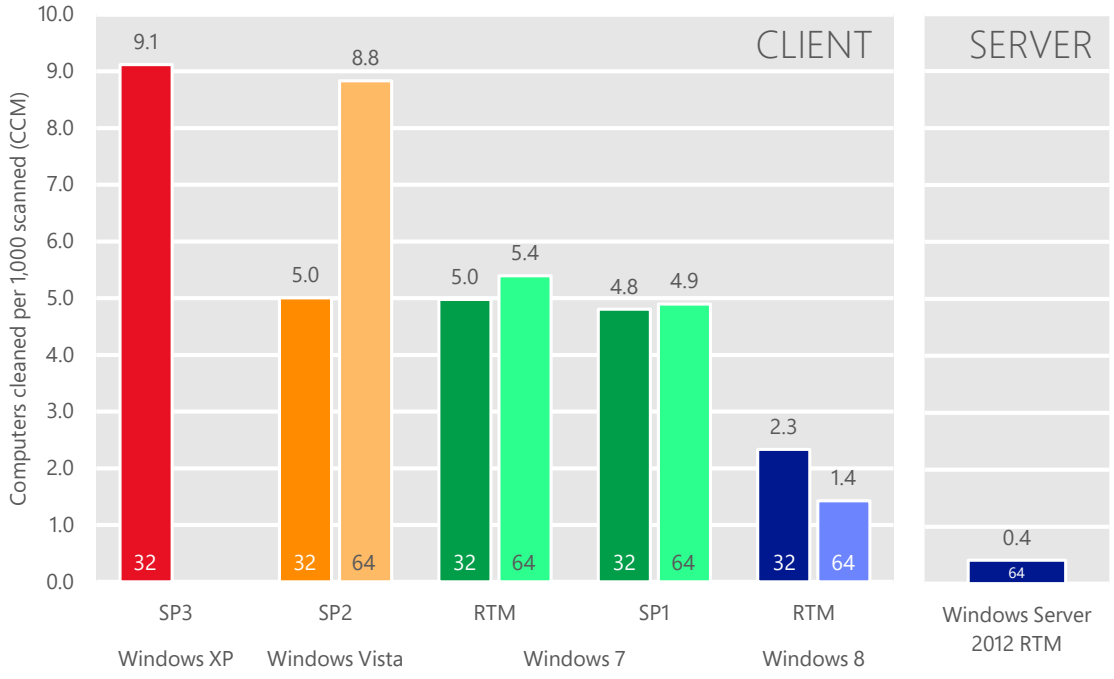
- On average, the MSRT reported that computers that were never found to be running real-time security software during a quarter were 7.1 times as likely to be infected with malware as computers that were always found to be protected. The CCM infection rate for unprotected computers ranged from 20.9 to 24.6, compared to a range of 3.1 to 4.5 for computers that were always protected.
- With infection rates ranging from 16.5 to 20.5, computers that were intermittently protected were 6.0 times as likely to be infected with malware as computers that were always protected—a ratio nearly as great as that for computers that were never found to be protected. As with unprotected computers, the infection rate for intermittently protected computers increased slightly from 2H12 to 1H13 and the infection rate for protected computers fell slightly over the same period.
- Users who don't run real-time security software aren't always unprotected by choice. A number of prevalent malware and potentially unwanted software families are capable of disabling some security products, potentially without the user even knowing. Other users may disable or

uninstall security software intentionally because of perceived performance issues, a belief that protection is not necessary, or a desire to run programs that would be quarantined or removed by security software. In other cases, users lose up-to-date real-time protection when they don't renew paid subscriptions for their antimalware software, which may come pre-installed with their computers as limited-time trial software. Whatever the reason, users who don't have functioning real-time antimalware protection face significantly greater risk from malware infection than users who do, as Figure 34 illustrates.

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

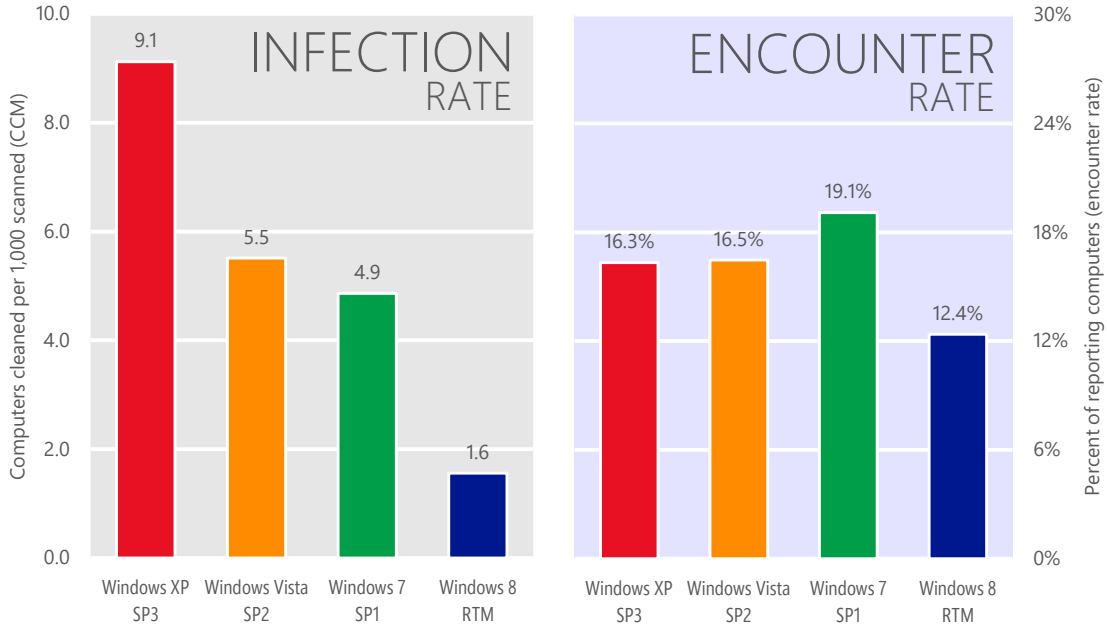


"32" = 32-bit edition; "64" = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.1 percent of total MSRT executions in 2Q13 shown.

- 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).
- As in previous periods, infection rates for more recently released operating systems and service packs tend to be lower than infection rates for earlier releases, for both client and server platforms. Encounter rates also tend to be significantly lower on server platforms than on client platforms: servers are not typically used to browse the web nearly as frequently as client computers, and web browser features such as Enhanced Security Configuration in Internet Explorer discourage using servers to visit untrusted websites.
- In general, newer operating system releases have lower infection rates than older releases. Each 32-bit operating system shown in Figure 35 has a lower CCM than the one before it, with Windows 8 the lowest of all at 2.3, just over one-fourth of the infection rate of Windows XP, the oldest operating system on the chart. The pattern holds true with 64-bit operating systems as well: Windows Vista, the oldest 64-bit operating system represented in the chart, had the highest infection rate, and Windows 8 the lowest.

Figure 36 shows the difference between infection and encounter rates for supported Windows client operating systems in 2Q13 (32-bit and 64-bit editions combined).

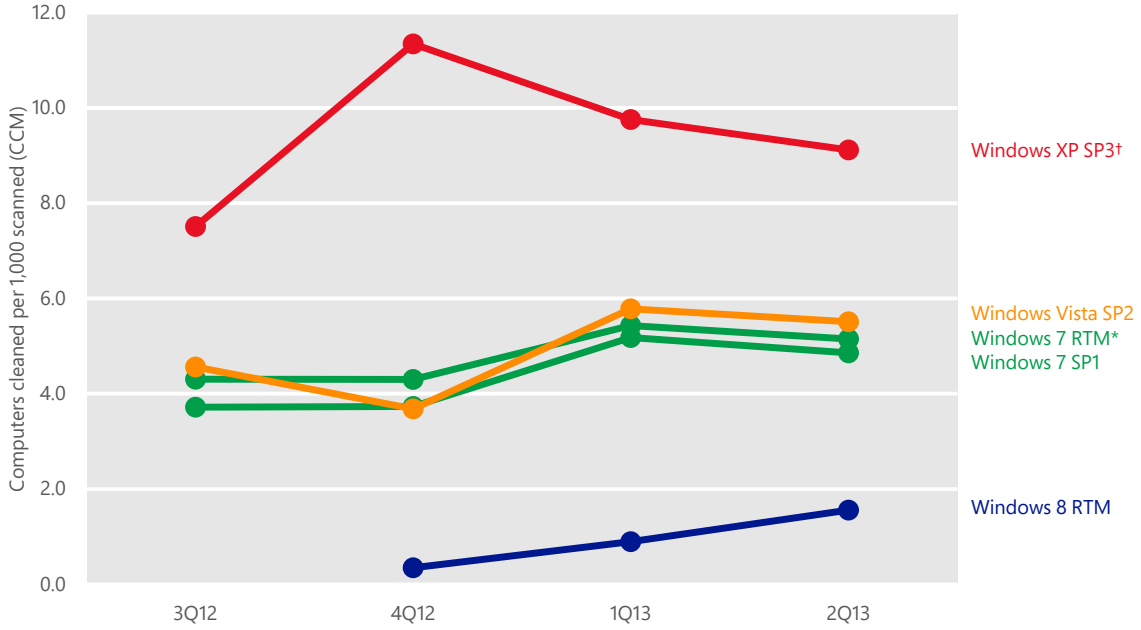
Figure 36. Infection and encounter rates for supported Windows client operating systems, 2Q13



- The infection rate chart on the left shows a clear distinction between newer and older operating system versions. The infection rate for Windows XP (a CCM of 9.1) is significantly higher than the infection rates for both Windows Vista and Windows 7 (5.5 and 4.9, respectively), which in turn are significantly higher than the infection rate for Windows 8 (1.6). Newer operating system versions are not vulnerable to several common exploits that are widely used against older versions, and include a number of security features and mitigations that older versions of Windows lack.
- By contrast, the *encounter* rate differences between operating systems are significantly smaller, totaling around 12–19 percent of all computers worldwide, regardless of operating system. Microsoft real-time security products are designed to block all threats they encounter, even if those threats cannot hurt the computer. For example, the worm family Win32/Conficker exploits a vulnerability that has never affected Windows 8, so Windows 8 cannot be infected by the threat. However, if a Windows 8 user receives a malicious file that attempts to exploit that vulnerability, Windows Defender should detect and block it anyway, and the detection will be counted as an encounter. (In fact, some of the most commonly encountered families worldwide in 1H13—including Conficker, INF/Autorun, Win32/CplLnk, and others—are ineffective against recently released versions of Windows in their default configuration.)

- The disparity between the two metrics highlights the importance of moving away from older operating system versions to newer, more secure ones. Computers running Windows XP in 1H13 encountered about 31 percent more malware worldwide than computers running Windows 8, but their infection rate was more than 5 times as high.
- Although encounter rate data is less effective than infection rate data at showing how secure different operating system versions are in relation to each other, it can provide insights about how attackers target different populations of computers. Some malware families and malicious web pages are designed to scan the computer's operating system and deliver specific threats to different versions, or even to avoid attacking some versions. That Windows 7, currently the most widely installed version of Windows, also has the highest encounter rate suggests that attackers are choosing to focus on the largest populations.

Figure 37. Infection rate (CCM) trends for supported client versions of Windows, 3Q12–2Q13



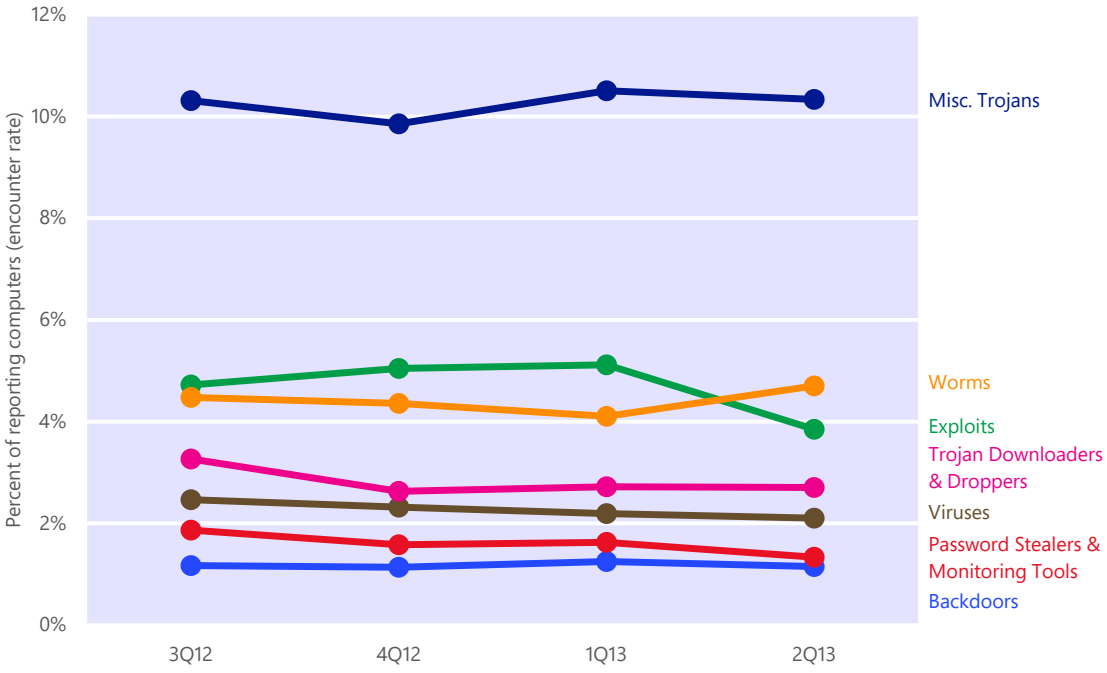
* Support ended April 9, 2013. †Extended support for Windows XP ends April 8, 2014.

Threat categories

The MMPC classifies individual threats into types based on a number of factors, including how the threat spreads and what it is designed to do. To simplify the presentation of this information and make it easier to understand, the *Microsoft*

Security Intelligence Report groups these types into 7 categories based on similarities in function and purpose.

Figure 38. Encounter rates by threat category, 3Q12–2Q13



- Totals for each time period may exceed 100 percent because some computers report more than one category of threat in each time period.
- The Miscellaneous Trojans category remained the most commonly encountered threat category in 2Q13, led by the generic detections Win32/Obfuscator and INF/Autorun and the trojan family Win32/Sirefef. See "Threat families" on page 64 for more information about these and other threats.
- Detections of worms increased in 2Q13, making the Worms category the second most commonly encountered threat category in the quarter. Increased detections of Win32/Dorkbot and Win32/Gamarue contributed substantially to the rise.
- As worms increased, exploit encounters went down. Detections of the multiplatform exploit family Blacole decreased by almost half between 1Q13 and 2Q13, as did exploits of a number of software vulnerabilities targeted by Blacole, such as CVE-2012-1723.

- The Password Stealers & Monitoring Tools category declined slightly over the period. Detections of the password stealer Win32/Fareit and the malware kit family Win32/Zbot, the most commonly encountered threats in this category, both declined in 2Q13.

Threat categories by location

Significant differences exist in the types of threats that affect users in different parts of the world. The spread of malware and its effectiveness are highly dependent on language and cultural factors as well as on the methods used for distribution. Some threats are spread using techniques that target people who speak a particular language or who use online services that are local to a specific geographic region. Other threats target vulnerabilities or operating system configurations and applications that are unequally distributed around the globe.

Figure 39 shows the relative prevalence of different categories of malware and potentially unwanted software in several locations around the world in 2Q13.

Figure 39. Threat category prevalence worldwide and in the 10 locations with the most computers reporting detections in 2Q13

Category	Worldwide	United States	Brazil	Russia	Turkey	India	Mexico	Germany	France	China	United Kingdom
Misc. Trojans	10.3%	8.0%	15.1%	23.6%	30.2%	15.8%	14.6%	6.9%	8.9%	16.3%	8.0%
Worms	4.7%	0.7%	8.4%	5.7%	21.4%	18.0%	17.7%	1.2%	2.1%	5.8%	0.9%
Exploits	3.9%	4.0%	3.1%	3.9%	7.7%	5.4%	3.7%	4.6%	3.6%	2.7%	4.1%
Trojan Downloaders & Droppers	2.7%	1.8%	8.2%	3.9%	10.7%	2.1%	5.6%	0.9%	5.1%	3.6%	1.6%
Viruses	2.1%	0.3%	3.3%	2.2%	8.8%	8.8%	3.5%	0.5%	0.8%	6.2%	0.5%
Password Stealers & Monitoring Tools	1.3%	0.8%	3.2%	2.5%	2.5%	2.8%	1.7%	1.2%	1.3%	1.1%	1.0%
Backdoors	1.2%	0.6%	1.7%	1.2%	2.8%	2.4%	2.4%	0.5%	0.9%	3.1%	0.8%

Totals for each location may exceed 100% because some computers reported threats from more than one category.

- Within each row of Figure 39, a darker color indicates that the category is more prevalent in the specified location than in the others and a lighter color indicates that the category is less prevalent. As in Figure 26 on page 46, the locations in the table are ordered by number of computers reporting detections in 1H13.
- Among these locations, Turkey had the highest malware encounter rates in almost every category, from trojans to worms to viruses.
- Worldwide, Miscellaneous Trojans was the most commonly encountered malware category. The Miscellaneous Trojans concentration was highest in Turkey, where 30.2 percent of computers encountered malware in the category, followed by Russia at 23.6 percent and China at 16.3 percent. The generic detection Win32/Obfuscator was the most commonly detected threat in the category in Turkey, where 7.0 percent of the computers encountered Obfuscator.
- Worms were also most prevalent in Turkey, where 21.4 percent of computers encountered worms during the period, led by Win32/Gamarue, encountered by 7.3 percent of computers in Turkey in 2Q13. Worms were also prevalent in India, where 18.0 percent of computers encountered worms, and in Mexico, at 17.7 percent. Gamarue was the most prevalent worm in India in 2Q13, and Win32/Dorkbot and Gamarue topped the list in Mexico. (See page 66 for more information about Gamarue.)
- Exploits were especially prevalent in Turkey and India, followed by Germany, the UK, and the US. The generic detection HTML/IframeRef was the most commonly encountered exploit in Turkey (with a 5.8 percent encounter rate) and Germany (1.74 percent). Win32/CplLnk was the most commonly encountered exploit in India (3.7 percent).
- The Trojan Downloaders & Droppers category was especially prevalent in Turkey and Brazil. Win32/Wintrim was the most commonly encountered family in this category in Turkey (with a 3.0 percent encounter rate in 2Q13), and was also prevalent in Brazil (2.5 percent).
- Viruses were especially prominent in Turkey and India, with China close behind. Win32/Sality and Win32/Ramnit were prevalent in both Turkey and India, and ALisp/Bursted was prevalent in China.

See "Appendix C: Worldwide infection and encounter rates" on page 127 for more information about malware around the world.

Threat families

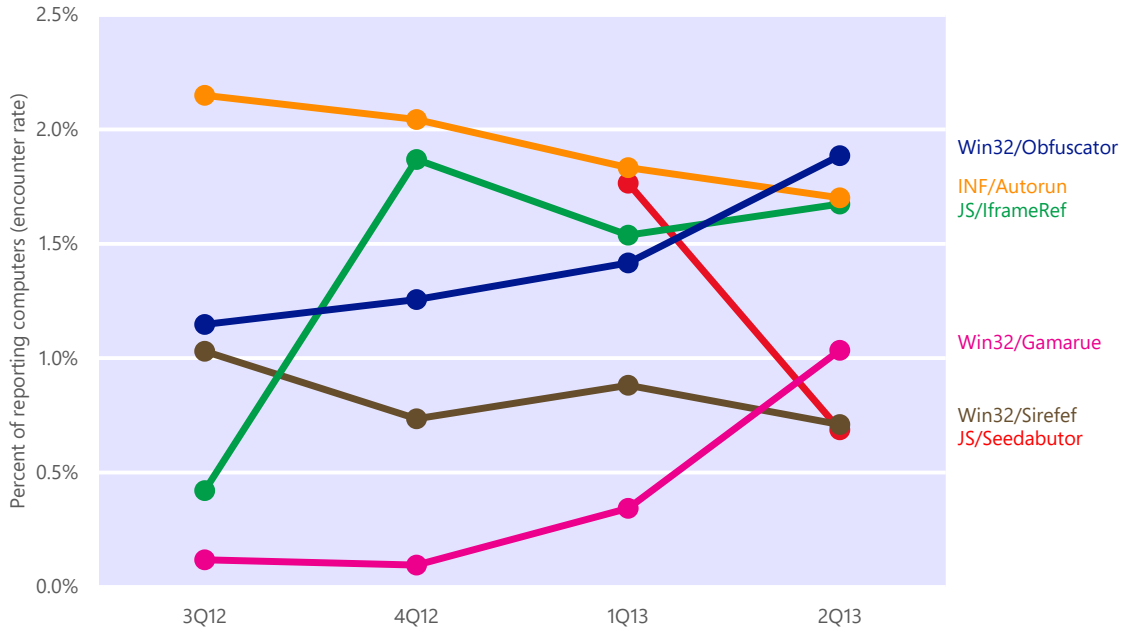
Figure 40 lists the top 10 malware and potentially unwanted software families that were detected on computers by Microsoft antimalware products worldwide in the first half of 2013, with other quarters included for comparison.

Figure 40. Quarterly trends for the top 10 malware families encountered by Microsoft antimalware products in 1H13, shaded according to relative encounter rate

	Family	Most significant category	3Q12	4Q12	1Q13	2Q13
1	INF/Autorun	Miscellaneous Trojans	2.15%	2.04%	1.83%	1.70%
2	Win32/Obfuscator	Miscellaneous Trojans	1.15%	1.26%	1.42%	1.89%
3	HTML/IframeRef	Exploits	0.42%	1.87%	1.54%	1.67%
4	JS/Seedabutor	Miscellaneous Trojans	—	—	1.76%	0.69%
5	Win32/Dorkbot	Worms	0.95%	1.01%	0.82%	0.95%
6	Win32/Sirefef	Miscellaneous Trojans	1.03%	0.74%	0.88%	0.71%
7	Win32/Sality	Viruses	0.80%	0.81%	0.78%	0.73%
8	Win32/Conficker	Worms	0.86%	0.82%	0.72%	0.68%
9	Win32/Gamarue	Worms	0.12%	0.09%	0.34%	1.03%
10	JS/BlacoleRef	Miscellaneous Trojans	0.87%	0.57%	0.45%	0.74%

For a different perspective on some of the changes that have occurred throughout the year, Figure 41 shows the detection trends for a number of families that increased or decreased significantly over the past four quarters.

Figure 41. 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.
- IframeRef, the third most commonly encountered threat in 1H13, is a generic detection for specially formed HTML inline frame (IFrame) tags that redirect

to remote websites that contain malicious content. Detections of IframeRef declined in 1Q13 from their earlier high in 4Q12, but increased slightly in 2Q13.

- JS/Seedabutor, the fourth most commonly encountered threat in 1H13, comprises several variants that were first detected as IframeRef in 2012 and reclassified as a new family in January 2013. (Detections of IframeRef did not decrease by a similar amount in 1Q13 because of the discovery of a heavily used new variant, Trojan:JS/IframeRef.K). Like IframeRef, Seedabutor variants attempt to redirect the computer user's browser to another website.[14]
- Win32/Sirefef, the sixth most commonly encountered threat in 1H13, is a malware platform that receives and runs modules that perform different malicious functions, including perpetrating click fraud and using the infected computer's resources to "mine" for bitcoins, a type of virtual currency. Detection signatures for Sirefef were added to the MSRT in February 2013, and the tool removed the trojan from about 500,000 computers over the following month. For more information about Sirefef, see the following entries in the MMPC blog at blogs.technet.com/mmpc:
  - The Wonder of Sirefef Plunder (May 20, 2013)
  - Reversal of fortune: Sirefef's registry illusion (August 19, 2013)
- Win32/Gamarue, the fourth most commonly encountered threat in 2Q13 and the ninth most prevalent threat for the half-year overall, is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers. The threefold increase in the Gamarue encounter rate between 1Q13 and 2Q13 is primarily the result of improved detection techniques, following the discovery of a new series of components (designated

[14] The Seedabutor family was redesignated as early warning telemetry in 3Q13, after the time period examined by this report. Detections of threats that are designated as early warning telemetry are not reported to the computer user as malware (and will not be included in the next volume of this report), but Microsoft continues to receive reports about the files downloaded by the detected trojan. Microsoft uses the early warning telemetry designation when detection of a threat begins to produce a large number of false positives, which indicates that the usage pattern of the threat has changed—in this case, the attackers have begun to use Seedabutor to drop large numbers of clean files along with random drops of malware, evidently in an effort to make security software less effective. Using early warning telemetry enables Microsoft to continue to monitor the threat without inconveniencing customers and vendors with repeated blocks and removals of clean software.

Worm:Win32/Gamarue.N, Worm:Win32/Gamarue.gen!Ink, and others) that spread Gamarue over removable drives.

For more information about Gamarue, see the following entries in the MMPC blog at blogs.technet.com/mmpc:

- Get gamed and rue the day... (October 25, 2011)
- The strange case of Gamarue propagation (February 27, 2013)

Threat families by platform

Malware does not affect all platforms equally. Some threats are spread by exploits that are ineffective against one or more operating system versions. Some threats are more common in parts of the world where specific platforms are more or less popular than elsewhere. In other cases, differences between platforms may be caused by simple random variation. Figure 42 demonstrates how detections of the most prevalent families in 2Q13 ranked differently on different operating system/service pack combinations.

Figure 42. The malware families most commonly encountered by Microsoft antimalware solutions in 2Q13, and how they ranked in prevalence on different platforms

Rank 2Q13	Family	Most significant category	Rank (Windows 8 RTM)	Rank (Windows 7 SP1)	Rank (Windows Vista SP2)	Rank (Windows XP SP3)
1	Win32/Obfuscator	Miscellaneous Trojans	1	1	4	6
2	INF/Autorun	Miscellaneous Trojans	2	3	13	1
3	HTML/IframeRef	Exploits	3	2	1	2
4	Win32/Gamarue	Worms	4	4	24	7
5	Win32/Dorkbot	Worms	8	5	25	8
6	JS/BlacoleRef	Miscellaneous Trojans	15	6	6	9
7	Win32/Sality	Viruses	6	12	52	5
8	Win32/Sirefef	Miscellaneous Trojans	20	7	2	12
9	JS/Seedabutor	Miscellaneous Trojans	5	13	26	3
10	Win32/Conficker	Worms	13	10	28	4
13	Java/CVE-2012-1723	Exploits	43	9	3	20

- Microsoft real-time antimalware products detect and block threats that attempt to infect computers even if those attempts would not have succeeded otherwise. The generic family INF/Autorun, which propagates

using a technique that is ineffective on Windows 7 and Windows 8, was nevertheless the third and second most commonly encountered threat family, respectively, on those platforms in 2Q13.[15]

- The generic detections Win32/Obfuscator, Autorun, and HTML/IframeRef, the three most commonly encountered threats overall in 2Q13, were also the top three threats on Windows 7 and Windows 8 individually. IframeRef and Autorun were the most commonly encountered threats on Windows Vista and Windows XP, respectively.
- Autorun, Win32/Sality, JS/Seedabutor, and Win32/Conficker had higher encounter rates on XP than on any other platform.
- Win32/Sirefef, Java/CVE-2012-1723, and JS/BlacoleRef were encountered more frequently on the Vista SP2 platform than on the other platforms.

Rogue security software

Rogue security software has become one of the most common methods that attackers use to swindle money from victims. Rogue security software, also known as *scareware*, is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure users into participating in fraudulent transactions. These programs typically mimic the general look and feel of legitimate security software programs and claim to detect a large number of nonexistent threats while urging users to pay for the so-called "full version" of the software to remove the nonexistent threats.

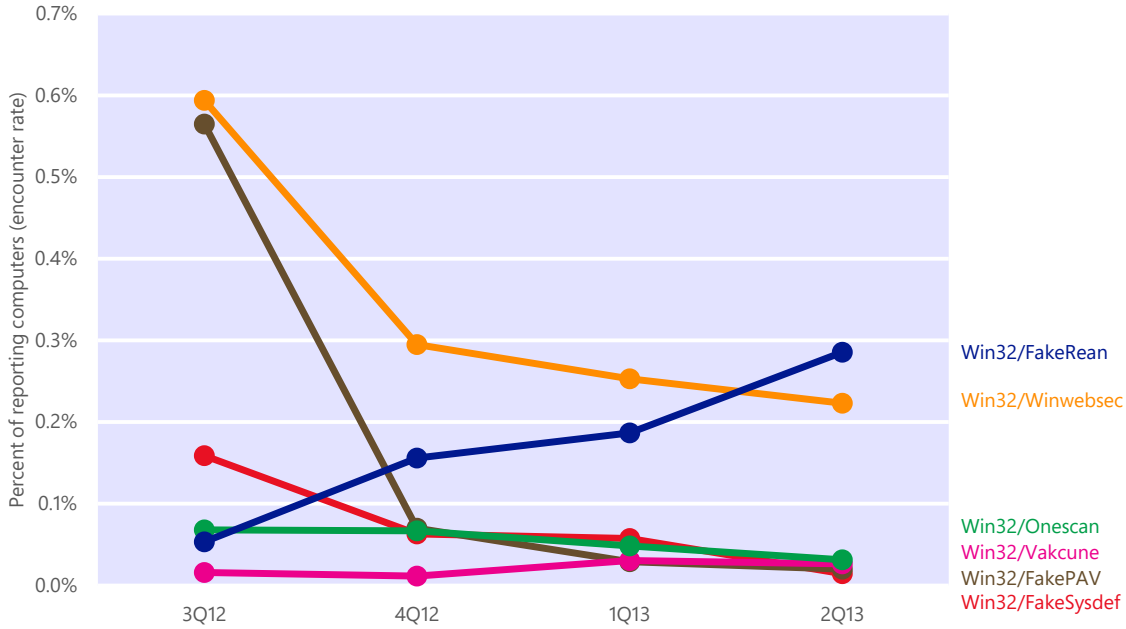
Attackers typically install rogue security software programs through exploits or other malware, or use social engineering to trick users into believing the programs are legitimate and useful. Some versions emulate the appearance of the Windows Security Center or unlawfully use trademarks and icons to misrepresent themselves. (See http://www.microsoft.com/security/resources/videos.aspx for an informative series of videos designed to educate general audiences about rogue security software.)

[15] Recent changes to Windows XP and Windows Vista, which have been available as automatic updates on Microsoft update services since 2011, make the technique ineffective on those platforms as well. See support.microsoft.com/kb/971029 for more information.

Figure 43. False branding used by a number of commonly detected rogue security software programs

Figure 44 shows detection trends for the most common rogue security software families detected in 1H13.

Figure 44. Trends for the most common rogue security software families encountered in 1H13, by quarter



- Win32/FakeRean, the most commonly encountered rogue security software program in 2Q13, has been distributed since 2008 under several different names, which are often generated at random based upon the operating system of the affected computer. Its distributors tend to concentrate their efforts into short-term campaigns during which they propagate FakeRean at high volumes, followed by periods of inactivity.

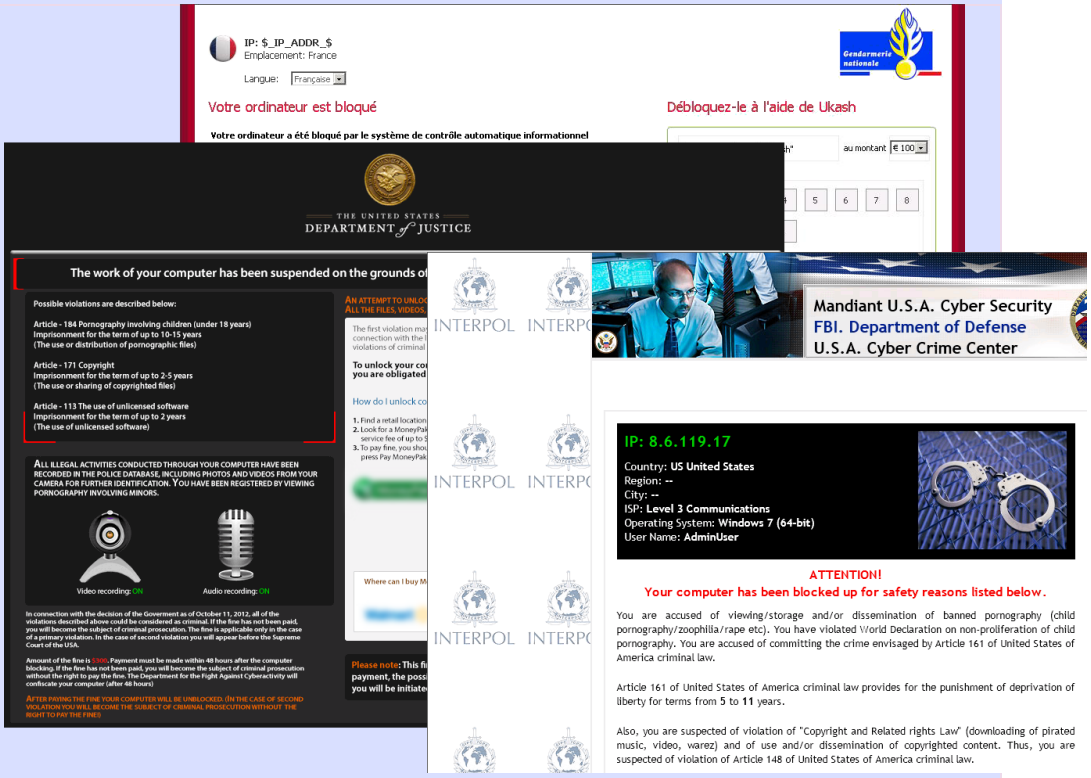
- Detections of Win32/Winwebsec have decreased considerably since 2012, but it remained the most commonly encountered rogue security software family in 1Q13 and in the first half of the year overall. Winwebsec has been distributed under a variety of names, with the user interface and other details changing to reflect each variant's individual branding; currently prevalent names include Antivirus Security Pro, AVASoft Professional Antivirus, Smart Fortress 2012, Win 8 Security System, and several others. These different distributions of the trojan use various installation methods, with file names and system modifications that can differ from one variant to the next. The attackers behind Winwebsec are also believed to be responsible for MacOS_X/FakeMacdef, the "Mac Defender" rogue security software program for Apple Mac OS X that first appeared in May 2011.
- Win32/Onescan and Win32/Vakcune are Korean-language rogue security software programs. Onescan has been a significant threat in Korea for a number of years, but encounters have declined in 2013 to less than half of their 2012 levels. In recent months, the authors of Onescan have shifted their focus from rogue security software to computer optimization software that has not yet been observed to be associated with malware.

Figure 45. A variant of Win32/OneScan, a Korean-language rogue security software program

Focus on ransomware

Recent media coverage has brought attention to the problem of *ransomware*, a type of malware that is designed to render a computer or its files unusable until the computer user pays a certain amount of money to the attacker. It often masquerades as an official-looking warning from a well-known law enforcement agency, such as the US Federal Bureau of Investigation (FBI) or the Metropolitan Police Service of London (also known as Scotland Yard); it accuses the computer user of committing a computer-related crime and demands that the user pay a fine via electronic money transfer to regain control of the computer. Some recent ransomware threats are also known as "FBI Moneypak" or the "FBI virus" for their common use of law enforcement logos and requests for payment using Green Dot MoneyPak, a brand of reloadable debit card. A ransomware infection does not mean that any illegal activities have actually been performed on the infected computer.

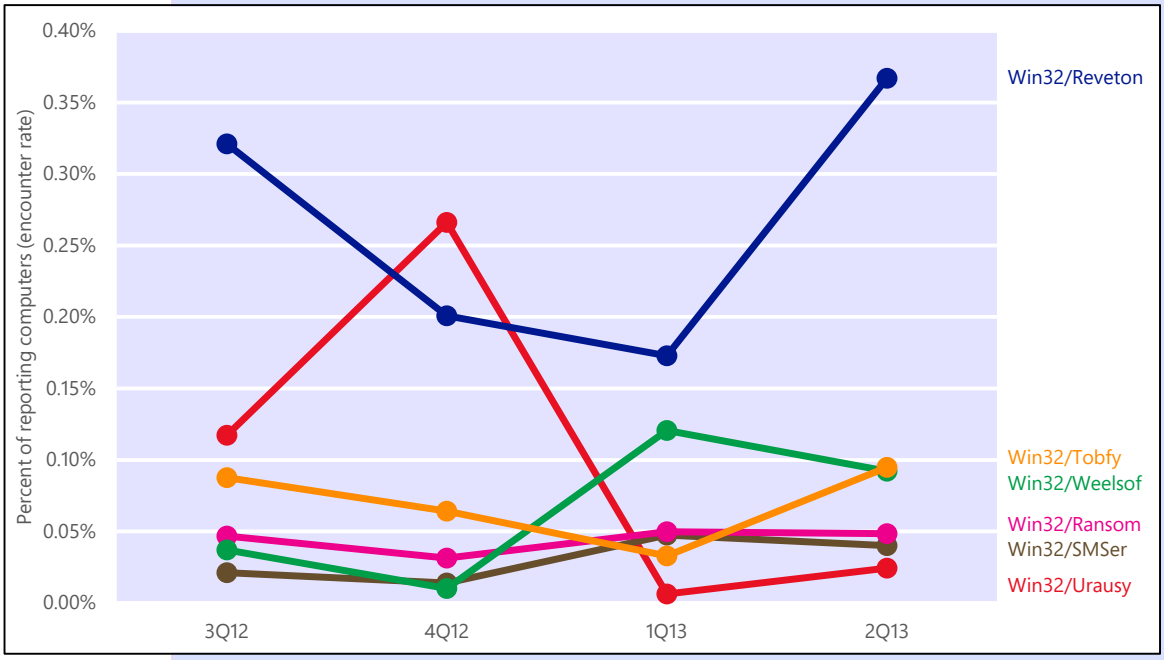
Figure 46. Lock screens used by different ransomware families, masquerading as warnings from various national and international police forces



Some ransomware families operate by displaying a lock screen and preventing access to any of the computer's functions. Others encrypt the computer user's files with a password and offer to provide the user with the password upon payment of the ransom. In both cases, the computer is essentially held hostage for a ransom that, the perpetrators say, will release the computer if paid. Frequently, access to the computer is not restored even upon payment.

Figure 47 displays encounter rate trends for the most commonly encountered ransomware families worldwide.

Figure 47. Encounter rate trends for the top 6 ransomware families in 1H13



- Win32/Reveton was the most commonly encountered ransomware family worldwide in 1H13. Reveton displays behavior that is typical of many ransomware families: it locks computers and displays a webpage that covers the entire desktop of the infected computer, and demands that the user pay a fine for the supposed possession of illicit material. The webpage that is displayed and the identity of the law enforcement agency that is allegedly responsible for it are often customized, based on the user's current location. Reveton encounters declined slightly in 1Q13 before increasing and spiking again in 2Q13. Detections especially increased in the Czech Republic, Slovakia, and Cyprus, which contributed to the worldwide rise. The Czech

Republic was the location with the highest Reveton encounter rate in 2Q13 at 0.83 percent.

For additional information about Reveton, see the entry "Revenge of the Reveton" (April 18, 2012) in the MMPC blog at blogs.technet.com/mmpc.

- Win32/Weelsof, the second most commonly detected ransomware family worldwide in 1H13, was encountered in rapidly increasing numbers in the first quarter of the year, then declined moderately in the second. Ireland, France, and Greece saw the highest encounter rates for this ransomware in 2Q13. Weelsof is known to target computers from specific countries and regions, displaying fake warnings that claim to be from the appropriate national police force. Detection signatures for Weelsof were added to the MSRT in November 2012.

  For additional information about Weelsof, see the entry "MSRT November '12 - Weelsof around the world" (December 4, 2012) in the MMPC blog.

- Win32/Tobfy, the third most commonly detected ransomware family worldwide in 1H13, showed an increase in 2Q13 that made it the second most commonly detected ransomware family by a narrow margin during that quarter. The United States had the highest encounter rate for Tobfy in 2Q13, at 0.21 percent, followed by Mexico and Canada.

- Detections of Win32/Urausy, which had been the most commonly detected malware family worldwide in 4Q12, declined significantly in 1Q13 before increasing slightly in 2Q13. Detections increased significantly in 2Q13 in most of the locations where Urausy was most prevalent, led by Austria, Switzerland, and Cyprus.

Figure 48. Win32/Urausy encounter rate trends for the 10 countries or regions where it was most often detected in 1H13

	Country/region	3Q12	4Q12	1Q13	2Q13
1	Austria	0.03%	0.04%	0.28%	0.94%
2	Switzerland	0.04%	0.13%	0.34%	0.86%
3	Belgium	0.03%	0.07%	0.28%	0.79%
4	Greece	0.00%	0.07%	0.23%	0.73%
5	Germany	0.03%	0.06%	0.24%	0.69%
6	Cyprus	—	0.03%	0.12%	0.80%
7	Croatia	—	0.08%	0.18%	0.71%
8	Ireland	0.00%	0.06%	0.20%	0.62%
9	Spain	0.03%	0.04%	0.18%	0.61%
10	Portugal	0.01%	0.07%	0.12%	0.64%

Microsoft recommends that victims of ransomware infections not pay the so-called fine. Ransomware is distributed by malicious attackers, not legitimate authorities, and paying the ransom is no guarantee that the attacker will restore the affected computer to a usable state. Microsoft provides tools and utilities, such as the Microsoft Safety Scanner and Windows Defender Offline, that can help remove a variety of malware infections even if the computer's normal operation is being blocked.

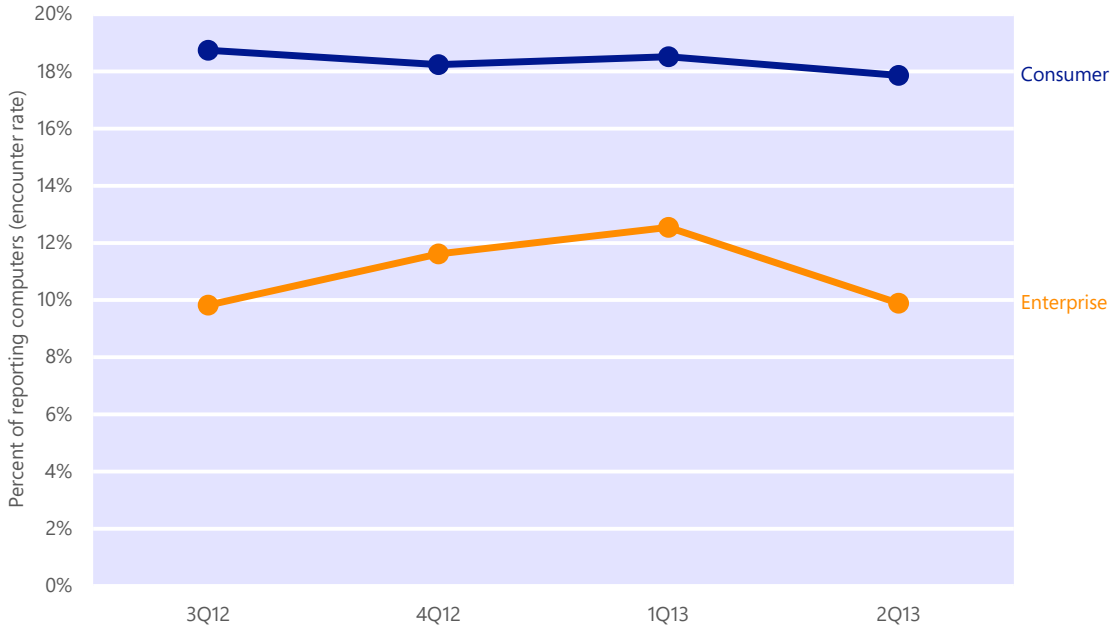
Visit www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx for more information about ransomware and how computer users can avoid being taken advantage of by these threats.

Home and enterprise threats

The usage patterns of home users and enterprise users tend to be very different. Enterprise users typically use computers to perform business functions while connected to a network, and may have limitations placed on their Internet and email usage. Home users are more likely to connect to the Internet directly or through a home router and to use their computers for entertainment purposes, such as playing games, watching videos, shopping, and communicating with friends. As a result, Microsoft enterprise-focused security products (such as System Center 2012 Endpoint Protection) tend to report malware encounter

rates and patterns that distinctly differ from those reported by Microsoft consumer-focused security products (such as Microsoft Security Essentials). 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 49. 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 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 50 and Figure 51 list the top 10 families detected by enterprise and consumer security products, respectively, in 1H13.

Figure 50. Quarterly trends for the top 10 families detected by Microsoft enterprise security products in 1H13, by percentage of computers encountering each family

	Family	Most significant category	3Q12	4Q12	1Q13	2Q13
1	JS/Seedabutor	Miscellaneous Trojans	—	—	7.3%	2.4%
2	HTML/IframeRef	Exploits	0.6%	5.8%	2.6%	1.9%
3	Win32/Conficker	Worms	2.3%	2.1%	1.8%	1.4%
4	INF/Autorun	Miscellaneous Trojans	1.8%	1.8%	1.6%	1.4%
5	Win32/Sirefef	Miscellaneous Trojans	1.0%	0.8%	1.5%	1.2%
6	JS/BlacoleRef	Miscellaneous Trojans	1.5%	1.1%	1.2%	1.3%
7	Java/CVE-2012-1723	Exploits	1.1%	1.7%	1.3%	0.9%
8	Blacole	Exploits	1.3%	1.4%	1.5%	0.7%
9	Win32/Dorkbot	Worms	0.8%	0.8%	0.7%	0.7%
10	Win32/Obfuscator	Miscellaneous Trojans	0.7%	0.6%	0.6%	0.6%

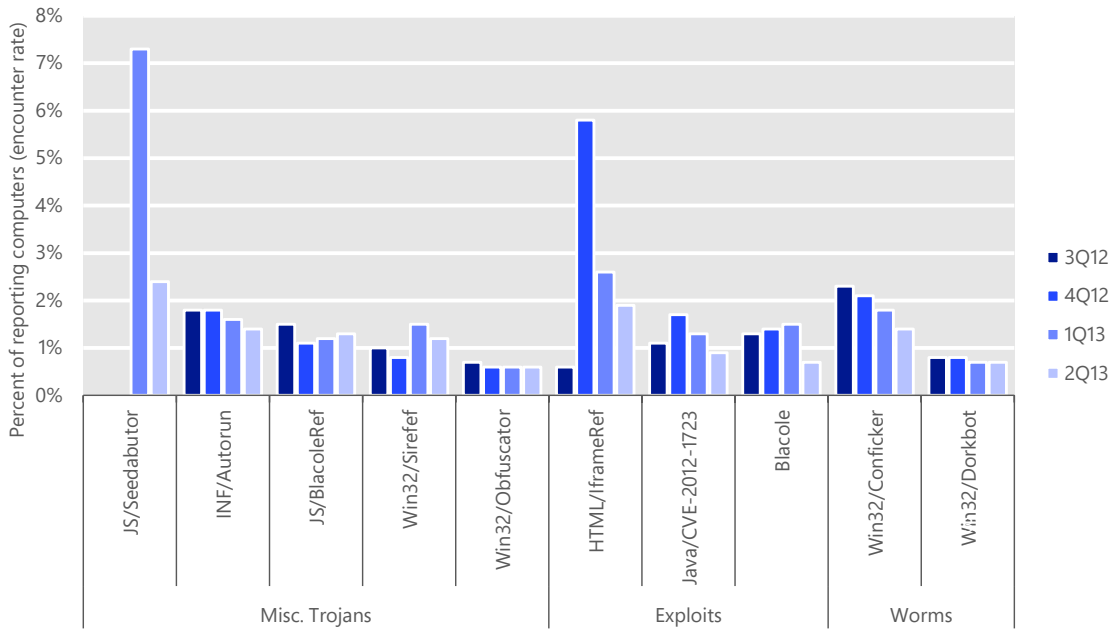
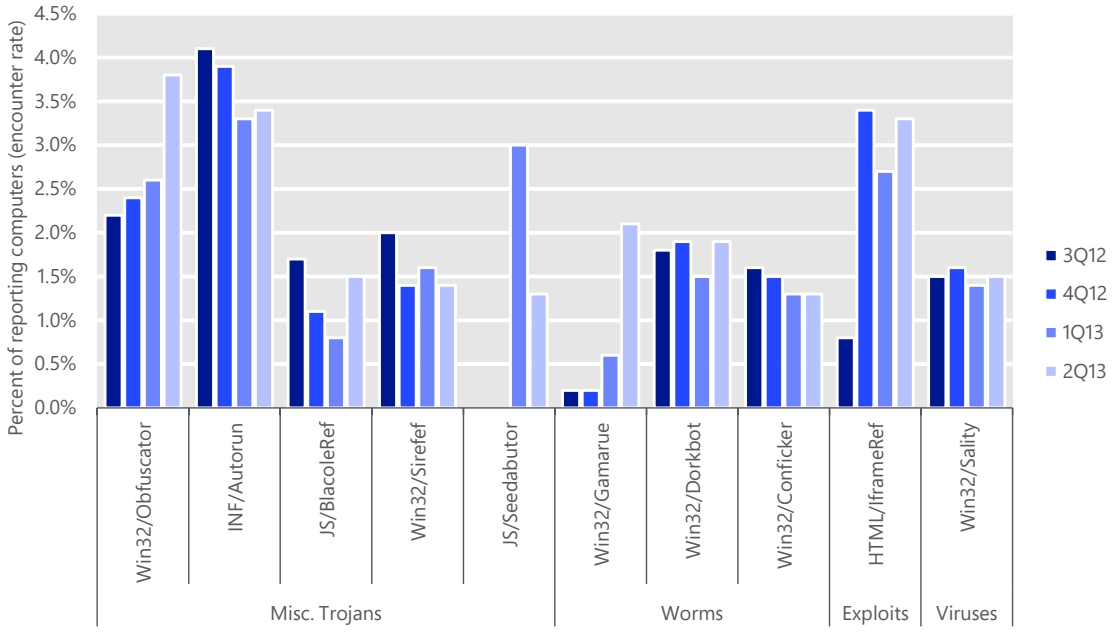


Figure 51. Quarterly trends for the top 10 families detected by Microsoft consumer security products in 1H13, by percentage of computers encountering each family

	Family	Most significant category	3Q12	4Q12	1Q13	2Q13
1	INF/Autorun	Miscellaneous Trojans	4.1%	3.9%	3.3%	3.4%
2	Win32/Obfuscator	Miscellaneous Trojans	2.2%	2.4%	2.6%	3.8%
3	HTML/IframeRef	Exploits	0.8%	3.4%	2.7%	3.3%
4	JS/Seedabutor	Miscellaneous Trojans	—	—	3.0%	1.3%
5	Win32/Dorkbot	Worms	1.8%	1.9%	1.5%	1.9%
6	Win32/Sirefef	Miscellaneous Trojans	2.0%	1.4%	1.6%	1.4%
7	Win32/Sality	Viruses	1.5%	1.6%	1.4%	1.5%
8	Win32/Gamarue	Worms	0.2%	0.2%	0.6%	2.1%
9	Win32/Conficker	Worms	1.6%	1.5%	1.3%	1.3%
10	JS/BlacoleRef	Miscellaneous Trojans	1.7%	1.1%	0.8%	1.5%



- 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).

Guidance: Defending against malware

Effectively protecting users from malware requires an active effort on the part of organizations and individuals. For in-depth guidance, see Protecting Against Malicious and Potentially Unwanted Software in the "Mitigating Risk" section of the *Microsoft Security Intelligence Report* website.

Potentially unwanted software

Potentially unwanted software refers to programs that pose a moderate/low security risk but can affect a user's privacy, security, or computing experience. Figure 52 lists the top 10 locations with the most encounters for potentially unwanted software during the first half of this year.

Figure 52. Encounter rate trends for the locations with the most computers reporting potentially unwanted software detections in 1H13

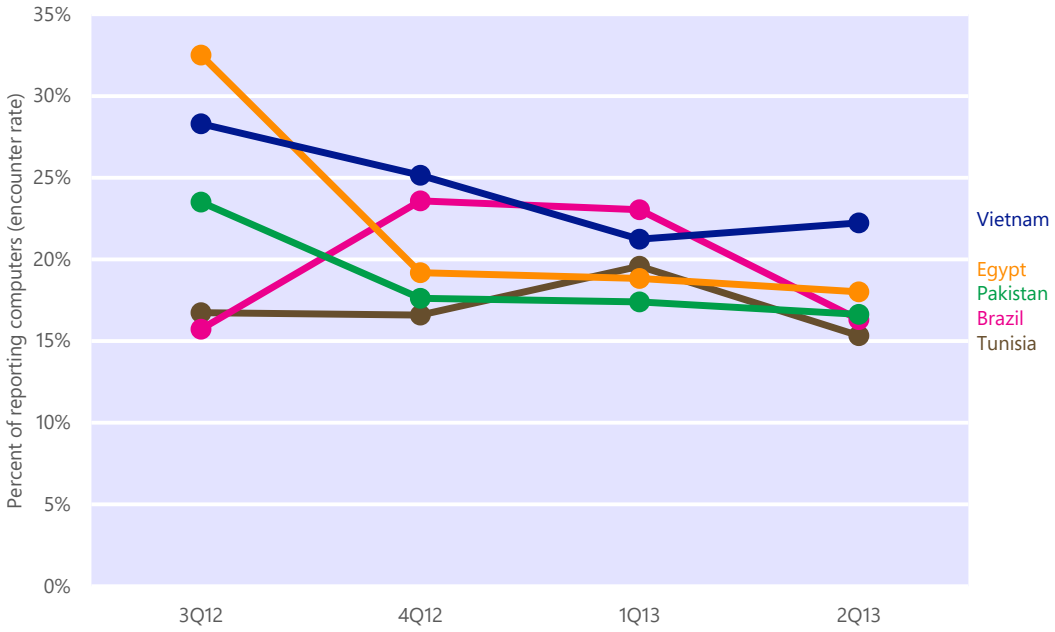
	Country/Region	3Q12	4Q12	1Q13	2Q13	Chg. 2H–1H
1	United States	7.42%	4.29%	4.99%	3.79%	-25.04% ▼
2	Brazil	15.73%	23.58%	23.04%	16.31%	0.09% ▲
3	Russia	17.52%	14.43%	15.41%	11.58%	-15.53% ▼
4	Turkey	32.90%	16.44%	16.11%	12.23%	-42.55% ▼
5	India	16.73%	12.34%	11.59%	9.28%	-28.21% ▼
6	Mexico	13.11%	12.82%	13.21%	10.07%	-10.24% ▼
7	Germany	7.68%	5.44%	6.74%	3.55%	-21.56% ▼
8	France	10.34%	10.03%	12.37%	6.38%	-7.92% ▼
9	China	6.37%	4.56%	4.03%	3.47%	-31.39% ▼
10	United Kingdom	8.24%	6.07%	7.40%	4.97%	-13.53% ▼

- The potentially unwanted software rate for the United States declined more than 25 percent from 2H12 to 1H13. Encounter rates for the adware families Win32/Hotbar and Win32/GameVance and the potentially unwanted software family Win32/Keygen trended downward from quarter to quarter, which influenced this drop.
- Computers in Russia experienced reduced encounter rates for Win32/Pameseg, which drove a decrease of more than 15 percent between 2H12 and 1H13. A number of Pameseg variants were reassigned to new families in April, which accounts for much of the decrease in Pameseg encounters.
- Turkey's encounter rate for potentially unwanted software dropped by more than 42 percent between 2H12 and 1H13. A 17.7 percent reduction in

JS/Pornpop encounter rates, driven by the MMPC's adoption of new criteria for designating potentially unwanted software, contributed to the decline.[16]

- In India, the potentially unwanted software encounter rate decreased by 28.2 percent between 2H12 and 1H13, as encounters with the adware family Win32/Adkubru declined by nearly 5 percentage points alone.
- China experienced reduced encounter rates for Keygen and JS/Popupper, which influenced the 31.4 percent drop between 2H12 and 1H13 for potentially unwanted software.

Figure 53. Trends for the five locations with the highest potentially unwanted software encounter rates in 1H13 (minimum 100,000 reporting computers)

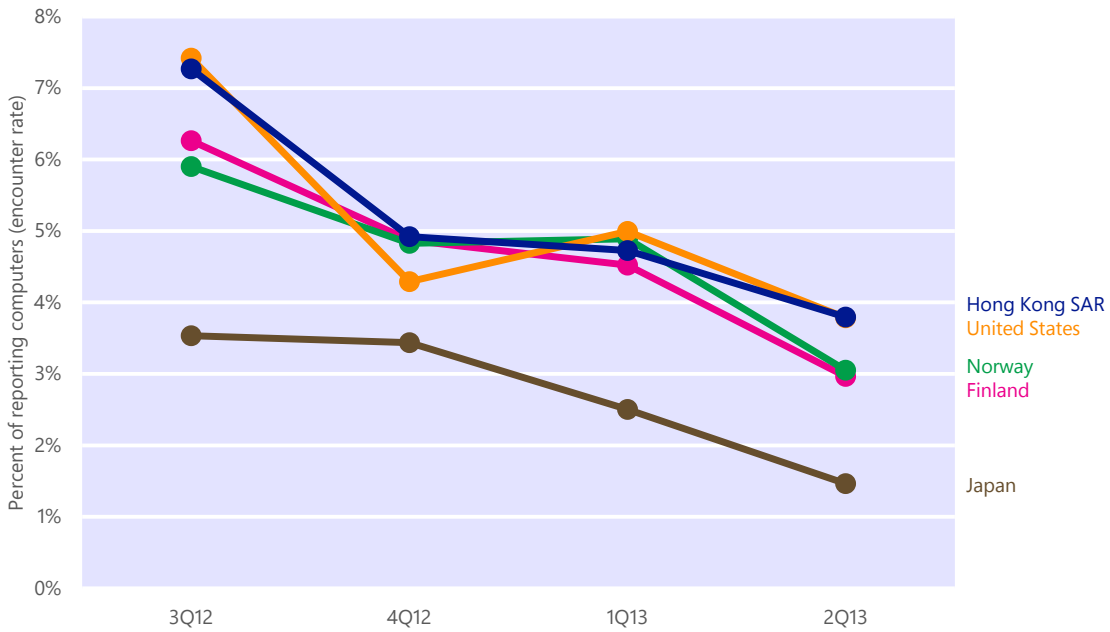


- Vietnam's encounter rate dropped from 3Q12 to 1Q13, but increased slightly in 2Q13. The top three reports were for hack tools Win32/Keygen and Win32/Patch, and settings modifier Win32/PossibleHostsFileHijack. Keygen is a detection for tools that generate keys for pirated software. Attackers often package malware in bundles along with the tools and the pirated software or media.

[16] Microsoft has published the criteria that the company uses to classify programs as potentially unwanted software at www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx. For programs that have been classified as potentially unwanted software, Microsoft provides a dispute resolution process to allow for reporting of potential false positives and to provide software vendors with the opportunity to request investigation of a rating with which they do not agree.

- Keygen also led in Egypt, making up 12.87 percent of encounters there, followed by Patch and Win32/Wpakill. Overall encounter rates in Egypt decreased in 4Q12 and have remained steady, trending slightly downward in 2Q13.
- In Pakistan, encounter rates for INF/Autorun, Win32/Sality, and Win32/Ramnit declined between 2H12 and 1H13, which contributed to Pakistan's improved overall encounter rate. Win32/Gamarue encounters increased 9.8 percent in 2Q13, which accounted for the small overall increase that quarter.
- Brazil's encounter rate jumped in 4Q12 and remained steady in 1Q13. The country had the fourth highest number of potentially unwanted software encounters in 2Q13. Again, Keygen was the most prevalent, with new adware addition Win32/FindLyrics a close second. Software bundler Win32/Protlerdob was also high on the list. This program presents itself as a free movie download, but is often bundled with a number of programs that may charge for services.
- Tunisia dropped to a 15 percent encounter rate in 2Q13. A higher number of reports in the previous quarter can be attributed to Keygen and Wpakill, as well as adware Win32/Gisav, which Microsoft first detected in 1Q13.

Figure 54. Trends for the five locations with the lowest potentially unwanted software encounter rates in 1H13 (100,000 reporting computers minimum)



- Japan's encounter rate dropped from 2.5 percent in 1Q13 to 1.46 percent in 2Q13. This was partly caused by a drop in reports for Win32/Keygen, Win32/OpenCandy and Win32/DealPly. Microsoft also added new detections for the other top encounters, Win32/PriceGong and Win32/FindLyrics.
- Encounter rates also declined in Finland, because of a drop in reports for the top five detections: Keygen, PriceGong, Win32/Hotbar, Win32/Wpakill, and OpenCandy.
- In Norway, Keygen encounter rates decreased from 1.58 percent in 1Q13 to 1.24 percent in 2Q13. Encounters with PriceGong, a detection added in 1Q13, also fell from 1.10 percent to 0.53 percent. The overall rate in Norway decreased in 2Q13.
- Hong Kong also trended downward, with a drop in encounter rates for Keygen, Win32/FastSaveApp, and Wpakill.
- A decline in reports for Keygen, Hotbar, and Win32/GameVance helped decrease the overall encounter rate for the United States. Microsoft added detections for adware families PriceGong and Win32/InfoAtoms in 1Q13, which accounts for the increase in reports during the previous reporting period.

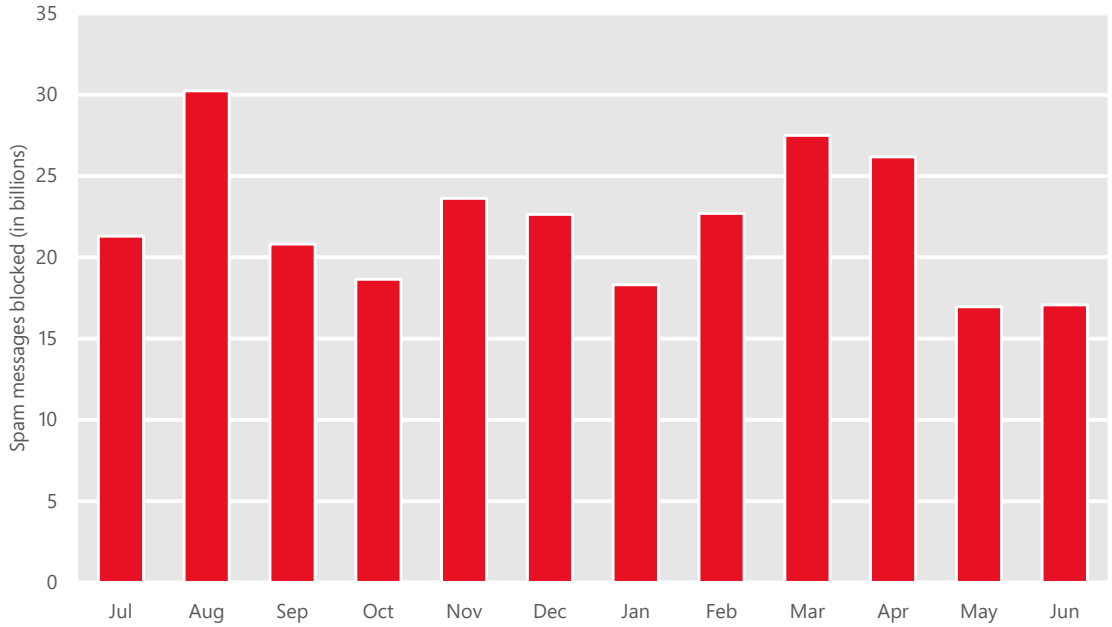
Email threats

More than 75 percent of the email messages sent over the Internet are unwanted. Not only does all this unwanted email tax recipients' inboxes and the resources of email providers, but it also creates an environment in which emailed malware attacks and phishing attempts can proliferate. Email providers, social networks, and other online communities have made blocking spam, phishing, and other email threats a top priority.

Spam messages blocked

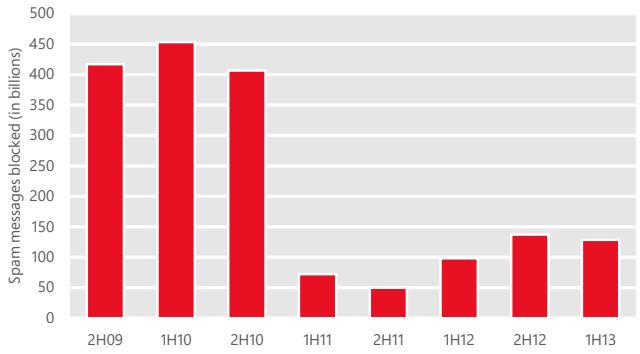
The information in this section of the *Microsoft Security Intelligence Report* is compiled from telemetry data provided by Exchange Online Protection, which provides spam, phishing, and malware filtering services. Exchange Online Protection is used by tens of thousands of Microsoft enterprise customers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

Figure 55. Messages blocked by Exchange Online Protection, July 2012–June 2013



- Blocked mail volumes in 1H13 were consistent with 2H12, and remain well below levels seen prior to the end of 2010, as shown in Figure 56. 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

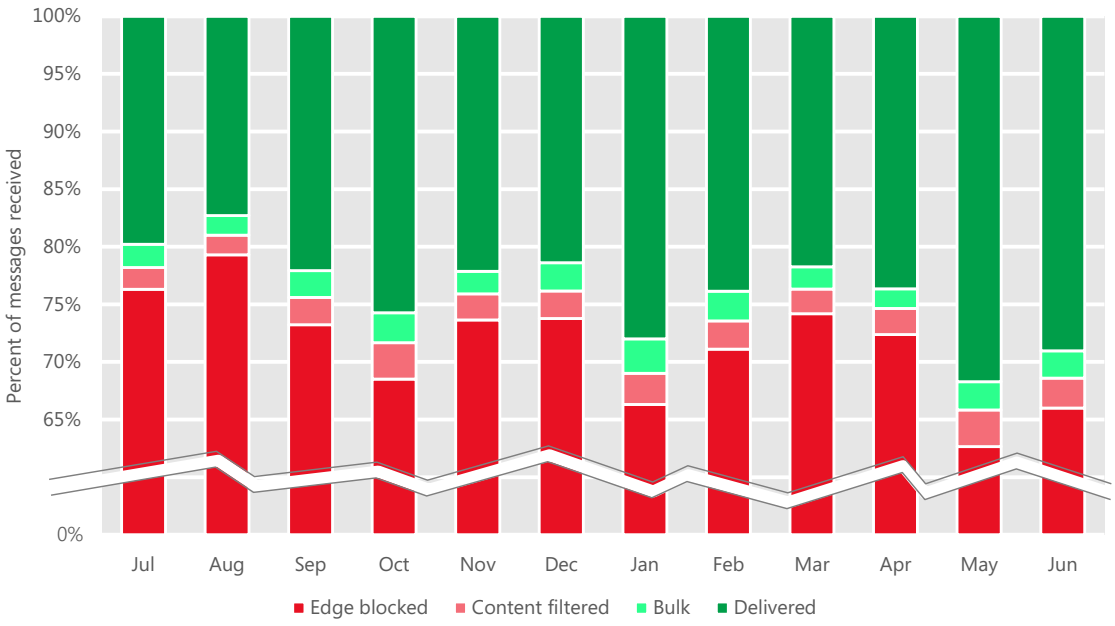
Figure 56. Messages blocked by Exchange Online Protection each half-year period, 2H09–1H13



Cutwail (August 2010) and Rustock (March 2011).[17] 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.

Exchange Online Protection performs spam filtering in two stages. Most spam is blocked by servers at the network edge, which use reputation filtering and other non–content-based rules to block spam or other unwanted messages. Messages that are not blocked at the first stage are scanned using content-based rules, which detect and filter many additional email threats, including attachments that contain malware.

Figure 57. Percentages of incoming messages blocked, categorized as bulk email, and delivered, July 2012–June 2013



- Between 62.7 and 74.2 percent of incoming messages were blocked at the network edge each month in 1H13, which means that only 25.8 to 37.3

[17] 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.

percent of incoming messages had to be subjected to the more resource-intensive content filtering process. Between 7.6 and 10.0 percent of the remaining messages (1.7 to 2.7 percent of all incoming messages) were filtered as spam each month.

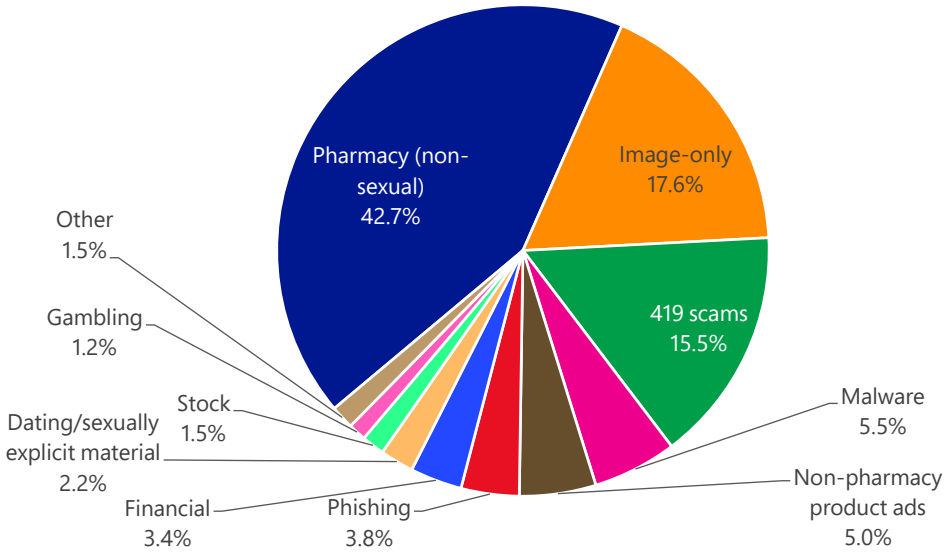
- Exchange Online Protection identifies bulk email messages that some users consider unwanted but that aren't categorized as spam by edge blocks or content filters. These messages typically include email newsletters, advertisements, and marketing messages that users claim they never asked for, or don't remember subscribing to. Exchange Online Protection flags these messages as bulk in an incoming header so customers and individual users can use rules in Microsoft Outlook or Exchange to filter, move, or deliver them as desired.

  Bulk email volumes did not vary significantly from month to month in 1H13. Between 6.7 and 10.2 percent of all delivered messages were categorized as bulk each month.

Spam types

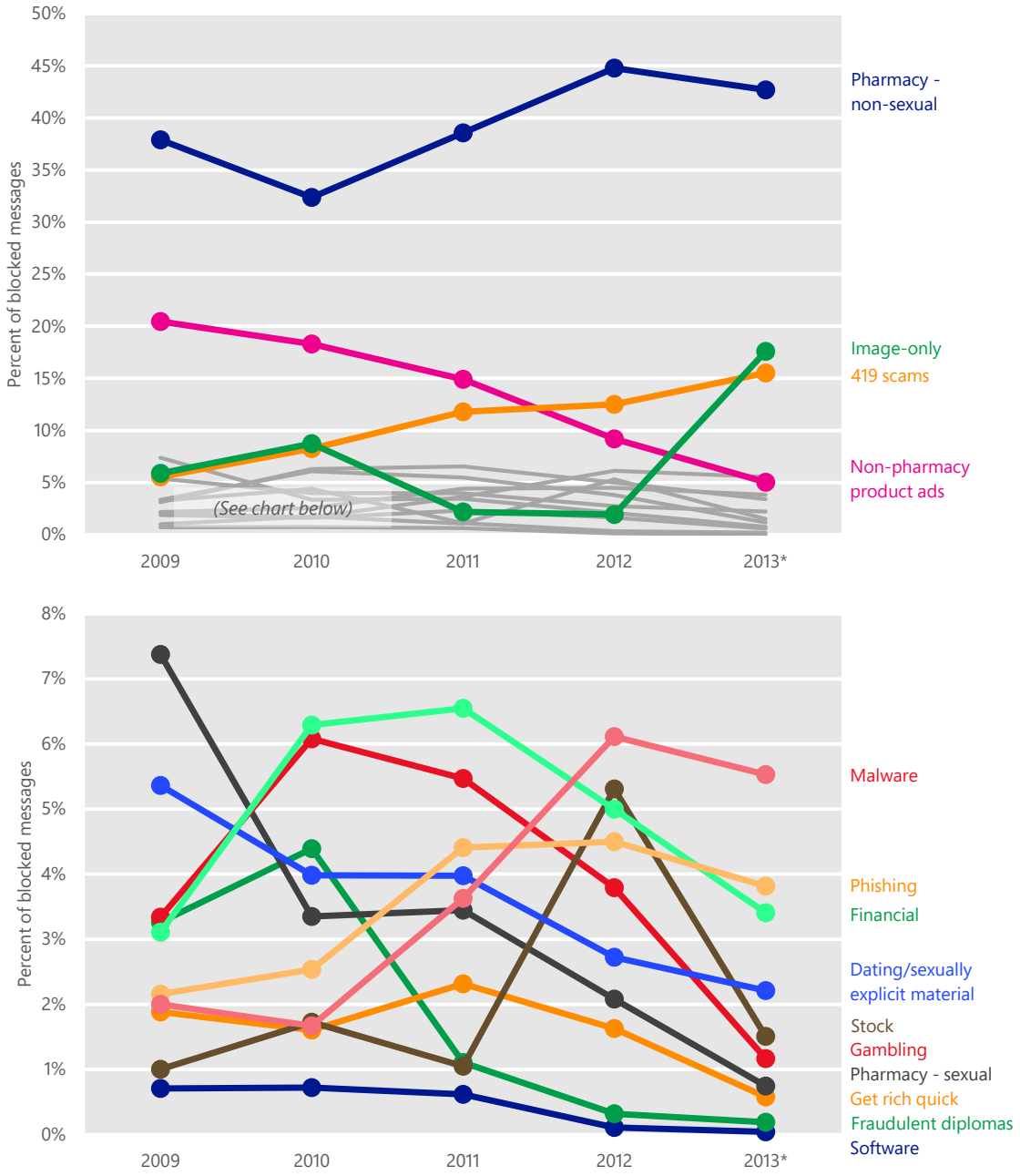
The Exchange Online Protection content filters recognize several different common types of spam messages. Figure 58 shows the relative prevalence of the spam types that were detected in 1H13.

Figure 58. Inbound messages blocked by Exchange Online Protection filters in 1H13, by category



- Advertisements for non-sexual pharmaceutical products accounted for 42.7 percent of the messages blocked by Exchange Online Protection content filters in 1H13, a slight decrease from 43.8 percent in 2H12.
- Spam messages associated with advance-fee fraud (so-called *419 scams*) accounted for 15.5 percent of messages blocked, a slight increase from 14.3 percent in 2H12. An advance-fee fraud is a common confidence trick in which the sender of a message purports to have a claim on a large sum of money but is unable to access it directly for some reason, typically involving bureaucratic red tape or political corruption. The sender asks the prospective victim for a temporary loan to be used for bribing officials or paying fees to get the full sum released. In exchange, the sender promises the target a share of the fortune, typically a much larger sum than the original loan, but does not deliver.
- Spam messages that include images and no text, which spammers sometimes send in an effort to evade detection by antispam software, increased significantly to 17.6 percent of messages blocked in 1H13, up from 1.9 percent in 2012.

Figure 59. Inbound messages blocked by Exchange Online Protection content filters, 2009–2013, by category



* First half

- Advertisements for non-sexual pharmaceutical products have accounted for the largest share of spam for the past several years, and increase from about one-third of all spam in 2010 to almost one-half in 2012 and 2013.
- Most categories of spam decreased in 1H13, with 419 scams and image-only spam being the only categories that increased as a percentage of the total.

- Non-pharmacy product ads, sexually related pharmaceutical ads, fraudulent diploma ads, gambling-related ads, and ads for sexually explicit material or dating services all continued multi-year periods of decline in 1H13.

Geographic origins of botnet spam

To measure the impact that botnets have on the spam landscape, Exchange Online Protection monitors spam messages sent from IP addresses that have been reported to be associated with known botnets and performs geographic lookups on the originating IP addresses. Determining where botnet spam is sent from can help government and industry response teams better understand the magnitude of security problems affecting different areas of the globe.

Figure 60 shows the countries/regions around the world that sent the most spam from botnets during the first half of 2013.

Figure 60. The countries and regions sending the most spam from botnets in 1H13

	Country/Region	IP addresses sending spam
1	United States	29,216
2	China	16,094
3	United Kingdom	7,728
4	India	5,779
5	Russia	5,553
6	Germany	5,044
7	Canada	4,859
8	Brazil	3,893
9	Australia	3,635
10	France	3,548

Guidance: Defending against threats in email

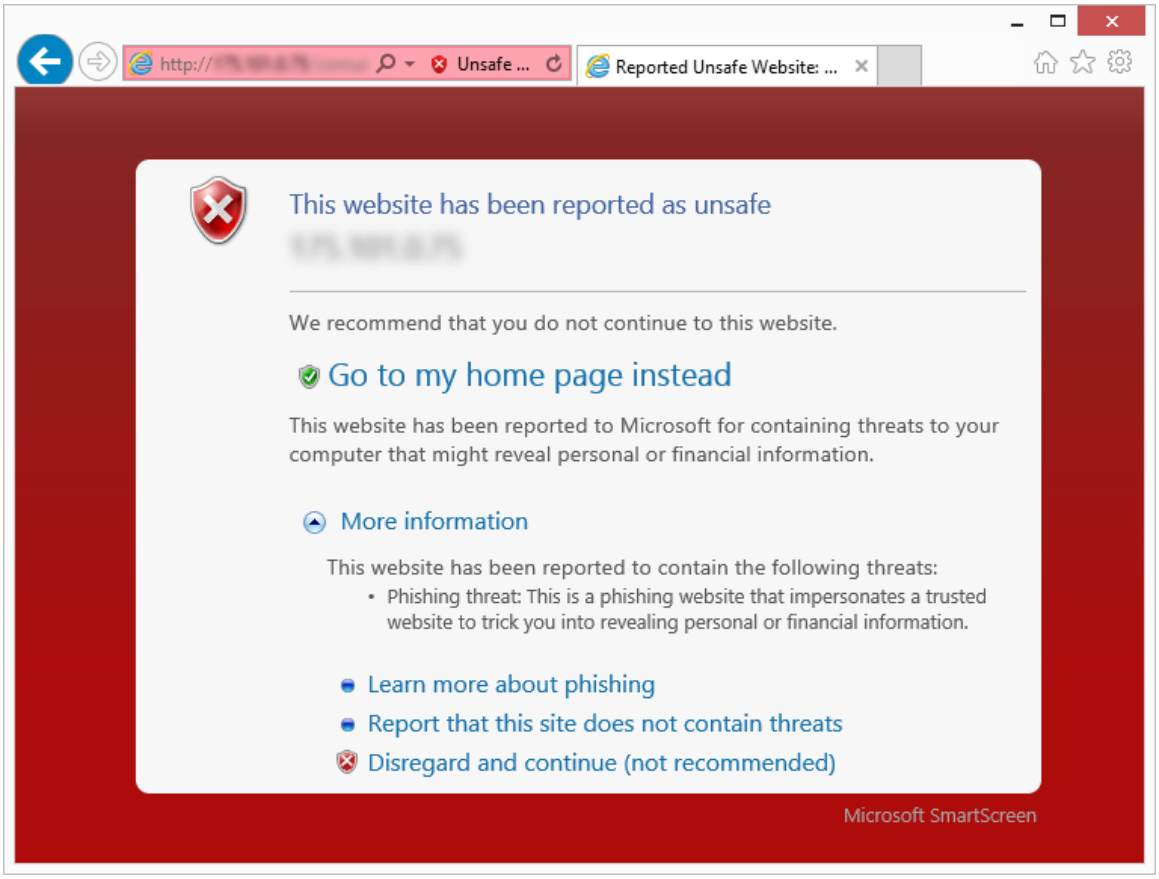
In addition to using a filtering service such as Exchange Online Protection, organizations can take a number of steps to reduce the risks and inconvenience of unwanted email. Such steps include implementing email authentication techniques and observing best practices for sending and receiving email. For in-depth guidance, see Guarding Against Email Threats in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website.

Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear to be completely legitimate, and 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 such sites. 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.

The information in this section is compiled from a variety of internal and external sources, including telemetry data produced by SmartScreen Filter (in Windows Internet Explorer versions 8 through 10) and the Phishing Filter (in Internet Explorer 7), from a database of known active phishing and malware hosting sites reported by users of Internet Explorer and other Microsoft products and services, and from malware data provided by Microsoft antimalware technologies. (See "Appendix B: Data sources" on page 125 for more information about the products and services that provided data for this report.)

Figure 61. SmartScreen Filter in Internet Explorer blocks reported phishing and malware distribution sites to protect users



Phishing sites

Microsoft gathers information about phishing sites and impressions from *phishing impressions* that are generated by users who choose to enable the Phishing Filter or SmartScreen Filter in Internet Explorer. A phishing impression is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being blocked, as illustrated in Figure 62.

Figure 62. How Microsoft tracks phishing impressions

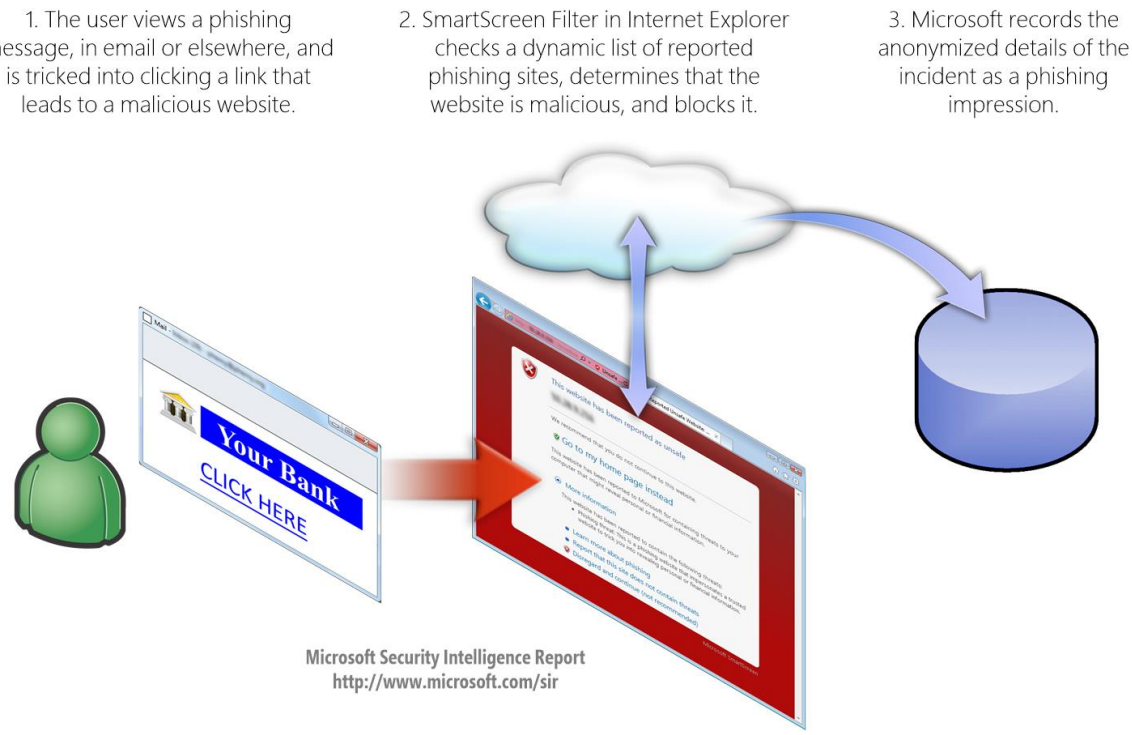
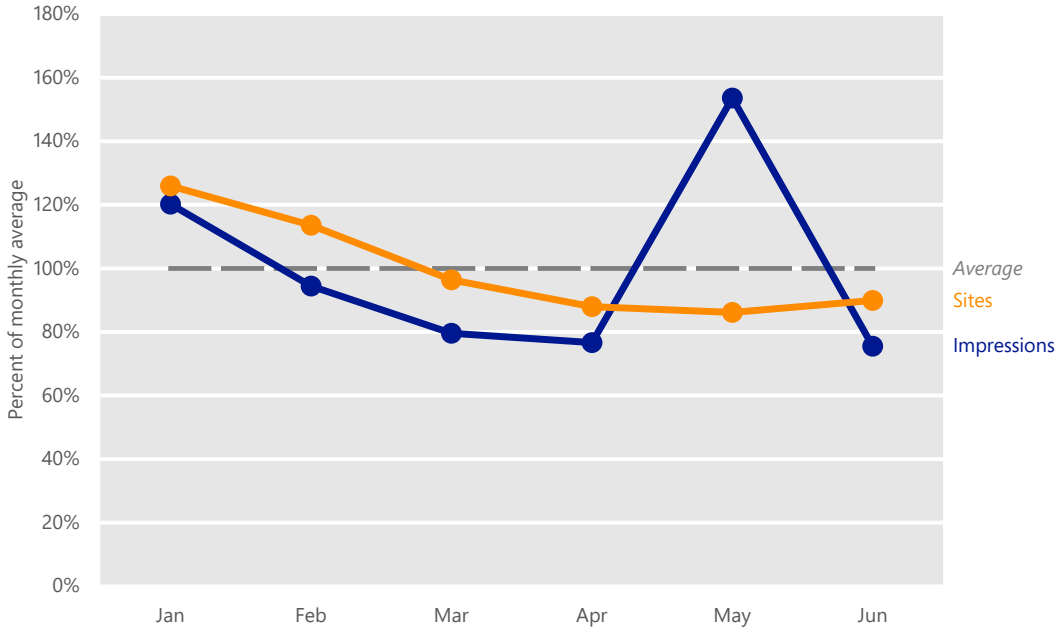


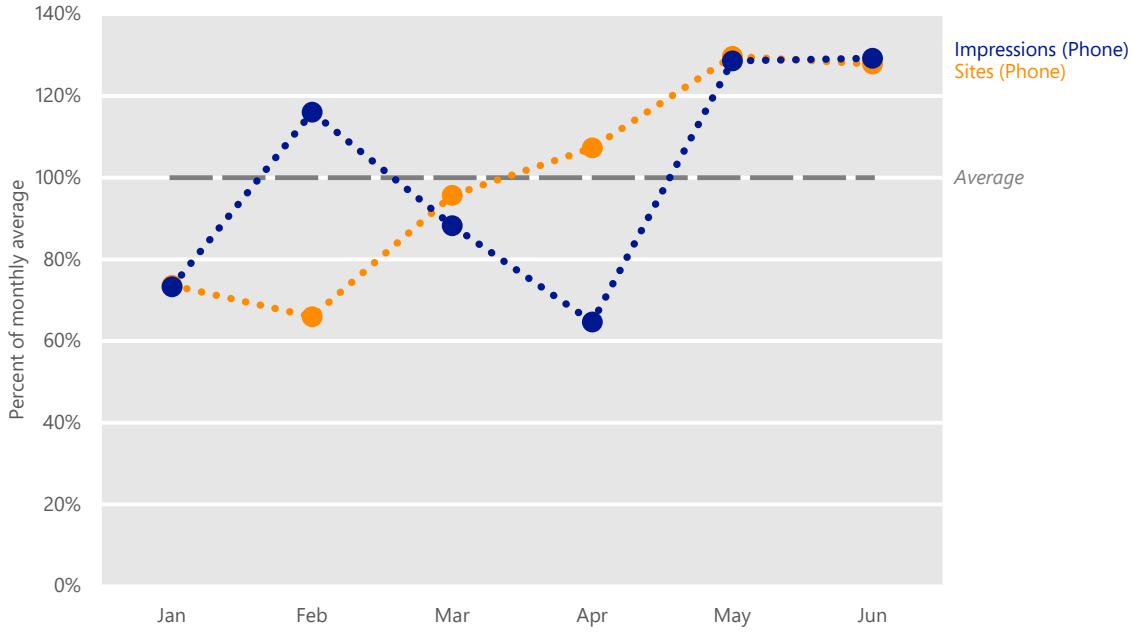
Figure 63 and Figure 64 illustrate the volume of phishing impressions tracked by SmartScreen Filter each month in 1H13 across all devices and on mobile devices running Windows Phone 8, compared to the volume of distinct phishing URLs visited.

Figure 63. Phishing sites and impressions reported by SmartScreen Filter across all devices, January–June 2013, relative to the monthly average for each



- The numbers of active phishing sites and impressions rarely correlate strongly with each other. Phishers sometimes engage in campaigns that temporarily drive more traffic to each phishing page without necessarily increasing the total number of active phishing pages they maintain at the same time. The spike in impressions across all devices in May, when impressions rose to 153.6 percent of the monthly average, is a characteristic pattern and may have been caused by one or more such campaigns. With the exception of the May spike in impressions, both sites and impressions were mostly stable throughout 1H13, with both declining gradually between January and June.

Figure 64. Phishing sites and impressions reported by SmartScreen Filter on Windows Phone 8, January–June 2013, relative to the monthly average for each



- As mobile Internet usage grows, so does the volume of phishing impressions from mobile devices. Impressions reported by Internet Explorer running on Windows Phone 8 varied significantly from month to month; the number of impressions reported in the high month of June was more than double the number reported in the low month of April.

Target institutions

Some types of sites tend to consistently draw many more impressions per site than others. The next four figures show the percentage of phishing impressions and unique phishing URLs visited each month from January to June 2013 for the most frequently targeted types of institutions.

Figure 65. Impressions across all devices for each type of phishing site, January–June 2013, as reported by SmartScreen Filter

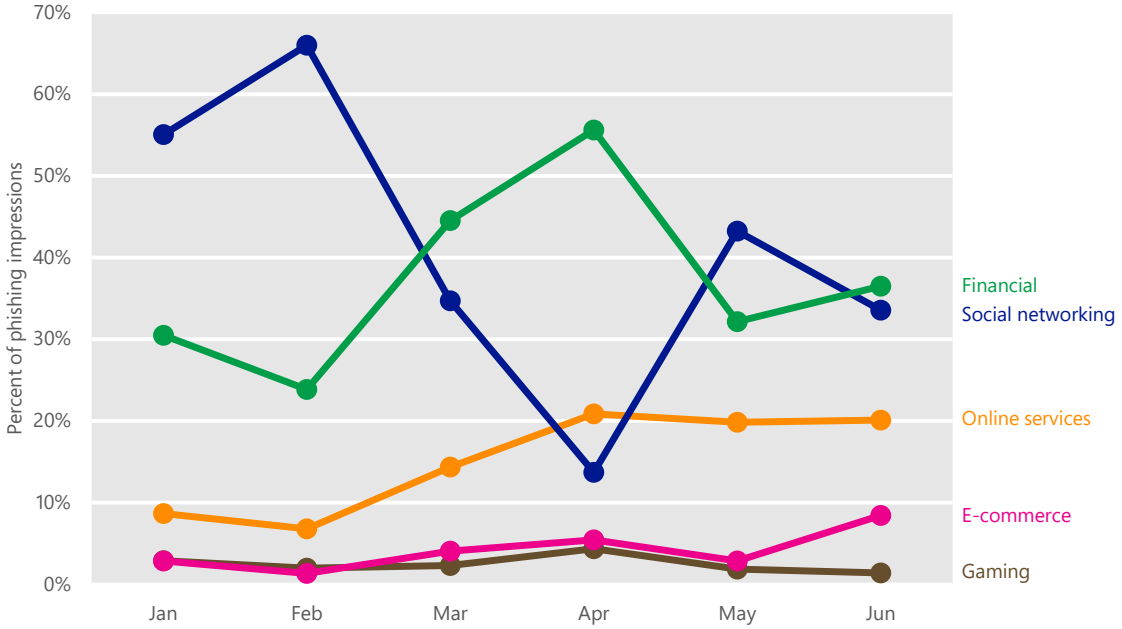
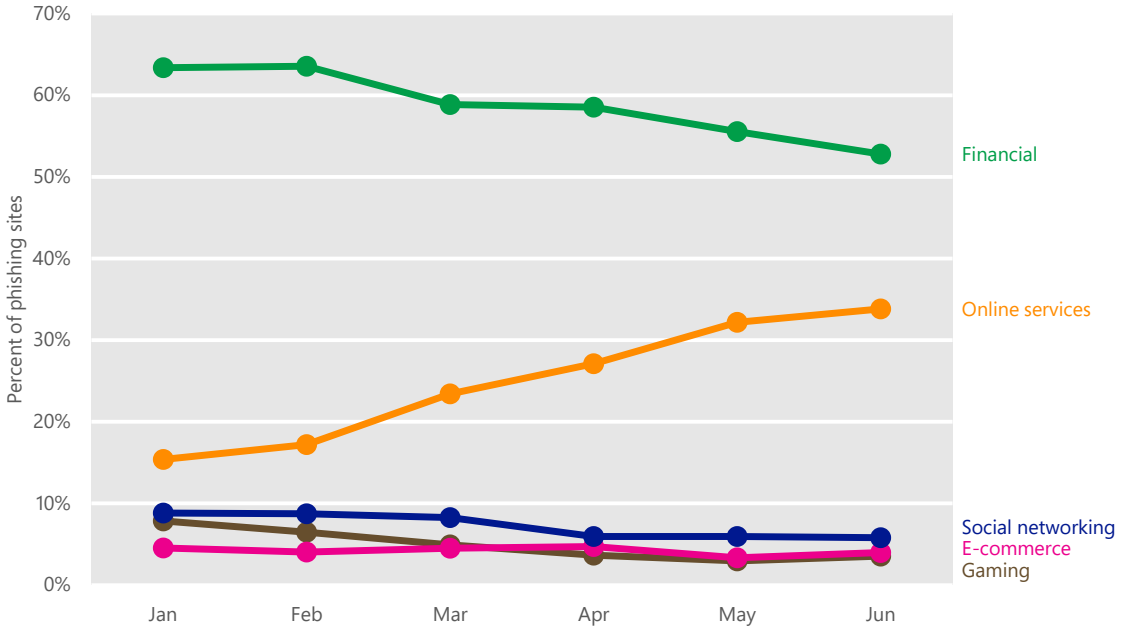


Figure 66. Unique phishing URLs visited by Internet Explorer running on all devices for each type of phishing site, January–June 2013



- Financial institutions have always been popular phishing targets because of their potential for providing direct illicit access to victims' bank accounts. Sites that targeted financial institutions accounted for the majority of active

phishing sites each month in 1H13, and were responsible for the largest or second-largest number of impressions each month.

- Phishing sites that targeted social networks received large numbers of impressions most months in 1H13, reaching a high of 66 percent of all phishing impressions in February. Despite the number of impressions, sites that targeted social networks only accounted for between 5.8 and 8.8 percent of unique phishing URLs visited each month. Most social networking activity involves a small number of very popular websites, so phishers can target large numbers of victims without having to maintain many different phishing sites. By contrast, financial activity worldwide takes place over a much larger number of sites, and attackers need to tailor their phishing sites individually to target each one.
- The number of active phishing sites that target online services increased steadily throughout 1H13, from 15.4 percent of all phishing sites in January to 33.8 percent in June. Impressions increased commensurately, from 8.7 percent of all impressions in January to 20.1 percent in June.
- The increase in the relative number of financial institution phishing impressions in March and April, along with the corresponding dip in the relative number of social network phishing impressions, suggest the existence of one or more organized phishing campaigns targeting financial institutions during those months. The same phenomenon can be observed in the phishing impression data from Windows Phone 8, as shown in Figure 67.

Figure 67. Impressions reported by SmartScreen Filter on Windows Phone 8 for each type of phishing site, January–June 2013

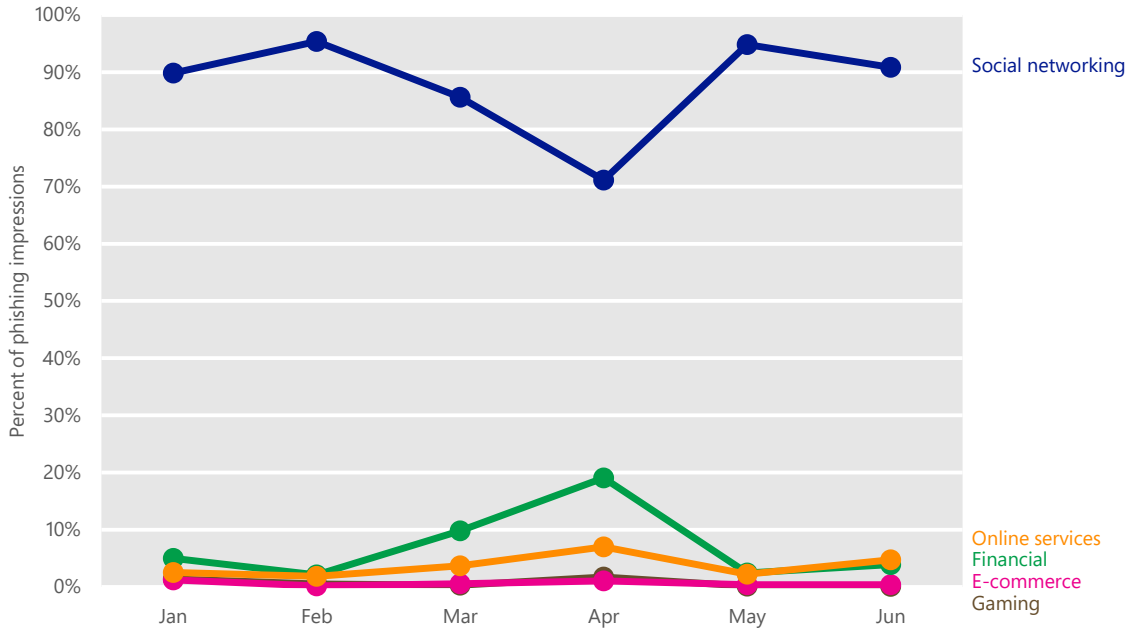
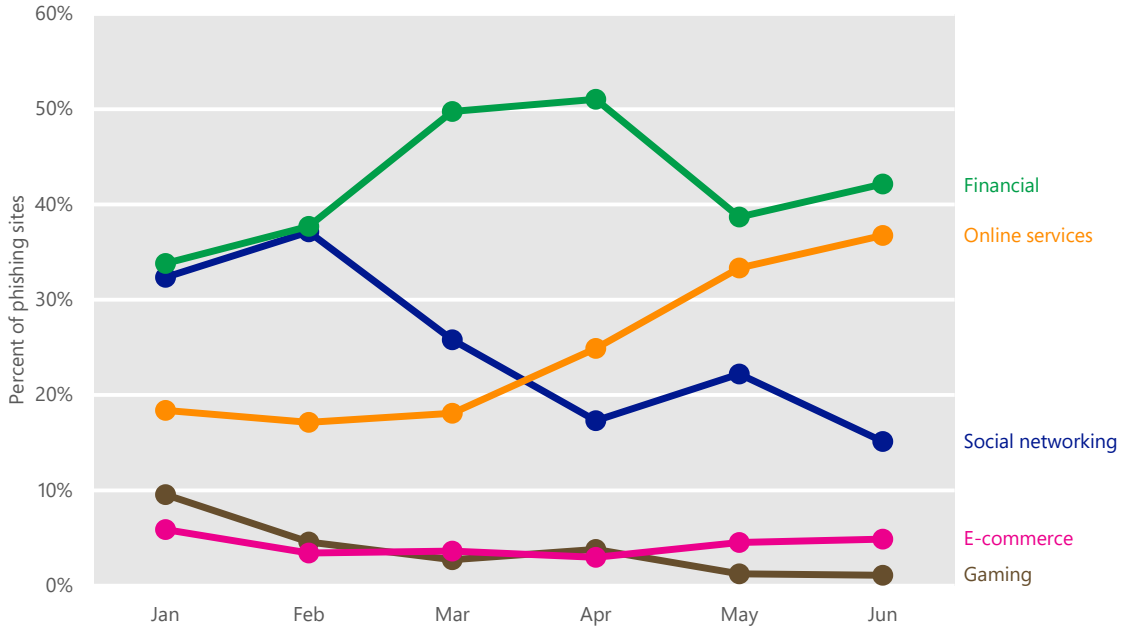


Figure 68. Unique phishing URLs visited by Internet Explorer on Windows Phone 8 for each type of phishing site, January–June 2013, by type of target



- The popularity of social networking activity on mobile platforms is reflected in the phishing impressions reported by devices running Windows Phone 8. Phishing sites that targeted social networking sites were responsible for more than three times as many mobile impressions as all other phishing

sites combined for most months in 1H13. The number of social networking impressions remained high throughout the period, even as the number of unique phishing URLs that targeted social networks declined by more than half between January and June.

- Although the volume of unique phishing URLs that targeted financial institutions visited on Windows Phone 8 was relatively high throughout the period, total impressions for financial phishing pages was low.
- The increase in phishing URLs that targeted online services seen in Figure 66 was also apparent among Windows Phone 8 users specifically, although total impressions on Windows Phone 8 did not increase significantly throughout the period.

Global distribution of phishing sites

Phishing sites are hosted all over the world on free hosting sites, on compromised web servers, and in numerous other contexts. Performing geographic lookups of IP addresses in the database of reported phishing sites makes it possible to create maps that show the geographic distribution of sites and to analyze patterns.

Figure 69. Phishing sites per 1,000 Internet hosts for locations around the world in 1Q13 (top) and 2Q13 (bottom)

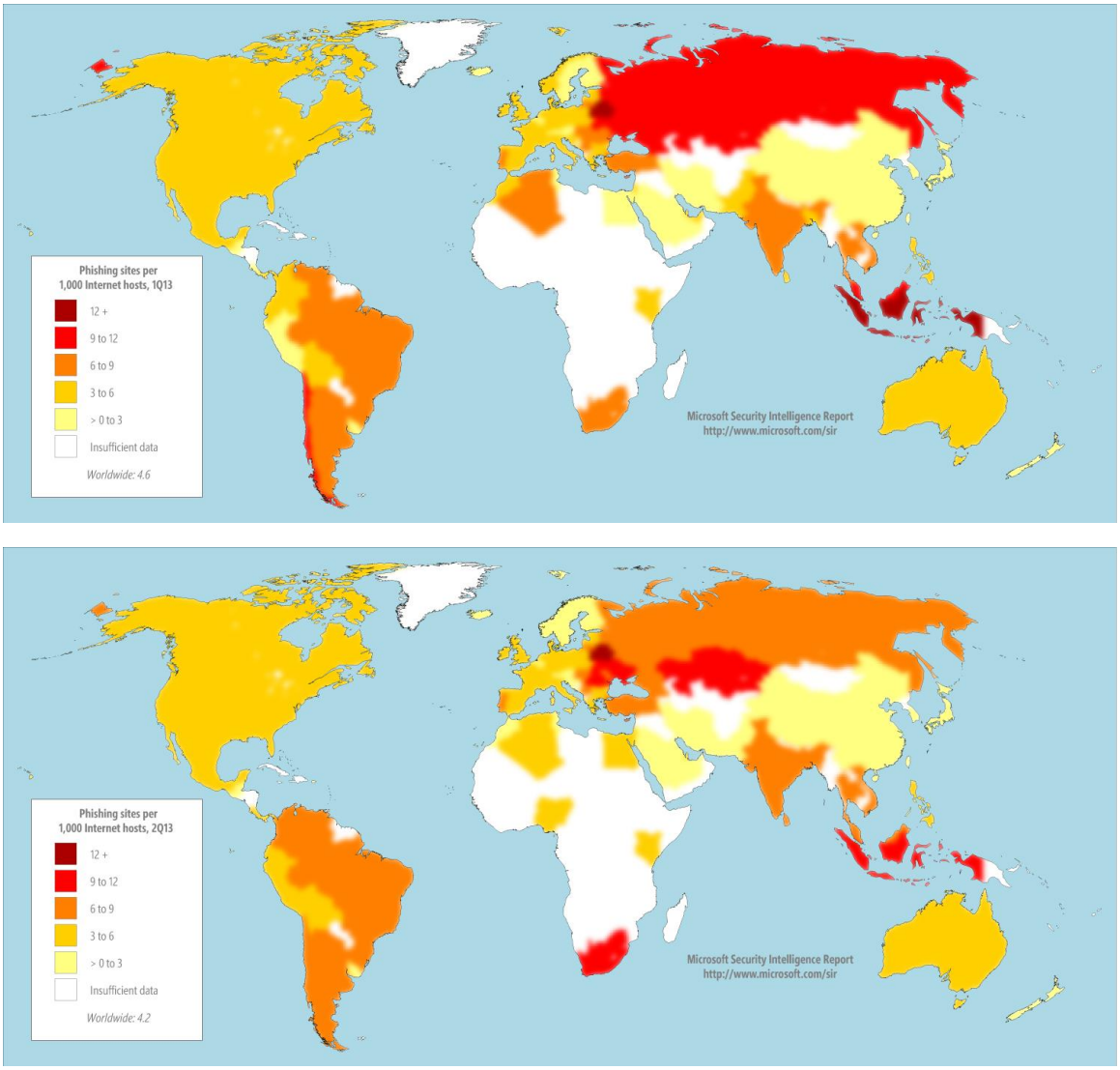
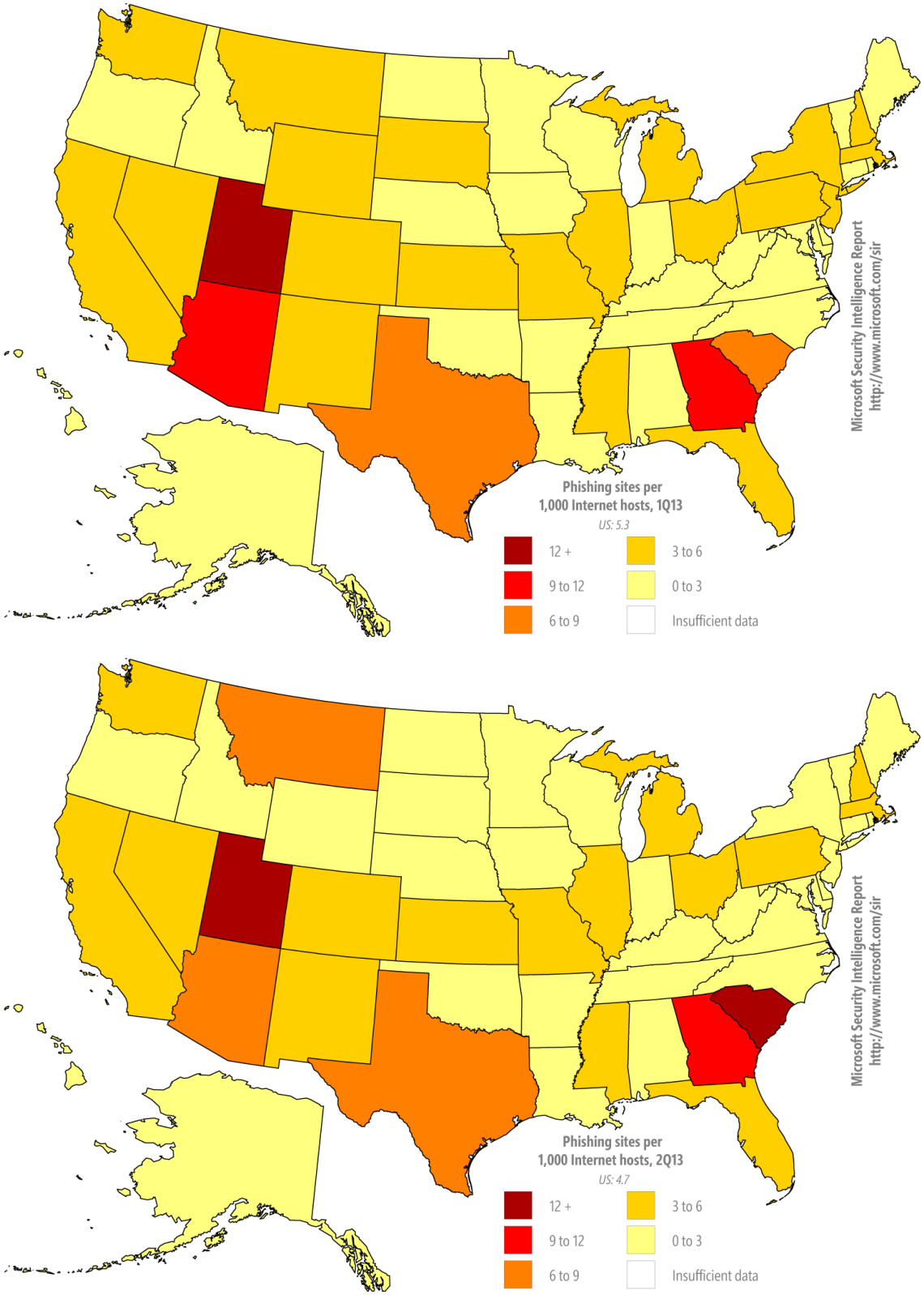


Figure 70. Phishing sites per 1,000 Internet hosts for US states in 1Q13 (top) and 2Q13 (bottom)



- SmartScreen Filter detected 4.6 phishing sites per 1,000 Internet hosts worldwide in 1Q13, and 4.2 per 1,000 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).
- Those US states with the highest concentrations of phishing sites include Utah (13.4 per 1,000 Internet hosts in 4Q12), Georgia (10.0), and Arizona (7.7). States with low concentrations of phishing sites include West Virginia (0.4), Minnesota (0.9), and North Dakota (1.0).

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 71. SmartScreen Filter in Internet Explorer displays a warning when a user attempts to download an unsafe file

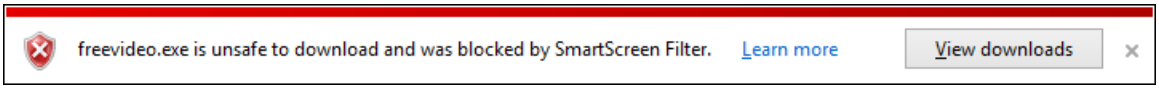
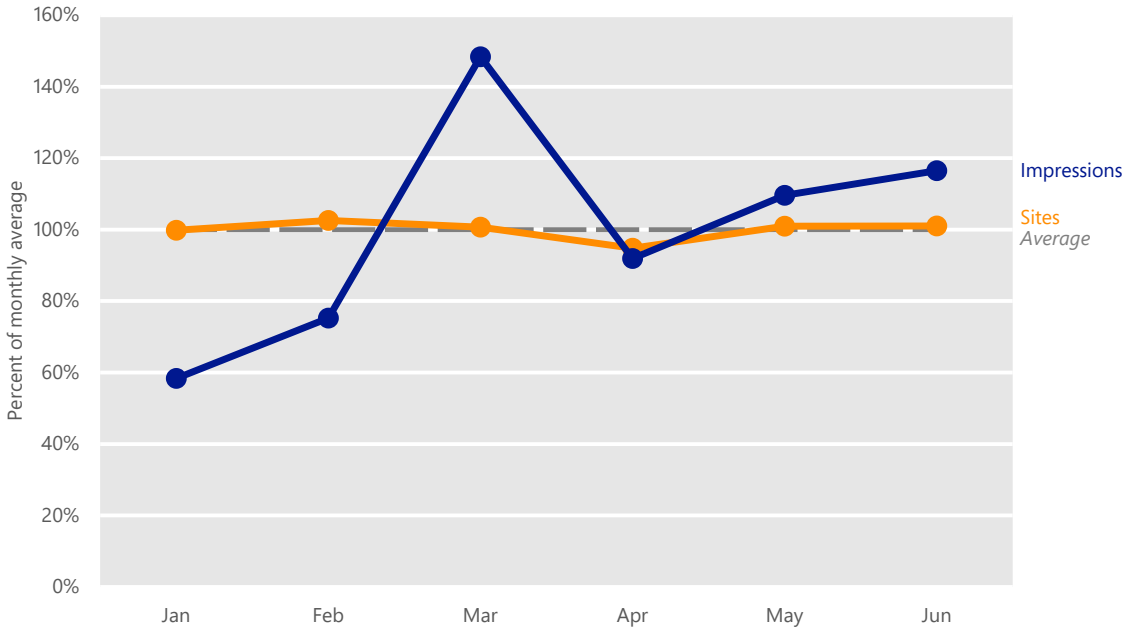


Figure 72 compares the volume of active malware hosting sites in the Microsoft database each month with the volume of malware impressions tracked by Internet Explorer.

Figure 72. Malware hosting sites and impressions tracked each month in 1H13, relative to the monthly average for each



- Although the number of active malware hosting sites remained very consistent each month in 1H13, impressions nearly doubled in March before returning to a more typical level in April. This increase suggests the possible existence of one or more short-term campaigns in March.

Malware categories

Figure 73 and Figure 74 show the types of threats hosted at URLs that were blocked by SmartScreen Filter in 1Q13.

Figure 73. Categories of malware found at sites blocked by SmartScreen Filter in 1H13, by percent of all malware impressions

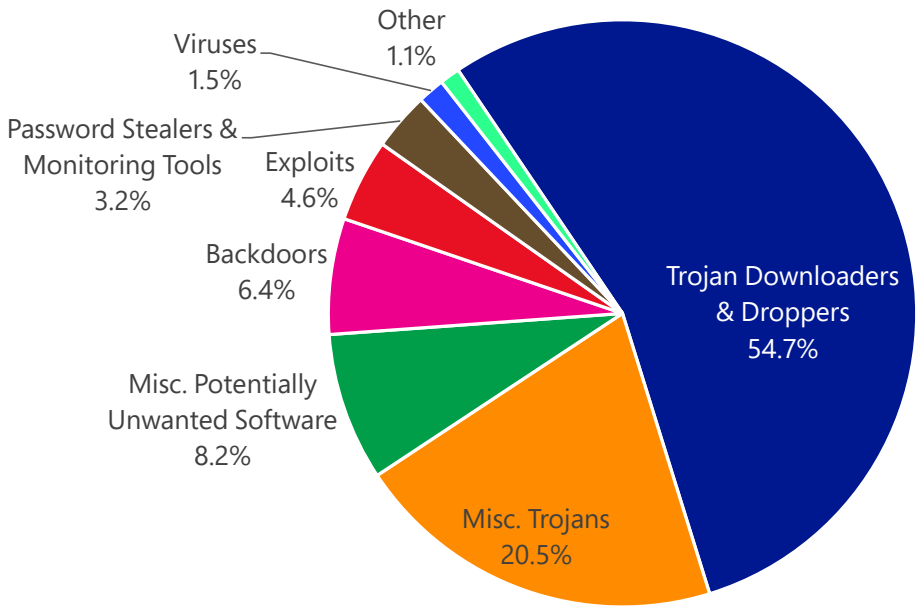


Figure 74. Top families found at sites blocked by SmartScreen Filter in 1H13, by percent of all malware impressions

	Family	Most significant category	Percent of malware impressions
1	Win32/Delf	Trojan Downloaders & Droppers	20.4%
2	Win32/Microjoin	Trojan Downloaders & Droppers	11.0%
3	Win32/Swisyn	Trojan Downloaders & Droppers	8.3%
4	Win32/Bdaejec	Backdoors	4.6%
5	Win32/Orsam	Miscellaneous Trojans	3.9%
6	Win32/Rongvhin	Miscellaneous Trojans	2.2%
7	Win32/Kraddare	Trojan Downloaders & Droppers	2.1%
8	Win32/Obfuscator	Miscellaneous Potentially Unwanted Software	2.1%
9	MSIL/Truado	Trojan Downloaders & Droppers	1.8%
10	AndroidOS/CVE-2011-1823	Exploits	1.8%
11	Win32/Dynamer	Miscellaneous Trojans	1.6%
12	Win32/DelfInject	Miscellaneous Potentially Unwanted Software	1.4%
13	Unix/Lotoor	Exploits	1.4%
14	Win32/Vundo	Miscellaneous Trojans	1.2%
15	Win32/Yakdowpe	Trojan Downloaders & Droppers	1.0%

- Many of the families on the list are generic detections for a variety of threats that share certain identifiable characteristics.
- Win32/Delf, the family responsible for the most malware impressions in 1H13, is a generic detection for various threats written in the Delphi programming language. It was not among the top 15 families found at sites blocked by SmartScreen Filter in 2H12.
- Win32/Microjoin, in second place, is a generic detection for tools that bundle malware files with clean files in an effort to deploy malware without being detected by security software. Sites that hosted Microjoin accounted for 11.0 percent of malware impressions in 1H13, an increase from 7.1 percent in 2H12.
- Win32/Swisyn, the family responsible for the most malware impressions in 2H12, dropped to third in 1H13. Swisyn is a family of trojans that drops and executes malware on infected computers. These files may be embedded as resource files, and are often bundled with legitimate files in an effort to evade detection. Sites that hosted Swisyn accounted for 8.3 percent of malware impressions in 1H13, a decrease from 20.8 percent in 2H12.
- Two threats that target the Android operating system were among the top 15 families found at sites blocked by SmartScreen Filter in 1H13. AndroidOS/CVE-2011-1823 and Unix/Lotoor are both detections for exploits that target vulnerabilities in the operating system in an attempt to gain root privilege. See "Operating system exploits" on page 39 for more information about these threats.

Global distribution of malware hosting sites

As with phishing sites, Figure 75 and Figure 76 show the geographic distribution of malware hosting sites reported to Microsoft in 1H13.

Figure 75. Malware distribution sites per 1,000 Internet hosts for locations around the world in 1Q13 (top) and 2Q13 (bottom)

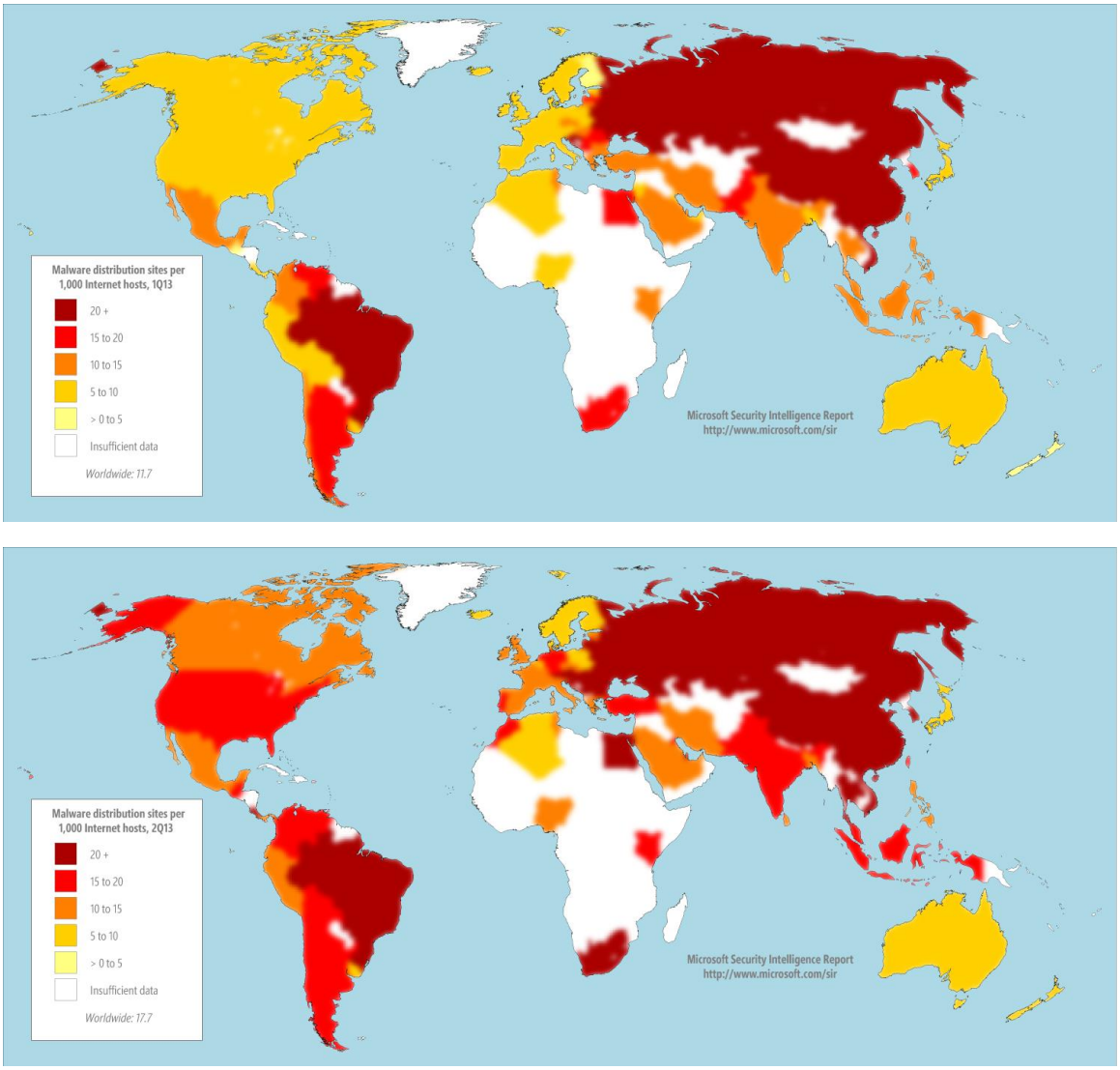
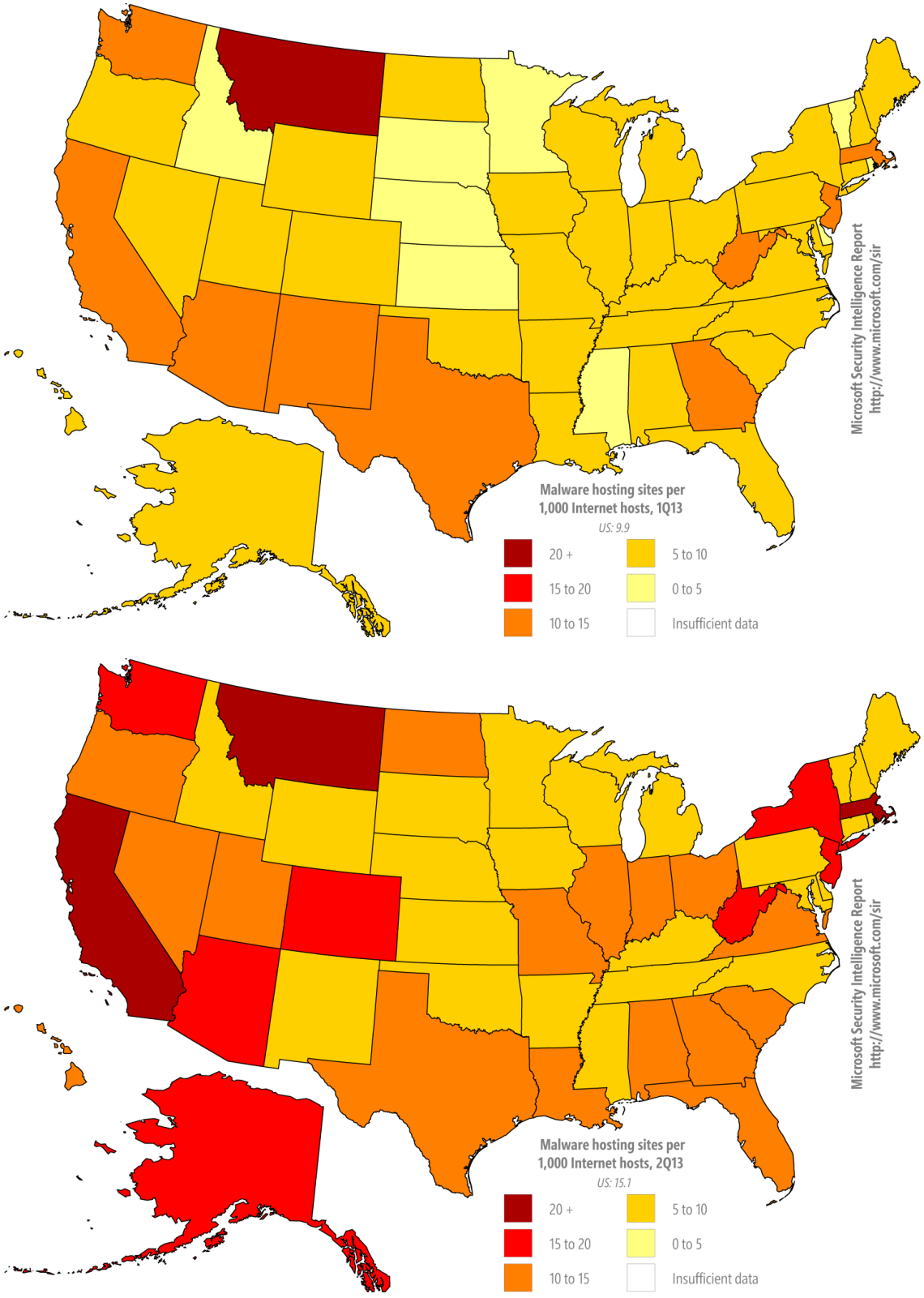


Figure 76. Malware distribution sites per 1,000 Internet hosts for US states in 1Q13 (top) and 2Q13 (bottom)



- 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).
- US states with high concentrations of malware hosting sites include Montana (40.9 per 1000 Internet hosts in 2Q13), Massachusetts (22.2), and California (2.13). States with low concentrations of malware hosting sites include Vermont (5.5), Idaho (5.7), and Kansas (6.2).

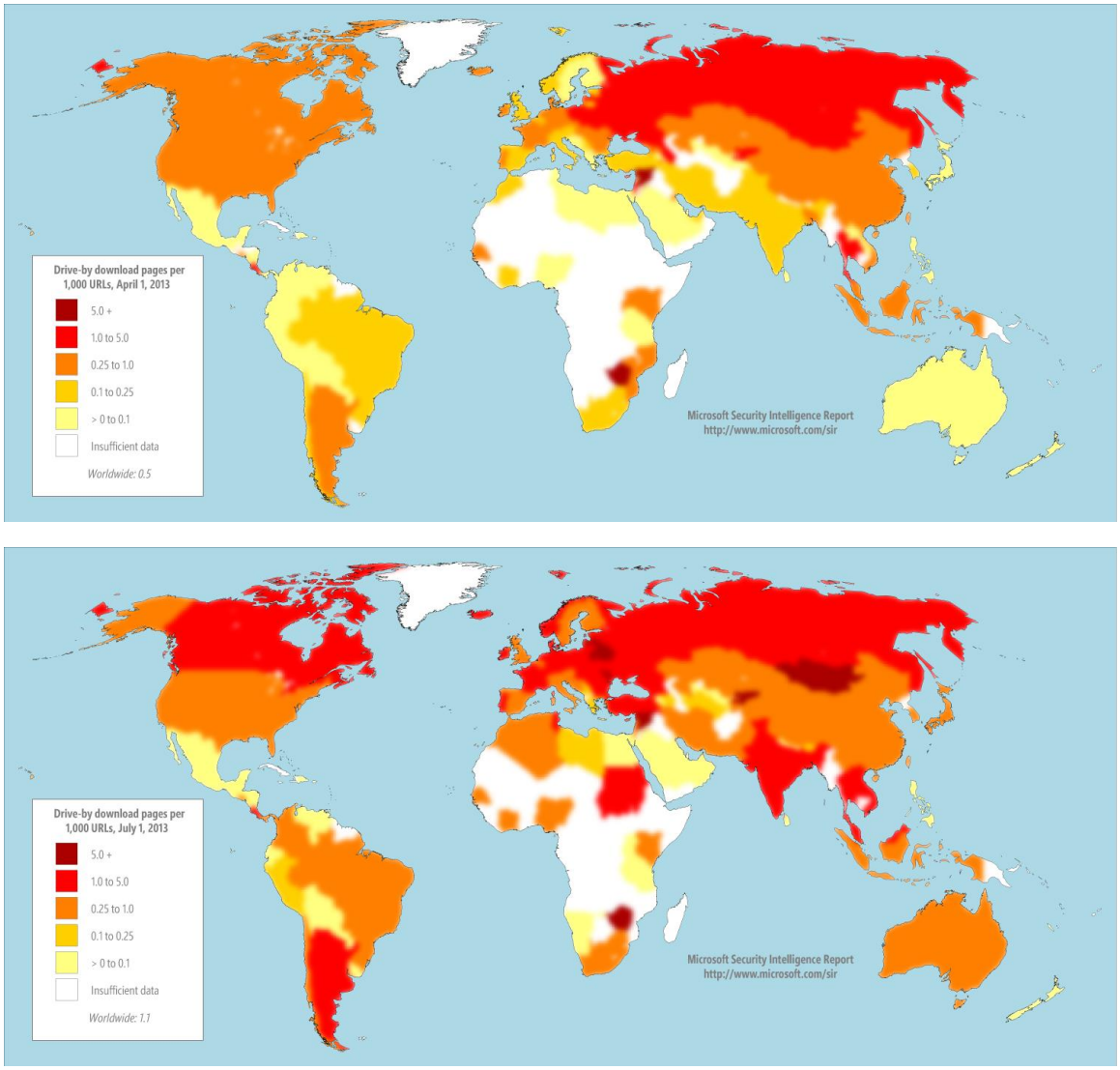
Drive-by download sites

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.

Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. Bing analyzes websites for exploits as they are indexed and displays warning messages when listings for drive-by download pages appear in the list of search results. (See Drive-By Download Sites at the *Microsoft Security Intelligence Report* website for more information about how drive-by downloads work and the steps Bing takes to protect users from them.)

Figure 77 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 1Q13 and 2Q13, respectively.

Figure 77. Drive-by download pages indexed by Bing at the end of 1Q13 (top) and 2Q13 (bottom), per 1000 URLs in each country/region

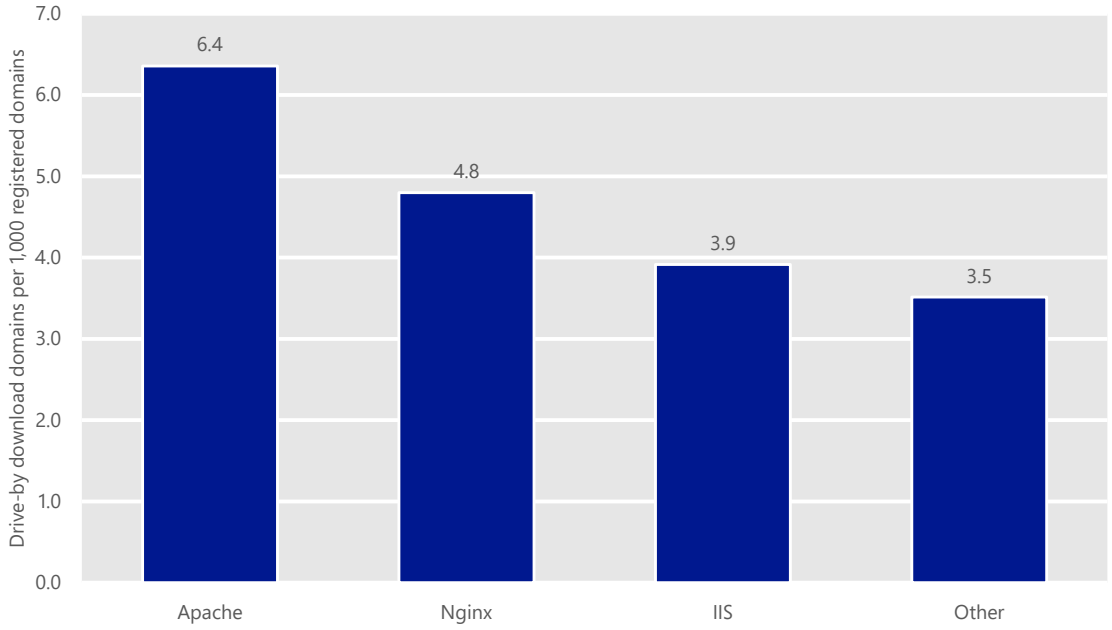


- Each map shows the concentration of drive-by download URLs tracked by Bing in each country or region on a reference date at the end of the associated quarter, expressed as the number of drive-by download URLs per every 1,000 URLs hosted in the country/region.
- Significant locations with high concentrations of drive-by download URLs in both quarters include Syria, with 9.5 drive-by URLs for every 1,000 URLs tracked by Bing at the end of 2Q13; Latvia, with 6.6; and Belarus, with 5.6.

Some web server software platforms are more likely to host drive-by download sites than others because of a number of factors, such as the prevalence of

exploit kits targeting specific platforms. Figure 78 shows the relative prevalence of drive-by download sites on different web server platforms.

Figure 78. Drive-by download hosts per 1,000 registered domains at the end of 1H13, by web server platform



- Figure 78 is normalized: for each server platform, it shows the number of registered domains hosting drive-by download sites on the platform for every 1,000 registered domains running that platform. "Registered domains" are either second- or third-level domains, depending on the rules of the TLD (for example, microsoft.com or microsoft.co.uk). If a registered domain has any subdomains, such as www, they are all considered together.
- Websites that run the open-source Apache HTTP Server displayed the highest rate of drive-by download incidence, with 6.4 registered domains hosting drive-by download sites per 1,000 registered domains running Apache web servers. The prevalence of drive-by download sites on the Apache platform may be related to the spread of the "Darkleech" exploit kit, discovered in April 2013, which targets the Apache HTTP Server. See page 35 for more information about the Darkleech kit.
- The open-source Nginx web server displayed the second highest rate of drive-by download incidence (4.8 per 1,000 registered domains), followed by Microsoft Internet Information Services (IIS) for Windows Server (3.9 per 1,000 registered domains). All other web server platforms, each of which were used by less than 1 percent of registered domains worldwide,

collectively displayed a drive-by download incidence rate of 3.5 per 1,000 registered domains.

Guidance: Protecting users from unsafe websites

One of the best ways organizations can protect their users from malicious and compromised websites is by mandating the use of web browsers with appropriate protection features built in and by promoting safe browsing practices. For in-depth guidance, see the following resources in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website:

- Promoting Safe Browsing
- Protecting Your People

Mitigating risk

Malware at Microsoft: Dealing with threats in the Microsoft environment

Microsoft IT

Microsoft IT provides information technology services internally for Microsoft employees and resources. Microsoft IT manages 600,000 devices for 180,000 users across more than 100 countries and regions worldwide, with approximately 2 million remote connections per month. Safeguarding a computing infrastructure of this size requires implementation of strong security policies, technology to help keep malware off the network and away from mission-critical resources, and dealing with malware outbreaks swiftly and comprehensively when they occur.

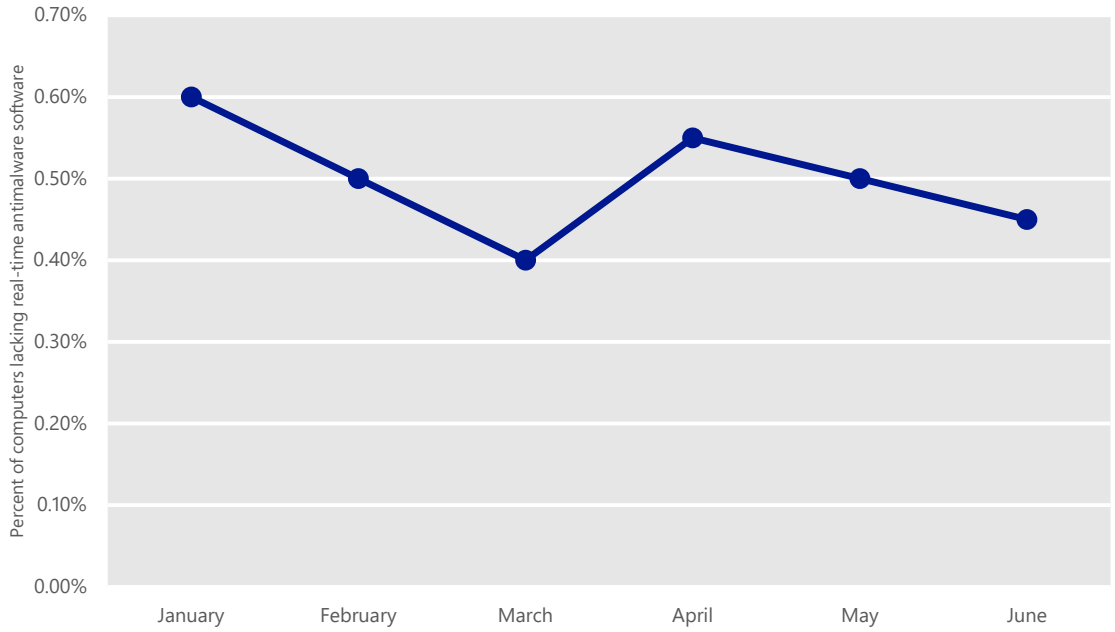
This section of the report compares the potential impact of malware to the levels of antimalware compliance from approximately 350,000 workstation computers managed by Microsoft IT between January and June 2013. This data is compiled from multiple sources, including System Center Endpoint Protection, Network Access Protection, DirectAccess, and manual submission of suspicious files. Comparing the nature and volume of the malware detected on these computers to the level of protection they receive can illustrate significant trends and give insights as to the effectiveness of antimalware software and security best practices.

Antimalware usage

Real-time antimalware software is required on all user devices that connect to the Microsoft corporate network. Microsoft's supported antimalware solution for users is System Center Endpoint Protection 2012 (SCEP). To be considered compliant with antimalware policies and standards, user computers must be running the latest version of the SCEP client, antimalware signatures must be no more than six days old, and real-time protection must be enabled.

Figure 79 shows the level of antimalware noncompliance in the Microsoft user workstation environment for each month in 1H13.

Figure 79. Percent of computers at Microsoft not running real-time antimalware software in 1H13

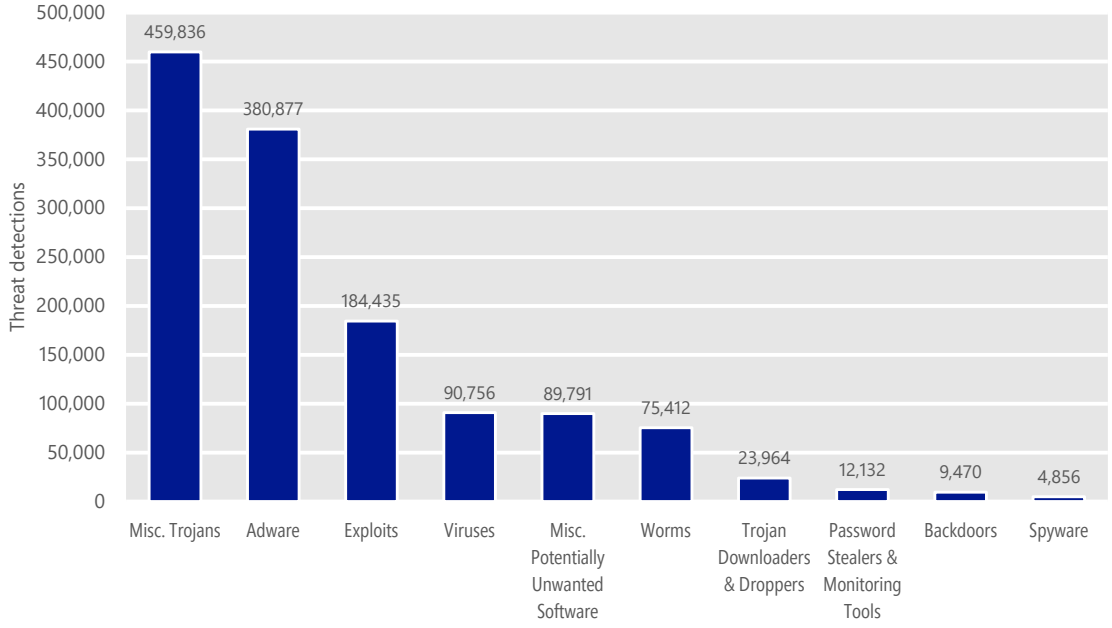


At an average of 99.5 percent compliance during the six-month period, the antimalware compliance rate at Microsoft is very high. In any network of this size, it is almost inevitable that a small number of computers will be in a noncompliant state at any given time. In most cases, these are computers that are being rebuilt or are otherwise in a state of change when online, rather than computers that have had their antimalware software intentionally disabled. Microsoft IT believes that a compliance rate in excess of 99 percent among 350,000 computers is an acceptable level of compliance. In most cases, attempting to boost a large organization's compliance rate the rest of the way to 100 percent will likely be a costly endeavor, and the end result—100 percent compliance—will be unsustainable for any length of time.

Malware and potentially unwanted software detections

Figure 80 shows detections of categories of malware and potentially unwanted software at Microsoft in 1H13.

Figure 80. Malware and potentially unwanted software detected by System Center Endpoint Protection at Microsoft in 1H13, by category

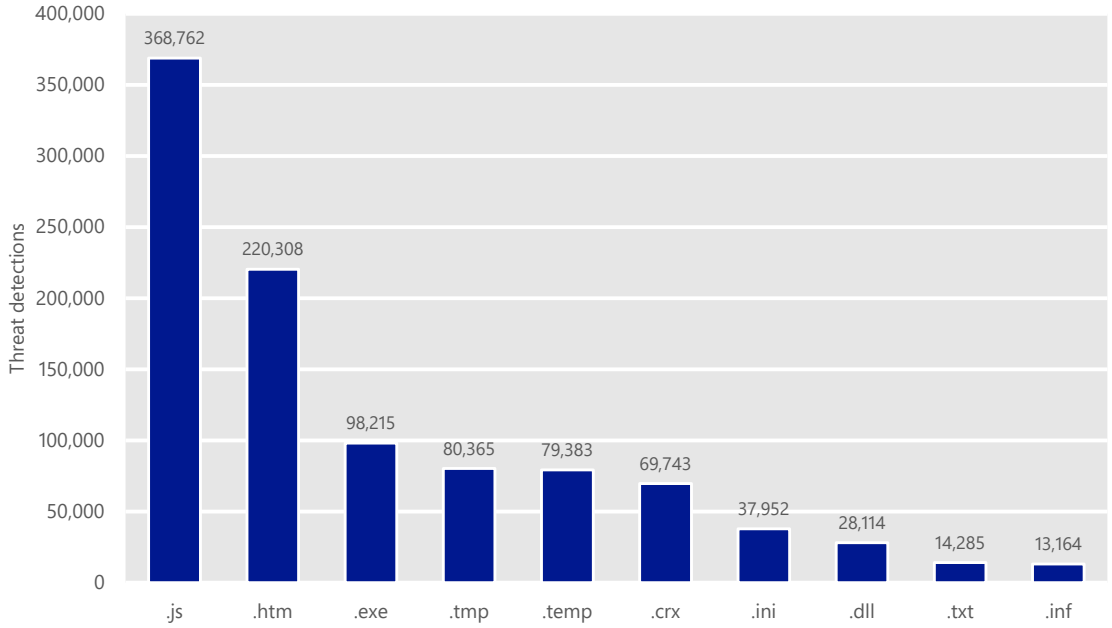


In this section, malware detections are defined as files and processes flagged by System Center Endpoint Protection, regardless of the success or failure of automated containment or remediation. Malware detections are a measure of attempted malware activity, and do not necessarily indicate that a computer has been successfully infected. (Note that the methodology for assessing encounters used elsewhere in this report counts unique computers with detections, an approach that differs from the methodology used here in which individual detections are counted. For example, if a computer encountered one malware family in April and another one in June, it would only be counted once for the purposes of figures such as Figure 26 on page 46. In the preceding Figure 80, it would be counted twice, once for each detection.)

Miscellaneous Trojans was the most prevalent category, with Adware in second, followed by Exploits and Viruses. Overall, the threat mixture seen at Microsoft is similar to the threat mixture encountered worldwide, as explored in the "Malware" section beginning on page 45.

Figure 81 shows the top 10 file types among threat detections at Microsoft in 1H13.

Figure 81. Threat detections at Microsoft in 1H13, by file type



Because web browsing was the most frequently used transmission vector for infection attempts at Microsoft in 1H13 (see Figure 82), the prevalence of HTML (.htm) and JavaScript (.js) files among threat detections is unsurprising. Malicious program files (.exe) and malware disguised as temporary files (.tmp, .temp) were also detected relatively frequently.

Transmission vectors

Examining the processes targeted by malware can help illustrate the methods that attackers use to propagate it. Figure 82 lists the top 5 transmission vectors used by the malware encountered at Microsoft in 1H13.

Figure 82. The top 5 transmission vectors used by malware encountered at Microsoft in 1H13

Rank	Description
1	Web browsing
2	File transfer applications
3	File transfers in the operating system
4	Email
5	Non-Microsoft software

As noted earlier, web browsing was the transmission vector most commonly used by infection attempts detected on Microsoft computers in 1H13.

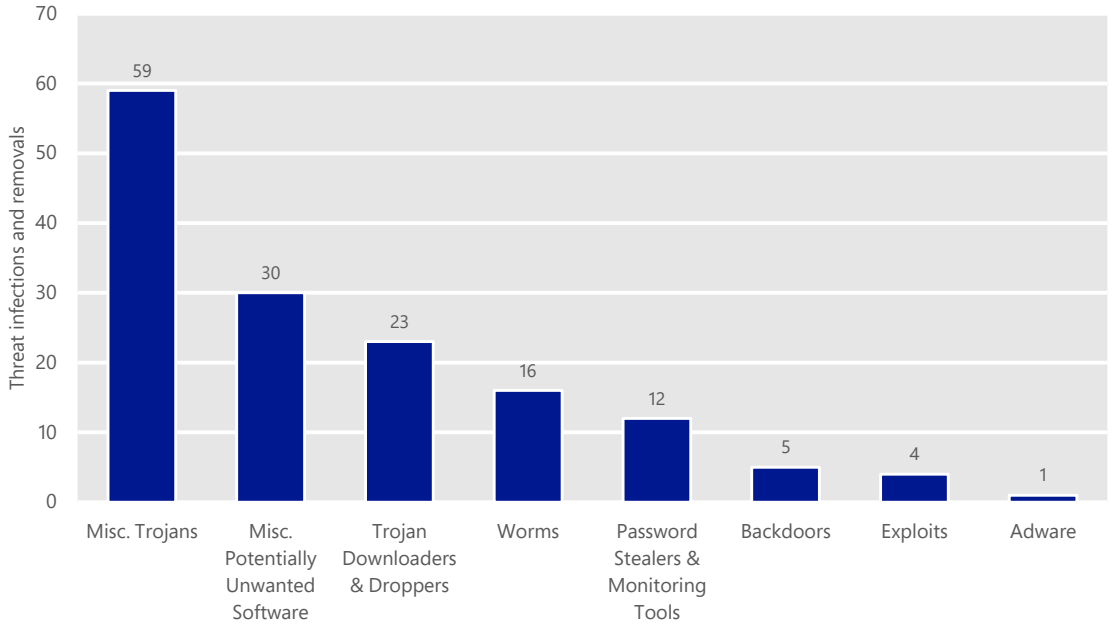
(*Transmission vector* means the method by which the malware was delivered to the local computer—a web browser in this particular discussion, probably when the user visited a malicious or compromised webpage or attempted to download a malicious file. It does not necessarily mean that the malware targeted the web browser for infection.) File transfer applications, such as Microsoft SkyDrive, Microsoft SharePoint, and peer-to-peer (P2P) applications were the second most commonly used transmission vector after web browsing. File transfers that use the operating system—Windows Explorer, in other words—were in third. Email, a popular transmission vector for attackers for many years, was fourth, followed by non-Microsoft software.

Malware and potentially unwanted software infections

Because almost all of the computers at Microsoft run real-time security software at all times, most infection attempts are detected and blocked before they are able to infect the target computer. When SCEP does disinfect a computer, it is usually because its signature database has been updated to enable it to detect a threat that it did not recognize when the computer first encountered the threat. This lack of recognition may be because the threat is a new malware family, a new variant of a known family, a known variant that has been encrypted or otherwise repackaged to avoid detection, or because of some other reason. The MMPC constantly analyzes malware samples submitted to it, develops appropriate detection signatures, and deploys them to customers who use SCEP, Microsoft Security Essentials, and Windows Defender.

Figure 83 summarizes the threats that SCEP detected on and removed from computers at Microsoft between January and June of 2013.

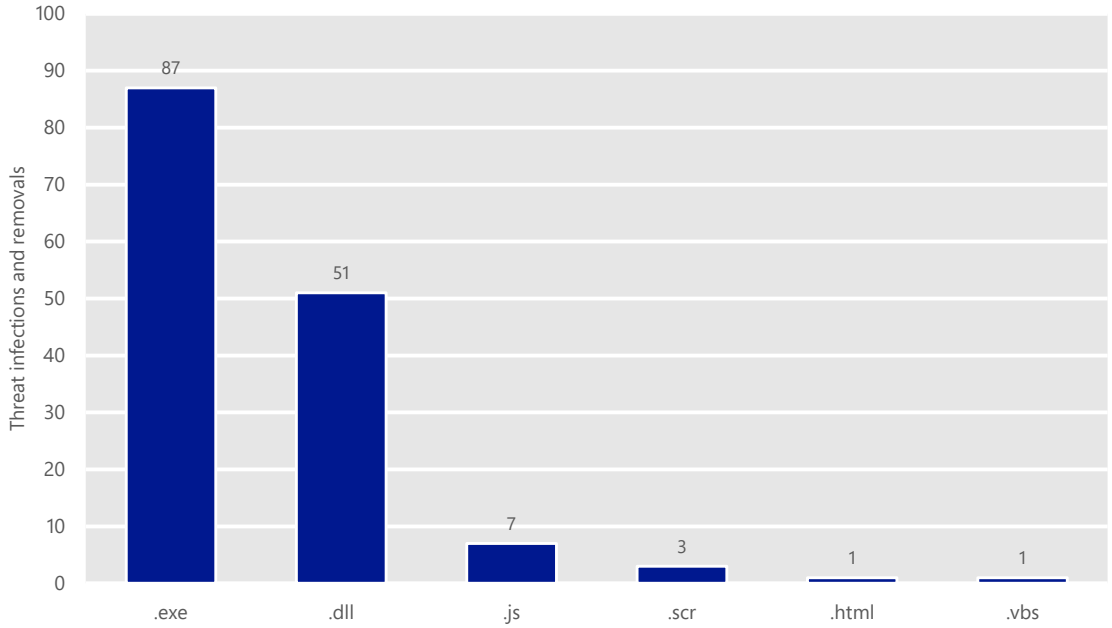
Figure 83. Computers at Microsoft cleaned of malware and potentially unwanted software in 1H13, by category



As with detections, Miscellaneous Trojans was the most common threat category to infect computers at Microsoft in 1H13, but the rest of the list shows significant differences. Adware, which was responsible for the second highest number of detections, actually resulted in the smallest number of infections, with adware being cleaned from only one computer companywide during the first half of 2013. Meanwhile, Trojan Downloaders & Droppers, which was one of the less frequently detected threat categories during the period, was responsible for the third largest number of detections.

Figure 84 shows the top 10 file types used by malware to infect computers at Microsoft in 1H13.

Figure 84. Infections and removals at Microsoft in 1H13, by file type



Of the four malware charts presented in this section, Figure 84 is potentially the most important because it provides information about threats that SCEP could not detect when they were first encountered—and therefore provides a clue about the areas in which malware authors have been focusing their efforts in recent months. The .exe extension, which denotes executable program files, was the most commonly used file type among successful infections, followed by .dll, which denotes dynamic-link library files. Malicious HTML and JavaScript files, despite their popularity among infection attempts as shown in Figure 81, were only responsible for a small number of actual infections.

What IT departments can do to minimize these trends

- Evaluate management tools available on the market to develop a plan and implement a third-party update mechanism to disseminate non-Microsoft updates.
- Ensure that all software deployed on computers in the environment is updated regularly. If the software provider offers an automatic update utility such as Microsoft Update, ensure that it is enabled by default. See "Turn automatic updating on or off" on windows.microsoft.com for instructions on enabling automatic updates of Microsoft software.

- Ensure that SmartScreen Filter is enabled in Internet Explorer. See "SmartScreen Filter: frequently asked questions" on windows.microsoft.com for more information.
- Use Group Policy to enforce configurations for Windows Update and SmartScreen Filter. See Knowledge Base article KB328010 on support.microsoft.com and "SmartScreen Filter and Resulting Internet Communication in Windows 8 and Windows Server 2012" on technet.microsoft.com for instructions.
- Set the default configuration for antimalware to enable real-time protection across all drives, including removable devices.
- Move to a 64-bit hardware architecture.
- Identify business dependencies on Java and develop a plan to minimize its use where not needed.
- Use AppLocker to block installation and use of potentially unwanted software such as Java or peer-to-peer (P2P) applications. See "AppLocker: Frequently Asked Questions" on technet.microsoft.com for more information.
- Implement the Enhanced Mitigation Experience Toolkit (EMET) to minimize exploitation of vulnerabilities in all manufactured software. See Knowledge Base article KB2458544 on support.microsoft.com for more information.
- Strengthen authentication by using smart cards. See "Smart Cards" on technet.microsoft.com for more information.
- Use Network Access Protection (NAP) and DirectAccess (DA) to enforce compliance polices for firewall, antimalware, and patch management on remote systems connecting to corporate network. See "Network Access Protection" on msdn.microsoft.com and "Windows 7 DirectAccess Explained" on technet.microsoft.com for more information.

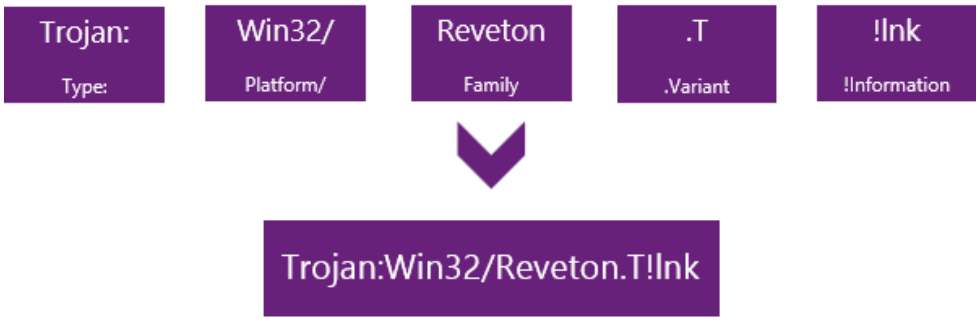
Appendixes

Appendix A: Threat naming conventions

Microsoft names the malware and potentially unwanted software that it detects according to the Computer Antivirus Research Organization (CARO) Malware naming scheme.

This scheme uses the following format:

Figure 85. The Microsoft malware naming convention



When Microsoft analysts research a particular threat, they will determine what each of the components of the name will be.

Type

The type describes what the threat does on your computer. Worms, trojans, viruses, and adware are some of the most common types of threats Microsoft detects.

Platform

The platform refers to the operating system (such as Windows, Mac OS X, and Android) that the threat is designed to work on. Platforms can also include programming languages and file formats.

Family

A group of threats with the same name is known as a family. Sometimes different security software companies use different names.

Variant letters

Variant letters are used sequentially for each different version or member of a family. For example, the detection for the variant ".AF" would have been created after the detection for the variant ".AE".

Additional information

Additional information is sometimes used to describe a specific file or component that is used by another threat in relation to this threat. In the example above, the !lnk indicates that the threat is a shortcut file used by the Trojan:Win32/Reveton.T variant, as shortcut files usually use the extension .lnk.

Appendix B: Data sources

Data included in the *Microsoft Security Intelligence Report* is gathered from a wide range of Microsoft products and services. The scale and scope of this telemetry data allows the report to deliver the most comprehensive and detailed perspective on the threat landscape that is available in the software industry:

- Bing, the search and decision engine from Microsoft, contains technology that performs billions of webpage scans per year to seek out malicious content. After such content is detected, Bing displays warnings to users about it to help prevent infection.
- Exchange Online Protection protects the networks of tens of thousands of enterprise customers worldwide by helping to prevent malware from spreading through email. Exchange Online Protection scans billions of email messages every year to identify and block spam and malware.
- The Malicious Software Removal Tool (MSRT) is a free tool that Microsoft designed to help identify and remove prevalent malware families from customer computers. The MSRT is primarily released as an important update through Windows Update, Microsoft Update, and Automatic Updates. A version of the tool is also available from the Microsoft Download Center. The MSRT was downloaded and executed more than 600 million times each month on average in 1H13. The MSRT is not a replacement for an up-to-date antivirus solution because of its lack of real-time protection and because it uses only the portion of the Microsoft antivirus signature database that enables it to target specifically selected, prevalent malicious software.
- The Microsoft Safety Scanner is a free downloadable security tool that provides on-demand scanning and helps remove malware and other malicious software. The Microsoft Safety Scanner is not a replacement for an up-to-date antivirus solution, because it does not offer real-time protection and cannot prevent a computer from becoming infected.
- Microsoft Security Essentials is a free real-time protection product that combines an antivirus and antispyware scanner with phishing and firewall protection.
- Microsoft System Center Endpoint Protection (formerly Forefront Client Security and Forefront Endpoint Protection) is a unified product that

provides protection from malware and potentially unwanted software for enterprise desktops, laptops, and server operating systems. It uses the Microsoft Malware Protection Engine and the Microsoft antivirus signature database to provide real-time, scheduled, and on-demand protection.

- Outlook.com has more than 400 million active email users in more than 30 countries/regions around the world.
- SmartScreen Filter, a feature in Internet Explorer 8, 9, and 10, offers users protection against phishing sites and sites that host malware. Microsoft maintains a database of phishing and malware sites reported by users of Internet Explorer and other Microsoft products and services. When a user attempts to visit a site in the database with the filter enabled, Internet Explorer displays a warning and blocks navigation to the page.
- Windows Defender in Windows 8 provides real-time scanning and removal of malware and potentially unwanted software.
- Windows Defender Offline is a downloadable tool that can be used to create a bootable CD, DVD, or USB flash drive to scan a computer for malware and other threats. It does not offer real-time protection and is not a substitute for an up-to-date antimalware solution.

Figure 86. US privacy statements for the Microsoft products and services used in this report

Product or service	Privacy statement URL
Bing	www.microsoft.com/privacystatement/en-us/bing/default.aspx
Exchange Online	www.microsoft.com/online/legal/v2/?docid=22&langid=en-us
Internet Explorer 10	windows.microsoft.com/en-US/internet-explorer/ie10-win8-privacy-statement
Malicious Software Removal Tool	www.microsoft.com/security/pc-security/msrt-privacy.aspx
Microsoft Security Essentials	windows.microsoft.com/en-us/windows/security-essentials-privacy
Microsoft Safety Scanner	www.microsoft.com/security/scanner/en-us/privacy.aspx
Outlook.com	privacy.microsoft.com/en-us/fullnotice.mspx
System Center Endpoint Protection	technet.microsoft.com/en-us/library/hh508835.aspx
Windows Defender in Windows 8	windows.microsoft.com/en-US/windows-8/windows-8-privacy-statement?#T1=supplement&section_36
Windows Defender Offline	windows.microsoft.com/en-us/windows/windows-defender-offline-privacy

Appendix C: Worldwide infection and encounter rates

"Malware prevalence worldwide," on page 45, explains how threat patterns differ significantly in different parts of the world. Figure 87 shows the infection and encounter rates for the first and second quarters of 2013 for 97 locations around the world. See "Malware prevalence worldwide" on page 45 for information about how infection and encounter rates are calculated.

For a more in-depth perspective on the threat landscape in any of these locations, see the "Regional Threat Assessment" section of the *Microsoft Security Intelligence Report* website.

Figure 87. Infection and encounter rates for locations around the world , 1Q13–2Q13, by quarter

Country/region	CCM 1Q13	CCM 2Q13	Encounter rate 1Q13	Encounter rate 2Q13
Worldwide	*6.3*	*5.8*	*17.82%*	*17.04%*
Albania	20.1	23.0	28.64%	28.93%
Algeria	19.2	17.8	37.51%	32.24%
Argentina	6.0	5.7	18.09%	20.09%
Armenia	8.3	8.7	31.42%	31.13%
Australia	3.7	3.8	11.62%	9.95%
Austria	2.3	2.1	11.48%	10.58%
Bangladesh	12.6	12.3	28.02%	26.23%
Belarus	6.6	7.5	26.21%	30.01%
Belgium	2.9	2.5	16.73%	13.28%
Bosnia and Herzegovina	13.5	15.2	27.36%	28.45%
Brazil	7.2	6.7	25.57%	26.75%
Bulgaria	7.9	7.2	24.47%	21.74%
Canada	4.1	3.5	14.76%	12.34%
Chile	5.5	5.1	15.26%	16.49%
China	0.7	0.6	28.85%	25.88%
Colombia	5.7	6.3	22.09%	23.81%
Costa Rica	3.1	2.8	13.40%	13.38%
Croatia	7.2	6.4	20.86%	18.43%

Country/region	CCM 1Q13	CCM 2Q13	Encounter rate 1Q13	Encounter rate 2Q13
Cyprus	6.6	6.1	18.63%	17.28%
Czech Republic	2.1	1.8	15.46%	13.36%
Denmark	2.1	1.7	10.14%	8.05%
Dominican Republic	13.7	16.0	21.27%	23.21%
Ecuador	9.9	13.6	28.46%	31.57%
Egypt	23.8	25.0	35.44%	36.11%
El Salvador	4.8	5.2	19.07%	18.98%
Estonia	2.4	2.1	12.71%	11.33%
Finland	1.2	0.8	8.43%	6.52%
France	2.8	2.5	14.53%	15.57%
Georgia	23.5	25.6	35.11%	39.58%
Germany	2.9	2.7	13.21%	11.06%
Ghana	7.5	7.9	22.38%	28.49%
Greece	6.7	6.1	26.03%	21.35%
Guatemala	6.3	5.5	17.48%	20.83%
Hong Kong SAR	2.5	2.2	10.70%	9.39%
Hungary	5.5	4.6	19.01%	16.20%
Iceland	2.1	2.0	8.40%	7.50%
India	10.6	13.4	29.31%	29.44%
Indonesia	13.4	13.6	31.21%	31.83%
Iraq	27.1	31.5	32.69%	34.53%
Ireland	2.4	2.2	12.24%	10.39%
Israel	6.8	6.4	16.30%	15.74%
Italy	4.7	4.1	20.29%	20.03%
Jamaica	7.2	8.8	18.56%	22.33%
Japan	1.9	1.1	6.97%	6.97%
Jordan	14.4	17.0	24.46%	26.77%
Kazakhstan	8.4	11.6	29.34%	34.39%
Kenya	7.4	7.1	—	21.46%
Korea	43.0	24.3	33.36%	30.00%
Kuwait	10.5	11.5	19.85%	18.63%

Country/region	CCM 1Q13	CCM 2Q13	Encounter rate 1Q13	Encounter rate 2Q13
Latvia	4.3	3.9	19.70%	16.59%
Lebanon	14.1	17.0	24.83%	26.19%
Lithuania	7.0	6.7	23.14%	22.87%
Macedonia, FYRO	15.4	16.4	27.49%	26.53%
Malaysia	8.2	9.3	21.47%	22.33%
Mexico	9.6	10.1	24.52%	29.18%
Moldova	8.4	10.1	29.12%	28.67%
Morocco	21.7	21.7	27.10%	28.61%
Myanmar	10.9	9.4	30.99%	26.31%
Nepal	15.3	18.3	—	35.50%
Netherlands	3.3	2.7	14.68%	12.29%
New Zealand	3.3	3.7	11.08%	10.80%
Nigeria	7.0	6.8	18.87%	20.15%
Norway	1.8	1.6	8.29%	7.28%
Oman	13.5	12.8	—	22.91%
Pakistan	25.2	29.2	41.72%	42.46%
Palestinian Authority	24.8	26.1	34.44%	35.74%
Panama	5.6	5.9	17.52%	29.23%
Peru	9.4	17.0	28.03%	34.99%
Philippines	13.4	17.5	29.69%	29.55%
Poland	7.0	5.6	19.02%	17.40%
Portugal	4.1	3.6	21.76%	18.08%
Puerto Rico	5.2	5.4	10.89%	10.41%
Qatar	9.2	10.0	19.25%	20.21%
Romania	13.5	13.2	23.13%	21.27%
Russia	5.4	4.5	28.61%	29.70%
Saudi Arabia	12.1	12.0	23.91%	23.93%
Senegal	7.8	8.4	—	27.25%
Serbia	10.8	10.5	24.30%	23.00%
Singapore	4.1	4.1	12.04%	11.51%
Slovakia	3.3	3.0	16.39%	13.88%

Country/region	CCM 1Q13	CCM 2Q13	Encounter rate 1Q13	Encounter rate 2Q13
Slovenia	3.4	3.2	15.00%	14.00%
South Africa	7.1	6.8	17.36%	16.74%
Spain	5.0	4.2	18.01%	19.12%
Sri Lanka	7.9	7.4	23.79%	21.34%
Sweden	2.1	1.7	9.52%	7.94%
Switzerland	2.5	2.3	10.28%	10.30%
Taiwan	5.2	4.2	18.90%	17.31%
Thailand	19.0	17.5	29.08%	26.55%
Tunisia	13.7	15.4	31.82%	34.78%
Turkey	22.5	23.6	41.25%	47.35%
Ukraine	7.6	7.3	31.54%	30.65%
United Arab Emirates	12.1	12.4	21.84%	21.32%
United Kingdom	2.9	2.6	13.53%	12.32%
United States	8.0	8.0	14.10%	11.51%
Uruguay	3.3	3.2	13.30%	15.28%
Venezuela	5.7	7.9	22.74%	27.16%
Vietnam	17.0	18.9	35.05%	36.57%
Worldwide	*6.3*	*5.8*	*17.82%*	*17.04%*

Glossary

For additional information about these and other terms, visit the MMPC glossary on www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx.

419 scam
See *advance-fee fraud*.

advance-fee fraud
A common confidence trick in which the sender of a message purports to have a claim on a large sum of money but is unable to access it directly for some reason, typically one that involves bureaucratic red tape or political corruption. The sender asks the prospective victim for a temporary loan to be used for bribing officials or for paying fees to get the full sum released. In exchange, the sender promises the target a share of the fortune that amounts to a much larger sum than the original loan, but does not deliver. Advance-fee frauds are often called *419 scams*, in reference to the article of the Nigerian Criminal Code that addresses fraud.

adware
A program that displays advertisements. Although some adware can be beneficial by subsidizing a program or service, other adware programs may display advertisements without adequate consent.

backdoor trojan
A type of trojan that provides attackers with remote unauthorized access to and control of infected computers. Bots are a subcategory of backdoor trojans. Also see *botnet*.

botnet
A set of computers controlled by a *command-and-control* (C&C) computer to execute commands as directed. The C&C computer can issue commands directly (often through Internet Relay Chat [IRC]) or by using a decentralized mechanism, such as peer-to-peer (P2P) networking. Computers in a botnet are often called *bots*, *nodes*, or *zombies*.

C&C
Short for *command and control*. See *botnet*.

CCM
Short for *computers cleaned per mille* (thousand). The number of computers cleaned for every 1,000 executions of the Microsoft Malicious Software Removal

Tool (MSRT). For example, if the MSRT has 50,000 executions in a particular location in the first quarter of the year and removes infections from 200 computers, the CCM for that location in the first quarter of the year is 4.0 (200 ÷ 50,000 × 1,000). Also see *encounter rate*.

clean
To remove malware or potentially unwanted software from an infected computer. A single cleaning can involve multiple disinfections.

command and control
See *botnet*.

denial of service (DoS)
A condition that occurs when the resources of a target computer are deliberately exhausted, which effectively overwhelms the computer and causes it to fail to respond or function for its intended users. There are a number of different types of attack that may be used to result in a denial of service condition using different types of flooding, or malformed network traffic. Also see *distributed denial of service (DDoS)*.

detection
The discovery of malware or potentially unwanted software on a computer by antimalware software. Disinfections and blocked infection attempts are both considered detections.

detection signature
A set of characteristics that can identify a malware family or variant. Signatures are used by antimalware products to determine whether a file is malicious or not.

disclosure
Revelation of the existence of a vulnerability to a third party.

disinfect
To remove a malware or potentially unwanted software component from a computer or to restore functionality to an infected program. Compare with *clean*.

distributed denial of service (DDoS)
A form of denial of service (DoS) that uses multiple computers to attack the target. Considerable resources may be required to exhaust a target computer and cause it to fail to respond. Often multiple computers are used to perform these types of malicious attack and increase the attack's chances of success. This

type of attack can succeed, for example, when a number of compromised computers, such as those that comprise a botnet, are commandeered and ordered to access a target network or server over and over again within a small period of time.

DNS
See *Domain Name System*.

DNS amplification
A distributed denial-of-service (DDoS) technique in which attackers use misconfigured public DNS servers to flood a target system with DNS response traffic.

DNS hijacking
An attack technique that uses malicious or compromised DNS servers to return false responses to DNS queries.

Domain Name System
The infrastructure used for name resolution on the Internet. It comprises a hierarchical collection of name servers that translate alphanumeric domain names to numeric IP addresses, and vice versa.

downloader
See *trojan downloader/dropper*.

encounter
An instance of security software detecting a threat and blocking, quarantining, or removing it from the computer.

encounter rate
The percentage of computers running Microsoft real-time security software that report detecting malware or potentially unwanted software, or report detecting a specific threat or family, during a period. Also see *infection rate*.

exploit
Malicious code that takes advantage of software vulnerabilities to infect a computer or perform other harmful actions.

firewall
A program or device that monitors and regulates traffic between two points, such as a single computer and the network server, or one server to another.

generic
A type of signature that is capable of detecting a variety of malware samples from a specific family, or of a specific type.

IFrame
Short for inline frame. An IFrame is an HTML document that is embedded in another HTML document. Because the IFrame loads another webpage, it can be used by criminals to place malicious HTML content, such as a script that downloads and installs spyware, into non-malicious HTML pages that are hosted by trusted websites.

in the wild
A phrase to denote malware that is currently detected on active computers connected to the Internet, as compared to those confined to internal test networks, malware research laboratories, or malware sample lists.

infection
The presence of malware or potentially unwanted software on a computer, or the act of delivering or installing malware or potentially unwanted software on a computer. Also see *encounter*.

infection rate
See *CCM*.

jailbreaking
See *rooting*.

malware
Any software that is designed specifically to cause damage to a user's computer, server, or network. Viruses, worms, and trojans are all types of malware. By default, Microsoft security products automatically block, quarantine, or remove malicious software that is determined to have a significantly negative impact on affected computers.

malware impression
A single instance of a user attempting to visit a page known to host malware and being blocked by SmartScreen Filter in Internet Explorer versions 8 through 10. Also see *phishing impression*.

name server
A server that translates alphanumeric domain names to numeric IP addresses and vice versa. Name servers are components of the Domain Name System (DNS).

P2P
See *peer-to-peer (P2P)*.

password stealer (PWS)
Malware that is specifically used to transmit personal information, such as user names and passwords. A PWS often works in conjunction with a keylogger.

payload
The actions conducted by a piece of malware for which it was created. Payloads can include, but are not limited to, downloading files, changing system settings, displaying messages, and logging keystrokes.

peer-to-peer (P2P)
A system of network communication in which individual nodes are able to communicate with each other without the use of a central server.

phishing
A method of credential theft that tricks Internet users into revealing personal or financial information online. Phishers use phony websites or deceptive email messages that mimic trusted businesses and brands to steal personally identifiable information (PII) such as user names, passwords, credit card numbers, and identification numbers.

phishing impression
A single instance of a user attempting to visit a known phishing page with Internet Explorer versions 7 through 10, and being blocked by the Phishing Filter or SmartScreen Filter. Also see *malware impression*.

potentially unwanted software
A program with potentially unwanted functionality that is brought to the user's attention for review. This type of software may affect the user's privacy, security, or computing experience.

ransomware
A type of malware that prevents use of a computer or access to the data that it contains until the user pays a certain amount of money to a remote attacker (the "ransom"). Computers that have ransomware installed usually display a screen that contain information on how to pay the ransom. A user cannot usually access anything on the computer beyond the screen.

rogue security software
Software that appears to be beneficial from a security perspective but that provides limited or no security capabilities, generates a significant number of

erroneous or misleading alerts, or attempts to socially engineer the user into participating in a fraudulent transaction.

rooting
Obtaining administrative user rights on a mobile device through the use of exploits. Device owners sometimes use such exploits intentionally to gain access to additional functionality, but these exploits can also be used by attackers to infect devices with malware that bypasses many typical security systems. The term *rooting* is typically used in the context of Android devices; the comparable process on iOS devices is more commonly referred to as *jailbreaking*.

sandbox
A specially constructed portion of a computing environment in which potentially dangerous programs or processes may run without causing harm to resources outside the sandbox.

settings modifier
A program that changes computer settings with or without the user's knowledge.

signature
See *detection signature*.

social engineering
A technique that defeats security precautions by exploiting human vulnerabilities. Social engineering scams can be both online (such as receiving email messages that ask the recipient to click the attachment, which is actually malware) and offline (such as receiving a phone call from someone posing as a representative from one's credit card company). Regardless of the method selected, the purpose of a social engineering attack remains the same—to get the targeted user to perform an action of the attacker's choice or reveal information that can be used to compromise the user.

spam
Bulk unsolicited email. Malware authors may use spam to distribute malware, either by attaching the malware to email messages or by sending a message that contains a link to the malware. Malware may also harvest email addresses for spamming from compromised computers or may use compromised computers to send spam.

spyware
A program that collects information, such as the websites that a user visits, without adequate consent. Installation may be without prominent notice or without the user's knowledge.

SQL injection
A technique in which an attacker enters a specially crafted Structured Query Language (SQL) statement into an ordinary web form. If form input is not filtered and validated before being submitted to a database, the malicious SQL statement may be executed, which could cause significant damage or data loss.

tool
In the context of malware, a software program that may have legitimate purposes but may also be used by malware authors or attackers.

trojan
A generally self-contained program that does not self-replicate but performs malicious action on the computer.

trojan downloader/dropper
A form of trojan that installs other malicious files to a computer that it has infected, either by downloading them from a remote computer or by obtaining them directly from a copy contained in its own code.

virus
Malware that replicates, typically by infecting other files in the computer, to allow the execution of the malware code and its propagation when those files are activated.

vulnerability
A weakness, error, or poor coding technique in a program that may allow an attacker to exploit it for a malicious purpose.

wild
See *in the wild*.

worm
Malware that spreads by spontaneously sending copies of itself through email or by using other communication mechanisms, such as instant messaging (IM) or peer-to-peer (P2P) applications.

Threat families referenced in this report

The definitions for the threat families referenced in this report are adapted from the Microsoft Malware Protection Center encyclopedia (www.microsoft.com/security/portal), which contains detailed information about a large number of malware and potentially unwanted software families. See the encyclopedia for more in-depth information and guidance for the families listed here and throughout the report.

JS/Aimesu. A threat that exploits vulnerabilities in unpatched versions of Java, Adobe Reader, or Flash Player. It then installs other malare on the computer, including components of the "Blackhole" and "Cool" exploit kits.

Win32/Alureon. A data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.

INF/Autorun. 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.

Win32/Banker. A family of data-stealing trojans that captures banking credentials such as account numbers and passwords from computer users and relays them to the attacker. Most variants target customers of Brazilian banks; some variants target customers of other banks.

Win32/Banload. A family of trojans that download other malware. Banload usually downloads Win32/Banker, which steals banking credentials and other sensitive data and sends it back to a remote attacker.

Win32/Bdaejec. A trojan that allows unauthorized access and control of an affected computer, and that may download and install other programs without consent.

Blacole. An exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised

website that contains the exploit pack, various malware may be downloaded and run.

JS/BlacoleRef. An obfuscated script, often found inserted into compromised websites, that uses a hidden inline frame to redirect the browser to a Blacole exploit server.

Win32/Brontok. A mass-mailing email worm that spreads by sending copies of itself as email attachments to addresses gathered from files on the infected computer, and by copying itself to removable volumes. Brontok can disable security software and may conduct DoS attacks against certain websites.

ALisp/Bursted. A virus written in the AutoLISP scripting language used by the AutoCAD computer-aided design program. It infects other AutoLISP files with the extension .lsp.

Win32/Chir. A family with a worm component and a virus component. The worm component spreads by email and by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The virus component may infect .exe, .scr, and HTML files.

JS/Colkit. A detection for obfuscated, malicious JavaScript code that redirects to or loads files that may exploit a vulnerable version of Java, Adobe Reader, or Adobe Flash, possibly in an attempt to load malware onto the computer.

Win32/Conficker. 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 also downloads arbitrary files.

JS/Coolex. A detection for scripts from an exploit pack known as the "Cool Exploit Kit." These scripts are often used in ransomware schemes in which an attacker locks a victim's computer or encrypts the user's data and demands money to make it available again.

Win32/CplLnk. A generic detection for specially crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046.

AndroidOS/CVE-2011-1823. A detection for specially crafted Android programs that attempt to exploit a vulnerability in the Android operating system to gain root privilege.

Java/CVE-2012-1723. A family of malicious Java applets that attempt to exploit vulnerability CVE-2012-1723 in the Java Runtime Environment (JRE) to download and install files of an attacker's choice onto the computer.

Win32/DealPly. Adware that displays offers related to the user's web browsing habits. It may be bundled with certain third-party software installation programs.

Win32/Delf. A detection for various threats written in the Delphi programming language.

Win32/DelfInject. A detection for various threats that inject themselves into running processes.

Win32/Dorkbot. A worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

Win32/Dynamer. A generic detection for a variety of threats.

MacOS_X/FakeMacdef. A rogue security software family that affects Apple Mac OS X. It has been distributed under the names MacDefender, MacSecurity, MacProtector, and possibly others.

Win32/FakeRean. A rogue security software family distributed under a variety of randomly generated names, including Privacy Protection, Security Protection, Antivirus Protection 2012, XP Security Protection 2012, and many others.

Win32/Fareit. A malware family that has multiple components: a password stealing component that steals sensitive information and sends it to an attacker, and a DDoS component that could be used against other computers.

Win32/FastSaveApp. An adware program that displays offers related to the user's web browsing habits. It may use the name "SaveAs" or "SaveByClick".

Win32/FindLyrics. An adware program that displays ads related to the user's web browsing habits.

Win32/Gamarue. A worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.

Win32/GameVance. Software that displays advertisements and tracks anonymous usage information in exchange for a free online gaming experience at the Web address "gamevance.com".

Win32/Gisav. An adware program that displays offers related to the user's web browsing habits. It can be downloaded from the program's website, and can be bundled with some third-party software installation programs.

HTML/IframeRef. A generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.

Win32/InfoAtoms. An adware program that displays advertisements related to the user's web browsing habits and inserts advertisements into websites.

Backdoor:Perl/IRCbot.E: A backdoor trojan that drops other malicious software and connects to IRC servers to receive commands from attackers.

JS/Javrobat. An exploit that tries to check whether certain versions of Adobe Acrobat or Adobe Reader are installed on the computer. If so, it tries to install malware.

Win32/Keygen. A detection for tools that generate product keys for various software products.

Win32/Kraddare. Adware that displays Korean-language advertisements.

Unix/Lotoor. A detection for specially crafted Android programs that attempt to exploit vulnerabilities in the Android operating system to gain root privilege.

Win32/Microjoin. A generic detection for tools that bundle malware files with clean files in an effort to deploy malware without being detected by security software.

Win32/Obfuscator. 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.

Win32/Onescan. A Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, Smart Vaccine, and many others.

Win32/OpenCandy. An adware program that may be bundled with certain third-party software installation programs. Some versions may send user-specific information, including a unique machine code, operating system information, locale, and certain other information to a remote server without obtaining adequate user consent.

Win32/Orsam. A generic detection for a variety of threats.

Win32/Pameseg. A fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.

Win32/Patch. A family of tools intended to modify or "patch" programs that may be evaluation copies or unregistered versions with limited features for the purpose of removing the limitations.

Win32/Pluzoks. A trojan that silently downloads and installs other programs without consent and that could include the installation of additional malware or malware components.

JS/Popupper. A detection for a particular JavaScript script that attempts to display pop-under advertisements.

JS/Pornpop. A generic detection for specially crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

Win32/PossibleHostsFileHijack. An indicator that the computer's HOSTS file may have been modified by malicious or potentially unwanted software, which can cause access to certain Internet domains and websites to be redirected or denied.

Win32/Pramro. A trojan that creates a proxy on the infected computer for email and HTTP traffic, and is used to send spam email.

Win32/PriceGong. An adware program that shows certain deals related to the search terms entered on any web page.

Win32/Protlerdob. A software installer with a Portuguese language user interface. It presents itself as a free movie download but bundles with it a number of programs that may charge for services.

BAT/Qhost. A generic detection for trojans that modify the HOSTS file on the computer to redirect or limit Internet traffic to certain sites.

Win32/Ramnit. A family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to removable drives and steals sensitive information such as saved File Transfer Protocol (FTP) credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Win32/Ransom. A detection for malicious programs that seize control of the computer on which they are installed. This trojan usually locks the screen and prevents the user from using the computer. It usually displays an alert message.

Win32/Reveton. A ransomware family that targets users from certain countries. It locks the computer and displays a location-specific webpage that covers the desktop and demands that the user pay a fine for the supposed possession of illicit material.

Win32/Rongvhin. A family of malware that perpetrates click fraud. It might be delivered to the computer via hack tools for the game CrossFire.

Win32/Sality. 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.

JS/Seedabutor. A JavaScript trojan that attempts to redirect the browser to another website.

Win32/Sirefef. A malware platform that receives and runs modules that perform different malicious activities.

Java/SMSer. A ransomware trojan that locks an affected user's computer and requests that the user send a text message to a premium-charge number to unlock it.

Win32/Swisyn. A trojan that drops and executes arbitrary files on an infected computer. The dropped files may be potentially unwanted or malicious programs.

Win32/Tobfy. A family of ransomware trojans that targets users from certain countries. It locks the computer and displays a localized message demanding the payment of a fine for the supposed possession of illicit material. Some variants may also take webcam screenshots, play audio messages, or affect certain processes or drivers.

MSIL/Truado. A trojan that poses as an update for certain Adobe software.

Win32/Urausy. A family of ransomware trojans that locks the computer and displays a localized message, supposedly from police authorities, demanding the payment of a fine for alleged criminal activity.

Win32/Virut. 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 Internet Relay Chat (IRC) server.

Win32/Vobfus. A family of worms that spreads via network drives and removable drives and downloads/executes arbitrary files. Downloaded files may include additional malware.

Win32/Vundo. A multi-component family of programs that deliver pop-up advertisements and may download and execute arbitrary files. Vundo is often installed without a user's consent as a browser helper object (BHO).

Win32/Wecykler. A family of worms that spread via removable drives, such as USB drives, that may stop security processes and other processes on the computer, and log keystrokes that are later sent to a remote attacker.

Win32/Weelsof. A family of ransomware trojans that targets users from certain countries. It locks the computer and displays a localized message demanding the payment of a fine for the alleged possession of illicit material. Some variants may take steps that make it difficult to run or update virus protection.

Win32/Wintrim. A family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can monitor the user's activities, download applications, and send system information back to a remote server.

Win32/Winwebsec. A rogue security software family distributed under the names AVASoft Professional Antivirus, Smart Fortress 2012, Win 8 Security System, and others.

Win32/Wpakill. A family of tools that attempt to disable or bypass WPA (Windows Product Activation), WGA (Windows Genuine Advantage), or WAT (Windows Activation Technologies) checks by altering Windows operating system files, terminating processes, or stopping services.

Win32/Yakdowpe. A family of trojans that connect to certain websites to silently download and install other programs without consent.

Win32/Zbot. A family of password-stealing trojans that also contain backdoor functionality allowing unauthorized access and control of an affected computer.

Index

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