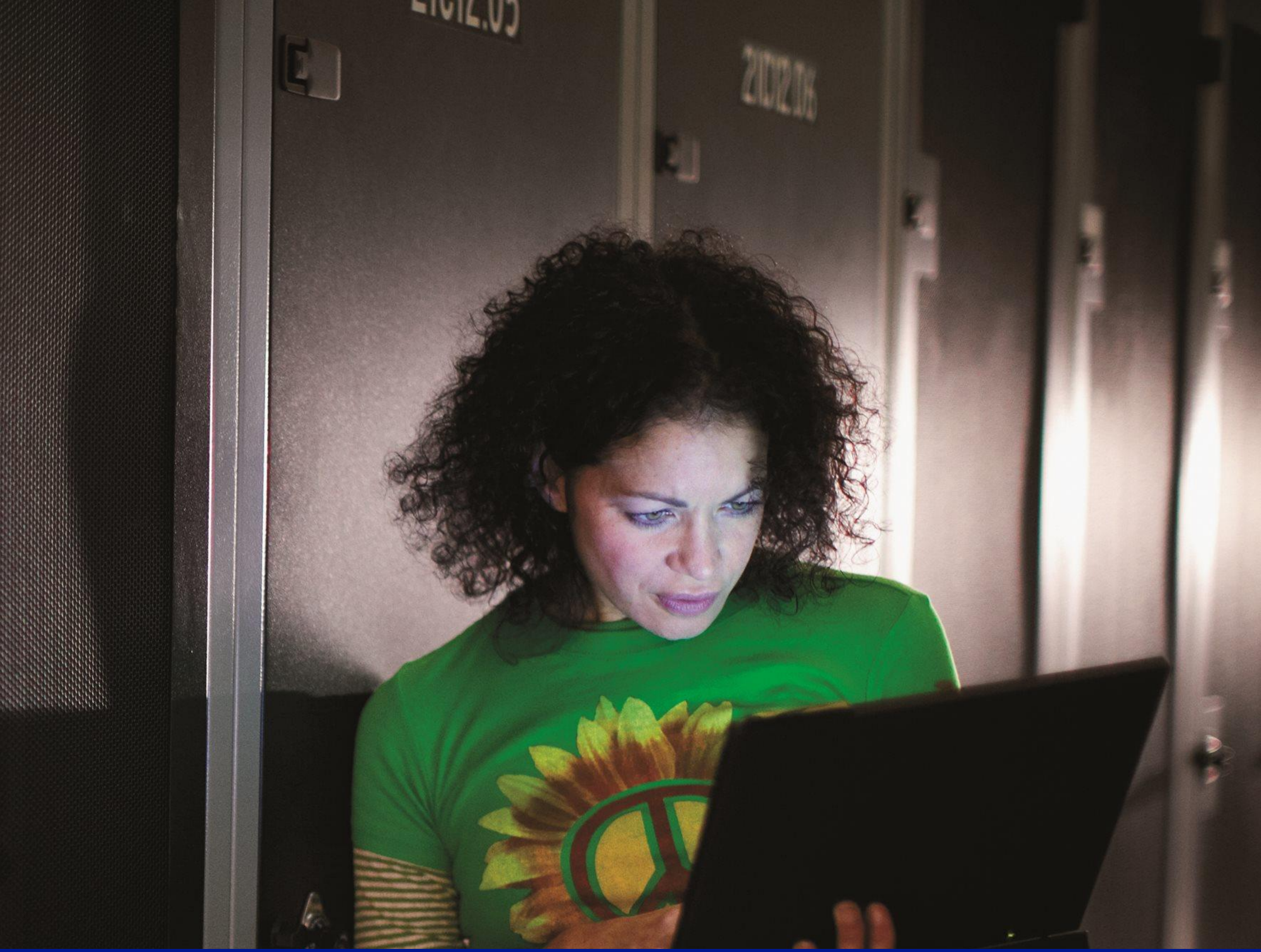


Microsoft Security Intelligence Report

Volume 22 | January through March, 2017

Microsoft

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Authors

Eric Avena
Windows Defender Research Team

Roger Capriotti
Microsoft Edge Product Marketing team

Zheng Dong
Windows Defender ATP Research

Eric Douglas
Windows Defender Research Team

Matt Duncan
Windows Active Defense

Matthew Duncan
Windows Active Defense Data Engineering and Analytics

Sarah Fender
Azure Security

Meths Ferrer
Windows Active Defense

Zarestel Ferrer
Security Research

Elia Florio
Windows Active Defense

Amir Fouda
Windows Defender Research Team

Tanmay Ganacharya
Windows Defender Research Team

Ram Gowrishankar
Windows Defender Research Team

Hil Gradascevic
Windows Defender Research Team

Volv Grebennikov
Bing

Vidya Gururaja Rao
Windows Active Defense Data Engineering and Analytics

Chris Hallum
Windows Active Defense Product Marketing team

Paul Henry
Wadeware LLC

Susan Higgs
Windows Defender ATP Research

Michael Johnson
Windows Defender Research Team

Kasia Kaplinska
Cloud and Enterprise Marketing

Seema Kathuria
Enterprise Cybersecurity Group

Dana Kaufman
Identity Security and Protection Team

Tim Kerk
Windows Defender Research Team

Nasos Kladakis
Enterprise Mobility + Security Product Marketing team

Daniel Kondratyuk
Identity Security and Protection Team

Andrea Lelli
Windows Defender Research Team

Carmen Liang
Windows Defender Research Team

Ryan McGee
Cloud and Enterprise Marketing

Matt Miller
Windows Active Defense

Chad Mills
Windows Defender ATP Research

Phillip Misner
Security Research

Abdul Mohammed
Windows Defender Research Team

Hamish O'Dea
Windows Defender Research Team

Matt Oh
Security Research

Prachi Rathee
Windows Active Defense Data Engineering and Analytics

Robert Rozycki
Windows Active Defense Data Engineering and Analytics

Jonathan San Jose
Windows Defender Research Team

Karthik Selvaraj
Windows Defender Research Team

Charlynn Settlage
Windows Devices Group

Authors (continued)

Mark Simos
Enterprise Cybersecurity Group

Holly Stewart
Windows Defender Research Team

Elda Tan Seng
Windows Defender Research Team

Tomer Teller
Azure Security

Sandhya Venkatraman
Windows Active Defense Data Engineering and Analytics

Maria Vlachopoulou
Security Research

Erik Wahlstrom
Windows Defender Research Team

Alex Weinert
Identity Security and Protection Team

Jason Yim
Windows Active Defense Data Engineering and Analytics

Contributors

Iaan D'Souza- Wiltshire
Content Publishing Team

Sherrie Lotito
Global Communications Team

Louie Mayor
Content Publishing Team

Dolcita Montemayor
Content Publishing Team

John Payseno
Corporate, External, and Legal Affairs

Viet Shelton
Global Communications Team

Daniel Simpson
Content Publishing Team

Sian Suthers
Global Communications Team

Steve Wacker
Wadeware LLC

Table of contents

Foreword

Welcome to the 22nd edition of the *Microsoft Security Intelligence Report*, a bi-annual publication that we create for our customers, partners, and the industry. The purpose of this report is to educate organizations about the current state of threats, recommended best practices, and solutions. What sets it apart from other security reports is the tremendous breadth and depth of intelligence it draws from.

The intelligence that informs this report comes from security-related signals from the consumer and commercial on-premises systems and cloud services that Microsoft operates on a global scale. For example, every month we scan 400 billion emails for phishing and malware, process 450 billion authentications, and execute 18+ billion webpage scans.

In this edition of the report, we've made two significant changes: First, we have organized the data sets into two categories, cloud and endpoint, because we believe it is important to provide visibility across both. Second, we are sharing data about a shorter time period, one quarter (January 2017 – March 2017), instead of six months. We plan to share data on a more regular basis moving forward, so that you can have more timely visibility into the threat landscape. This increase in frequency is rooted in a principle that guides Microsoft technology investments as well: using data and intelligence to help our customers respond to threats faster.

We continue to develop new capabilities in our platforms that use machine learning, automation, and advanced real-time detection techniques. Our aim is to strengthen our customers' ability to not only protect against evolving sophisticated threats, but also quickly detect and respond when a breach occurs.

We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their organizations, software, and users.

Microsoft Security

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 quarter of 2017, with trend data presented on a monthly 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, 1H17 represents the first half of 2017 (January 1 through June 30), and 4Q16 represents the fourth quarter of 2016 (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

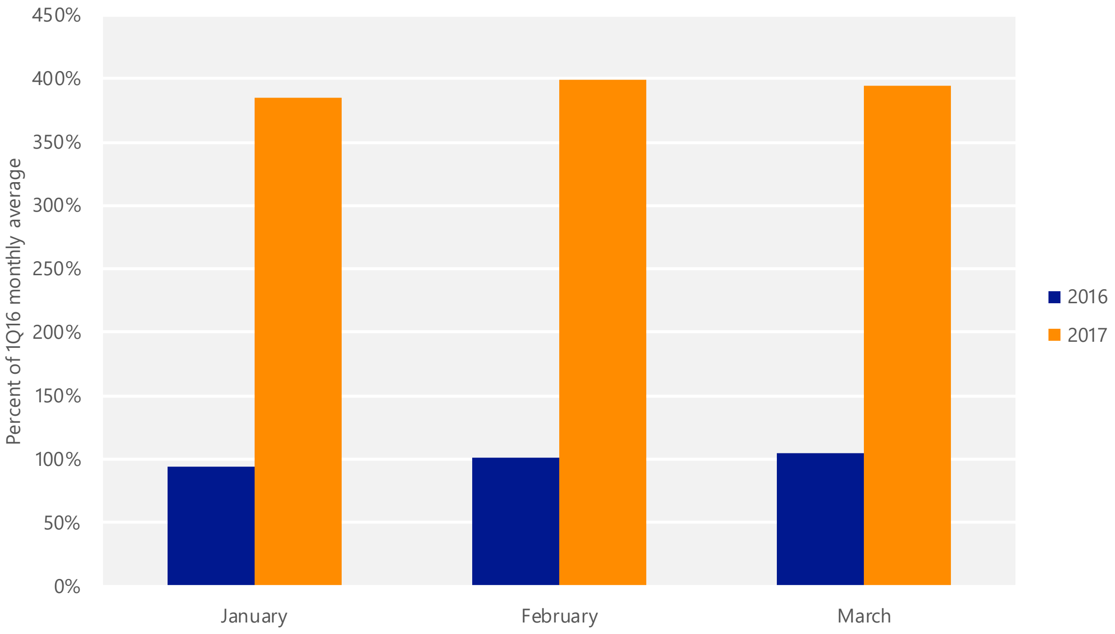
This report uses the Windows Defender Security Intelligence (WDSI; formerly called the Microsoft Malware Protection Center, or MMPC) naming standard for families and variants of malware. For information about this standard, see "Appendix A: Threat naming conventions" on page 43. In this report, any threat 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 and cloud-based detections. For the purposes of this report, a threat is defined as a malicious or unwanted software family or variant that is detected by the Microsoft Malware Protection Engine.

Cloud threat intelligence

Compromised accounts and password safety

Consumer and Enterprise Microsoft accounts are a tempting target for attackers, and the frequency and sophistication of attacks on cloud-based accounts are accelerating. The Identity Security and Protection team has seen a 300 percent increase in user accounts attacked over the past year. A large majority of these compromises are the result of weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services.[1]

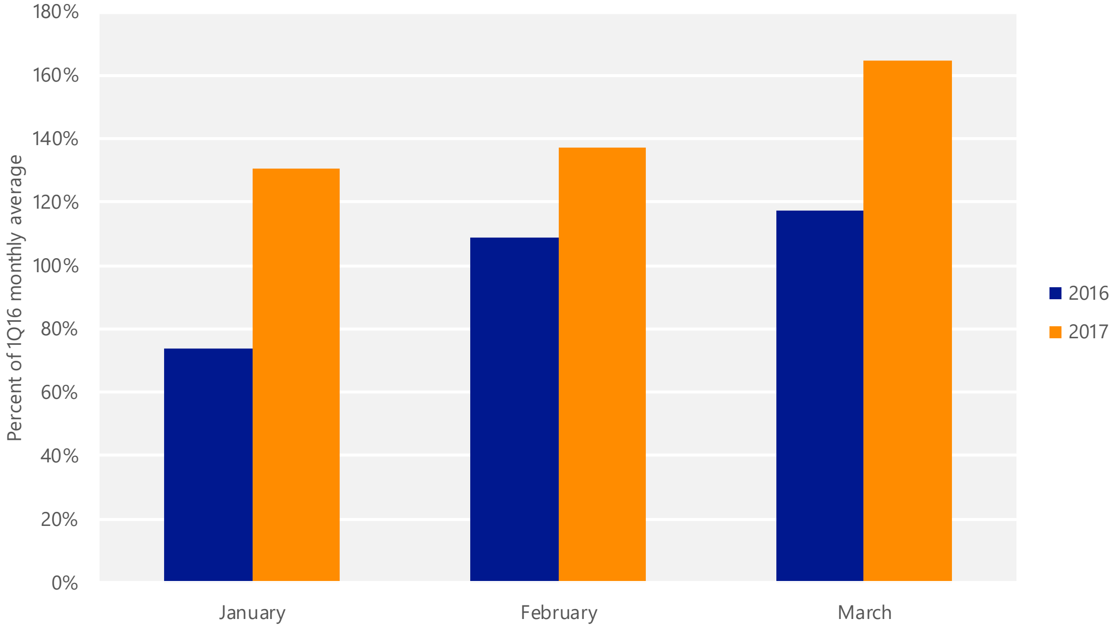
Figure 1. Observed accounts under attack during the first three months of 2016 and 2017



The number of Microsoft account sign-ins attempted from malicious IP addresses has increased by 44 percent from 1Q16 to 1Q17. Security policy based on risk-based conditional access, including comparing the requesting device's IP address to a set of known "trusted IP addresses" or "trusted devices," may help reduce risk of credential abuse and misuse.

[1] Microsoft requires users to choose strong passwords that can't be easily guessed for consumer Microsoft accounts, and recommends that organizations adopt similar policies for their identity management systems.

Figure 2. Total volume of Microsoft account sign-in attempts blocked from malicious IP addresses during the first three months of 2016 and 2017



As an increasing number of sites are breached and passwords phished, attackers attempt to reuse the stolen credentials on multiple services. Therefore, one of the most critical things a user can do to protect themselves is to use a unique password for every site and never reuse passwords across multiple sites. Also, organizations can further minimize risk by training users to avoid the use of simple passwords (easy to guess/crack), using alternative authentication methods or multi-factor authentication, and implementing solutions for credential protection and risk-based conditional access.

Microsoft automated systems detect and block millions of password attacks each day. When an attacker is observed using a valid credential, the request is challenged and the user is required to provide additional validation in order to sign in. Attackers, for their part, can be sophisticated and skilled at mimicking real users, making the task of safeguarding accounts a constantly evolving challenge.

Microsoft offers several solutions to help reduce risk of credential compromise and privileged account abuse:

- Windows Hello for Business lets a user authenticate to a Microsoft account or a non-Microsoft service that supports Fast IDentity Online (FIDO) authentication by having the user set up a gesture (Windows Hello or a PIN), as opposed to having to use a network password to log into the user’s device. This authentication method can be a good alternative to password usage to evade phishing based on password cracking.

- Credential Guard uses virtualization-based security to isolate secrets such as network passwords so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket.
- Microsoft Azure Active Directory Identity Protection provides a consolidated view into risk events and potential vulnerabilities that can affect your organization’s identities. Based on risk events, Identity Protection calculates a user risk level for each user, enabling you to configure risk-based policies to automatically protect the identities of your organization. These policies, along with other conditional access controls provided by Azure Active Directory and Enterprise Mobility + Security, can automatically block the user or offer suggestions that include password resets and multi-factor authentication enforcement.
- Microsoft Privileged Identity Management offers protection for the credentials of privileged accounts, which are accounts that administer and manage IT systems. Cyber-attackers target these accounts to gain access to an organization’s data and systems. To secure privileged access, you should isolate the accounts and systems from the risk of being exposed to a malicious user.
- Azure Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution that helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication via a range of easy verification options including:
  - Phone calls
  - Text messages
  - Mobile app notifications
  - Mobile app verification codes
  - Third-party OATH tokens

  To lower the exposure time of privileges and increase your visibility into their use, users are limited to only taking on their (elevated) privileges "just in time” when they need to perform a task.

Cloud service weaponization

Cloud services such as Microsoft Azure are perennial targets for attackers seeking to compromise and weaponize virtual machines and other services. In a cloud weaponization threat scenario, an attacker establishes a foothold within a cloud infrastructure by compromising and taking control of one or more virtual machines. The attacker can then use these virtual machines to launch attacks, including brute force attacks against other virtual machines, spam campaigns that can be used for email phishing attacks, reconnaissance such as port scanning to identify new attack targets, and other malicious activities.

Azure Security Center actively monitors for cloud weaponization attempts. Figure 3 shows the distribution of the outbound attacks discovered by Azure Security Center advanced detection mechanisms.

Figure 3. Outbound attacks detected by Azure Security Center, 1Q17[2]

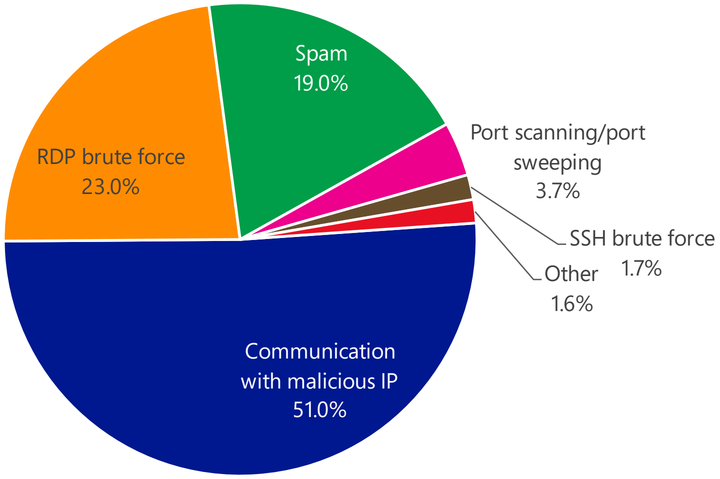


Figure 4 and Figure 5 show where incoming and outgoing attacks originate from.

[2] Communications with malicious IP addresses may be slightly lower than shown due to false positives from a threat intelligence data source.

Figure 4. Incoming attacks detected by Azure Security Center in 1Q17, by country/region of origin

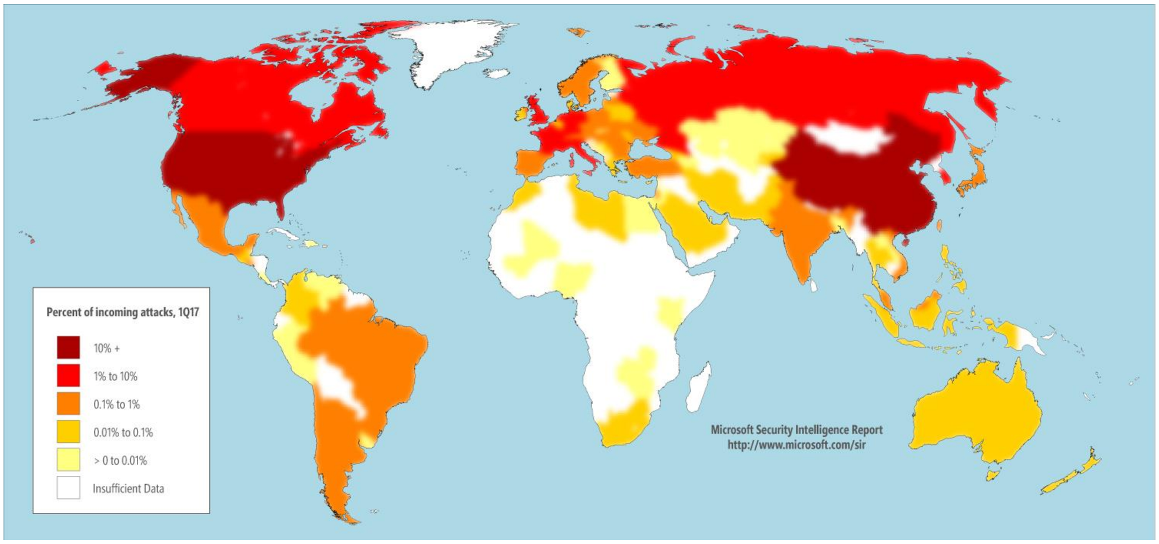
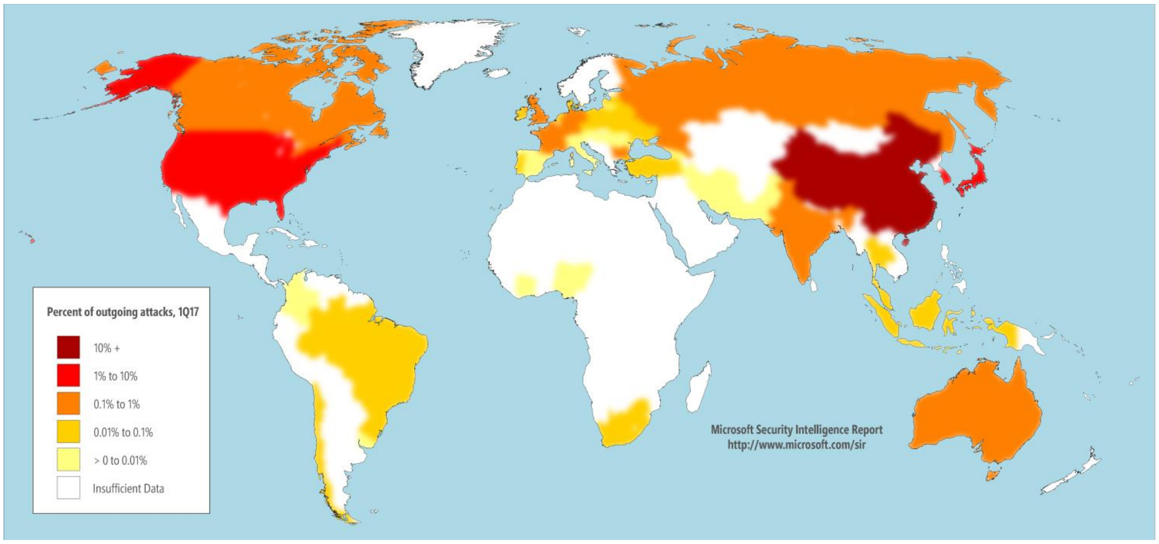

Percent of incoming attacks, 1Q17
10% +
1% to 10%
0.1% to 1%
0.01% to 0.1%
> 0 to 0.01%
Insufficient Data
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Figure 5. Outgoing communication to malicious IP addresses detected by Azure Security Center in 1Q17, by address location


Percent of outgoing attacks, 1Q17
10% +
1% to 10%
0.1% to 1%
0.01% to 0.1%
> 0 to 0.01%
Insufficient Data
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

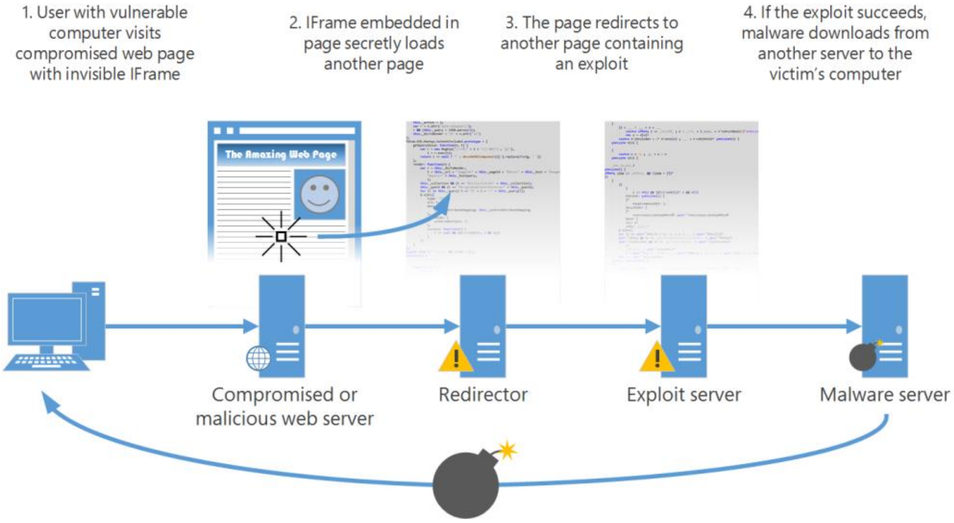
- More than two-thirds of incoming attacks on Azure services in 1Q17 came from IP addresses in China and the United States, at 35.1 percent and 32.5 percent, respectively. Korea was third at 3.1 percent, followed by 116 other countries and regions.
- Compromised virtual machines often communicate with command-and-control (C&C) servers at known malicious IP addresses to receive instructions. More than 89 percent of the malicious IP addresses contacted by compromised Azure virtual machines in 1Q17 were located in China, followed by the United States at 4.2 percent.

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.

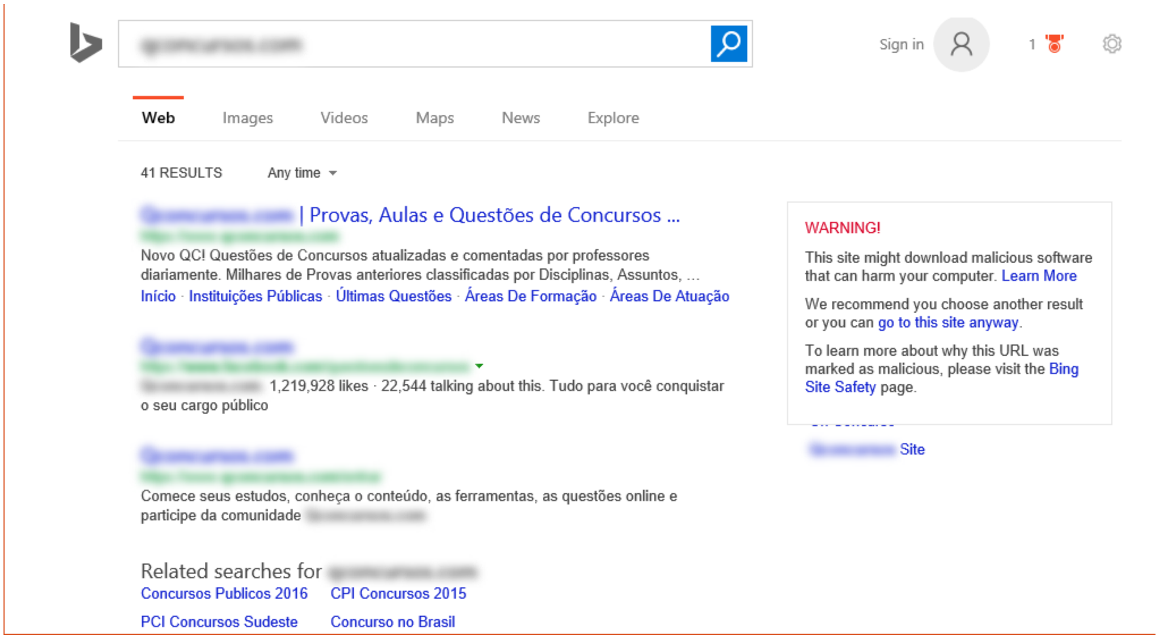
Drive-by download pages are usually hosted on legitimate websites to which an attacker has posted exploit code. Attackers gain access to legitimate sites through intrusion or by posting malicious code to a poorly secured web form, like a comment field on a blog. Compromised sites can be hosted anywhere 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 6. One example of a drive-by download attack


1. User with vulnerable computer visits compromised web page with invisible IFrame
2. IFrame embedded in page secretly loads another page
3. The page redirects to another page containing an exploit
4. If the exploit succeeds, malware downloads from another server to the victim's computer
The Amazing Web Page
Compromised or malicious web server
Redirector
Exploit server
Malware server

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. If the site owner is registered with Bing as a webmaster, they are sent a warning about the malicious content, and can request a reevaluation of the site after taking care of the problem. 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 7.

Figure 7. A drive-by download warning from Bing



[redacted]

[redacted] | Provas, Aulas e Questões de Concursos ...

[redacted]

Novo QC! Questões de Concursos atualizadas e comentadas por professores diariamente. Milhares de Provas anteriores classificadas por Disciplinas, Assuntos, ...

Início · Instituições Públicas · Últimas Questões · Áreas De Formação · Áreas De Atuação

[redacted]

[redacted]

[redacted] 1,219,928 likes · 22,544 talking about this. Tudo para você conquistar o seu cargo público

[redacted]

[redacted]

Comece seus estudos, conheça o conteúdo, as ferramentas, as questões online e participe da comunidade [redacted]

Related searches for [redacted]

Concursos Publicos 2016 CPI Concursos 2015

PCI Concursos Sudeste Concurso no Brasil

WARNING!

This site might download malicious software that can harm your computer. Learn More

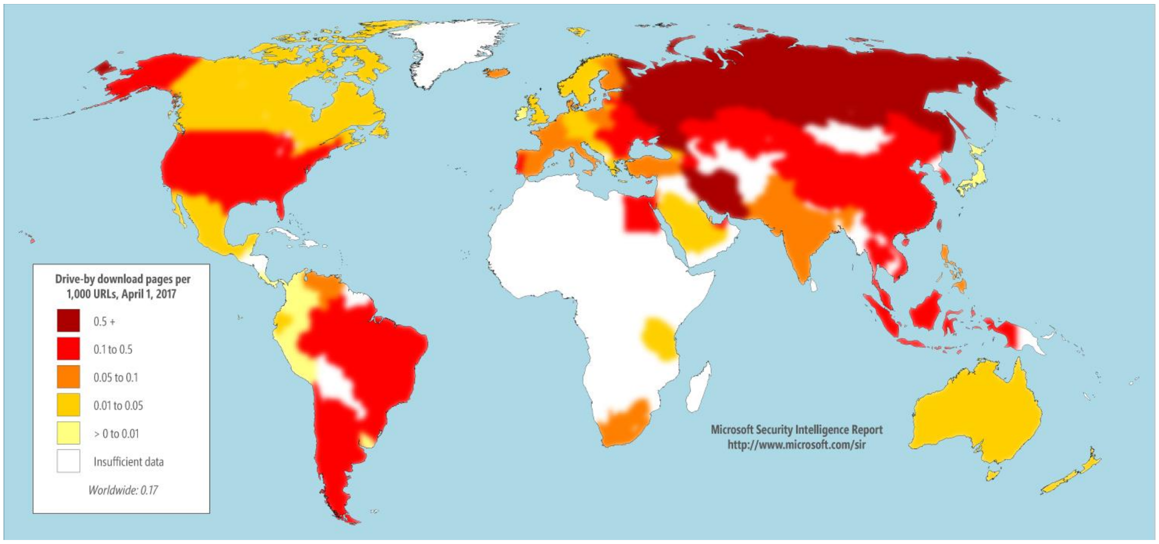
We recommend you choose another result or you can go to this site anyway.

To learn more about why this URL was marked as malicious, please visit the Bing Site Safety page.

[redacted] Site

Figure 8 shows the concentration of drive-by download pages in countries and regions throughout the world in March 2017.

Figure 8. Drive-by download pages indexed by Bing in March 2017, per 1,000 URLs in each country/region


Drive-by download pages per 1,000 URLs, April 1, 2017
0.5 +
0.1 to 0.5
0.05 to 0.1
0.01 to 0.05
> 0 to 0.01
Insufficient data
Worldwide: 0.17
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- Bing detected 0.17 drive-by download pages for every 1,000 pages in the index in March 2017.

Figure 9 and Figure 10 show trends for the locations with the highest and lowest concentrations of drive-by download pages in 2017.

Figure 9. Monthly trends for countries/regions with the highest concentration of drive-by download pages in March 2017

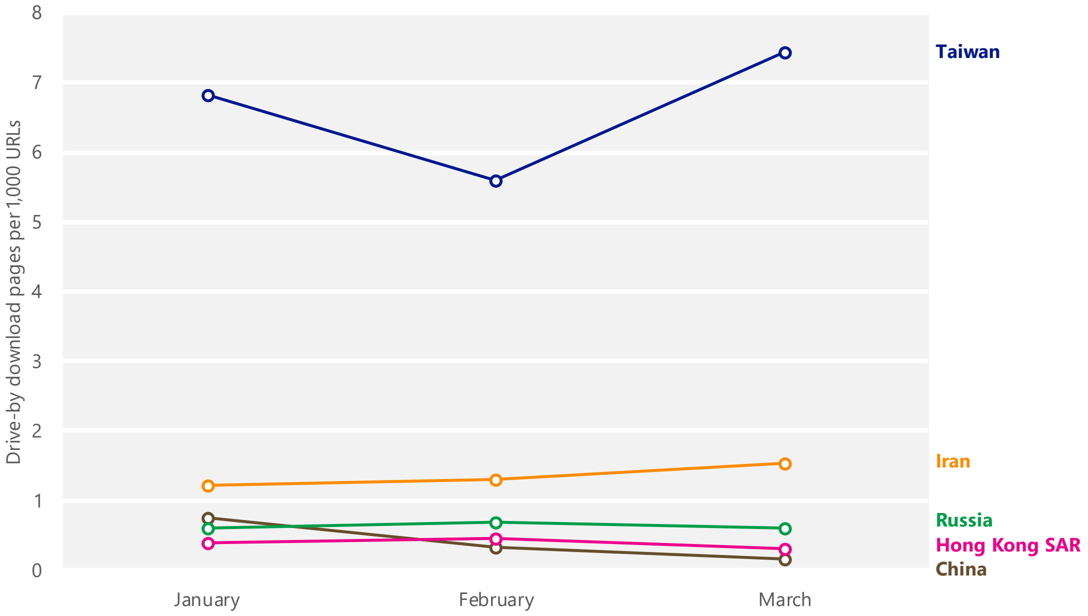
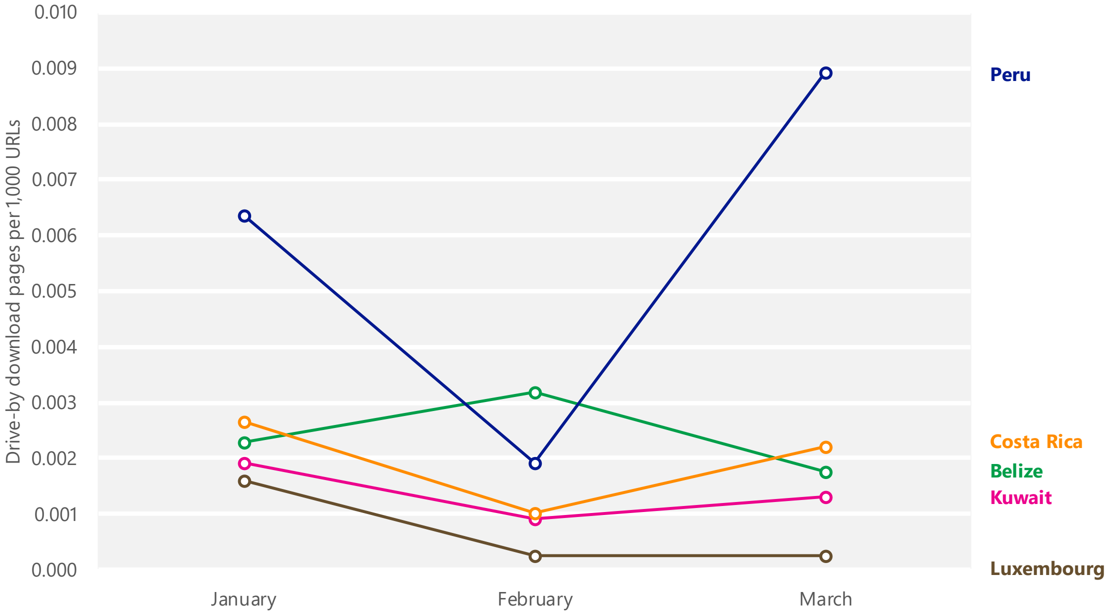


Figure 10. Monthly trends for countries/regions with the lowest concentration of drive-by download pages in March 2017



- Locations with the highest concentration of drive-by download pages in March 2017 include Taiwan (7.4 per 1,000 URLs), Iran (1.5), and Russia (0.6).
- Locations with the lowest concentration of drive-by download pages in March 2017 include Luxembourg (0.001 per 1,000 URLs), Kuwait (0.001), and Belize (0.002).

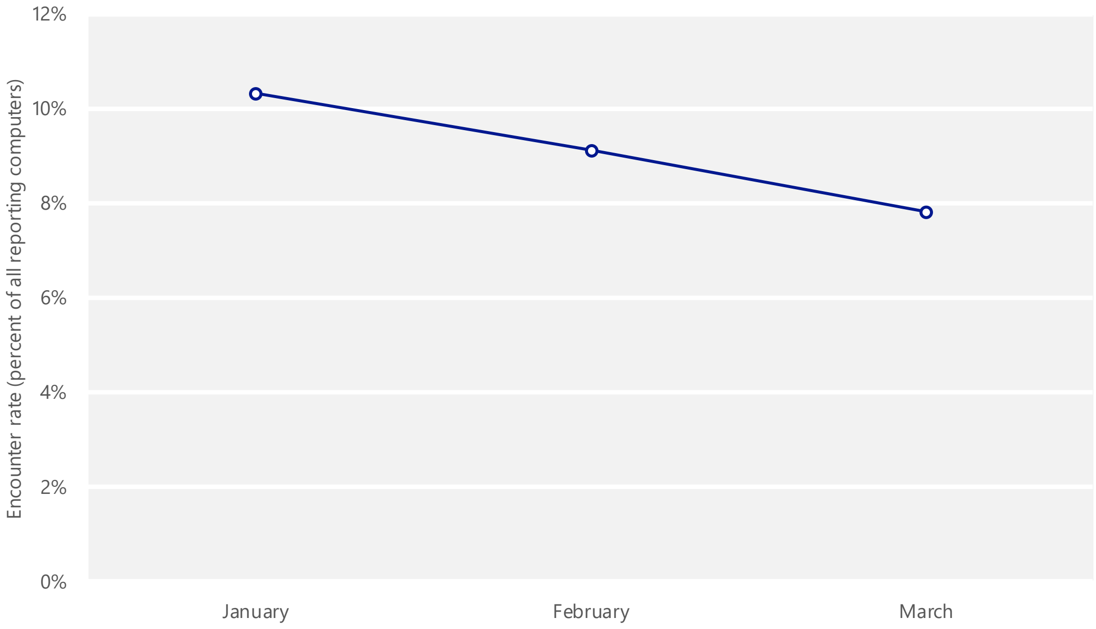
Endpoint threat intelligence

Malicious and unwanted software

Encounter rate

Encounter rate is the percentage of computers running Microsoft real-time security products that report a malware encounter.[3] For example, the encounter rate for the malware family Win32/Banload in Brazil in March 2017 was 0.4 percent. This data means that, of the computers in Brazil that were running Microsoft real-time security software in March 2017, 0.4 percent reported encountering the Banload family, and 99.6 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.[4]

Figure 11. Worldwide monthly encounter rates, January–March 2017

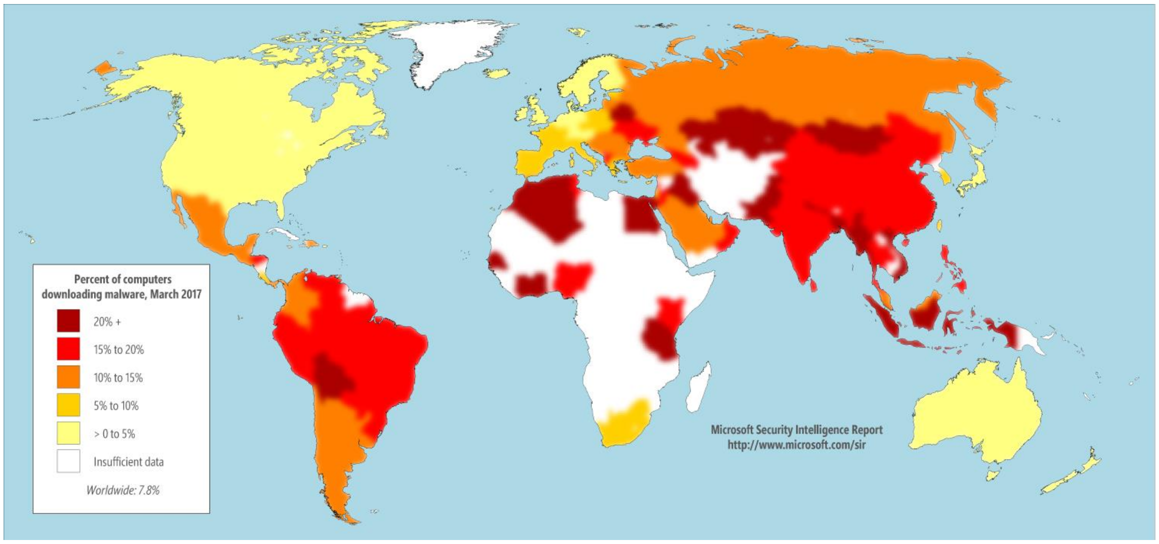


[3] Encounter rate does not include threats that are blocked by a web browser before being detected by antimalware software.

[4] For information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 45.

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 encounter rates, patterns, and trends in different locations around the world. Using encounter rates, Microsoft learns about the most prevalent threats on both global and per country bases, and uses this information to enhance its security products and services to address those threats.

Figure 12. Encounter rates by country/region, March 2017


Percent of computers downloading malware, March 2017
20% +
15% to 20%
10% to 15%
5% to 10%
> 0 to 5%
Insufficient data
Worldwide: 7.8%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- Locations with high encounter rates included Bangladesh, Pakistan, Indonesia, and Egypt, all of which had an average monthly encounter rate of 24.0 percent or higher in 1Q17.
  - Threats that were unusually common in Bangladesh included the worm family Win32/Ippedo (ranked fourth in Bangladesh in March 2017, 28th worldwide), the virus family Win32/Floxif (tenth in Bangladesh, 163rd worldwide), and the worm family Win32/Vercuser (31st in Bangladesh, 214th worldwide).
  - Threats that were unusually common in Pakistan included Win32/Nuqel (fourth in Pakistan, 35th worldwide), Ippedo (tenth in Pakistan, 28th worldwide), and Win32/Tupym (19th in Pakistan, 149th worldwide), all of which are worms.
  - Threats that were unusually common in Indonesia included the worm families Win32/Gamarue (second in Indonesia, 10th worldwide),

  Win32/Macoute (fourth in Indonesia, 33rd worldwide), and Win32/Copali (eighth in Indonesia, 65th worldwide).

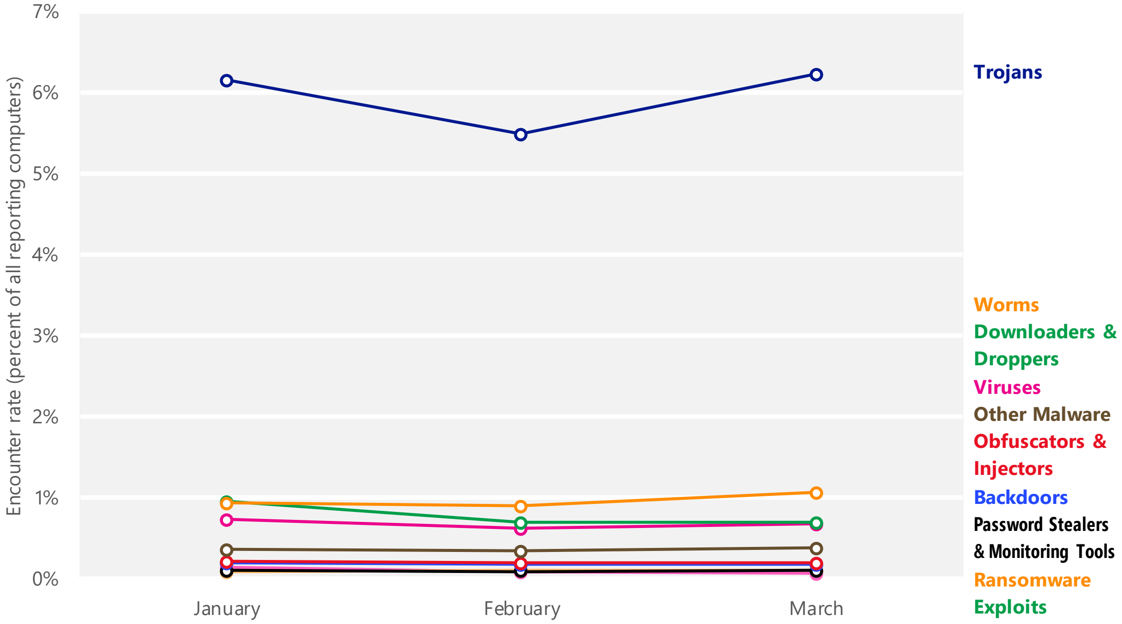
  - Threats that were unusually common in Egypt included the worm family JS/Bondat (seventh in Egypt, 19th worldwide), the virus family Win32/Grenam (11th in Egypt, 34th worldwide), and the backdoor family MSIL/Bladabindi (18th in Egypt, 201st worldwide).

- Locations with low encounter rates included Japan, Finland, Sweden, and Norway, all of which had an average monthly encounter rate of 3.6 percent or lower in 1Q17.
  - Threats that were unusually rare in Japan included the virus family Win32/Neshta (ranked 75th in Japan in March 2017, 24th worldwide), and the worm families Gamarue (122nd in Japan, 10th worldwide) and VBS/Jenxcus (158th in Japan, 12th worldwide).
  - Threats that were unusually rare in Finland included the worm families INF/Autorun (87th in Finland, 21st worldwide), Jenxcus (97th in Finland, 12th worldwide), and Win32/Conficker (136th in Finland, 23rd worldwide).
  - Threats that were unusually rare in Sweden included the trojan family Win32/Mupad (75th in Sweden, 22nd worldwide) and the worm families Autorun (87th in Sweden, 21st worldwide) and Gamarue (107th in Sweden, 10th worldwide).
  - Threats that were unusually rare in Norway included Mupad (67th in Norway, 22nd worldwide), Autorun (68th in Norway, 21st worldwide), and Jenxcus (90th in Norway, 12th worldwide).

Threat categories

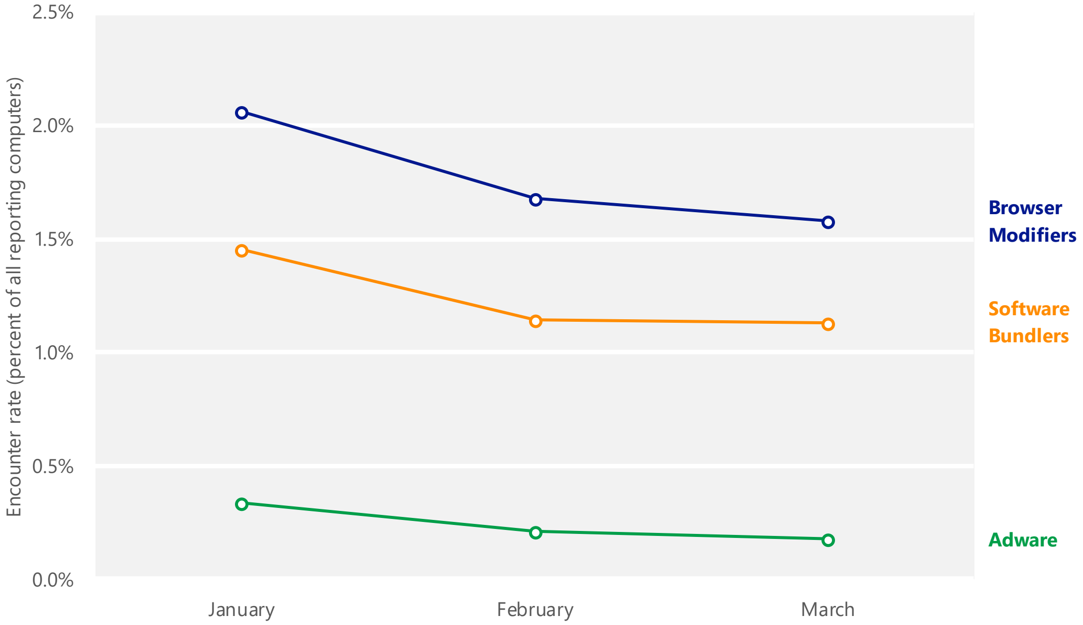
Windows Defender Security Intelligence (WDSI; formerly called the Microsoft Malware Protection Center, or MMPC) classifies individual threats into types based on a number of factors, including how the threat spreads and what it is designed to do. To simplify the presentation of this information and make it easier to understand, the *Microsoft Security Intelligence Report* groups these types into categories based on similarities in function and purpose.

Figure 13. Encounter rates for significant malicious software categories, January–March 2017



- Trojans were the most commonly encountered category of malicious software in 1Q17 by a large margin, led by Win32/Xadupi.
- The Worms category increased slightly from January through March, due in part to an increase in encounters involving Win32/Gamarue.
- Encounters involving the Downloaders and Droppers category fell from second place in January to third in March, due in part to a decline in detections of JS/Nemucod.
- Encounter rates for other categories were much lower and more consistent from month to month.

Figure 14. Encounter rates for unwanted software categories, January–March 2017



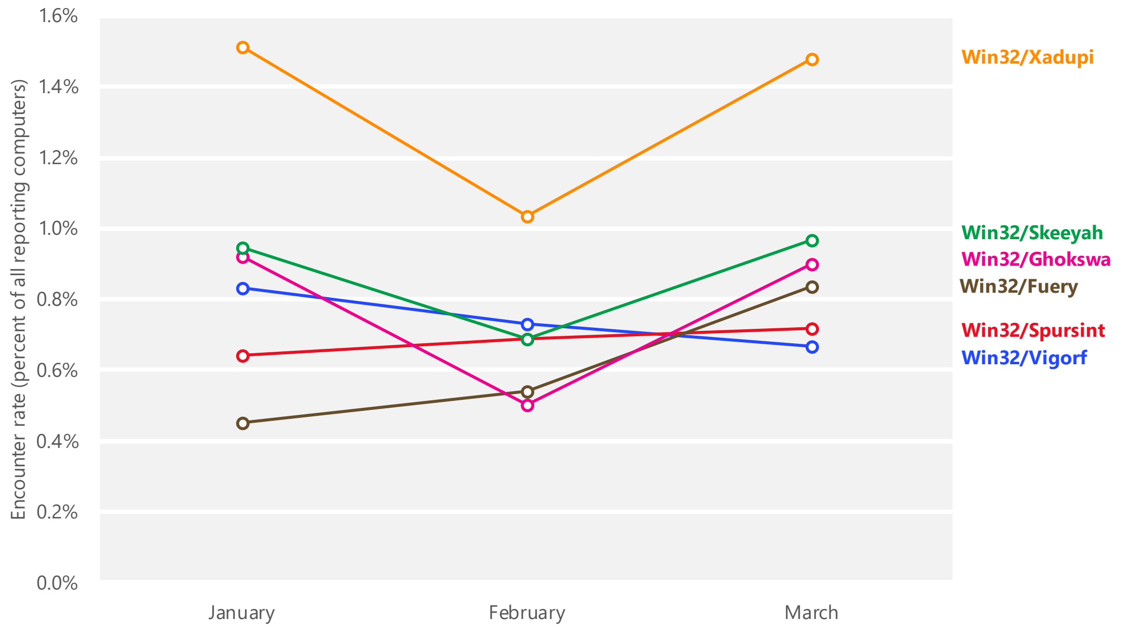
- Unwanted software encounters declined steadily throughout 1Q17 for all three unwanted software categories.[5]
- Browser modifiers were the most commonly encountered category of unwanted software in 1Q17, led by Win32/Diplugem and Win32/Foxiebro.
- Software bundlers were the second most commonly encountered category of unwanted software in 1Q17, led by Win32/ICLoader.
- Adware encounters were significantly less common than the other unwanted software categories, led by Win32/Adposhel.

Threat families

Figure 15 and Figure 16 show trends for the top malicious and unwanted software families that were detected on computers by Microsoft real-time antimalware products worldwide in 1Q17.

[5] Microsoft has published the criteria that the company uses to classify programs as unwanted software at https://www.microsoft.com/wdsi/antimalware-support/malware-and-unwanted-software-evaluation-criteria. 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.

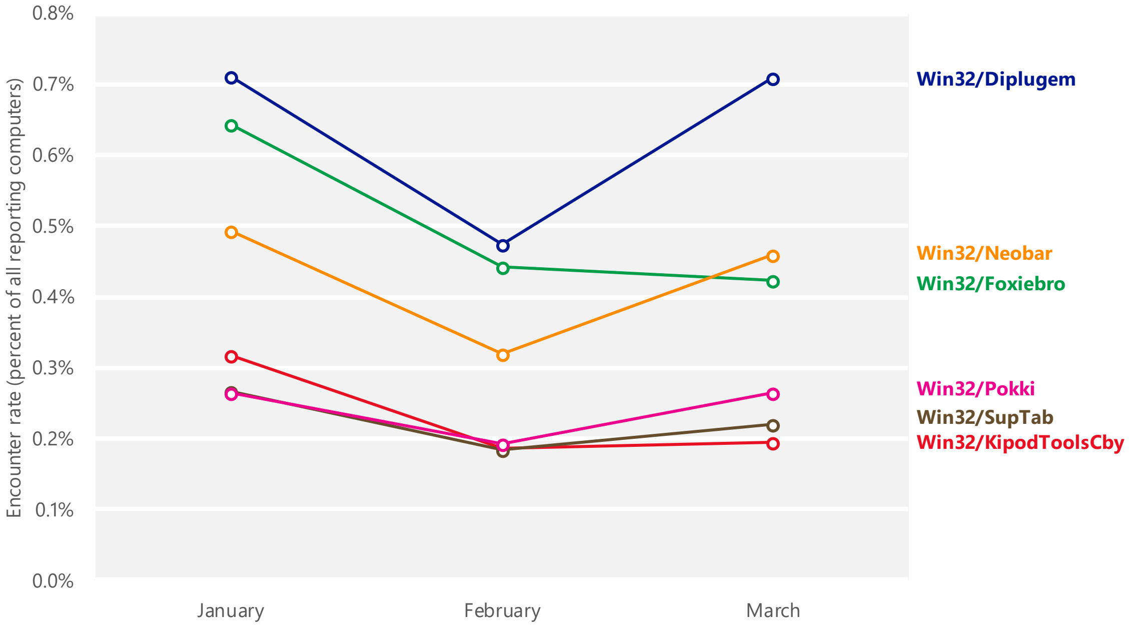
Figure 15. Encounter rate trends for the top malicious software families, January–March 2017



- Win32/Xadupi, the most common malicious software family worldwide in 1Q17, is a trojan that poses as a useful application, usually called WinZipper or QKSee, but can silently download and install other malware. It is often installed silently by the browser modifiers Win32/Sasquor and Win32/SupTab.
- Xadupi and its associated families, including Sasquor, SupTab, Ghokswa, Win32/Chuckenit, and others, are part of a malware suite that is sometimes called "Fireball." See the entry "Understanding the true size of 'Fireball'" (June 22, 2017) on the Windows Security blog at blogs.technet.microsoft.com/mmpc for more information.
- Win32/Skeeyah is a generic detection for a variety of trojans that share certain characteristics.
- Win32/Ghokswa is a trojan that is often downloaded by Xadupi. It installs modified versions of the Chrome or Firefox browsers, replacing any existing copy of the browsers that were already on the system. The modified versions have different search and home page settings that the user may be unable to change, and update components that may download additional unwanted software.
- Win32/Fuery is a cloud-based detection for files that have been automatically identified as malicious by the cloud-based protection feature

of Windows Defender. For more information about the feature and guidance for administering it in network environments, see the article "Block at First Sight" at technet.microsoft.com, and the entry "Windows Defender Antivirus cloud protection service: Advanced real-time defense against never-before-seen malware" (July 18, 2017) on the Windows Security blog at blogs.technet.microsoft.com/mmpc.

Figure 16. Encounter rate trends for the top unwanted software families, January–March 2017



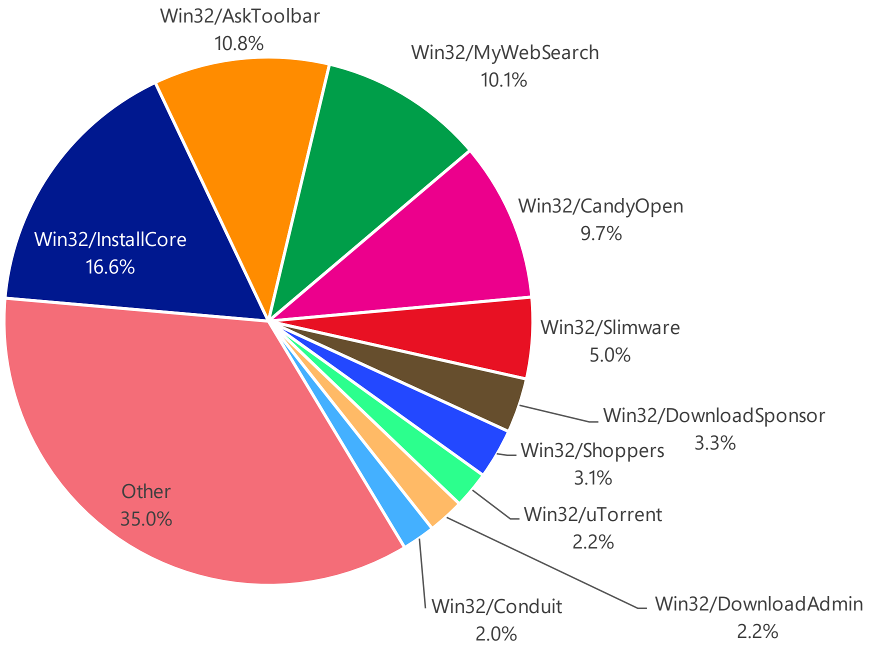
- The most commonly encountered unwanted software families were all browser modifiers.
- Win32/Diplugem is a browser modifier that installs browser extensions without obtaining the user's consent. The browser extensions show extra advertisements as the user browses the web and can inject additional advertisements into web search results pages.
- Win32/Neobar is a browser modifier that can change web browser settings without adequate consent. It is often installed by software bundlers, and has used the names Best YouTube Downloader, Torrent Search, BonusBerry, and several others.
- Win32/Foxiebro is a browser modifier that can inject ads to search results pages, modify web pages to insert ads, and open ads in new tabs.

PUA statistics

Microsoft has published the criteria used to classify programs as unwanted software at https://www.microsoft.com/wdsi/antimalware-support/malware-and-unwanted-software-evaluation-criteria. Characteristics of unwanted software can include depriving users of adequate choice or control over what the software does to the computer, preventing users from removing the software, or displaying advertisements without clearly identifying their source. Microsoft security products classify unwanted software as threats, and block or remove them when they are encountered.

Some programs don't meet the criteria to be considered unwanted software but still exhibit behaviors that may be considered undesirable, particularly in enterprise environments. Microsoft classifies these programs as *potentially unwanted applications* (PUA). For example, a program that displays additional advertisements in the browser might not be classified as unwanted software if it clearly identifies itself as the source of the ads, but may be considered potentially unwanted. Users often end up installing these programs because they were installing an application that they wanted, and the installer offered to install additional software—usually with the offer acceptance checked by default and often without the user realizing they are agreeing to install the additional software. These programs can also cause problems for network administrators—they can affect computer performance, increase the workload for the IT help desk, put computers and data at risk of being compromised through exploits, and make it more difficult to identify malware infections among the noise. To provide organizations with additional options for dealing with programs classified as PUA, Microsoft offers enterprise users of System Center Endpoint Protection (SCEP) the ability to block them from being installed on their networks.

Figure 17. PUA families blocked in March 2017



- PUA:Win32/InstallCore and PUA:Win32/CandyOpen are detections for installer programs that were built with software bundler utilities (called InstallCore and OpenCandy, respectively) that offer monetization opportunities to software developers, such as pay-per-install services for programs that offer to download other programs alongside the requested application. The OpenCandy installer was frequently encountered bundled with µTorrent, a popular file-sharing program, and paint.net, an image and photo editing program. InstallCore was often bundled with audio and video file conversion programs.

Microsoft offers enterprise users of System Center Endpoint Protection the ability to block PUA from being installed on their networks.

- PUA:Win32/AskToolbar and PUA:Win32/MyWebSearch are toolbar programs that are frequently offered for download with other programs through pay-per-install arrangements.
- PUA:Win32/Slimware scans the computer and claims to find dubious "problems" (for example, junk files), and asks for payment to fix them. It also shows advertisements outside its own application.

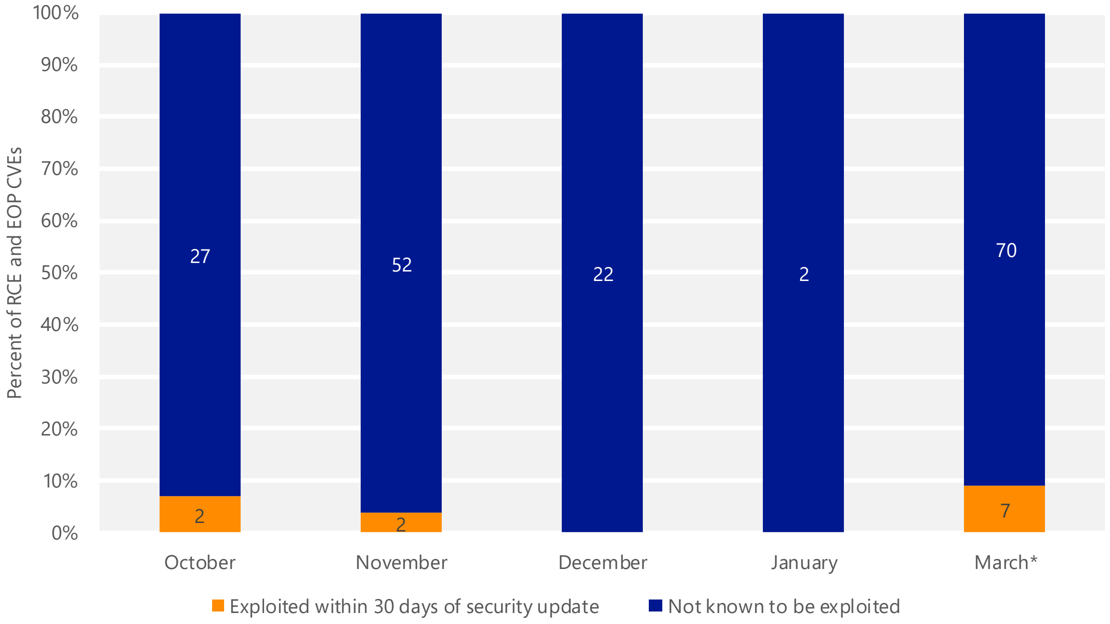
Exploits

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 other software components that are installed on a computer.

Exploitation of vulnerabilities in Microsoft software

The most severe vulnerabilities are those that enable remote code execution (RCE) or elevation of privilege (EOP), because they can enable an attacker to take control of a computer. Figure 18 shows the percentage of disclosed RCE and EOP vulnerabilities in Microsoft software that were exploited in the wild within 30 days of disclosure during each month in 4Q16 and 1Q17. (Exploitation risk tends to decrease significantly after 30 days, as most organizations have typically tested and deployed the update by that point.)

Figure 18. Remote code executable (RCE) and elevation of privilege (EOP) vulnerability disclosures in Microsoft software known to be exploited before the corresponding security update release or within 30 days afterward, October 2016–March 2017



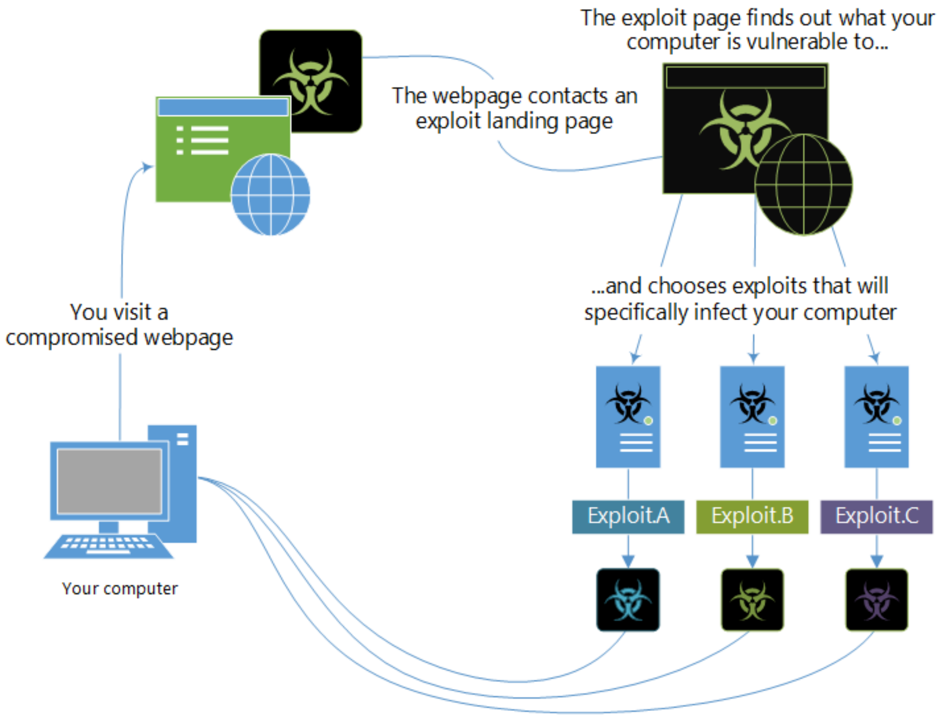
* All updates originally scheduled for February were postponed to March. See https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/ for details.

On average, about 8 percent of RCE and EOP vulnerabilities were exploited within 30 days of the corresponding security update release, with two months having no such exploits at all. This data represents a continuation of a multi-year trend of relatively low exploitation of the most severe vulnerabilities, due in part to the Security Development Lifecycle (SDL) and to additional hardening measures that are present in the latest versions of Microsoft products (notably Windows 10, which was not affected by any of the 11 zero-day vulnerabilities addressed with Microsoft security updates over the six-month period).

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 8 for more information about drive-by downloads.)

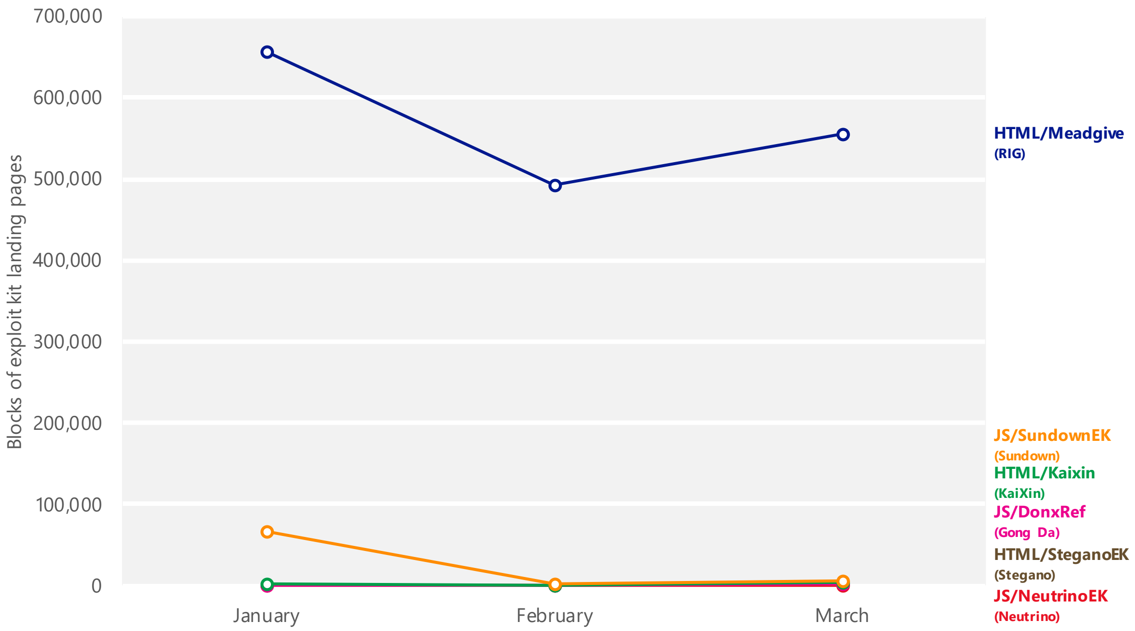
Figure 19. How a typical exploit kit works


The exploit page finds out what your computer is vulnerable to...
The webpage contacts an exploit landing page
You visit a compromised webpage
...and chooses exploits that will specifically infect your computer
Exploit.A
Exploit.B
Exploit.C
Your computer

The IExtensionValidation interface in Internet Explorer 11 allows real-time security software to block ActiveX controls from loading on pages the security software determines to be malicious, including exploit kit landing pages. (Microsoft Edge, the newest Microsoft web browser and the default browser in

Windows 10, does not support ActiveX plug-ins at all, and therefore does not use IExtensionValidation.) Figure 20 shows the prevalence of several top web-based exploit kits blocked by Internet Explorer 11 in 1Q17.

Figure 20. Trends for the top exploit kit-related threats detected and blocked by IExtensionValidation in Internet Explorer 11 in 1Q17



The Angler and Neutrino exploit kits vanished in June and September of 2016, respectively.

- The Angler (Axpergle) and Neutrino exploit kits, which accounted for the vast majority of exploit kit blocks during the first half of 2016, vanished in June and September of 2016, respectively. (See "Exploit kits remain a cybercrime staple against outdated software – 2016 threat landscape review series" (January 23, 2017) on the Windows Security blog at blogs.technet.microsoft.com/mmpc for more information and statistics.) The RIG kit (detected as Meadgive) was the largest beneficiary of the disappearance of Angler and Neutrino, and held a commanding share of the exploit kit market through the first three months of 2017, with all other kits far behind.
- Exploit kit traffic volumes were significantly lower in 1Q17 than a year prior. Angler alone regularly received more than a million blocks a month in 2016 before it disappeared. Although RIG has picked up traffic since the disappearance of Angler and Neutrino, it has yet to approach the levels displayed by the top kits in early 2016, and preliminary statistics from 2Q17 suggest that RIG has begun to decline as well.

- Windows 10 computers face much less risk from exploits than computers running older versions of Windows. Many of the vulnerabilities targeted by the most prevalent kits are not present in Windows 10; in other cases, mitigations built into Windows 10 prevent an attacker from exploiting a vulnerability productively. Microsoft Edge, the default web browser in Windows 10, does not support ActiveX controls, and therefore cannot be used to host any of the vulnerable browser add-ons that exploit kits often target. These advantages are magnified by the fact that exploit kits often avoid presenting landing pages to computers running Windows 10 or Microsoft Edge at all, in an effort to avoid being detected on computers they are unlikely to successfully exploit.

Notable exploits in 1Q17

Many of the more dangerous exploits are used in *targeted attacks* before appearing in the wild in larger volumes. 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. Some, though not all, of these exploits are later adopted by exploit kits and used in widespread attacks. Figure 21 lists some of the exploits Microsoft has observed being used in targeted attacks in 2017.

Figure 21. Notable exploits disclosed in early 2017

CVE	Exploit type	Type	Affecting	Security Bulletin	Used in Widespread attacks?
CVE-2017-0149	Internet Explorer Memory Corruption Vulnerability (VBSCRIPT)	RCE	Internet Explorer	MS17-006	NO
CVE-2017-0144	Windows SMB Remote Code Execution Vulnerability	RCE	Microsoft Windows	MS17-010	YES
CVE-2017-0005	Windows GDI Elevation of Privilege Vulnerability	EOP	Microsoft Windows	MS17-013	NO

- CVE-2017-0149 was a zero-day remote code execution (RCE) vulnerability exploited in limited targeted attacks in Asia that affected the VBScript component of Internet Explorer, which is enabled by default in legacy document modes to support old websites for compatibility reasons. Microsoft Edge does not support VBScript and is unaffected by this exploit.

Microsoft published Security Bulletin MS17-006 in March 2017 to address the issue.

In response to several zero-day exploits affecting the VBScript engine discovered over the past two years, at the end of 1Q17 Microsoft published a mitigation for Internet Explorer to enable users and administrators to easily block VBScript execution in all document modes. Planned future updates of Windows will disable VBScript by default in Internet Explorer 11 for websites in the Internet Zone and the Restricted Sites Zone. For more information, see the following entries on the Microsoft Edge Developer blog at blogs.windows.com/msedgedev:

  - Disabling VBScript execution in Internet Explorer 11 (April 12, 2017)
  - An update on disabling VBScript in Internet Explorer 11 (July 7, 2017)

- CVE-2017-0144, the so-called "EternalBlue" vulnerability, is an RCE vulnerability targeting the Server Message Block version 1 (SMBv1) implementation in Windows. Microsoft published Security Bulletin MS17-010 in March 2017 to address the issue. An exploit for the vulnerability was disclosed by the Shadow Brokers hacker group in April 2017 as part of a leak of highly advanced, government-grade exploits apparently developed for use in cyberwarfare. In May, the exploit was used by the ransomware worm Win32/WannaCrypt (also called "WannaCry") to infect thousands of computers running versions of Windows earlier than Windows 10, which is not affected by the attack.

  See "Staying safe from WannaCrypt" on page 28 for more information about WannaCrypt. For more information about CVE-2017-0144 and other Shadow Brokers exploits, see "Protecting customers and evaluating risk" (April 14, 2017) on the Microsoft Security Response Center blog at blogs.technet.microsoft.com/msrc, and "Analysis of the Shadow Brokers release and mitigation with Windows 10 virtualization-based security" (June 16, 2017) on the Windows Security blog at blogs.technet.microsoft.com/mmpc.

- CVE-2017-0005 was a zero-day vulnerability in the Graphics Device Interface (GDI) implementation in Windows that was exploited in limited targeted attacks by an actor or group Microsoft refers to as ZIRCONIUM. The exploit was crafted to gain elevated privileges on computers running Windows 7 and Windows Server 2008. Mitigations built into the Windows 10

Anniversary Update (1607), released in August 2016, prevent elevation of privilege (EOP) on computers running the latest versions of Windows 10.

For more information about the exploit and how it was used, see this blog post from the Windows Defender ATP research team: Detecting and mitigating elevation-of-privilege exploit for CVE-2017-0005 (March 27, 2017) on the Windows Security blog at blogs.technet.microsoft.com/mmpc.

Recommendations for guarding against these and other dangerous exploits:

- Apply security updates as soon as possible. Every day a security update is available without being installed means increased risk of exploitation.
- Install the most recent release of Windows 10 to take advantage of its improved hardening and security mitigations.
- Use Microsoft Edge as the preferred browser to take advantage of additional mitigations and sandbox technologies.
- If possible, disable the legacy SMBv1 protocol and filter external SMB traffic to the corporate network. See the entry "Disabling SMBv1 through Group Policy" (June 15, 2017) on the Microsoft Security Guidance blog for details.
- Consider disabling VBScript execution in Internet Explorer 11 using tools available in the Windows 10 Creators Update.

Ransomware

Ransomware is a type of malware that restricts access to data by encrypting files or locking computer screens. It then attempts to extort money from victims by asking for "ransom" in exchange for access to the data. Early ransomware families displayed what looked like official warnings from well-known law enforcement agencies, accusing the computer user of committing a computer-related crime and demanding that the user pay a fine via electronic money transfer or a virtual currency to regain control of the computer. In recent years, many of the more commonly encountered ransomware families have dropped this pretense; they simply encrypt important files on the computer and offer to sell the user the private key to decrypt them. Attackers often demand payment in Bitcoin, a popular virtual currency, or through other difficult-to-trace means.

Microsoft recommends that victims of ransomware infections not pay the so-called fine. Ransomware is distributed by malicious attackers, not legitimate authorities, and paying the ransom is no guarantee that the attacker will restore the affected computer to a usable state. Microsoft provides free tools and utilities, such as the Microsoft Safety Scanner and Windows Defender Offline, that can help remove a variety of malware infections even if the computer's normal operation is being blocked. See https://www.microsoft.com/wdsi/threats/ransomware for additional ransomware guidance from Windows Defender Security Intelligence.

Staying safe from WannaCrypt and Petya

Two new ransomware families, Win32/WannaCrypt (also known as WannaCry) and Win32/Petya, emerged in early 2017 to target out-of-date Windows operating systems.[6] The ransomware attacks were widespread, affecting computers around the world, and garnered considerable media coverage. Microsoft had already identified and provided a fix for the vulnerabilities targeted by these new attacks via Security Bulletin MS17-010. Windows 10 includes mitigations that prevent common exploitation techniques by these and other threats. All users and organizations should install all available security updates, including MS17-010, and ensure that automatic updates are enabled. In addition to exploiting vulnerabilities, Petya can use stolen credentials to move laterally across a local network and infect nonvulnerable computers, so it's especially important to keep all the computers in a network up to date to prevent an initial infection.

For technical information about both WannaCrypt and Petya, including suggestions for threat mitigation, see the following posts on the Windows Security blog at https://blogs.technet.microsoft.com/mmpc:

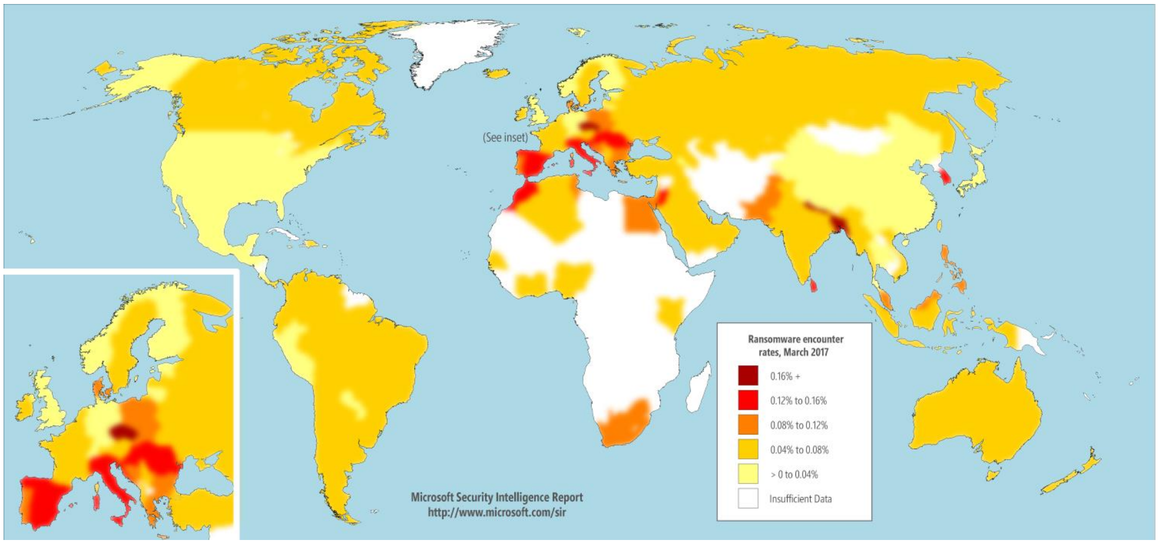
- WannaCrypt ransomware targets out-of-date systems (May 12, 2017)
- New ransomware, old techniques: Petya adds worm capabilities (June 27, 2017)
- Windows 10 platform resilience against the Petya ransomware attack (June 29, 2017)

For the Microsoft perspective, read "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack" (May 14, 2017) on the Microsoft On the Issues blog at blogs.microsoft.com/on-the-issues.

[6] These families emerged in 2Q17 and are therefore not included in the statistics presented in this volume of the *Microsoft Security Intelligence Report*, which covers data up to and including 1Q17 only. See the next volume for WannaCrypt and Petya encounter statistics.

Ransomware affects different parts of the world in varying degrees. Figure 22 shows encounter rates for ransomware families by country and region in March 2017.

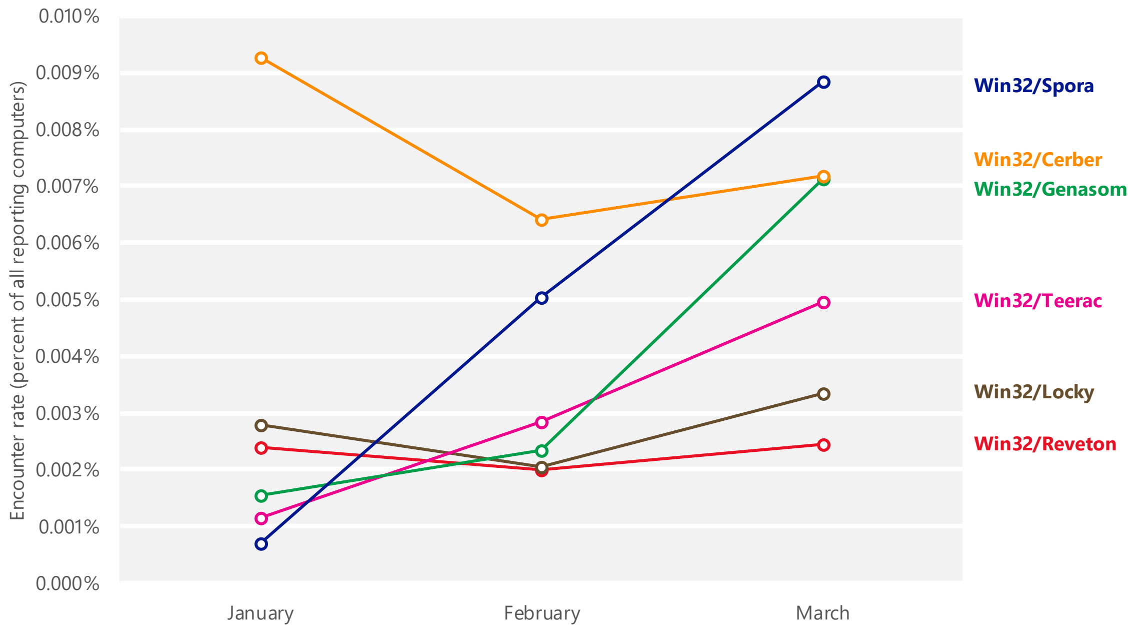
Figure 22. Encounter rates for ransomware families by country/region in March 2017


(See inset)
Ransomware encounter rates, March 2017
0.16% +
0.12% to 0.16%
0.08% to 0.12%
0.04% to 0.08%
> 0 to 0.04%
Insufficient Data
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- Locations with the highest ransomware encounter rates include the Czech Republic (0.17 percent), Korea (0.15 percent), and Italy (0.14 percent).
- Locations with the lowest ransomware encounter rates include Japan (0.012 percent in March 2017), China (0.014 percent), and the United States (0.02 percent).
- Ransomware disproportionately targeted computers in Europe in 1Q17. In addition to the Czech Republic (0.17 percent), Italy (0.14 percent), Hungary (0.14 percent), Spain (0.14 percent), Romania (0.13 percent), Croatia (0.13 percent), and Greece (0.12 percent) all had much higher ransomware encounter rates than the average in March 2017.

Figure 23 displays encounter rate trends for several of the most commonly encountered ransomware families worldwide.

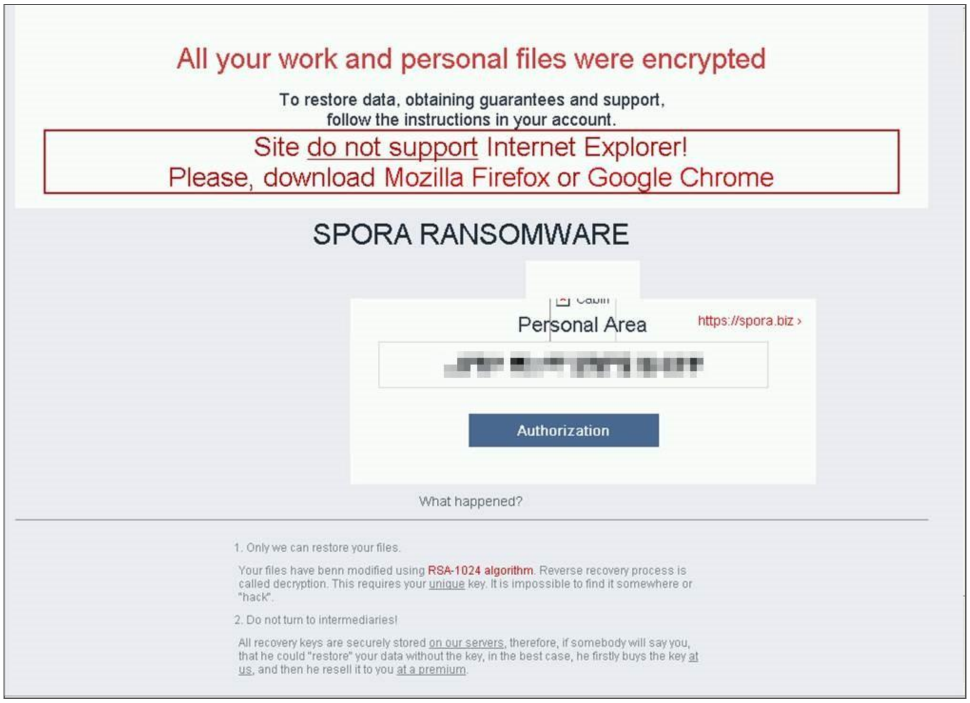
Figure 23. Trends for several commonly encountered ransomware families in 1Q17, by month



Spora encrypts files with several popular extensions, including .doc, .docx, .jpg, .pdf, .xls, .xlsx, and .zip.

- Win32/Spora, first discovered in January 2017, has rapidly become one of the most widespread ransomware families this year. It was the most commonly encountered ransomware family in March 2017. Spora encrypts files with several popular extensions, including .doc, .docx, .jpg, .pdf, .xls, .xlsx, and .zip. It avoids encrypting files in the Games, Program Files (x86), Program Files, and Windows folders. Early versions of Spora targeted Russian speakers, although English language versions have also been seen.

Figure 24. Screen from Win32/Spora



All your work and personal files were encrypted

To restore data, obtaining guarantees and support,
follow the instructions in your account.

Site do not support Internet Explorer!
Please, download Mozilla Firefox or Google Chrome

SPORA RANSOMWARE

[redacted]

What happened?

1. Only we can restore your files.

Your files have benn modified using RSA-1024 algorithm. Reverse recovery process is called decryption. This requires your unique key. It is impossible to find it somewhere or "hack".

2. Do not turn to intermediaries!

All recovery keys are securely stored on our servers, therefore, if somebody will say you, that he could "restore" your data without the key, in the best case, he firstly buys the key at us, and then he resell it to you at a premium.

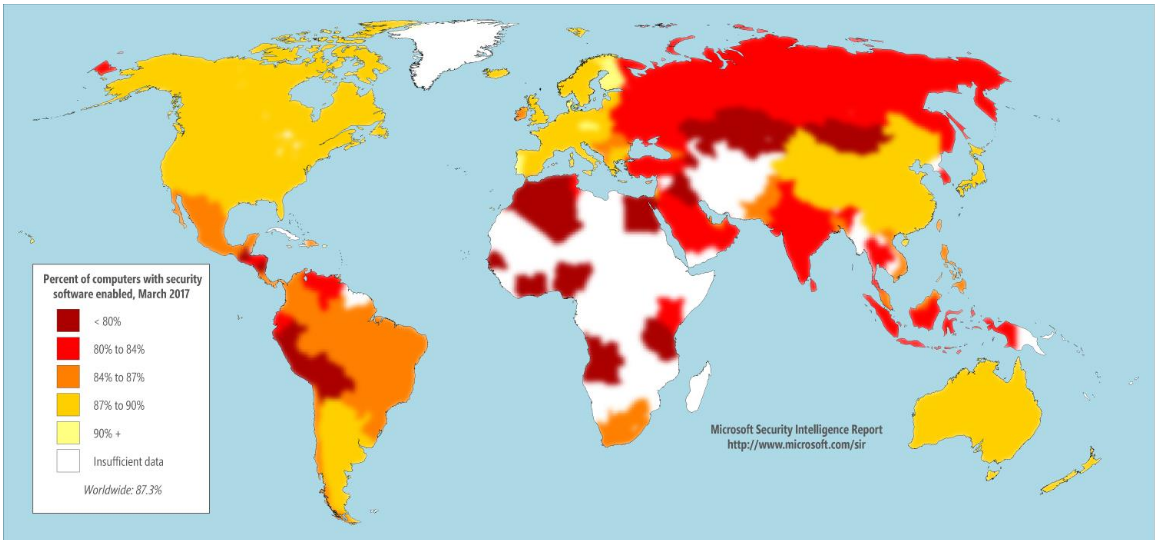
- Win32/Cerber was the most commonly encountered ransomware family in 1Q17 overall, although it fell to second in March as Spora rose. It is often spread via the RIG (Meadgive) and Magnitude (Pangimop) exploit kits. Cerber is a ransomware-as-a-service family, sold to prospective attackers by its creators and designed to be easy to use by novices.
- Win32/Genasom is a generic detection for a variety of ransomware families that share certain characteristics.

For more information about defending against ransomware, see the entry "Windows 10 Creators Update provides next-gen ransomware protection" (June 8, 2017) on the Windows Security blog at blogs.technet.microsoft.com/mmpc.

Security software use

Recent releases of the Malicious Software Removal Tool (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 25 shows the percentage of computers worldwide that the MSRT found to be running up-to-date real-time security software in March 2017.

Figure 25. Percent of computers reporting security software enabled, March 2017

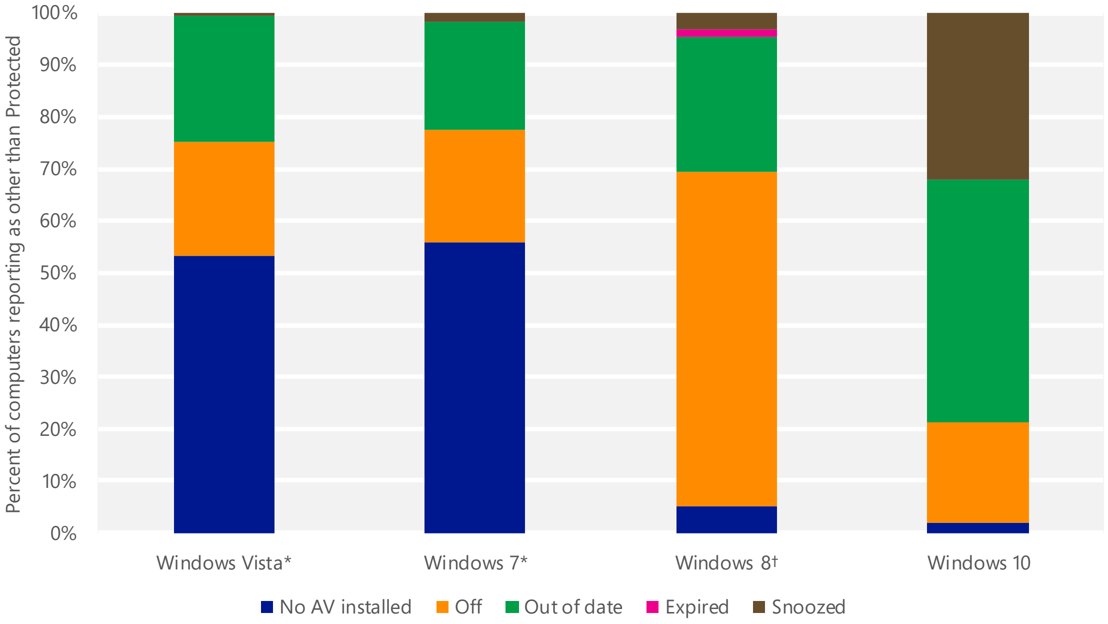

Percent of computers with security software enabled, March 2017
< 80%
80% to 84%
84% to 87%
87% to 90%
90% +
Insufficient data
Worldwide: 87.3%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- All of the countries and regions shown in Figure 25 had more than 73 percent of computers reporting as protected in March 2017.
- The locations with the highest percentage of computers reporting as protected by real-time security software include Finland, at 92.2 percent in March 2017; Portugal, at 90.3 percent; and Denmark, at 90.2 percent.
- Locations with the fewest computers reporting as fully protected include Peru, at 78.3 percent; Venezuela, at 80.4 percent; and Turkey, at 80.6 percent.

Security software use by platform

The reasons computers go unprotected can vary significantly by platform, as Figure 26 illustrates.

Figure 26. Computers running supported client versions of Windows reporting statuses other than Protected in March 2017



* Windows Vista and Windows 7 do not report expired subscriptions. †Includes Windows 8.1.

- On Windows Vista and Windows 7, unprotected computers predominantly report having no antimalware software installed at all. On subsequent Windows versions, 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, computers on which real-time security software is installed but turned off account for the largest percentage of unprotected computers. This is not always deliberate: a number of prevalent malware families are capable of disabling some security products, potentially without the user even knowing. In other cases, users might disable 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.
- On Windows 10, out-of-date signatures were the most common reason computers lacked protection. Computers on which real-time monitoring had been temporarily turned off, or "snoozed," accounted for the second-highest share. By keeping the antivirus software (e.g. Windows Defender) on computers up-to-date (not turning it off knowingly), computers can be better protected against these threats.

Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. 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.

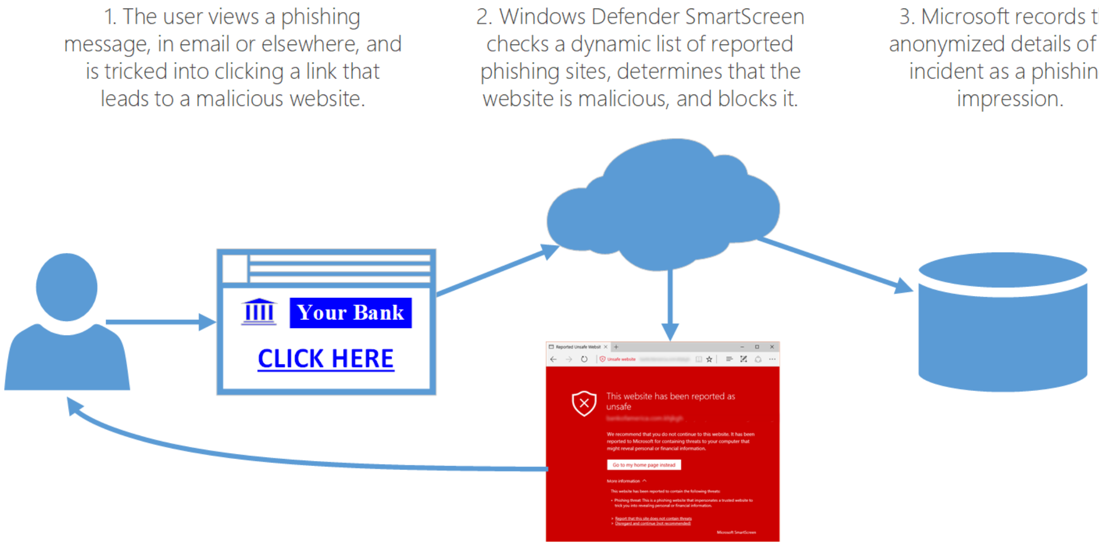
The information in this section is compiled from a variety of sources, including telemetry data produced by Windows Defender SmartScreen in Internet Explorer versions 8 through 11 and Microsoft Edge, from a database of known active phishing and malware hosting sites reported by users of Microsoft Edge, Internet Explorer, and other Microsoft products and services, and from malware data provided by Microsoft antimalware technologies. (See "Appendix B: Data sources" on page 45 for more information about the products and services that provided data for this report.)

Phishing sites

Microsoft gathers information about phishing sites and impressions from *phishing impressions* that are generated by users who choose to enable SmartScreen.[7] A phishing impression is a single instance of a user attempting to visit a known phishing site with SmartScreen enabled and being warned, as illustrated in Figure 27.

[7] See "Appendix B: Data sources" on page 45 for privacy statements and other information about the products and services used to provide data for this report.

Figure 27. How Microsoft tracks phishing impressions


1. The user views a phishing message, in email or elsewhere, and is tricked into clicking a link that leads to a malicious website.
2. Windows Defender SmartScreen checks a dynamic list of reported phishing sites, determines that the website is malicious, and blocks it.
3. Microsoft records the anonymized details of the incident as a phishing impression.
Your Bank
CLICK HERE
Reported Unsafe Websit
Unsafe website

[redacted]

This website has been reported as unsafe

[redacted]

We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

Go to my home page instead

More information ^

This website has been reported to contain the following threats:

- Phishing threat: This is a phishing website that impersonates a trusted website to trick you into revealing personal or financial information.

> Report that this site does not contain threats
> Disregard and continue (not recommended)

Microsoft SmartScreen

Target institutions

Some types of sites tend to consistently draw many more impressions per site than others. Figure 28 and Figure 29 show the breakdown of phishing sites and impressions by category as reported by SmartScreen.

Figure 28. Phishing sites reported by SmartScreen for each type of phishing site, January–March 2017

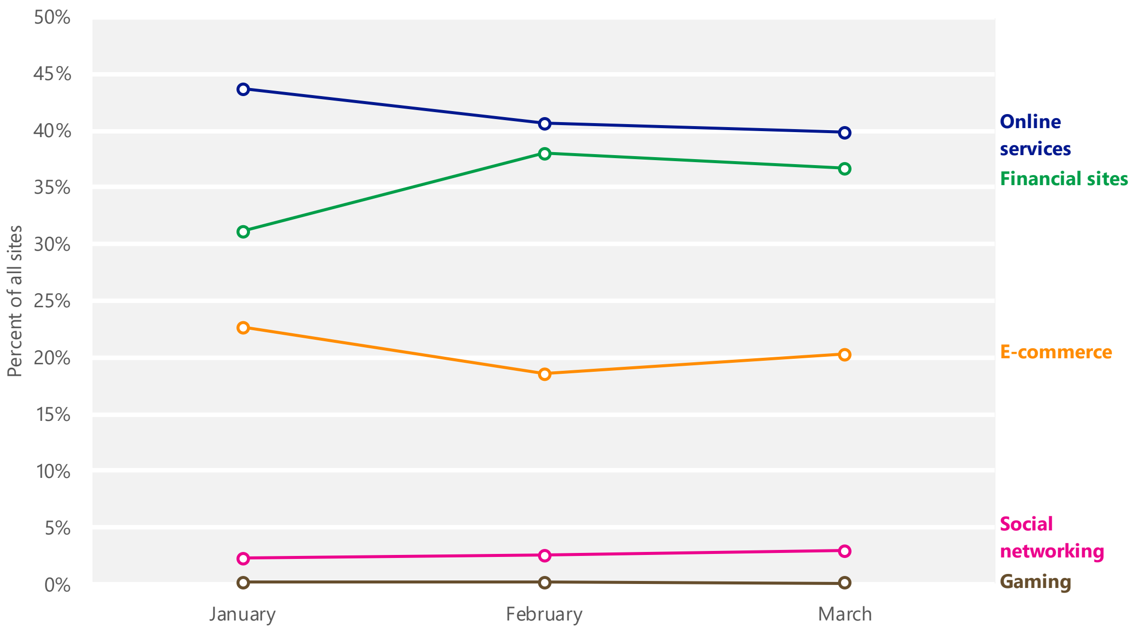
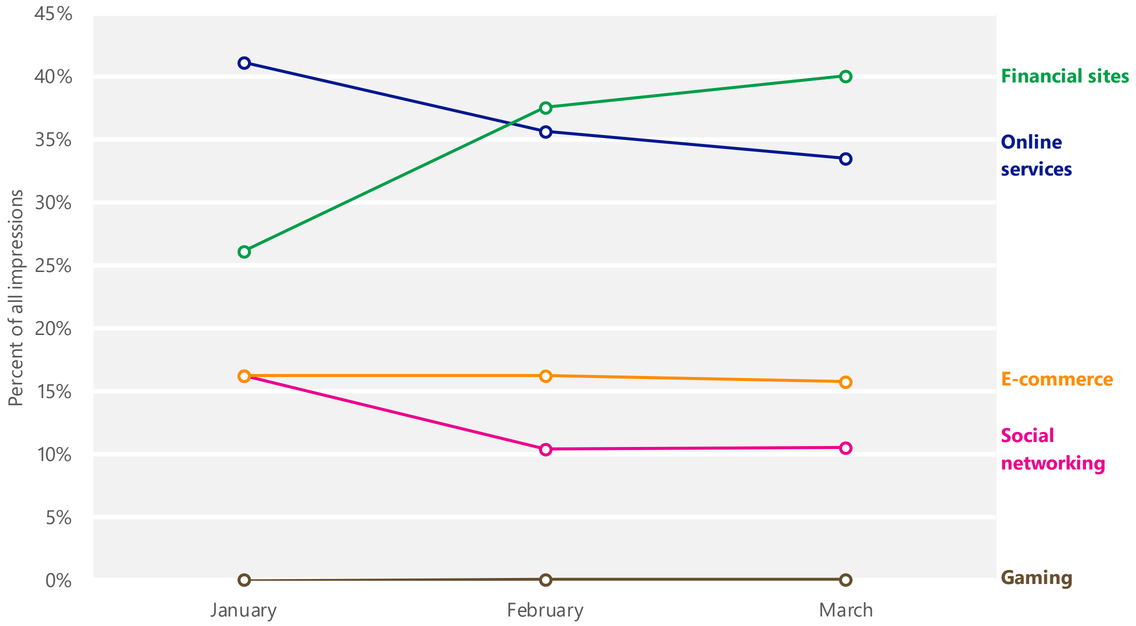


Figure 29. Phishing impressions reported by SmartScreen for each type of phishing site, January–March 2017

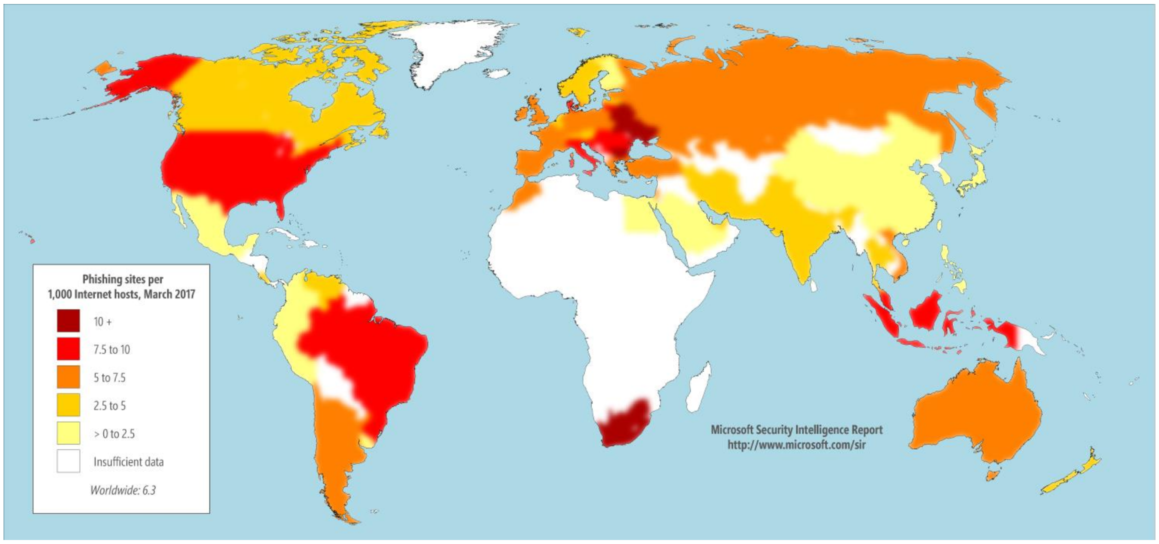


- Phishing sites that targeted online services accounted for the largest number of active phishing URLs during 1Q17, and also received the largest share of impressions during the period, despite decreasing in relative terms in February and March.
- Financial institutions have always been popular phishing targets because of their potential for providing direct illicit access to victims' bank accounts. Sites that targeted financial institutions accounted for the second-largest share of both attacks and impressions during 1Q17 overall, and accounted for the largest share of impressions in February and March.
- The other three categories each accounted for a small percentage of both sites and impressions.

Global distribution of phishing sites and clients

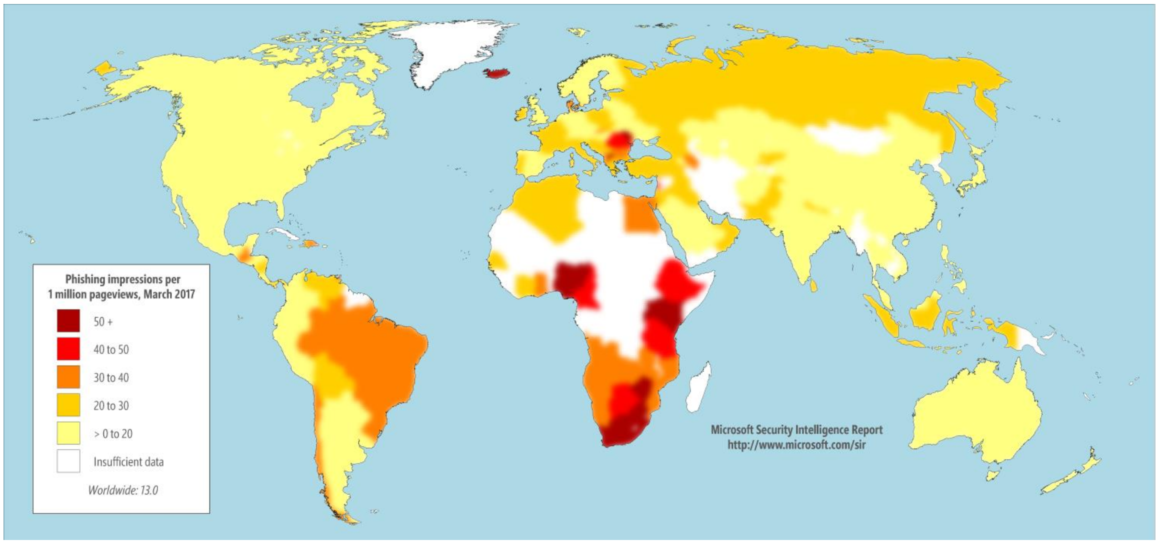
Phishing impression information from SmartScreen includes anonymized information about the IP addresses of the clients making the reports, as well as the IP addresses of the phishing sites themselves. Performing geographic lookups on these addresses makes it possible to analyze patterns among both the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

Figure 30. Phishing sites per 1,000 Internet hosts for locations around the world in March 2017


Phishing sites per
1,000 Internet hosts, March 2017
10 +
7.5 to 10
5 to 7.5
2.5 to 5
> 0 to 2.5
Insufficient data
Worldwide: 6.3
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- SmartScreen detected 6.3 phishing sites per 1,000 Internet hosts worldwide in March 2017.
- Locations hosting higher than average concentrations of phishing sites include Ukraine (13.2 per 1,000 Internet hosts in March), South Africa (10.3), Indonesia (9.6), and Denmark (9.7). Locations with low concentrations of phishing sites include China (0.6), Taiwan (0.6), Korea (0.7), and Mexico (1.2).

Figure 31. Phishing impressions by client location per 1,000,000 pageviews in March 2017


Phishing impressions per
1 million pageviews, March 2017
50 +
40 to 50
30 to 40
20 to 30
> 0 to 20
Insufficient data
Worldwide: 13.0
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- SmartScreen reported 13.0 phishing impressions per 1,000,000 pageviews in March 2017.

- Locations with unusually high rates of phishing impressions included Iceland (99.4 phishing impressions per 1,000 pageviews in March), South Africa (57.9), and Nigeria (55.5).
- Locations with unusually low rates of phishing impressions include China (0.7 impressions per 1,000,000 pageviews in March), Korea (1.4), and Japan (2.8).

Malware hosting sites

SmartScreen helps provide protection against sites that are known to host malware, in addition to phishing sites. SmartScreen 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 and to better combat malware distribution.

Figure 32. SmartScreen in Microsoft Edge and Internet Explorer displays a warning when a user attempts to download an unsafe file

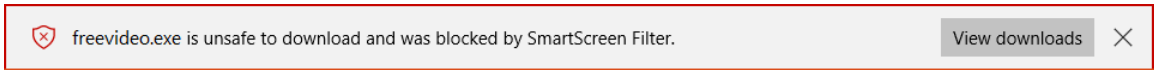
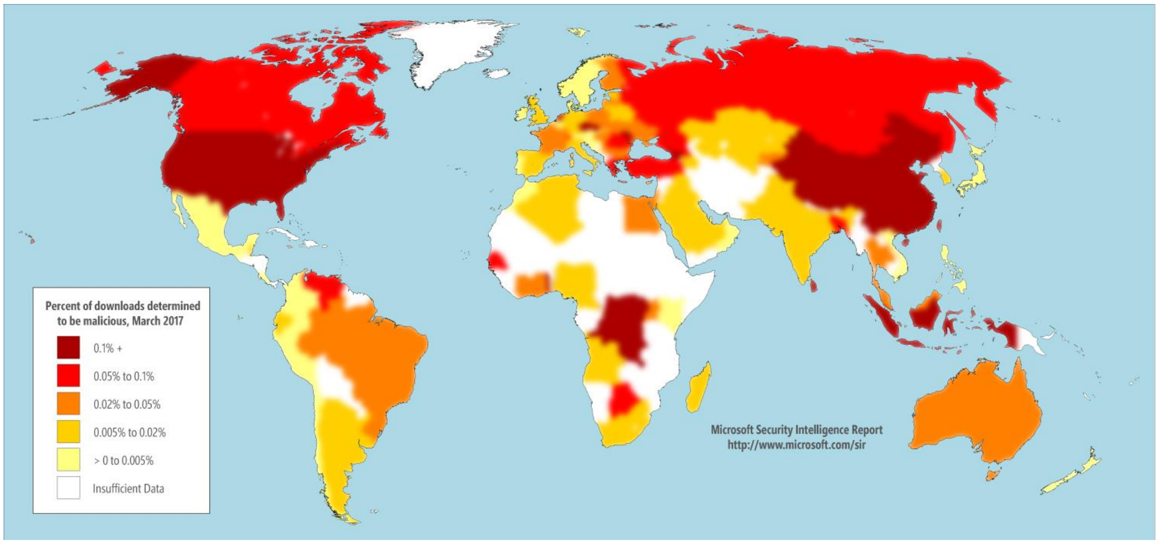

freevideo.exe is unsafe to download and was blocked by SmartScreen Filter.

Figure 33 shows the percentage of all downloads blocked as malicious in different countries and regions in March 2017.

Figure 33. Percent of downloads determined to be malicious, by host location, March 2017


Percent of downloads determined to be malicious, March 2017
0.1% +
0.05% to 0.1%
0.02% to 0.05%
0.005% to 0.02%
> 0 to 0.005%
Insufficient Data
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

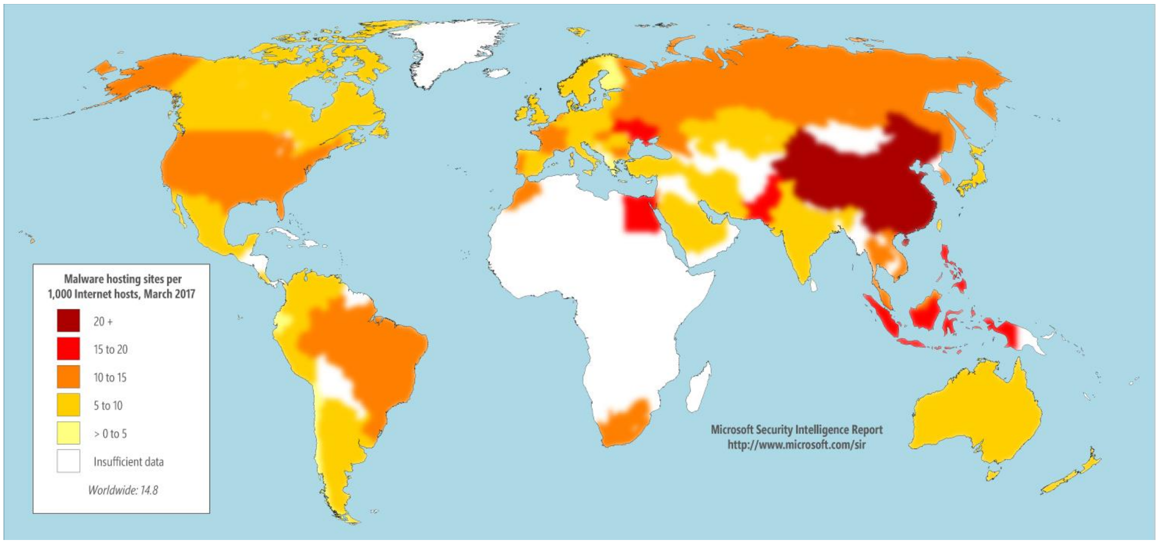
- Locations with the highest percentages of malicious downloads include China (3.5 percent of all downloads in March 2017), Georgia (0.5 percent), and Indonesia (0.2 percent).

- Locations with the lowest percentages of malicious downloads include New Zealand (0.0003 percent in March 2017), Ireland (0.0008 percent), and Sweden (0.001 percent).

Global distribution of malware hosting sites and clients

Figure 34 and Figure 35 show the geographic distribution of malware hosts and computers reporting impressions in March 2017.

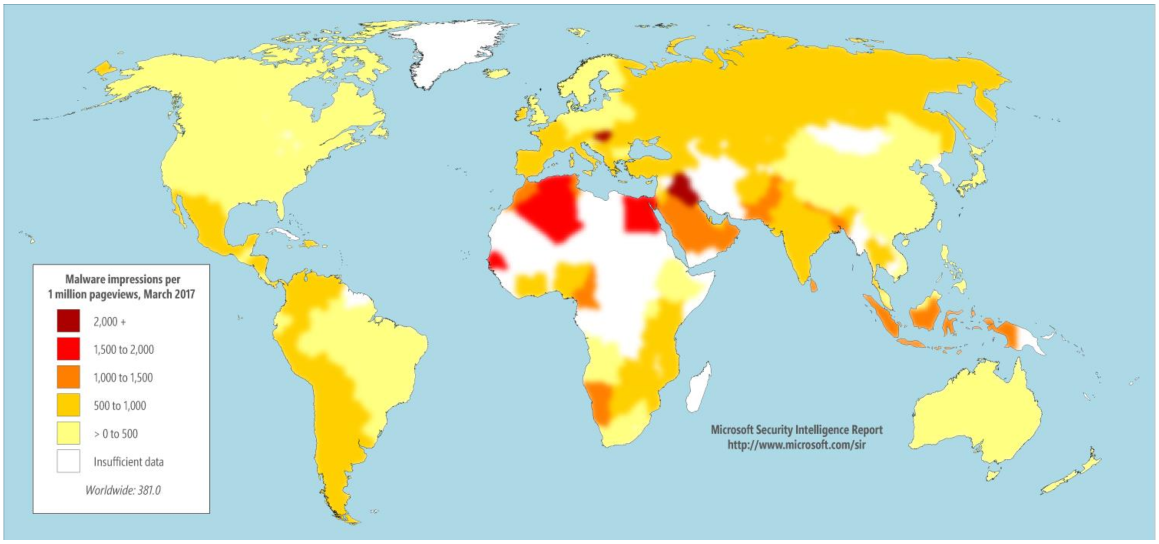
Figure 34. Malware distribution sites per 1,000 Internet hosts for locations around the world in March 2017


Malware hosting sites per 1,000 Internet hosts, March 2017
20 +
15 to 20
10 to 15
5 to 10
> 0 to 5
Insufficient data
Worldwide: 14.8
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- SmartScreen detected 14.8 malware hosting sites per 1,000 Internet hosts worldwide in March 2017.
- China, which had one of the lowest concentrations of phishing sites in the world (0.8 phishing sites per 1,000 Internet hosts in March), had one of the highest concentrations of malware hosting sites (45.9 malware hosting sites per 1,000 hosts in March). Other locations with high concentrations of malware hosting sites included Singapore (21.6), Ukraine (19.0), and Hong Kong SAR (18.9). Locations with low concentrations of malware hosting sites included Finland (4.1), Taiwan (5.3), and Turkey (5.3).

> China, which had one of the lowest concentrations of phishing sites in the world, had one of the highest concentrations of malware hosting sites.

Figure 35. Malware impressions by client location per 1,000,000 pageviews in March 2017



- Malware impressions were much more common than phishing impressions in 1Q17. SmartScreen reported 381.0 malware impressions per 1,000,000 pageviews in March, compared to 13.0 phishing attempts per 1,000,000 pageviews.
- Locations that were heavily affected by malware impressions included Hungary (2,055.8 malware impressions per 1,000,000 pageviews in March), Egypt (1,975.4), and Indonesia (1,329.5).
- Locations with unusually low malware impression rates included Korea (54.4), Japan (147.6), and the United States (211.9).

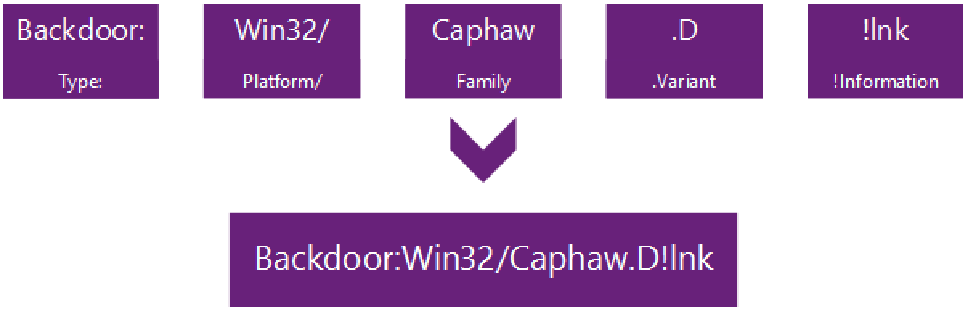
Appendixes

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 36. The Microsoft malware naming convention



When Microsoft analysts research a particular threat, they 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 that 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:

- Azure Security Center is a service that helps organizations prevent, detect, and respond to threats by providing increased visibility into the security of cloud workloads and using advanced analytics and threat intelligence to detect attacks.
- 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 the Microsoft-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 1Q17. 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 Office 365 Advanced Threat Protection.
- Windows Defender in Windows 8, Windows 8.1, and Windows 10 provides real-time scanning and removal of malware and unwanted software.
- Windows Defender Advanced Threat Protection is a new service built into Windows 10 Anniversary Update that enables enterprise customers to detect, investigate, and remediate advanced persistent threats and data breaches on their networks.
- 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.
- Windows Defender SmartScreen, a feature in Microsoft Edge and Internet Explorer, offers users protection against phishing sites and sites that host malware. Microsoft maintains a database of phishing and malware sites reported by users of Microsoft Edge, 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.

Figure 37. US privacy statements for the Microsoft products and services used in this report

Product or service	Privacy statement URL
Azure Security Center	www.microsoft.com/en-us/privacystatement/OnlineServices/Default.aspx
Bing	privacy.microsoft.com/en-us/privacystatement/
Exchange Online, Office 365	www.microsoft.com/online/legal/v2/?docid=43
Internet Explorer 11	privacy.microsoft.com/en-us/internet-explorer-ie11-preview-privacy-statement
Malicious Software Removal Tool	www.microsoft.com/en-us/safety/pc-security/msrt-privacy.aspx
Microsoft Edge	privacy.microsoft.com/en-us/privacystatement/
Microsoft Safety Scanner	www.microsoft.com/security/scanner/en-us/privacy.aspx
Microsoft Security Essentials	windows.microsoft.com/en-us/windows/security-essentials-privacy
System Center Endpoint Protection	https://www.microsoft.com/privacystatement/en-us/SystemCenter2012R2/Default.aspx#tilepspSystemCenter2012R2EndpointProtectionModule
Windows Defender in Windows 10	privacy.microsoft.com/en-us/privacystatement/
Windows Defender Offline	privacy.microsoft.com/en-us/windows-defender-offline-privacy

Appendix C: Worldwide encounter rates

“Encounter rate” on page 13 explains how threat patterns differ significantly in different parts of the world. Figure 38 shows the encounter rates for 1Q17 for locations around the world.[8] See page 13 for information about how encounter rates are calculated.

Figure 38. Encounter rates for locations around the world, 1Q17, by month (100,000 computers reporting minimum)

Country/region	January 2017	February 2017	March 2017
Worldwide	*10.3%*	*9.1%*	*7.8%*
Albania	16.3%	14.2%	15.4%
Algeria	25.1%	22.0%	24.3%
Argentina	13.0%	11.5%	11.1%
Armenia	22.7%	19.2%	18.3%
Australia	5.3%	4.7%	3.5%
Austria	6.0%	5.2%	3.3%
Azerbaijan	20.8%	18.2%	18.7%
Bangladesh	28.3%	25.7%	26.6%
Belarus	25.3%	21.8%	22.1%
Belgium	6.9%	6.1%	3.7%
Bolivia	19.4%	18.0%	21.1%
Bosnia and Herzegovina	16.9%	13.6%	14.0%
Brazil	19.4%	16.8%	17.0%
Bulgaria	19.5%	15.6%	14.6%
Cambodia	28.0%	24.9%	24.2%
Canada	6.0%	5.0%	3.2%
Chile	12.0%	10.3%	10.8%
China	15.6%	16.7%	19.0%

[8] Encounter rate are shown for locations with at least 100,000 computers running Microsoft real-time security products during a month. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.

Country/region	January 2017	February 2017	March 2017
Colombia	15.7%	14.6%	13.3%
Costa Rica	13.0%	11.1%	9.4%
Côte d’Ivoire	20.8%	18.4%	20.6%
Croatia	14.3%	11.2%	10.2%
Cyprus	12.0%	9.3%	9.9%
Czech Republic	8.6%	7.0%	6.2%
Denmark	4.8%	4.3%	2.1%
Dominican Republic	17.3%	15.4%	14.9%
Ecuador	18.8%	16.9%	17.9%
Egypt	25.8%	21.4%	24.8%
El Salvador	15.5%	14.0%	13.7%
Estonia	10.5%	8.7%	8.5%
Finland	3.6%	3.1%	2.0%
France	8.1%	7.4%	5.5%
Georgia	17.9%	14.2%	16.0%
Germany	5.4%	4.5%	2.9%
Ghana	20.5%	18.3%	21.2%
Greece	12.0%	9.0%	8.0%
Guatemala	15.5%	13.7%	12.8%
Honduras	17.8%	16.4%	16.4%
Hong Kong SAR	8.0%	7.5%	6.4%
Hungary	17.7%	14.1%	14.1%
Iceland	5.8%	4.6%	4.9%
India	16.4%	14.1%	15.5%
Indonesia	25.6%	22.4%	25.6%
Iraq	25.7%	22.3%	23.5%
Ireland	5.1%	4.9%	2.6%
Israel	11.8%	8.4%	7.2%
Italy	10.5%	9.2%	7.1%
Jamaica	14.1%	12.3%	12.8%
Japan	3.0%	2.5%	1.1%
Jordan	18.5%	16.2%	16.9%

Country/region	January 2017	February 2017	March 2017
Kazakhstan	22.5%	20.7%	22.2%
Kenya	17.9%	15.5%	17.1%
Korea	10.5%	9.0%	8.3%
Kuwait	12.9%	11.5%	12.9%
Latvia	15.2%	12.3%	11.6%
Lebanon	17.0%	14.2%	15.2%
Lithuania	15.2%	12.5%	11.3%
Luxembourg	6.3%	5.3%	4.8%
Macedonia, FYRO	18.7%	14.8%	15.4%
Malaysia	14.1%	12.7%	11.9%
Malta	9.9%	7.7%	8.0%
Mexico	14.1%	12.8%	12.1%
Moldova	23.5%	20.1%	19.5%
Mongolia	26.3%	21.8%	24.6%
Morocco	22.5%	19.6%	21.6%
Myanmar	26.5%	22.7%	22.2%
Nepal	24.8%	21.8%	22.2%
Netherlands	7.4%	5.9%	3.3%
New Zealand	5.3%	4.3%	3.1%
Nigeria	16.7%	14.7%	16.5%
Norway	5.1%	3.9%	1.6%
Oman	15.1%	14.0%	16.0%
Pakistan	27.8%	24.9%	26.2%
Palestinian Authority	24.5%	21.7%	22.7%
Panama	12.1%	10.5%	10.7%
Paraguay	16.7%	14.6%	15.5%
Peru	18.2%	16.3%	16.9%
Philippines	19.7%	17.7%	19.2%
Poland	9.3%	8.0%	5.8%
Portugal	12.8%	10.7%	8.3%
Puerto Rico	7.5%	6.4%	6.0%
Qatar	13.7%	11.8%	10.7%

Country/region	January 2017	February 2017	March 2017
Réunion	9.6%	8.1%	7.9%
Romania	18.0%	14.7%	12.3%
Russia	17.2%	15.1%	12.0%
Saudi Arabia	17.1%	15.1%	15.0%
Senegal	21.1%	17.9%	20.3%
Serbia	18.1%	14.4%	14.3%
Singapore	7.9%	7.2%	5.3%
Slovakia	9.6%	8.0%	7.6%
Slovenia	13.2%	10.4%	9.2%
South Africa	10.7%	9.3%	8.9%
Spain	12.9%	11.4%	8.0%
Sri Lanka	19.5%	17.2%	17.5%
Sweden	4.7%	4.0%	1.8%
Switzerland	4.9%	4.0%	2.2%
Taiwan	11.6%	10.8%	9.6%
Tanzania	23.5%	19.6%	22.2%
Thailand	22.9%	19.7%	18.0%
Trinidad and Tobago	12.1%	9.9%	9.4%
Tunisia	21.0%	18.0%	19.5%
Turkey	17.0%	13.8%	14.1%
Ukraine	25.0%	21.6%	18.1%
United Arab Emirates	14.2%	12.4%	10.2%
United Kingdom	4.6%	4.3%	2.5%
United States	4.7%	4.0%	2.4%
Uruguay	12.2%	11.1%	10.7%
Venezuela	21.4%	18.1%	19.5%
Vietnam	24.8%	23.5%	21.2%
Worldwide	*10.3%*	*9.1%*	*7.8%*

Glossary

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.

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

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

Bitcoin
A form of digital currency. Bitcoins can be used to buy things online or exchange them for real money.

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

credentials
See *account credentials*.

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.

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.

dropper
See *downloader/dropper*.

elevation of privilege (EOP)
The act of exploiting a vulnerability to gain greater privileges on a compromised computer, usually in preparation for remote code execution (RCE). A vulnerability that allows this action is called an elevation of privilege vulnerability.

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.

EOP
See *elevation of privilege (EOP)*.

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.

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

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.

malicious software
Programs that perform malicious actions on a computer, such as stealing banking details, locking a computer until the user pays a ransom, or using the computer to send spam. Malicious software is a type of malware. Also see *unwanted software*.

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
The general name for programs that perform unwanted actions on a computer, such as stealing personal information. Microsoft classifies malware as either malicious software or unwanted software.

malware impression
A single instance of a user attempting to visit a page known to host malware and being blocked by Windows Defender SmartScreen in Microsoft Edge or Internet Explorer. Also see *phishing impression*.

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 and being blocked by Windows Defender SmartScreen in Microsoft Edge or Internet Explorer. Also see *malware impression*.

potentially unwanted application (PUA)

A program that doesn't meet the criteria to be considered unwanted software, but still exhibits behaviors that may be considered undesirable, particularly in enterprise environments.

PUA

See *potentially unwanted application (PUA)*.

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.

RCE

See *remote code execution (RCE)*.

remote code execution (RCE)

The act of exploiting a vulnerability to execute arbitrary code on a remote computer. A vulnerability that allows this action is called a remote code execution vulnerability.

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*.

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.

unwanted software
A program with potentially unwanted functionality that may affect the user’s privacy, security, or computing experience. Unwanted software is a type of malware. Also see *malicious software*.

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.

zero-day exploit
An exploit that targets a zero-day vulnerability.

zero-day vulnerability
A vulnerability in a software product for which the vendor has not yet published a security update.

Threat families referenced in this report

The definitions for the threat families referenced in this report are adapted from the Windows Defender Security Intelligence encyclopedia (microsoft.com/wdsi/threats), which contains detailed information about a large number of malicious software and unwanted software families. See the encyclopedia for more in-depth information and guidance for the families listed here and throughout the report.

Win32/Adposhel. Adware that can show extra ads inside and outside the web browser.

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/Cerber. A ransomware-as-a-service family that encrypts files on the computer and demands payment in Bitcoins for the decryption key.

Win32/Chuckenit. A threat that unchecks checkboxes in installation dialogue boxes without the user's knowledge.

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/Copali. A family of worms that can download other malware, including Win32/Zbot. They spread through infected network and removable drives.

Win32/Diplugem. A browser modifier that installs browser add-ons without obtaining the user's consent. The add-ons show extra advertisements as the user browses the web, and can inject additional ads into web search results pages.

Win32/Floxif. A family of viruses that infect Windows executable and DLL files to download and install other malware onto the computer.

Win32/Foxiebro. A browser modifier that can inject ads to search results pages, modify web pages to insert ads, and open ads in new tabs.

Win32/Fuery. A cloud-based detection for files that have been automatically identified as malicious by the cloud-based protection feature of Windows Defender.

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

Win32/Genasom. A generic detection for a variety of ransomware families that share certain characteristics.

Win32/Ghokswa. A trojan that installs modified versions of web browsers with different search and home page settings that the user may be unable to change. It may also install additional unwanted software.

Win32/Grenam. A multi-component family that includes a trojan component that runs at startup, a worm component that spreads via removable drives, and a virus component that renames executables.

Win32/ICLoader. A software bundler distributed from software crack sites, which installs unwanted software alongside the desired program. It sometimes installs other unwanted software, such as Win32/Neobar.

Win32/Ippedo. A worm that can send sensitive information to a malicious hacker. It spreads through removable drives, such as USB flash drives.

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.

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.

Win32/Locky. Ransomware that encrypts files on the computer, and directs the user to a Tor webpage to pay for the decryption key. It often arrives via spam as an infected Microsoft Word .doc file.

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

Win32/Mupad. A threat that can modify browser and proxy settings, which can result in lower browser security. It may be downloaded from torrent sites.

JS/Nemucod. A family of .zip attachments that try to install other malware when opened.

Win32/Neobar. A browser modifier that can change web browser settings without adequate consent. It is often installed by software bundlers, and has used the names Best YouTube Downloader, Torrent Search, BonusBerry, and several others.

Win32/Neshta. A virus that infects files by prepending its code to Windows executables.

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/Pokki. 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/Sasquor. A browser modifier that modifies search and home page settings, and installs services and scheduled tasks to prevent the user from changing them back. It can also download additional malware, including Win32/SupTab and Win32/Xadupi.

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

Win32/Spora. Ransomware that encrypts files with several popular extensions, including .doc, .docx, .jpg, .pdf, .xls, .xlsx, and .zip. It avoids encrypting files in the Games, Program Files (x86), Program Files, and Windows folders.

Win32/Spursint. A cloud-based detection for files that have been automatically identified as malicious by the cloud-based protection feature of Windows Defender.

Win32/SupTab. A browser modifier that installs itself and changes the browser's default search provider, without obtaining the user's consent for either action.

Win32/Tupym. A worm that copies itself to the system folder of the affected computer, and attempts to contact remote hosts.

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/Vigorf. A generic detection for a variety of threats.

Win32/Xadupi. A trojan that poses as a useful application, usually called WinZipper or QKSee, but can silently download and install other malware. It is often installed silently by the browser modifiers Win32/Sasquor and Win32/SupTab.

Index

Microsoft

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