Microsoft

Microsoft Security Intelligence Report

Volume 19 | January through June, 2015

Authors

Charlie Anthe
Cloud and Enterprise Security

Patti Chrzan
Microsoft Digital Crimes Unit

Elia Florio
Microsoft Malware Protection Center

Chad Foster
Bing

Paul Henry
Wadeware LLC

Jeff Jones
Corporate Communications

Nam Ng
Worldwide Cybersecurity & Data Protection

Niall O'Sullivan
Microsoft Digital Crimes Unit

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Anthony Penta
Safety Platform

Ina Ragragio
Microsoft Malware Protection Center

Tim Rains
Worldwide Cybersecurity & Data Protection

Paul Rebriy
Bing

Contributors

Peter Cap
Microsoft Malware Protection Center

Bulent Egilmez
Office 365 - Information Protection

Tanmay Ganacharya
Microsoft Malware Protection Center

Kathryn Gillespie
Microsoft IT

Jeff Glover
Microsoft IT

Roger Grimes
Microsoft IT

Satomi Hayakawa
CSS Japan Security Response Team

Ben Hope
Microsoft Malware Protection Center

Yurika Kakiuchi
CSS Japan Security Response Team

Jenn LeMond
Microsoft IT

Alisha Mark
Corporate Communications

Dolcita Montemayor
Microsoft Malware Protection Center

Daric Morton
Microsoft Services

Jeong Mun
Microsoft Malware Protection Center

Cody Nicewanner
Operating Systems Group

Wendi Okun
Legal & Corporate Affairs

Ferdinand Plazo
Microsoft Malware Protection Center

Laura A. Robinson
Microsoft IT

Norie Tamura
CSS Japan Security Response Team

Steve Wacker
Wadeware LLC

Vladimir Zubko
Microsoft Malware Protection Center

Table of contents

About this report

The *Microsoft Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, malware, and 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 2015, 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, 1H15 represents the first half of 2015 (January 1 through June 30), and 4Q14 represents the fourth quarter of 2014 (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. 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 generic detections. For the purposes of this report, a threat is defined as a malware or unwanted software family or variant that is detected by the Microsoft Malware Protection Engine.

Foreword

Welcome to Volume 19 of the *Microsoft Security Intelligence Report (SIR)*. I've contributed to the SIR for almost ten years now. If I had to describe how the threat landscape has changed during that time using only one word, I'd say it's "cumulative."

Ten years ago we reported on a range of threats that included trojans, worms, trojan downloaders & droppers, exploits, bots (backdoor trojans), among others. These types of threats were primarily motivated by a desire to disrupt networks, as worms did years earlier, or to seek profit.

Fast forward ten years and we still see the same categories of threats and even some of the same threat families employed. During this time, attackers have had to evolve their tactics to get malware onto computers that have also been evolving with continuously elevating security levels. As vulnerabilities in operating systems have become harder to find and exploit, attackers have relied increasingly on social engineering to compromise computer systems.

In addition to these types of attacks, we have seen more threat actors with different motivations emerge over the years, including hacktivists and practitioners of military and economic espionage. Rogue security software or fake antivirus software that was used to trick people into installing malware and disclosing credit card information to attackers has been replaced by ransomware that seeks to extort victims by encrypting their data. Commercial exploit kits now dominate the list of top exploits we see trying to compromise unpatched computers, which means the exploits that computers are exposed to on the Internet are professionally managed and constantly optimized at an increasingly quick rate. Targeted attacks have become common as opposed to the exception.

Attackers continue to try to use the tactics that they did years ago, and have added to their repertoire of dirty tricks. This is why I use the word "cumulative" to describe how things have changed. If I could use a second word to describe how they have changed I would use "accelerated." The focus and pace that some attackers have been demonstrating recently have certainly increased over time.

Notice I didn't use the word "advanced." Although attackers have accumulated more tricks and tactics and seem to be using them in a more focused, fast-paced way, they still focus on a relatively small number of ways to compromise computers, including:

- Unpatched vulnerabilities
- Misconfigured computers
- Weak passwords
- Social engineering

The great news if you are a CISO or security professional is that you've never had so much information and so many security capabilities and tools as you do today to defend your organization's data.

Please enjoy the report.

Tim Rains
Chief Security Advisor
Enterprise Cybersecurity Group
Microsoft

Featured intelligence

STRONTIUM: A profile of a persistent and motivated adversary

A research team at the Microsoft Malware Protection Center (MMPC) proactively monitors the threat landscape for emerging threats. Part of this job involves keeping tabs on targeted attack groups, which are often the first ones to introduce new exploits and techniques that are later used widely by other attackers. One such group, which Microsoft has code-named STRONTIUM, is of particular interest because of its aggressive, persistent tactics and techniques, and its repeated use of new zero-day exploits to attack its targets. Microsoft is sharing some of the information it has gathered on this prominent attack group in the hope that it will raise awareness of the group's activities and help organizations take immediate advantage of available mitigations that can significantly reduce the risks that they face from this and similar groups.

Adversary profile

STRONTIUM has been active since at least 2007. Whereas most modern untargeted malware is ultimately profit-oriented, STRONTIUM mainly seeks sensitive information. Its primary institutional targets have included government bodies, diplomatic institutions, and military forces and installations in NATO member states and certain Eastern European countries. Additional targets have included journalists, political advisors, and organizations associated with political activism in central Asia. *STRONTIUM* is Microsoft's code name for this group, following its internal practice of assigning chemical element names to activity groups; other researchers have used code names such as *APT28*,[1] *Sednit*,[2] *Sofacy*,[3] and *Fancy Bear* as labels for a group or groups that have displayed

---

[1] *APT28: A Window into Russia's Cyber Espionage Operations?*, FireEye, Inc., October 14, 2014, https://www2.fireeye.com/apt28.html.

[2] Loucif Kharouni et al., *Operation Pawn Storm: Using Decoys to Evade Detection*, Trend Micro, October 22, 2014, www.trendmicro.com/vinfo/us/security/news/cyber-attacks/pawn-storm-espionage-attacks-use-decoys-deliver-sednit.

[3] *Tactical Intelligence Bulletin: Sofacy Phishing*, PwC, October 22, 2014, pwc.blogs.com/files/tactical-intelligence-bulletin---sofacy-phishing-.pdf.

activity similar to the activity observed from STRONTIUM. The group's persistent use of spear phishing tactics and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

How STRONTIUM attacks a target

STRONTIUM primarily uses two kinds of attack. It uses *spear phishing*—phishing attempts targeted at specific individuals—to perform reconnaissance and steal login credentials to gather information about potential high-value targets associated with the institution under attack. Following the reconnaissance phase, it uses a variety of methods to infect the computers of high-value targets with malware, often by exploiting previously unknown vulnerabilities in browser add-ons and other software.

> Whereas most modern untargeted malware is ultimately profit-oriented, STRONTIUM mainly seeks sensitive information.

Reconnaissance and target identification

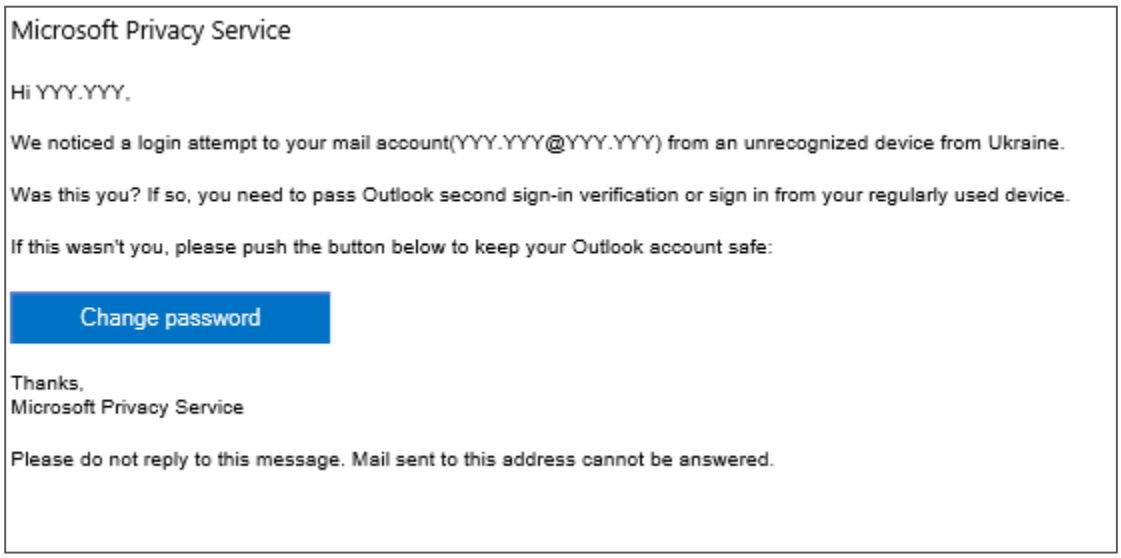
STRONTIUM typically begins its attack on an institution by identifying and profiling potential victims with connections to the institution. Microsoft has seen indications that STRONTIUM relies on open-source intelligence (OSINT), such as email lists and information harvested from public forums or social networking sites, to identify targets for spear phishing. Microsoft also believes that STRONTIUM relies on past successful phishing attacks to augment its dataset, by making use of any email communications it can identify between prior targets and the current target.

STRONTIUM casts a wide net with its reconnaissance activities, seeking login credentials for email and other systems from a large number of people, which it then weeds through to assess its value. Microsoft believes STRONTIUM used its spear phishing attacks to target several thousand individuals during the first half of 2015. Although STRONTIUM isn't choosy with its targets, it is persistent. When STRONTIUM identifies an individual to target, the group will repeatedly conduct spear phishing attacks against it over a long duration, possibly a year or more, until one of the attempts succeeds.

STRONTIUM's spear phishing modus operandi focuses on making the recipient concerned about unauthorized use of an account. A recent attack campaign involved sending messages with the subject line "Privacy alert" purporting to originate from a well-known email service, informing the user that their account

has been accessed from an unrecognized device in a different country. Because the targeted individuals are often professionals who have access to sensitive information, this can be an effective way to entice users to click a "change password" link that actually leads to a webpage under the attacker's control.

Figure 1. An example of a credential-stealing spear phishing message sent by STRONTIUM



Typically, the link will lead to a domain name that is similar to a legitimate domain name used by the service in an effort to fool the user into thinking the message is legitimate. Figure 2 lists some examples.

Figure 2. Examples of domain names spoofed by STRONTIUM in recent attacks

Legitimate domain name	Spoofed domain name controlled by STRONTIUM
accounts.google.com	accounts.g00qle.com
us-mg6.mail.yahoo.com	us-mg6mailyahoo.com
profile.live.com	privacy-live.com
mail.ukr.net	mail-ukr.net
www.nato.int	nato-news.com
www.bbc.com	bbc-press.org
www.osce.org	osce-press.com
www.eff.org	electronicfrontierfoundation.org

If the attack is successful, STRONTIUM uses the captured credentials to access the victim's email account to identify additional targets and for additional analysis and attacks. Even if the recipient doesn't enter their login credentials

into the malicious webpage, the act of clicking the link can provide STRONTIUM with valuable information. In addition to providing STRONTIUM with the recipient's IP address, clicking the link transmits a user-agent string to the web server that typically includes details about the recipient's browser and operating system versions, and sometimes includes information about the browser add-ons the recipient is using. This can provide STRONTIUM with insight into what software is deployed in the organization, and possibly help it plan future drive-by download activities.

Figure 3. JavaScript is used to collect information about the visitor's browser for drive-by download attacks

```
    string_of_json += "\"plugins\":[ ";
    //string_of_json += DetectJavaForMSIE();
    if(navigator.userAgent.indexOf("MSIE") > -1 || navigator.userAgent.indexOf(

        string_of_json += DetectJavaForMSIE();
        string_of_json += DetectFlashForMSIE();
        string_of_json += EnumeratePlugins();
        //string_of_json += DetectPdfForMSIE();
        //string_of_json += DetectFlashForMSIE();

    }
    else {
        string_of_json += EnumeratePlugins();
    }
    string_of_json = string_of_json.substring(0, string_of_json.length - 1);
    string_of_json += "]";
    var st = string_of_json_start + string_of_json + string_of_json_end;
    return st;
}

function getXmlHttpRequest() {
```

```
function xmlHTTPResponseHandler()
{
    var url = "http://www.nato.int/cps/en/[redacted].htm";
    if( xmlHttp.readyState == 4 && xmlHttp.status == 200 ) {
        url = xmlHttp.responseText;
        window.location.replace(url);
    }
```

Attacking the target

The ultimate goal of the reconnaissance phase is to compile a list of high-value individuals who have information or access that STRONTIUM wants. With this list at hand, the group moves to the next phase of operations: installing malware on

the high-value targets' computers, and thereby gaining access to the institution's network.

STRONTIUM primarily uses email to deliver malware to targeted individuals, although some researchers have reported delivery through social networking channels as well. Typical messages, such as the one shown in Figure 4, are tied to current events: an upcoming conference, for example, or a real world news event in which the recipient might be interested. STRONTIUM's email senders are usually associated with well-known email providers, and use plausible-seeming names and titles that are designed to give the messages credibility. Depending on the specific attack used, the message typically includes a link for "additional information," which will launch a drive-by download or social engineering attack when clicked. Other messages include malicious attachments instead of links, typically a document file containing an exploit.

Figure 4. An example of a lure email message sent by STRONTIUM

```
Subject: Mission_In_Central_African_Republic

*Dear Sir!*

Please be advised that The Spanish Army personnel and a large number of the
Spanish Guardia Civil officers
currently deployed in the Central African Republic (CAR) as part of the
European EUFOR RCA mission will return
to Spain in early March as the mission draws to a close.

Visit
http://eurasiaglobalnews.com/YYY-spains-armed-forces-conclude-mission-central-
african-republic/
for the addition info.

*Best regards,*

*Capt. John Smith, Defence Adviser, Public Diplomacy Division NATO,
Brussels defence.adviser.smith@gmail.com <defence.adviser.smith@gmail.com>*
```

Little is known about how and what information STRONTIUM gathers to tailor its attacks to specific high-value individuals. As discussed earlier, the user-agent and potential fingerprinting information gathered from phishing victims may play a part in planning the individual attacks by giving the group insight into what software may be in widespread use within the institution. In general,

STRONTIUM can take advantage of a variety of attacks that span general tactics and cover a wide range of technologies, including zero-day exploits.

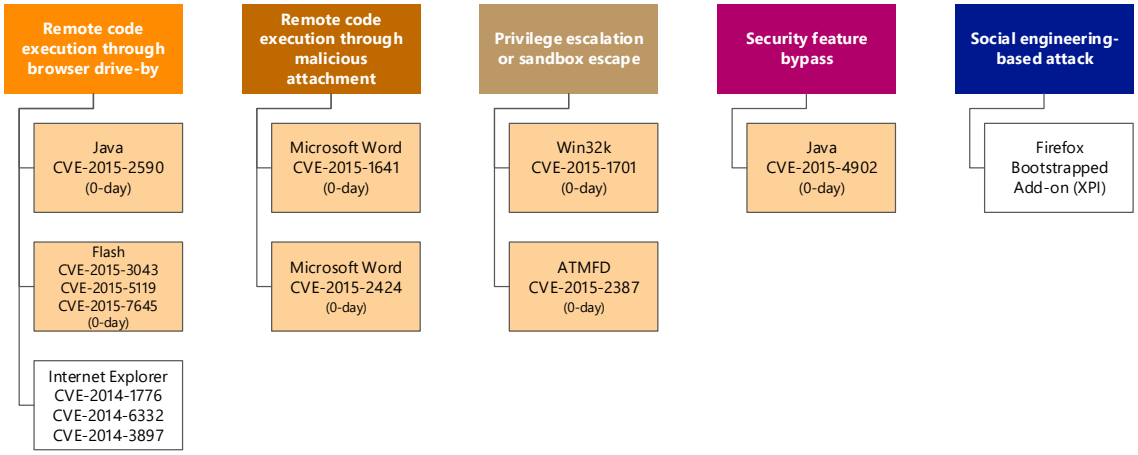
Zero-day exploits—exploits that target vulnerabilities for which the affected software vendor has not yet released a security update—form a significant part of STRONTIUM's arsenal. It is not yet clear whether the group researches vulnerabilities and develops the exploits themselves, or purchases them on the black market.

Microsoft researchers have observed STRONTIUM moving swiftly to take advantage of newly disclosed vulnerabilities; notably, the group deployed a number of zero-day exploits disclosed in a July 2015 leak of information from the security company Hacking Team. In other cases, STRONTIUM deployed exploits within days of a vendor releasing a security update that addressed the associated vulnerability, relying on the fact that not everyone installs security updates immediately after they are published.

Zero-day exploits form a significant part of STRONTIUM's arsenal.

The exploits used by STRONTIUM include a wide range of products from multiple vendors, including Adobe Flash Player, the Oracle Java Runtime Environment (JRE), Microsoft Word and Internet Explorer, and some components of the Windows kernel. Figure 5 lists some of the exploits used by STRONTIUM in recent campaigns, including a number of zero-day exploits (shaded). All of the vulnerabilities listed in Figure 5 were quickly addressed by security updates as part of the vendors' rapid response processes. (See "Guidance" on page 16 for information about how organizations can use up-to-date software to defend against targeted attacks.)

Figure 5. Some of the exploits used by STRONTIUM in attack campaigns in 2014 and 2015



In addition to using zero-day exploits, STRONTIUM also makes use of exploits that target older vulnerabilities for which security updates have been available for a long time. Microsoft believes that in some cases, the group learns during the reconnaissance phase that the targeted institution may be exposed to risks by running older or out-of-support platforms and software, by not testing and applying security updates quickly, or by not taking advantage of the latest mitigations and defense mechanisms shipped with more recent product versions—and then acts accordingly.

In a development observed in October 2015, the shellcode that executes after a successful memory corruption exploit displayed a number of characteristics that researchers had not observed from the malware previously:

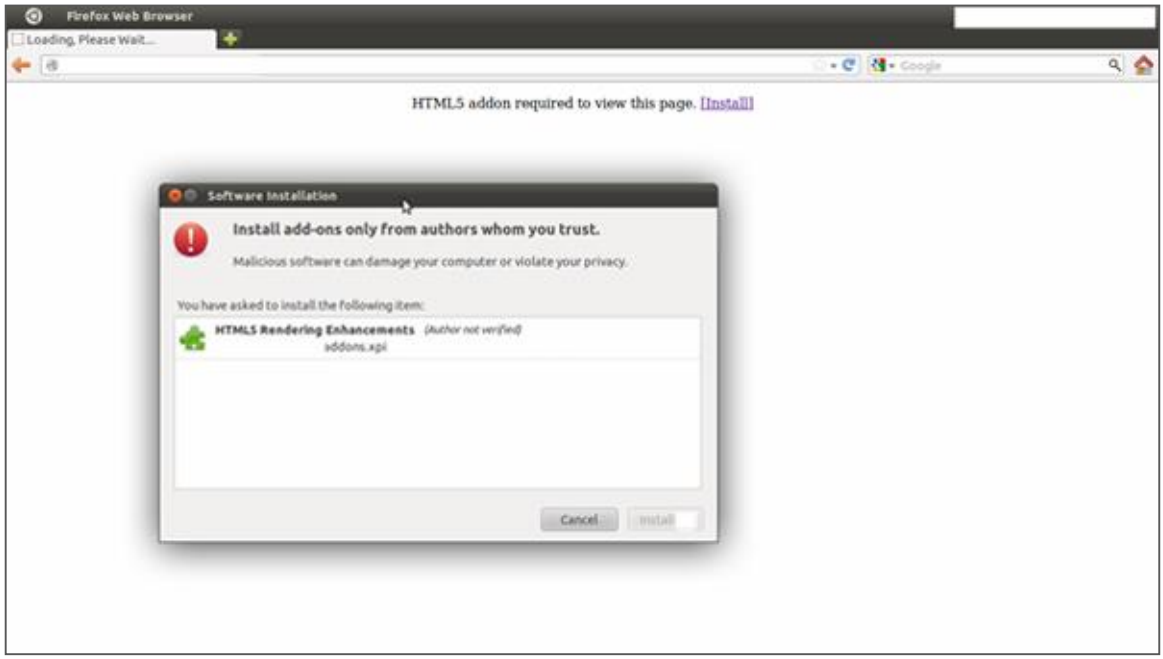
- API resolution: ROR 0x0D hashing, resolution made just before using the API
- Downloader: usage of HttpQueryInfo and WININET to fetch remote payloads in memory
- Compression: usage of ntdll!RtlDecompressBuffer()LZNT1 compression for remote payloads
- Privilege escalation: executed as DLL, but in-memory (diskless)

Figure 6. In-memory decompression and execution of remote payloads performed by STRONTIUM shellcode

```
1000025B
1000025B                            decompress:
1000025B 89 85 20 09 00 00                      mov     [ebp+shStru.ptrBuf4_rwx300000], eax
10000261 8D BD 24 09 00 00                      lea     edi, [ebp+shStru.FinalUncompressedSize]
10000267 57                                     push    edi
10000268 8B BD 08 09 00 00                      mov     edi, [ebp+shStru.CompressedBufferSize]
1000026E 57                                     push    edi
1000026F 8B BD 0C 09 00 00                      mov     edi, [ebp+shStru.ptrBuf2_rwx_download] ;
10000275 57                                     push    edi
10000276 68 00 00 30 00                         push    300000h         ; UncompressedBufferSize
1000027B 50                                     push    eax             ; UncompressedBuffer
1000027C 68 02 00 00 00                         push    COMPRESSION_FORMAT_LZNT1
10000281 68 84 01 E2 77                         push    77E20184h
10000286 FF D5                                  call    ebp             ; ntdll32!RtlDecompressB
10000288 8B 85 28 09 00 00                      mov     eax, [ebp+shStru.hWininet] ; passing WIN
1000028E 50                                     push    eax
1000028F 8B 85 20 09 00 00                      mov     eax, [ebp+shStru.ptrBuf4_rwx300000]
10000295 FF D0                                  call    eax             ; call 1st payload
10000297 E9 60 04 00 00                         jmp     loc_100006FC
```

In addition to relying on exploits, STRONTIUM also uses social engineering to trick victims into installing malware. Since March of 2015, for example, Microsoft has observed STRONTIUM successfully compromising Mozilla Firefox users by convincing them to install a malicious browser add-on based on a publicly available module ("Bootstrapped Addon Social Engineering Code Execution") developed for the Metasploit security testing framework.

Figure 7. STRONTIUM installs malware via a malicious bootstrapped add-on in Mozilla Firefox



Establishing control

After gaining administrative privileges on the computer through an exploit or social engineering, STRONTIUM uses a dropper to deploy a backdoor component, CORESHELL, which eventually downloads other modules. (Microsoft products sometimes detect the primary components as variants in the Win32/Foosace family, although the group has used other malware in the past.) The DLL backdoor is installed via execution of rundll32 with an export named "*init*" or "*InitW*." The dropper deletes itself after execution, while the DLL backdoor and any additional components are typically copied under the following folders:

- C:\Program Files\Common Files\Microsoft Shared\MSInfo\
- C:\Users\<*user name*>\AppData\Local\Microsoft Help\
- C:\ProgramData\

The dropper also writes the command and control (C&C) configuration information to the registry or an encrypted file. This strategy complicates forensic discovery of the attacker's infrastructure if the backdoor DLL is discovered, because the configuration information must be located separately.

Figure 8. Command & control configuration locations used by STRONTIUM

Format	Path
Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\<*path*>
File (Windows XP)	%ALLUSERSPROFILE%\msd
File (other Windows)	%PROGRAMDATA%\msd

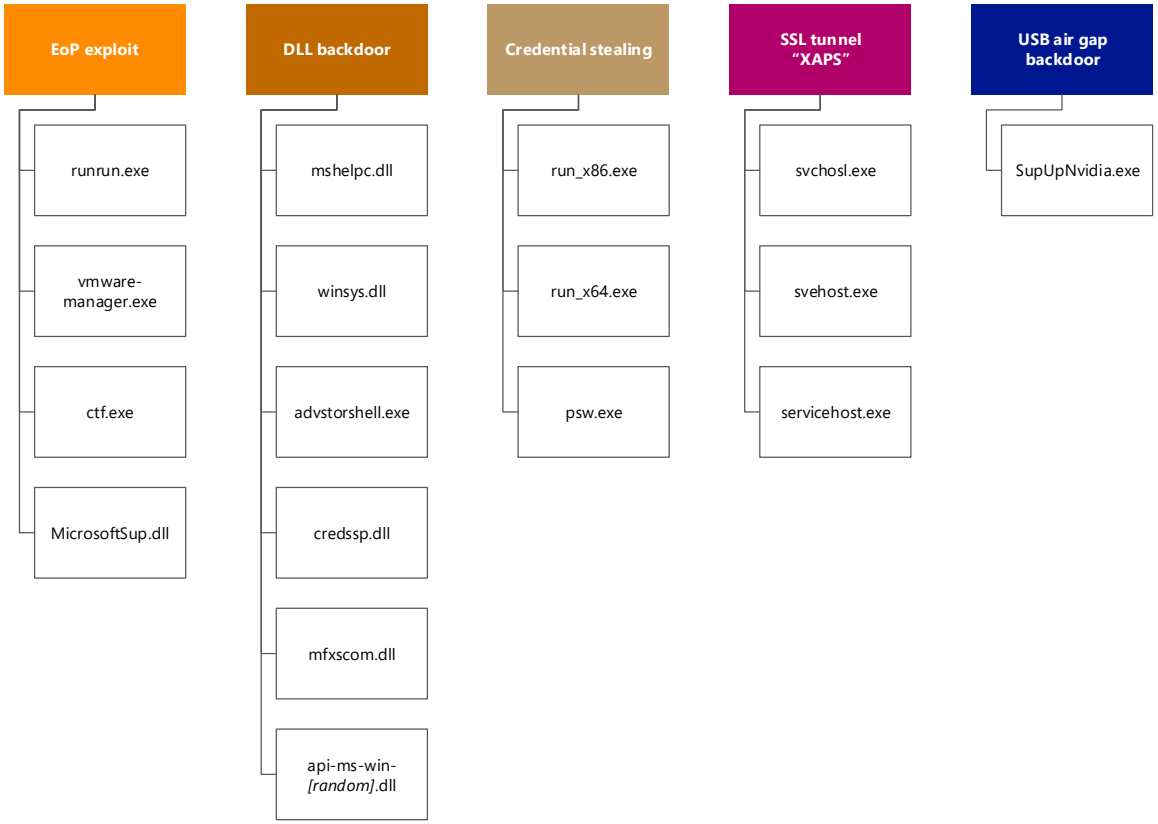
STRONTIUM ensures that its backdoor will run every time the computer starts by creating autostart extensibility point (ASEP) registry entries and shortcuts, which differ depending on what the attacker has chosen for the victim and which backdoor variant is used. (See "Advanced Malware Cleaning Techniques for the IT Professional" on page 96 of *Microsoft Security Intelligence Report, Volume 11 (January–June 2011)*, available from the Microsoft Download Center, for guidance on using Sysinternals tools to monitor ASEPs for signs of malware infection.) The most common ASEPs used by STRONTIUM for its malware include the following:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjectDelayLoad\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
- HKEY_CURRENT_USER\Environment\UserInitMprLogonScript = <*batch file*>
- %ALLUSERSPROFILE%\Application Data\Microsoft\Internet Explorer\Quick Launch\
- %USERPROFILE%\Application Data\Microsoft\Internet Explorer\Quick Launch\

The STRONTIUM backdoor is composed of several pieces with different functions. The attacker can deploy a large set of tools to perform tasks including key logging, email address and file harvesting, information gathering about the local computer, and remote communication with C&C servers. STRONTIUM also uses a component that is designed to infect connected USB storage devices, so that information can be captured from *air-gapped* computers that are not on

the network when a user transfers the USB device to the air-gapped computer and then back to the network again.

Figure 9. Different types of STRONTIUM components and filenames used during recently observed incidents



The STRONTIUM group also appears to be active on non-Windows systems.

Microsoft has seen solid indicators that STRONTIUM used malicious backdoors to take control of proxy servers, mail servers, and other systems running the Linux operating system. Microsoft also observed the group using domains that seem to be customized for different operating systems, including *mac.softupdates.info* and *linux.softupdates.info*. Although Microsoft does not generally study attacks on non-Windows systems, a multiplatform attack strategy is very much in line with what has been observed about STRONTIUM in general—that they have capabilities that cover a wide range of technologies—and any incident response against this adversary should take both Windows and non-Windows computers into consideration.

Taking action

The STRONTIUM backdoor can communicate over different network protocols, including HTTP, SMTP, and POP3. Typically, the backdoor tests its connectivity with a series of HTTP POST requests to legitimate websites, and then establishes communication with its C&C servers. The domains STRONTIUM uses for its C&C servers are typically designed to avoid attracting attention if administrators notice them when reviewing network traffic, such as *softupdates.info* and *malwarecheck.info*, suggestive of software update and malware reputation services.

> The domains STRONTIUM uses are designed to avoid attracting attention.

In recent incidents during 2015, Microsoft observed STRONTIUM using a tunnel component designed to provide a remote encrypted interactive shell to a pre-configured IP address using proxy software on the victim's computer, such as the popular open-source Squid proxy. The tunneling module, which is customized for different targets, is slightly larger than 1 MB and is statically linked with an OpenSSL library. Based on debug information left in some samples, some researchers have reported that the name of the component may be "XAPS OBJECTIVE" or "XTUNNEL."[4] The C&C server for this tunnel could be either hardcoded in the binary or passed as a command-line parameter at startup.

Figure 10. "XAPS" in the STRONTIUM tunnel module binary

```
000F9ED0  00 00 00 00 2E 65 78 65 00 00 00 00 43 00 4F 00  .....exe....C.O.
000F9EE0  4E 00 49 00 4E 00 24 00 00 00 00 00 31 23 51 4E  N.I.N.$.....1#QN
000F9EF0  41 4E 00 00 31 23 49 4E 46 00 00 00 31 23 49 4E  AN..1#INF...1#IN
000F9F00  44 00 00 00 31 23 53 4E 41 4E 00 00 52 53 44 53  D...1#SNAN..RSDS
000F9F10  3C F3 97 0F AB 5B A3 47 93 2A 3C FE 9E 9A F8 2D  <ó—.«[£G"*<þžšø-
000F9F20  01 00 00 00 43 3A 5C 55 73 65 72 73 5C 55 73 65  ....C:\Users\Use
000F9F30  72 5C 44 65 73 6B 74 6F 70 5C 78 61 70 73 5F 74  r\Desktop\xaps_t
000F9F40  68 72 6F 75 67 68 5F 73 71 75 69 64 5F 64 65 66  hrough_squid_def
000F9F50  61 75 6C 74 5F 70 72 6F 78 79 5C 52 65 6C 65 61  ault_proxy\Relea
000F9F60  73 65 5C 58 41 50 53 5F 4F 42 4A 45 43 54 49 56  se\XAPS_OBJECTIV
000F9F70  45 2E 70 64 62 00 00 00 00 00 00 00 00 00 00 00  E.pdb...........
000F9F80  00 00 00 00 00 D0 4F 00 8C AF 4F 00 00 00 00 00  .....ÐO.Œ¯O.....
```

Samples for this component include the items in the following table:

[4] Gastbeitrag, "Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag," Netzpolitik.org, June 19, 2015, https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/.

Figure 11. Known samples for the STRONTIUM XAPS tunnelling component

MD5 hash	SHA-1 hash	File name
800af1c9d341b846a856a1e686be6a3e	0450aaf8ed309ca6baf303837701b5b23aac6f05	svehost.dll
9d86ba47a0b876cdc7fb0c9ad471cd67	64515c7ce8bcc656d54182675bd2d9ffceffe845	svchosl.exe
1957f5370d584a2acd74179340ef3005	3ec270193815fa2bd853ea251d93fdfffcbc40d6	svehost.exe
f5a54476d3d05c8f0804f3d2d5818928	e5039bb420f9a3a23aaa9ee7392bd05dfee42540	svehost.exe
4ac8d16ff796e825625ad1861546e2e8	1535d85bee8a9adb52e8179af20983fb0558ccb3	servicehost.exe

After gaining a foothold on one computer, STRONTIUM attempts to move laterally through the organization by compromising additional computers to gain access to more data and high-value targets. STRONTIUM uses publicly available tools such as WinExe (a remote command-line execution tool) and Mimikatz (a Windows credential gathering tool) to move between computers via methods such as Pass the Hash (PtH). In recent incidents Microsoft observed STRONTIUM using a customized version of Mimikatz that was recompiled with a privilege escalation exploit (CVE-2015-1701, addressed by Security Bulletin MS15-051) and stored captured credential information in a dedicated file, *pi.log*.

Figure 12. A customized version of Mimikatz storing passwords in the file *pi.log*

```
00401C77 ; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE
00401C77 _WinMain@16     proc near               ; CODE XREF: __
00401C77
00401C77 var_8           = byte ptr -8
00401C77 var_4           = byte ptr -4
00401C77 hInstance       = dword ptr  8
00401C77 hPrevInstance   = dword ptr  0Ch
00401C77 lpCmdLine       = dword ptr  10h
00401C77 nShowCmd        = dword ptr  14h
00401C77
00401C77                 push    ebp
00401C78                 mov     ebp, esp
00401C7A                 push    ecx
00401C7B                 push    ecx
00401C7C                 cmp     dword_446984, 1
00401C83                 push    ebx
00401C84                 mov     ebx, offset off_446478
00401C89                 jnz     short loc_401C92
00401C8B                 push    offset aPi_log  ; "pi.log"
00401C90                 jmp     short loc_401C9A
```

STRONTIUM has displayed an advanced understanding of military and classified government networks, and uses a component that is designed to extract information from air-gapped computers. This module registers a device callback

via RegisterDeviceNotification[5] and receives a notification every time a USB mass storage device is inserted into a compromised computer. Depending on the variant deployed, the backdoor may simply harvest the entire contents of the USB device and save it on the local computer for later extraction, or it may also use Autorun malware to transfer itself to the device so that it can attempt to compromise any other computers it is later inserted into, including air-gapped computers.[6]

Figure 13. The device notification routine registered by a STRONTIUM USB module

```
004021FC 74 6E                          jz      short loc_40226C
004021FE 2D 17 02 00 00                 sub     eax, 217h       ; WM_DEVICECHANGE ?
00402203 56                             push    esi
00402204 8B 75 14                       mov     esi, [ebp+lParam]
00402207 57                             push    edi
00402208 8B 7D 10                       mov     edi, [ebp+wParam]
0040220B 75 4B                          jnz     short defwndproc_and_exit
0040220D 81 FF 00 80 00 00              cmp     edi, 8000h      ; DBT_DEVICEARRIVAL
00402213 75 43                          jnz     short defwndproc_and_exit
00402215 83 7E 04 02                    cmp     dword ptr [esi+4], 2
00402219 75 3D                          jnz     short defwndproc_and_exit
0040221B 0F B7 46 10                    movzx   eax, word ptr [esi+10h]
0040221F 83 F8 01                       cmp     eax, 1
00402222 74 34                          jz      short defwndproc_and_exit
00402224 83 F8 02                       cmp     eax, 2
00402227 74 2F                          jz      short defwndproc_and_exit
00402229 8B 4E 0C                       mov     ecx, [esi+0Ch]
0040222C 32 C0                          xor     al, al
0040222E 8B FF                          mov     edi, edi
00402230
00402230                        loopDrives:                     ; CODE XREF: pfunc_Window+4B↓j
00402230 F6 C1 01                       test    cl, 1
00402233 75 08                          jnz     short loc_40223D
00402235 FE C0                          inc     al
00402237 D1 E9                          shr     ecx, 1
00402239 3C 1A                          cmp     al, 26          ; Z:\
0040223B 7C F3                          jl      short loopDrives
0040223D
0040223D                        loc_40223D:                     ; CODE XREF: pfunc_Window+43↑j
0040223D 8D 4D 0C                       lea     ecx, [ebp+Msg]
00402240 51                             push    ecx
00402241 04 41                          add     al, 'A'         ; Drive Letter
```

Some STRONTIUM victims have reported the presence of computers running Kali Linux on their networks. Kali Linux is a Linux distribution that combines a variety of tools for the purpose of penetration testing and security assessment. It contains tools for password attacks, sniffing & spoofing, maintaining access, hardware hacking, reverse engineering, information gathering, vulnerability analysis, wireless attacks, web application attacks, stress testing, and forensic and

[5] See msdn.microsoft.com/library/windows/desktop/aa363431%28v=vs.85%29.aspx for more information about this function.

[6] Changes to the way the AutoRun feature works make it more difficult for this technique to succeed in recent versions of Windows. See blogs.technet.com/b/security/archive/2011/06/27/defending-against-autorun-attacks.aspx for more information.

exploitation analysis. The tool lists within each category are quite extensive and the distribution is actively maintained, so that STRONTIUM can always take advantage of the latest open-source tools. STRONTIUM does not deploy this Linux distribution on an existing computer that belongs to the targeted institution; rather, it uses a VPN connection to join one of its own Kali Linux computers to the victim's network, possibly using the tunnel component that was previously deployed. This approach allows STRONTIUM to only ephemerally expose its toolset to the victim's network.

Guidance

STRONTIUM is a very challenging adversary for a targeted institution to defend against: it possesses a broad range of technical exploitation capabilities, significant access to resources such as previously undiscovered zero-day exploits, and the determination to keep up an attack for months or years until it succeeds. Nevertheless, there are steps an organization can take to significantly reduce its attack surface and decrease the probability of a successful compromise.

STRONTIUM is a challenging adversary for a targeted institution to defend against.

- Stay up-to-date on vendor security updates and deploy them quickly after they are released. All of the exploits discussed in this section have been addressed by security updates from Microsoft and other vendors. STRONTIUM depends heavily on the presence of out-of-date software installations inside target institutions, so keeping software up-to-date denies the group the use of some of its most effective tools.
- Take advantage of the mitigations built into your software. Recent versions of Windows and other software include critical mitigations that render many of STRONTIUM's exploits ineffective when deployed. Figure 5 on page 8 lists a number of zero-day exploits that STRONTIUM has used in recent campaigns. Most of these exploits will fail if tried on a computer running the latest versions of Windows and Office, even without security updates that address the vulnerabilities:
  - The STRONTIUM exploits that target CVE-2015-1641 and CVE-2015-2424, which affect Microsoft Word and have been addressed by Security Bulletins MS15-033 and MS15-070 respectively, depend on static hard-coded ROP chains that fail when address space layout randomization

(ASLR) is enabled. Office 2013 and Office 2016 both run with ASLR enabled by default, rendering these exploits ineffective.

Figure 14. Snippet of the ROP chain used in the CVE-2015-2424 exploit; it fails against Office installations with ASLR enabled

```
szMarker        db 't00tt00t'
ROP             dd 7C809AF1h            ; kernel32!VirtualAlloc
                dd 771463EAh            ; ret addr
                dd 0D10000h             ; lpAddress
                dd 200000h              ; dwSize 0x200000
                dd 3000h                ; flAllocationType = MEM_COMMIT|MEM_RESERVE
                dd 40h                  ; flProtect = PAGE_EXECUTE_READWRITE
NOP_PADDDING    dd 90909090h
                dd 90909090h
                dd 90909090h
                dd 90909090h
; ---------------------------------------------------------------------------

Shellcode_Start:
                jmp     fist_jump
; ---------------------------------------------------------------------------

get_poc:                                ; CODE XREF: seg000:fist_jump↓p
                pop     esi             ; ESI = 100147F
                xor     ebx, ebx
                mov     bl, 67h
                xor     ecx, ecx
                mov     ecx, 51h
                mov     edi, esi

loc_100146F:                            ; CODE XREF: seg000:01001473↓j
                lodsb
                xor     al, bl
                stosb
                loop    loc_100146F
                jmp     dec_fist_stage
```

- The exploit targeting CVE-2015-3043, a vulnerability in Adobe Flash Player addressed by Adobe Security Bulletin APSB15-06, fails in Internet Explorer running on an up-to-date installation of Windows 8.1 or Windows 10 because of Control Flow Guard, a mitigation introduced in a Windows 8.1 security update in November 2014. Control Flow Guard mitigates virtual function hijacking attempts such as the one involving the cancel() method shown in Figure 15.

Figure 15. Snippet from the STRONTIUM ActionScript exploit code targeting CVE-2015-3043 in Adobe Flash Player, which fails against CFG mitigation

```
_loc_9 = _loc_7 * 4;
_loc_10 = readVectorInt(varVectorPoisoned, 0, _loc_9 + 32);
_loc_6 = (_loc_10 - _loc_9) - 24;
addrOfShellcode = _loc_6 + this.intOff1000;
_loc_11 = readVectorInt(varVectorPoisoned, 0, _loc_9 + 16);
_loc_13 = findRopGadgets(varVectorPoisoned, _loc_6, _loc_11);
_loc_14 = _loc_13[0] + 8;
_loc_15 = _loc_13[1] + 8;

writeVectorInt(varVectorPoisoned, 0, _loc_9 + 16, _loc_6 + 16);
writeVectorInt(varVectorPoisoned, 0, 0, 4096);
writeVectorInt(varVectorPoisoned, 0, 4, addrOfShellcode);
writeVectorInt(varVectorPoisoned, 0, 16, _loc_15);
writeVectorInt(varVectorPoisoned, 0, 28, _loc_14);

//try to call corrupted function pointer to trigger RCE
k = 0;
while(k < (varArrFileRef.length - 1))
{
    varArrFileRef[k].cancel();
    k++;
}
```

- The kernel vulnerabilities exploited by STRONTIUM (CVE-2015-1701, addressed by Security Bulletin MS15-051, and CVE-2015-2387, addressed by Security Bulletin MS15-077) could not work in Windows 8 and newer platforms running on hardware that supports Supervisor Mode Execution Protection (SMEP) and other kernel mitigations.[7] In fact, the exploit is coded to abort execution if running on an operating system other than Windows 7.

[7] See "Exploit Mitigation Improvements in Windows 8" (https://media.blackhat.com/bh-us-12/Briefings/M_Miller/BH_US_12_Miller_Exploit_Mitigation_Slides.pdf) for more information.

Figure 16. STRONTIUM's CVE-2015-1701 exploit terminates execution on the newest versions of Windows

```
getOSversion:
                lea     eax, [ebp+VersionInformation]
                push    eax             ; lpVersionInformation
                mov     [ebp+VersionInformation.dwOSVersionInfoSize], 114h
                call    ds:GetVersionExW
                test    eax, eax
                jz      short exit_EAX_ZERO

checkOSversion:                         ; win 6.1 = WINDOWS 7
                cmp     [ebp+VersionInformation.dwMajorVersion], 6
                jnz     short exit_EAX_ZERO ; skip if Windows 8 or above
                cmp     [ebp+VersionInformation.dwMinorVersion], 1
                jnz     short exit_EAX_ZERO ; skip if Windows 8 or above

setupEPROCESSoffsets:
                push    esi
                mov     const_00000036, 36h
                mov     const_0000002C, 2Ch
                mov     const_00000040, 40h
                mov     const_000000F8, 0F8h
                call    getPSlookupAPI_from_ntoskrnl
                xor     esi, esi
                mov     PsLookupProcessByProcessId, eax ; EAX=kernel func
                cmp     eax, esi
                jnz     short continueExploitation
                xor     eax, eax
                jmp     short pop_and_exit
; ---------------------------------------------------------------------------

exit_EAX_ZERO:                          ; CODE XREF: runThreadWIN32k_EOP+2C↑j
                                        ; runThreadWIN32k_EOP+35↑j ...
                xor     eax, eax
                jmp     short exit
```

- Enforce segregation of privileges on user accounts and apply all possible safety measures to protect Admin accounts from being compromised; STRONTIUM relies on pass-the-hash techniques and elevation of privileges to successfully move laterally across networks. See "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 2," available at the Microsoft Download Center, for more information.
- In enterprise environments in which isolated computer networks (air-gapped) and Internet connected networks co-exist, enforce strong policies to prevent sharing and usage of removable media across the air gap.
- Conduct enterprise software security awareness training, and build awareness about malware infection prevention. STRONTIUM heavily relies on social engineering to entice individual targets into clicking links to malware. Security training can raise awareness around this attack vector.
- Institute multi-factor authentication. As STRONTIUM extensively uses credential-stealing spear phishing attacks, multi-factor authentication can be an effective tool to prevent unauthorized access even if credentials are stolen.

- Prepare your network to be forensically ready, so that you can achieve containment and recovery if a compromise occurs. A forensically ready network that records authentications, password changes, and other significant network events can help to quickly identify affected systems.
- Keep personnel and personal data private. STRONTIUM uses open-source intelligence (OSINT) to obtain its initial lists of victims, which might include things like name and email address, but can expand into employment information and other items of interest. These are all pieces of information STRONTIUM can use to devise a realistic attack. The more information STRONTIUM has available, the better they can target you. Make sure your email is kept confidential and privacy settings on social media don't disclose sensitive information publicly.

Focus on Brazil:

Win32/Banload and Banking Malware

Online banking is big business in Brazil, where more than half of all banking transactions have been made using Internet-connected devices in recent years.[8] Unfortunately, the popularity of online banking in Brazil has drawn the attention of criminals, who have made the country a world capital for banking malware for the last several years.

Win32/Banload, the most commonly encountered malware family in Brazil in 2Q15, is a generic detection for threats that download malware designed to steal banking credentials, which themselves are usually identified as other threats. (Encounter rates for these related threats are generally much lower than for Banload, in part because Microsoft real-time security products block Banload variants before they can download additional malware; therefore, examining Banload encounter rates is a useful proxy for understanding the banking malware problem in general.) Together, Banload and its related families have been a major part of the malware problem in Brazil for nearly ten years.

> Criminals have made Brazil a world capital for banking malware for the last several years.

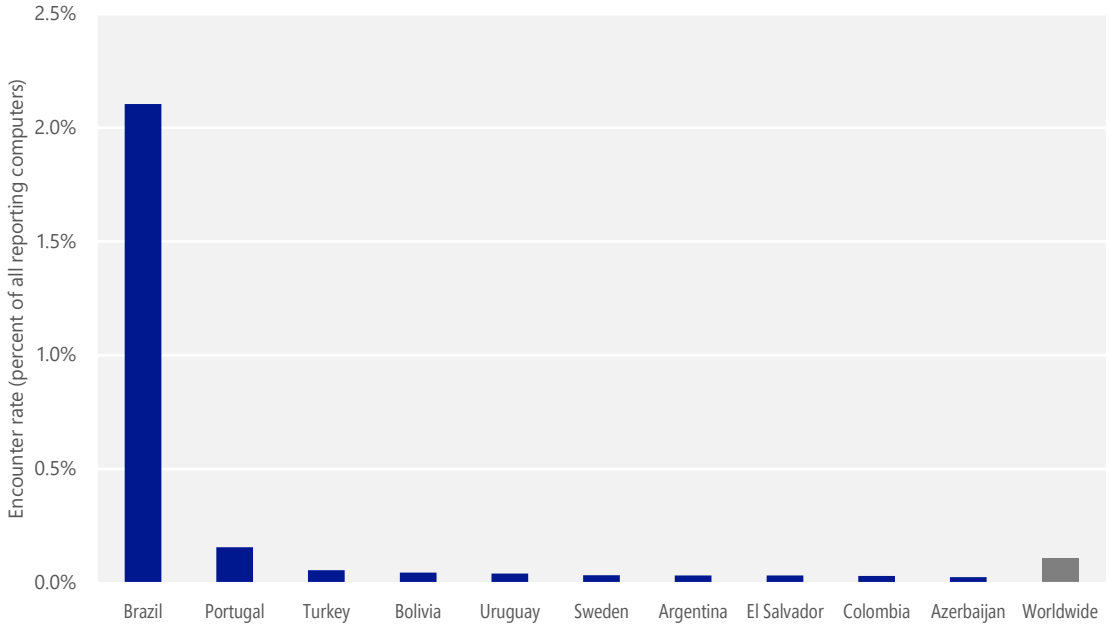
Distribution and trends

Although some variants have been found to target banks elsewhere, Banload remains an almost exclusively Brazilian threat. More than 93 percent of Banload encounters in 2Q15 occurred in Brazil, and the encounter rate for Banload in Brazil was 2.1 percent in 2Q15, compared to 0.16 percent in Portugal, the location with the second highest Banload encounter rate. While Banload was the

[8] Michael Oleaga, "Online Banking Growing in Brazil: More Than Half Made Digital Transactions in 2013," *Latin Post*, April 2, 2014, http://www.latinpost.com/articles/9959/20140402/online-banking-growing-brazil-more-half-made-digital-transactions.htm.

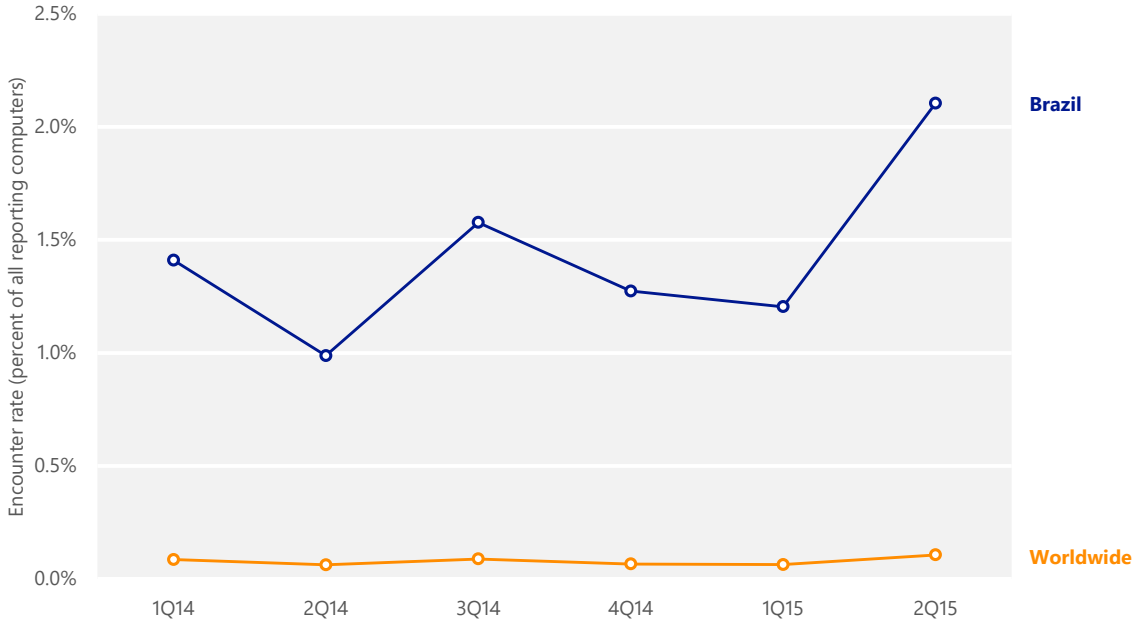
most commonly encountered threat family in Brazil in 2Q15, it ranked just 39th worldwide.

Figure 17. The top ten countries/regions encountering Win32/Banload in 2Q15



Banload has consistently been encountered at much higher rates in Brazil than in the rest of the world. Over the past six quarters the encounter rate for Banload in Brazil has fluctuated between 1.0 percent and 2.1 percent, while the worldwide Banload encounter rate has ranged between 0.06 percent and 0.11 percent. Despite a generally rising trend that accelerated in 2Q15, the fluctuations shown in Figure 18 are fairly typical for Banload and do not necessarily presage significantly increased encounter rates in the future.

Figure 18. Banload encounter rate trends worldwide and in Brazil, 1Q14–2Q15



Propagation and technical details

Threats detected as Banload are created and distributed by many different parties, who may have little or no connection to each other. Most variants operate in similar ways. Banload might be installed by other malware, or use social engineering to trick the user into launching it. After it is installed, it contacts a remote host and downloads additional files, which then attempt to steal banking credentials and transmit them back to the attacker. Banload variants have been observed to connect to many different remote hosts, including malicious sites as well as legitimate sites that have been compromised. As with many other malware families, the hosts are not confined to any particular region; attackers typically establish malicious hosts wherever a vulnerable server can be found to compromise.

> Many Banload variants attempt to disable security products installed on the computer.

Some Banload variants check the configured system language upon installation and only download additional files if it is set to Portuguese. Although Banload usually does not attempt to steal banking credentials itself, many variants transmit other details about the computer environment to the attacker, such as the computer name, user name, and Windows version.

Many Banload variants attempt to disable security products installed on the computer, including G-Buster Browser Defense, a browser add-on that many large Brazilian banks provide to their customers to protect banking sessions from malware. Some variants modify the registry so that Banload will automatically launch each time the computer is started.

Win32/Banker and credential stealers

The malware threats downloaded by Banload variants are often detected as Win32/Banker and Win32/Bancos. Banker and Bancos are generic detections for data-stealing trojans that capture online banking credentials, such as account names and passwords, and relay the captured information to a remote attacker. As with Banload, these threats are created by many different people who often have no connection to each other apart from their common purpose of stealing banking credentials. Banker and Bancos variants typically monitor browser activity for banking sessions involving large and well-known Brazilian banks, including:

- Banco Bradesco (*bradesco.com.br*)
- Banco do Brasil (*bb.com.br*)
- Banco do Estado do Rio Grande do Sul (*banrisul.com.br*)
- Banco Itaú (*itau.com.br*)
- Banco Safra (*safra.com.br*)
- Banco Santander (*santander.com.br*)
- Caixa Econômica Federal (*caixa.gov.br*)
- Citibank (*citibank.com.br*)
- HSBC (*hsbc.com.br*)

As with Banload, many Banker and Bancos variants attempt to disable security products installed on the computer, including G-Buster Browser Defense, and modify the registry so the malware will automatically launch each time the computer is started.

Win32/BrobanDel and boleto malware

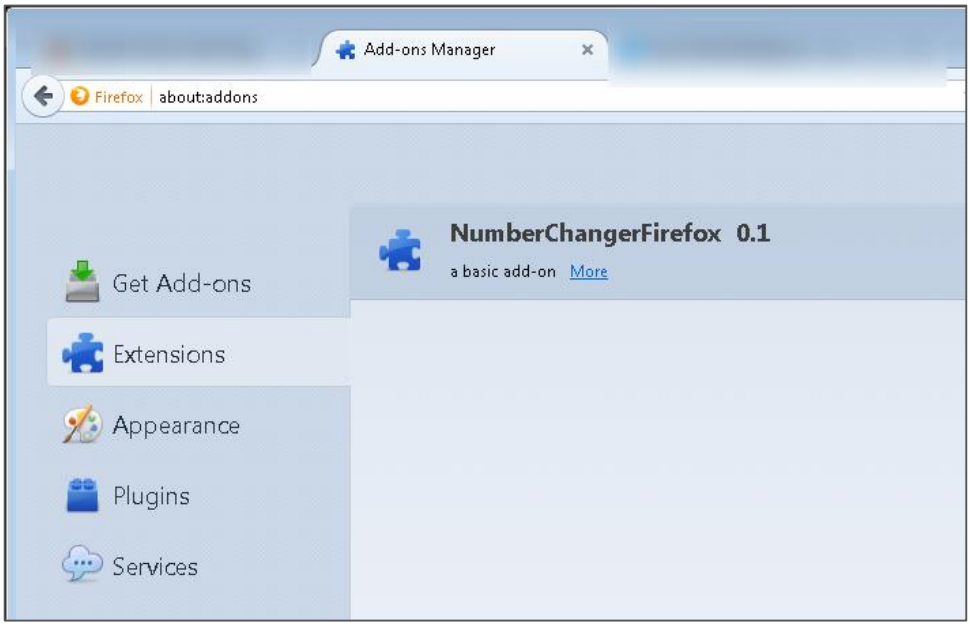
Another type of banking malware that has affected Brazil recently targets *boletos bancários*, a popular payment method there. A boleto bancário, usually simply called a boleto, is a payment order generated by a merchant or other

payee, similar to an invoice. Boletos are popular in Brazil because they provide a mechanism for people to pay bills or other debts without having a bank account; they can be paid in cash at a wide range of locations, including banks, post offices, and supermarkets. In recent years, online boletos have become popular: payers receive them over the Internet and can either pay them electronically from a bank account or can print them out for payment like conventional paper boletos. It is these online boletos that have been targeted by a new type of banking malware.

Figure 19. An example of a boleto bancário, a popular method of payment in Brazil

Every boleto has a unique identification number that specifies the bank, payee, and amount to be paid, among other information. The identification number is printed at the top of the boleto and encoded as a barcode at the bottom. A typical boleto malware variant (often detected as Win32/BrobanDel) installs itself as a browser add-on and monitors webpages for patterns that match a boleto. When it identifies a boleto, it alters the identification number so that when the recipient pays it, the money will be paid into an account controlled by the attacker, rather than the payee's account. The malware may re-encode the barcode to match the altered number, or simply corrupt it so that it cannot be optically scanned, requiring the cashier to enter the identification number by hand.

Figure 20. A malicious extension installed by Win32/BrobanDel to detect and alter boletos



New variants of Banload and the other families discussed in this section are discovered every day, and variants discovered in the future may exhibit different behaviors than those described here. Visit the Microsoft Malware Protection Center encyclopedia at https://www.microsoft.com/mmpc for the latest information about this and other threats.

Guidance

Effectively protecting users from malware requires an active effort on the part of organizations and individuals. For in-depth guidance, see "Top security solutions" at the Microsoft Malware Protection Center website at www.microsoft.com/mmpc.

Specific steps that IT administrators and individual users can take to protect themselves from malware include the following:

- Install security updates for all software as soon as is practical. Promptly installing security updates remains one of the best ways to defend against newly discovered threats.
- Configure computers to use Microsoft Update rather than Windows Update to automatically receive updates for a wide range of Microsoft products. Ensure that security updates from other software vendors are distributed automatically when possible.

- Install a comprehensive, real-time antimalware product from a reputable vendor on all of your organization's computers, and ensure that they receive frequent, regular definition or signature file updates.
- Take advantage of advanced Windows security features such as User Account Control and AppLocker to prevent unauthorized programs from running without permission.
- Use caution when clicking links to webpages and when opening attachments to email messages.
- Use a web browser such as Internet Explorer or Microsoft Edge that offers advanced protection against phishing and malicious webpages.

Worldwide threat assessment

Vulnerabilities

Vulnerabilities, in the context of computer security, are weaknesses in software that could allow an attacker to compromise the integrity, availability, or confidentiality of the software. 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

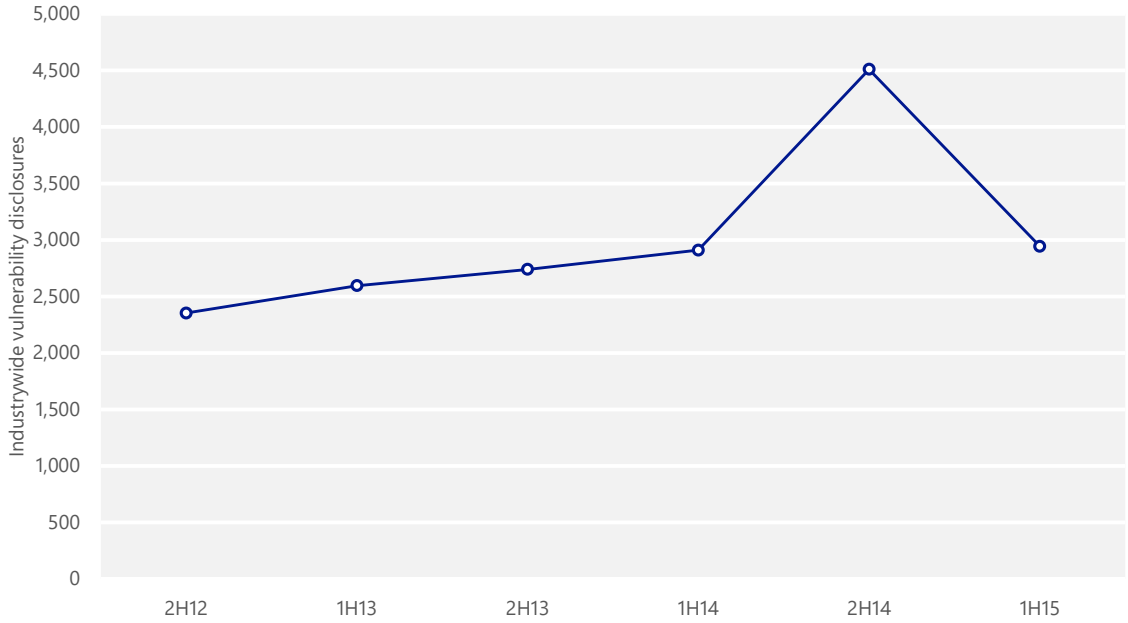
A *disclosure*, as the term is used in the *Microsoft Security Intelligence Report*, is the revelation of a software vulnerability to the public at large. Disclosures can come from a variety of sources, including publishers of the affected software, security software vendors, independent security researchers, 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.[9]

Figure 21 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 2H12. (See "About this report" on page v for an explanation of the reporting period nomenclature used in this report.)

[9] 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 21. Industrywide vulnerability disclosures, 2H12–1H15



- After increasing significantly in 2H14, vulnerability disclosures across the industry decreased 34.7 percent in 1H15 to just under 3,000, very close to the level seen a year previously in 1H14.
- The large increase in disclosures in 2H14 was predominantly the result of work performed by the Computer Emergency Response Team (CERT) Coordination Center (CERT/CC) in September and October 2014 to scan Android applications in the Google Play Store for man-in-the-middle vulnerabilities using an automated tool.[10] CERT/CC determined that thousands of Android apps fail to properly validate SSL certificates provided by HTTPS connections, which could allow an attacker on the same network as an Android device to perform a man-in-the-middle attack on the device.[11] This project resulted in the creation of almost 1400 individual CVEs affecting thousands of different publishers of Android apps and code libraries. With no comparable research projects having been undertaken in 1H15, the total number of disclosures returned to a more typical level, as expected.

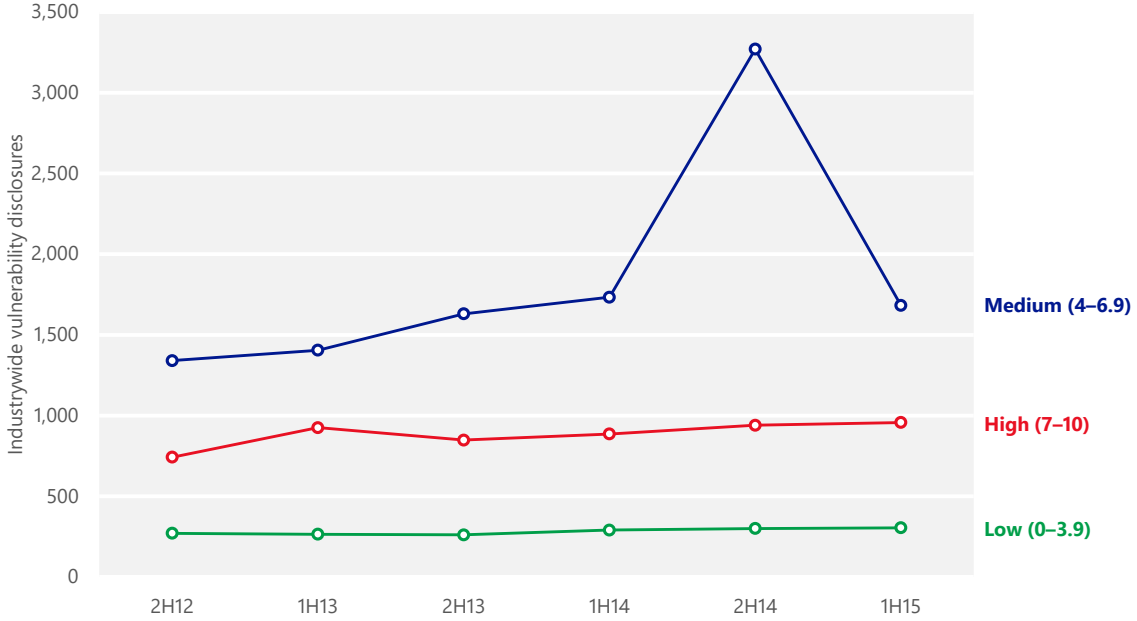
---

[10] Will Dormann, "Finding Android SSL Vulnerabilities with CERT Tapioca," *Cert/CC Blog*, September 3, 2014, www.cert.org/blogs/certcc/post.cfm?EntryID=204.
[11] CERT Coordination Center, "Vulnerability Note VU#582497: Multiple Android applications fail to properly validate SSL certificates," *Vulnerability Notes Database*, www.kb.cert.org/vuls/id/582497.

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 A Complete Guide to the Common Vulnerability Scoring System Version 2.0 at first.org for more information.)

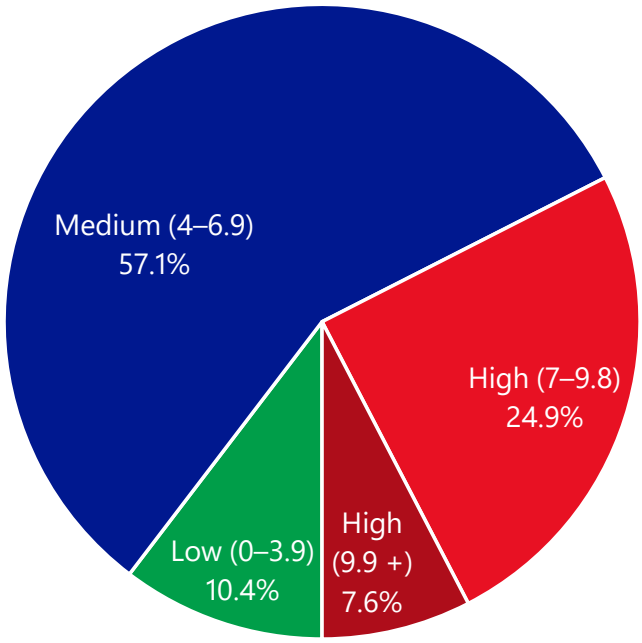
Figure 22. Industrywide vulnerability disclosures by severity, 2H12–1H15



- Disclosures of medium-severity vulnerabilities—those with CVSS scores from 4 to 7.9—dropped by nearly half from 2H14, but remained the most common type of vulnerability in 1H15. A research project in 2H14 uncovered SSL vulnerabilities in a large number of Android apps in the Google Play store, explaining the rise and subsequent fall of medium-severity vulnerabilities. (See page 32 for more information about this project.)
- By contrast, the number of disclosures of high-severity and low-severity vulnerabilities remained mostly stable, with both categories increasing by less than 2 percent from 1H14 to 2H14. High-severity vulnerabilities accounted for the second-highest share of vulnerability disclosures in 1H15, at 32.5 percent, and low-severity vulnerabilities accounted for the smallest share, at 10.4 percent.

- As shown in Figure 23, the highest-severity vulnerabilities—those scoring 9.9 or higher on the CVSS scale—accounted for 7.6 percent of all vulnerabilities in 1H15.

Figure 23. Industrywide vulnerability disclosures in 1H15, by severity

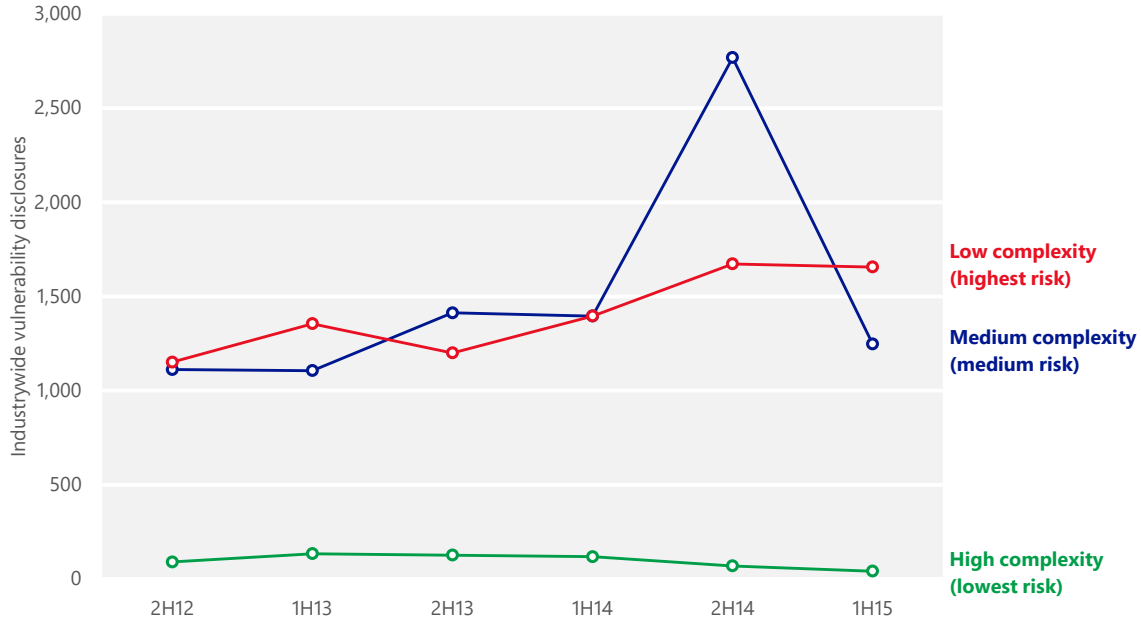


Vulnerability complexity

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 A Complete Guide to the Common Vulnerability Scoring System Version 2.0 at first.org for more information about the CVSS complexity ranking system.) Figure 24 shows complexity trends for vulnerabilities disclosed since 2H12. Note that Low complexity in Figure 24 indicates greater risk, just as High severity indicates greater risk in Figure 22.

Figure 24. Industrywide vulnerability disclosures by access complexity, 2H12–1H15



- Disclosures of low-complexity vulnerabilities—those that are the easiest to exploit—decreased slightly in 1H15, but accounted for the largest category of disclosures, at 56.3 percent of all disclosures.
- Medium-complexity vulnerabilities decreased 54.9 percent from 2H14 to 1H15 to account for 42.4 percent of all vulnerabilities for the period. A research project in 2H14 uncovered SSL vulnerabilities in a large number of Android apps in the Google Play Store, explaining the increase and subsequent decrease of medium-complexity vulnerabilities. (See page 32 for more information about this project.)

> A research project in 2H14 uncovered SSL vulnerabilities in a large number of Android apps.

- Disclosures of high-complexity vulnerabilities decreased slightly in 1H15, and accounted for 1.0 percent of all disclosures for the period.

Operating system, browser, and application vulnerabilities

Comparing vulnerabilities that affect a computer's operating system to vulnerabilities that affect other components, such as applications and utilities, requires a determination of whether the affected component is considered part of the 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.

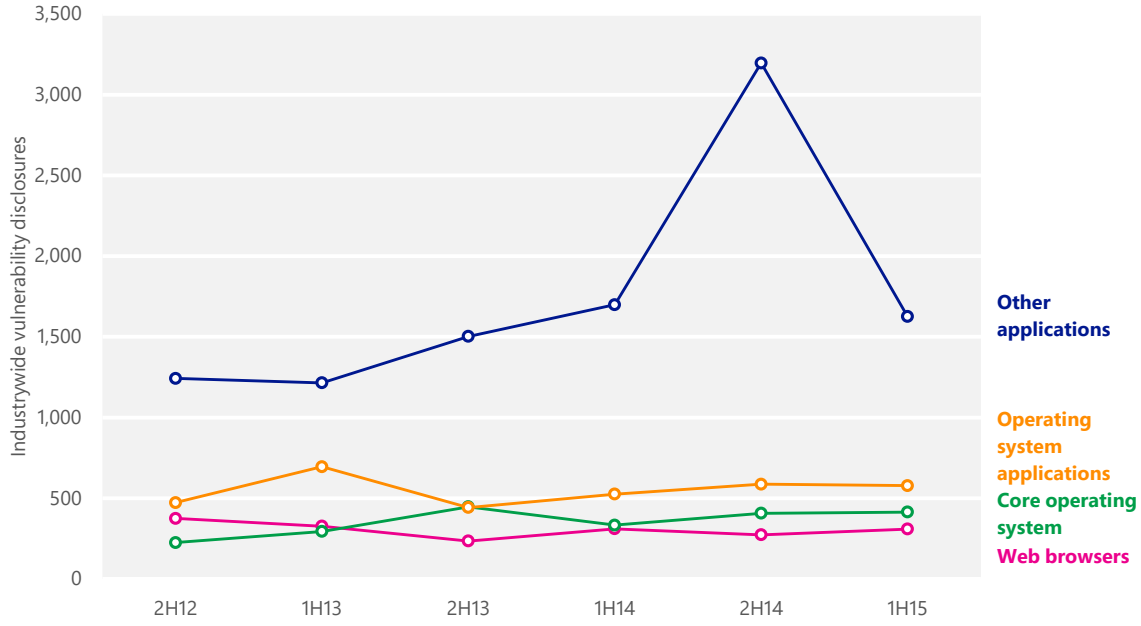
To facilitate analysis of operating system and browser vulnerabilities, the *Microsoft Security Intelligence Report* distinguishes among four different kinds of vulnerabilities:

- *Core operating system vulnerabilities* are those with at least one operating system platform enumeration ("/o") in the NVD that do not also have any application platform enumerations ("/a").[12]
- *Operating system application vulnerabilities* are those with at least one /o platform enumeration and at least one /a platform enumeration listed in the NVD, except as described in the next bullet point.
- *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.
- *Other application vulnerabilities* are those with at least one /a platform enumeration in the NVD that do not have any /o platform enumerations, except as described in the previous bullet point.

Figure 25 shows industrywide vulnerabilities for operating systems, browsers, and applications since 2H12.

[12] See nvd.nist.gov/cpe.cfm for information about the Common Platform Enumeration (CPE) standard for naming information technology systems, software, and packages.

Figure 25. Industrywide operating system, browser, and application vulnerabilities, 2H12–1H15

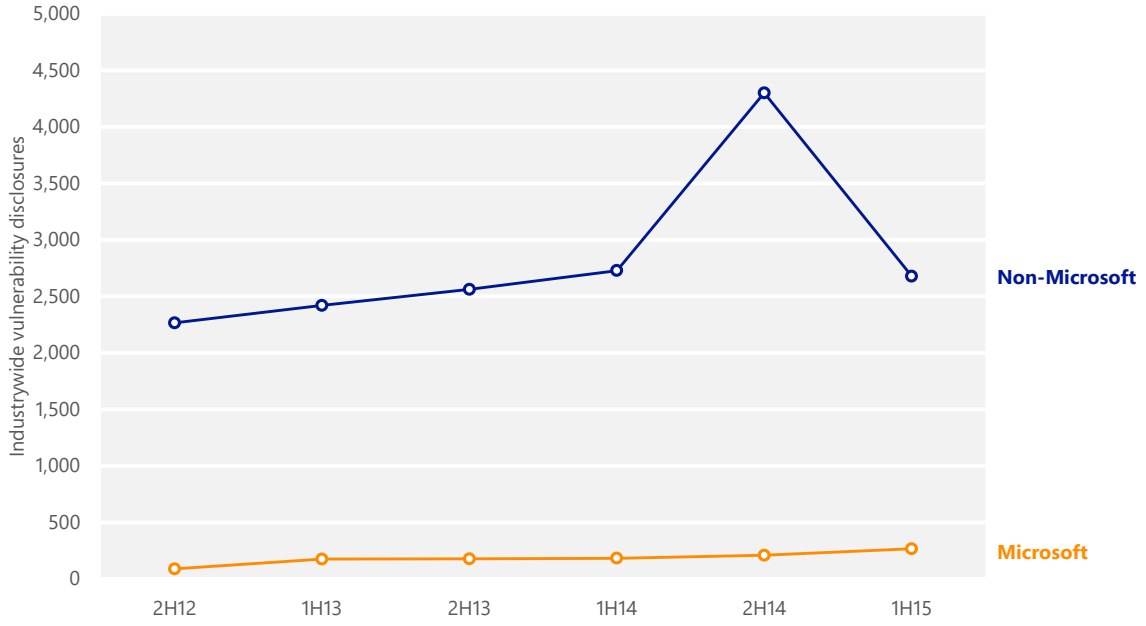


- Disclosures of vulnerabilities in applications other than web browsers and operating system applications decreased by nearly half from 2H14 to 1H15, but remained the most common type of vulnerability in 1H15, accounting for 55.6 percent of all disclosures for the period. A research project in 2H14 uncovered SSL vulnerabilities in a large number of Android apps in the Google Play Store, explaining the increase and subsequent decrease of application vulnerabilities. (See page 32 for more information about this project.)
- Operating system application vulnerability disclosures decreased 1.5 percent from 2H14, and accounted for 19.7 percent of all disclosures in 1H15.
- Core operating system vulnerability disclosures increased 1.7 percent from 2H14, and accounted for 14.1 percent of all disclosures in 1H15.
- Browser vulnerability disclosures increased 13.2 percent from 2H14, and accounted for 10.6 percent of all disclosures in 1H15.

Microsoft vulnerability disclosures

Figure 26 shows trends for vulnerability disclosures affecting Microsoft products compared to the rest of the industry.

Figure 26. Vulnerability disclosures for Microsoft and non-Microsoft products, 2H12–1H15



- Microsoft vulnerability disclosures increased from 209 disclosures in 2H14 to 266 in 1H15, an increase of 27.3 percent.

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 discovered after deployment.

"Life in the Digital Crosshairs," at sdlstory.com, is a multimedia presentation that explores the genesis and development of the SDL from its origins in the Windows team's well-documented all-hands security push in the early 2000s. It includes interviews with several of the pivotal figures in the history of the SDL and Microsoft's focus on secure software. Security professionals and anyone else with an interest in secure development are likely to find the site invaluable for putting the SDL into historical context and understanding what the future holds.

To learn more about how the SDL is applied in the present day, 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 organizations 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).

Exploits

An *exploit* is a piece of code that uses software vulnerabilities to access information on a computer or install malware. Exploits target vulnerabilities in operating systems, web browsers, applications, or software components that are installed on a computer.

In some scenarios, targeted components are add-ons that may be 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.[13]

Encounter rate is the percentage of computers running Microsoft real-time security products that report a malware encounter.

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.[14]

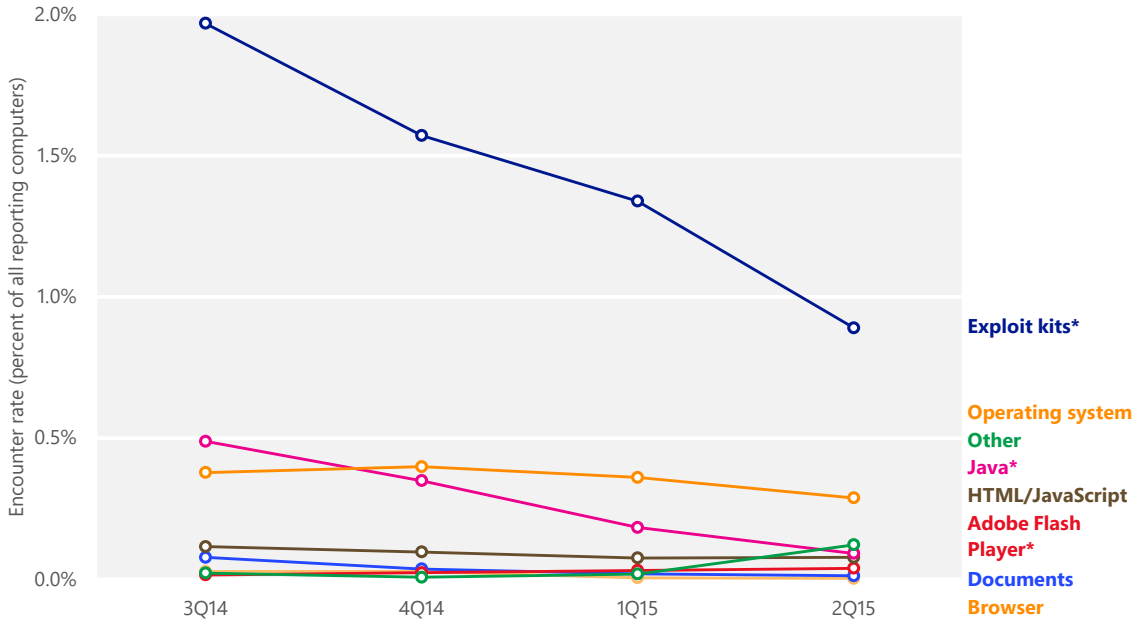
Microsoft real-time security products can detect and block attempts to exploit known vulnerabilities whether the computer is affected by the vulnerabilities or not. For example, the CVE-2010-2568 CplLnk vulnerability has never affected Windows 8, but if a Windows 8 user receives a malicious file that attempts to exploit that vulnerability, Windows Defender is designed to detect and block it anyway. Encounter data provides important information about which products and vulnerabilities are being targeted by

[13] See the Microsoft Security Update Guide, Second Edition at the Microsoft Download Center (www.microsoft.com/download) for guidance to help protect your IT infrastructure while creating a safer, more secure computing and Internet environment.
[14] See technet.microsoft.com/security/bulletin to search and read Microsoft Security Bulletins.

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 27 shows the prevalence of different types of exploits detected by Microsoft antimalware products from 3Q14 to 2Q15, by encounter rate. *Encounter rate* is the percentage of computers running Microsoft real-time security products that report a malware encounter. For example, the encounter rate for Java exploit attempts in 2Q15 was 0.35 percent, meaning that 0.35 percent of computers running Microsoft real-time security software in 2Q15 encountered Java exploit attempts, and 99.65 percent did not. In other words, a computer selected at random would have had about a 0.35 percent chance of encountering a Java exploit attempt in 2Q15. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[15] See page 58 for more information about the encounter rate metric.

Figure 27. Encounter rates for different types of exploit attempts, 3Q14–2Q15



* Figures for exploit kits, Java, and Adobe Flash Player exploits are affected by IExtensionValidation in Internet Explorer, which blocks many threats before they are encountered. See page 55 for more information.

[15] For information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 129.

- Computers that report more than one type of exploit are counted for each type detected.
- Encounters with exploit kits decreased by more than a third between 4Q14 and 2Q15, but remained the most commonly encountered type of exploit in the second half of the year, with an encounter rate more than three times as high as the next most common type of exploit. See "Exploit kits" on page 44 for more information about these exploits.

Encounters with exploit kits decreased by more than a third, but remained the most commonly encountered type of exploit in 2H15.

- The number of encounters with exploits that target operating systems remained mostly stable in 1H15, becoming the second most commonly encountered type of exploits during the period. See "Operating system exploits" on page 49 for more information.
- Encounters with Java exploits decreased each quarter, becoming the third most commonly encountered type of exploit in 1H15. See "Java exploits" on page 47 for more information.
- The "Other" category increased from very low levels in 1Q15 and previous periods to become the third most commonly encountered exploit category in 2Q15, mostly because of encounters involving Win32/Sdbby. Sdbby is a generic detection for malware that bypasses the User Account Control (UAC) prompt to gain administrative privileges on a computer. It was encountered at very low volumes in 1Q15, then became the fourth most commonly encountered exploit family in 2Q15.
- The number of encounters involving other types of exploits remained mostly stable during the second half of the year, and each accounted for a small percentage of total exploits.

Exploit families

Figure 28 lists the exploit-related malware families that were detected most often during the first half of 2015.

Figure 28. Quarterly encounter rate trends for the exploit families most commonly detected and blocked by Microsoft real-time antimalware products in 1H15, shaded according to relative prevalence

Exploit	Type	3Q14	4Q14	1Q15	2Q15
JS/Axpergle	Exploit kit	0.87%	0.86%	0.85%	0.64%
CVE-2010-2568 (CplLnk)	Operating system	0.35%	0.35%	0.30%	0.23%
JS/Fiexp	Exploit kit	0.31%	0.30%	0.21%	0.05%
Win32/Anogre	Exploit kit	0.60%	0.42%	0.22%	0.04%
JS/Neclu	Exploit kit	0.11%	0.06%	0.03%	0.14%
HTML/IframeRef	Generic	0.10%	0.09%	0.07%	0.05%
HTML/Meadgive	Exploit kit	0.15%	0.08%	0.06%	0.05%
JS/NeutrinoEK	Exploit kit	0.00%	0.01%	0.07%	0.04%
Win32/Sdbby	Other	—	—	0.00%	0.09%
CVE-2014-6332	Operating system	—	0.03%	0.04%	0.05%

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

- Exploit kits accounted for six of the 10 most commonly encountered exploits during 1H15. See "Exploit kits" on page 44 for more information about exploit kits.
- Exploits targeting the Java Runtime Environment (JRE) have gone from seven of the top 10 individual exploits detected in 2H13 to none in 1H15. A number of changes that were made to Java and Internet Explorer over the past two years have made it much more difficult for attackers to take advantage of Java-based vulnerabilities, which is the most likely explanation for this significant decrease. (See "Java exploits" on page 47 for more information.)
- CVE-2010-2568, the most commonly targeted individual vulnerability in 1H15, is a vulnerability in Windows Shell. Detections are often identified as variants in the Win32/CplLnk family, although several other malware families attempt to exploit the vulnerability as well. An attacker exploits CVE-2010-2568 by creating a malformed shortcut file—typically distributed through social engineering or other methods—that forces a vulnerable computer to load a malicious file when the shortcut icon is displayed in Windows Explorer. The vulnerability was first discovered being used by the malware family Win32/Stuxnet in mid-2010, and it has since been exploited by a number of other families, many of which predated the disclosure of the vulnerability and were subsequently adapted to attempt to exploit it. Microsoft published Security Bulletin MS10-046 in August 2010 to address

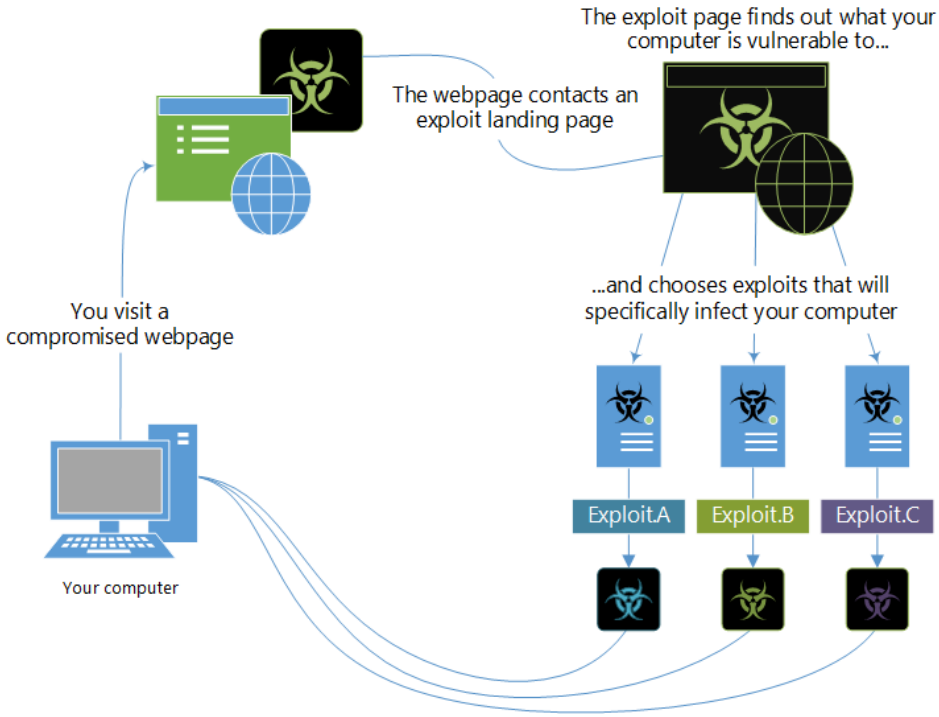
the issue, and Windows 8 and Windows 8.1 have never been vulnerable to exploits of CVE-2010-2568.

- HTML/IframeRef 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 inline frames might be changed frequently.
- CVE-2014-6332 is a vulnerability in Windows Object Linking and Embedding (OLE) that can be used to launch remote attacks on a computer through Internet Explorer in some circumstances. Microsoft released Security Bulletin MS14-064 in November 2014 to address this issue. See "The life and times of an exploit" on pages 3–10 of *Microsoft Security Intelligence Report, Volume 18 (July–December 2014)*, available from the Microsoft Download Center, for more information about this vulnerability and what Microsoft has done to mitigate it.

Exploit kits

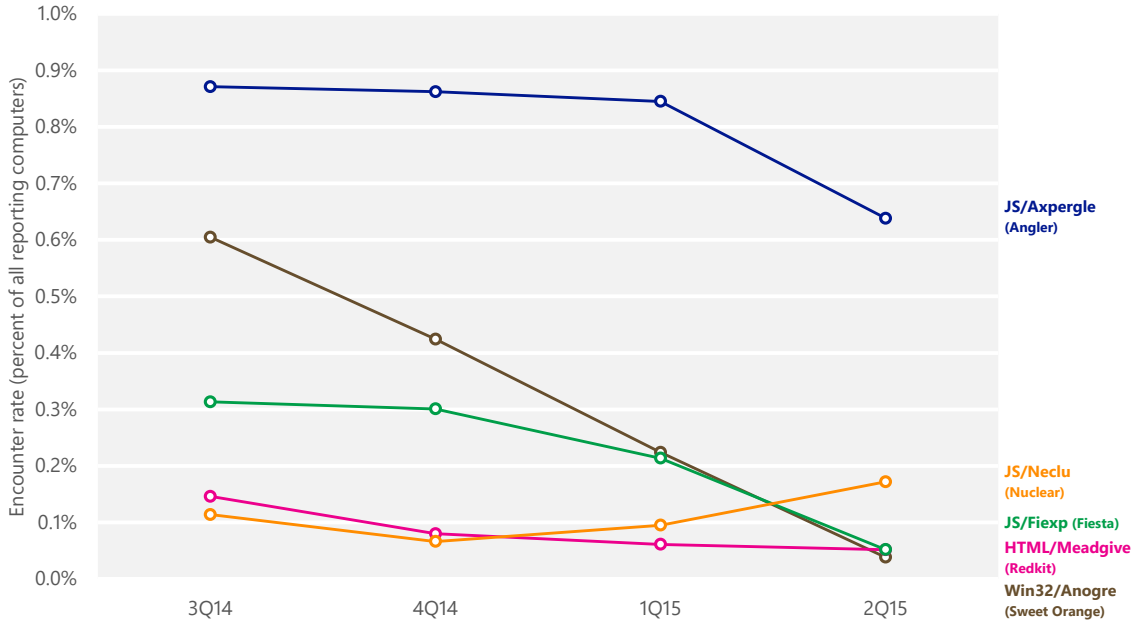
Exploit kits are collections of exploits bundled together and sold as commercial software or as a service. Prospective attackers buy or rent exploit kits on malicious hacker forums and through other illegitimate outlets. A typical kit comprises a collection of webpages that contain exploits for several vulnerabilities in popular web browsers and browser add-ons. When the attacker installs the kit on a malicious or compromised web server, visitors who don't have the appropriate security updates installed are at risk of having their computers compromised through drive-by download attacks. (See page 105 for more information about drive-by downloads.)

Figure 29. How a typical exploit kit works



Microsoft security products detect and block the characteristic techniques that a number of common exploit kits use to infect computers, along with several generic HTML and JavaScript exploit techniques. Figure 30 shows the prevalence of several top web-based exploit kits and techniques during each of the four most recent quarters.

Figure 30. Trends for the top exploit kit-related threats detected and blocked by Microsoft real-time antimalware products in 1H15



- JS/Axpergle, a detection for the so-called Angler exploit kit, was the most commonly encountered exploit kit family in 1H15. The Angler kit first appeared in 3Q14 and rapidly increased in prominence during the second quarter. It is known to target a number of vulnerabilities in Silverlight (CVE-2013-0074), Internet Explorer (CVE-2013-2551), Adobe Flash Player (CVE-2014-8439, CVE-2015-0311, and CVE-2015-0313, among others), and Java (CVE-2013-2460), although exploit kit authors frequently change the exploits included in their kits in an effort to stay ahead of software publishers and security software vendors.

- After decreasing to low levels in 2H14, detections of the Nuclear exploit kit (detected as JS/Neclu) reversed course and began trending upward in 2015, making it the second most commonly encountered exploit kit in 2Q15.

- Encounters involving the Sweet Orange and Fiesta exploit kits (detected as Win32/Anogre and JS/Fiexp, respectively), the second and third most commonly encountered exploit kits in 2H14, decreased to much lower levels in 1H15.

Exploit kit authors update the exploits they use frequently, adding exploits for newly discovered vulnerabilities while dropping poorly performing ones.

Exploit kit authors update the exploits they use frequently, adding exploits for newly discovered vulnerabilities while dropping poorly performing ones. Figure

31 lists some of the exploits that researchers have observed being added to a number of prominent exploit kits in 1H15.

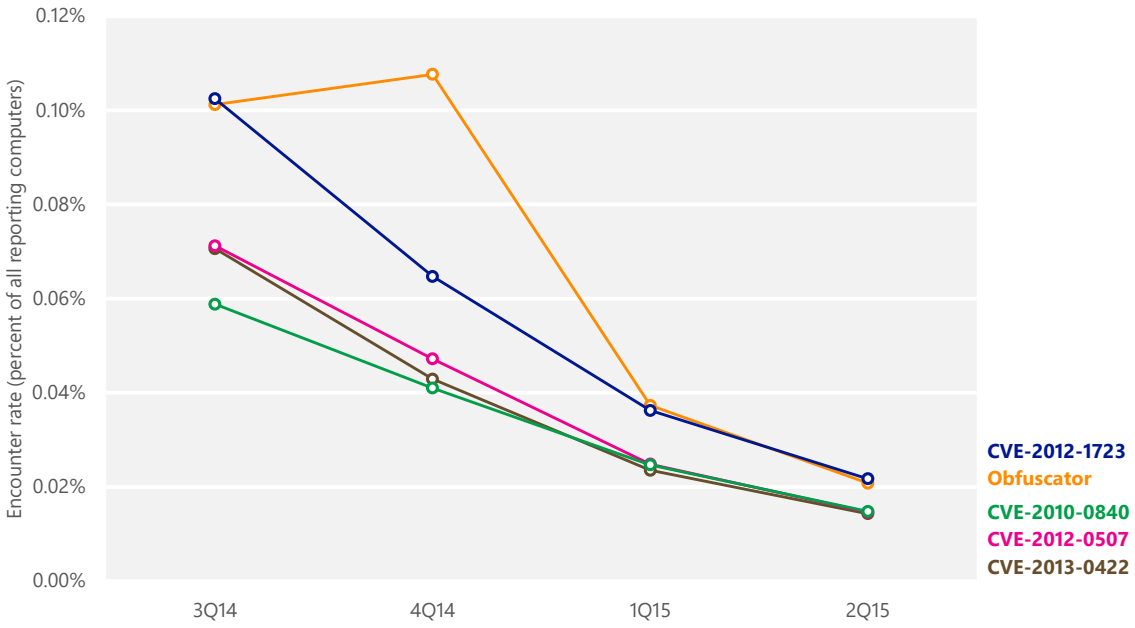
Figure 31. Newly discovered exploits observed being used by exploit kits in 1H15

Vulnerability	Exploit type	Addressed by	Exploit kit(s)
CVE-2015-0310	Adobe Flash Player	APSB15-02	Angler (JS/Axpergle)
CVE-2015-0311	Adobe Flash Player	APSB15-03	Angler
CVE-2015-0313	Adobe Flash Player	APSB15-04	Angler
CVE-2015-0336	Adobe Flash Player	APSB15-05	Nuclear (JS/Neclu); Angler
CVE-2015-0359	Adobe Flash Player	APSB15-06	Angler
CVE-2015-3090	Adobe Flash Player	APSB15-09	Angler
CVE-2015-3104	Adobe Flash Player	APSB15-11	Angler
CVE-2015-3105	Adobe Flash Player	APSB15-11	Magnitude (HTML/Pangimop)
CVE-2015-3113	Adobe Flash Player	APSB15-14	Magnitude

Java exploits

Figure 32 shows the prevalence of different Java exploits by quarter.

Figure 32. Trends for the top Java exploits detected and blocked by Microsoft real-time antimalware products in 1H15

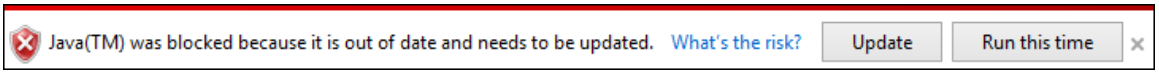


- Overall, encounters with Java exploits continued to decrease significantly in 1H15. This decrease is likely caused by several important changes in the way web browsers evaluate and execute Java applets:
  - The IExtensionValidation interface in Internet Explorer 11, released in late 2013, provides a mechanism for security software to validate that a webpage is safe before allowing instantiation of ActiveX controls, such as the control that hosts embedded Java applets. If a webpage is determined to be malicious, the ActiveX controls are blocked from loading, and the actual Java exploit itself is therefore never encountered. (See "Exploit detection with Internet Explorer and IExtensionValidation" on page 55 for more information.) Subsequent Internet Explorer security updates released in 2014 added an isolated heap mechanism and a deferred-free method to mitigate use-after-free bugs, which further hardened Internet Explorer against Java exploitation.
  - Beginning with Java 7 update 51, released in January 2014, the Java Runtime Environment (JRE) requires Java applets running in web browsers to be digitally signed by default.

IExtensionValidation in Internet Explorer 11 provides a mechanism for security software to validate that a webpage is safe before allowing instantiation of ActiveX controls.

- In September 2014, Microsoft published updates for versions 8 through 11 of Internet Explorer to begin blocking out-of-date ActiveX controls, including controls that host older versions of the JRE in the browser. As explained in this section, the most commonly encountered Java exploits all target vulnerabilities that were addressed with security updates years ago, but remain present in out-of-date Java installations. When a webpage attempts to load one of the vulnerable versions of Java in Internet Explorer with the update applied, the control is blocked by default and the user is urged to update Java to a more secure version.

Figure 33. Internet Explorer blocks out-of-date ActiveX controls from running



- CVE-2012-1723, the most commonly encountered individual Java exploit in 2Q15 and the second most common in 1Q15, is a type-confusion vulnerability in the Java Runtime Environment (JRE) that 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 addressed it

the same month with its June 2012 Critical Patch Update. The vulnerability was observed being exploited in the wild beginning in early July 2012, and has been used in a number of exploit kits.

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

> Internet Explorer has begun blocking out-of-date ActiveX controls, including controls that host older versions of the JRE in the browser.

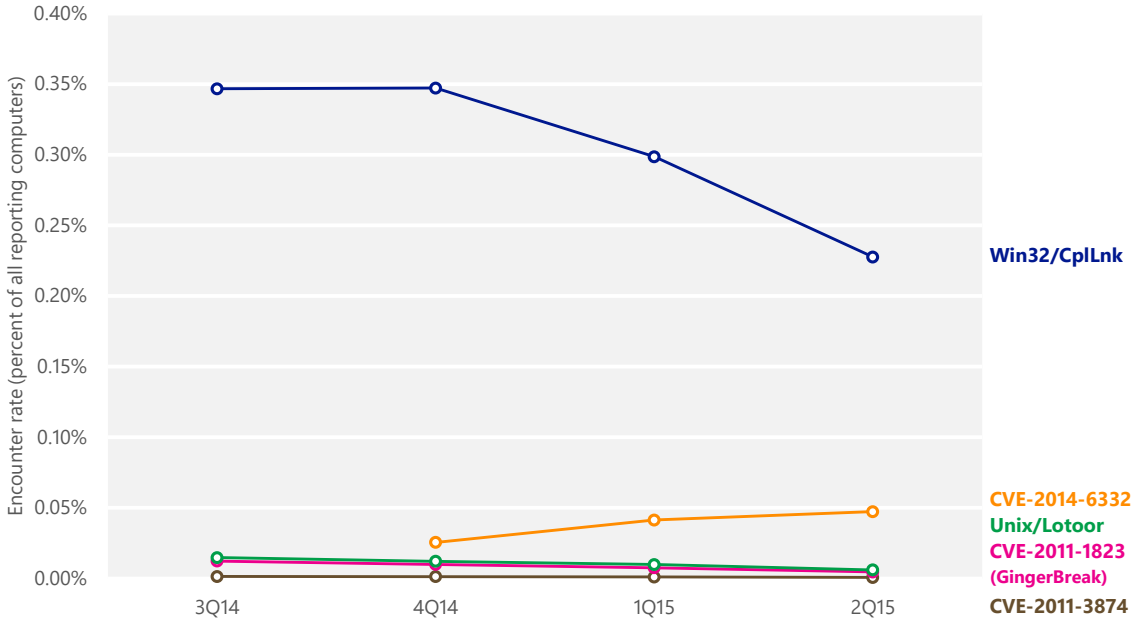
- Obfuscator is a generic detection for programs that have been modified by malware obfuscation, often in an attempt to avoid detection by security software. Files identified as Java/Obfuscator can represent exploits that target many different Java vulnerabilities.
- CVE-2010-0840 is a JRE vulnerability that was first disclosed in March 2010 and addressed by Oracle with a security update the same month. The vulnerability was previously exploited by some versions of the Blackhole exploit kit (detected as JS/Blacole), which has been inactive in recent years.
- 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.
- CVE-2013-0422 first appeared in January 2013 as a zero-day vulnerability. 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.

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, malicious or infected files that affect other operating systems are sometimes downloaded. Figure 34 shows trends for the individual exploits most commonly detected and blocked or removed during each of the past four quarters.

Figure 34. Individual operating system exploits detected and blocked by Microsoft real-time antimalware products, 3Q14–2Q15



- Win32/CplLnk, an exploit that targets a vulnerability in Windows Shell, remained the most commonly encountered operating system exploit in 1H15. 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.
- CVE-2014-6332 is a vulnerability in Windows Object Linking and Embedding (OLE) that can be used to perform remote attacks on a computer through Internet Explorer in some circumstances. Microsoft released Security Bulletin MS14-064 in November 2014 to address this issue. See "The life and times of an exploit" on pages 3–10 of *Microsoft Security Intelligence Report, Volume 18 (July–December 2014)*, available from the Microsoft Download Center, for

more information about this vulnerability and what Microsoft has done to mitigate it.

- Three of the five most commonly encountered operating system exploits on Windows computers in 1H15 actually target the Android mobile operating system published by Google and the Open Handset Alliance. 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. Most detections that affect Android involve 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.

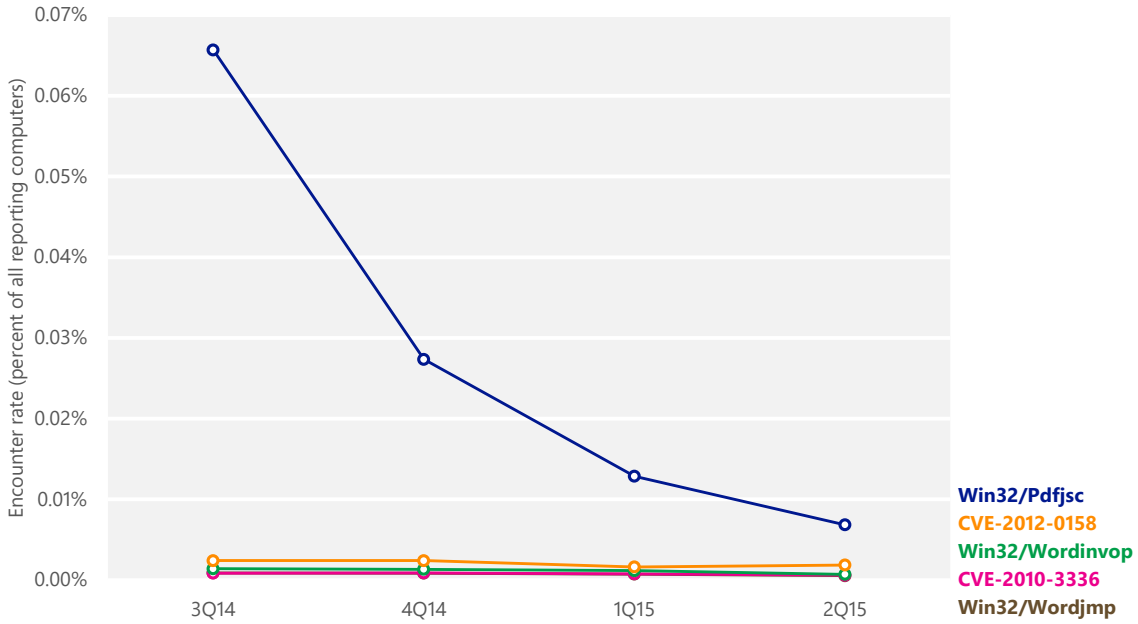
  Three of the five most commonly encountered operating system exploits on Windows computers in 1H15 actually target the Android mobile operating system.

  - 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.
  - 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 might 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.
  - CVE-2011-3874 can also be used to gain root privileges on devices running some versions of Android. Google published a source code update in November 2011 that addressed the vulnerability.

Document exploits

Document exploits are exploits that target vulnerabilities in the way a document editing or viewing application processes a particular file format. Figure 35 shows encounter rates for individual exploits.

Figure 35. Individual document exploits detected and blocked by Microsoft real-time antimalware products, 3Q14–2Q15

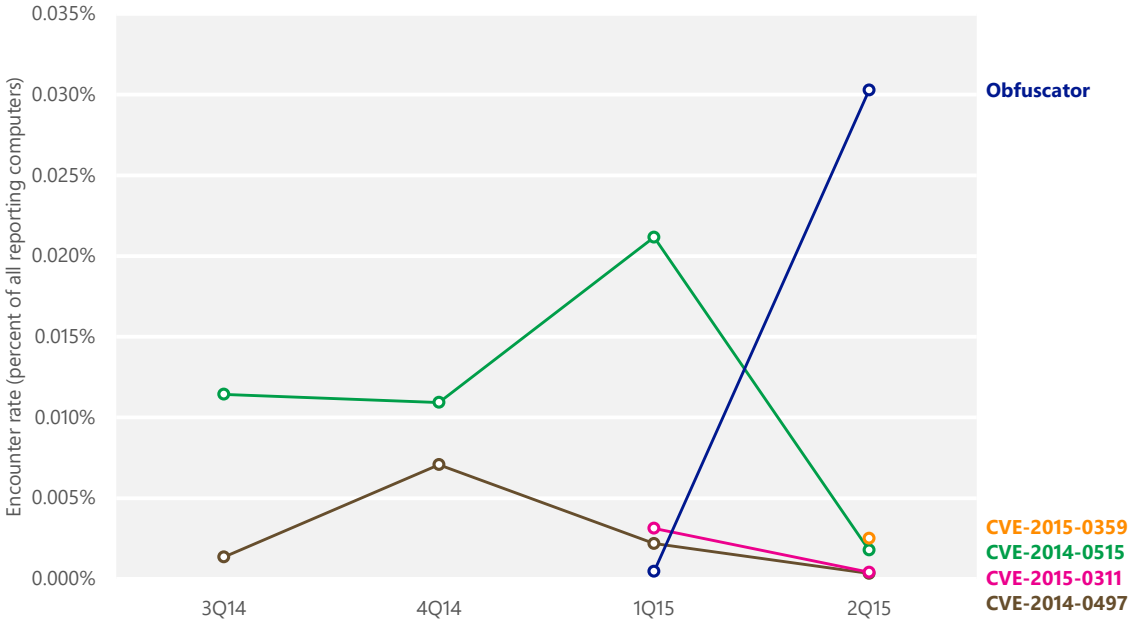


- Most detections of exploits that affect Adobe Reader and Adobe Acrobat were associated with the exploit family Win32/Pdfjsc, a detection for PDF files containing malicious JavaScript that targets CVE-2010-0188 and other vulnerabilities. Adobe released Security Bulletin APSB10-07 in February 2010 to address CVE-2010-0188. Pdfjsc and related exploits were particularly prevalent in eastern Europe. Pdfjsc mostly targets older Java vulnerabilities, so attackers may find it less useful as more computers are updated to newer versions of Java, which could explain the decrease in encounters over the past several quarters.

Adobe Flash Player exploits

Figure 36 shows the prevalence of different Adobe Flash Player exploits by quarter.

Figure 36. Adobe Flash Player exploits detected and blocked by Microsoft real-time antimalware products, 3Q14–2Q15

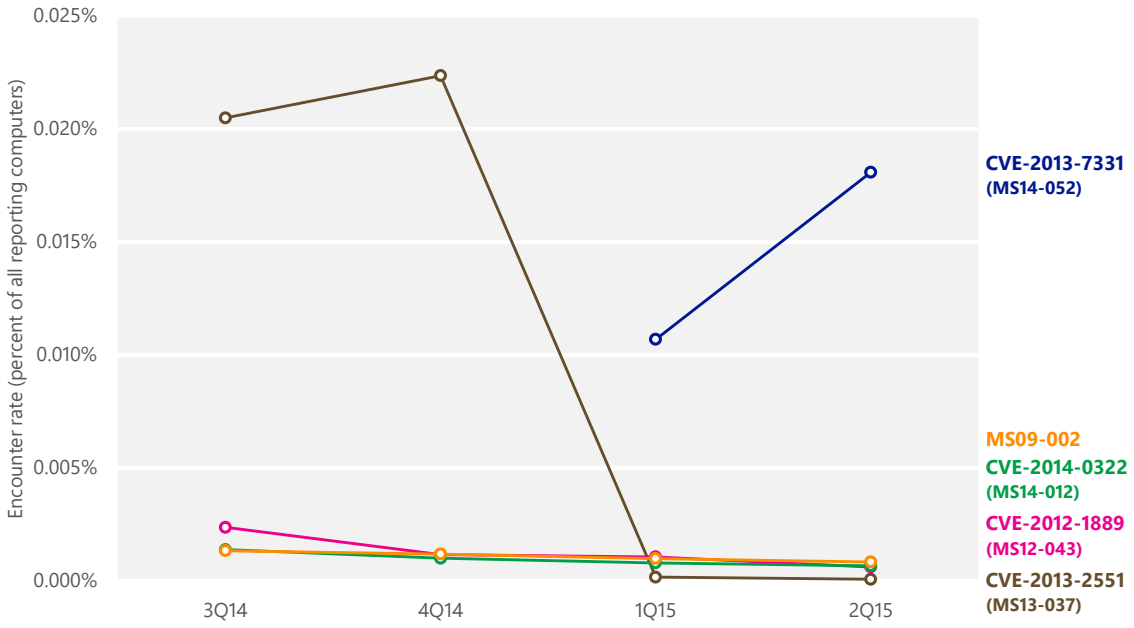


- Encounters involving Obfuscator variants that target Adobe Flash Player increased from very low levels in 1Q15 to become the largest source of Flash Player-related exploit encounters in 2Q15. Most of these encounters involved two newly discovered threats: Exploit:SWF/Obfuscator.K targets CVE-2014-8439, CVE-2015-0311, CVE-2015-0313, and CVE-2015-0359; Exploit:SWF/Obfuscator.L mainly targets CVE-2015-0336.
- CVE-2014-0515, the most commonly exploited Adobe Flash Player vulnerability in 1Q15 and the second most common in 1H15 overall, is a buffer overflow vulnerability. Adobe released Security Bulletin APSB14-13 on April 28, 2014 to address the issue.
- CVE-2015-0359, a double free vulnerability, was first disclosed in April 2015 and became the second most commonly encountered Adobe Flash Player exploit in the second quarter. Adobe released Security Bulletin APSB15-06 on April 14 to address the issue.
- CVE-2014-0497 is an integer underflow vulnerability. Adobe released Security Bulletin APSB14-04 on February 4, 2014 to address the issue.

Browser exploits

Figure 37 shows the prevalence of different browser exploits by quarter.

Figure 37. Browser exploits detected and blocked by Microsoft real-time antimalware products, 3Q14–2Q15



- Exploits targeting CVE-2013-7331, a vulnerability affecting the Microsoft.XMLDOM ActiveX control in Internet Explorer, accounted for the largest share of browser-related exploits encountered in 1H15. Exploiting this vulnerability allows an attacker to confirm the existence or nonexistence of arbitrarily specified paths and hostnames in the local environment. Microsoft published Security Bulletin MS14-052 in September 2014 to address the issue.
- Exploits targeting vulnerabilities addressed by Security Bulletin MS09-002, published by Microsoft in February 2009, accounted for the second largest share of browser-related exploits encountered in 1H15. Of these, most targeted CVE-2009-0075, an uninitialized memory corruption vulnerability in Internet Explorer 7.
- Encounters involving exploits targeting CVE-2013-2551, a use-after-free vulnerability in versions 6 through 10 of Internet Explorer, accounted for the largest share of browser-related exploit encounters in 2H14, then fell to negligible levels in 1H15 as exploit kit authors dropped them in favor of exploits targeting CVE-2013-7331.

Exploit detection with Internet Explorer and IExtensionValidation

IExtensionValidation is an interface introduced in Internet Explorer 11 that real-time security software can implement to block ActiveX controls from loading on malicious pages. When Internet Explorer loads a webpage that includes ActiveX controls, if the security software has implemented IExtensionValidation, the browser calls the security software to scan the HTML and script content on the page before loading the controls themselves. If the security software determines that the page is malicious (for example, if it identifies the page as an exploit kit landing page), it can direct Internet Explorer to prevent individual controls or the entire page from loading.

Figure 38. Internet Explorer 11 can block pages that contain ActiveX controls if security software determines that the page is malicious

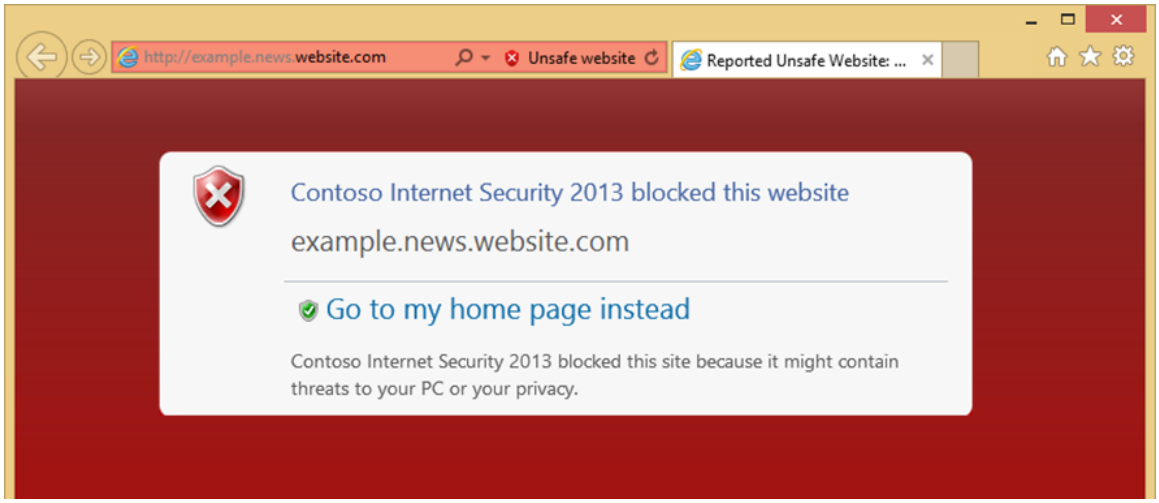
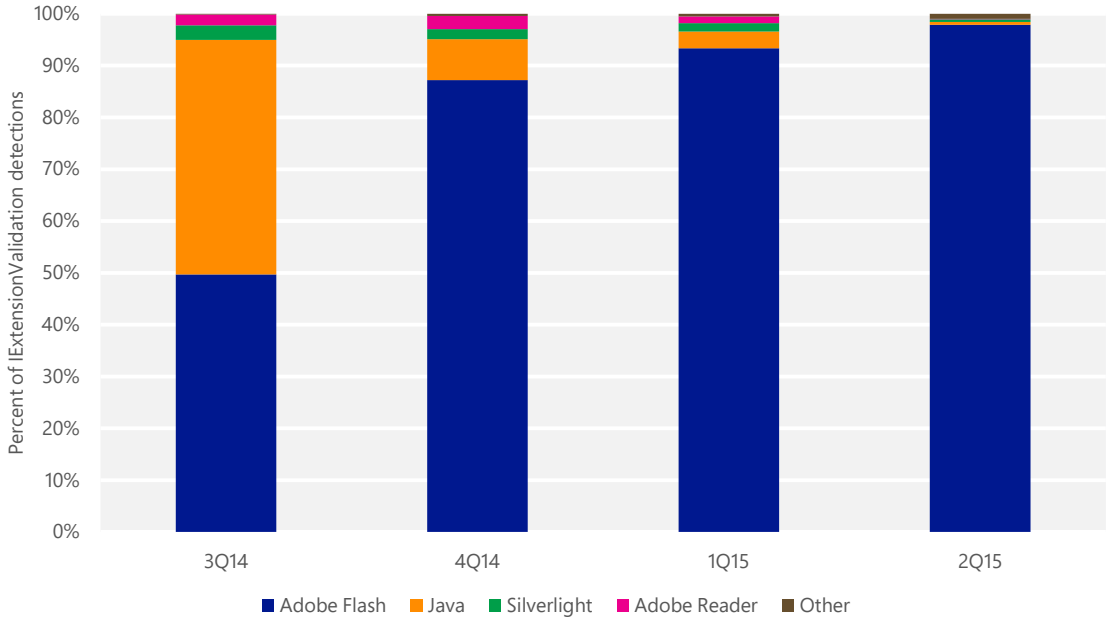


Figure 39 shows the types of ActiveX controls identified on malicious webpages in Internet Explorer 11 for each quarter in 2014.

Figure 39. ActiveX controls detected on malicious webpages through IExtensionValidation, 3Q14–2Q15, by control type



- Adobe Flash Player objects were the most commonly detected type of object hosted on malicious pages in each of the past four quarters.
- After accounting for a high of 45.3 percent of object detections in 3Q14, detections of Java applets on malicious pages decreased to just 0.5 percent of detections by 2Q15. A number of changes that have been made to Java and Internet Explorer over the past two years have made it much more difficult for attackers to take advantage of Java-based vulnerabilities, which is the most likely explanation for this significant decrease. (See "Java exploits" on page 47 for more information.)

Adobe Flash objects were the most commonly detected type of object hosted on malicious pages.

- Silverlight, Adobe Reader, and other malicious objects each accounted for less than 3 percent of object detections each quarter.

Exploits used in targeted attacks

A *targeted attack* is an attack against the computers or networks of a specific group of companies or individuals. This type of attack usually attempts to gain access to the computer or network before trying to steal information or disrupt the infected computers. Figure 40 lists some of the exploits Microsoft has observed being used in targeted attacks in 1H15.

Figure 40. Some of the exploits used in targeted attacks in 1H15

CVE	Exploit type	Affecting	Security update
CVE-2015-0097	Word HTA	Microsoft Word	MS15-022
CVE-2015-1641	Word RTF	Microsoft Word	MS15-033
CVE-2015-1701	Win32k EoP	Microsoft Windows	MS15-051
CVE-2015-1769	USB vector	Microsoft Windows	MS15-085
CVE-2015-1770	Word OSF	Microsoft Word	MS15-059
CVE-2015-2360	Win32k EoP	Microsoft Windows	MS15-061
CVE-2015-3043	Flash codec	Adobe Flash Player	APSB15-06

See the entry "Targeted Attacks Video Series" (June 13, 2013) on the Microsoft Cyber Trust blog at blogs.microsoft.com/cybertrust for an informative series of videos and papers about targeted attacks, the techniques used by attackers, and some of the steps that organizations can take to secure their networks against targeted attacks.

Malware and unwanted software

Most attempts by malware to infect computers are unsuccessful. More than three-quarters of Internet-connected personal computers worldwide are protected by real-time security software that constantly monitors the computers and network traffic for threats and blocks them before they can infect the computers, if possible. Therefore, a comprehensive understanding of the malware landscape requires consideration of infection attempts that are blocked as well as infections that are removed.

Microsoft uses two different metrics to measure malware and unwanted software prevalence:[16]

- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter.[17] For example, the encounter rate for the malware family JS/Bondat in Mexico in 2Q15 was 4.2 percent. This data means that, of the computers in Mexico that were running Microsoft real-time security software in 2Q15, 4.2 percent reported encountering the Bondat family, and 95.8 percent did not. Encountering a threat does not mean the computer has been infected. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[18]

---

[16] Microsoft regularly reviews and refines its data collection methodology to improve its scope and accuracy. For this reason, the statistics presented in this volume of the *Microsoft Security Intelligence Report* may differ slightly from comparable statistics in previous volumes.

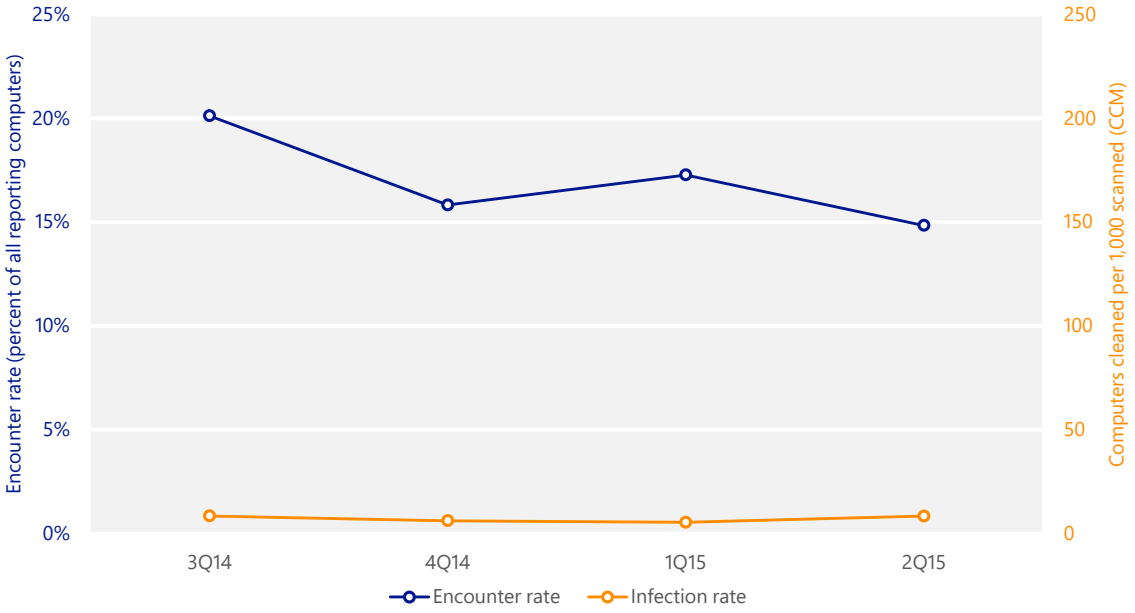
[17] Encounter rate does not include threats that are blocked by a web browser before being detected by antimalware software. In particular, **IExtensionValidation** in Internet Explorer 11 enables security software to block pages that contain exploits from loading. (See "Exploit detection with Internet Explorer and IExtensionValidation" on page 55 for information about **IExtensionValidation** and the threats it blocks.) For this reason, encounter rate figures may not fully reflect all of the threats encountered by computer users.

[18] For information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 129.

- *Computers cleaned per mille*, or *CCM*, is an infection rate metric that is defined as the number of computers cleaned for every 1,000 unique computers that run the Malicious Software Removal Tool (MSRT), a free tool distributed through Microsoft update services that removes more than 200 highly prevalent or serious threats from computers. Because it is not a real-time tool, the MSRT only detects and removes threats that are already present on the computer; it does not block infection attempts as they happen.

Figure 41 illustrates the difference between these two metrics.

Figure 41. Worldwide encounter and infection rates, 2Q14–2Q15, by quarter



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

As Figure 41 shows, and as one would expect, malware encounters are much more common than malware infections. On average, about 17.0 percent of reporting computers worldwide encountered malware over the past four quarters. At the same time, the MSRT removed malware from about 7.1 out of every 1,000 computers, or 0.71 percent. Together, encounter and infection rate information can help provide a broader picture of the malware landscape by offering different perspectives on how malware propagates and how computers get infected.

Brantall, Rotbrow, and Filcout

Where noted, the figures in this report omit detections of Win32/Brantall, Win32/Rotbrow, and Win32/Filcout. These three families were involved in an incident in which a rogue developer with access to commercial source code modified the source code to serve as a stealth distribution method for malware without being detected by major security software vendors. When the modification was discovered, it resulted in a significant installed base of commercial software being reclassified as malicious, which had an outsized effect on infection rates. Microsoft believes that the unmodified infection and encounter figures do not create an accurate picture of the worldwide threat landscape over the past year and a half. As a result, totals for the Brantall, Filcout, and Rotbrow families have been removed from the infection and encounter figures presented here where appropriate, as noted.

See "The Sefnit saga: a timeline" on pages 57–64 of *Microsoft Security Intelligence Report, Volume 17 (January–June 2014)*, available from the Microsoft Download Center, for a more in-depth explanation of the incident, along with detection statistics and a timeline of events.

Malware and unwanted software 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.[19]

[19] For more information about this process, see the entry "Determining the Geolocation of Systems Infected with Malware" (November 15, 2011) in the Microsoft Cyber Trust Blog (blogs.microsoft.com/cybertrust).

Figure 42. Encounter rate trends for the locations with the most computers reporting malware and unwanted software encounters in 1H15, by number of computers reporting

Country/Region	3Q14	4Q14	1Q15	2Q15
United States	15.4%	11.6%	11.0%	9.8%
Brazil	32.9%	21.7%	20.5%	20.2%
Russia	27.3%	24.1%	22.8%	17.7%
India	38.2%	32.0%	34.9%	31.3%
France	22.8%	13.0%	15.8%	13.2%
Turkey	35.1%	27.9%	32.0%	28.1%
China	18.1%	15.2%	13.1%	13.7%
United Kingdom	17.2%	11.4%	12.7%	11.7%
Mexico	30.0%	21.7%	22.6%	21.2%
Canada	18.1%	12.5%	14.0%	12.5%

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- Locations in Figure 42 are ordered by the number of computers reporting detections in 1H15.
- As Figure 41 on page 59 illustrates, the worldwide encounter rate increased slightly in 1Q15 before decreasing again in 2Q15, and this pattern is reflected in several of the locations in Figure 42 as well. India, France, Turkey, the United Kingdom, Mexico, and Canada all had small encounter rate increases in the first quarter of 2015, followed by decreases to around the same level as 2Q14. In general, however, encounter rates remained largely stable through the first half of 2015 in all of these locations, without any unusually large increases or decreases.
- The browser modifiers Win32/KipodToolsCby and Win32/CouponRuc and the adware family Win32/SaverExtension, the three most commonly encountered families worldwide in 1H15, were also the three most commonly encountered families in the United States, France, Turkey, the United Kingdom, Mexico, and Canada, and were all in the top six families encountered in Russia and India. See "Threat families" beginning on page 74 for more information about these and other malware and unwanted software families.
- Encounters in the United States in 1H15 were dominated by unwanted software, which accounted for nine of the ten most commonly encountered families. Of these, six were browser modifiers, including CouponRuc and

KipodToolsCby, the first and third most commonly detected threat families in the US, respectively.

The browser modifiers KipodToolsCby, CouponRuc, and Win32/IeEnablerCby were the most commonly detected families in Brazil in 1H15. Families that ranked unusually high in Brazil included Win32/Banload (ranked fourth in Brazil, 54th worldwide), which is usually used to steal login credentials for Brazilian banks, and the worm family JS/Proslikefan (14th in Brazil, 101st worldwide). (See "Win32/Banload and Banking Malware" on page 21 for more information about Banload in Brazil.)

As is typically the case, the threat landscape in China was dominated by malware families that are much less common worldwide.

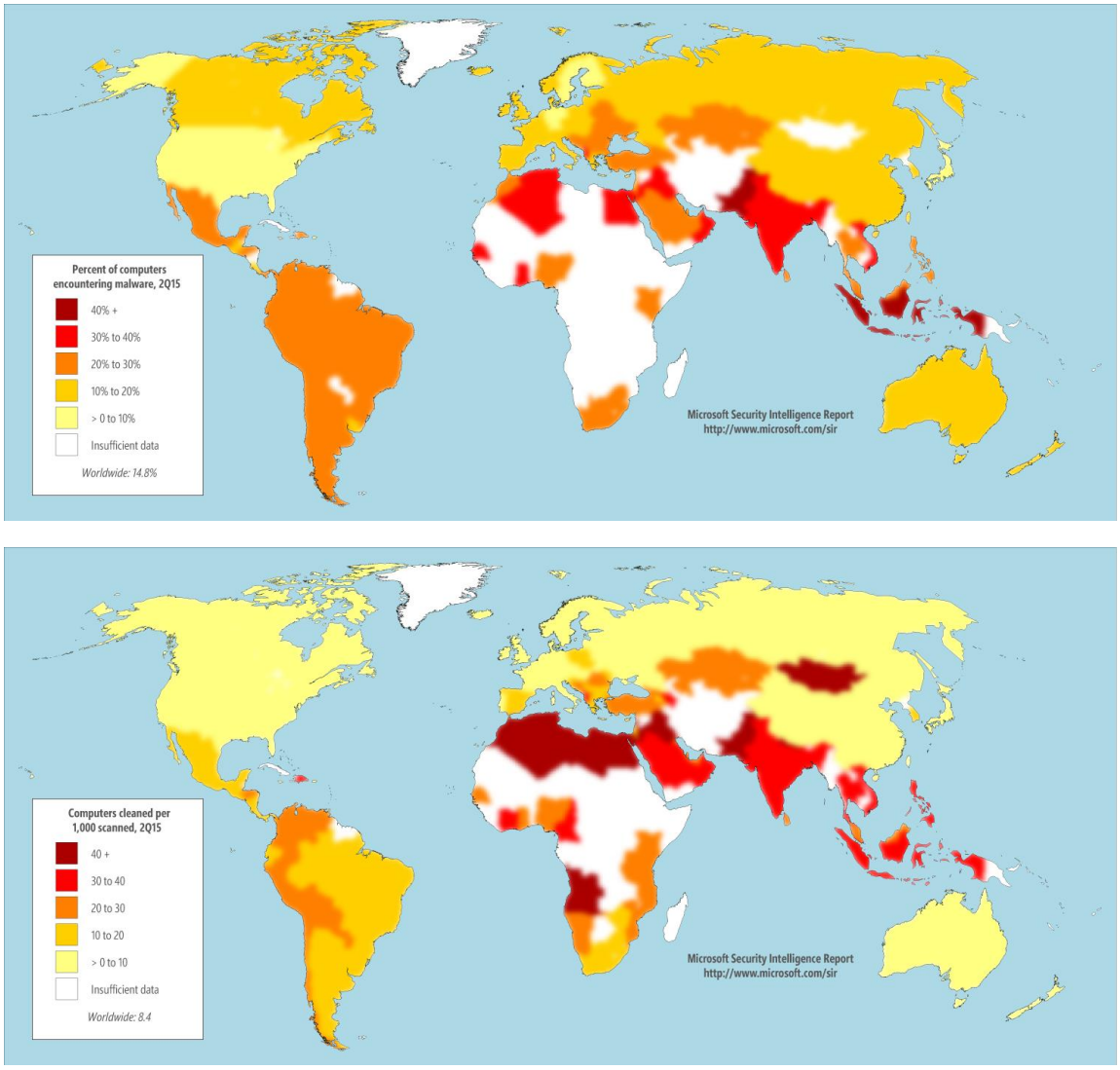
- Encounters in Russia were led by Win32/Peals, a family of trojans, and the downloader family Win32/Ogimant, which has a Russian-language interface and masquerades as a downloader for peer-to-peer and torrent services. Detections of Ogimant in Russia decreased from 3.6 percent in 1Q15 to 0.75 percent in 2Q15, but it remained the second most commonly detected family in Russia in 1H15, overall, behind Peals. Other families that were unusually common in Russia in 1H15 included the trojan family Win32/Radonskra (ranked ninth in Russia, 84th worldwide) and the generic trojan detection Win32/Peaac (10th in Russia, 48th worldwide).
- The mix of threats encountered in India and Turkey were largely similar to the worldwide mix, but each location also reported significant encounters with a threat that appeared to be strongly targeted at a specific region. The worm family MSIL/Mofin (ranked 12th in India, 115th worldwide) was unusually common in India, where more than 85 percent of all Mofin encounters occurred in 1H15. And the trojan family Win32/BeeVry (11th in Turkey, 134th worldwide) was unusually common in Turkey, where more than 98 percent of all BeeVry encounters occurred in 1H15.
- As is typically the case, the threat landscape in China in 1H15 was dominated by malware families that are much less common worldwide. Of the threats most commonly encountered in China, only the generic detections Win32/Obfuscator, INF/Autorun, and Win32/Dynamer and the trojan family Win32/Ramnit were also commonly encountered worldwide. All of the most commonly encountered families in China in 1H15 were malware families. The most commonly detected unwanted software family in China (KipodToolsCby) ranked 48th there overall. Families that were unusually

prevalent in China included the virus DOS/JackTheRipper (ranked second in China, 119th worldwide), the downloader HTML/Adodb (fifth in China, 108th worldwide), and the worm ALisp/Kenilfe (seventh in China, 125th worldwide).

- The downloader family W97M/Adnel was unusually prevalent in the United Kingdom (ranked 12th in the UK, 98th worldwide).
- The rogue security software family JS/FakeCall was unusually prevalent in Canada (ranked 11th in Canada, 96th worldwide).

For a different perspective on threat patterns worldwide, Figure 43 shows the infection and encounter rates in locations around the world in 2Q15.

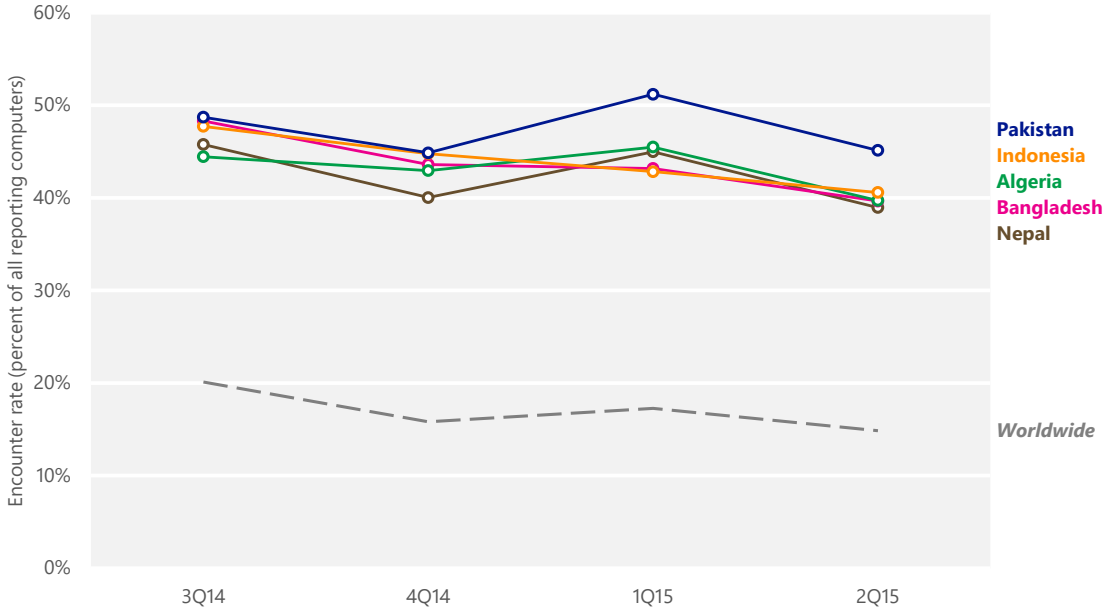
Figure 43. Encounter rates (top) and infection rates (bottom) by country/region in 2Q15



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

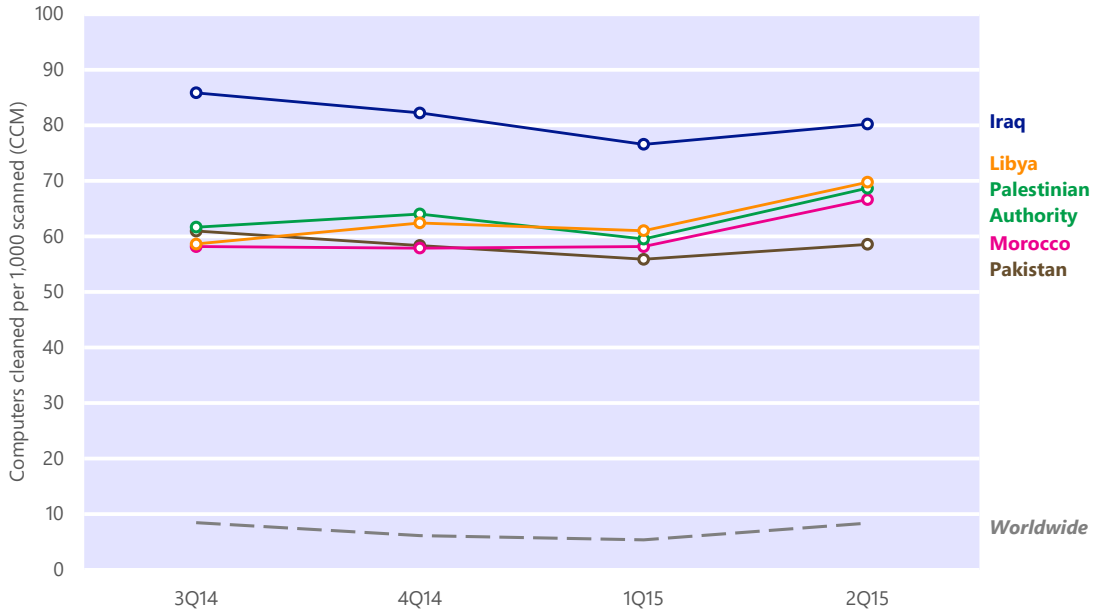
The next several figures illustrate trends for specific locations around the world with particularly high or low incidences of threat detection. Figure 44 and Figure 45 show trends for the locations with the highest rates of detection as determined by encounter rate and CCM, respectively.

Figure 44. Trends for the five locations with the highest encounter rates in 1H15 (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

Figure 45. Trends for the five locations with the highest infection rates in 1H15, by CCM (100,000 MSRT computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

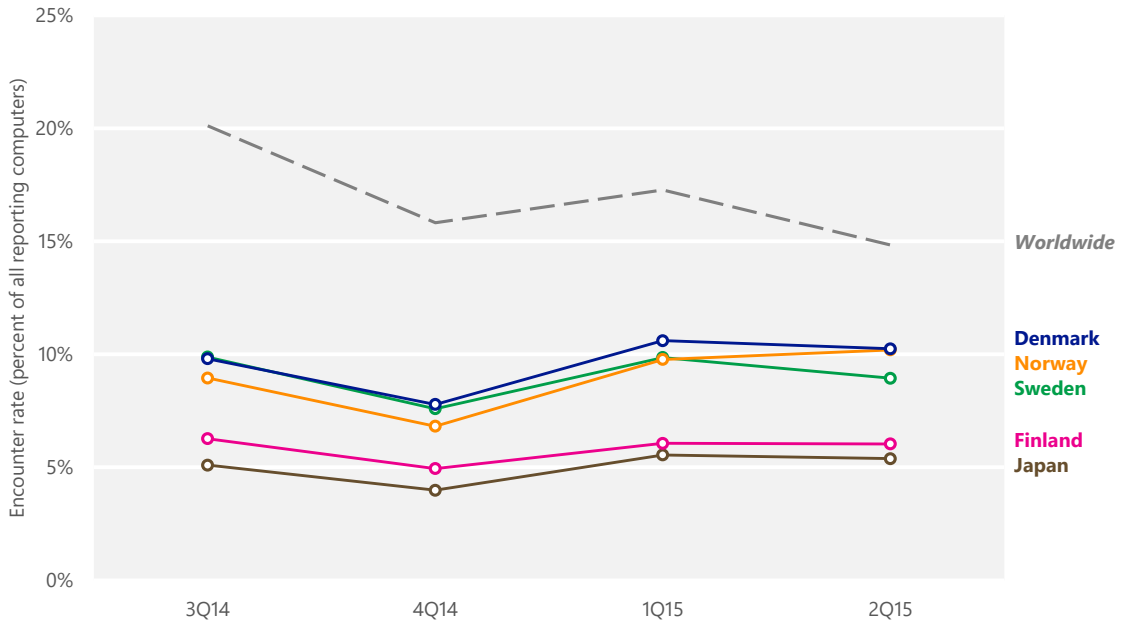
- The locations with the highest encounter rates were Pakistan, Indonesia, Algeria, Bangladesh, and Nepal.
  - Pakistan, Indonesia, and Algeria also had the highest encounter rates in 2H14.
  - As in 2H14, exploit kits were relatively rare in the locations with the highest encounter rates. JS/Axpergle, the most commonly encountered exploit kit worldwide in 1H15, ranked no higher than 34th in any of the locations with the highest encounter rates.
  - Unwanted software was highly prevalent in these locations, as it was worldwide in 1H15. The browser modifiers Win32/KipodToolsCby and Win32/CouponRuc and the adware family Win32/SaverExtension, the three most commonly encountered families worldwide in 1H15, were all among the top nine families encountered in all of the locations with the highest encounter rates.
  - Families that were unusually prevalent in Pakistan included Win32/Nuqel (ranked 11th in Pakistan, 34th worldwide), a worm, and the virus family Win32/Chir (13th in Pakistan, 69th worldwide). In both cases, the encounter rate for the family in Pakistan was more than twice as high as in any other country or region.
  - Families that were unusually prevalent in Indonesia included the exploit Win32/CplLnk (ranked fifth in Indonesia, 20th worldwide) and the virus family Win32/Slugin (ranked 13th in Indonesia, 92nd worldwide).
  - Win32/Macoute, a worm, was unusually prevalent in Algeria (ranked 17th in Algeria, 148th worldwide). Most Macoute encounters worldwide took place in Algeria and several other locations in Africa, including Senegal, Ghana, and Tunisia.
  - The worm family Win32/Vercuser was unusually prevalent in Bangladesh (ranked 14th in Bangladesh, 102nd worldwide) and a number of nearby locations, including Nepal, Pakistan, and India.

As in 2H14, exploit kits were relatively rare in the locations with the highest encounter rates.

- The locations with the highest infection rates were Iraq, Libya, the Palestinian territories, Morocco, and Pakistan.

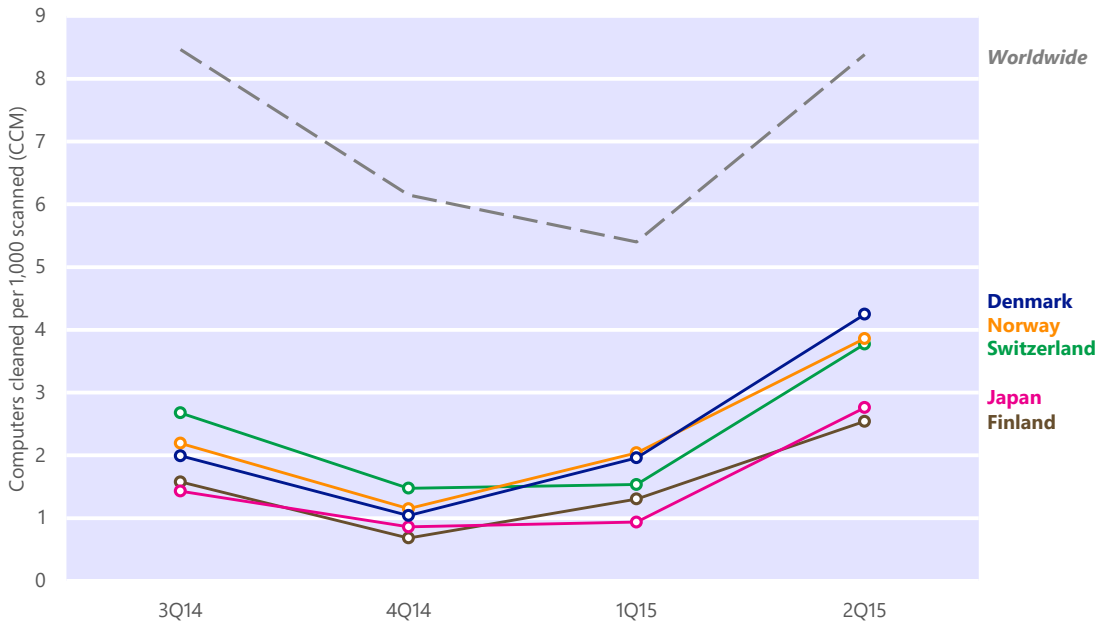
- The worm family VBS/Jenxcus was the most common malware family infecting computers in 1H15 in all of these locations except Morocco, where it was second. Infection rates for Jenxcus were particularly high across the Middle East, and low in North America and Europe.
- Infections involving the backdoor family MSIL/Bladabindi, which ranked 26th among infecting families worldwide, were particularly common in Iraq (where it ranked fourth), Libya (third), the Palestinian territories (11th), and Morocco (seventh). Like Jenxcus, Bladabindi had its greatest impact in the Middle East.
- In Morocco, the most common infecting malware family was the worm family Win32/Yeltminky, which had its highest infection rate there (a CCM of 23.8 in Morocco in 2Q15, compared to 3.3 in Algeria, the next highest location). Yeltminky is a family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute the copies.

Figure 46. Trends for locations with low encounter rates in 1H15 (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

Figure 47. Trends for locations with low infection rates in 1H15, by CCM (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- The Nordic countries, including Denmark, Finland, Iceland, Norway, and Sweden, have perennially been among the healthiest locations in the world with regard to malware exposure, as has Japan. In 1H15, the infection and encounter rates for these locations were typically about half of the worldwide averages. (See the blog entry series "Lessons from Least Infected Countries" at blogs.technet.com/b/security/p/series-lessons-from-least-infected-countries.aspx for more information about locations that typically have low infection and encounter rates.)

> All five locations had similar encounter and infection statistics in 1H15.

- All of these locations, even geographically- and culturally-distant Japan, had similar encounter and infection statistics in 1H15. Unwanted software dominated encounters in each location, led by browser modifiers Win32/KipodToolsCby, Win32/CouponRuc, and Win32/AlterbookSP; adware family Win32/SaverExtension; and software bundler Win32/InstalleRex.
- Infection rates trended up significantly in all five locations in 2Q15 because of removals of Win32/CompromisedCert, an advertising program pre-installed on some Lenovo laptops that installed a compromised trusted root certificate, and Win32/IeEnablerCby, a browser modifier that bypasses user

consent dialogs to install software without the user's explicit permission. See page 78 for more information about IeEnablerCby.

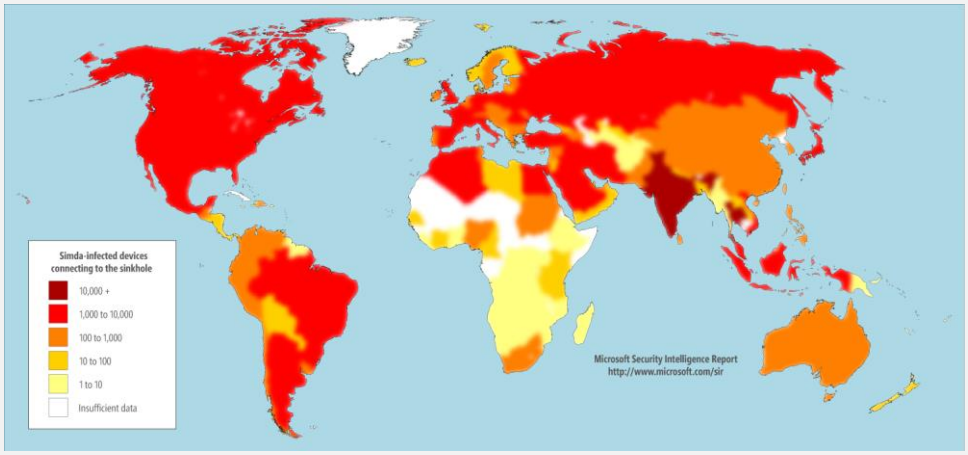
- Threats that are particularly uncommon in these locations include Win32/Frethog, a game password stealer that is most prevalent in Asia; Win32/Yeltminky, a worm that is most prevalent in the Middle East; Win32/Gamarue, a worm that is prevalent in southeast Asia and the Middle East; and Win32/Ramnit, a virus that is prevalent in southern and southeast Asia.

Microsoft and partners disrupt the Simda.AT botnet

On April 12, 2015, Interpol and the Dutch National High Tech Crime Unit (DNHTCU) announced the disruption of Backdoor:Win32/Simda.AT, a significant malware threat affecting more than 770,000 devices in more than 190 countries and regions.

Win32/Simda is a family of threats that can provide an attacker with backdoor access to and control of an infected device. They can then steal passwords and gather information about the device to send to the attacker. The Simda.AT variant first appeared in 2012, and is often downloaded to a vulnerable device by a drive-by download. Aside from the information-stealing behavior common to Simda variants, Simda.AT redirects search traffic from popular websites such as Bing, Google, and Facebook to its own domain, and can download other malware from a remote host. Simda was the 55th most commonly encountered malware family worldwide in 1H15, with the overwhelming majority of encounters involving the Simda.AT variant.

Figure 48. Average number of Simda-infected devices connecting to the sinkhole each month, April–July, 2015



Interpol coordinated the operation and the DNHTCU, with the support of the Federal Bureau of Investigation (FBI), successfully took down Simda.AT's active command and control infrastructure across four countries including the Netherlands, Luxembourg, Russia, and the United States. The Microsoft Malware Protection Center (MMPC) and the Microsoft Digital Crimes Unit (DCU) led the analysis of the malware threat in partnership with CDI Japan, Kaspersky Lab, and Trend Micro.

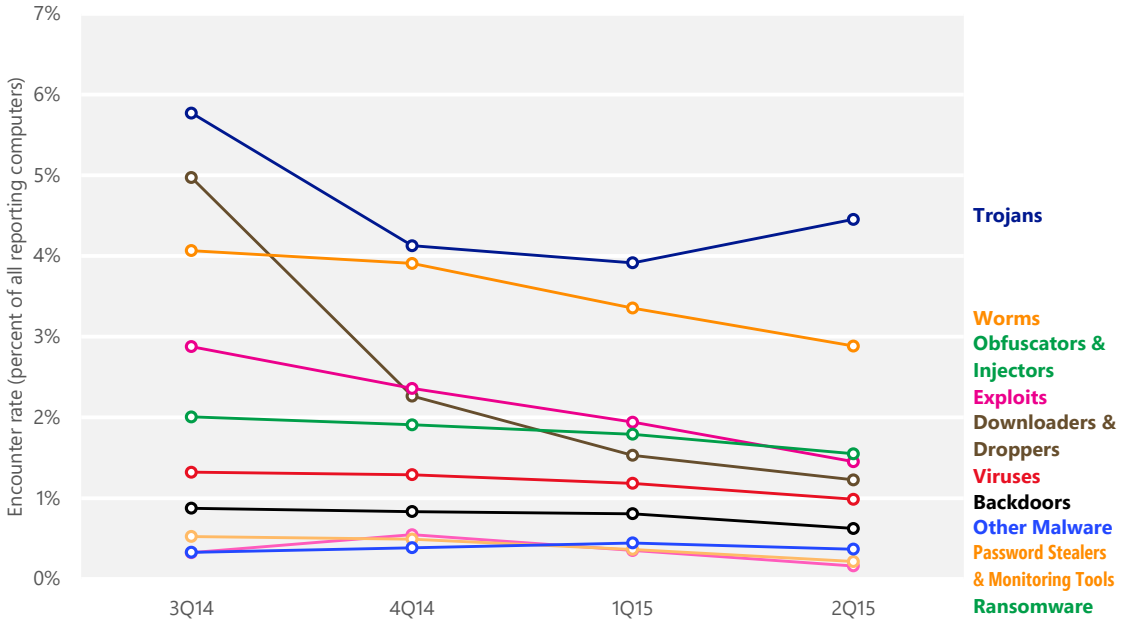
The MMPC activated the Coordinated Malware Eradication (CME) platform to provide in-depth research, telemetry, samples, and cleaning solutions to law enforcement and Microsoft partners. This information helped law enforcement take action against Simda.AT and its infrastructure, while providing remediation and recovery options for infected devices around the world.

For more information about the takedown and technical information about the Simda.AT backdoor, see the entry "Microsoft partners with Interpol, industry to disrupt global malware attack affecting more than 770,000 PCs in past six months" (April 12, 2015) on the MMPC blog at blogs.technet.com/mmpc.

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 categories based on similarities in function and purpose.

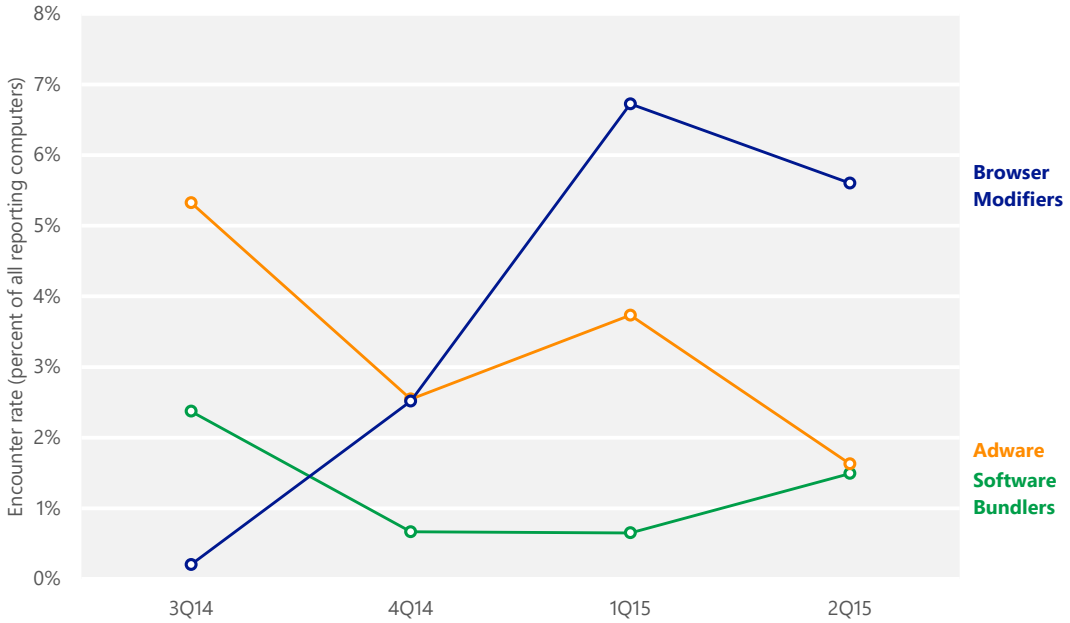
Figure 49. Encounter rates for significant malware categories, 3Q14–2Q15



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- The number of encounters for most categories of malware remained stable or decreased throughout the first half of 2015, with the exception of Trojans, which increased to 4.5 percent in 2Q15 after dipping slightly in the first quarter. Encounters with the three most commonly detected trojan families, Win32/Peals, Win32/Kilim, and Win32/Skeeyah, all increased significantly in 2Q15, contributing to the overall increase, which was partly ameliorated by the disruption of the Win32/Ramnit family. See "Threat families" beginning on page 74 for more information about these and other malware and unwanted software families.

Figure 50. Encounter rates for unwanted software categories, 3Q14–2Q15



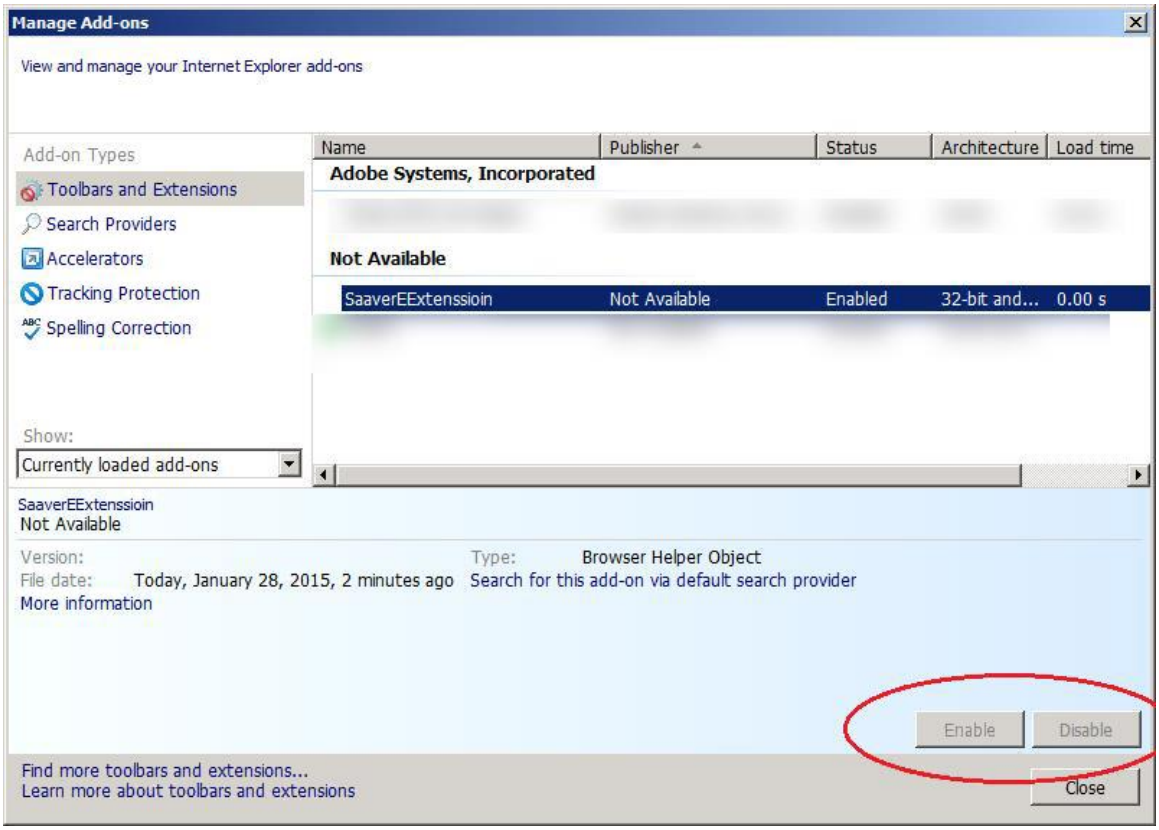
Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- Encounters involving browser modifiers more than doubled between 1Q15 and 2Q15 because of changes to Microsoft detection criteria for unwanted software. In January, Microsoft security products began detecting as unwanted software browser add-ons that limit user control over their browser in a number of ways, including disabling certain browser controls, limiting the user's ability to choose their default search provider, and bypassing consent dialogs for newly installed add-ons. See "Threat families" beginning on page 74 for more information about this change.

> Encounters involving browser modifiers more than doubled because of changes to detection criteria.

- Encounters involving adware increased from 2.5 percent in 4Q14 to 3.7 percent in 1Q15, then fell to 1.6 percent. Much of the increase and subsequent decrease was related to Win32/SaverExtension, a browser add-on that shows ads in the browser without revealing their source, and prevents itself from being removed normally.

Figure 51. SaverExtension prevents itself from being removed



- Detections of software bundlers increased slightly in 1Q15 because of Win32/InstalleRex, a software bundler that installs other unwanted software families.

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 can be highly dependent on language and socioeconomic 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 world.

Figure 52 shows the relative prevalence of different categories of malware in several locations around the world in 2Q15.

Figure 52. Threat category prevalence worldwide and in the 10 locations with the most computers reporting encounters in 2Q15

Category	Worldwide	United States	Brazil	Russia	India	France	Turkey	China	United Kingdom	Mexico	Canada
Browser Modifiers	5.6%	9.1%	11.6%	7.0%	22.3%	14.2%	16.5%	0.6%	10.8%	13.9%	11.2%
Trojans	4.5%	4.2%	12.6%	20.6%	17.9%	5.7%	25.9%	10.2%	4.4%	9.0%	5.1%
Worms	2.9%	0.6%	8.8%	4.5%	31.2%	1.9%	17.2%	5.6%	0.8%	20.8%	0.6%
Adware	1.6%	4.5%	7.0%	5.1%	8.2%	7.7%	9.6%	0.2%	4.7%	6.3%	5.3%
Obfuscators & Injectors	1.5%	1.0%	5.3%	7.3%	8.5%	1.9%	7.7%	4.9%	1.7%	3.1%	1.6%
Software Bundlers	1.5%	1.7%	1.5%	0.5%	5.2%	2.2%	3.5%	0.2%	2.3%	2.9%	2.5%
Exploits	1.5%	3.4%	2.4%	1.3%	4.7%	2.5%	4.5%	1.7%	4.4%	2.9%	5.6%
Downloaders & Droppers	1.2%	2.3%	6.4%	6.6%	4.2%	2.7%	3.6%	3.2%	3.1%	2.0%	3.3%
Viruses	1.0%	0.4%	2.2%	1.5%	8.2%	0.4%	6.6%	7.4%	0.3%	1.2%	0.4%
Backdoors	0.6%	0.7%	1.4%	2.0%	3.5%	0.9%	3.2%	1.8%	0.9%	1.5%	0.7%
Other Malware	0.4%	0.9%	0.3%	0.3%	1.7%	0.5%	1.4%	1.3%	0.6%	0.6%	1.5%
Password Stealers & Monitoring Tools	0.2%	0.4%	1.0%	0.8%	0.8%	0.3%	1.0%	0.5%	0.4%	0.5%	0.6%
Ransomware	0.2%	0.6%	0.5%	0.6%	0.1%	0.7%	0.6%	0.0%	0.4%	0.8%	0.7%

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- Within each row of Figure 52, 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 42 on page 61, the locations in the table are ordered by number of computers reporting detections in 1H15.
- India experienced higher encounter rates for Backdoors, Browser Modifiers, Obfuscators & Injectors, Other Malware, Software Bundlers, Viruses, and Worms than the other locations in Figure 52.
- Turkey had the highest encounter rate for Trojans, led by Win32/Peals and Win32/Kilim, and Adware, led by Win32/SaverExtension.

- Canada had the highest encounter rate for Exploits, led by JS/Axpergle, a detection for the Sweet Orange exploit kit. See "Exploit kits" on page 44 for more information. Axpergle encounters also contributed to relatively high encounter rates for Exploits in the United States and United Kingdom.
- Russia had the highest encounter rate for Downloaders & Droppers, led by Win32/Ogimant. Brazil also had a high Downloaders & Droppers encounter rate, led by Win32/Banload. (See "Win32/Banload and Banking Malware" on page 21 for more information about Banload in Brazil.)

India experienced higher encounter rates for Backdoors, Browser Modifiers, Obfuscators & Injectors, Other Malware, Software Bundlers, Viruses, and Worms than the other locations.

- Though relatively quite rare overall, ransomware was unusually prevalent in North America and Europe, led by Win32/Crowti, JS/Krypterade, and Win32/Reveton.
- Mexico had a relatively high encounter rate for Worms, led by Win32/Bondat and VBS/Jenxcus. Computers in Mexico accounted for nearly a third of Bondat encounters worldwide in 1H15.
- Computers in France had a relatively high encounter rate for Adware, led by Win32/SaverExtension and Win32/EoRezo.
- China had a relatively high encounter rate for Viruses, led by DOS/JackTheRipper.

See "Appendix C: Worldwide encounter and infection rates" on page 127 for more information about malware around the world. Also, see "Linking Cybersecurity Policy and Performance" at aka.ms/securityatlas for an in-depth examination of the socioeconomic factors that correlate with high infection rates in different parts of the world.

Threat families

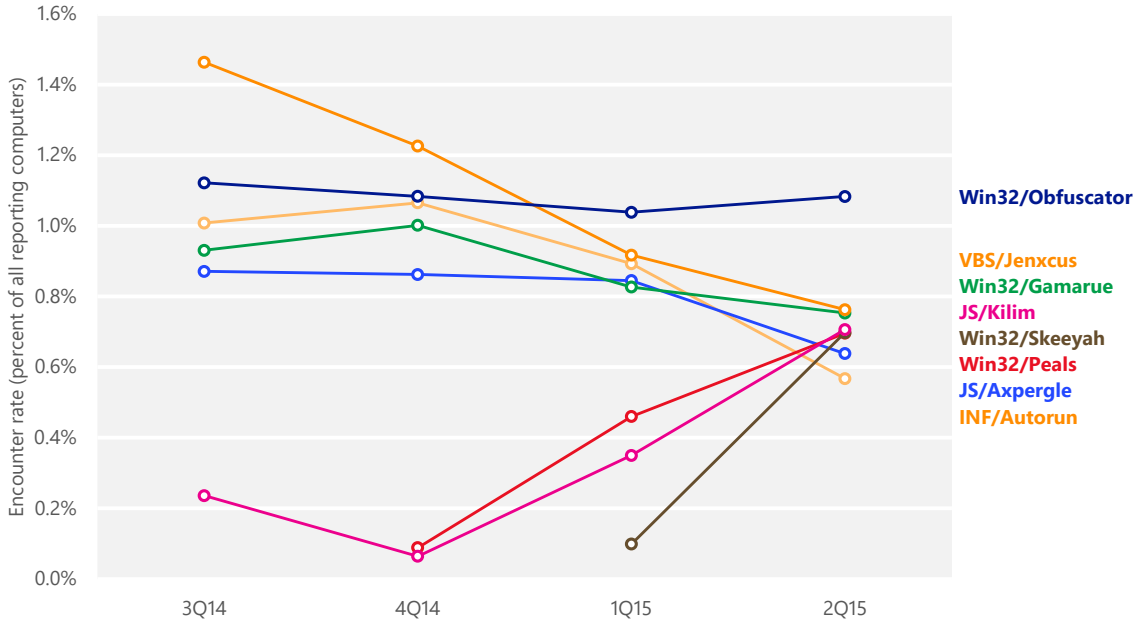
Figure 53 and Figure 54 show trends for the top malware families that were detected on computers by Microsoft real-time antimalware products worldwide in 1H15.

Figure 53. Quarterly trends for the top 10 malware families encountered by Microsoft real-time antimalware products in 1H15, shaded according to relative encounter rate

Rank	Family	Most significant category	3Q14	4Q14	1Q15	2Q15
1	Win32/Obfuscator	Obfuscators & Injectors	1.12%	1.08%	1.04%	1.08%
2	VBS/Jenxcus	Worms	1.46%	1.23%	0.92%	0.76%
3	Win32/Gamarue	Worms	0.93%	1.00%	0.83%	0.75%
4	JS/Axpergle	Exploits	0.87%	0.86%	0.85%	0.64%
5	INF/Autorun	Obfuscators & Injectors	1.01%	1.07%	0.89%	0.57%
6	Win32/Peals	Trojans	—	0.09%	0.46%	0.70%
7	Win32/Kilim	Trojans	0.24%	0.06%	0.35%	0.71%
8	Win32/Skeeyah	Trojans	—	—	0.10%	0.70%
9	Win32/Ramnit	Viruses	0.47%	0.46%	0.43%	0.33%
10	Win32/Sality	Viruses	0.48%	0.47%	0.42%	0.35%

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

Figure 54. Encounter rate trends for a number of notable malware families in 1H15



- Win32/Obfuscator, the most commonly encountered threat in 1H15, 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.

- Encounters involving VBS/Jenxcus declined steadily over the past four quarters, but it remained the second-most commonly encountered family in 1H15. Jenxcus is a worm coded in VBScript that opens a backdoor on an infected computer, enabling an attacker to control it remotely. In addition to spreading via removable drives, Jenxcus was often transmitted via a fake Adobe Flash Player update from spoofed YouTube webpages. Encounters involving Jenxcus decreased significantly after the Microsoft Digital Crimes Unit launched a takedown operation in June of 2014 that successfully disrupted the Jenxcus botnet. The original owners of the botnet subsequently left the project, but the Jenxcus code is now being used by other criminal organizations.

  Win32/Gamarue, the third most commonly encountered threat in 1H15, was especially prevalent in southeast Asia and the Middle East.

  See "The Microsoft DCU and the legal side of fighting malware" on pages 29–32 of *Microsoft Security Intelligence Report, Volume 17 (January–June 2014)*, available from the Microsoft Download Center, for more information about the Microsoft takedown of the Jenxcus botnet. For additional technical information about Jenxcus, see the following entries in the MMPC blog (blogs.technet.com/mmpc):

  - MSRT February 2014 – Jenxcus (February 11, 2014)
  - Microsoft Digital Crimes Unit disrupts Jenxcus and Bladabindi malware families (June 30, 2014)

- Win32/Gamarue, the third most commonly encountered threat in 1H15, was especially prevalent in southeast Asia and the Middle East. Gamarue 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. 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)

- Win32/Kilim is a family of trojans that makes money for the attacker by generating fake likes and shares on Facebook. Prior to 2015, Kilim

encounters were heavily concentrated in Turkey, and were rare elsewhere. Since then, encounters have increased tenfold from 4Q14 levels, with most of the increase occurring outside Turkey.

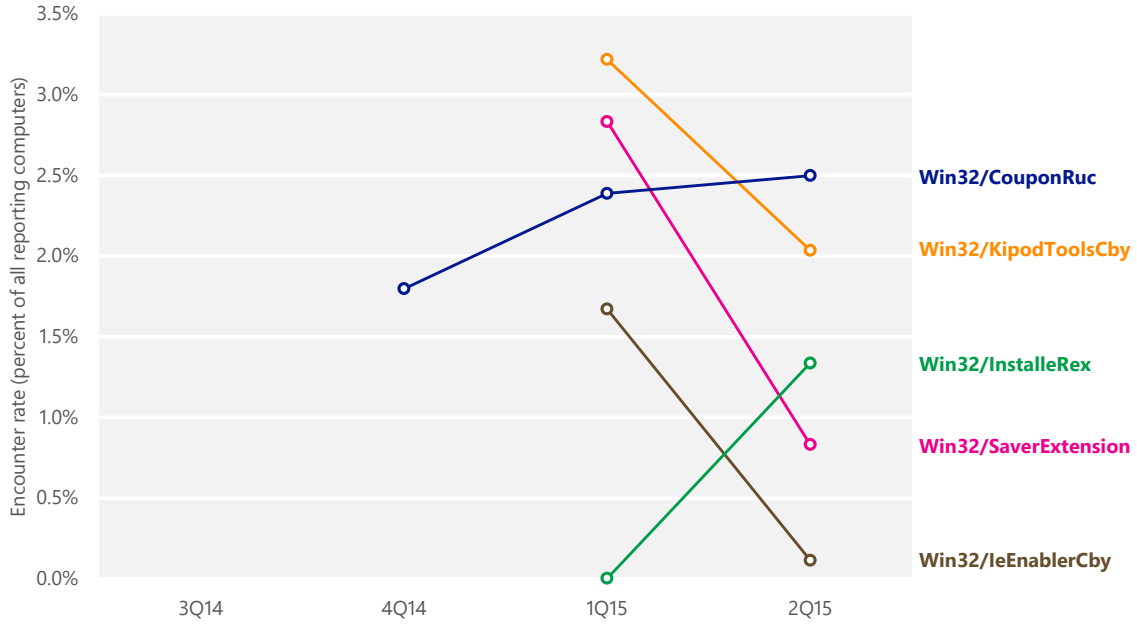
- Encounters involving two newly designated generic detections, Win32/Peals and Win32/Skeeyah, increased rapidly to account for a significant share of encounters worldwide by 2Q15.
- JS/Axpergle, a detection for the Angler exploit kit, is the only exploit-related family in the top ten in 1H15. See "Exploit families" on page 42 for more information about Axpergle and other exploit kits.
- The encounter rate for Win32/Ramnit decreased from 0.52 percent in 1Q15 to 0.40 percent in 2Q15 following its disruption in February by the European Cybercrime Center (EC3) with the assistance of the MMPC. For more information, see the entry "Microsoft Malware Protection Center assists in disrupting Ramnit" (February 25, 2015) on the MMPC blog at blogs.technet.com/mmpc.
- Families that dropped out of the list of the most commonly encountered malware families between 2H14 and 1H15 include the downloader families Win32/Tugspay and Win32/Ogimant and the exploit kit family Win32/Anogre.

Figure 55 and Figure 56 show trends for the top unwanted software families that were detected on computers by Microsoft real-time antimalware products worldwide in 1H15.

Figure 55. Quarterly trends for the top five unwanted software families encountered by Microsoft real-time antimalware products in 1H15, shaded according to relative encounter rate

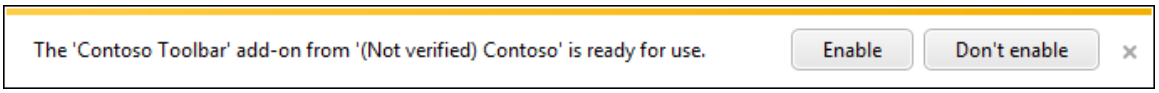
	Family	Most Significant Category	3Q14	4Q14	1Q15	2Q15
1	Win32/KipodToolsCby	Browser Modifiers	—	—	3.22%	2.03%
2	Win32/CouponRuc	Browser Modifiers	—	1.80%	2.39%	2.50%
3	Win32/SaverExtension	Adware	—	—	2.83%	0.83%
4	Win32/IeEnablerCby	Browser Modifiers	—	—	1.67%	0.11%
5	Win32/InstalleRex	Software Bundlers	—	—	0.00%	1.34%

Figure 56. Encounter rate trends for the top unwanted software families in 1H15



- All of the five most commonly encountered unwanted software families in 1H15 were first detected in 4Q14 or 1Q15.
- Win32/KipodToolsCby and Win32/IeEnablerCby are browser modifiers that bypass user consent dialogs to install software without the user's explicit permission. Microsoft security products started detecting these browser modifiers in January after Microsoft changed its unwanted software detection criteria to include attempts to bypass user consent for actions such as installing new browser add-ons. KipodToolsCby and IeEnablerCby were both encountered at high levels in 1Q15 as Microsoft security products detected and removed large numbers of installations from previous periods. Encounters subsequently decreased significantly in 2Q15, following the removal of these older installations.

Figure 57. An add-on consent dialog bar from Internet Explorer 11. Add-ons that disable consent dialogs are now detected as unwanted software.



For more information about this change and its ramifications, see the following entries on the MMPC blog at blogs.technet.com/mmpc:

- Staying in control of your browser: New detection changes (October 17, 2014)

- A timeline of consent and control (December 11, 2014)

- Win32/CouponRuc is an adware program that installs a browser extension without user consent. It can prevent the user from removing it or other add-ons normally, or changing other browser settings.
- Win32/SaverExtension is an adware program that displays advertisements on webpages without identifying itself as the source, which is a violation of Microsoft's objective criteria for classifying unwanted software.[20] It can also install additional browser extensions that the user cannot remove normally.
- Win32/InstalleRex is a software bundler that installs unwanted software, including CouponRuc and SaverExtension. It can be installed by third-party software bundlers. When it installs itself, it alters its own "Installed On" date in Programs and Features to be a year older than the actual date of installation, so that a user who tries to remove it by looking at recently installed programs might have difficulty identifying it.

> KipodToolsCby and IeEnablerCby are browser modifiers that bypass user consent dialogs to install software without the user's explicit permission.

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 might be caused by simple random variation.

As Figure 58 demonstrates, the threats encountered by client and server platforms tend to be quite different.

[20] Microsoft has published the criteria that the company uses to classify programs as unwanted software at www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx. For programs that have been classified as 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.

Figure 58. The malware and unwanted software families most commonly encountered on supported Windows client and server platforms in 2Q15

	Client family	Most significant category	2Q15	Server family	Most significant category	2Q15
1	Win32/CouponRuc	Browser Modifiers	2.56%	Win32/Peals	Trojans	0.40%
2	Win32/KipodToolsCby	Browser Modifiers	2.03%	Win32/KipodToolsCby	Browser Modifiers	0.38%
3	Win32/InstalleRex	Software Bundlers	1.41%	Win32/Crowti	Ransomware	0.33%
4	Win32/Obfuscator	Obfuscators & Injectors	1.11%	Win32/Conficker	Worms	0.32%
5	Win32/AlterbookSP	Browser Modifiers	0.85%	Win32/AlterbookSP	Browser Modifiers	0.28%
6	Win32/SaverExtension	Adware	0.85%	Win32/Sality	Viruses	0.28%
7	Win32/Kilim	Trojans	0.71%	Win32/Skeeyah	Trojans	0.27%
8	VBS/Jenxcus	Worms	0.71%	Win32/Obfuscator	Obfuscators & Injectors	0.24%
9	Win32/Gamarue	Worms	0.71%	INF/Autorun	Obfuscators & Injectors	0.23%
10	Win32/Skeeyah	Trojans	0.70%	JS/Axpergle	Exploits	0.22%

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- Unwanted software was encountered significantly more often on client platforms than on server platforms. Five of the top ten families encountered by client versions of Windows in 1Q15—Win32/CouponRuc, Win32/KipodToolsCby, Win32/InstalleRex, Win32/AlterbookSP, and Win32/SaverExtension—were unwanted software families, compared to just two (KipodToolsCby and AlterbookSP) of the top ten families encountered on servers. The discrepancy reflects the very different ways servers are used to access the Internet, enforced by features such as Enhanced Security Configuration in Internet Explorer.

Attackers often use PHP-based malware to compromise vulnerable servers.

- PHP/SimpleShell was only the 515th most prevalent family overall in 2Q15, but ranked 13th on server platforms. When installed on a compromised web server, it creates a webpage that an attacker can use to run shell commands on the server. A number of popular content management systems (CMSes) are written in the PHP scripting language, including WordPress, Drupal, and MediaWiki, and attackers often use PHP-based malware to compromise vulnerable servers for purposes such as sending spam and hosting exploit kit landing pages.

Figure 59 and Figure 60 demonstrate how detections of the most prevalent malware and unwanted software families in 2Q15 ranked differently on different operating system/service pack combinations.

Figure 59. The malware families most commonly encountered by Microsoft real-time antimalware solutions in 2Q15, and how they ranked in prevalence on different platforms

Rank 2Q15	Family	Most significant category	Rank (Windows Vista SP2)	Rank Windows 7 SP1)	Rank (Windows 8 RTM)	Rank (Windows 8.1 RTM)
1	Win32/Obfuscator	Obfuscators & Injectors	2	2	3	1
2	VBS/Jenxcus	Worms	11	5	1	4
3	Win32/Gamarue	Worms	9	6	2	3
4	Win32/Kilim	Trojans	3	3	7	5
5	Win32/Skeeyah	Trojans	4	7	5	2
6	Win32/Peals	Trojans	1	4	6	7
7	JS/Axpergle	Exploits	82	1	340	130
8	INF/Autorun	Obfuscators & Injectors	8	8	4	6
9	Win32/Sality	Viruses	48	9	10	8
10	Win32/Ramnit	Trojans	45	13	9	9

Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- Encounters involving JS/Axpergle, a detection for the Angler exploit kit and the only exploit-related family in the top ten in 1H15, were almost entirely confined to computers running Windows 7; although Axpergle ranked first on that platform, it ranked 82nd on Windows Vista and ranked outside the top 100 on Windows 8 and Windows 8.1. The malicious webpages that exploit kits use to spread malware often include scripts that detect certain aspects of the computer's computing environment and only present their exploits to computers that meet criteria specified by the attacker. The Angler exploit kit clearly affects Windows 7 far more than other platforms, which may partially be caused by the integration of Adobe Flash Player into Internet Explorer in Windows 8 and 8.1. The Angler exploit kit relies heavily on exploiting vulnerabilities in old, out-of-date versions of Flash Player, which must be installed as an add-on and updated separately from Internet Explorer in versions of Windows prior to Windows 8. Because Flash Player is integrated into Internet Explorer in Windows 8 and Windows 8.1, it receives security updates through Windows Update and Microsoft Update along with other operating system components, which makes it easier for users to stay current on security updates for the component.
- Apart from Axpergle, the list of the most commonly encountered malware families was largely consistent from platform to platform. Win32/Peals,

Win32/Skeeyah, and Win32/Obfuscator were all among the five most commonly encountered malware platform on each supported client platform.

Figure 60. The unwanted software families most commonly encountered by Microsoft real-time antimalware solutions in 2Q15, and how they ranked in prevalence on different platforms

Rank 2Q15	Family	Most significant category	Rank (Windows Vista SP2)	Rank Windows 7 SP1)	Rank (Windows 8 RTM)	Rank (Windows 8.1 RTM)
1	Win32/CouponRuc	Browser Modifiers	2	1	1	1
2	Win32/KipodToolsCby	Browser Modifiers	1	2	2	3
3	Win32/InstalleRex	Software Bundlers	6	4	3	2
4	Win32/SaverExtension	Adware	4	5	4	4
5	Win32/AlterbookSP	Browser Modifiers	3	3	5	5

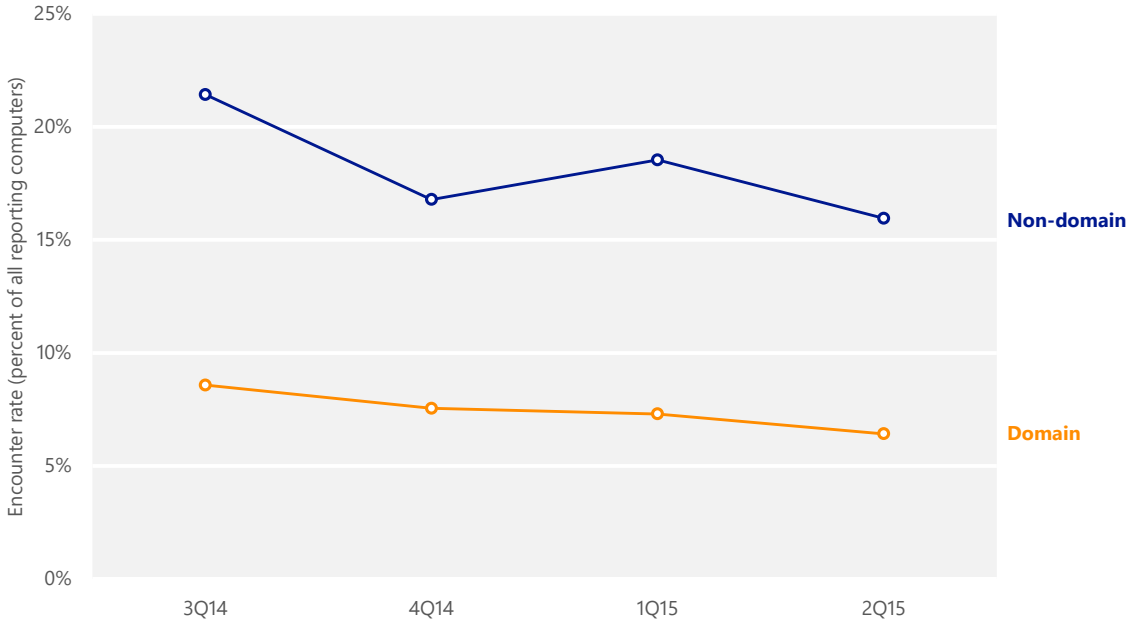
- Unlike malware, unwanted software delivery mechanisms typically make little effort to distinguish between different platforms, and as a result the list of the most commonly encountered unwanted software families is almost identical on each supported platform.

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. These different usage patterns mean that home users tend to be exposed to a different mix of computer threats than enterprise users.

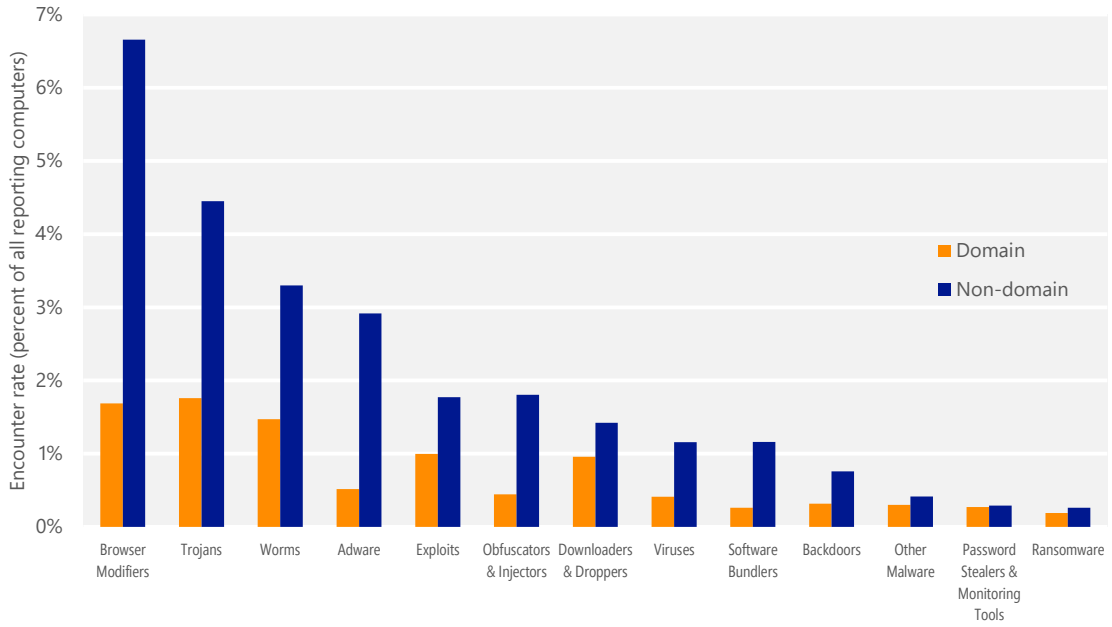
The infection telemetry data produced by Microsoft antimalware products and tools includes information about whether the infected computer belongs to an Active Directory Domain Services (AD DS) domain. Such domains are used almost exclusively in enterprise environments, and computers that do not belong to a domain are more likely to be used at home or in other non-enterprise contexts. Comparing the threats encountered by domain-joined computers and non-domain computers can provide insights into the different ways attackers target enterprise and home users and which threats are more likely to succeed in each environment.

Figure 61. Malware encounter rates for domain-based and non-domain computers, 3Q14–2Q15



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

Figure 62. Malware and unwanted software encounter rates for domain-based and non-domain computers, 1H15, by category



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- 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. As Figure 61 shows, the encounter rate for consumer computers was about 2.5 times as high as the rate for enterprise computers in 1H15.

- In addition to encountering less malware in general, computers in enterprise environments tend to encounter different kinds of threats than consumer computers, as shown in Figure 62. Non-domain computers encountered disproportionate amounts of unwanted software compared to domain-based computers, with Adware, Browser Modifiers, and Software Bundlers each appearing between three and six times as often on non-domain computers. Meanwhile, domain-based computers encountered Password Stealers & Monitoring Tools malware nearly as often as their non-domain counterparts, despite encountering less than half as much malware as non-domain computers overall.

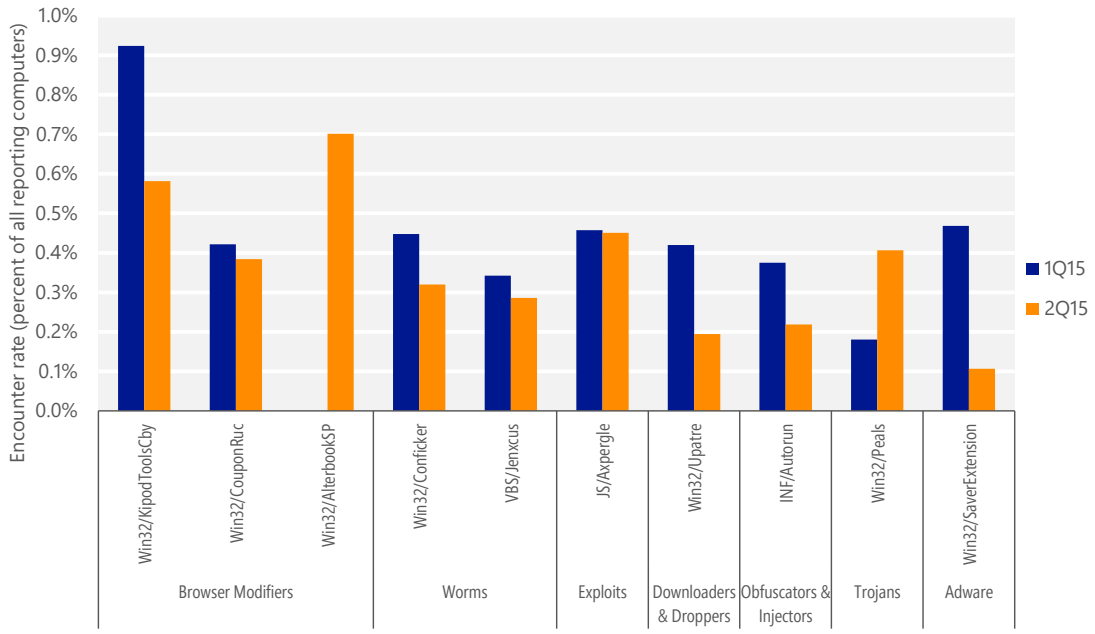
Enterprise computers tend to encounter malware at a lower rate than consumer computers.

  - One password stealer in particular, Win32/Dyzap, was encountered by domain-based computers more than four times as often as non-domain computers (an encounter rate of 0.12 percent on domain-based computers, compared to 0.03 percent on non-domain computers.) Dyzap steals login credentials for a long list of banking websites using man-in-the-browser (MITB) attacks. It is usually installed on the infected computer by the downloader family Win32/Upatre, which is typically delivered via social engineering techniques that target enterprise audiences (for example, spam messages that mimic business faxes or overnight package delivery notifications).

Figure 63 and Figure 64 list the top 10 malware families detected on domain-joined and non-domain computers, respectively, in 1H15.

Figure 63. Quarterly trends for the top 10 malware and unwanted software families detected on domain-joined computers in 1H15, by percentage of computers encountering each family

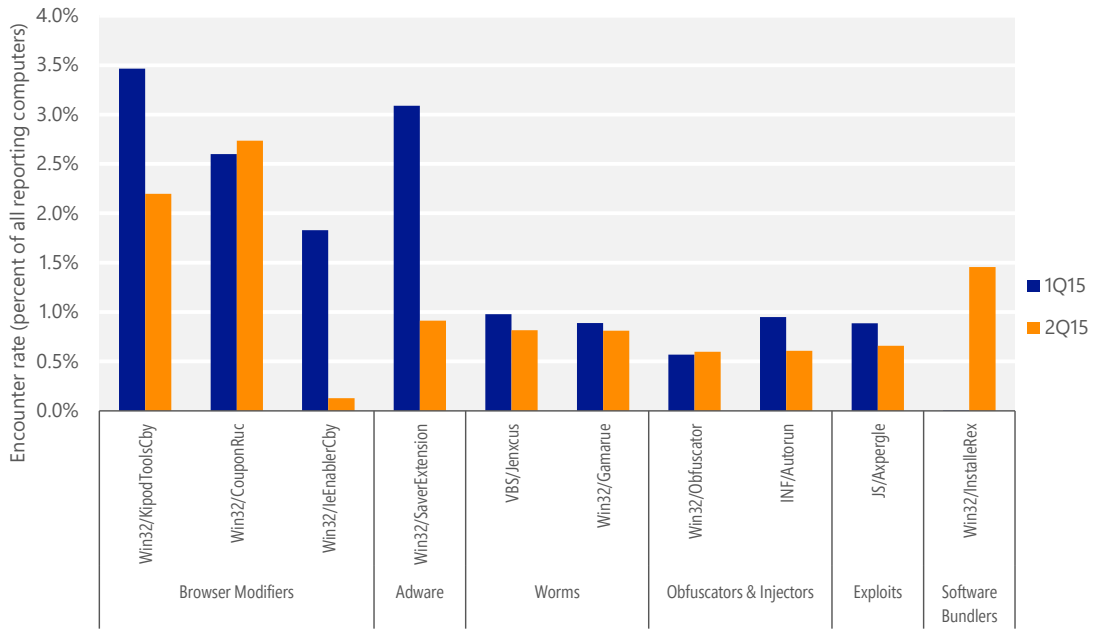
Family	Most significant category	1Q15	2Q15
Win32/KipodToolsCby	Browser Modifiers	0.92%	0.58%
JS/Axpergle	Exploits	0.46%	0.45%
Win32/CouponRuc	Browser Modifiers	0.42%	0.38%
Win32/Conficker	Worms	0.45%	0.32%
Win32/AlterbookSP	Browser Modifiers	—	0.70%
VBS/Jenxcus	Worms	0.34%	0.29%
Win32/Upatre	Downloaders & Droppers	0.42%	0.19%
INF/Autorun	Obfuscators & Injectors	0.38%	0.22%
Win32/Peals	Trojans	0.18%	0.41%
Win32/SaverExtension	Adware	0.47%	0.11%



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

Figure 64. Quarterly trends for the top 10 malware and unwanted software families detected on non-domain computers in 1H15, by percentage of computers encountering each family

Family	Most significant category	1Q15	2Q15
Win32/KipodToolsCby	Browser Modifiers	3.47%	2.20%
Win32/CouponRuc	Browser Modifiers	2.60%	2.74%
Win32/SaverExtension	Adware	3.09%	0.91%
Win32/Obfuscator	Obfuscators & Injectors	1.13%	1.18%
Win32/IeEnablerCby	Browser Modifiers	1.83%	0.13%
VBS/Jenxcus	Worms	0.98%	0.82%
Win32/Gamarue	Worms	0.89%	0.81%
INF/Autorun	Obfuscators & Injectors	0.95%	0.61%
JS/Axpergle	Exploits	0.89%	0.66%
Win32/InstalleRex	Software Bundlers	0.004%	1.46%



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- Six families—INF/Autorun, JS/Axpergle, Win32/CouponRuc, Win32/KipodToolsCby, VBS/Jenxcus, and Win32/SaverExtension—were common to both lists. All were more frequently encountered on non-domain computers than on domain-joined computers. See "Threat families" on page 74 for more information about these families.

- The four families that were unique to the top 10 list for domain-joined computers but not for non-domain computers are the worm family Win32/Conficker, the browser modifier Win32/AlterbookSP, the downloader family Win32/Upatre, and the trojan family Win32/Peals.
- Conficker is a worm that was disrupted several years ago, but continues to be encountered in domain environments because of its use of a built-in list of common and weak passwords to spread between computers.
- AlterbookSP is a browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
- Upatre installs malware and unwanted software on the affected computer without the user's consent. It is frequently distributed as an attachment to spam email messages. For more information about Upatre and how it spreads, see the following entries in the MMPC blog at blogs.technet.com/mmpc:
  - Wire transfer spam spreads Upatre (December 12, 2014)
  - Upatre update: infection chain and affected countries (March 12, 2015)

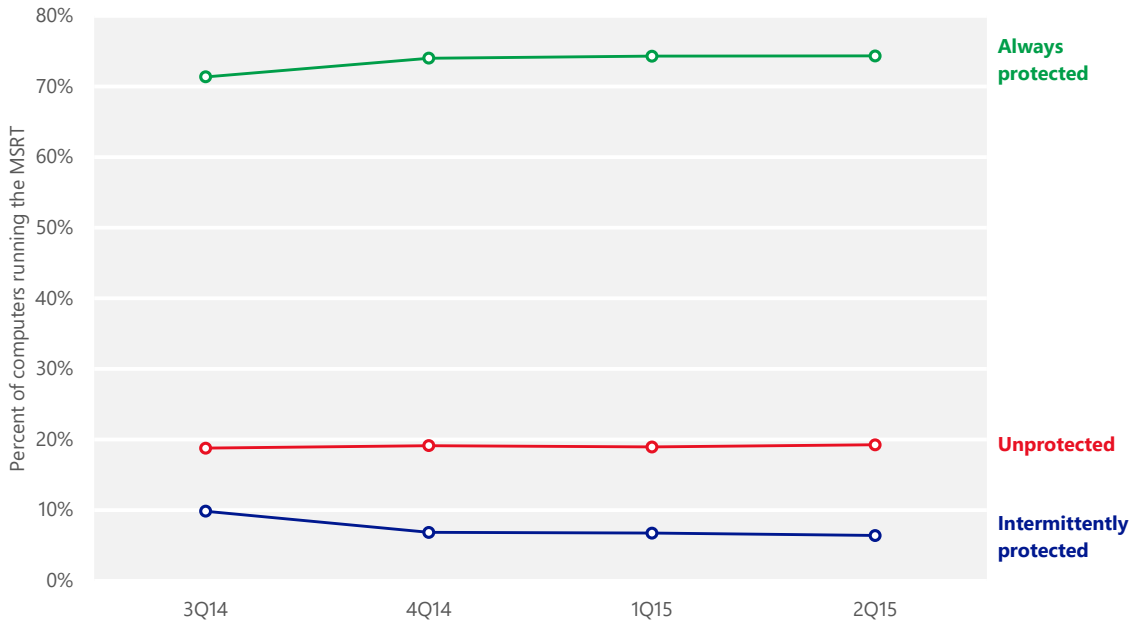
Conficker was disrupted several years ago, but continues to be encountered in domain environments because of its use of a built-in list of common and weak passwords to spread between computers.

See "Malware at Microsoft: Dealing with threats in the Microsoft environment" on page 110 for information about the threat landscape on computers at Microsoft and to learn about the actions Microsoft IT takes to protect users, data, and resources.

Security software use

Recent releases of the MSRT collect and report details about the state of real-time antimalware software on a computer, if the computer's administrator has chosen to opt in to provide data to Microsoft. This telemetry data makes it possible to analyze security software usage patterns around the world and correlate them with infection rates. Figure 65 shows the percentage of computers worldwide that the MSRT found to be protected or unprotected by real-time security software each quarter in 2H14 and 1H15.

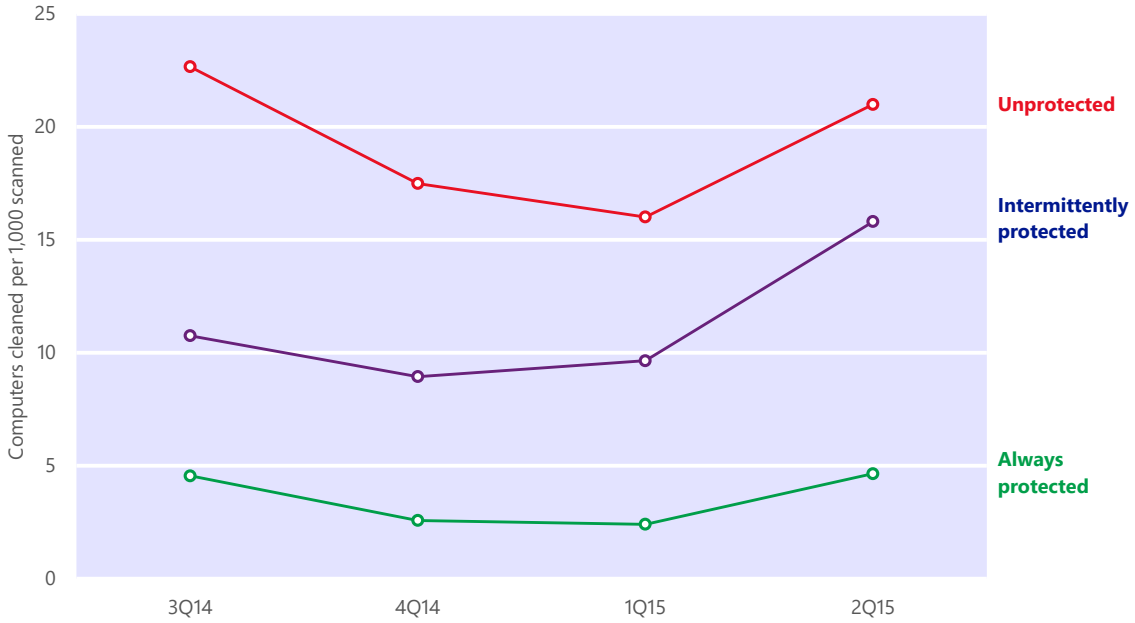
Figure 65. Percentage of computers worldwide protected by real-time security software, 3Q14–2Q15



- A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In Figure 65, "Protected" represents computers that had real-time security software active and up-to-date every time the MSRT ran during a quarter; "Intermittently protected" represents computers that had security software active during one or more MSRT executions, but not all of them. "Unprotected" represents computers that did not have security software active during any MSRT executions that quarter.
- Overall, about three-fourths of computers worldwide were found to be always protected at every monthly MSRT execution in each of the past four quarters, varying between 71.4 percent and 74.3 percent.
- Computers that never reported running security software accounted for between 18.8 and 19.3 percent of computers worldwide each quarter. Intermittently protected computers—those that were found to be running real-time security software during at least one MSRT execution in a quarter, but not all of them—accounted for between 6.4 and 9.9 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 66 compares infection rates with protection levels worldwide for each of the last four quarters.

Figure 66. Infection rates for protected and unprotected computers, 3Q14–2Q15



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- The MSRT reported that computers that were never found to be running real-time security software during 1H15 were about six times as likely to be infected with malware as computers that were always found to be protected.
- Computers that were intermittently protected were about three times more likely to be infected with malware in 1H15 than computers that were always protected.
- Users who don't run real-time security software aren't always unprotected by choice: a number of prevalent malware families are capable of disabling some security products, potentially without the user even knowing. Other users might 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 might come pre-installed with their computers as limited-time trial software. (See "The challenge of expired security software" on pages 21–28 of *Microsoft Security Intelligence Report, Volume 17 (January–June 2014)*, available from the Microsoft Download Center, for more information about

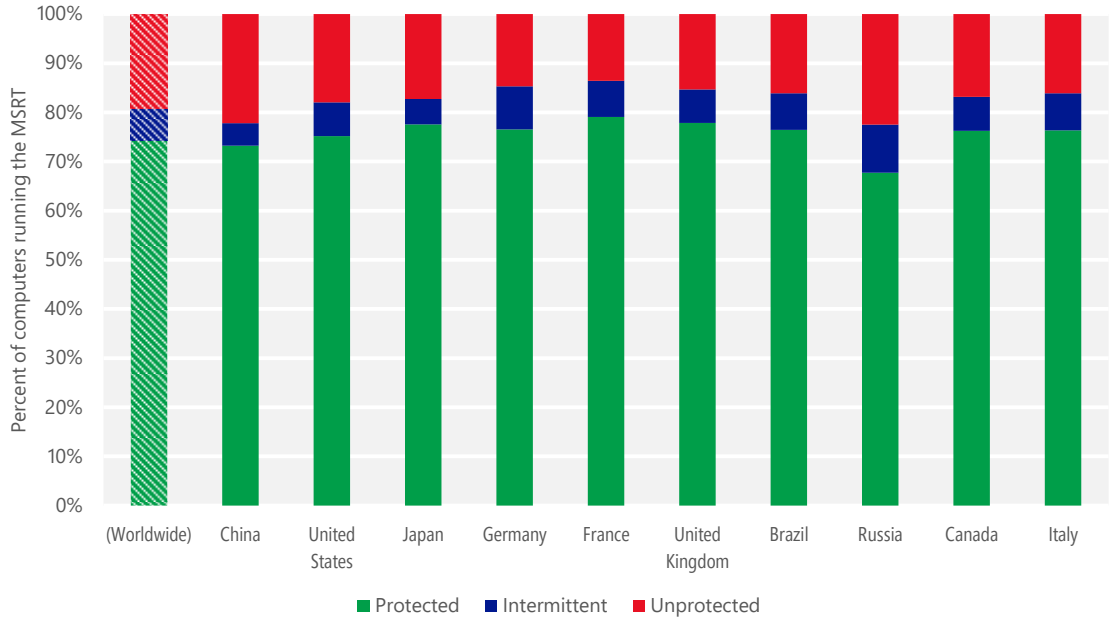
> Users who don't run real-time security software aren't always unprotected by choice.

the causes and consequences of expired security 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 66 illustrates.

Security software use worldwide

Just as infection and encounter rates differ from one country or region to another, so do security software usage rates, as shown in Figure 67.

Figure 67. Average security software protection state for the locations with the most computers executing the MSRT in 1H15



- Computers that reported being fully protected in these locations ranged between 67.7 percent and 79.1 percent, with all locations except China and Russia exceeding the worldwide rate of 74.3 percent of computers reporting as fully protected.
- Computers that reported being fully unprotected in these locations ranged between 13.6 percent and 22.5 percent, with Russia and China reporting larger percentages of fully unprotected computers than the world overall.
- Computers that were protected in some months but not in others accounted for between 4.6 percent and 9.8 percent in these locations.

The rate of security software usage in a country or region often correlates with its infection rate. Figure 68 and Figure 69 show the percentage of computers in

different countries and regions that reported being fully protected and fully unprotected, respectively, in 2Q15.

Figure 68. Percent of computers reporting as Protected during every MSRT execution in 2Q15, by country/region

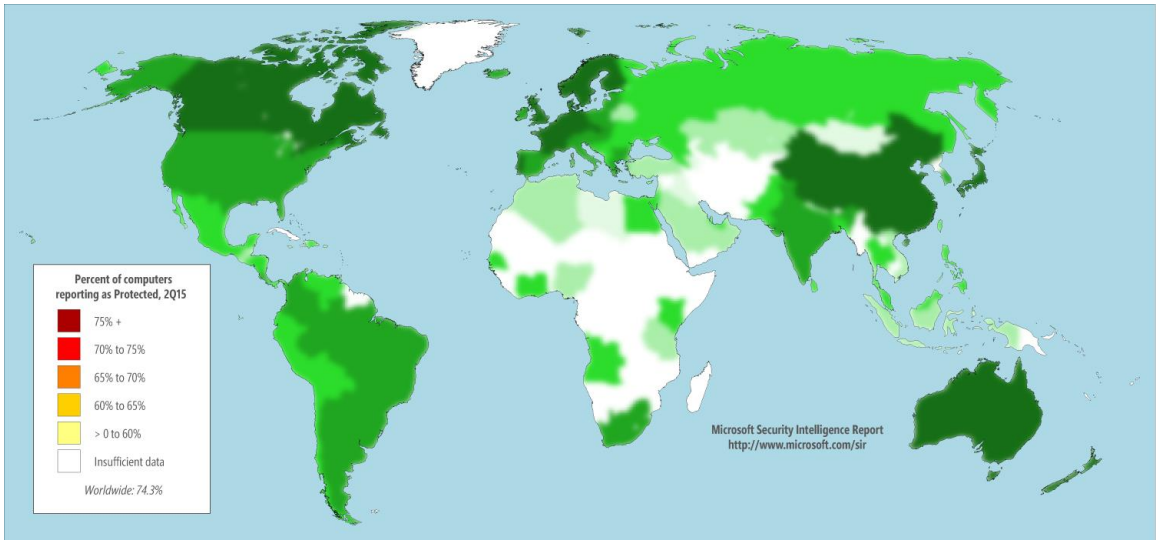
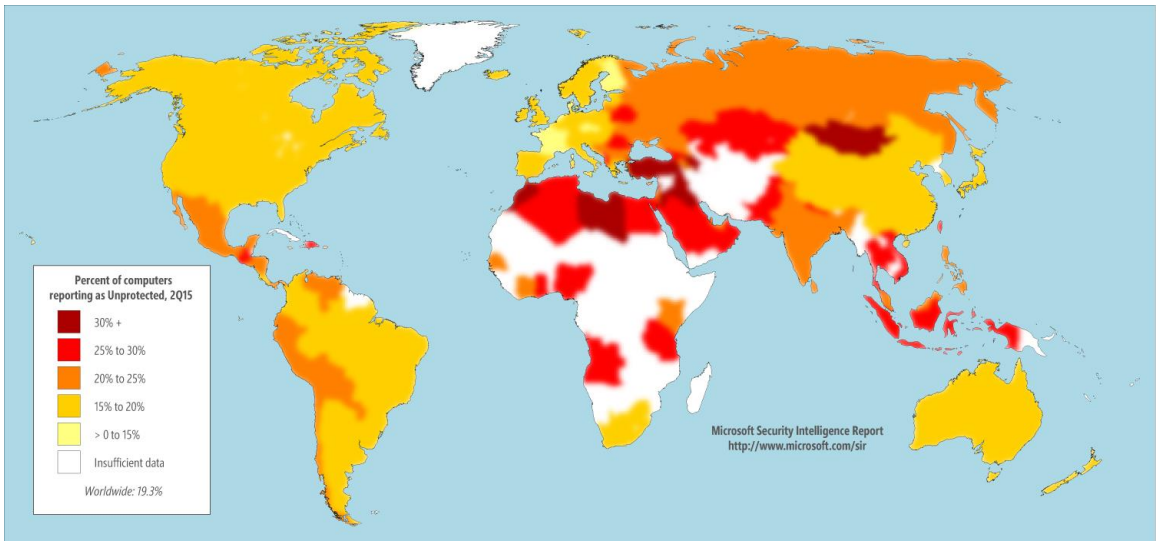


Figure 69. Percent of computers reporting as Unprotected during every MSRT execution in 2Q15, by country/region



- The locations with the most computers reporting as fully protected by real-time security software include Finland, with 83.9 percent of computers reporting as fully protected in 2Q15; Denmark, at 79.5 percent; and Norway, at 78.9 percent. Locations with the fewest computers reporting as fully protected include Libya, at 46.9 percent; Iraq, at 53.3 percent; and Azerbaijan, at 57.9 percent.

- The ranking of countries and regions by unprotected rate is largely an inverse of their ranking according to protected rate. The locations with the fewest computers reporting as fully unprotected include Finland, at 10.4 percent; Denmark, at 14.2 percent; and the Czech Republic, at 14.4 percent. Locations with the most computers reporting as fully unprotected include Libya, at 41.7 percent; Iraq, at 39.5 percent; and Azerbaijan, at 32.5 percent.

Countries and regions with high percentages of computers reporting as fully unprotected also tend to have high infection rates, as Figure 70 shows.

Figure 70. Infection rates for the locations with the highest percentage of computers reporting as fully unprotected in 1H15

Country/region	1H15 average unprotected %	CCM 1Q15	CCM 2Q15	Unprotected CCM 1Q15	Unprotected CCM 2Q15
Libya	40.76%	61.0	69.8	126.8	145.5
Iraq	39.29%	76.6	80.2	178.0	187.8
Azerbaijan	32.19%	29.0	34.1	72.5	80.7
Mongolia	32.19%	66.8	77.6	178.4	202.3
Morocco	32.19%	58.2	66.6	162.7	181.5
Palestinian Authority	32.18%	59.5	68.7	157.3	182.0
Jordan	31.04%	36.6	45.3	98.8	120.4
Turkey	30.24%	22.5	26.3	59.7	63.6
Lebanon	30.22%	31.7	42.5	90.9	114.3
Vietnam	29.71%	30.4	35.8	77.6	92.6
Worldwide	*19.11%*	*5.4*	*8.4*	*15.7*	*20.7*

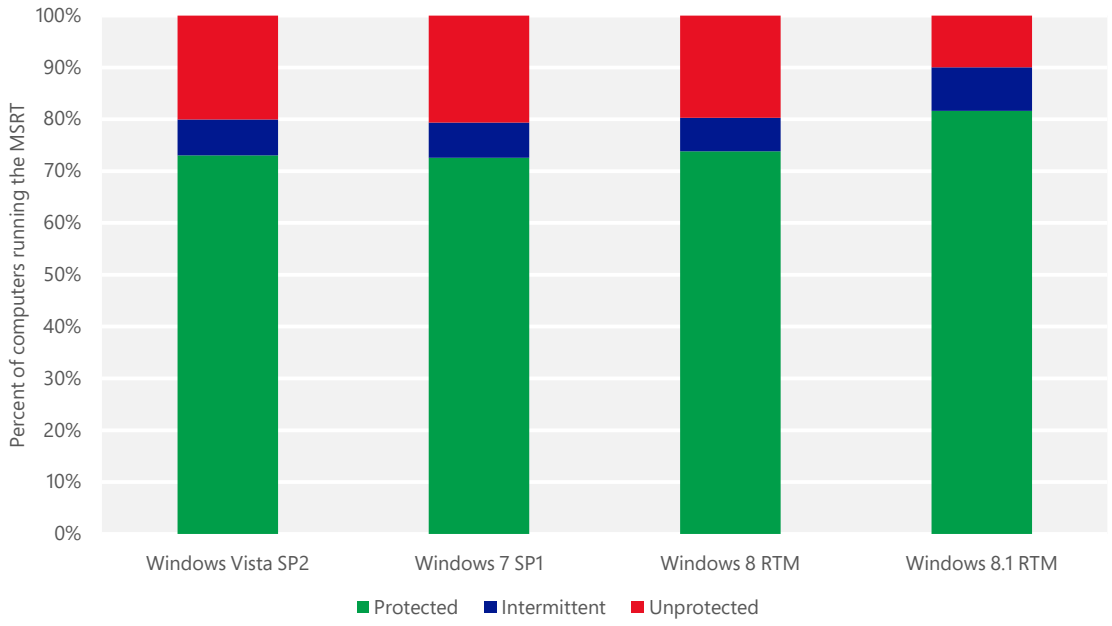
Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 60 for more information.

- The locations in the table all had overall infection rates ranging between 3.1 and 14.2 times as high as the worldwide average each quarter.
- The infection rates for fully unprotected computers in these locations ranged between 3.1 and 11.4 times as high as the infection rates for fully unprotected computers worldwide, and between 7.6 and 33.0 times as high as the infection rates for all computers worldwide. In Mongolia, the location with the highest infection rates in Figure 70, the MSRT detected and removed malware on 20.2 percent of the fully unprotected computers that executed it at least once in 2Q15 (a CCM of 202.3).

Security software use by platform

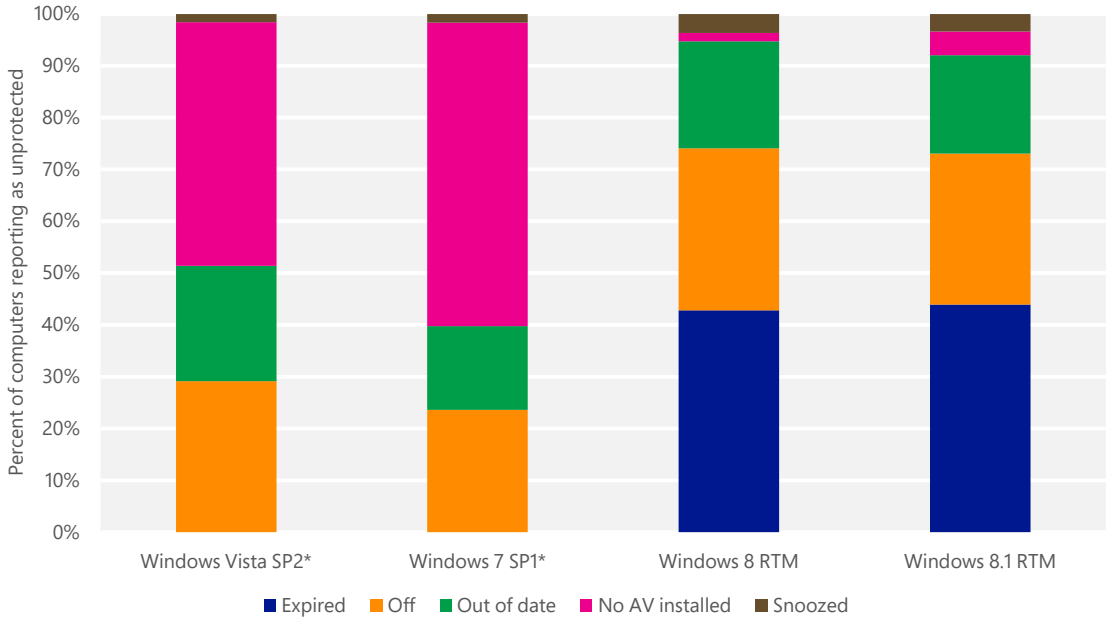
Protection rates can also vary by operating system, as shown in Figure 71.

Figure 71. Average quarterly security software protection state for supported client versions of Windows in 1H15



- Only 10.0 percent of computers running Windows 8.1 reported being unprotected during every MSRT execution each quarter on average, about half of the rate reported by computers running any other supported client version of Windows. At the same time, Windows 8.1 had a higher rate of intermittent protection than any other platform, primarily because of active security products expiring during the period. In most cases, this is probably because of commercial security products pre-installed on new computers with trial subscriptions that expire within a few months unless the purchaser pays to extend the subscription.
- The reasons computers go unprotected can vary significantly by platform, as Figure 72 illustrates.

Figure 72. Status reported by unprotected computers running supported client versions of Windows in 1H15



* Windows Vista and Windows 7 do not report expired subscriptions.

- On Windows Vista and Windows 7, unprotected computers predominantly report having no antimalware software installed at all. On Windows 8 and Windows 8.1, Windows Defender is enabled by default if no other antimalware software is present, so the number of computers reporting no antimalware software is very low.
- On Windows 8 and Windows 8.1, expired versions of commercial antimalware products that are no longer receiving signature updates account for the largest percentage of unprotected computers.

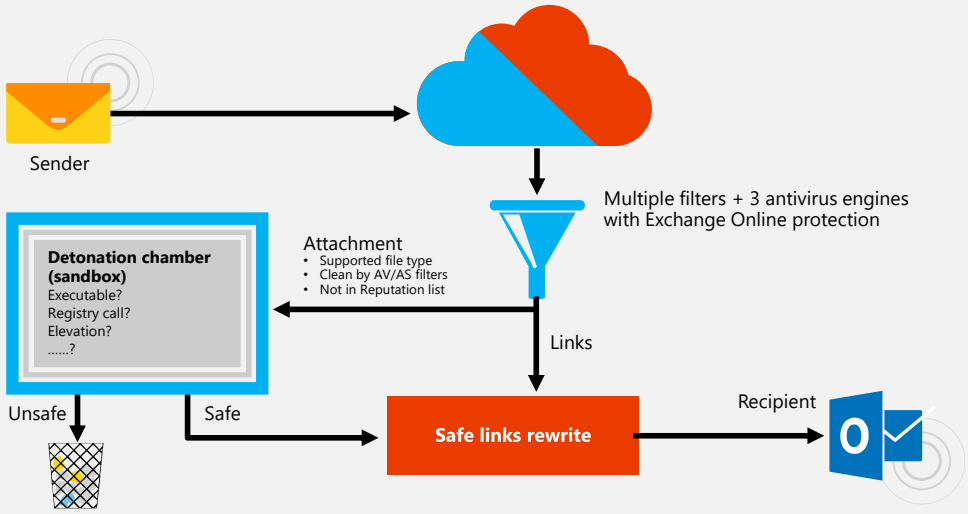
Advanced Threat Protection takes malware defense to the next level

Computer security is a constant arms race: security professionals and antimalware vendors continually seek ways to better protect computers and people from harm, while attackers continually look for ways to defeat those protections. Conventional antimalware products offer protection against known threats, but are significantly less effective against unknown and unidentifiable malware. The advent of targeted attack groups, such as the one described in "STRONTIUM: A profile of a persistent and motivated adversary" beginning on page 3, has raised the bar for defenders, as these groups often have the resources to craft custom malware variants and test them against popular security products to ensure that they will not be detected. Although security

software vendors try to respond to new threats with detection signature updates as quickly as possible, new malware variants may still have several crucial hours or days to compromise computers, free from detection.

Office 365 and Exchange Online seek to close that gap for their customers with Advanced Threat Protection, which was introduced earlier this year. For years, Exchange Online has offered customers multiple layers of protection from malicious files, including scanning incoming email attachments with multiple antimalware engines from different vendors to take advantage of a broad set of detection signatures and capabilities. Now, Advanced Threat Protection provides an additional layer of defense against threats and malicious links that have never been seen before.

Figure 73. How Advanced Threat Protection works with Exchange Online



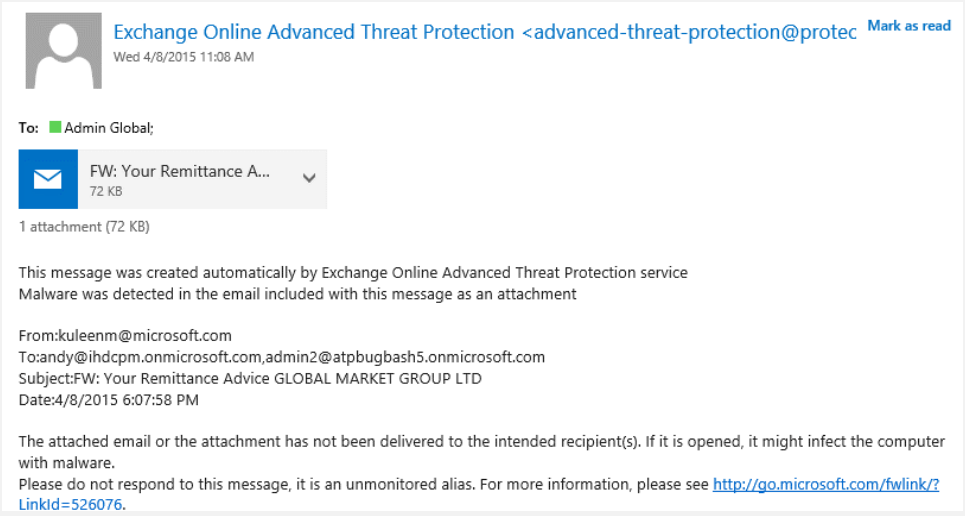
Safe attachments

Using a real-time security software product from a reputable vendor and keeping the detection signatures up-to-date remains one of the best ways individuals and organizations can protect themselves against most of the threats they face. Antimalware software relies predominately on detection signatures written to target specific malicious binaries, or groups of closely related threats that can be detected heuristically. This approach can be a very effective defense against most malware, which attackers typically try to distribute widely in order to compromise large numbers of computers for their purposes. Unfortunately, conventional antimalware software is often less effective against targeted attacks mounted by groups such as STRONTIUM (see page 3). These groups, which focus on targeting computers at specific institutions, often use specially crafted threats that they test against popular antimalware solutions ahead of time to

ensure that they will not be detected. By the time detection signatures are available to stop such a threat, it may have already compromised the organization.

Exchange Online Advanced Threat Protection adds a new layer of defense against email-borne threats that uses behavioral analysis to detect incoming files that may be harmful, and blocks them before they can reach their intended recipients. When an incoming message includes a potentially dangerous attached file, Exchange Online launches it in a detonation chamber—a virtual sandboxed environment in which potential threats can run without posing harm to any other resources—and monitors it for malicious behavior such as suspicious registry changes, attempts to access memory dumps, changes to executables, and other actions that malware characteristically takes. This monitoring makes it possible to detect and block threats that have never been seen before and for which no detection signatures are available. Exchange Online Advanced Threat Protection includes anti-sandbox detection features such as vulnerability detection to combat advanced threats that avoid taking malicious actions when they determine they are being run in a virtual machine.

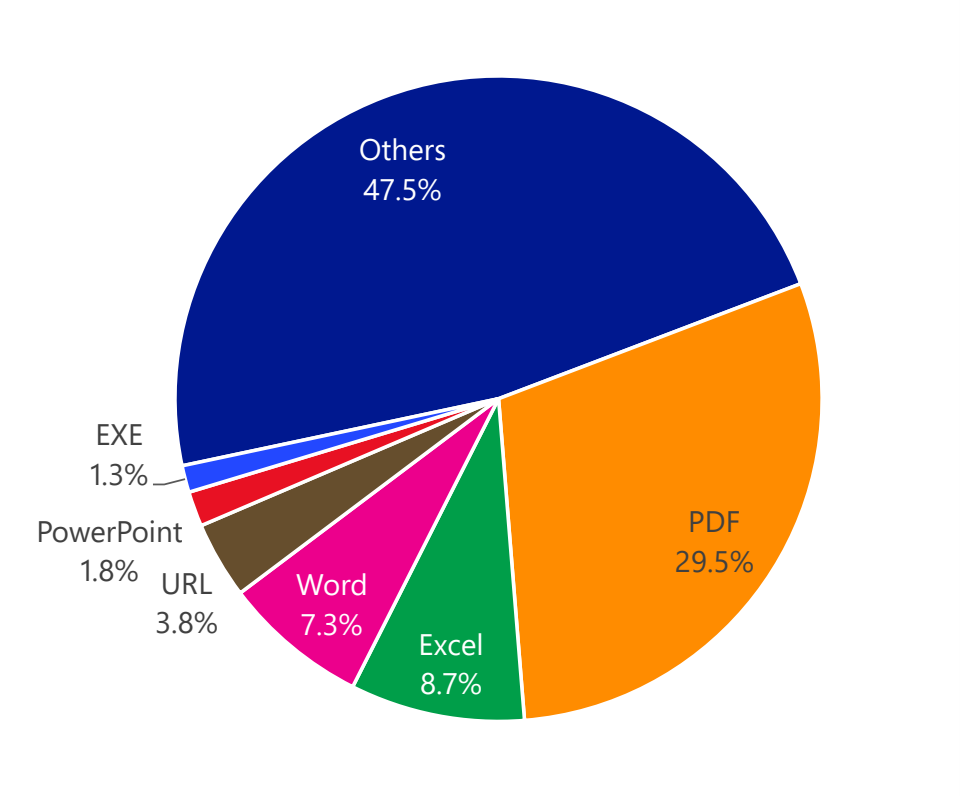
Figure 74. Exchange Online Advanced Threat Protection notifies administrators when malware is detected



Administrators can configure how Exchange Online reacts when it determines that an attachment contains malware. Exchange Online can be configured to block delivery of the message, notify administrators, and include a copy of the blocked message so they can analyze it themselves and determine whether additional action is necessary. The process of analyzing a message typically takes about four to five minutes; administrators can set a 30 minute time limit for

analysis, after which the message will either be delivered or blocked, as administrators see fit.

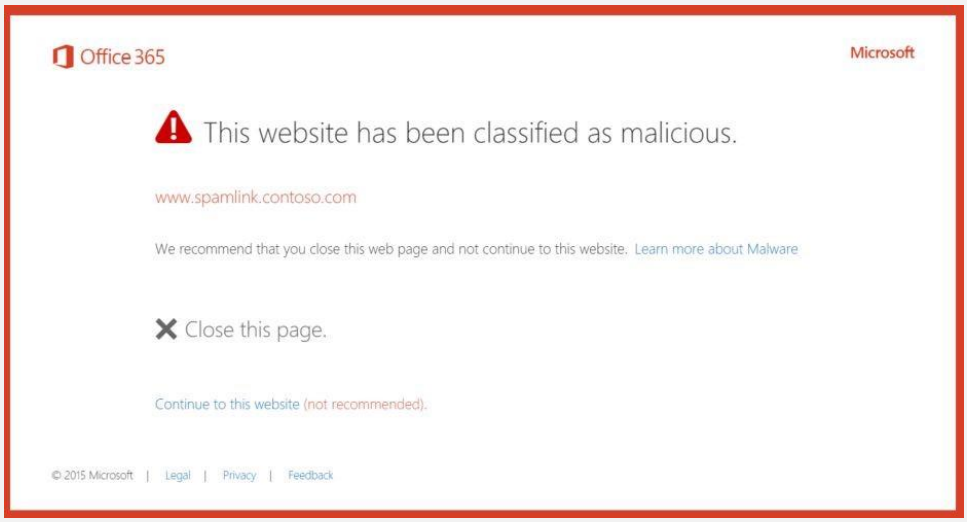
Figure 75. Types of malicious files blocked by Exchange Online Advanced Threat Protection over a two-month period in 2015



Safe links

In addition to sending malware to recipients directly, attackers often send email messages that contain links to malware or drive-by download pages, in hopes that the recipients will click the links and become infected. To provide protection against malicious links, administrators can configure Exchange Online Advanced Threat Protection to rewrite any links in incoming messages to proxy through the Exchange Online service. When a user clicks on a rewritten link, Exchange Online checks the intended destination URL against its database of malicious URLs. If the URL is not determined to be malicious, the user is quickly and seamlessly redirected to their intended destination. If the URL is determined to be malicious, a blocking page is displayed instead. Exchange Online Advanced Threat Protection checks each URL at the time the link is clicked, which means it can protect users from malicious links that were not known to be malicious at the time the message was originally sent.

Figure 76. Exchange Online Advanced Threat Protection blocks malicious links in email messages



Exchange Online Advanced Threat Protection can be configured to track when users clicks malicious links to help administrators monitor potential targeted attacks and determine which computers may have been exposed to malware. Customers with privacy or compliance concerns can disable the link tracking feature.

Advanced Threat Protection is available for subscribers of select Exchange or Office 365 plans for an additional small per-user fee. For more information, see https://products.office.com/exchange/online-email-threat-protection.

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 Help prevent malware infection on your PC at the Microsoft Malware Protection Center website at www.microsoft.com/mmpc.

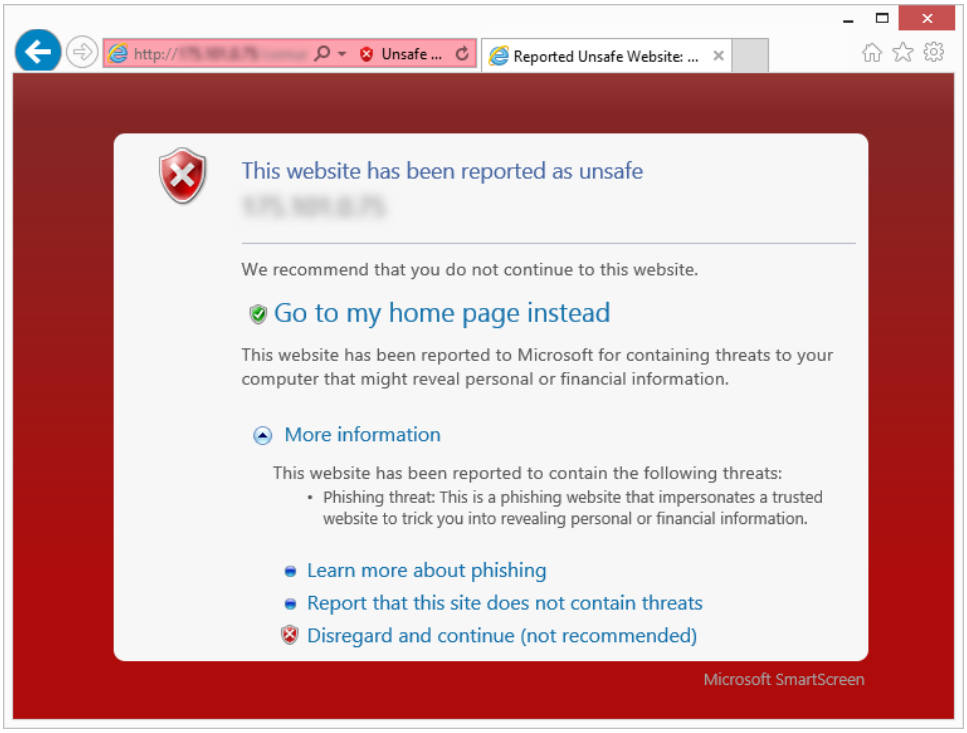
For help understanding the threats that pose the greatest risk to your environment and how to defend against them, see "Fixing the #1 Problem in Computer Security: A Data-Driven Defense," available from Microsoft TechNet.

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 efforts 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 sources, including telemetry data produced by SmartScreen Filter (in Internet Explorer versions 8 through 11 and pre-release versions of Microsoft Edge) 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 77. 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.[21] A phishing impression is a single instance of a user attempting to visit a known phishing site with SmartScreen Filter enabled and being warned, as illustrated in Figure 78.

[21] See "Appendix B: Data sources" on page 129 for information about the products and services used to provide data for this report.

Figure 78. How Microsoft tracks phishing impressions

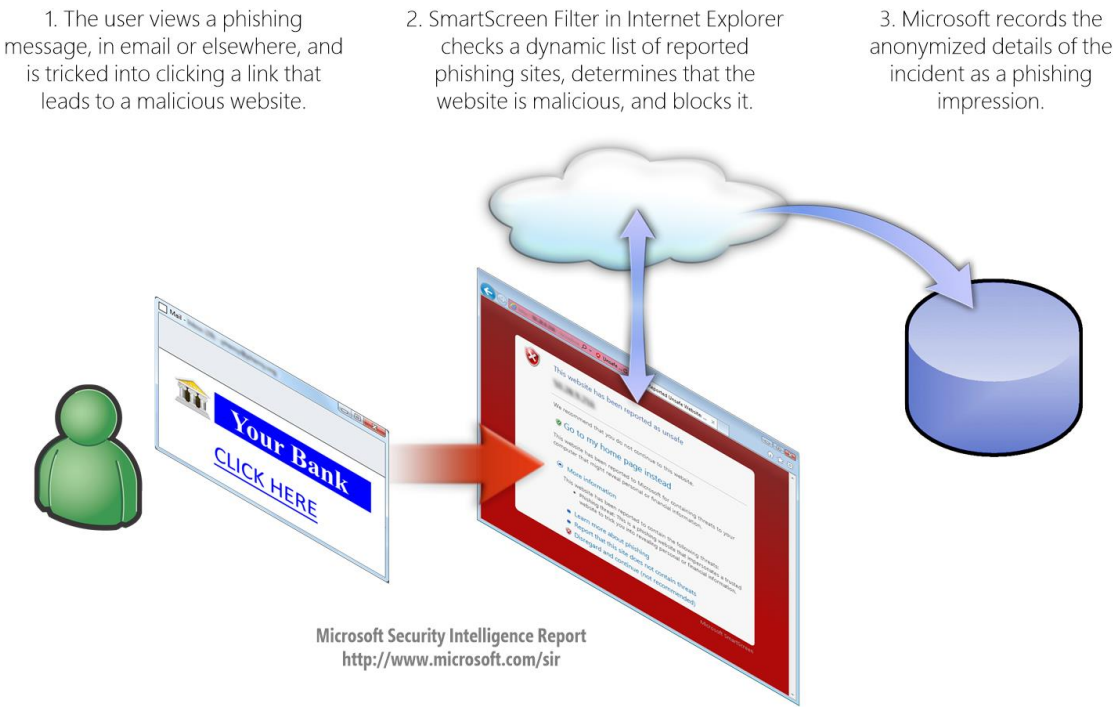
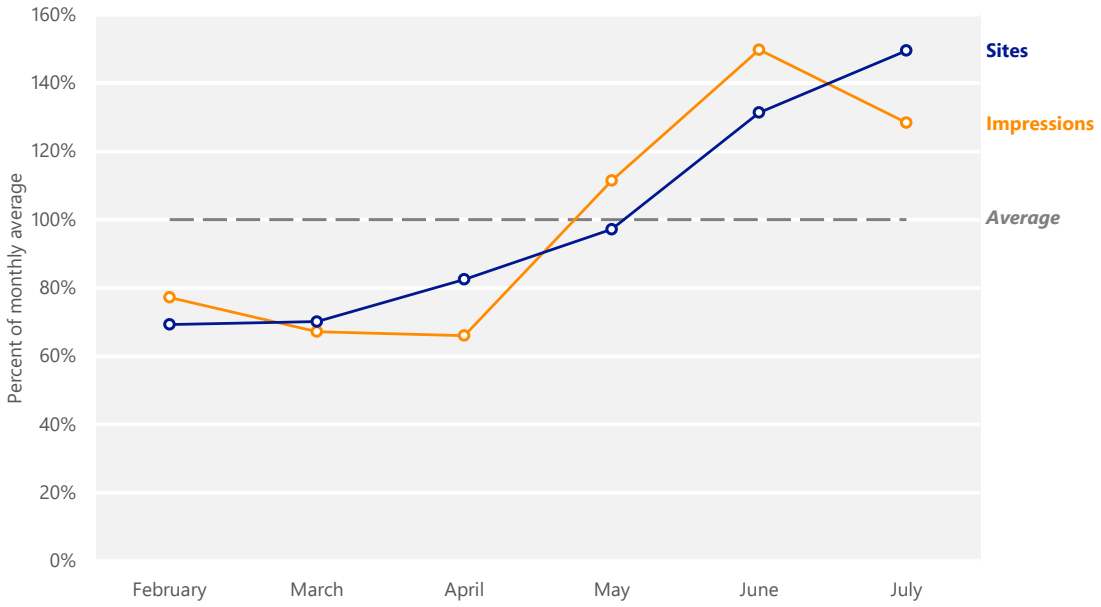


Figure 79 illustrates the volume of phishing impressions tracked by SmartScreen Filter each month from February through July of 2015, compared to the volume of distinct phishing URLs visited.

Figure 79. Phishing sites and impressions reported by SmartScreen Filter, February–July 2015, relative to the monthly average for each

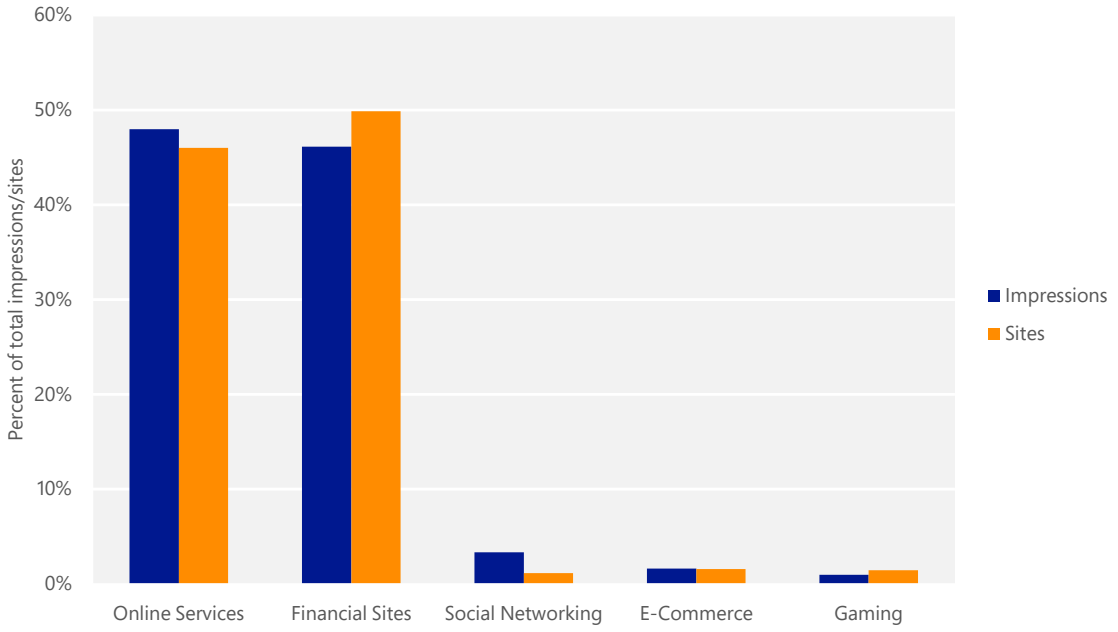


- Numbers of active phishing sites and phishing impressions both increased between February and July, indicative of a general increase in phishing activity. Because phishers are frequently observed using campaigns to drive large amounts of traffic to a relatively small number of pages, however, the two metrics are generally not strongly correlated, and the dual increase through June and July may be largely coincidental.

Target institutions

Some types of sites tend to consistently draw many more impressions per site than others. Figure 80 shows the breakdown of phishing impressions by category as reported by SmartScreen Filter.

Figure 80. Impressions reported by SmartScreen Filter for each type of phishing site, February–July 2015



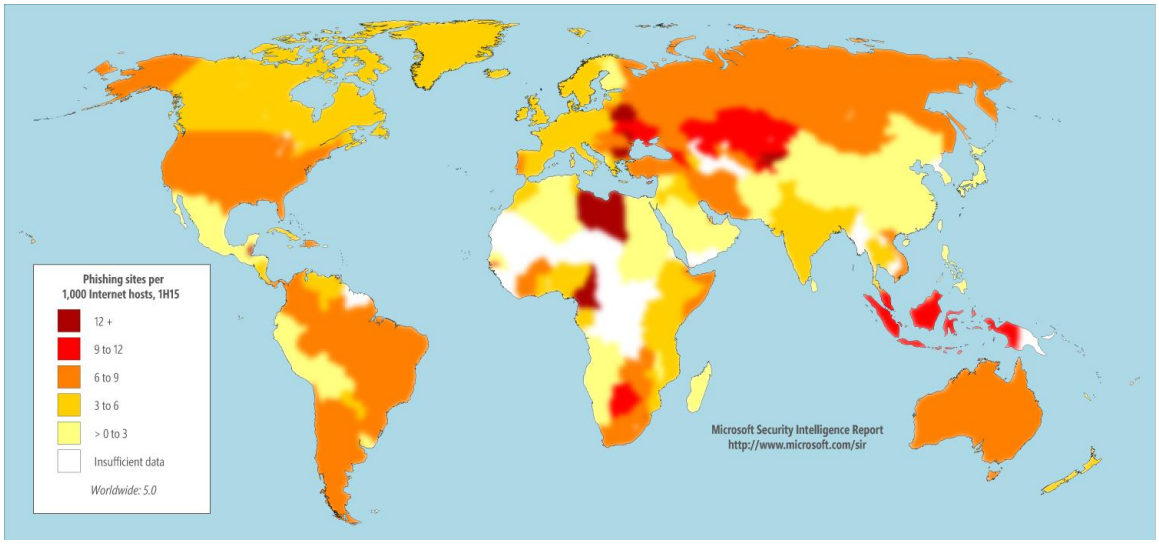
- Financial institutions have always been popular phishing targets because of their potential for providing direct illicit access to victims' bank accounts. Sites that targeted financial institutions accounted for the largest number of active phishing attacks during the period, as well as the second largest number of impressions. (See "Win32/Banload and Banking Malware" on page 21 for information about regional problems with banking malware in Brazil.)

- Phishing sites that targeted online services received the largest share of impressions during the period, and accounted for the second largest number of active phishing URLs.
- The other three categories each accounted for a small percentage of both sites and impressions.

Global distribution of phishing sites and clients

Phishing impression information from SmartScreen Filter includes anonymized information about the IP addresses of the clients making the reports, as well as the IP addresses of the phishing sites themselves. Performing geographic lookups on these addresses makes it possible to analyze patterns among both the computers that host phishing sites and the users that they target.

Figure 81. Phishing sites per 1,000 Internet hosts for locations around the world in 1H15



- SmartScreen Filter detected approximately 5.0 phishing sites per 1,000 Internet hosts worldwide in 1H15.
- Locations hosting higher than average concentrations of phishing sites include Bulgaria (98.5 per 1,000 Internet hosts in 1Q15), Libya (15.6), and Belize (14.5). Locations with low concentrations of phishing sites include Taiwan (1.2), the United Arab Emirates (1.4), and Korea (1.6).

Malware hosting sites

SmartScreen Filter 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 82. SmartScreen Filter in Internet Explorer displays a warning when a user attempts to download an unsafe file

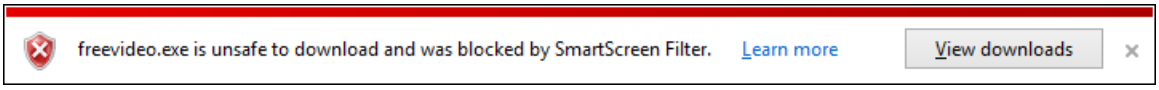
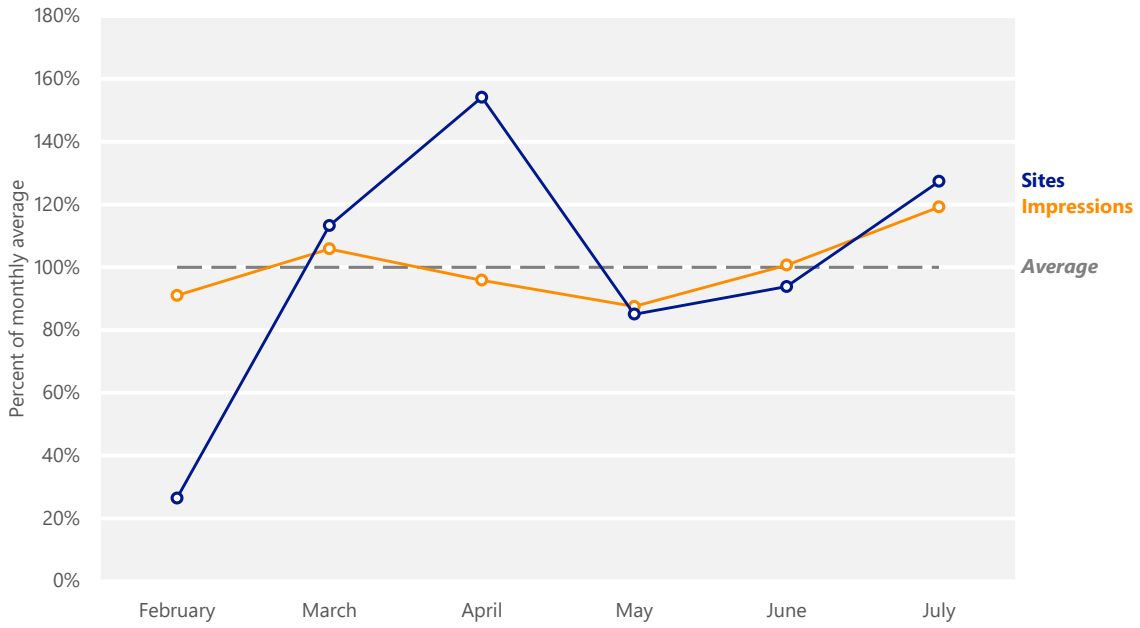


Figure 83 compares the volume of active malware hosting sites in the Microsoft database each month with the volume of malware impressions tracked.

Figure 83. Malware hosting sites and impressions tracked each month, February–July 2015, relative to the monthly average for each

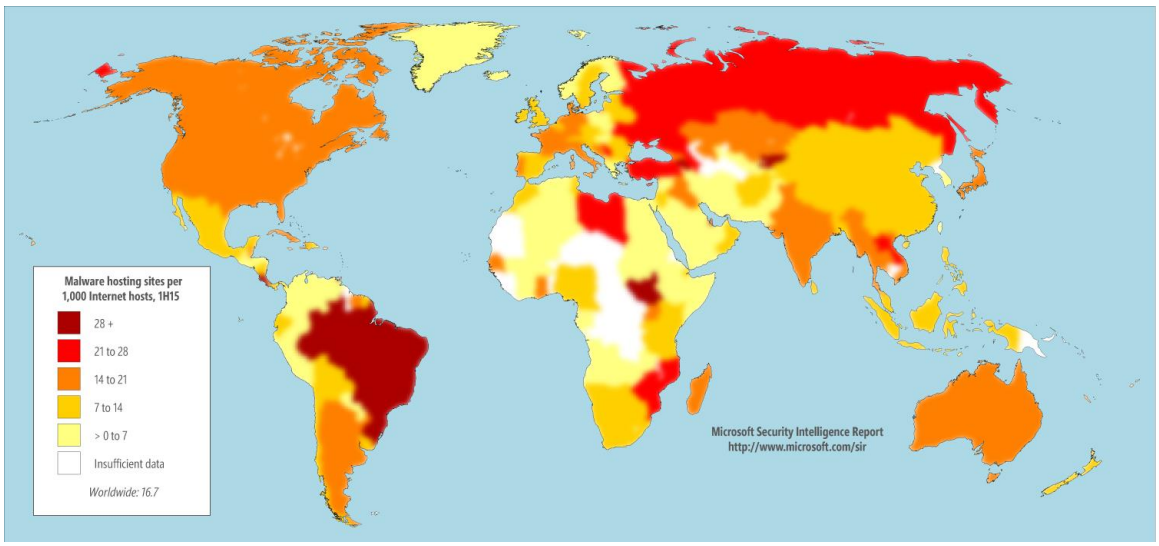


- As with phishing sites and impressions, malware hosting sites and impressions rarely correlate strongly with one another. The number of impressions remained largely stable each month from February through July, while the number of active malware hosting sites tracked by SmartScreen Filter increased sharply from February to April, then retreated to lower levels for the remainder of the period.

Global distribution of malware hosting sites and clients

Figure 84 shows the geographic distribution of malware hosts and computers reporting impressions in 1H15.

Figure 84. Malware distribution sites per 1,000 Internet hosts for locations around the world in 1H15



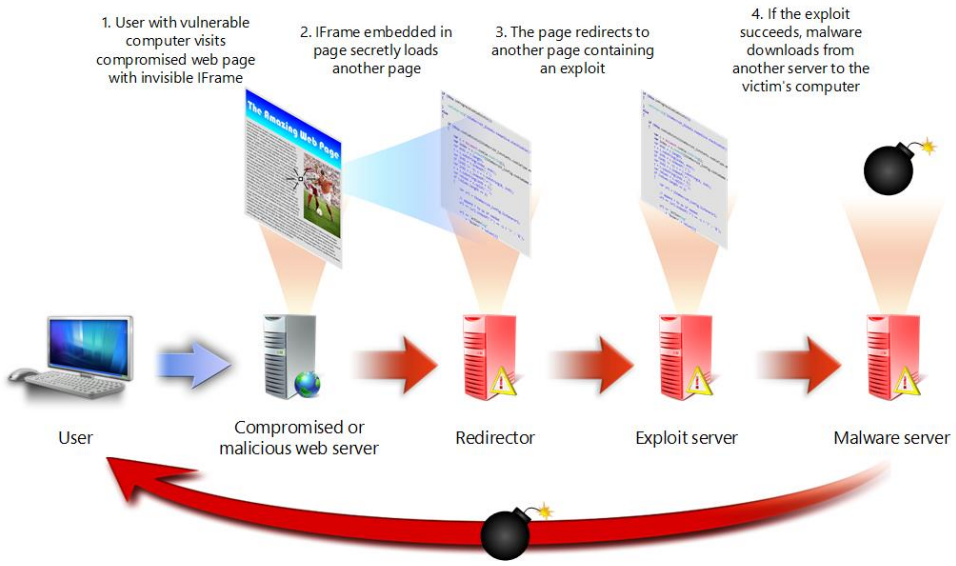
- SmartScreen Filter detected approximately 16.7 malware hosting sites per 1,000 Internet hosts worldwide in 1H15.
- Locations with large concentrations of malware hosting sites included Brazil (41.0 per 1,000 Internet hosts in 1H15), Costa Rica (38.8), and Russia (23.9). Locations with low concentrations of malware hosting sites included Taiwan (2.8), Saudi Arabia (4.3), and Finland (4.4).

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.

Drive-by download pages are usually hosted on legitimate websites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere in the world and concern nearly any subject imaginable, making it difficult for even an experienced user to identify a compromised site from a list of search results.

Figure 85. One example of a drive-by download attack



Search engines such as Bing have taken a number of measures to help protect users from drive-by downloads. As Bing indexes webpages, they are assessed for malicious elements or malicious behavior. Because the owners of compromised sites are usually victims themselves, the sites are not removed from the Bing index. Instead, clicking the link in the list of search results displays a prominent warning, saying that the page may contain malicious software, as shown in Figure 86.

Figure 86. A drive-by download warning from Bing

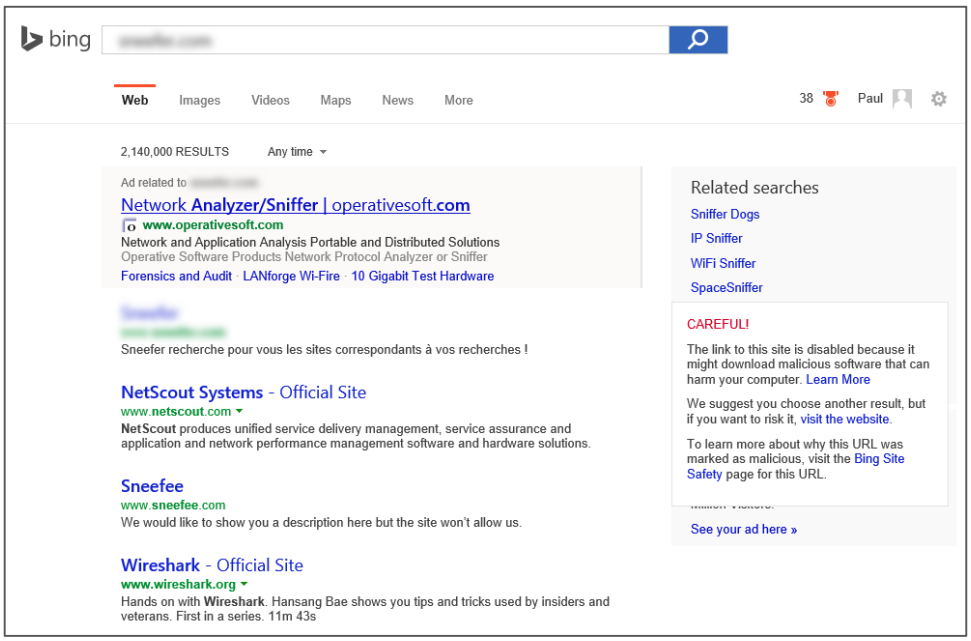
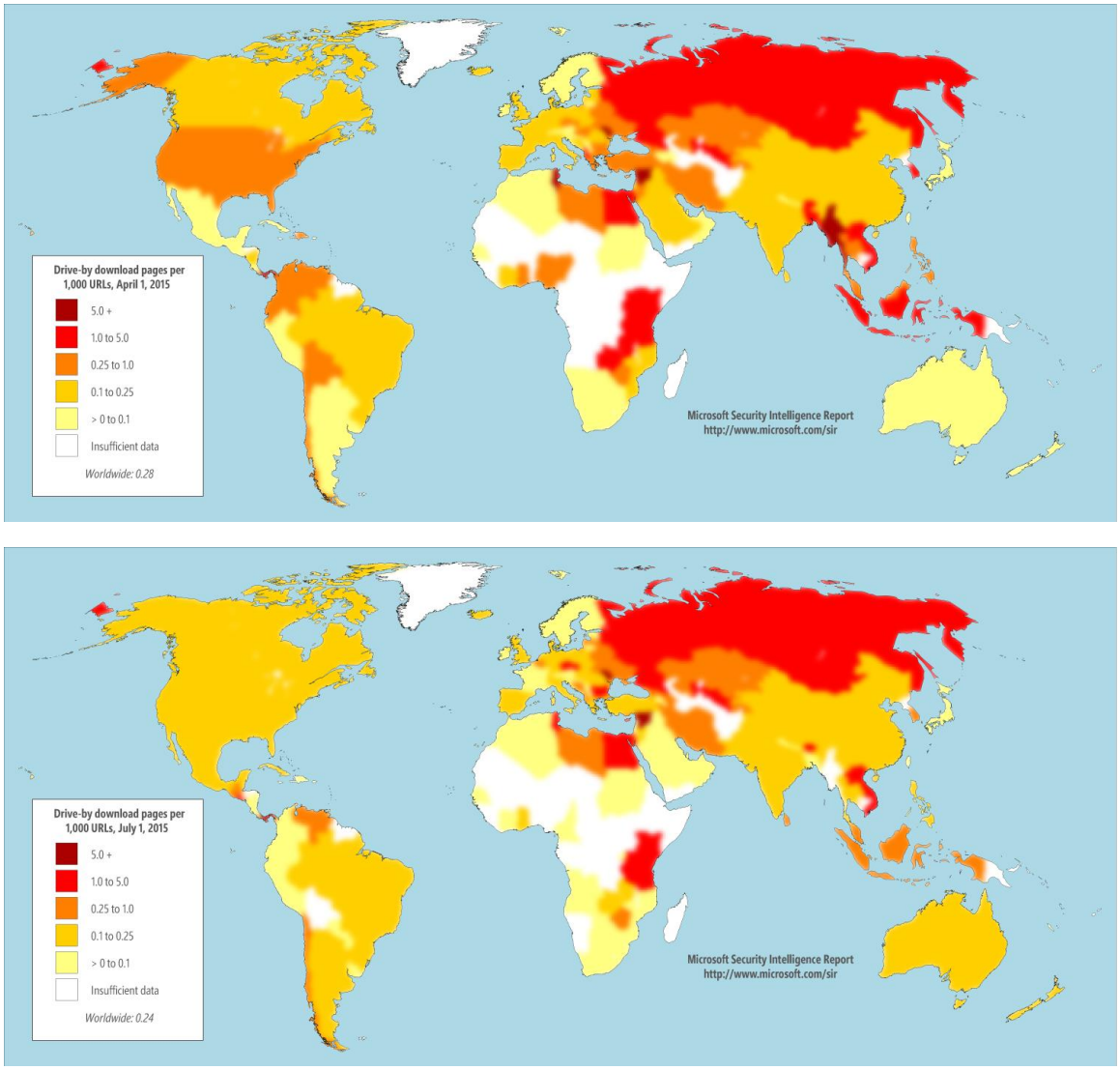


Figure 87 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 1Q15 and 2Q15, respectively.

Figure 87. Drive-by download pages indexed by Bing at the end of 1Q15 (top) and 2Q15 (bottom), per 1,000 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 Panama, with 8.7 drive-by URLs for every 1,000 URLs tracked by Bing at the end of 2Q15; Vietnam, with 3.0; and Russia, with 1.7.

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 "Top security solutions" at www.microsoft.com/security/pc-security/solutions.aspx.

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 more than 600,000 devices for more than 150,000 users across more than 100 countries and regions worldwide. 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.

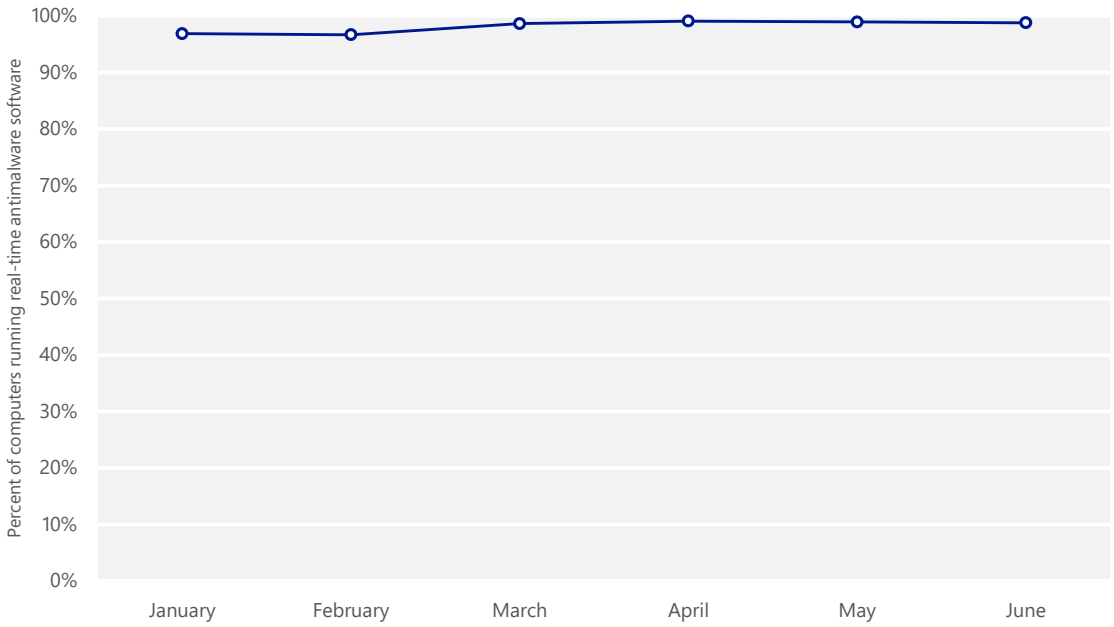
This section of the report compares the potential impact of malware to the levels of antimalware compliance from more than 500,000 workstation computers and devices managed by Microsoft IT between January and June 2015. This data is compiled from multiple sources, including System Center Endpoint Protection (SCEP), Windows Defender, DirectAccess, forensics, 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 provide 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. System Center Endpoint Protection 2012 (SCEP) and Windows Defender are the antimalware solutions that Microsoft IT deploys to its users. To be considered compliant with antimalware policies and standards, user computers must be running the latest version of the SCEP or Defender client, antimalware signatures must be no more than six days old, and real-time protection must be enabled.

Figure 88 shows the level of antimalware noncompliance in the Microsoft user workstation environment for each month in 1H15.

Figure 88. Percentage of computers at Microsoft running real-time antimalware software in 1H15



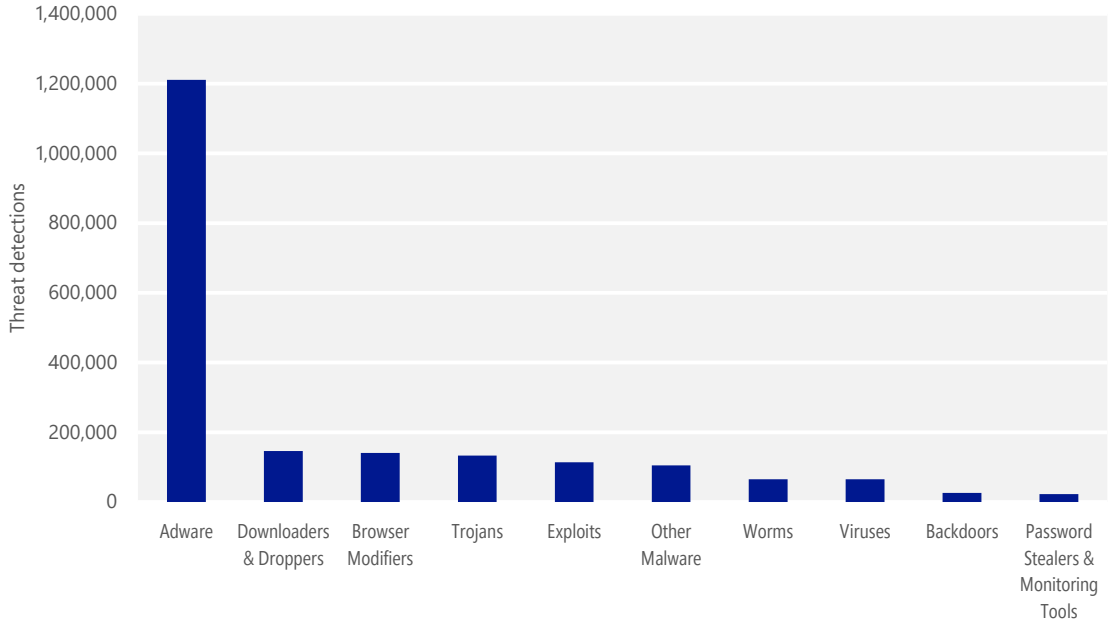
Despite a small drop in compliance at the beginning of the year that was mostly related to internal testing of current and future versions of Windows, the average monthly compliance rate at Microsoft exceeded 98 percent during the first half of the year. In any network of this size, it is almost inevitable 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 98 percent among approximately half a million 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 over time.

Malware detections

Figure 89 shows the categories of malware and unwanted software that were most frequently detected at Microsoft in 1H15.

Figure 89. Top categories of malware and unwanted software detected by System Center Endpoint Protection at Microsoft in 1H15

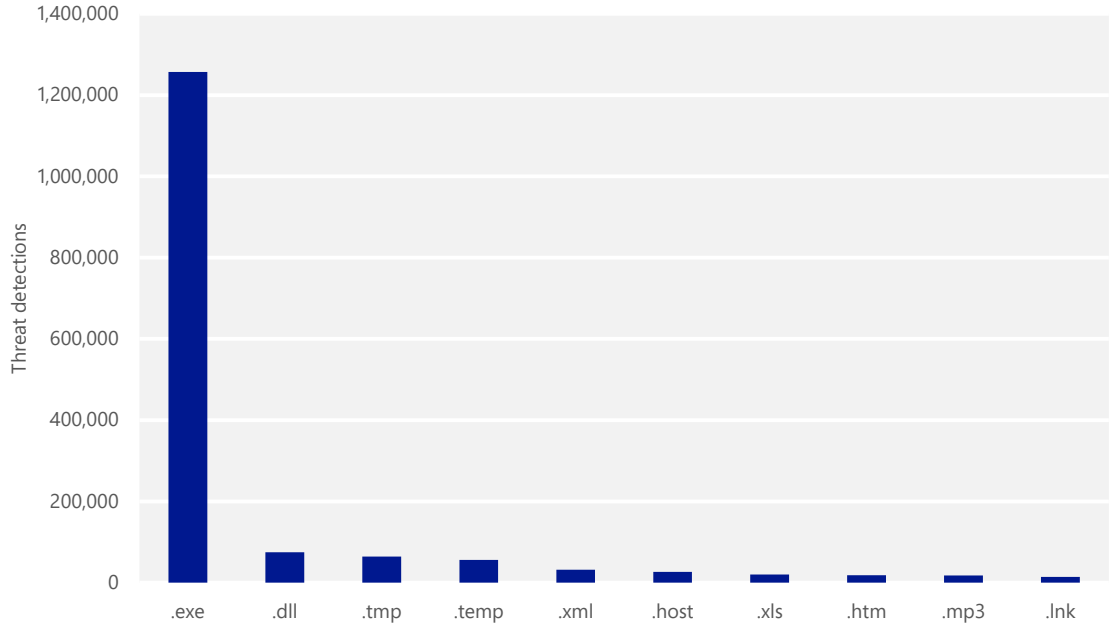


In this section, malware detections are defined as files and processes flagged by SCEP, regardless of the success or failure of automated containment or remediation. Malware detections are a measure of attempted malware activity, and do not necessarily indicate that a computer has been successfully infected. (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 in this section, in which individual detections are counted. For example, if a computer encountered one trojan family in February and another one in June, it would only be counted once for the purposes of figures such as Figure 49 on page 70. In the preceding Figure 89, it would be counted twice, once for each detection.)

Adware was the most prevalent category, with nearly one and a half times as many detections as all other categories combined. The outsized number of internal adware detections is caused by a pilot project that MSIT has undertaken with the Microsoft Security Response Center (MSRC) to improve detection of adware and other unwanted software. As this work is evaluated and found to produce valid and satisfactory results, any improved detection methods will be incorporated into Microsoft security products for the benefit of customers and end users.

Figure 90 shows the top 10 file types among threat detections at Microsoft in 1H15.

Figure 90. Top ten file types used by threats detected at Microsoft in 1H15



Executable program files with the .exe extension were the most commonly detected type of malicious file at Microsoft by a large margin. Many of these detections were related to the joint effort between MSIT and the MSRC to improve detection of unwanted software, as noted earlier. Malicious .dll files were the next most common type of threats, followed by the .tmp and .temp extensions, typically used for temporary files.

Transmission vectors

Examining the processes targeted by malware can help illustrate the methods that attackers use to propagate it. Figure 91 lists the top five transmission vectors used by the malware encountered at Microsoft in 1H15.

Figure 91. The top five transmission vectors used by malware encountered at Microsoft in 1H15

Rank	Description
1	Web browsing
2	File transfers in the operating system
3	Scheduled tasks in the operating system
4	Cloud backup/storage
5	File transfer applications

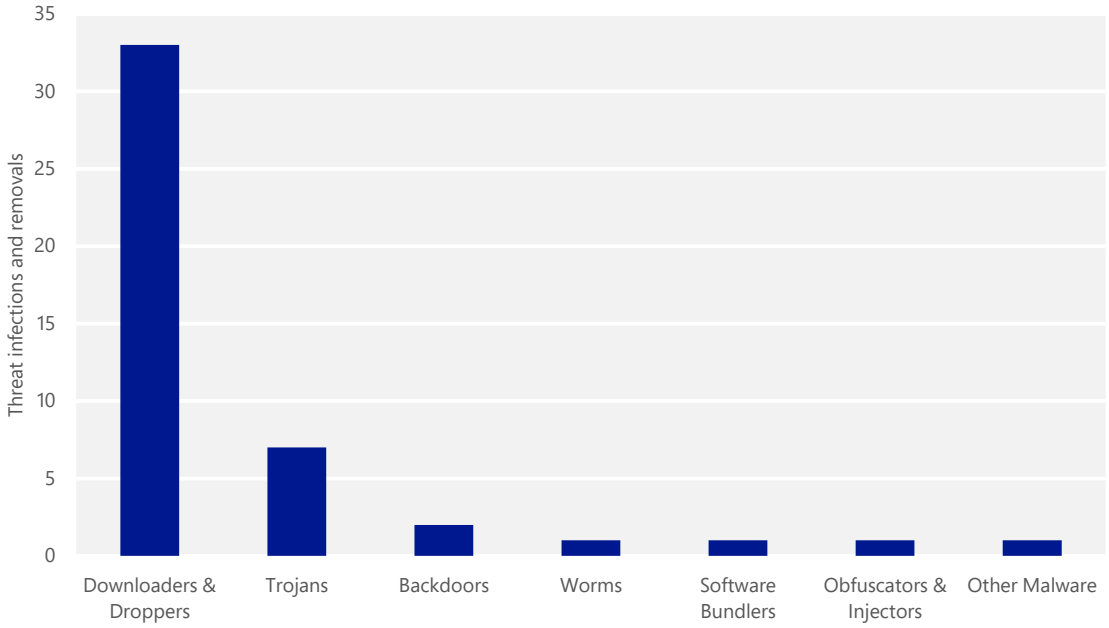
The transmission vector most commonly used by infection attempts detected on Microsoft computers in 1H15 involved web browsing, followed by file transfers made through Windows Explorer and scheduled operating system tasks. Cloud backup and storage services were fourth, followed by file transfer applications, including peer-to-peer (P2P) applications.

Malware 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 Defender or SCEP do disinfect a computer, it is usually because the software's 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 92 shows the most commonly detected categories of malware and unwanted software that SCEP and Defender removed from computers at Microsoft between January and June of 2015.

Figure 92. Infections and removals at Microsoft in 1H15, by category



As this chart shows, detection and infection statistics were significantly different in 1H15. Adware, which accounted for more than 1.2 million detections at Microsoft in 1H15, was not discovered on a single computer internally during the period. Most of the other categories also show clear differences between Figure 89 and Figure 92, although the ordering in the latter chart is significantly influenced by the low volumes involved.

Figure 93 shows the top 10 file types used by malware to infect computers at Microsoft in 1H15.

Figure 93. Infections and removals at Microsoft in 1H15, by file type

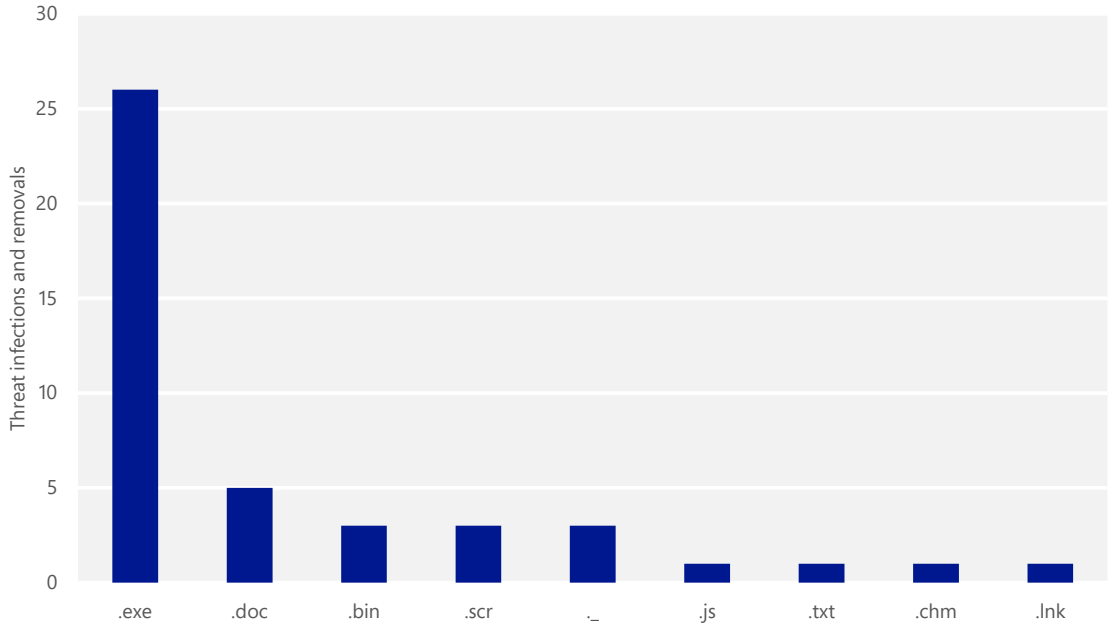


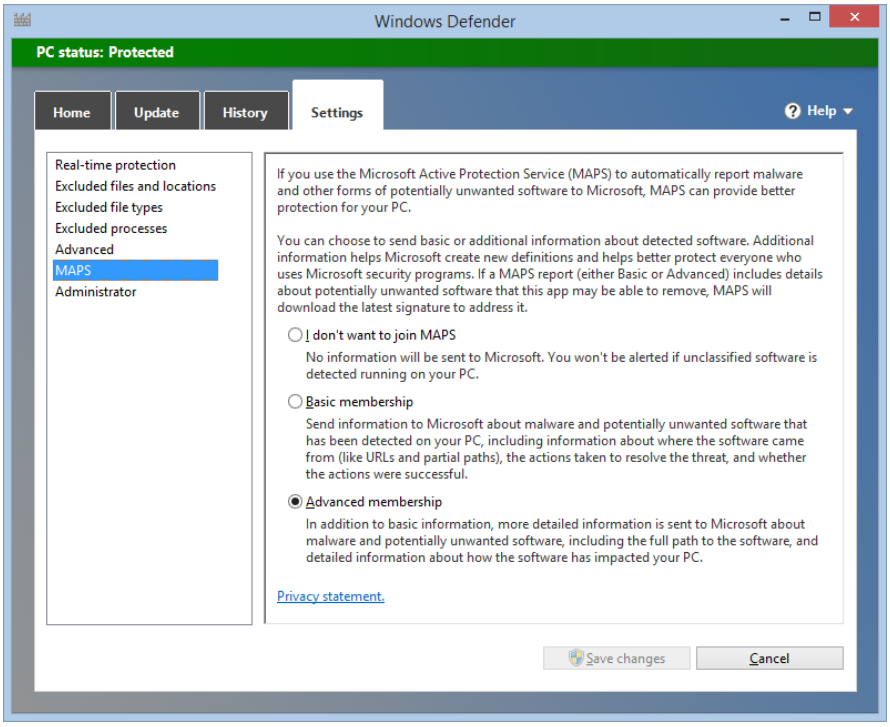
Figure 93 is important because it provides information about threats that Defender and SCEP did not detect when they were first encountered—and therefore provides a clue about the areas in which malware authors have been focusing their efforts in recent months. More than half of the malicious files removed from computers at Microsoft by Defender and SCEP in 1H15 had the extension .exe, used by executable program files, with seven extensions accounting for the remaining files. The .doc extension used for Microsoft Word binary files was next, followed by .bin, .scr, and "._", an extension consisting of a single underscore. Four other file types each accounted for a single removal.

What IT departments can do to protect their users

- Evaluate commercially available management tools, 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 similar to Microsoft Update, ensure that it is enabled by default. See "Turn automatic updating on or off" at 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" at windows.microsoft.com for more information.
- Use Group Policy to enforce configurations for Windows Update, Windows Firewall, and SmartScreen Filter. See Knowledge Base article KB328010 at support.microsoft.com, and "Windows Firewall with Advanced Security Deployment Guide" and "Manage Privacy: SmartScreen Filter and Resulting Internet Communication" at technet.microsoft.com for instructions.
- Set the default configuration for antimalware to enable real-time protection across all drives, including removable devices.
- Enable Microsoft Active Protection Service (MAPS) advanced membership in Windows Defender and Microsoft Security Essentials in your organization to protect your enterprise software security infrastructure in the cloud.

Figure 94. Enabling MAPS advanced membership in Windows Defender



- Identify business dependencies on Java and develop a plan to minimize its use where it is not needed.
- Use AppLocker to block the installation and use of unwanted software such as Java or peer-to-peer (P2P) applications. See "AppLocker: Frequently Asked Questions" at technet.microsoft.com for more information.

- Implement the Enhanced Mitigation Experience Toolkit (EMET), if possible, to minimize exploitation of vulnerabilities in all software in your environment. See technet.microsoft.com/security/jj653751 for more information.
- Implement strong password policies, and require employees to change their passwords periodically.
- Strengthen authentication by using smart cards. See "Smart Cards" at technet.microsoft.com for more information.

Use Network Access Protection (NAP) and DirectAccess (DA) to enforce compliance policies for firewall, antimalware, and patch management on remote systems that connect to a corporate network. See "Network Access Protection" at msdn.microsoft.com and "Windows 7 DirectAccess Explained" at technet.microsoft.com for more information.

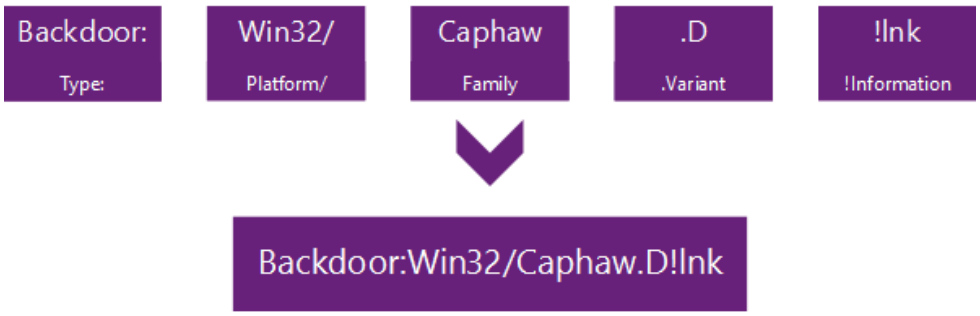
Appendixes

Appendix A: Threat naming conventions

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

This scheme uses the following format:

Figure 95. 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 a computer. Worms, trojans, and viruses 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 the identified threat. In the preceding example, the !lnk indicates that the threat is a shortcut file used by the Backdoor:Win32/Caphaw.D 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 whose users have opted in to provide usage data. 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 is Microsoft's hosted email service for business. Exchange Online antimalware and antispam services scan billions of 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 specific 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 1H15. The MSRT is not a replacement for an up-to-date real-time antivirus solution.
- 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, easy-to-download real-time protection product that provides basic, effective antivirus and antispyware protection for Windows Vista and Windows 7.
- Microsoft System Center Endpoint Protection (formerly Forefront Client Security and Forefront Endpoint Protection) is a unified product that provides protection from malware and 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.

- Office 365 is the Microsoft Office subscription service for business and home users. Select business plans include access to Exchange Online with Advanced Threat Protection.
- SmartScreen Filter, a feature in Internet Explorer and Microsoft Edge, 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, the browser displays a warning and blocks navigation to the page.
- Windows Defender in Windows 8 and Windows 8.1 provides real-time scanning and removal of malware and 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 96. US privacy statements for the Microsoft products and services used in this report

Product or service	Privacy statement URL
Bing	www.microsoft.com/en-us/privacystatement/default.aspx
Exchange Online	www.microsoft.com/online/legal/v2/?docid=22&langid=en-us
Internet Explorer 11	windows.microsoft.com/en-us/internet-explorer/ie11-preview-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
Office 365	www.microsoft.com/online/legal/v2/?docid=22&langid=en-us
System Center Endpoint Protection	https://www.microsoft.com/privacystatement/en-us/SystemCenter2012R2/Default.aspx#tilepspSystemCenter2012R2EndpointProtectionModule
Windows Defender in Windows 8.1	windows.microsoft.com/en-us/windows-8/windows-8-1-privacy-statement#T1=supplement&section_43
Windows Defender Offline	windows.microsoft.com/en-us/windows/windows-defender-offline-privacy

Appendix C: Worldwide encounter and infection rates

"Malware and unwanted software" on page 58 explains how threat patterns differ significantly in different parts of the world. Figure 97 shows the infection and encounter rates for 1Q15 and 2Q15 for locations around the world.[22] See page 58 for information about how infection and encounter rates are calculated.

Figure 97. Encounter and infection rates for locations around the world, 1Q15–2Q15, by quarter (100,000 computers reporting minimum)

Country/region	Encounter rate 1Q15	Encounter rate 2Q15	CCM 1Q15	CCM 2Q15
Worldwide	*17.3%*	*14.8%*	*5.4*	*8.4*
Albania	37.6%	31.1%	35.2	36.8
Algeria	45.5%	39.7%	54.0	57.2
Angola	—	—	35.5	40.9
Argentina	23.7%	21.4%	8.0	15.7
Armenia	35.3%	26.6%	11.6	13.5
Australia	11.9%	11.2%	2.2	5.0
Austria	12.8%	10.7%	2.1	4.1
Azerbaijan	31.9%	24.4%	29.0	34.1
The Bahamas	—	—	9.0	17.3
Bahrain	0.0%	21.8%	18.8	29.0
Bangladesh	43.2%	39.7%	29.8	32.8
Barbados	—	—	4.1	12.0
Belarus	29.9%	22.4%	7.3	8.8
Belgium	16.0%	13.5%	2.4	6.0
Bolivia	26.3%	24.1%	16.7	24.6

[22] Encounter rate and CCM are shown for locations with at least 100,000 computers running Microsoft real-time security products and the Malicious Software Removal Tool, respectively, during a quarter. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter and infection rates.

Country/region	Encounter rate 1Q15	Encounter rate 2Q15	CCM 1Q15	CCM 2Q15
Bosnia and Herzegovina	33.2%	26.7%	16.2	24.4
Brazil	20.5%	20.2%	8.0	16.2
Bulgaria	31.4%	24.1%	9.1	12.7
Cambodia	35.7%	34.4%	18.6	22.5
Cameroon	—	—	36.1	33.1
Canada	14.0%	12.5%	2.0	4.5
Chile	23.1%	20.9%	7.6	20.3
China	13.1%	13.7%	3.8	4.4
Colombia	24.2%	20.9%	9.9	25.1
Costa Rica	18.3%	14.5%	6.8	11.2
Côte d'Ivoire	—	—	32.5	30.8
Croatia	28.8%	22.3%	5.7	12.0
Cyprus	25.3%	18.8%	7.4	12.8
Czech Republic	18.1%	14.7%	4.6	6.7
Denmark	10.6%	10.2%	2.0	4.2
Dominican Republic	31.4%	27.2%	24.2	33.5
Ecuador	28.4%	23.9%	11.1	19.9
Egypt	39.8%	35.5%	49.8	55.8
El Salvador	24.0%	20.1%	7.4	17.3
Estonia	17.7%	14.3%	2.3	6.2
Finland	6.1%	6.0%	1.3	2.5
France	15.8%	13.2%	2.7	8.9
Georgia	37.2%	29.7%	25.4	27.2
Germany	11.1%	8.9%	2.1	4.6
Ghana	39.0%	36.2%	22.1	25.4
Greece	23.8%	17.1%	7.0	10.3
Guadeloupe	—	—	4.9	13.5
Guatemala	20.9%	18.2%	8.7	17.1
Honduras	25.8%	23.4%	11.6	25.8
Hong Kong SAR	11.8%	10.5%	3.5	7.0
Hungary	22.3%	17.6%	4.9	8.1

Country/region	Encounter rate 1Q15	Encounter rate 2Q15	CCM 1Q15	CCM 2Q15
Iceland	14.8%	11.0%	2.8	5.6
India	34.9%	31.3%	24.2	30.4
Indonesia	42.8%	40.6%	30.6	38.2
Iraq	41.4%	34.4%	76.6	80.2
Ireland	13.6%	12.3%	2.2	5.4
Israel	20.4%	16.1%	9.5	13.7
Italy	19.5%	15.3%	3.3	8.8
Jamaica	29.1%	24.3%	10.0	18.7
Japan	5.5%	5.4%	0.9	2.8
Jordan	39.5%	33.3%	36.6	45.3
Kazakhstan	31.4%	24.6%	21.6	21.6
Kenya	31.3%	28.9%	18.9	22.9
Korea	12.8%	10.3%	7.2	13.8
Kuwait	27.6%	22.7%	17.6	27.1
Latvia	23.1%	16.2%	3.2	6.1
Lebanon	33.5%	28.4%	31.7	42.5
Libya	—	—	61.0	69.8
Lithuania	24.7%	18.7%	5.0	8.9
Luxembourg	—	—	2.1	5.4
Macao SAR	—	—	5.1	8.1
Macedonia, FYRO	33.6%	28.5%	16.8	21.9
Malaysia	26.4%	23.9%	16.3	21.8
Malta	—	—	3.3	9.5
Martinique	—	—	3.3	11.0
Mauritius	—	—	11.4	20.8
Mexico	22.6%	21.2%	11.4	18.6
Moldova	29.3%	21.5%	10.3	12.4
Mongolia	—	—	66.8	77.6
Morocco	36.9%	29.2%	58.2	66.6
Mozambique	—	—	21.1	28.9
Namibia	—	—	16.3	23.1

Country/region	Encounter rate 1Q15	Encounter rate 2Q15	CCM 1Q15	CCM 2Q15
Nepal	45.0%	39.0%	39.1	43.7
Netherlands	12.9%	11.6%	1.8	4.3
New Zealand	12.8%	12.0%	2.6	4.7
Nicaragua	—	—	5.7	15.1
Nigeria	31.4%	28.0%	25.9	28.7
Norway	9.8%	10.2%	2.0	3.9
Oman	35.3%	30.6%	25.8	37.6
Pakistan	51.2%	45.1%	55.9	58.6
Palestinian Authority	44.9%	40.5%	59.5	68.7
Panama	22.6%	20.0%	8.1	15.0
Paraguay	—	—	10.4	20.3
Peru	25.3%	23.3%	13.5	23.4
Philippines	32.0%	29.1%	30.9	37.6
Poland	16.4%	13.0%	7.7	11.5
Portugal	22.3%	18.9%	3.3	9.4
Puerto Rico	19.5%	16.8%	6.8	13.4
Qatar	30.2%	24.3%	14.3	24.6
Réunion	18.8%	13.2%	3.3	10.9
Romania	29.4%	22.5%	16.5	20.9
Russia	22.8%	17.7%	4.7	6.6
Saudi Arabia	31.3%	26.4%	24.1	31.3
Senegal	42.1%	37.0%	20.6	24.4
Serbia	31.1%	25.6%	12.1	18.8
Singapore	14.8%	14.0%	4.5	8.9
Slovakia	18.9%	14.5%	6.7	9.0
Slovenia	20.2%	15.4%	3.4	6.9
South Africa	22.8%	20.4%	10.7	14.4
Spain	19.6%	16.4%	4.3	12.4
Sri Lanka	31.9%	26.6%	16.4	22.6
Sweden	9.9%	8.9%	2.0	4.1
Switzerland	12.4%	11.0%	1.5	3.8

Country/region	Encounter rate 1Q15	Encounter rate 2Q15	CCM 1Q15	CCM 2Q15
Taiwan	14.3%	13.6%	5.4	8.6
Tanzania	—	—	22.7	26.8
Thailand	26.8%	22.9%	22.3	31.0
Trinidad and Tobago	26.3%	21.9%	9.6	16.8
Tunisia	43.1%	36.4%	36.2	50.1
Turkey	32.0%	28.1%	22.5	26.3
Ukraine	31.1%	23.8%	7.3	8.9
United Arab Emirates	31.1%	25.4%	16.7	27.0
United Kingdom	12.7%	11.7%	2.3	5.8
United States	11.0%	9.8%	3.2	5.0
Uruguay	23.6%	19.6%	5.0	15.1
Venezuela	32.4%	29.9%	17.5	26.5
Vietnam	36.7%	33.2%	30.4	35.8
Zimbabwe	—	—	16.2	19.8
Worldwide	*17.3%*	*14.8%*	*5.4*	*8.4*

Glossary

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

account credentials
Information presented to a service provider to verify that the holder of the credentials is authorized to access an account. Account credentials typically take the form of user names paired with passwords, but other forms of identification are possible.

ActiveX control
A software component of Microsoft Windows that can be used to create and distribute small applications through Internet Explorer. ActiveX controls can be developed and used by software to perform functions that would otherwise not be available using typical Internet Explorer capabilities. Because ActiveX controls can be used to perform a wide variety of functions, including downloading and running programs, vulnerabilities discovered in them may be exploited by malware. In addition, cybercriminals may also develop their own ActiveX controls, which can do damage to a computer if a user visits a webpage that contains the malicious ActiveX control.

Address Space Layout Randomization (ASLR)
A security feature in recent versions of Windows that randomizes the memory locations used by system files and other programs, which makes it harder for an attacker to exploit the system by targeting specific memory locations.

air gap
The complete separation of a computer or network from others, with no wired or wireless data connections. Data can only be exchanged across an air gap by physically transporting removable media from one computer to another.

ASEP
See *autostart extensibility point*.

ASLR
See *Address Space Layout Randomization (ASLR)*.

autostart extensibility point (ASEP)
A place in the registry or file system that Windows checks for programs and processes that should be automatically launched after boot. Threats often add

themselves to one or more ASEPs to ensure that they run automatically whenever the computer is rebooted.

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*.

boleto
Short for *boleto bancário*. A popular payment method in Brazil, similar to an invoice. Some threats steal money by altering boletos in web pages or email messages.

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*.

browser modifier
A program that changes browser settings, such as the home page, without adequate consent. This also includes browser hijackers.

buffer overflow
An error in an application in which the data written into a buffer exceeds the current capacity of that buffer, thus overwriting adjacent memory. Because memory is overwritten, unreliable program behavior may result and, in certain cases, allow arbitrary code to run.

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 unwanted software from an infected computer. A single cleaning can involve multiple disinfections.

command and control
See *botnet*.

credentials
See *account credentials*.

definition
See *detection signature*.

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. Also see *definition*.

detonation chamber
A sandbox environment in which potentially dangerous files can be automatically launched and monitored for possible malicious activity.

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*.

double free vulnerability
A vulnerability triggered when code attempts to free the same memory address twice. This can cause memory corruption, which an attacker may be able to take advantage of if it is not handled properly.

downloader
See *downloader/dropper*.

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.

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.

exploit kit
A collection of exploits bundled together and sold as commercial software. A typical kit contains a collection of web pages that contain exploits for vulnerabilities in popular web browsers and add-ons, along with tools for managing and updating the kit

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.

hash
Text that has been encoded using a one-way cryptographic function that prevents it from being decrypted. Also refers to a checksum produced by a hash function to identify or authenticate data.

heuristics
A tool or technique that can help identify common patterns. This can be useful for making generic detections for a malware family.

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 content, such as a script that downloads and installs spyware, into non-malicious HTML pages that are hosted by trusted websites.

in the wild
Said of 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 on a computer, or the act of delivering or installing malware on a computer. Also see *encounter*.

infection rate
See *CCM*.

jailbreaking
See *rooting*.

login credentials
See *account credentials*.

Malicious Software Removal Tool
A free tool that Microsoft designed to help identify and remove specific prevalent malware families from customer computers. An updated version of the tool is released each month through Windows Update and other updating services. The MSRT is not a replacement for an up-to-date real-time antivirus solution.

malware
Short for *malicious software*. The general name for programs that perform unwanted actions on a computer, such as stealing personal information. Some malware can steal banking details, lock a computer until the user pays a ransom, or use the computer to send spam. Viruses, worms and trojans are all types of malware.

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 11. Also see *phishing impression*.

man-in-the-browser attack
A type of web-based threat where a malicious program makes changes to a website without the website owner knowing it is happening.

monitoring tool
Software that monitors activity, usually by capturing keystrokes or screen images. It may also include network sniffing software. Also see *password stealer (PWS)*.

MSRT
See *Malicious Software Removal Tool*.

multifactor authentication
Requiring a user to provide two or more forms of authentication, such as a username/password and a physical token, to access an account.

open source intelligence (OSINT)
Intelligence information collected from unclassified, publicly available sources.

OSINT
See *open source intelligence*.

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

pass-the-hash (PtH)
An attack technique wherein the attacker gains access to a resource by presenting a hashed credential directly for authentication, instead of presenting the password normally and allowing the authentication system to create the hash.

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. Also see *monitoring tool*.

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 11, and being blocked by the Phishing Filter or SmartScreen Filter. Also see *malware impression*.

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 to a remote attacker (the "ransom"). Computers that have ransomware installed usually display a screen containing information on how to pay the "ransom." A user cannot usually access anything on the computer beyond the screen.

return-oriented programming (ROP)
An exploit technique that involves gaining control of a program's control flow and calling a chain of instructions that already exist in memory, each of which ends in a return command.

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*.

ROP
See *return-oriented programming (ROP)*.

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.

signature
See *detection signature*.

sinkhole
A server or set of servers designed to absorb and analyze malware traffic.

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.

software bundler
A program that installs unwanted software on a computer at the same time as the software the user is trying to install, without adequate consent.

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 containing a link to the malware. Malware may also harvest email addresses for spamming from compromised machines or may use compromised machines to send spam.

spear phishing
Phishing that targets a specific person, organization, or group, containing additional information associated with that person, organization, or group to lure the target further into a false sense of security to divulge more sensitive information.

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.

targeted attack
A malware attack against a specific group of companies or individuals. This type of attack usually aims to get access to the computer or network, before trying to steal information or disrupt the infected machines.

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 takes malicious action on the computer.

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

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 unwanted software families. See the encyclopedia for more in-depth information and guidance for the families listed here and throughout the report.

W97M/Adnel. A family of macro malware that can download other threats to the computer, including TrojanDownloader:Win32/Drixed.

HTML/Adodb. A generic detection for script trojans that exploit a vulnerability in Microsoft Data Access Components (MDAC) that allows remote code execution. Microsoft released Security Bulletin MS06-014 in April 2006 to address the vulnerability.

Win32/AlterbookSP. A browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.

Win32/Anogre. A detection for the Sweet Orange exploit kit, which exploits vulnerabilities in some versions of Windows, Adobe Flash Player, and Java to install malware.

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.

JS/Axpergle. A detection for the Angler exploit kit, which exploits vulnerabilities in some versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

Win32/Bancos. A data-stealing trojan that captures online banking credentials and relays them to the attacker. Most variants target customers of Brazilian banks.

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/BeeVry. A trojan that modifies a number of settings to prevent the computer from accessing security-related websites, and lower the computer's security.

JS/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.

MSIL/Bladabindi. A family of backdoors created by a malicious hacker tool called NJ Rat. They can steal sensitive information, download other malware, and allow backdoor access to an infected computer.

JS/Bondat. A family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.

Win32/BrobanDel. A family of trojans that can modify boletos bancários, a common payment method in Brazil. They can be installed on the computer when a user opens a malicious spam email attachment.

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.

Win32/CompromisedCert. A detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on 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 downloads arbitrary files.

Win32/CouponRuc. A browser modifier that changes browser settings and may also modify some computer and Internet settings.

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

Win32/Crowti. A ransomware family that encrypts files on the computer and demands that the user pay a fee to decrypt them, using Bitcoins.

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

Win32/Dyzap. A threat that steals login credentials for a long list of banking websites using man-in-the-browser (MITB) attacks. It is usually installed on the infected computer by TrojanDownloader:Win32/Upatre.

Win32/EoRezo. Adware that displays targeted advertising to affected users while browsing the Internet, based on downloaded pre-configured information.

Win32/Foosace. A threat that creates files on the compromised computer and contacts a remote host.

Win32/Frethog. A large family of password-stealing trojans that targets confidential data, such as account information, from massively multiplayer online games.

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.

AndroidOS/GingerMaster. A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.

Win32/IeEnablerCby. A browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

Win32/InstalleRex. A software bundler that installs unwanted software, including Win32/CouponRuc and Win32/SaverExtension. It alters its own "Installed On" date in Programs and Features to make it more difficult for a user to locate it and remove it.

DOS/JackTheRipper. A virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.

VBS/Jenxcus. A worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.

ALisp/Kenilfe. A worm written in AutoCAD Lisp that only runs if AutoCAD is installed on the computer or network. It renames and deletes certain AutoCAD files, and may download and execute arbitrary files from a remote host.

Win32/Kilim. A trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.

Win32/KipodToolsCby. A browser modifier that installs additional browser add-ons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.

JS/Krypterade. Ransomware that fraudulently claims the computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

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

Win32/Macoute. A worm that can spread itself to removable USB drives, and may communicate with a remote host.

MSIL/Mofin. A worm that can steal files from your PC and send them to a malicious hacker. It spreads via infected removable drives, such as USB flash drives.

Win32/Nuqel. A worm that spreads via mapped drives and certain instant messaging applications. It may modify system settings, connect to certain websites, download arbitrary files, or take other malicious actions.

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/Ogimant. A threat that claims to help download items from the Internet, but actually downloads and runs files that are specified by a remote attacker.

HTML/Pangimop. A detection for the Magnitude exploit kit, also known as Popads. It attempts to exploit vulnerabilities in programs such as Java and Adobe Flash Player to install other malware.

Win32/Pdfjsc. A family of specially crafted PDF files that exploit Adobe Acrobat and Adobe Reader vulnerabilities. Such files contain malicious JavaScript that executes when the file is opened.

Win32/Peaac. A generic detection for various threats that display trojan characteristics.

Win32/Peals. A generic detection for various threats that display trojan characteristics.

JS/Proslikefan. A worm that spreads through removable drives, network shares, and P2P programs. It can lower the computer's security settings and disable antivirus products.

Win32/Radonskra. A family of threats that perform a variety of malicious acts, including stealing information about the computer, showing extra advertisements as the user browses the web, performing click fraud, and downloading other programs without consent.

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 FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.

Win32/Reveton. A ransomware family that targets users from certain countries or regions. 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/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.

Win32/SaverExtension. A browser add-on that shows ads in the browser without revealing their source, and prevents itself from being removed normally.

Win32/Sdbby. A threat that exploits a bypass to gain administrative privileges on a machine without going through a User Access Control prompt.

Win32/Simda. A threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.

PHP/SimpleShell. A backdoor that can give an attacker the ability to run shell commands on a compromised server.

Win32/Skeeyah. A generic detection for various threats that display trojan characteristics.

Win32/Slugin. A file infector that infects .exe and .dll files. It may also perform backdoor actions.

Win32/Stuxnet. A multi-component family that spreads via removable volumes by exploiting the vulnerability addressed by Microsoft Security Bulletin MS10-046.

Win32/Tugspay. A downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.

Win32/Upatre. A downloader that installs malware and unwanted software on the affected computer without the user's consent. It is frequently distributed as an attachment to spam email messages.

Win32/Vercuser. A worm that typically spreads via drive-by download. It also receives commands from a remote server, and has been observed dropping other malware on the infected computer.

Win32/Wordinvop. A detection for a specially-crafted Microsoft Word file that attempts to exploit the vulnerability CVE-2006-6456, addressed by Microsoft Security Bulletin MS07-014.

Win32/Wordjmp. An exploit that targets a vulnerability in Word 2002 and 2003 that could allow an attacker to remotely execute arbitrary code. Microsoft released Security Bulletin MS06-027 in June 2006 to address the vulnerability.

Index

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