Microsoft Security Intelligence Report

Volume 17 | January through June, 2014

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.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Authors

Dennis Batchelder
Microsoft Malware Protection Center

Joe Blackbird
Microsoft Malware Protection Center

Paul Henry
Wadeware LLC

Sriram Iyer
Application and Services Group

Jeff Jones
Microsoft Trustworthy Computing

Aneesh Kulkarni
Windows Services Safety Platform

Marc Lauricella
Microsoft Trustworthy Computing

Nam Ng
Microsoft Trustworthy Computing

Niall O'Sullivan
Microsoft Digital Crimes Unit

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Anthony Penta
Windows Services Safety Platform

Simon Pope
Microsoft Trustworthy Computing

Ina Ragragio
Microsoft Malware Protection Center

Tim Rains
Microsoft Trustworthy Computing

Jerome Stewart
Microsoft Digital Crimes Unit

Holly Stewart
Microsoft Malware Protection Center

Todd Thompson
Microsoft IT Information Security and Risk Management

Terry Zink
Exchange Online Protection

Geoff McDonald
Microsoft Malware Protection Center

Contributors

Tanmay Ganacharya
Microsoft Malware Protection Center

Roger Grimes
Microsoft IT

Chris Hale
Microsoft Trustworthy Computing

Satomi Hayakawa
CSS Japan Security Response Team

Ben Hope
Microsoft Malware Protection Center

Yurika Kakiuchi
CSS Japan Security Response Team

Sean Krulewitch
Application and Services Group

Jenn LeMond
Microsoft IT

Geoff McDonald
Microsoft Malware Protection Center

Scott Molenkamp
Microsoft Malware Protection Center

Dolcita Montemayor
Microsoft Malware Protection Center

Daric Morton
Microsoft Services

Takumi Onodera
Microsoft Premier Field Engineering, Japan

Laura A. Robinson
Microsoft IT

Norie Tamura
CSS Japan Security Response Team

Steve Wacker
Wadeware LLC

Iaan Wiltshire
Microsoft Malware Protection Center

Table of contents

Mitigating risk 109

Appendixes 123

About this report

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

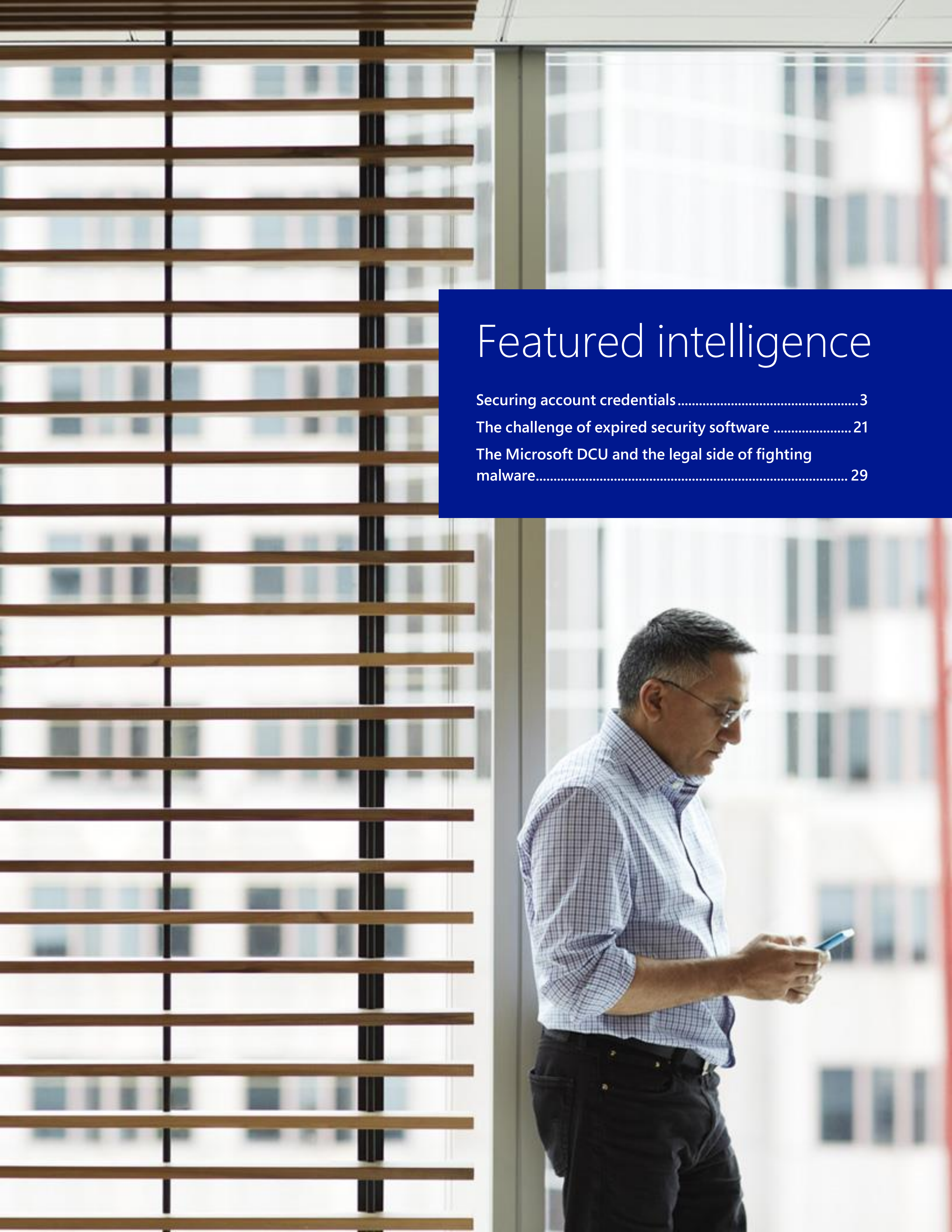
Reporting period

This volume of the *Microsoft Security Intelligence Report* focuses on the first and second quarters of 2014, 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, 1H14 represents the first half of 2014 (January 1 through June 30), and 4Q13 represents the fourth quarter of 2013 (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 125. 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 family or variant that is detected by the Microsoft Malware Protection Engine.



Featured intelligence

Securing account credentials

Computer users interact with a multitude of online services, and many of these services require them to enter their account credentials as a way to authenticate themselves to the service. Account compromise occurs when an unauthorized person knows the credentials for a user's account.

In one scenario that has unfortunately become all too common, account credentials are stolen in bulk by criminals through website breaches. Credentials can also be unwittingly provided directly by the victims themselves through phishing attacks, or harvested from systems that are infected with malware. Additional service protections such as multifactor authentication reduce the risk of account compromise, but the increased sophistication of attacks require continued vigilance.

Account compromise primer

This section is intended as a guide to the challenges that relate to securing account credentials and protecting them from compromise.

Online services and account credentials

Online services provide social networking, email, communications, news, image, video, forums, productivity, shopping, banking, storage, and access to many other types of websites and services. Whether for content personalization or for access to private data, users are typically required to enter their account credentials as a way to authenticate themselves to their services.

The most typical scenario is for users to present their credentials to an online service in the form of an *account name* and *password* pair that they enter into a login form. The account name on its own does not provide access to the account and therefore is not technically considered to be secret. By contrast, the password *is* a secret that is supposed to be known *only* to the legitimate account owner. It is the combination of both components that authenticates users to the online service.

This mechanism is intended to restrict access only to legitimate users that know both their account name and the password for the service, and will deny all incorrect password attempts on the assumption that the password secret is known only to the account owner.

Account compromise, takeover, and data theft

Account compromise occurs when an unauthorized person knows the credentials for that account. A compromised account is like a safe that is secured by a combination lock, for which an unauthorized person—such as a criminal—knows the combination. Compromise does not mean that someone else has necessarily opened the safe, only that they have the *means* to do so whenever they choose. And unlike a safe, an account's online service is usually publicly accessible on the open Internet. Even when there is no evidence that an unauthorized person has accessed the account, it is still treated as compromised, because unauthorized access may have occurred without being detected.

> Compromise does not mean someone has opened the safe, only that they have the *means* to do so when they choose.

An unauthorized person may have accessed a compromised account without the knowledge of the account's legitimate owner. The account owner may continue to have access to their account at the same time that the unauthorized person is also using the account (the account is *co-owned*) or may be completely locked out by the unauthorized person (the account is *taken over* or *hijacked*). In either case, information could have been taken from the account—that is, copied without the owner's permission—and the account itself could be misused for a variety of purposes, such as sending junk email (also known as spam) or distributing malware (malicious software).

Unfortunately, the phenomenon of account compromise and account takeover is relatively common for both consumers and enterprises. For enterprises, the number of data thefts is steadily increasing, year after year, according to Verizon's 2014 Data Breach Investigations Report.[1] Like those who target online consumers, financially motivated criminals who attack organizations are looking for bank information, payment instruments, and other data that they can quickly convert to cash. But unlike online consumers, organizations also contain assets

[1] Verizon, "2014 Data Breach Investigations Report." Verizon, 2014.

such as corporate data and trade secrets, which makes them far more valuable targets for espionage.

In almost all cases, account credentials are also a theft target for criminals because of their utility in gaining direct access to accounts and committing additional crimes. According to Verizon, in 2013, using stolen credentials became the number one method by which criminals gained entry to corporate resources and stole sensitive data.

The trade in stolen account credentials

Account credentials that are stolen in bulk directly from organizations' websites contribute a significant amount to the trade in stolen credentials. As part of its customer account protection operations during the period from November 2013 to June 2014, Microsoft tracked about 1700 distinct website credential thefts—comprising a little more than 2.3 million credentials—that were posted in public places on the Internet. This number represents only a small fraction of the credentials that are traded in forums and specialized websites on less publicly accessible spaces on the Internet that cater to the illicit trade in stolen credentials.

Figure 1. Number of publicly posted website credential thefts, per month, from November 2013 to June 2014

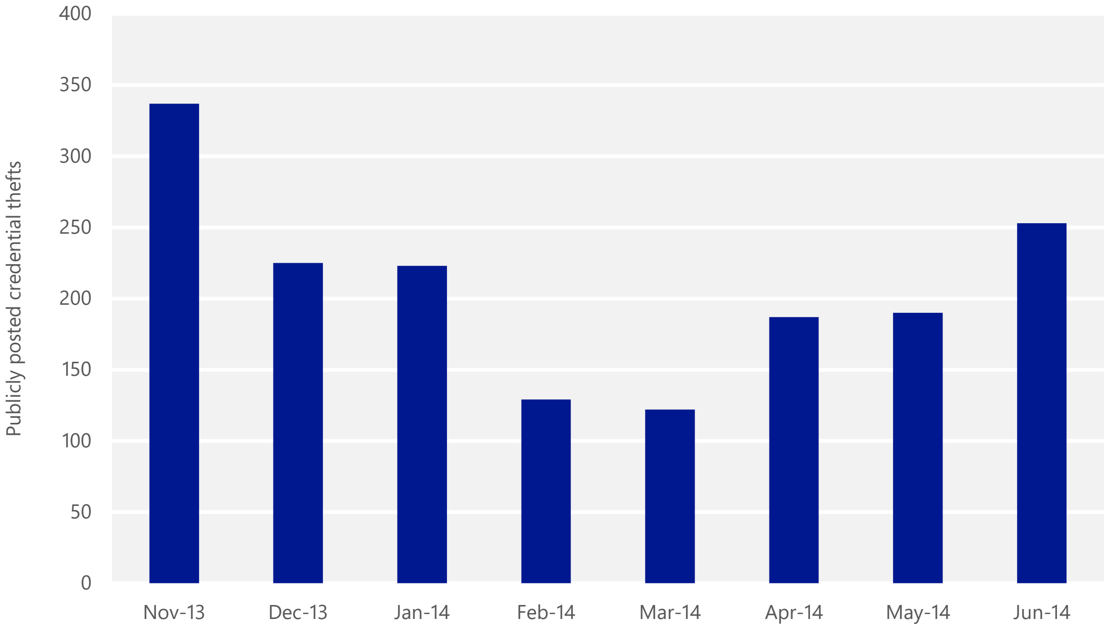
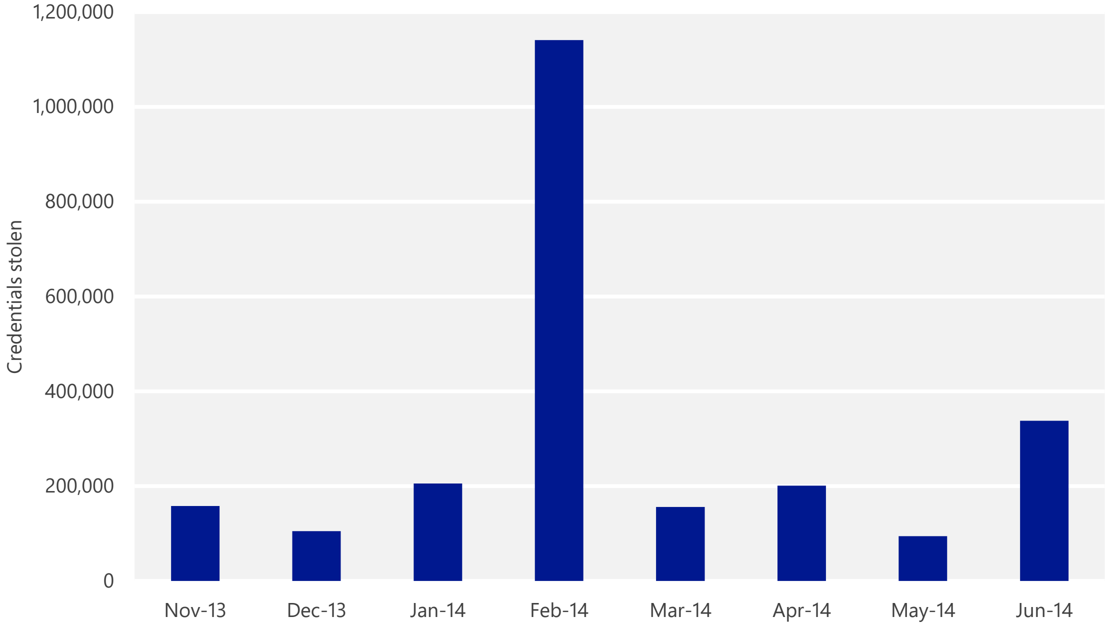


Figure 2. Number of stolen credentials from publicly-posted credential thefts, per month, from November 2013 to June 2014. The spike in February represents includes the public posting of 1 million hashed credentials that had been stolen from Forbes.[2]



Only a small fraction of website credential thefts received coverage in the press. Of these, there were several very large, publicly reported incidents that are worth recounting because they illustrate the serious nature of credential theft.

In October 2013, tens of millions of stolen credentials, including 2.9 million of then-current Adobe customers, had surfaced on the internet as a result of a successful attack against Adobe Systems.[3] In November, reportedly 42 million stolen customer account credentials from Cupid Media were discovered on the Internet, including those of 254,000 Australian users.[4] May of 2014 saw eBay breached, with a large part of 145 million users account credentials thought to

[2] A. Greenberg, "How The Syrian Electronic Army Hacked Us: A Detailed Timeline," Forbes.com, 20.Feb.2014. [Online]. http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/. [Accessed: 17-Jul-2014].

[3] B. Arkin, "Important Customer Security Announcement," *Adobe*, 3-Oct-2013. [Online]. Available: http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html [Accessed: 04-Aug-2014].

[4] L. Daniels, "Privacy breach: 254,000 Australian online dating profiles hacked," *Office of the Australian Information Commissioner*, 25-Jun-2014. [Online]. Available: http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-breach-245-000-australian-online-dating-profiles-hacked/. [Accessed: 17-Jul-2014].

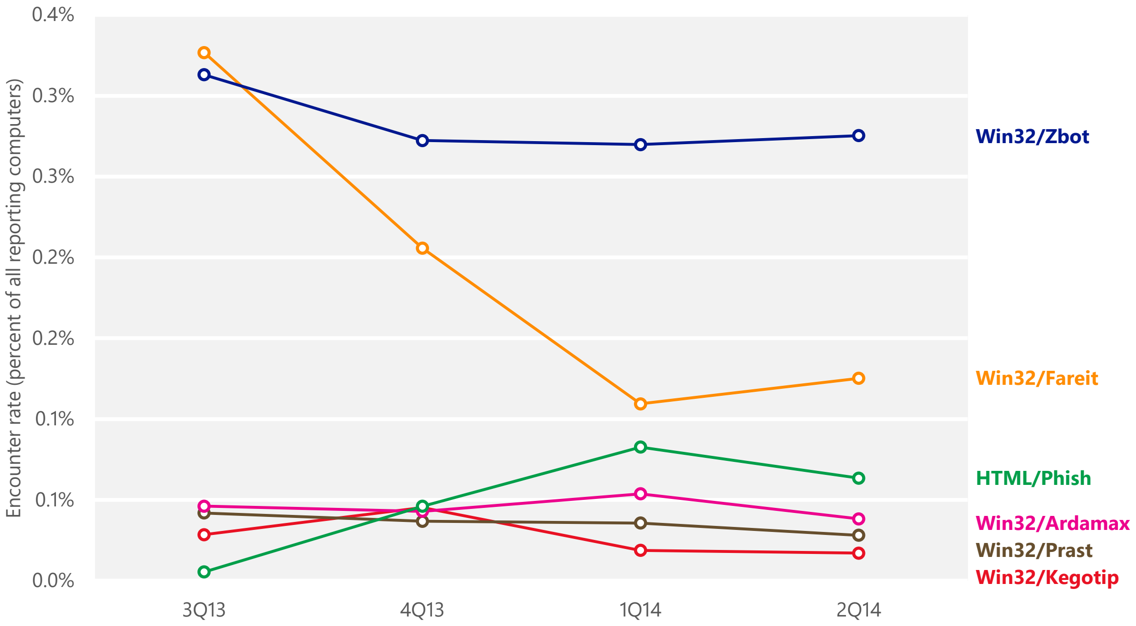
have been stolen by thieves,[5] according to eBay spokeswoman Amanda Miller. Miller said the thieves initially obtained access to eBay's corporate network after obtaining the login credentials for "a small number" of employees.

Estimating the size of the stolen credentials trade is difficult, because it appears that much of what is being traded is typically only the *secondary* market for stolen credentials. Large credential thefts—which consist of millions of credentials—sometimes do not enter the secondary market for general trade until the compromised accounts have been sufficiently exploited by the criminals who stole the credentials. This exploitation can be a period of many months, depending on the size of the credential theft and its direct, exploitable value to those who stole the data.

> Only a small fraction of website credential thefts receive coverage in the press.

In addition to attacks on websites, a substantial number of the illicit account credentials trade is unwittingly provided directly by victims themselves as a result of either phishing or devices infected with malware.

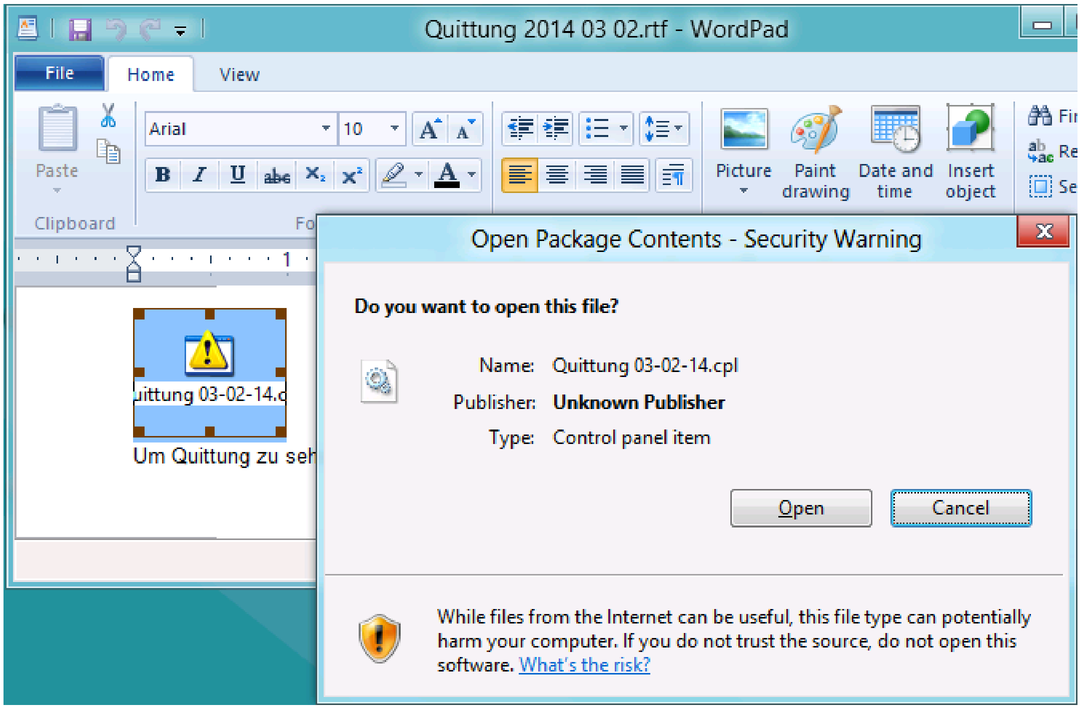
Figure 3. Trends for the most commonly encountered password stealers in 1H14



[5] A. Miller, "eBay Inc. To Ask eBay Users To Change Passwords," *ebay inc*, 21-May-2014. [Online]. Available: http://investor.ebayinc.com/releasedetail.cfm?releaseid=849396 . [Accessed: 17-Jul-2014].

Malware, short for *malicious software*, is the general name for programs that perform unwanted actions on a computer. Malware can contain keystroke logger functionality or other similar capabilities that record account credentials as they are entered, and then upload them to sites on the Internet where criminals retrieve the captured information. In some cases malware can be installed without knowledge on a victim's computer when they visit a malicious website that exploits an unpatched vulnerability in the user's browser, operating system, or applications; in other cases victims can be tricked into voluntarily installing a seemingly innocuous program that contains malware—and when the program is installed, the malware is installed with it.[6]

Figure 4. A malicious embedded file emailed to a prospective victim as part of a targeted attack



Open Package Contents - Security Warning

Do you want to open this file?

Name: Quittung 03-02-14.cpl

Publisher: **Unknown Publisher**

Type: Control panel item

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

In a typical phishing attack, an attacker sends a specially crafted email message that typically appears to be from one of the many online services that a potential victim might use, but the message lures the victim to click on a link that will take them to a webpage that is used to inject malware into their device. Another type of phishing scam simply tricks the victim into entering their credentials into what

[6] See the entry "A close look at a targeted attack delivery" (February 27, 2014) on the MMPC blog at blogs.technet.com/mmpc for an example of how attackers use social engineering to distribute malware.

appears to be a standard login screen for a particular service; when they do so, their account credentials are stolen. Website credential theft also provides attackers with useful sets of email addresses with which to conduct phishing attacks. Even when only account names are stolen, an attacker can simply craft an email to make it appear to be from the site, send the email to every user of the site, and ask them to click a link in the email to verify or change their password. When users click the link, they are sent to the attacker's website—which has been crafted to resemble that of the real site—and unsuspecting victims then enter their credentials, which are captured by the attacker. Alternatively, the user might be directed to a legitimate site that is itself compromised, with the same result—the user's credentials are compromised. (See "Phishing sites" on page 97 for more information about this technique.)

Better protection through multifactor authentication

One of the ways that services have attempted to mitigate stolen account credentials is to offer multifactor authentication to their users.[7] Typically, a user presents *something they know*—their secret password—as proof of authenticity. The basic idea behind multifactor authentication is for the user to present one or more additional proofs based on *something they have*—a device, for example—or *something they are*, such as a fingerprint or retinal scan. *Two-factor authentication* simply uses one of these additional proofs in addition to the user's password.

The most common form of two-factor authentication used by online services uses the *Short Message Service* (SMS) to send a unique message to a user to have them prove that they are in possession of a specific device. The online service sends a code via SMS to a mobile phone that is known to belong to the user after they correctly enter their account name and password. The user then reads the code sent via SMS and enters it into the login page as the final authentication step.

Another popular form of two-factor authentication is to use a one-time code generator (in the form of a security token on a key fob or wallet card, or as a smartphone app) that is registered with the online service. Every thirty seconds or so a new code is generated that follows a particular pattern that is unique to

[7] http://en.wikipedia.org/wiki/Multi-factor_authentication

the code generator. This approach allows the service to authenticate that the user possesses the code generator, because only that particular generator could have generated *that* particular sequence of numbers at the time of login. These methods of additional authentication have been widely used in the banking industry to provide additional security for accounts and high-value transactions, and are now offered across a broad range of online services, including email, communication, and data storage services.

In response, hackers now use a number of tailored attacks to compromise smartphones and other computers, which blunts the effectiveness of these additional protections. These attacks include compromising the code generator devices[8] and hijacking the SMS on user's smartphones to redirect one-time codes.[9] Even with these techniques, criminals still need to know the account name and password to attack an online service account unless they use man-in-the-middle attacks.[10] Although multifactor authentication is not a panacea for account compromise, it does create significant technical and operational barriers that increase costs for the attacker and reduce the risks from stolen credentials.

Plaintext, hashed, and encrypted credentials

With an increasing number of websites and online services having their credential data being stolen, it is perhaps surprising that so many of these websites store their password data in *plaintext*—that is, in a form that can be read simply by opening the file. Credentials that are stored in plaintext offer no protection if the credentials are stolen; encryption offers some protection but suffers from the risk that the cryptographic key may also be breached. One-way cryptographic hashing offers the most protection, provided that salting is used (explained in the following paragraph) along with a sufficiently computationally expensive algorithm. By way of example, the reported 42 million account

[8] Anon., "Frequently asked questions about RSA SecurID: Information for RSA Customers," *EMC.com*, Jun-2011. [Online]. Available: http://www.emc.com/collateral/guide/11455-customer-faq.pdf. [Accessed: 2-Nov-2014].
[9] C. Mulliner, R. Borgaonkar, P. Stewin, and J.-P. Seifert, "SMS-based one-time passwords: attacks and defense," in Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2013, pp. 150–159. Available: http://www.mulliner.org/collin/academic/publications/mulliner_dimva2013.pdf
[10] "Man-in-the-Middle Attack," *Wikipedia*. [Online]. Available: http://en.wikipedia.org/wiki/Man-in-the-middle_attack. [Accessed: 17-Jul-2014].

credentials stolen from Cupid Media were all in plaintext[11]—simply opening the file was sufficient to read the passwords.[12] The millions of account credentials stolen from Adobe Systems were encrypted using the 3DES (also known as triple-DES) encryption algorithm. Only if the key were stolen would decrypting passwords be easy to achieve. So long as the key remains secure, it will be difficult to decrypt the bulk of the stolen passwords. Even so, password security experts were still able to deduce the top 100 passwords in the Adobe credentials list without knowledge of the cryptographic key—the set of 100 passwords were used by nearly 6 million users. For this reason, encryption of unhashed passwords should be treated as little better than storing passwords in plaintext.

It is generally agreed that the minimally acceptable level of security in storing account passwords calls for them to be *salted* and *hashed*. Cryptographic hashing protects the password by encoding it in such a way that it is practically impossible to invert—that is, to recreate the password from its hashed value. Without salting, the same password will always hash to the same value (for the same hash algorithm), which makes it possible to compare the hashes of known passwords with the hashes of stolen credentials and thereby know the original password for any matches. Salting takes a sequence of random characters that are added to the password when computing its hash, and in doing so guarantees that the same passwords will never hash to the same value, providing their salt values are different. The salt values themselves are never protected and must be known for hashing to work correctly.

> The minimally acceptable level of security in storing account passwords calls for them to be salted and hashed.

Cryptographic hashing is different from symmetric, or single-key, encryption. Passwords that are symmetrically encrypted are protected in a way that allows the password to be decrypted—and therefore read—by anyone who has the key (a sequence of characters) that was used to encrypt the password. It functions similarly to a locked box; anyone with a physical key can access the contents of the box, and so too anyone can recover the original

[11] "Cupid Media Pty Ltd: Own motion investigation report," *Office of the Australian Information Commissioner*, 26-Jun-2014. [Online]. Available: http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/cupid-omi. [Accessed: 17-Jul-2014].

[12] D. Florencio, C. Herley, and P. van Oorschot, "An Administrator's Guide to Internet Password Research," in *Proceedings of USENIX LISA'14*, Nov. 9-14, 2014. Available: http://research.microsoft.com/pubs/227130/WhatsaSysadminToDo.pdf

password if they have the cryptographic key that was used to encrypt the password. The danger with encrypting passwords is that the cryptographic key must be available to decrypt (or encrypt) passwords for the purposes of determining whether a user's password is valid. Therefore, if the key is stolen along with the account credentials, the credentials are effectively unprotected.

The problem of weak passwords and endemic reuse

What makes stolen account credentials so valuable to cybercriminals is the extent to which users reuse their account names and passwords across different sites and services. Compromising a single account name and password can potentially leave the victim vulnerable across many other sites and services that they use. The more stolen credentials that a criminal obtains, the more likely it is that at least a significant fraction of these credentials will match those used by the same users at a *different* service. For example, because of the tendency of many users to reuse their account credentials across a number of different services to make them easier to remember, a large credential theft involving one major service could likely yield a set of stolen credentials with a significant match rate against those of other various popular online services.

In 2007, a study of user password habits[13] published by Microsoft Research concluded that the average user accessed 25 sites, and had around seven passwords in total that were reused across three sites on average. In the seven years since, the number of sites that a single password will be reused across has likely grown substantially, for two reasons: the overall increase in the number of services an average user now accesses, and the limitations of human memory. CSID is a provider of global identity protection and fraud detection technologies; the results of a CSID 2012 survey of consumer password habits[14] are consistent with the earlier findings. More than half of the respondents (61 percent) admitted to reusing the same password across multiple websites; just over half (54 percent) have five or fewer passwords. Interestingly, the survey revealed that the average consumer types only four or five different passwords a

[13] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*, 2007, pp. 657–666.
[14] "Consumer Password Habits Unveiled," *CSID*, 25-Sep-2012. [Online]. Available: http://www.csid.com/resources/white-papers/white-paper-mitigating-the-risk-of-poor-password-practices/. [Accessed: 29-Jun-2014].

day. The findings from both studies are consistent with the principle that people adopt strategies and shortcuts that will reduce their cognitive load.

Reusing passwords across online services is an easy way for people to reduce cognitive load, but it's not safe practice. It is impractical to remember 25 unique passwords and remember which password is for what service. The cognitive limitations of short-term memory also impose severe restrictions on our ability to form long-term memories—if we cannot successfully form short-term memories, our ability to convert those to long-term memories is severely impaired. In an effort to cope with these limitations, most users do two things to reduce cognitive load: they reuse the same password across a number of different services, and they choose memorable passwords for each service—often choosing passwords that can be easily attacked using offline attacks against the hashed passwords obtained from website credential thefts. A better approach to the management of difficult-to-remember, unique passwords is to use a secure credential store to manage online service and website passwords. Many mobile devices come with these features built-in, and securely replicate the account credentials between devices owned by the user. There are also a range of third-party services and applications that offer similar capabilities.

> Reusing passwords across online services is an easy way for people to reduce cognitive load, but it's not safe practice.

The success of offline attacks against the hashed passwords from credential thefts is dependent on both the difficulty of the cryptographic hash algorithm used to create the hash as well as the inherent strength of the password that was chosen. A typical attack will take the most common tens of thousands of passwords and run them through the same cryptographic hash algorithm that was used to create the password hashes. When the hash of the tested password matches that of the stolen credential, then the hash has been "cracked"—the attacker has learned the password.

Typically, if a simple dictionary attack does not yield results, the software used by the attacker will use rules to generate guesses that correspond to the password creation habits of a large fraction of users. For example, such rules typically append numbers and symbols to dictionary words, and mix capitalization according to patterns observed for known passwords to create candidates for testing such as "MyFavorite67" or "Qbesancon321". These relatively simple rule-based dictionary attacks can be tremendously effective; according to a 2011 study of 6 million user-generated passwords,[15] 98.8 percent of users chose a password that was on the list of the most common 10,000 passwords and were therefore easily cracked using off-the shelf password hash-cracking software and commodity personal computer hardware.

Password hashes that are created using a computationally expensive hash algorithm are also more difficult for the attacker and result in a lower yield—they are unable to crack as many hashes in the same amount of time. The difference in computational difficulty between hash algorithms can be many orders of magnitude. As an example, attacks against one of the most popular—and older—algorithms, MD5, can cycle through more than eight billion password combinations per second. By contrast, attacks against cryptographically strong algorithms such as SHA-512 yield only around 2,000 combinations per second on the same hardware, which makes the cracking of SHA-512 four million times harder. Of course, if the user chooses a weak password such as one of the top 10,000 or so that is in an attacker's dictionary, even a cryptographically strong hash algorithm such as SHA-512 offers little protection.

> Users can substantially increase their level of protection by using two-factor authentication, if offered by their service provider.

Therefore, if a site chooses a weak hash algorithm to protect user passwords—something users usually have no knowledge of—even complex passwords may be subject to cracking by an attacker with the right computing resources and determination.

To be sufficiently protected, users need to choose complex, unique passwords and online services need to store passwords as salted hashes using a computationally expensive hash algorithm (such as the SHA-256 family of hash algorithms). Users can substantially increase their level of protection by using two-factor authentication, if offered by their service provider.

Responding to recovered credentials

From time to time, national and regional government law enforcement agencies will recover stolen credentials as part of their operations. This section is intended to guide these law enforcement agencies through the issues involved in

[15] M. Burnett, "10,000 Top Passwords," *Xato - Passwords & Security*, 20-Jun-2011. [Online]. Available: https://xato.net/passwords/more-top-worst-passwords/. [Accessed: 01-Jul-2014].

deciding how to respond to the recovery of stolen credentials; in addition, it offers a perspective for enterprise and IT professionals on how they can coordinate to protect their customers.

In general, an effective government response to the recovery of stolen account credentials will involve three major areas of activity:

- Coordinate the response with trustworthy service providers.
- Ask service providers to check recovered credentials.
- Notify affected citizens in a responsible way.

These areas of activity are described in the following subsections.

Coordinate with trustworthy service providers

Governments and service providers need to coordinate to protect users when stolen credentials are recovered:

- **Government agencies should establish policy and procedures for handling stolen account credentials and working with service providers to restore customer accounts.** Governments are increasingly finding or discovering large amounts of potentially compromised account credentials. Government agencies should establish policies and procedures for handling such data. These policies should be publicly available and be designed to protect sensitive data and restore consumer privacy and security as quickly as possible.
- **Authenticating recovered stolen credentials can only be performed by service providers**. Government agencies or third-party organizations should not attempt to directly authenticate stolen credentials by attempting to access consumer accounts. They should work directly with the service providers, who can help restore the security and privacy of the consumer account. Silent alarms may trip at a service provider when their systems register a large number of attempted logins for different accounts that originate from the same location. For this reason, attempts by government agencies to directly authenticate the credentials may be ineffective.
- **Governments should act to protect customers by working with service providers to ensure compromise data is rapidly coordinated.** Different providers have different rules for what constitutes a valid account name in their systems. Some will require an email address from a set of known

domains; others will accept almost any email address as a valid account name. To protect users properly, service providers will need access to the right sets of recovered account credentials. The data needs to include account passwords and any user metadata that was recovered with the credentials, so that service providers can effectively protect users' accounts, including notifying users of compromise.

- **Government agencies should establish criteria before sharing recovered stolen credentials**. Governments should ensure that account providers have established documented procedures and systems for handling and processing sensitive data related to consumer account comprises. Governments should require that service providers receiving data do not abuse the credentials—by reselling, or using for marketing purposes, for example—and that the recovered credential data will be securely destroyed after processing.

Stolen credentials recovered by law enforcement agencies need to be authenticated by service providers to verify that both the account names and passwords match.

- **Recovered stolen credentials should *always* be encrypted at-rest**. Stolen credentials have a value to criminals, and care must be taken to ensure that the data is inaccessible to those without a legitimate need for access. Recovered credential data files should be encrypted with high-grade ciphers, and preferably with an asymmetric cipher when preparing data for delivery to a service provider. The use of a strong public key (2048 bits or higher) and strong cipher (such as used in PGP) should be sufficient to guarantee that only the intended recipient is able to decipher the data.
- **Government agencies often want to use another nation's government law enforcement agency as an intermediary when passing data to service providers in different countries.** Although this approach is not problematic in itself, it does impose additional delays before service providers receive the credentials, which extends the time afforded to criminals to access compromised accounts and create harm for users. With stolen credentials, the sooner that accounts can be tested, the less harm will result for users. Compromised accounts can be used to victimize users within minutes to days of being harvested. With this factor in mind, government agencies should consider handing encrypted credentials directly to the appropriate service providers, rather than creating delays in processing as a result of

passing the data through various agencies of different national governments' agencies.

Ask service providers to check recovered credentials

Stolen credentials that are recovered by law enforcement agencies need to be authenticated by service providers to verify that both the account names and passwords match. This approach is especially important for large data sets of credentials. Accounts cannot be marked as compromised simply because account names in the recovered credentials list match those of an online service provider—the providers need to verify that passwords match as well.

- **In general, only a fraction of the recovered credentials will match those in use with a service provider**. This fraction will vary depending on when the account credential was stolen, how it was stolen (malware, phishing, breach, and so on), and whether the account for the online service was targeted or whether it was a theft of credentials from an unrelated website. For small sets of credentials, the fraction that will match can range from small to very large, but for very large sets of credentials, the matching fraction is typically small. For large numbers of recovered stolen credentials, match rates will vary from provider to provider, but a match rate of around five percent is typical for most large sets of credentials. The reason for relatively low match rates is that although people widely reuse their account names (typically a single email address) across websites, they reuse the same password across multiple websites less frequently.
- **For large sets of credentials, forcing every account to be marked as compromised entails considerable cost to both users and service providers.** For service providers, marking every account as compromised can mean that help desks become overwhelmed with support calls, resulting in user dissatisfaction and a possible loss of customers as users seek to find other, more reliable services. If accounts are forced unnecessarily into recovery, even those users who do not contact service help desks will experience fatigue over time and be more likely to believe that the Internet is not a safe place, or that their service provider is either unnecessarily creating work for them, or that their service provider is not safe. Unnecessarily forcing account recovery on users also runs the risk of permanently locking them out of their own accounts if their account recovery information is incomplete or out-of-date, which can drive users away from a service and, in the long term, contribute to a growing distrust of the Internet.

- **Without authentication of credentials, criminals can target online service providers or account holders** by distributing counterfeit sets of credentials—real account names with fake passwords—that would have similar undesirable results.

Notify affected citizens in a responsible way

It's important to notify affected citizens of possible compromise so that they can take steps to recover their account and change their password if they have reused it for multiple services across the Internet. Before notifying citizens, the following important considerations apply:

- If the compromised account is for an email service, sending an email to the compromised email address will likely be ineffective. When an email account is being co-owned, the criminal can simply delete the notification email, which leaves the user none the wiser. Sending an email to an email account marked as compromised also does nothing; the user has no ability to view the email because they must undertake the account recovery process to gain access. In general, email notifications are *only* useful if they are sent to a backup email or SMS associated with the account, which will provide at least a chance that the user will see it.
- **Notification emails can be an opportunity for criminals to phish users**. Criminals will use all opportunities provided to them. When someone other than the official service provider sends out email to users to inform them that their account may have been compromised, criminals will use the look and feel of such notifications to craft phishing emails with links that mimic the official email but redirect the user to a phishing or malware site[16] where their credentials can be harvested or their device can be infected by malware. In general, it is almost always safer to allow service providers to use their standard, established procedures for account compromise notification rather than send bulk notifications to users who may or may not have had their account compromised. Accounts that have been marked as compromised by the service provider will prompt users to go through

[16] Anonymous, "Tricky Phishing Scam Mimics Facebook's Official E-Mails," Facecrooks, 26-Nov-2011. [Online]. Available: http://facecrooks.com/Scam-Watch/tricky-phishing-scam-mimics-facebooks-official-e-mails.html/. [Accessed: 05-Aug-2014].

account recovery when they next log in through an interruptible interface, such as a web browser.

- **Take advantage of the service providers' standard operating procedures for account compromise notification.** In many cases, service providers have policies and procedures for account compromise notification that are designed to limit the opportunities for criminals to cause additional harm while ensuring that affected users are notified that their account is compromised. Service providers often require affected users to undertake a standard account recovery procedure to restore access to their account. As part of this procedure, users are often offered material to educate them about practices that will help protect their account from additional compromise. Governments should take advantage of these standard operating procedures that are already in place, rather than creating customized notification systems for account compromise that may be less effective, and that may offer opportunities for exploitation by criminals.

Conclusion

Account compromise stakeholders include service providers, their customers, and governments seeking to protect their citizenry. Each of these stakeholders have a role to play in preventing, detecting, and responding to account compromise.

> Account compromise stakeholders include service providers, their customers, and governments.

Users can protect themselves from account compromise by choosing difficult-to-guess passwords[17] (preferably random-generated) that are unique and not reused across their online accounts. The use of a secure credential store to manage online service and website passwords will help to reduce or eliminate the cognitive load involved in remembering account names and passwords. Many mobile devices come with these features built-in, and securely replicate the account credentials between devices owned by the user—and there are a range of third-party services and applications that offer similar capabilities. To further increase protection, users can opt-in to additional security features that are offered by the service

[17] "Outlook.com account help," *Microsoft Windows How-to*. [Online]. Available: http://windows.microsoft.com/en-us/outlook/help-protect-account/. [Accessed: 05-Aug-2014]

provider, including the use of two-factor authentication. The use of two-factor authentication creates significant technical and operational barriers for an attacker, and substantially reduces the risk of account compromise for users.

Service providers can limit the impact and reduce the likelihood of account compromise by salting and hashing user passwords using a computationally complex hash algorithm (such as the SHA-256 family of hash algorithms); by providing useful guidance and mechanisms that help users choose strong passwords[18]; and, by having procedures and policies that detail service provider response in the event of account compromise. Providers can further protect users by offering additional levels of security, including the provision of two-factor authentication.

Governments can help to reduce the impact of account compromise on their citizens by ensuring that they follow effective procedures for processing stolen account credentials that they recover during law enforcement and similar operations. These procedures should address the following actions:

- How to coordinate with trustworthy service providers to effectively protect their citizens.
- How recovered account credentials should be verified as being authentic and indicative of account compromise.
- Who should notify affected citizens in ways that are effective and don't create opportunities for exploitation by criminals or unduly undermine trust in the Internet.

[18] "Create strong passwords," *Microsoft Safety & Security Center*. [Online]. Available: https://www.microsoft.com/security/pc-security/password-checker.aspx. [Accessed: 05-Aug-2014]

The challenge of expired security software

A number of popular real-time security products are offered in "trial" versions, which provide signature updates for a limited period—typically three months—but require a paid subscription to receive updates after the trial period ends. Even after it stops receiving updates, an expired security program may continue to block and remove threats it is able to detect, which may create the impression that the software continues to provide an adequate, if reduced, level of protection. Unfortunately, this sense of security is largely illusory.

Malware authors constantly strive to avoid detection by security software, so security software vendors regularly update their detection signature databases to remain vigilant about current threats. When a typical security program stops receiving updates, therefore, it quickly loses its ability to detect the threats that attackers are currently actively using. As this section of the *Microsoft Security Intelligence Report* demonstrates, computers that are "protected" by expired, out-of-date security products fare little better in practice than computers with no real-time security software at all.

Recent releases of the Malicious Software Removal Tool (MSRT) collect and report details about the state of real-time antimalware software on computers whose administrators have chosen to opt in to provide data to Microsoft. In Windows 8 and Windows 8.1, these details include information about the state of the software's signature database, including whether the software reports an expired subscription. This telemetry data makes it possible to analyze how expired security software affects computers and to identify correlations between expired security software and malware infection.[19]

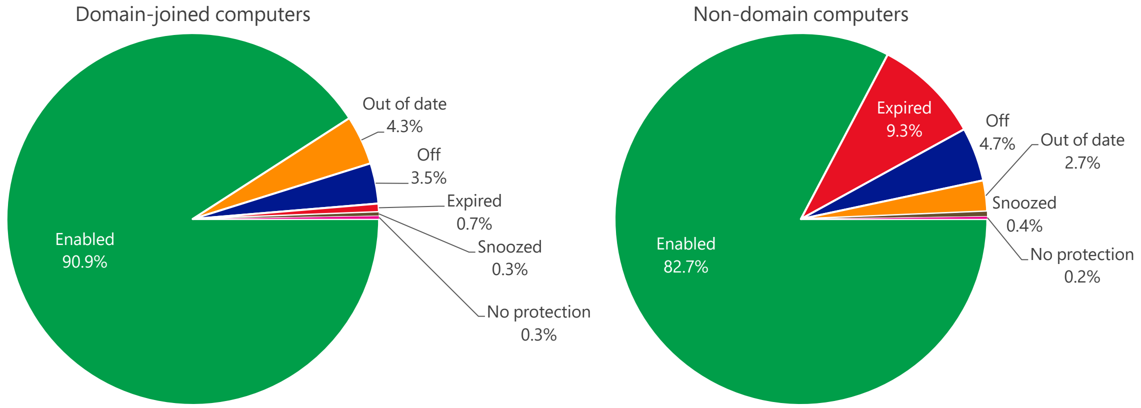
The Action Center API in Windows, which provides the security software telemetry to the MSRT, can report six possible states:

- Enabled. The detected security product is active and has the latest signature files available.
- Out of date. The detected security product is active, but the current set of signatures is outdated and new ones are available to download.
- Snoozed. The detected security product is active but is not performing real-time monitoring, typically because the product is upgrading itself. This state is usually temporary.
- Expired. The detected security product uses a paid subscription that has expired. This state usually indicates a compromised protection state (for example, the product probably no longer receives updated signature files and some features may be disabled).
- Off. The detected security product has been turned off. This state may be intentional, with the computer user or IT staff having disabled the software for some reason, or it may be caused by malware disabling the software.
- No protection. The MSRT did not detect any real-time security software on the computer.

The infection telemetry data produced by the MSRT includes information about whether the infected computer belongs to an Active Directory Domain Services (AD DS) domain. Because 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 two can help illustrate how protection status differs by environment. Figure 5 shows the protection status for computers that belonged to an Active Directory domain (left) and those that did not (right).

[19] See "Security software use" on page 89 for additional information about security software and infection rates, and see "Appendix B: Data sources" on page 127 for more information about the products and services that provided data for this report.

Figure 5. Antimalware protection state for domain-joined and non-domain computers running Windows 8 and Windows 8.1, 2H13–1H14

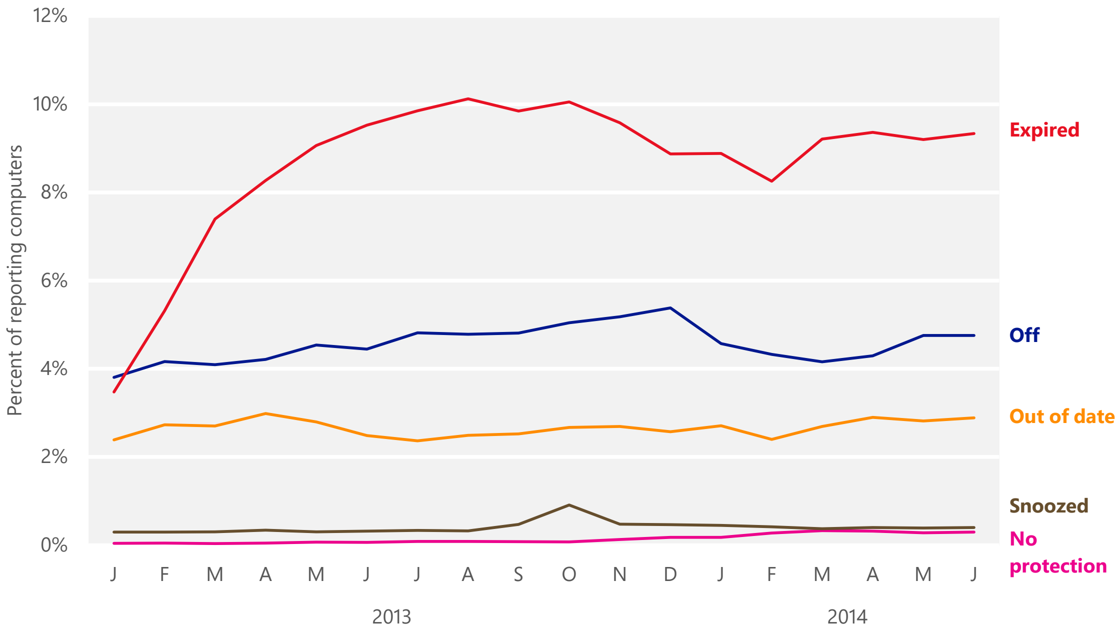


- As Figure 5 shows, expired subscriptions are almost entirely a consumer problem. Although expired subscriptions were detected on just 0.7 percent of domain-joined computers, they were detected on 9.3 percent of non-domain computers. Expired subscriptions constituted the single largest reason why non-domain computers were not adequately protected from malware.
- Overall, 90.9 percent of domain computers had real-time security software fully enabled, compared to 82.7 percent of non-domain computers. Expired subscriptions also accounted for almost the entire difference; percentages of the other possible statuses were generally similar between domain-joined and non-domain computers.

> Expired subscriptions are almost entirely a consumer problem.

For deeper insight into this problem, Figure 6 shows month-to-month statistics for non-domain computers that reported inadequate real-time protection between January 2013 and June 2014.

Figure 6. Trends for non-domain computers running Windows 8 and Windows 8.1 without up-to-date real-time security software enabled, January 2013–June 2014



- The percentage of computers reporting expired subscriptions started out relatively low in January 2013, which probably reflected a large volume of new computers purchased after the commercial release of Windows 8 in October 2012 that came with free trial subscriptions to security software pre-installed by computer manufacturers. This figure then increased gradually over the next several months as the trial subscriptions expired, reaching a peak of 10.1 percent in August 2013.

The reversal of the downward trend is likely caused by the expiration of trial subscriptions on new computers purchased during the 2013 holiday season.

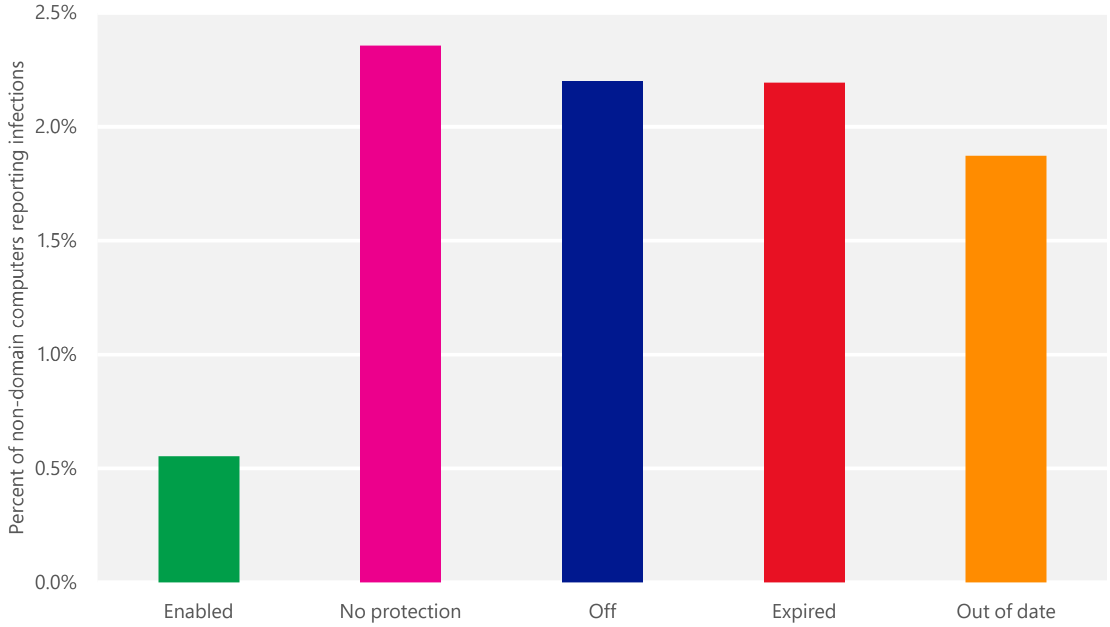
- The release of Windows 8.1 in October 2013 as a free update for Windows 8 customers is correlated with the start of a several-month-long downward trend in computers reporting expired subscriptions. When Windows 8.1 is installed on an existing Windows 8 computer, the Windows setup program determines whether the real-time security software on the computer is compatible with Windows 8.1. If it is not, Windows Defender is enabled as part of the setup process. This ensures that the computer receives adequate up-to-date protection from malware from a program that is compatible with the new version of the operating system.[20]

- The reversal of the downward trend in early 2014 is likely caused by the expiration of trial subscriptions on new computers purchased during the 2013 holiday season. Generally, security software that is pre-installed by computer manufacturers includes three-month trial subscriptions, which correlates closely with the observed increase in expired subscriptions beginning in March 2014.

How much protection does expired security software provide?

Computer users who run expired or out-of-date security software may believe that it continues to provide an adequate, if less than optimal, level of protection. As Figure 7 shows, this belief is misguided at best.

Figure 7. Infection rates for non-domain computers running Windows 8 and Windows 8.1 with and without adequate up-to-date real-time security software, 2H13–1H14



The MSRT removed malware from 0.6 percent of computers that reported having real-time security software that was enabled and up-to-date each month on average, compared to 2.4 percent of computers that reported no real-time

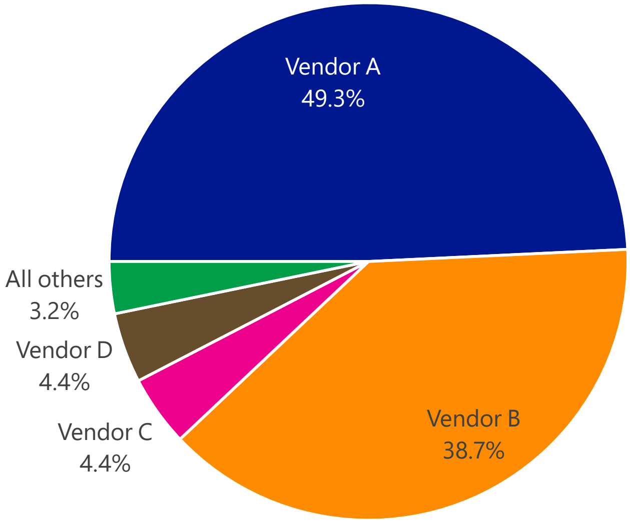
[20] Windows subsequently notifies the user that Windows Defender is enabled, and users may browse the Windows Store to acquire a different solution.

protection whatsoever and 2.2 percent of computers on which real-time protection was switched off. The rate for computers with expired protection was 2.2 percent—the same as computers with protection switched off, and nearly the same as computers with no protection at all. The figure for computers with out-of-date signature files was almost as high, at 1.9 percent. Overall, computers with expired security software were nearly 4 times as likely to be infected with malware as computers with enabled and up-to-date security software, and computers with out-of-date security software were about 3.4 times as likely to be infected.

What is the cause of this problem?

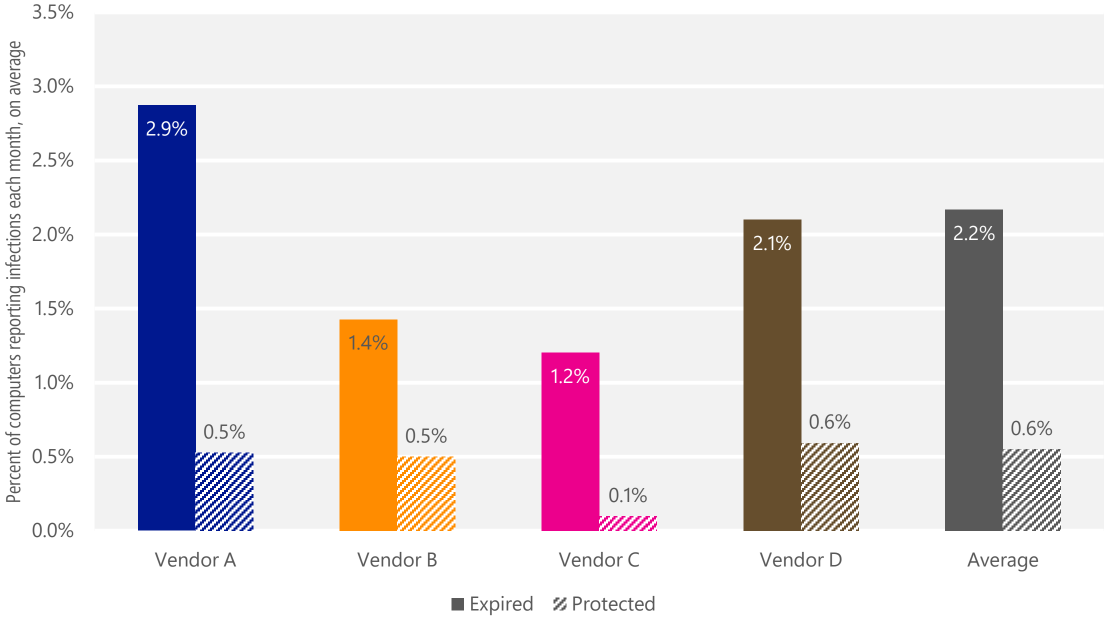
Although the Windows Action Center recognizes real-time security products from dozens of different vendors, expired trial versions are a problem for a much smaller number. As Figure 8 shows, just two vendors (vendors A and B) were responsible for 87.9 percent of expired trial versions, with two others (vendors C and D) accounting for most of the remainder.

Figure 8. Computers reporting expired security software, 2H13–1H14, by vendor



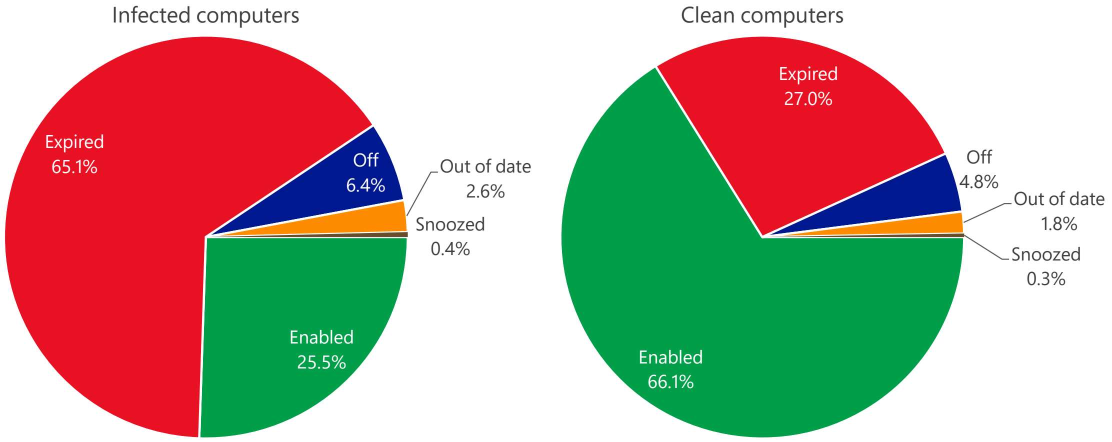
For these vendors, the existence of so many expired trial versions has a significant impact on their ability to offer protection, as Figure 9 shows. Computers with expired security software from Vendor A, in particular, were actually more likely to be infected than computers without any real-time security software at all (2.9 percent, compared to 2.4 percent of computers with no protection, as shown in Figure 7).

Figure 9. Infection statistics for real-time security products offered by the four vendors with the most expired installations in 1H14



Computer users who experience malware infections because of expired security software are likely to conclude that the protection offered by such products is largely illusory. An examination of infected and clean computers with security software from one such vendor, Vendor A, shows that expired security software misses far more infection attempts than it catches.

Figure 10. Protection status reported by infected computers (left) and clean computers (right) protected by Vendor A in 1H14



Guidance: Staying up-to-date with security software

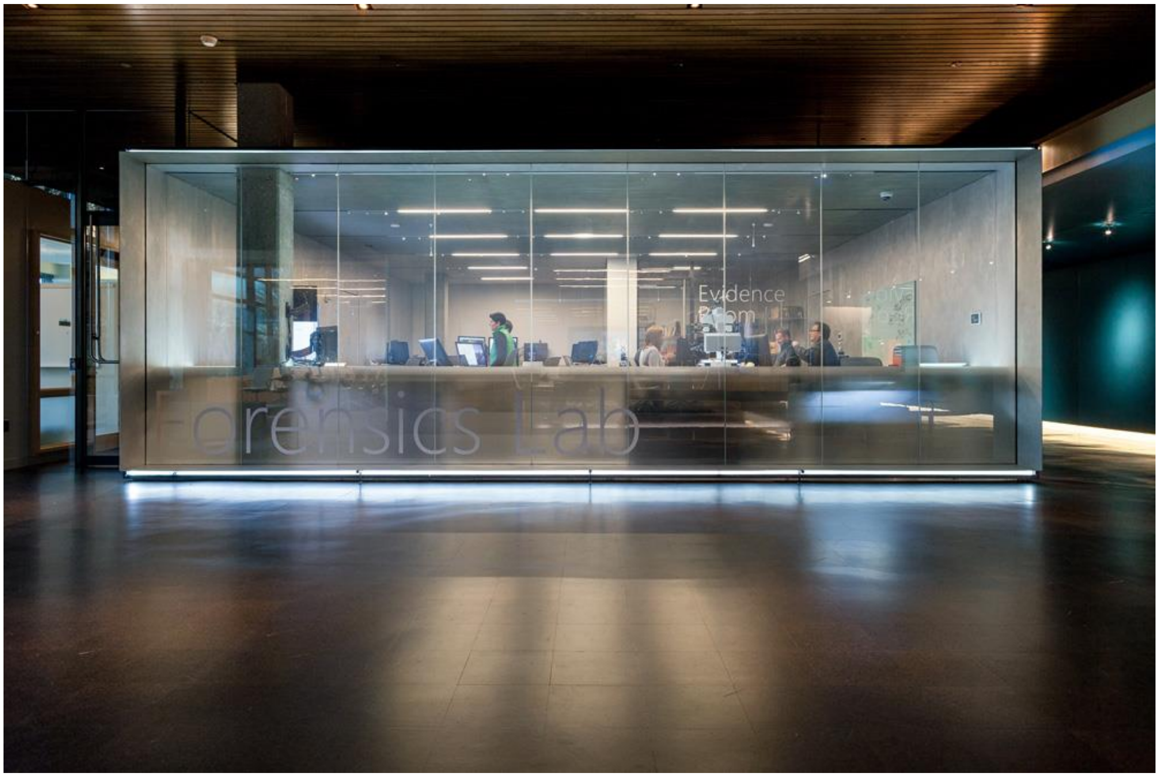
Computer users need to be aware that expired security software provides very little useful protection. Windows 8 and Windows 8.1 users can visit the Windows Store to find a wide range of antimalware solutions from reputable vendors for purchase or free download. Users of other Windows versions can visit windows.microsoft.com/en-US/windows/antivirus-partners for a list of vendors. Users can also download Microsoft Security Essentials (for Windows Vista and Windows 7) or enable Windows Defender (in Windows 8 and Windows 8.1) for no-cost, real-time malware protection from Microsoft.

The Microsoft DCU and the legal side of fighting malware

Microsoft Digital Crimes Unit

Microsoft is committed to fighting the battle against malware on all fronts. Groups such as the Microsoft Malware Protection Center (MMPC), the Microsoft Security Response Center (MSRC), and the Microsoft Security Engineering Center (MSEC) tackle the engineering side of computer security while the Microsoft Digital Crimes Unit (DCU) works on the legal side, partnering with law enforcement, government, and other organizations to fight malware using the combined power of Microsoft's platform and services, and the court of law.

Figure 11. The DCU Forensics Lab at the Microsoft campus in Redmond, Washington



The Microsoft Digital Crimes Unit (DCU) is an international team comprised of attorneys, investigators, forensic analysts, and business professionals based in 30 countries, working to transform the fight against digital crime. A part of Microsoft Legal and Corporate Affairs (LCA), the DCU strategy is to play offense against global criminal organizations that seek to profit from cybercrime. Partnering with commercial and private sector organizations and global law enforcement agencies, DCU seeks out out the criminals, and works to shut down or disrupt their operations.

DCU has three mission areas:

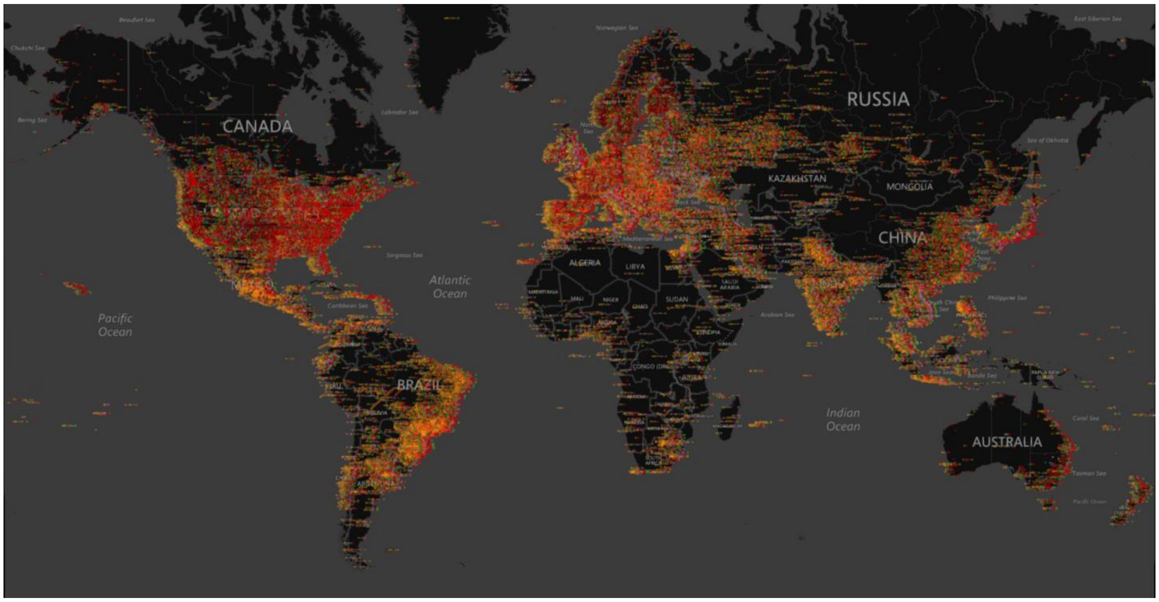
- Proactive malware disruption. DCU is uniquely positioned to take action against the perpetrators of cybercrime. DCU is able to react to malware crimes from a civil law perspective because malware written to run on Microsoft Windows infringes the Microsoft platform, which harms Microsoft customers and their customers. This perspective provides Microsoft with an offensive capability to go after botnets and other malware that no other company has—and DCU's results speak for themselves.
- Targeting intellectual property crimes. The intersection between counterfeit software and malware is of huge concern for Microsoft, as it should be a concern for all businesses, governments, and consumers. Microsoft partnered with IDC and the National University of Singapore in 2013 on a study that revealed that 30 percent of counterfeit software globally is pre-infected with malware.[21]
- Protecting vulnerable populations. DCU focuses on technology-facilitated crimes that target the most vulnerable populations, primarily children and the elderly. DCU investigates fraud and scams perpetrated against the elderly. In addition, we have licensed PhotoDNA, a proprietary image fingerprinting technology, for free to the International Center for Missing and Exploited Children (ICMEC) and the National Center for Missing and Exploited Children (NCMEC) to help identify cases of possible online exploitation of children. This technology is also licensed without charge to many of the top technology companies, and has become an industry standard.

[21] See the entry "New research forecasts the staggering cost of cybercrime" (March 18, 2014) on the Microsoft on the Issues blog (blogs.microsoft.com/on-the-issues) for more details about the study.

How DCU disrupts malware networks

Of the thousands of botnet families Microsoft is currently tracking, DCU has partnered to bring down or disrupt some of the worst. To date, this team has conducted 12 major operations targeting hundreds of botnet families. Often, these actions stop the harm. Sometimes, geographic boundaries, legal jurisdictions and/or ethical considerations limit DCU's actions to disruption of the criminal operations.

Figure 12. Locations of botnet-infected computers tracked by DCU



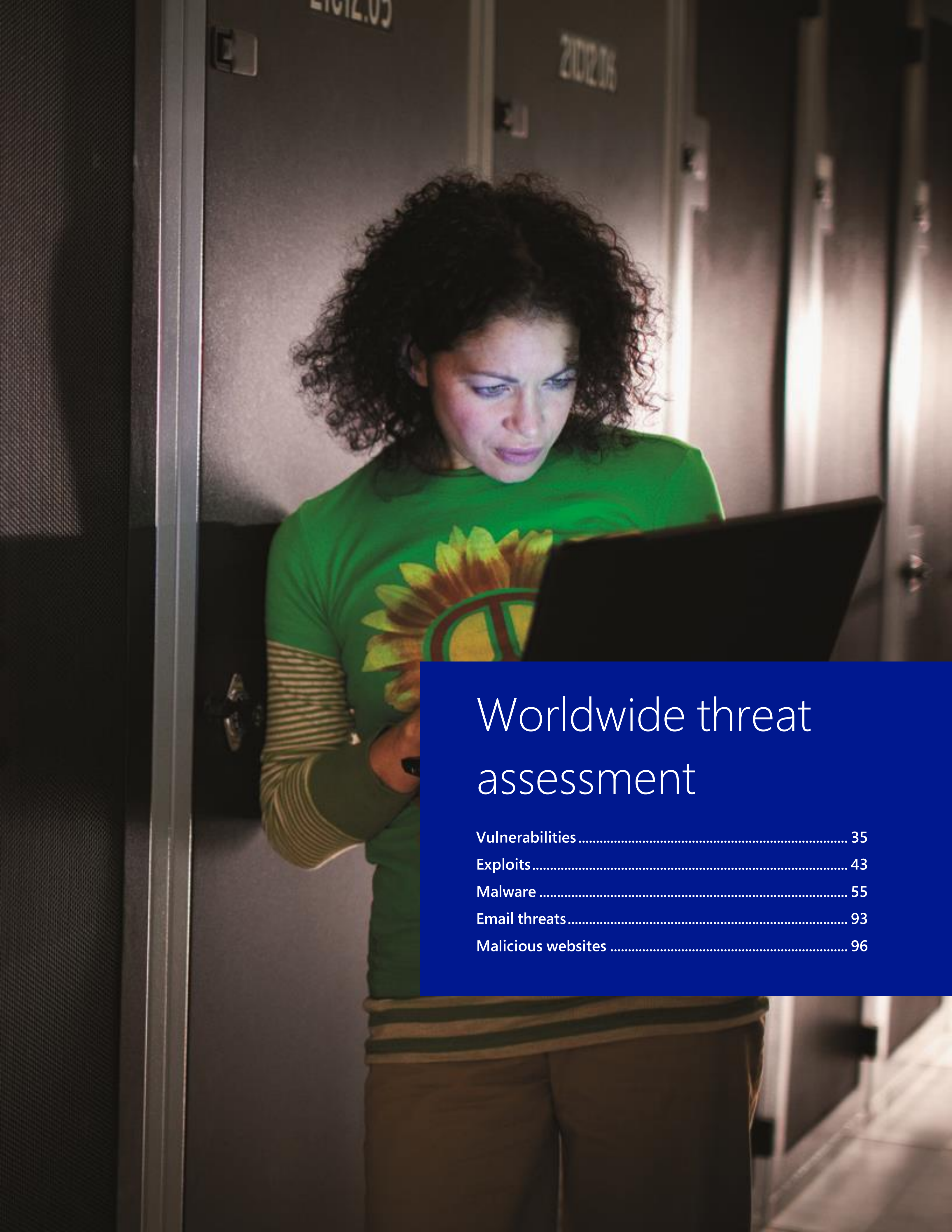
In just the last 180 days, DCU was involved in two notable malware disruptions. The first disruption targeted two malware families, MSIL/Bladabindi and VBS/Jenxcus, which affected millions of Microsoft users. The malware, created by individuals based in Algeria and Kuwait, was primarily distributed through the services of a dynamic DNS provider. The second malware disruption targeted Win32/Caphaw, a banking trojan also known as Shylock, which primarily targeted financial institutions based in the UK. This disruption was conducted in cooperation with the National Crime Agency UK as well as EUROPOL's EC3 (European Cybercrime Center). These two disruptions identified the largest number of victims of any previous operation—in excess of 33 million individuals.

> In just the last 180 days, DCU was involved in two notable malware disruptions.

Call to action

Effectively fighting cybercime requires a public-private partnership among governments, law enforcement, industry groups, and software companies such as Microsoft. DCU assistant general counsel Richard Boscovich presented Microsoft's view on the necessity of such partnerships on July 15, 2014 in testimony before the US Senate Judiciary Subcommittee on Crime and Terrorism. Video from the subcommittee hearing can be seen at www.c-span.org/video/?320442-1/hearing-cybercrime-networks-part-1.

Visit Microsoft Digital Detectives for more information on the Digital Crimes Unit.



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

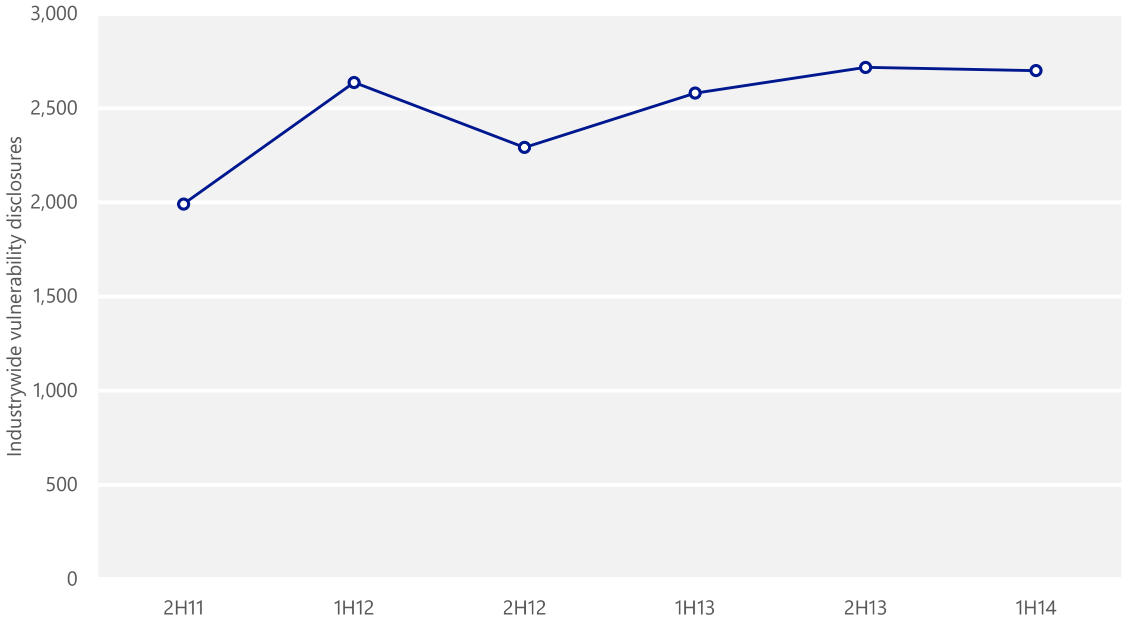
A *disclosure*, as the term is used in the *Microsoft Security Intelligence Report*, is the revelation of a software vulnerability to the public at large. Disclosures can come from a variety of sources, including publishers of the affected software, security software vendors, independent security researchers, 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.[22]

Figure 13 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 2H11. (See "About this report" on page v for an explanation of the reporting period nomenclature used in this report.)

[22] 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 13. Industrywide vulnerability disclosures, 2H11–1H14



- Vulnerability disclosures across the industry in 1H14 were down 0.6 percent from 2H13, and up 4.7 percent from 1H13. A decrease in operating system vulnerability disclosures from 2H13 to 1H14 was offset by increases in vulnerabilities affecting web browsers and other applications, which resulted in the total number of vulnerability disclosures being nearly unchanged. (See "Operating system, browser, and application vulnerabilities" on page 39 for more information.)

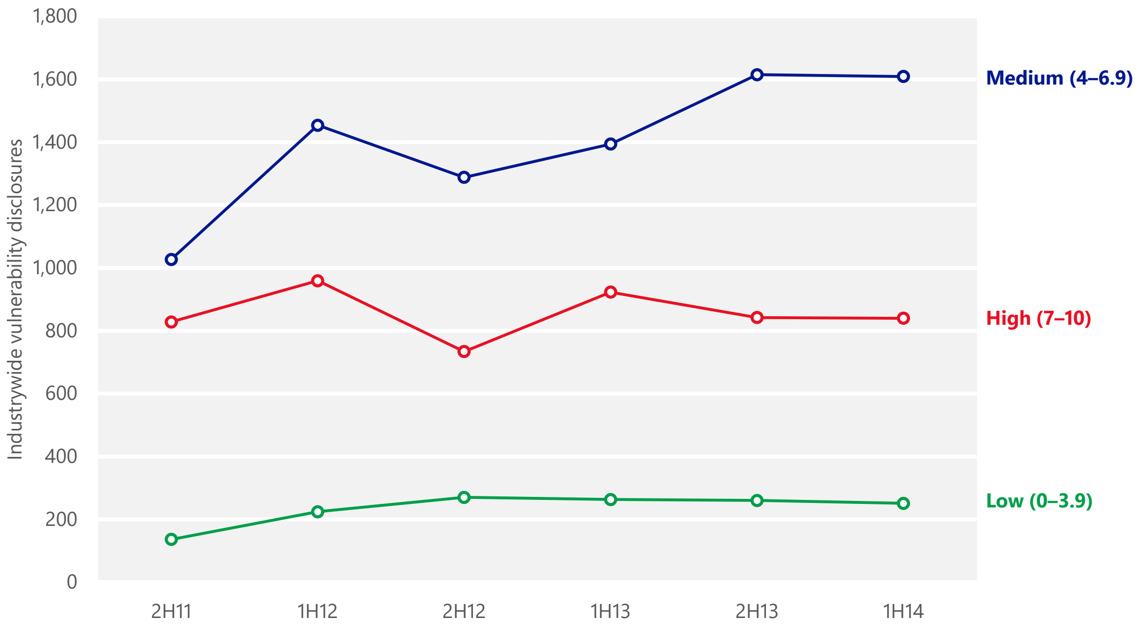
Industrywide vulnerability disclosures remained well below levels seem prior to 2009.

- Despite the general trend of small increases over the past few years, industrywide vulnerability disclosures in 1H14 remained well below levels seen prior to 2009, when totals of 3,500 disclosures or more per half-year period were not uncommon. For a historical view of the industry vulnerability disclosure trend, see the entry "Trustworthy Computing: Learning About Threats for Over 10 Years–Part 4" (March 15, 2012) at the Microsoft Cyber Trust Blog at blogs.microsoft.com/cybertrust.

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.)

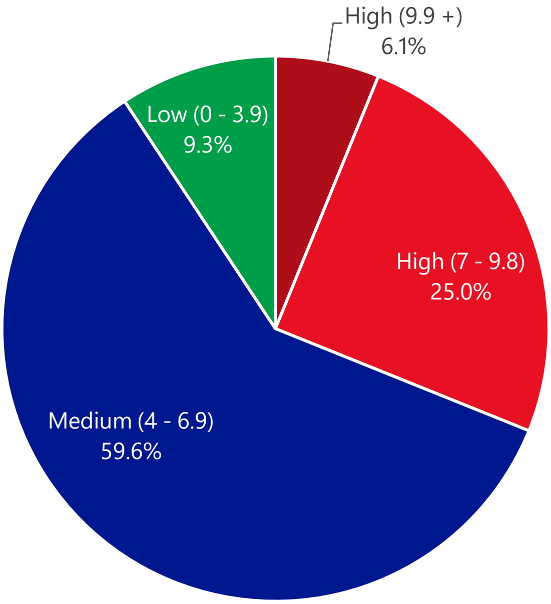
Figure 14. Industrywide vulnerability disclosures by severity, 2H11–1H14



- The industrywide vulnerability disclosure count remained stable from 2H13 to 1H14 across all three severity categories. High-severity vulnerability disclosures declined 0.2 percent, medium-severity vulnerability disclosures declined 0.4 percent, and low-severity vulnerability disclosures declined 3.5 percent.
- Medium-severity vulnerabilities—those with CVSS scores from 4 to 7.9—accounted for the largest share of vulnerability disclosures in 1H14, at 59.6 percent of all disclosures, and low-severity vulnerabilities accounted for the smallest share, at 9.3 percent. High-severity vulnerabilities accounted for nearly a third of all disclosures at 31.1 percent, with the highest-severity vulnerabilities—those scoring 9.9 or more on the CVSS scale—accounting for 6.1 percent of all vulnerabilities, as shown in Figure 15.

> High-severity vulnerabilities accounted for nearly a third of all disclosures.

Figure 15. Industrywide vulnerability disclosures in 1H14, by severity

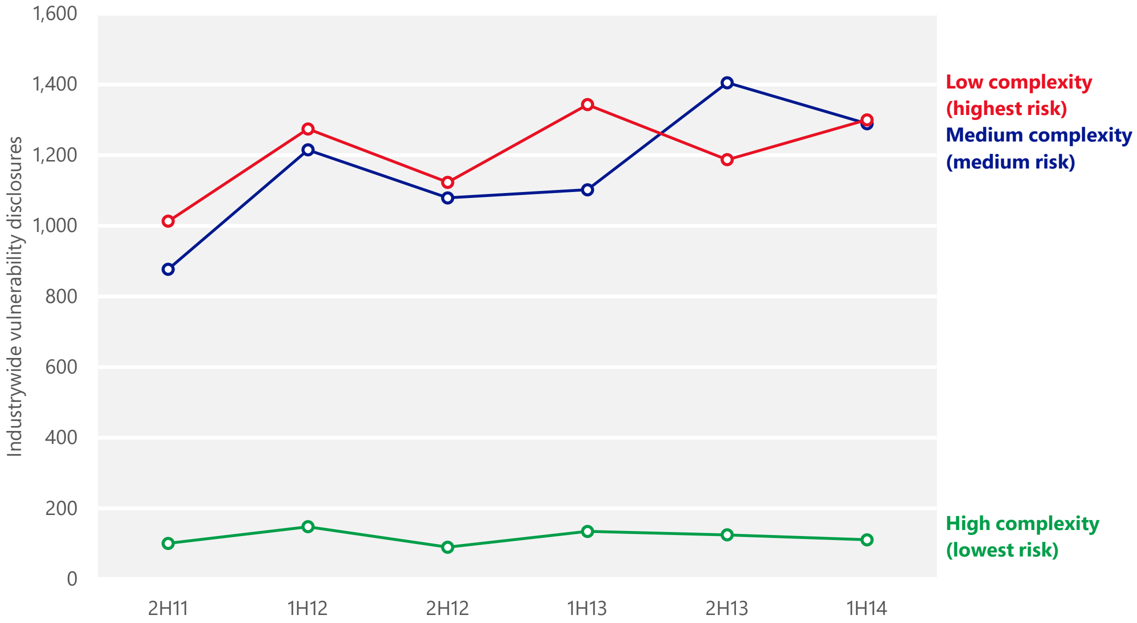


Vulnerability complexity

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 16 shows complexity trends for vulnerabilities disclosed since 2H11. Note that Low complexity in Figure 16 indicates greater risk, just as High severity indicates greater risk in Figure 14.

Figure 16. Industrywide vulnerability disclosures by access complexity, 2H11–1H14



- Disclosures of Low-complexity vulnerabilities—those that are the easiest to exploit—increased from 43.7 percent of all disclosures in 2H13 to 48.1 percent in 1H14, becoming the largest category during the period.
- Disclosures of Medium-complexity vulnerabilities accounted for 47.7 percent of all disclosures in 1H14, a decrease from 51.7 percent in 2H13.
- Disclosures of High-complexity vulnerabilities decreased to 4.1 percent of all disclosures in 1H14, down from 4.6 percent in 2H13.

Operating system, browser, and application vulnerabilities

Comparing operating system vulnerabilities to non-operating system vulnerabilities that affect other components requires determining whether a particular program or component should be considered part of an operating system. This determination is not always simple and straightforward, given the componentized nature of modern operating systems. Some programs (media players, for example) ship by default with some operating system software but can also be downloaded from the software vendor’s website and installed individually. Linux distributions, in particular, are often assembled from components developed by different teams, many of which provide crucial operating functions such as a graphical user interface (GUI) or Internet browsing.

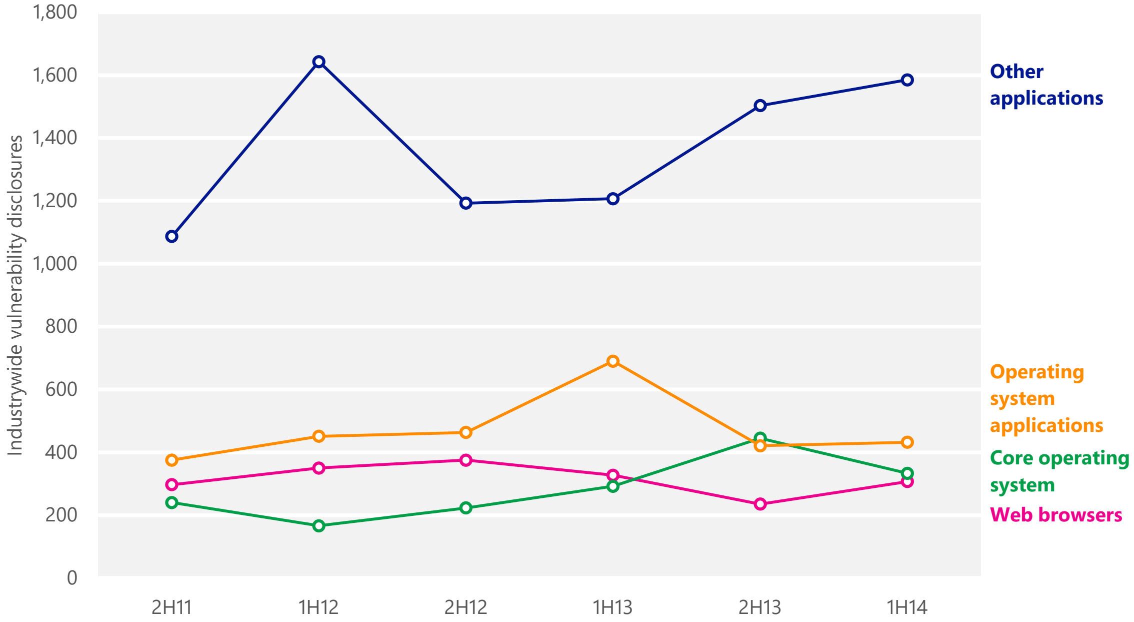
To facilitate analysis of operating system and browser vulnerabilities, the *Microsoft Security Intelligence Report* distinguishes among four different kinds of vulnerabilities:

- *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").[23]
- *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 17 shows industrywide vulnerabilities for operating systems, browsers, and applications since 2H11.

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

Figure 17. Industrywide operating system, browser, and application vulnerabilities, 2H11–1H14

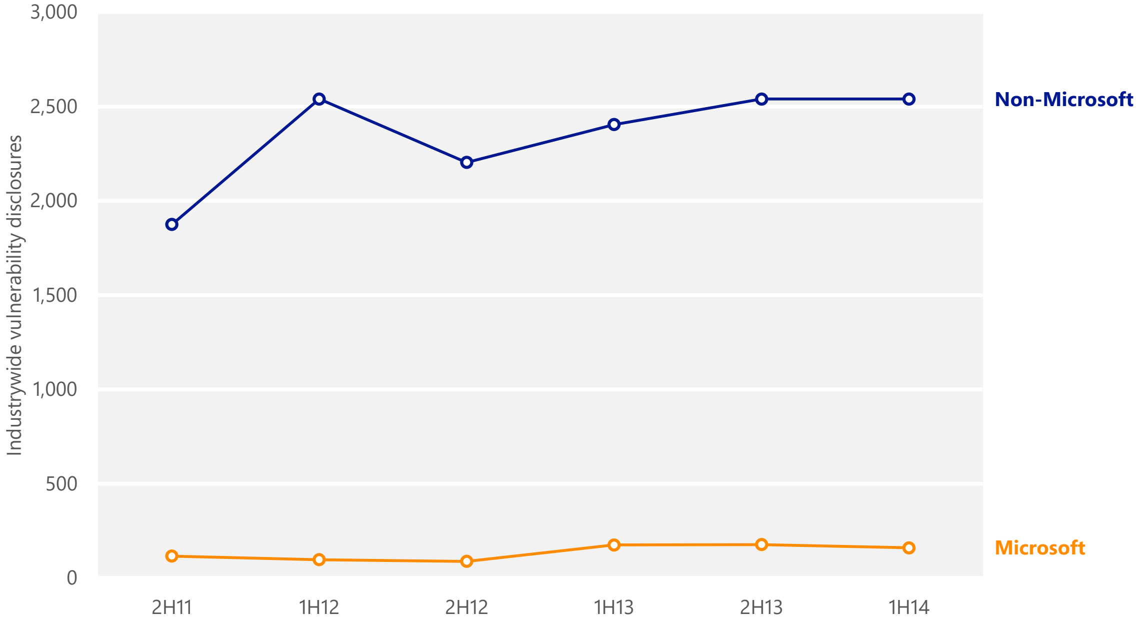


- Vulnerabilities in applications other than web browsers and operating system applications increased 5.5 percent in 1H14 and accounted for 59.7 percent of total disclosures for the period.
- Operating system application vulnerability disclosures increased 2.6 percent in 1H14, and accounted for 16.3 percent of total disclosures for the period.
- Core operating system vulnerability disclosures, the only category of disclosures to decrease in 1H14, declined 25.2 percent in 1H14, going from second to third place. Overall, operating system vulnerabilities accounted for 12.5 percent of total disclosures for the period.
- Browser vulnerability disclosures increased by 30.6 percent in 1H14, the largest percentage increase of any category, but still only accounted for 11.6 percent of total disclosures for the period.

Microsoft vulnerability disclosures

The percentage of industrywide vulnerability disclosures that affected Microsoft products decreased slightly in 1H14, as shown in Figure 18.

Figure 18. Vulnerability disclosures for Microsoft and non-Microsoft products, 2H11–1H14



- Microsoft vulnerability disclosures decreased from 177 disclosures in 2H13 to 160 in 1H14, a decrease of 9.6 percent.
- As a result of this decrease, the Microsoft percentage of all disclosures across the industry declined slightly over the same period, from 6.5 percent of all industrywide disclosures in 2H13 to 5.9 percent in 1H14.

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. 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 are pre-installed by the computer manufacturer before the computer is sold. A user may not even use the vulnerable add-on or be aware that it is installed. In addition, some software has no facility for updating itself, so even if the software vendor publishes an update that fixes the vulnerability, the user may not know that the update is available or how to obtain it and therefore remains vulnerable to attack.[24]

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.[25]

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

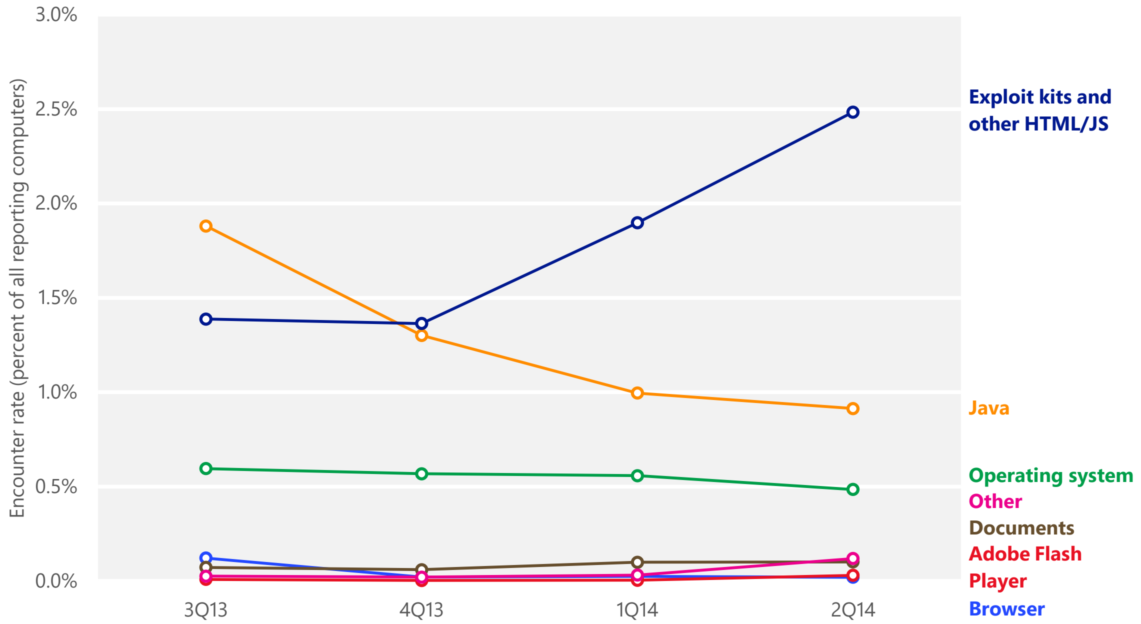
[24] See the Microsoft Security Update Guide, Second Edition at the Microsoft Download Center (www.microsoft.com/download) for guidance to help protect your IT infrastructure while creating a safer, more secure computing and Internet environment.

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

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 19 shows the prevalence of different types of exploits detected by Microsoft antimalware products in each quarter in 2013, 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 2Q14 was 1.0 percent, meaning that 1 percent of computers running Microsoft real-time security software in 2Q14 encountered Java exploit attempts, and 99 percent did not. In other words, a computer selected at random would have had about a 1 percent chance of encountering a Java exploit attempt in 2Q14. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[26] See page 55 for more information about the encounter rate metric.

Figure 19. Encounter rates for different types of exploit attempts, July 2013–June 2014



- Computers that report more than one type of exploit are counted for each type detected.

[26] For information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 127.

- Encounters with exploit kits and other HTML and JavaScript threats nearly doubled between 4Q13 and 2Q14, becoming the most commonly encountered type of exploit in the first half of the year. See "Exploit kits and other HTML/JavaScript exploits" on page 46 for more information about these exploits.
- Encounters with Java exploits decreased each quarter, but remained the second most commonly encountered type of exploit in 1H14. See "Java exploits" on page 49 for more information.
- Encounters with exploits that target operating systems decreased slightly and accounted for the third highest percentage of exploits.
- Encounters with document, Adobe Flash Player, and browser exploits remained mostly stable during the first half of the year, and each accounted for a small percentage of total exploits.

Exploit families

Figure 20 lists the exploit-related malware families that were detected most often during the first half of 2014.

Figure 20. Quarterly encounter rate trends for the top exploit families detected and blocked by Microsoft real-time antimalware products in 1H14, shaded according to relative prevalence

Exploit	Type	3Q13	4Q13	1Q14	2Q14
JS/Axpergle	Exploit kit	—	—	0.55%	1.04%
JS/Neclu	Exploit kit	—	0.00%	0.44%	0.65%
CVE-2010-2568 (CplLnk)	Operating system	0.51%	0.50%	0.50%	0.44%
HTML/Fashack	Exploit kit	—	—	—	0.34%
HTML/IframeRef*	Generic	0.69%	0.37%	0.34%	0.18%
JS/Fiexp	Exploit kit	0.01%	0.02%	0.18%	0.31%
CVE-2013-0422	Java	0.41%	0.22%	0.27%	0.14%
CVE-2012-1723	Java	0.77%	0.38%	0.24%	0.16%
JS/Blacole	Exploit kit	0.35%	0.21%	0.17%	0.15%
JS/Urntone	Exploit kit	0.03%	0.79%	0.30%	0.01%

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

- Exploit kits accounted for 5 of the 10 most commonly encountered exploits during the first half of the year. See page 46 for more information about exploit kits.

- CVE-2010-2568, the most commonly targeted individual vulnerability in 1H14, 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.
- 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 may be changed frequently.

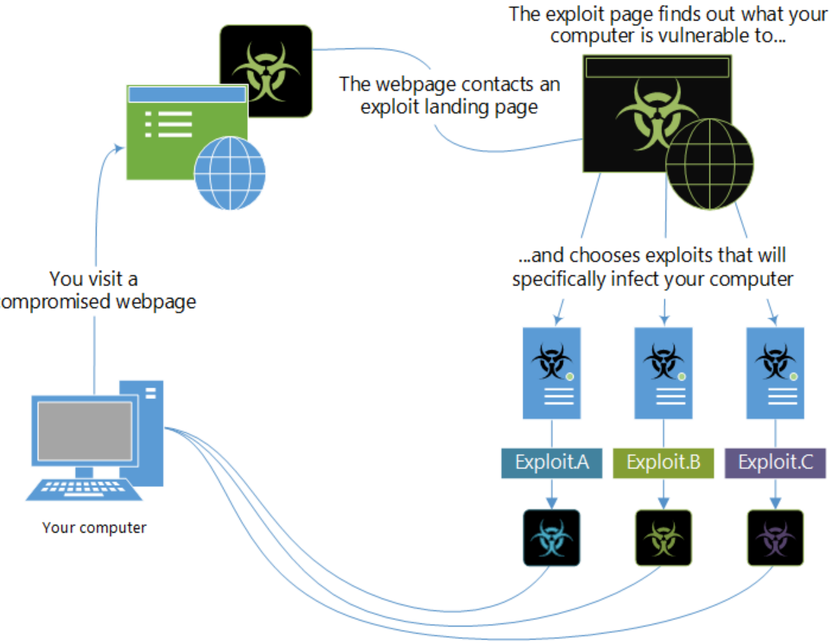
> Exploit kits accounted for 5 of the 10 most commonly encountered exploits during the first half of the year.

- Two of the top 10 exploits encountered in 1H14 are Java exploits. See page 49 for more information about these exploits.

Exploit kits and other HTML/JavaScript exploits

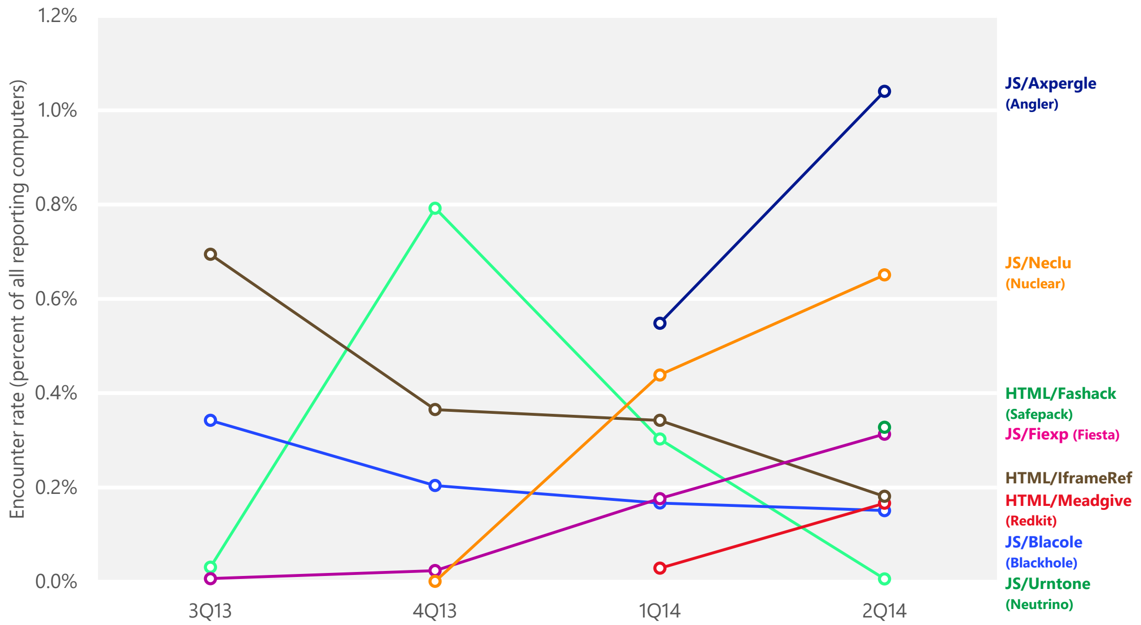
Exploit kits are collections of exploits bundled together and sold as commercial software or as a service. Prospective attackers buy or rent exploit kits on malicious hacker forums and through other illegitimate outlets. A typical kit contains a collection of webpages that contain exploits for several 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 infection through drive-by download attacks.

Figure 21. 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

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 22 shows the prevalence of several top web-based exploit kits and techniques during each of the four most recent quarters.

Figure 22. Trends for the top exploit kits and generic HTML/JavaScript threats detected and blocked by Microsoft real-time antimalware products in 1H14



- JS/Axpergle, a detection for the so-called Angler exploit kit, was the most commonly encountered exploit kit family in 1H14. The Angler kit first appeared in 1Q14 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-2013-0634 and CVE-2013-5329), 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.

- Other exploit kits that were new in 2014 included Safepack (detected as HTML/Fashack), also known as Fasthack, and Redkit (detected as HTML/Meadgive). Redkit, also called Infinity and Goon, was first encountered in 1Q14, and Safepack/Fasthack was first encountered in 2Q14. Both kits have been observed to target several of the same vulnerabilities as the Angler kit.

- The Nuclear exploit kit (detected as JS/Neclu) was the second most commonly encountered exploit kit during both quarters in 1H14. The Nuclear kit was first detected in 4Q13 at very low levels with only one known variant, Exploit:JS/Neclu.A. Encounters increased significantly in 2014 as several dozen new variants were discovered. The variants most commonly encountered in 1H14 were Exploit:JS/Neclu.C, a detection for malicious

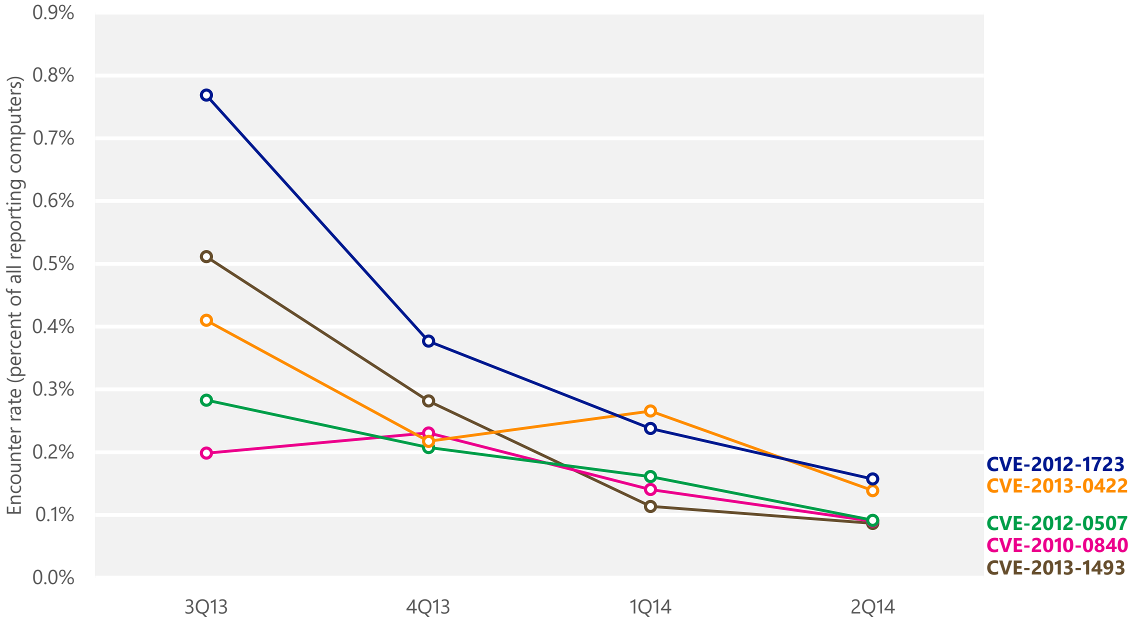
JavaScript embedded in an HTML page, and Exploit:HTML/Neclu.C, a detection for the HTML page itself.

- The Fiesta exploit kit (detected as JS/Fiexp) was responsible for the fourth largest number of exploit kit encounters in 2Q14. Like the Nuclear kit, the Fiesta kit was encountered at very low levels in 2013, with only three known variants at the time; as the number of known variants increased in 2014, so did encounters.
- Encounters involving the Neutrino exploit kit (detected as JS/Urntone), the most commonly encountered exploit kit in 4Q13, dwindled to negligible levels by 2Q14. News reports in March 2014 suggested that the author of the Neutrino kit had offered to sell the code base.[27]

Java exploits

Figure 23 shows the prevalence of different Java exploits by quarter.

Figure 23. Trends for the top Java exploits detected and blocked by Microsoft real-time antimalware products in 1H14



[27] Eduard Kovachs, "Neutrino exploit kit reportedly put up for sale by its author," *Softpedia*, March 3, 2014, news.softpedia.com/news/Neutrino-Exploit-Kit-Reportedly-Put-Up-for-Sale-by-Its-Author-430253.shtml.

- Overall, encounters with Java exploits decreased significantly in 1H14, driven by declines in exploits targeting CVE-2012-1723, CVE-2013-1493, and CVE-2010-0840. A new feature in Internet Explorer 11 provides an interface 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 (for example, if the security software identifies it as an exploit kit landing page), ActiveX controls are blocked from loading, and the actual Java exploit itself is therefore never encountered.
- CVE-2012-1723, the most commonly encountered Java exploit in 2Q14, is a type-confusion vulnerability in the Java Runtime Environment (JRE), which is exploited by tricking the JRE into treating one type of variable like another type. Oracle confirmed the existence of the vulnerability in June 2012, and 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 exploits for the vulnerability were added to the Blacole exploit kit shortly thereafter. CVE-2012-1723 exploits were removed from the Blacole kit in 2H13, contributing to the decline in its encounter rate.

  Overall, encounters with Java exploits decreased significantly in 1H14.

  For more information about this exploit, see the entry "The rise of a new Java vulnerability - CVE-2012-1723" (August 1, 2012) in the MMPC blog at blogs.technet.com/mmpc.
- CVE-2013-0422, the most commonly encountered Java exploit in 1Q14 and the second in 2Q14, 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.
- CVE-2012-0507, the third most commonly encountered Java exploit in 1H14, 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

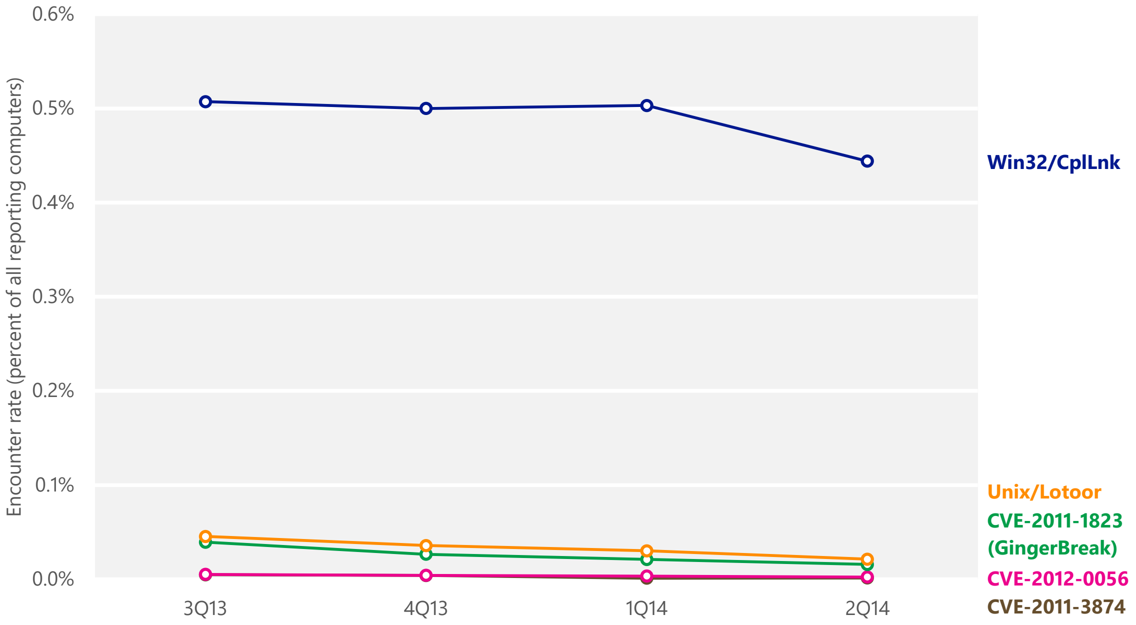
privileges of the current user, which means that an attacker can use it to perform reliable exploitation on other platforms that support the JRE, including Apple Mac OS X, Linux, VMWare, and others. Oracle released a security update in February 2012 to address the issue.

- Encounters involving CVE-2013-1493, a cross-platform vulnerability in the JRE's color management code, declined by more than 80 percent between 3Q13 and 2Q14. Initial exploits that targeted the vulnerability used heap-spraying techniques and leaked memory information to locate the accurate memory base location for exploitation. More recently, exploits have used methods such as obfuscated string and code structures in an effort to evade detection. Oracle issued a security update in March 2013 to address the vulnerability.

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 24 shows trends for the individual exploits most commonly detected and blocked or removed during each of the past four quarters.

Figure 24. Individual operating system exploits detected and blocked by Microsoft real-time antimalware products, July 2013–June 2014



- In general, exploits that target Windows have become rare. Four of the five most commonly encountered operating system exploits on Windows computers in 1H14 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.

> In general, exploits that target Windows have become rare.

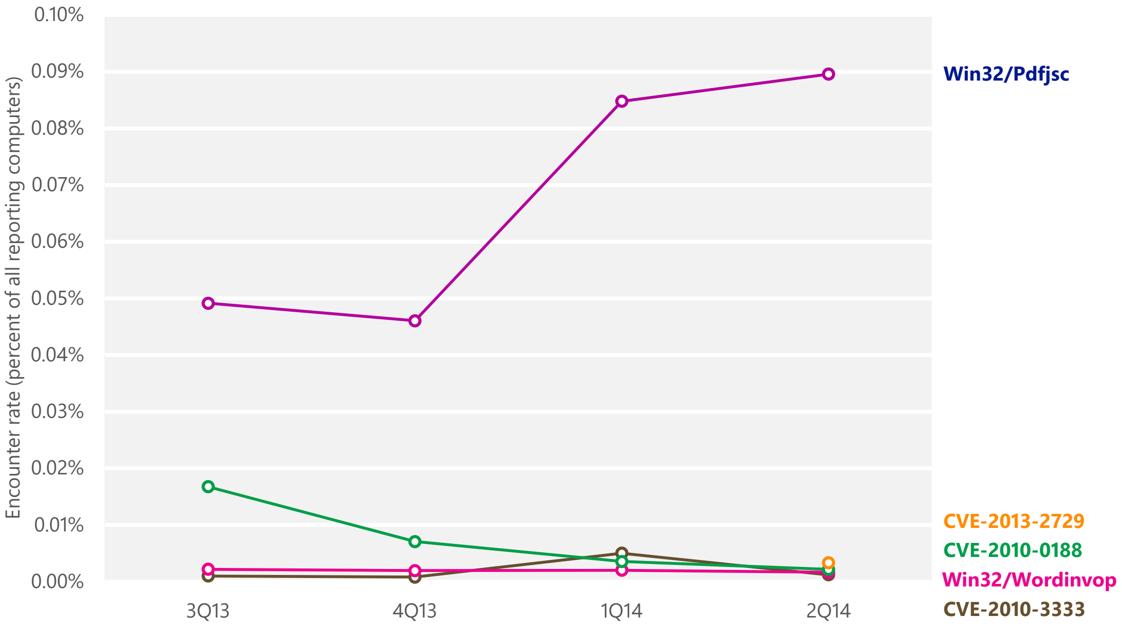
- Win32/CplLnk, an exploit that targets a vulnerability in Windows Shell, remained the most commonly encountered operating system exploit in 1H14. An attacker exploits the vulnerability (CVE-2010-2568) by creating a malformed shortcut file that forces a vulnerable computer to load a malicious file when the shortcut icon is displayed in Windows Explorer. Microsoft released Security Bulletin MS10-046 in August 2010 to address this issue.
- 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.
    - 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 may be bundled with clean applications, and includes an exploit for the CVE-2011-1823 vulnerability disguised as an image file. Google published a source code update in May 2011 that addressed the vulnerability.

- ○ CVE-2012-0056 and CVE-2011-3874 can also be used to gain root privileges on Android devices.

Document exploits

Document exploits are exploits that target vulnerabilities in the way a document editing or viewing application processes a particular file format. Figure 25 shows encounter rates for individual exploits.

Figure 25. Individual document exploits detected and blocked by Microsoft real-time antimalware products, July 2013–June 2014

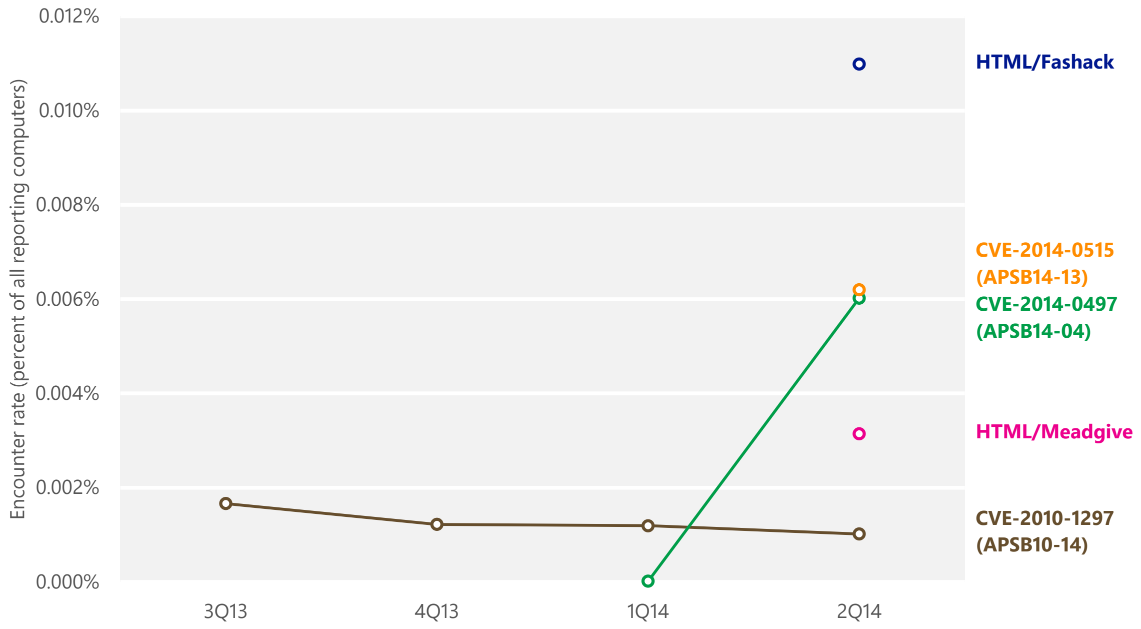


- Detections of exploits that affect Adobe Reader and Adobe Acrobat nearly doubled between 4Q13 and 1Q14. Most of these detections were associated with the exploit family Win32/Pdfjsc, a detection for PDF files containing malicious JavaScript that targets CVE-2010-0188 and other vulnerabilities. Adobe released Security Bulletin APSB10-07 in February 2010 to address CVE-2010-0188. Pdfjsc and related exploits were particularly prevalent in Russian-speaking regions.

Adobe Flash Player exploits

Figure 26 shows the prevalence of different Adobe Flash Player exploits by quarter.

Figure 26. Adobe Flash Player exploits detected and blocked by Microsoft real-time antimalware products, July 2013–June 2014



- Two of the most commonly encountered Adobe Flash Player exploit families in 2Q14, HTML/Fashack and HTML/Meadgive, are detections for exploit kits that target vulnerabilities in a number of popular browsers and add-ons. See page 46 for more information about exploit kits.
- CVE-2014-0515, the second most commonly exploited Adobe Flash Player vulnerability in 2Q14, is a buffer overflow vulnerability. Adobe released Security Bulletin APSB14-13 on April 28, 2014 to address the issue.
- CVE-2014-0497, the third most commonly exploited Adobe Flash Player vulnerability in 2Q14, is an integer underflow vulnerability. Adobe released Security Bulletin APSB14-04 on February 4, 2014 to address the issue.

Malware

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 prevalence:[28]

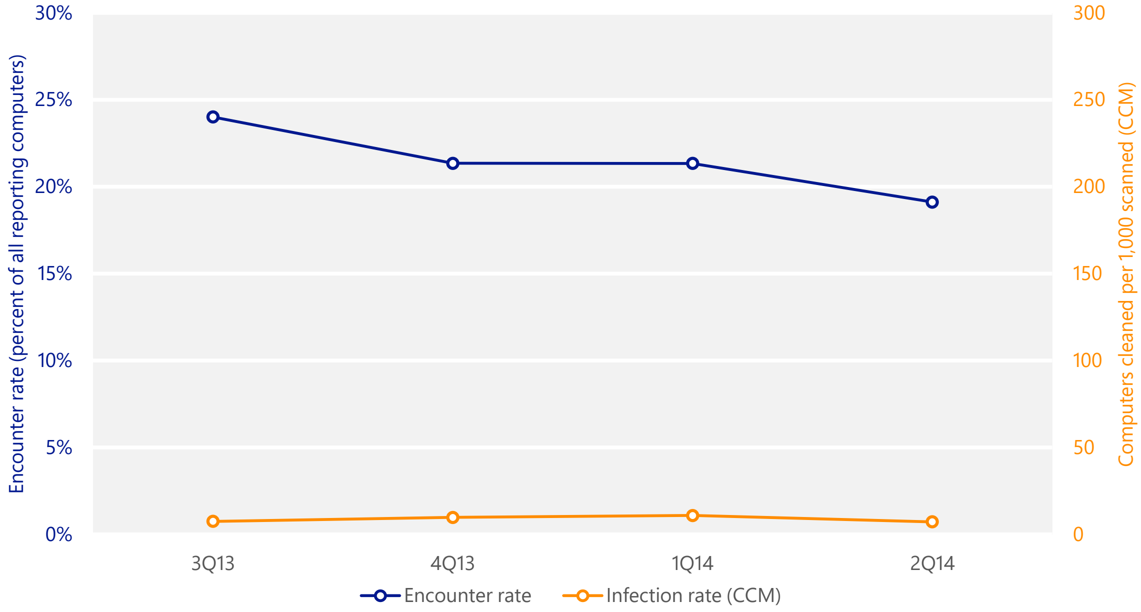
- *Encounter rate* is simply the percentage of computers running Microsoft real-time security products that report a malware encounter. For example, the encounter rate for the malware family Win32/Sefnit in Brazil in 2Q14 was 1.25 percent. This data means that, of the computers in Brazil that were running Microsoft real-time security software in 2Q14, 1.25 percent reported encountering the Sefnit family, and 98.75 percent did not. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[29]
- *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

[28] 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.
[29] For information about the products and services that provide data for this report, see "Appendix B: Data sources" on page 127.

present on the computer; it does not block infection attempts as they happen.

Figure 27 illustrates the difference between these two metrics.

Figure 27. Worldwide encounter and infection rates, 3Q13–2Q14, by quarter



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

As Figure 27 shows, and as one would expect, malware encounters are much more common than malware infections. On average, about 21.5 percent of reporting computers worldwide encountered malware over the past four quarters. At the same time, the MSRT removed malware from about 8.8 out of every 1,000 computers, or 0.88 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.

Malware encounters are much more common than malware infections.

The Sefnit saga: a timeline

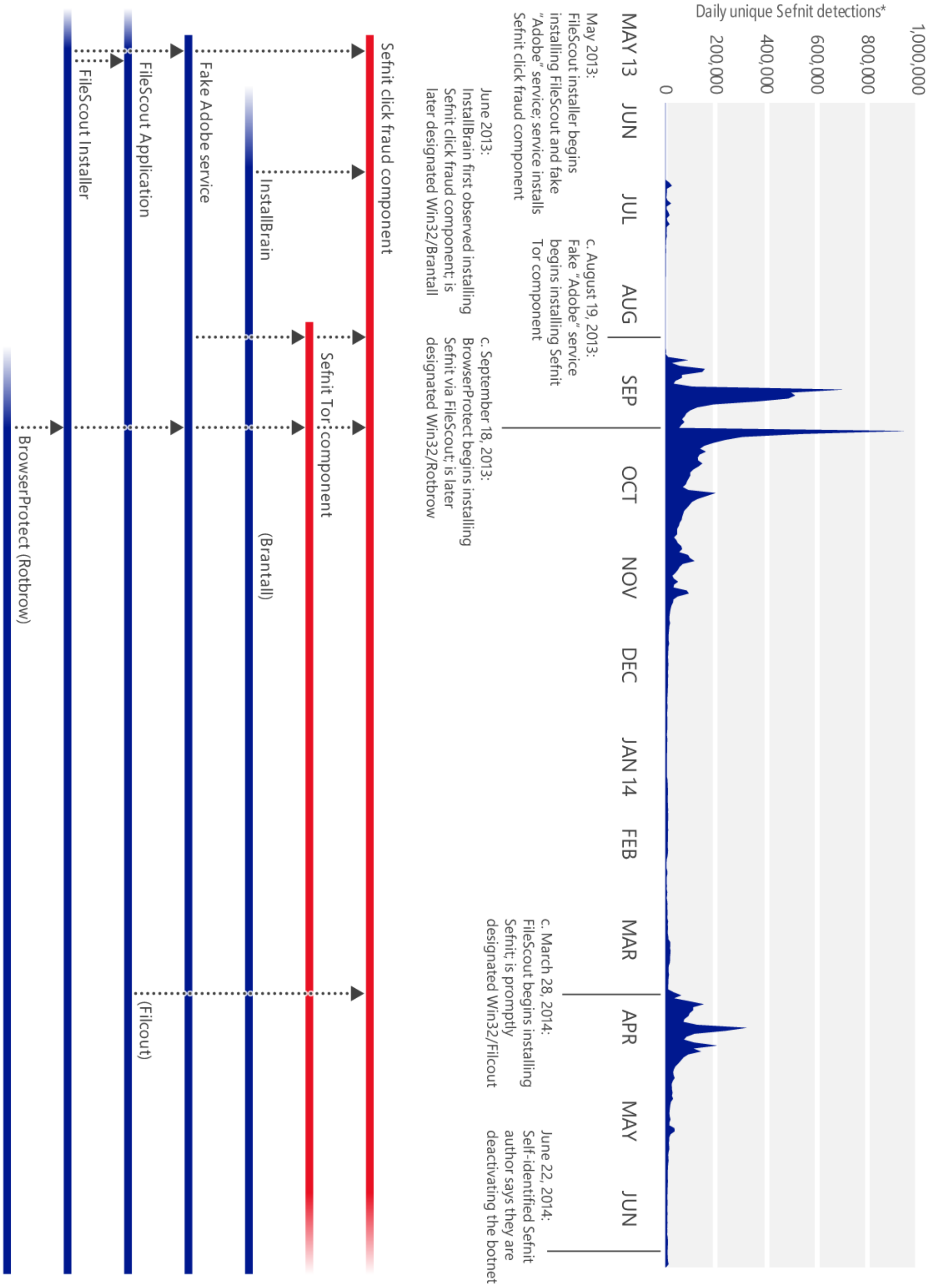
"A trio of threats makes waves in 4Q13," on page 42 of *Microsoft Security Intelligence Report, Volume 16 (July–December 2013)*, explained how the appearance of two new downloaders (Win32/Rotbrow and Win32/Brantall) and the reappearance of an older trojan (Win32/Sefnit) had a significant effect on worldwide infection rates as measured by the report. After detections of these malware families declined to low levels at the end of 2013, Sefnit suddenly reappeared in high volume in 2014, once again by misusing commercial software as a stealth distribution method for malware without being detected by major security software vendors, and once again having an outsized effect on infection rates.

This section of the *Microsoft Security Intelligence Report* endeavors to provide an account of the Sefnit story from the initial stages to the shuttering of the Sefnit botnet. It explains how rogue developers with access to commercial software source code used it as a key component of both the 2013 and 2014 outbreaks, and how Microsoft responded to these unusual tactics. It explains the role Microsoft played in reaching out to the affected software vendor and getting the Sefnit botnet deactivated. Lastly, it explains how and why the Sefnit incident had a significant effect on the way malware infection and encounter rates are being reported in this volume.

The prehistory of Sefnit

Win32/Sefnit is a bot that allows a remote attacker to use a computer to perform various activities. It has been distributed through peer-to-peer (P2P) file sharing networks disguised as a legitimate program, and by being bundled with other software. Researchers have observed Sefnit being used to perform a number of tasks that are designed to make money for the attacker, including click fraud, performing Bitcoin mining, sending out email scams, and defrauding the Bing Rewards program. Early versions of Sefnit, from 2010 and 2011, used click hijacking to redirect users' web browsers through advertising networks for some search results, thereby earning money for the attackers through affiliate programs. This behavior made it easier for security software vendors to neutralize Sefnit botnets, because users who noticed that their searches had been redirected often submitted samples to antimalware researchers to help them create improved detection signatures. The click hijacking component was removed from newer versions of Sefnit in 2011 and Sefnit was believed to no longer be very active in the wild. Detection signatures for Sefnit were first added to the MSRT in January 2012.

Figure 28. Timeline of activities involving Win32/Sefnit and related families, May 2013–June 2014

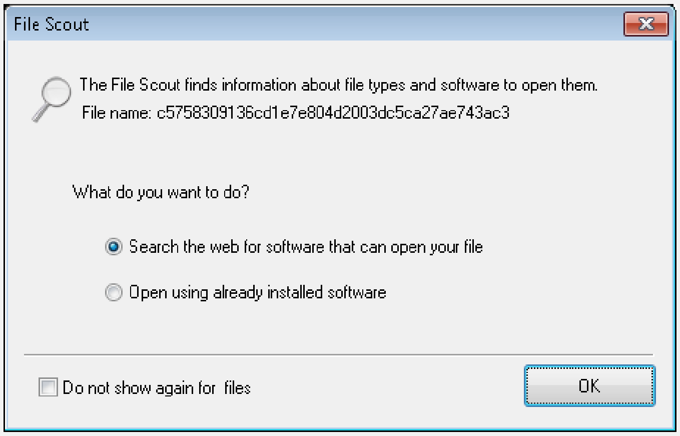


Testing the waters

The reintroduction of Sefnit in mid-2013 involved three software products, all of which are published by the same Israel-based software company.

- *InstallBrain* is a technology for packaging software into installation programs. Launching an installer created by InstallBrain installs the application the user wants, while also offering to install multiple other programs during the installation process. The InstallBrain-created installer configures itself to remain on the computer after the installation is complete, running in the background as a service. Beginning in mid-2013, attackers hijacked the server-side update mechanism for the InstallBrain service and began using it to silently download and install malware onto computers. (For clarity, installation programs created using InstallBrain are referred to collectively as "InstallBrain" in this section, as is the InstallBrain service.) Microsoft has detected malicious InstallBrain installers as Win32/Brantall since June 2013.
- *File Scout* is a utility that replaces the standard "Open with" dialog that appears when a file of an unknown type is launched from the Desktop. File Scout offers to find and download software that can open the unknown file. Programs downloaded by File Scout are packaged using InstallBrain and, during the time period discussed here, would in some cases be installed alongside malicious software. Microsoft has detected malicious File Scout variants as Win32/Filcout since April 2014.

Figure 29. The File Scout file open dialog



File Scout

The File Scout finds information about file types and software to open them.
File name: c5758309136cd1e7e804d2003dc5ca27ae743ac3

What do you want to do?

● Search the web for software that can open your file

○ Open using already installed software

□ Do not show again for files

- *Browser Protector* (also called Browser Defender, Browser Manager, BitGuard, and other names) is a browser add-on that claims to provide protection against malicious software. Microsoft has detected malicious Browser Protector variants as Win32/Rotbrow since October 2013.

In May 2013, after being dormant for more than a year, Sefnit distribution resumed at a low level by way of a new installation program for File Scout. When File Scout was installed on a computer, the new installer also installed a service that falsely identifies itself as "Adobe Flash Player Update" (later detected as Trojan:Win32/Sefnit.AU). Forensic investigation later revealed that the compromised File Scout program and the fake Adobe Flash Player update service were compiled 15 minutes apart using the same compiler, and were developed from the same source code.

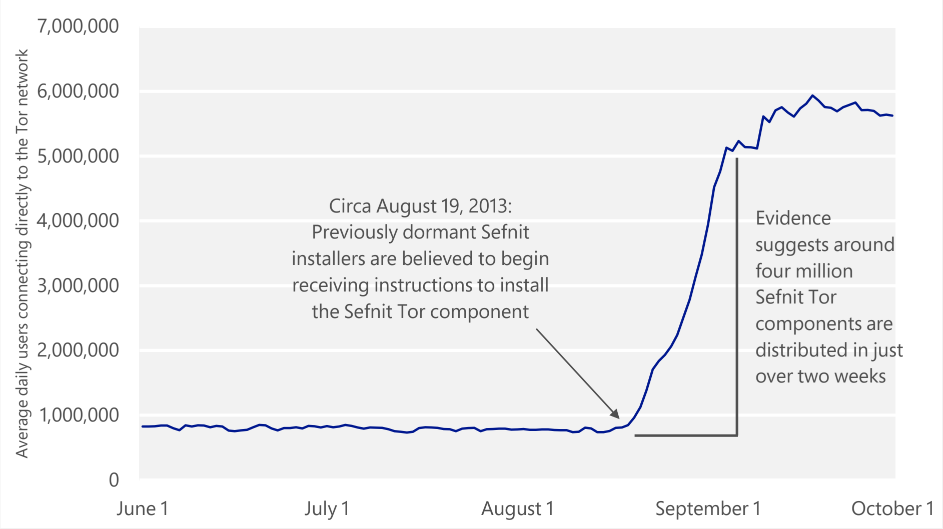
The fake Adobe Flash Player update service began installing the click fraud component of Sefnit at very low levels. Evidence suggests that only a small percentage of the fake Adobe Flash Player update service installations were installing Sefnit at this time, with the rest of the installations remaining dormant. Microsoft did not initially see a connection between the new malware samples and the dormant Sefnit samples, so the first samples were designated with a different name, Win32/Mevade.

The following month, the rogue InstallBrain service began to install the Sefnit click fraud component on computers directly. In many or most cases, this service had been installed on the computer earlier when someone used an InstallBrain-created installation package (possibly obtained through File Scout) to install legitimate, unrelated software on the computer. After completing this earlier installation, InstallBrain remained resident on the computer as a service, potentially for quite some time. It was these pre-existing InstallBrain services that began installing Sefnit in June 2013. As with File Scout, the rogue InstallBrain service initially distributed Sefnit at very low levels, with Microsoft detecting only a few thousand infection attempts per day worldwide or fewer through August.

The return of Sefnit

In late August 2013, the computers infected with the fake Adobe Flash Player update service installed alongside File Scout were commanded to download and install a Sefnit component that used the Tor network for botnet command and control. Tor is an open source project that provides users with a way to access Internet resources anonymously by relaying traffic through the computers of other Tor users. It has a number of legitimate uses, but it can also be used with malicious intent, as with the Sefnit botnet. The Sefnit component that used the Tor component had been around for years, but had never been seen in such large quantities before. Based on usage estimates provided by the Tor Project, this action apparently added more than four million new clients to the Tor network in just over two weeks, with about a million more added over the following month.

Figure 30. The effect of Win32/Sefnit on the user base of the Tor network



Circa August 19, 2013: Previously dormant Sefnit installers are believed to begin receiving instructions to install the Sefnit Tor component

Evidence suggests around four million Sefnit Tor components are distributed in just over two weeks

Data courtesy of the Tor Project (metrics.torproject.org)

Detections of Mevade, as Microsoft security products still identified the new Sefnit variants, increased rapidly, from less than 700 per day during the third week of August to around half a million per day a few weeks later. An even larger surge would come in late September (around the time Microsoft redesignated Mevade as new variants of Sefnit) when compromised versions of Browser Protector, the add-on that claimed to offer protection from malware, began to install File Scout on millions of computers, along with the fake Adobe Flash Player update service, the Sefnit Tor client, and the Sefnit click fraud component. Microsoft security products detected and blocked or removed Sefnit infections from nearly a million computers in a single day at the height of the infection campaign, and continued to detect Sefnit on about 100,000 computers per day through late September and early October.

Sefnit detections retreated to comparatively low levels in December and through the first few months of 2014. Then, in late March, compromised versions of the File Scout utility—which, despite its connections to Sefnit, had never exhibited malicious behavior itself—was observed installing Sefnit on computers directly. Detections of Sefnit increased again, reaching a peak of around 300,000 computers per day in mid-April.

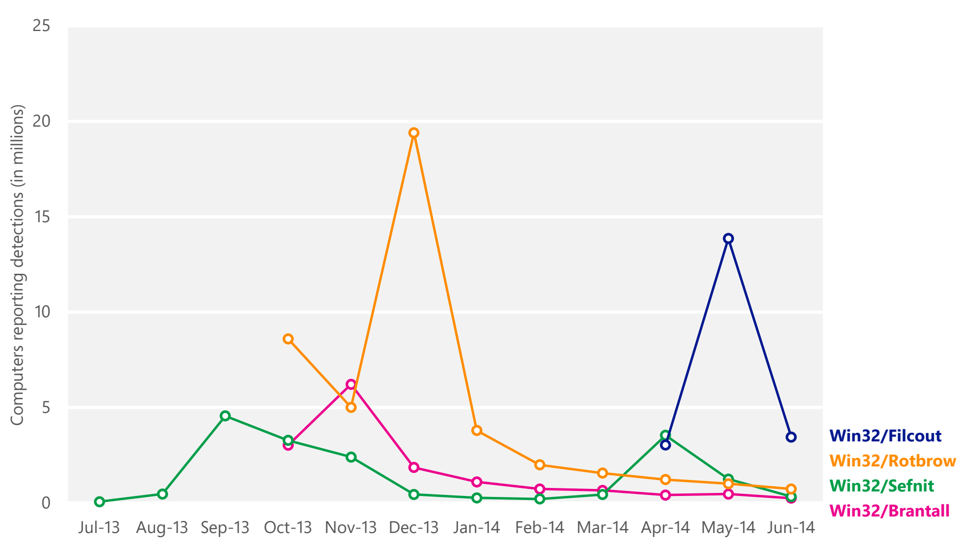
Fighting back

In May and June 2014, Microsoft researchers met with the software company that publishes InstallBrain, Browser Protector, and File Scout, and established that rogue developers who had access to the company's source code and servers were responsible for inserting the malicious code to distribute Sefnit. On June 22, the self-identified author of the Sefnit malware declared that they would be deactivating the Sefnit botnet and central servers, and would prevent further distribution of the malware. Microsoft has confirmed that the Sefnit command-and-control servers have been shut down, and no major Sefnit activity has been observed since then.

Infection statistics

Figure 31 illustrates how the changing distribution methods used by the Sefnit authors affected the threat landscape.

Figure 31. Computers reporting detections of Win32/Sefnit and related families, July 2013–June 2014 (MSRT detections excluded)

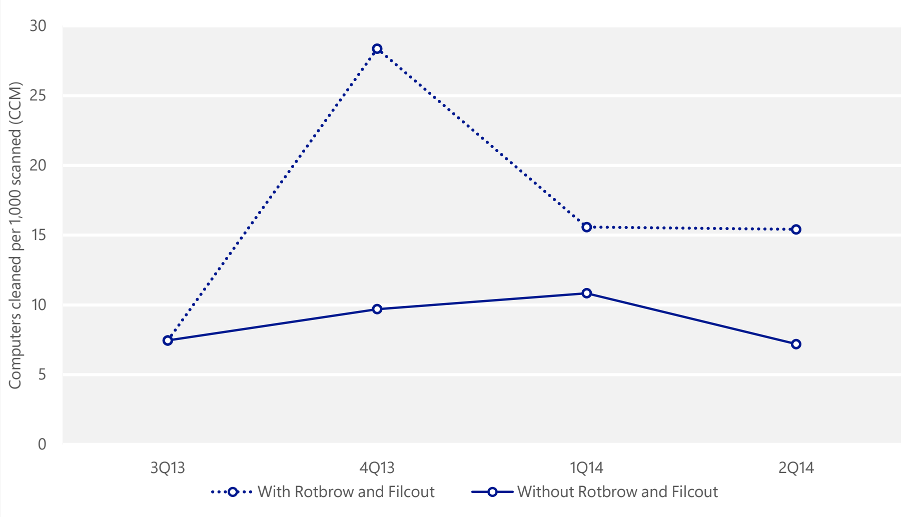


The increase in Sefnit detections began in late August and early September, before its means of distribution were fully recognized. When detection signatures for Rotbrow and Brantall were added to Microsoft real-time security products in October, both families were quickly detected at significant volumes, with Brantall detections peaking in November and Rotbrow detections peaking a month later at a much higher level. Detections of Sefnit subsequently dwindled to negligible levels as its distribution methods were closed off. Sefnit detections increased again in April as Filcout began to distribute it directly, and then declined again as Filcout infections were dealt with.

Sefnit and the *SIR*

Sefnit's use of these programs for distribution has had a significant impact on the way Microsoft calculates encounter and infection rates for the *Microsoft Security Intelligence Report*. Ideally, malware is blocked by real-time security software before it can infect a computer, or is removed shortly after infection during a routine scan as signature files are updated to detect it. Because File Scout, Browser Protector, and InstallBrain had not previously been overtly malicious, Microsoft and a number of other security software vendors had not made any attempt to detect and remove them. When the Sefnit attackers subsequently adapted them for malware distribution, security software vendors began to detect the newly malicious programs, which led to large numbers of removals involving programs that may have been installed several months earlier. As a result, the unmodified infection and encounter rate figures tend to be dominated by removals of these programs.

Figure 32. Infection rates with and without Win32/Rotbrow and Win32/Filcout



Microsoft believes that the unmodified figures do not create an accurate picture of the worldwide threat landscape over the past year. As a result, totals for Brantall, Filcout, and Rotbrow have been removed from the infection and encounter figures presented here where appropriate, as noted.

Guidance: Keeping code secure

A software vendor's code base is one of its most important assets, and keeping it safe should always be a top concern. Although most security development guidance tends to focus on securing code from outside attackers by finding and fixing vulnerabilities, it's important to consider the potential threat that malicious insiders can pose as well.

- Secure development processes such as the Security Development Lifecycle (www.microsoft.com/sdl) incorporate multiple layers of code review and threat modeling that may help a development team notice tampering before a product is released.
- Proper management of the supply chain is especially important in a world in which componentized and outsourced product development have become increasingly commonplace. The paper "Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity," available from the Microsoft Download Center, provides a simple framework for the pragmatic inclusion of software integrity risk management practices in the product development process and online services operations.

Malware prevalence worldwide

The telemetry data generated by Microsoft security products from computers whose administrators or users choose to opt in to provide data to Microsoft includes information about the location of the computer, as determined by IP geolocation. This data makes it possible to compare infection and encounter rates, patterns, and trends in different locations around the world.[30]

Figure 33. Encounter rate trends for the locations with the most computers reporting malware encounters in 1H14, by number of computers reporting

	Country/Region	3Q13	4Q13	1Q14	2Q14
1	United States	16.7 %	13.0 %	13.0 %	12.3 %
2	Brazil	43.1 %	36.8 %	34.0 %	30.5 %
3	Russia	31.7 %	28.9 %	28.7 %	26.4 %
4	Turkey	41.3 %	45.5 %	45.7 %	40.5 %
5	France	24.2 %	23.0 %	20.2 %	16.8 %
6	India	51.0 %	47.1 %	50.5 %	41.7 %
7	Mexico	39.8 %	36.7 %	38.6 %	32.1 %
8	Germany	18.1 %	14.8 %	13.6 %	13.5 %
9	Italy	28.3 %	26.1 %	25.5 %	20.4 %
10	United Kingdom	18.2 %	14.5 %	13.5 %	13.3 %

Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

- Locations in Figure 33 are ordered by the number of computers reporting detections in 1H14.
- Encounter and infection rates generally declined in 2Q14 because of significant declines for the trojan families Win32/Wysotot and Win32/Sefnit.
- The worm family VBS/Jenxcus was particularly prevalent in Latin America, India, and the Middle East. It was the most commonly detected family in Brazil and Mexico in 2Q14 and the second most common family in India, but ranked only 54th in Germany and 57th in the United States. See "Threat families" on page 76 for more information about Jenxcus and other prevalent families.

[30] 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).

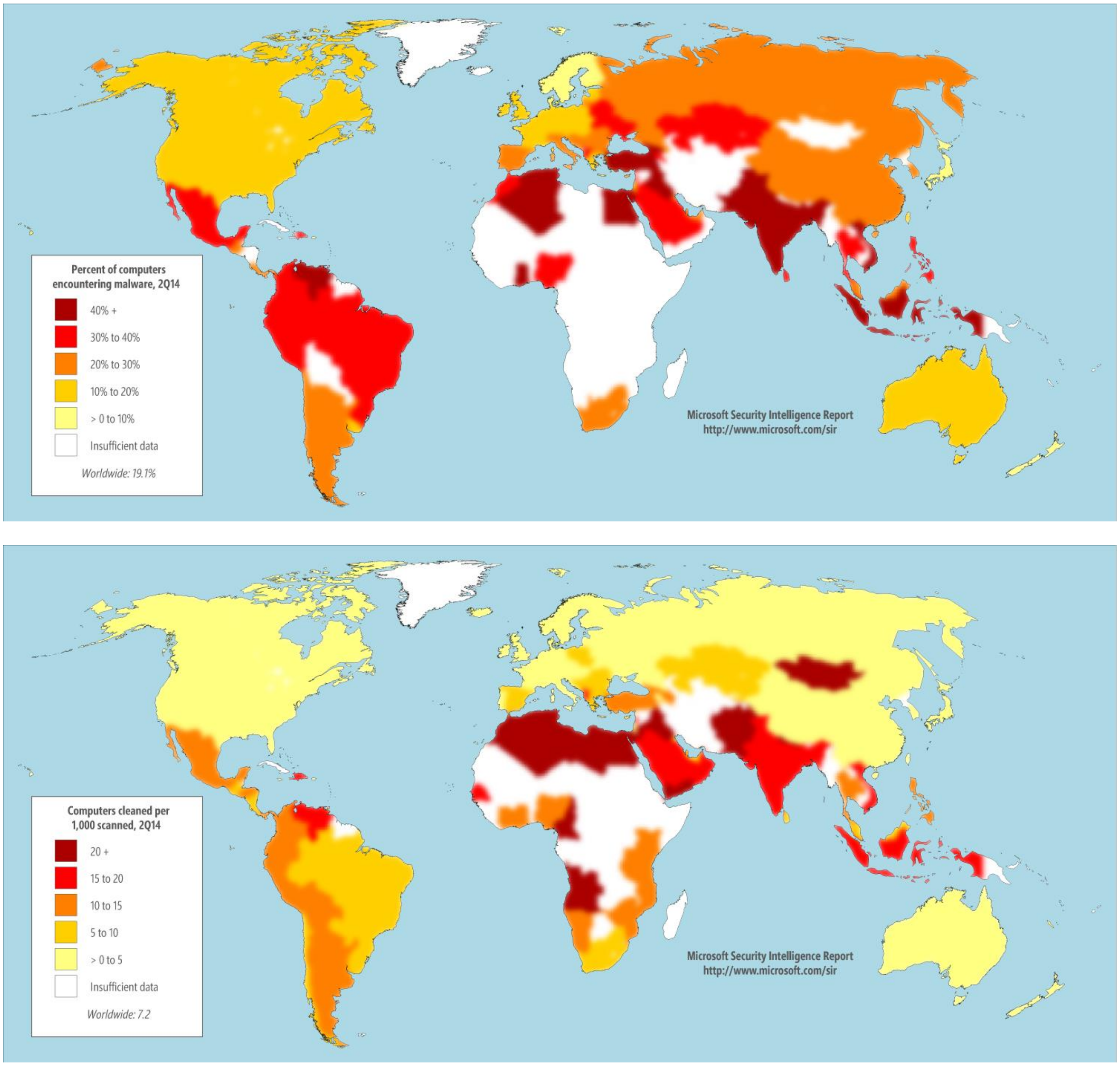
- Wysotot also displayed regional encounter patterns. It was the most commonly encountered family in Brazil, Turkey, and France in 1Q14, but ranked 14th in Russia and 15th in the US.
- Adware predominated in the United States and France in 1Q14, when the top three malware families in the US and the top five families in France were all adware families.
- In addition to Wysotot and Jenxcus, malware families that were unusually prevalent in Brazil include the worm family JS/Proslikefan (the third most commonly encountered family in Brazil in 1H14, but only 46th worldwide), and the trojan family Win32/Febipos (seventh in Brazil, 82nd worldwide). See the entry "Browser extension hijacks Facebook profiles" (May 10, 2013) on the MMPC blog at blogs.technet.com/mmpc for more information about Febipos in Brazil.
- Malware families that were unusually prevalent in Russia include the adware family Win32/BetterSurf, the generic detection Win32/Obfuscator, and the worm family Win32/Dorkbot. Win32/Ogimant, the most commonly detected family in Russia in 2Q14, was highly prevalent in Russia and several other former Soviet republics, but was virtually unknown elsewhere.

Encounter and infection rates generally declined in 2Q14 because of Wysotot and Sefnit.

- The trojan family JS/Kilim, the most commonly encountered family in Turkey in 1H14, was very rare elsewhere. Other families that were particularly prevalent in Turkey include Wysotot and the trojan family JS/Faceliker. (See the entry "Turkey: Understanding high malware encounter rates in SIRv15" (December 23, 2013) on the MMPC blog for more information about malware in Turkey.)
- In India, the worm family Win32/Gamarue and the trojan family Win32/Ramnit were unusually prevalent.
- Jenxcus was the most commonly encountered malware family in Mexico by a wide margin, with an encounter rate more than three times as high as the next most common family.
- Adware was common in Germany and Italy, notably Win32/Lollipop (fifth in Germany and Italy in 1Q14, 18th worldwide)
- The adware families Win32/AddLyrics and Win32/Feven and the exploit family JS/Axpergle were unusually prevalent in the United Kingdom.

For a different perspective on threat patterns worldwide, Figure 34 shows the infection and encounter rates in locations around the world in 2Q14.

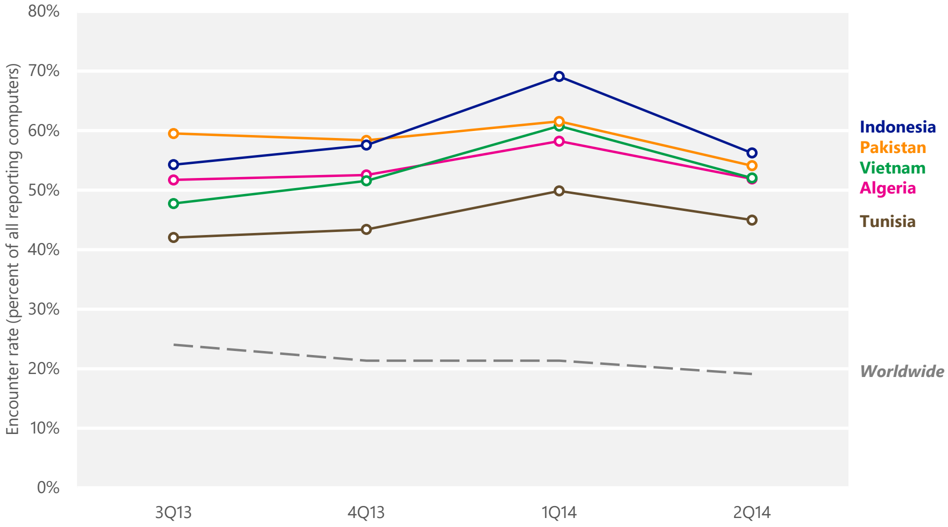
Figure 34. Encounter rates (top) and infection rates (bottom) by country/region in 2Q14


Percent of computers encountering malware, 2Q14
40% +
30% to 40%
20% to 30%
10% to 20%
> 0 to 10%
Insufficient data
Worldwide: 19.1%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir
Computers cleaned per 1,000 scanned, 2Q14
20 +
15 to 20
10 to 15
5 to 10
> 0 to 5
Insufficient data
Worldwide: 7.2
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

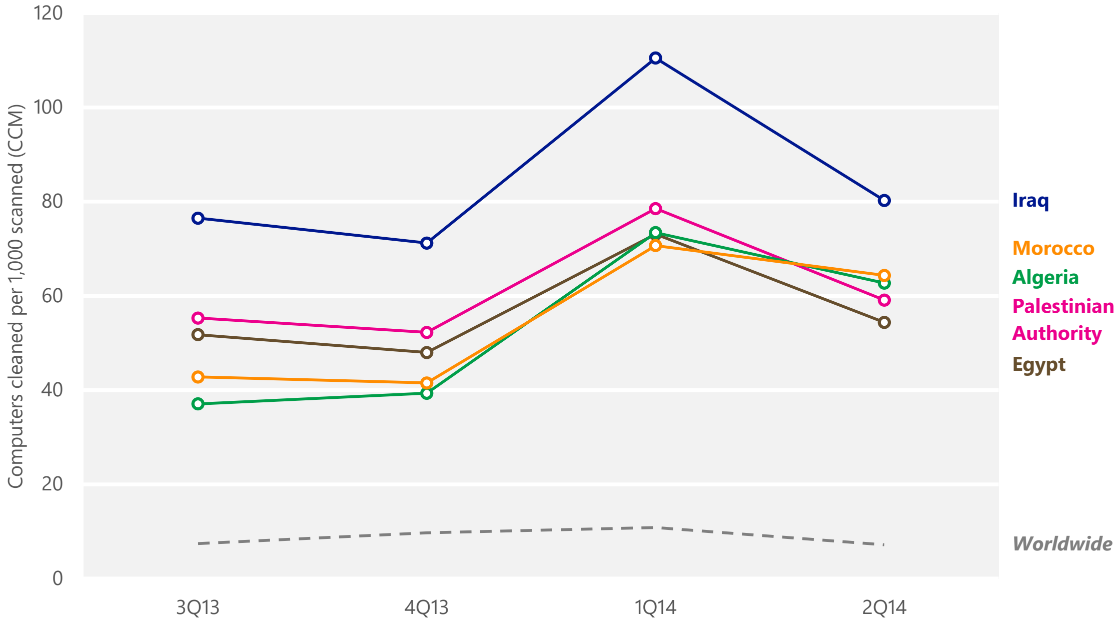
The next several figures illustrate trends for specific locations around the world with particularly high or low incidences of threat detection. Figure 35 and Figure 36 show trends for the locations with the highest rates of detection as determined by encounter rate and CCM, respectively.

Figure 35. Trends for the five locations with the highest malware encounter rates in 1H14 (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

Figure 36. Trends for the five locations with the highest malware infection rates in 1H14, by CCM (100,000 MSRT computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

- The locations with the highest encounter rates were Indonesia, Pakistan, Vietnam, Algeria, and Tunisia.
  - Viruses and worms accounted for seven of the top 10 malware families in Indonesia in the first half of 2014, including Win32/Slugin, a virus

family that was only detected in seven other countries and regions, all at much lower encounter rates than Indonesia. The most commonly detected families in Indonesia in 1H14 were the trojan family Win32/Ramnit and the exploit Win32/CplLnk, neither of which were among the top 10 most commonly encountered families worldwide.

    - The list of top malware families encountered in Pakistan was also dominated by viruses and worms, including the worm families VBS/Jenxcus and INF/Autorun, and the virus family Win32/Sality. The worm family Win32/Chir was disproportionately prevalent there, with computers in Pakistan accounting for more than half of all Chir encounters worldwide. Chir is a worm that can spread via email, shared drives, and also has a virus component that infects other files. In Pakistan, it often arrives with a file name that includes "Jinsi Maloomat" (or "Gensi Maloomat"), a reference to an Urdu-language book.

    - Six of the most commonly detected malware families in Vietnam were not among the 10 most commonly detected families worldwide, including the trojan families Ramnit and JS/Faceliker and the exploit CplLnk. The well-known worm Win32/Conficker was the 10th most commonly encountered family in 1H14 in Vietnam, the only location listed in Figure 35 to have Conficker in the top 10.

    - Jenxcus was encountered by more than a quarter of reporting computers in Algeria in 1H14, nearly three times as many as the next most common malware family. Unusually prevalent families in Algeria include Ramnit, CplLnk, and the backdoor family MSIL/Bladabindi.

    - Jenxcus was also the most commonly detected malware family in Tunisia, being encountered by more than twice as many computers as any other family. Unusually prevalent families in Tunisia include MSIL/Bepush, a downloader family that downloads and installs add-ons for the Google Chrome and Mozilla Firefox browsers, and the generic trojan detection Win32/Meredrop.

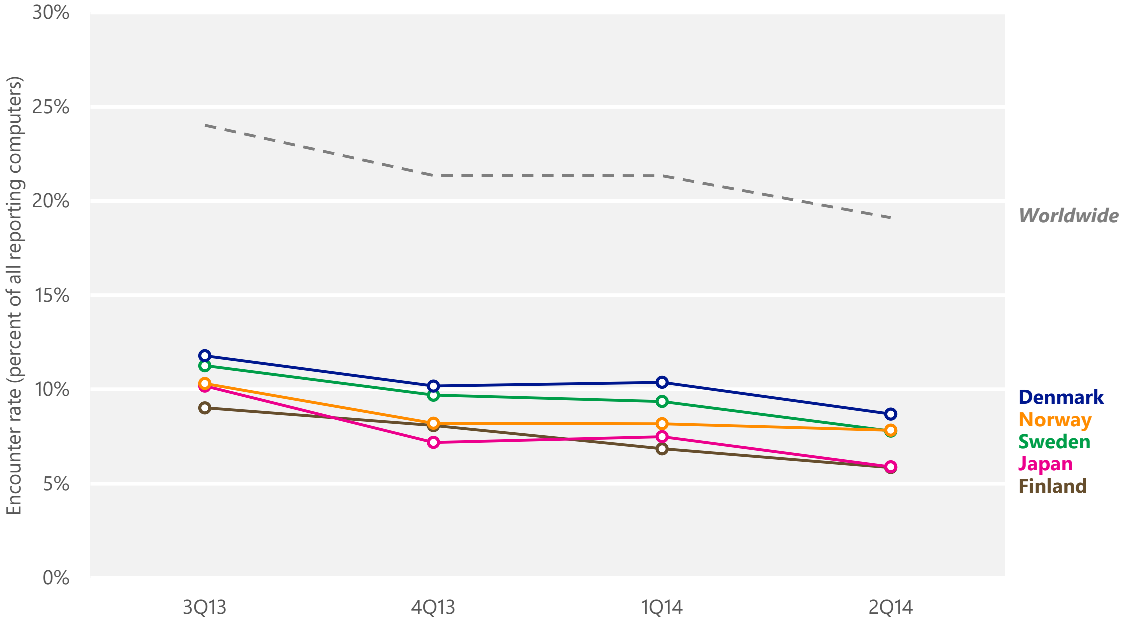
- The locations with the highest infection rates were Iraq, Morocco, Algeria, the Palestinian territories, and Egypt.

    - Jenxcus, Bladabindi, and Sality were the most common malware families infecting computers in Iraq in 1H14. In fourth place was the worm family

Win32/Wecykler, which had its highest infection rate there (a CCM of 11.0 in Iraq in 2Q14, compared to 2.2 in Afghanistan, the next highest location). Wecykler is a family of worms that spread via removable drives, such as USB drives; they may stop security processes and other processes on the computer, and log keystrokes which they later send to a remote attacker.

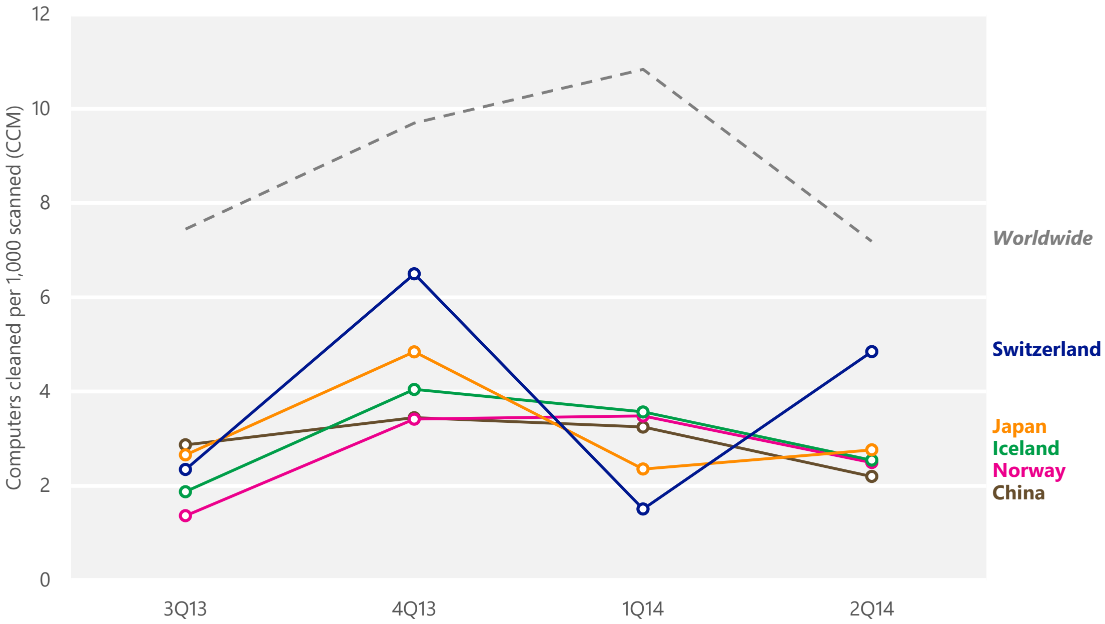
  - In Morocco, the top infecting malware families were Jenxcus and the worm family Win32/Yeltminky, which had its highest infection rate there (a CCM of 13.2 in Morocco in 2Q14, compared to 2.1 in Algeria, the next highest location). Yeltminky is a family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute the copies.
  - Jenxcus and Sality were the top infecting malware families in both Egypt and the Palestinian territories. Other top families in the Palestinian territories include Bladabindi and the trojan family MSIL/Spacekito. Top families in Egypt include the trojan families Win32/Wysotot and Win32/Nitol.
- For more information about malware in many of these countries/regions, see "The Threat Landscape in the Middle East and Southwest Asia," a five-part series on the Microsoft Cyber Trust blog (blogs.microsoft.com/cybertrust):
  - Part 1: Relatively High Malware Infection Rates (March 12, 2014)
  - Part 2: Relatively High Malware Encounter Rates (March 13, 2014)
  - Part 3: Regional Anti-virus Software Usage (March 17, 2014)
  - Part 4: Regional Windows XP Market Share (March 18, 2014)
  - Part 5: Socio-economic Factors and Regional Malware Infection Rates (March 19, 2014)

Figure 37. Trends for locations with low malware encounter rates in 1H14 (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

Figure 38. Trends for locations with low malware infection rates in 1H14, by CCM (100,000 reporting computers minimum)



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 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 1H14, these locations typically had encounter and infection rates between about one-third and one-half of the worldwide average. (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.)

- The exploit family JS/Axpergle, the adware family Win32/BetterSurf, and the trojan families Win32/Sefnit and Win32/Wysotot were all among the most commonly encountered or infecting threat families in most of these locations. Switzerland, in particular, was heavily affected by Sefnit, which was detected in greater numbers in 4Q13 and 2Q14, similar to the overall infection rate in Switzerland. See "The Sefnit saga: a timeline" on page 57 for more information about this family.

  Axpergle is a detection for the so-called Angler exploit kit, which was the most commonly detected exploit kit family in 1H14. See "Exploit kits and other HTML/JavaScript exploits" on page 46 for more information.

- Win32/FakePAV was among the most prevalent malware families in Denmark and Norway in 1H14. FakePAV is a rogue security software family that mimics the general look and feel of legitimate security software programs and claims to detect a large number of nonexistent threats while urging users to pay for the so-called "full version" of the software to remove the nonexistent threats. Rogue security software was once a significantly more prominent category of malware but has become less prevalent over the past year or two, although some families remain relatively common in wealthy countries and regions.

Some rogue security software families remain relatively common in wealthy countries and regions.

- Win32/Lecpetex was the sixth most commonly encountered malware family in Norway in 1H14. Lecpetex is a trojan that uses the infected computer's resources to "mine" for Litecoins, a type of digital currency similar to Bitcoin.

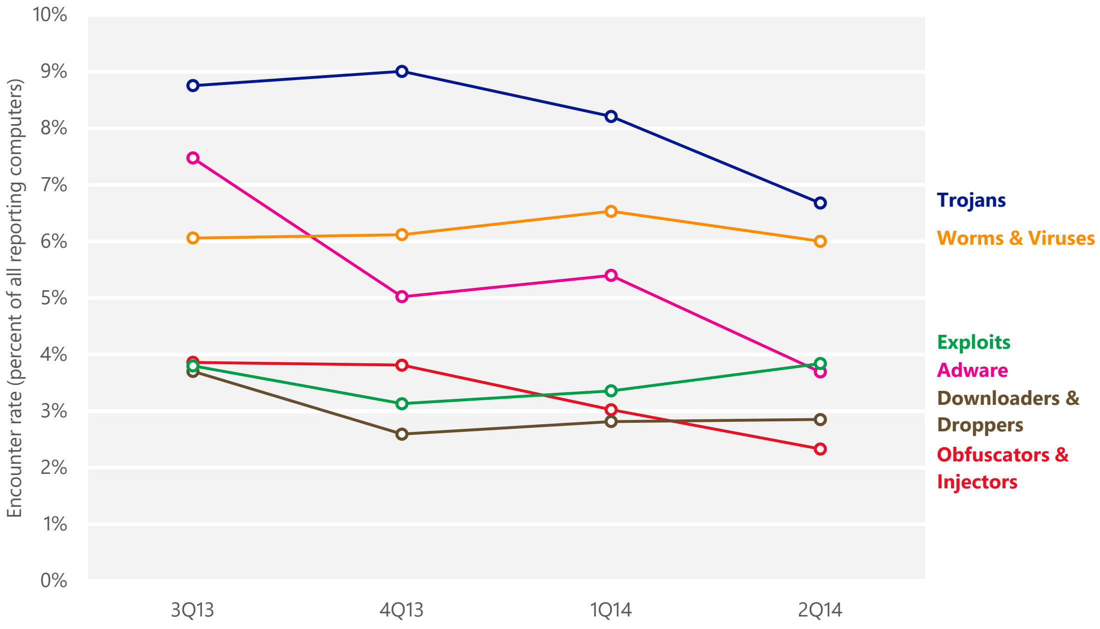
- Despite its physical and cultural distance from the other locations, the threat mix in Japan was fairly similar, with exploit kit families such as Axpergle and adware families such as Win32/AddLyrics leading the detections. Exploit kit-related families were generally more prevalent in Japan than in the other low-detection locations, including JS/Neclu (a detection for the Nuclear exploit kit), HTML/Pangimop (Magnitude), and JS/Urntone (Neutrino).

- The threat mix in China was largely dissimilar to the other locations with low infection rates, led by the password stealer Win32/Frethog. Frethog is a large family of password-stealing trojans that target confidential data such as account information from multiplayer online games, including World of Warcraft, Hao Fang Battle Net, Lineage, and A Chinese Odyssey. The backdoor family Win32/Hupigon was also unusually prevalent in China.

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 39. Encounter rates for significant threat categories, July 2013–June 2014



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

- Totals for each time period may exceed 100 percent because some computers report more than one category of threat in each time period.
- Encounters with most categories of malware decreased or were mostly stable between 1Q14 and 2Q14. Exploits was the only category to show a significant increase, led by JS/Axpergle (a detection for the Angler exploit kit) and JS/Neclu (a detection for the Nuclear exploit kit). See "Exploit kits and

other HTML/JavaScript exploits" on page 46 for more information about these families.

- The Trojans category, the most commonly encountered category in 1H14, decreased in both the first and second quarters of the year, aided by a 61 percent decline in detections of Win32/Wysotot between 4Q13 and 2Q14.
- Encounters involving Adware dropped by nearly a third as several significant adware families retreated from peak levels in 1Q14 or 4Q13, due in part to refined detection criteria. See "Threat families" on page 76 for more information about these families.
- The Backdoors, Password Stealers & Monitoring Tools, Browser Modifiers, Ransomware, and Other Malware categories all remained stable at around 0 to 1 percent each quarter and are not shown in Figure 39.

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 40 shows the relative prevalence of different categories of malware in several locations around the world in 2Q14.

Figure 40. Threat category prevalence worldwide and in the 10 locations with the most computers reporting encounters in 2Q14

Category	Worldwide	United States	Brazil	Russia	Turkey	France	India	Mexico	Germany	Italy	United Kingdom
Trojans	6.7%	3.5%	11.6%	9.7%	25.9%	4.9%	13.4%	8.7%	4.4%	6.0%	3.3%
Worms & Viruses	6.0%	0.9%	12.5%	5.5%	16.4%	2.3%	28.4%	19.4%	1.2%	3.9%	1.1%
Exploits	3.8%	5.0%	3.2%	2.8%	3.0%	3.5%	4.4%	3.1%	3.9%	3.5%	4.9%
Adware	3.7%	3.3%	6.8%	5.5%	5.3%	5.7%	4.2%	5.5%	3.6%	4.7%	3.6%
Downloaders & Droppers	2.9%	1.5%	4.8%	7.3%	4.7%	2.4%	6.3%	3.2%	1.6%	4.9%	2.0%
Obfuscators & Injectors	2.3%	0.9%	3.5%	4.4%	4.8%	1.5%	6.6%	3.1%	1.6%	2.1%	1.4%
Backdoors	1.0%	0.3%	1.2%	1.1%	1.8%	0.7%	2.7%	1.2%	0.5%	0.8%	0.8%
Password Stealers & Monitoring Tools	0.7%	0.6%	1.0%	0.8%	0.9%	0.4%	0.9%	0.7%	0.4%	1.7%	0.6%
Other Malware	0.6%	0.7%	0.7%	0.1%	0.3%	1.8%	0.3%	1.2%	0.7%	0.7%	0.6%
Browser Modifiers	0.3%	0.6%	0.3%	0.1%	0.0%	0.4%	0.1%	0.2%	0.1%	0.2%	0.2%
Ransomware	0.3%	0.3%	0.0%	0.8%	0.2%	0.3%	0.1%	0.2%	0.4%	0.6%	0.4%

Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

- Within each row of Figure 40, 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 33 on page 65, the locations in the table are ordered by number of computers reporting detections in 1H14.

- India experienced higher encounter rates across most threat categories than the other locations in Figure 40.

- Turkey had a particularly high rate of encounters involving the Trojans category, led by Win32/Wysotot, JS/Kilim (for which Turkey accounted for about two-thirds of all encounters in 1H14), and JS/Faceliker.

- The United States and United Kingdom had the highest encounter rates for Exploits, led by increases in JS/Axpergle (a detection for the Angler exploit kit) and JS/Neclu (a detection for the Nuclear exploit kit) in 2Q14. See "Exploit kits and other HTML/JavaScript exploits" on page 46 for more information about these families.
- France had the highest Other Malware encounter rate, led by Win32/OptimizerElite, a misleading program that uses legitimate files in the Prefetch folder to claim that the computer is damaged, and offers to "fix" the damage for a price.

See "Appendix C: Worldwide infection and encounter rates" on page 129 for more information about malware around the world.

Threat families

Figure 41 lists the top 10 malware families that were detected on computers by Microsoft real-time antimalware products worldwide in 1H14, with other quarters included for comparison.

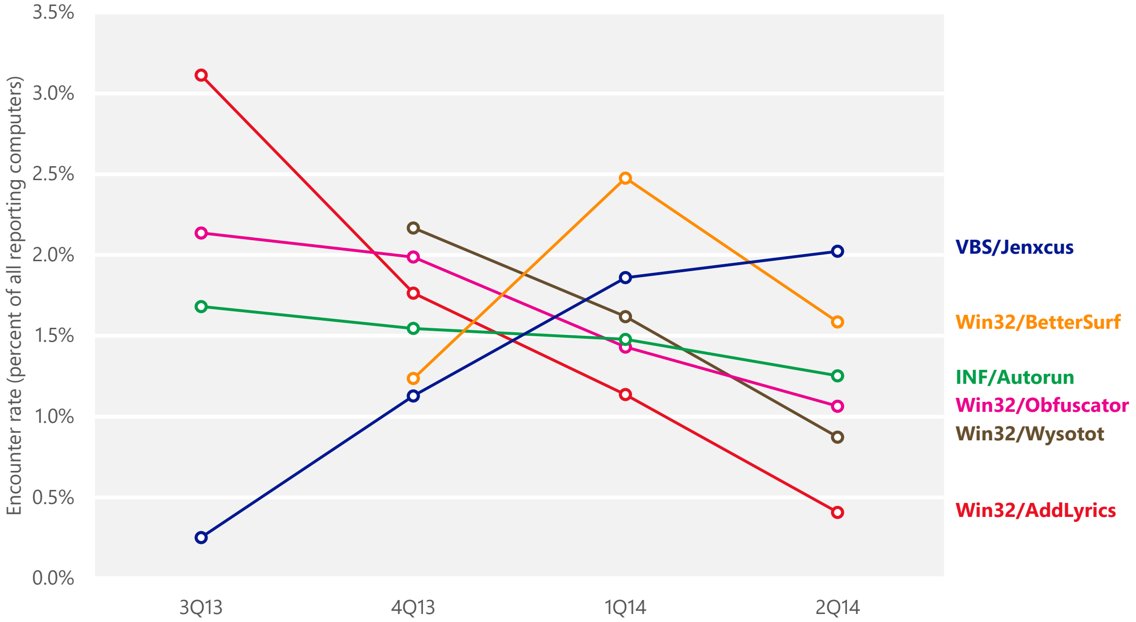
Figure 41. Quarterly trends for the top 10 malware families encountered by Microsoft real-time antimalware products in 1H14, shaded according to relative encounter rate

	Family	Most significant category	3Q13	4Q13	1Q14	2Q14
1	Win32/BetterSurf	Adware	—	1.24%	2.48%	1.59%
2	VBS/Jenxcus	Worms & Viruses	0.25%	1.13%	1.86%	2.02%
3	INF/Autorun	Worms & Viruses	1.68%	1.55%	1.48%	1.25%
4	Win32/Obfuscator	Obfuscators & Injectors	2.14%	1.99%	1.43%	1.06%
5	Win32/Wysotot	Trojans	—	2.17%	1.62%	0.87%
6	Win32/Gamarue	Worms & Viruses	1.37%	1.39%	1.38%	1.10%
7	JS/Axpergle	Exploits	—	—	0.55%	1.04%
8	Win32/Adpeak	Adware	—	—	0.85%	0.71%
9	Win32/AddLyrics	Adware	3.11%	1.76%	1.14%	0.41%
10	JS/Faceliker	Trojans		0.73%	0.86%	0.50%

Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

For a different perspective on some of the changes that have occurred throughout the year, Figure 42 shows the detection trends for a number of malware families that increased or decreased significantly over the past four quarters.

Figure 42. Encounter rate trends for a number of notable malware families, July 2013–June 2014



- Win32/BetterSurf, the most commonly encountered malware family in 1H14 overall and in 1Q14, is an adware family that displays advertisements within websites and search engine results. It first appeared in 4Q13 and peaked at 2.48 percent in 1Q14 before declining to 1.59 percent in 2Q14.
- VBS/Jenxcus, the most commonly encountered malware family in 2Q14 and the second most commonly encountered family in 1H14 overall, 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 Flash Player update from spoofed YouTube web pages. In June, the Microsoft Digital Crimes Unit launched a takedown operation that successfully disrupted the Jenxcus botnet.

> In June, DCU launched a takedown operation that successfully disrupted the Jenxcus botnet.

See "The Microsoft DCU and the legal side of fighting malware" on page 28 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)

- INF/Autorun, the third most commonly encountered threat worldwide during the period, is a generic detection for worms that spread between mounted volumes using the AutoRun feature in some versions of Windows. Changes to the feature have made this technique less effective, but attackers continue to distribute malware that attempts to target it and Microsoft antimalware products detect and block these attempts even when they would not be successful. (See the entry "Defending Against Autorun Attacks" (June 27, 2011) on the Microsoft Cyber Trust blog at blogs.microsoft.com/cybertrust for more information.)
- Win32/Obfuscator, the fourth most commonly encountered threat in 1H14, 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.
- Win32/Wysotot is a family of trojans that change the start page of the user's web browser. It is usually installed by software bundlers that advertise free software or games. Wysotot was first detected in October 2013. For more information about Wysotot, see the entry "MSRT March 2014 – Wysotot" (March 11, 2014) in the MMPC blog at blogs.technet.com/mmpc.
- Win32/Gamarue, the fifth most commonly encountered threat in 1H14, 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)
- JS/Axpergle is a detection for the Angler exploit kit, which exploits vulnerabilities in some versions of Internet Explorer, Microsoft Silverlight,

Adobe Flash Player, and the Java Runtime Environment (JRE). It has been observed downloading Win32/Reveton, a ransomware family. See "Exploit kits and other HTML/JavaScript exploits" on page 46 for more information about Axpergle and other exploit kits.

- Win32/Adpeak and Win32/Addlyrics are adware programs that display unwanted advertisements in various contexts. Adpeak is often called ScorpionSaver; it injects ads into webpages and does not mention where the ads came from. AddLyrics, a browser add-on that displays lyrics to songs when they are viewed on YouTube, also displays its own ads on some web pages. It was highly prevalent in 3Q13 but dropped significantly in every quarter since then.
- JS/Faceliker is a malicious script that performs "likejacking" attacks: it casts Facebook "like" actions in support of certain content without the user's knowledge or consent, which raises the targeted content's profile on the social network but frequently causes embarrassment for the user.

Threat families by platform

Malware does not affect all platforms equally. Some threats are spread by exploits that are ineffective against one or more operating system versions. Some threats are more common in parts of the world where specific platforms are more or less popular than elsewhere. In other cases, differences between platforms may be caused by simple random variation. Figure 43 demonstrates how detections of the most prevalent families in 2Q14 ranked differently on different operating system/service pack combinations.

Figure 43. The malware families most commonly encountered by Microsoft real-time antimalware solutions in 2Q14, and how they ranked in prevalence on different platforms

Rank 2Q14	Family	Most significant category	Rank (Windows Vista SP2)	Rank (Windows 7 SP1)	Rank (Windows 8 RTM)	Rank (Windows 8.1 RTM)
1	VBS/Jenxcus	Worms & Viruses	9	1	1	1
2	Win32/BetterSurf	Adware	2	2	2	4
3	JS/Axpergle	Exploits	47	3	184	10
4	INF/Autorun	Worms & Viruses	11	4	4	3
5	Win32/Obfuscator	Obfuscators & Injectors	1	6	5	2
6	Win32/Gamarue	Worms & Viruses	29	5	3	6
7	Win32/Wysotot	Trojans	3	8	6	8
8	Win32/Clikug	Trojans	7	9	8	5
9	Win32/Adpeak	Adware	5	11	13	7
10	JS/Neclu	Exploits	89	7	202	9

Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

- The list of most commonly encountered families was largely consistent from platform to platform. VBS/Jenxcus was the most commonly encountered family on all supported client versions of Windows except Windows Vista in 2H14. Win32/BetterSurf was the second most common family on all platforms other than Windows 8.1, where it was fourth.

- Microsoft real-time antimalware products detect and block threats that attempt to infect computers even if those attempts would not otherwise succeed. The generic family INF/Autorun, which propagates using a technique that is ineffective on Windows 7, Windows 8, and Windows 8.1, was nevertheless among the most commonly encountered threat family on all three platforms in 2Q14.[31]

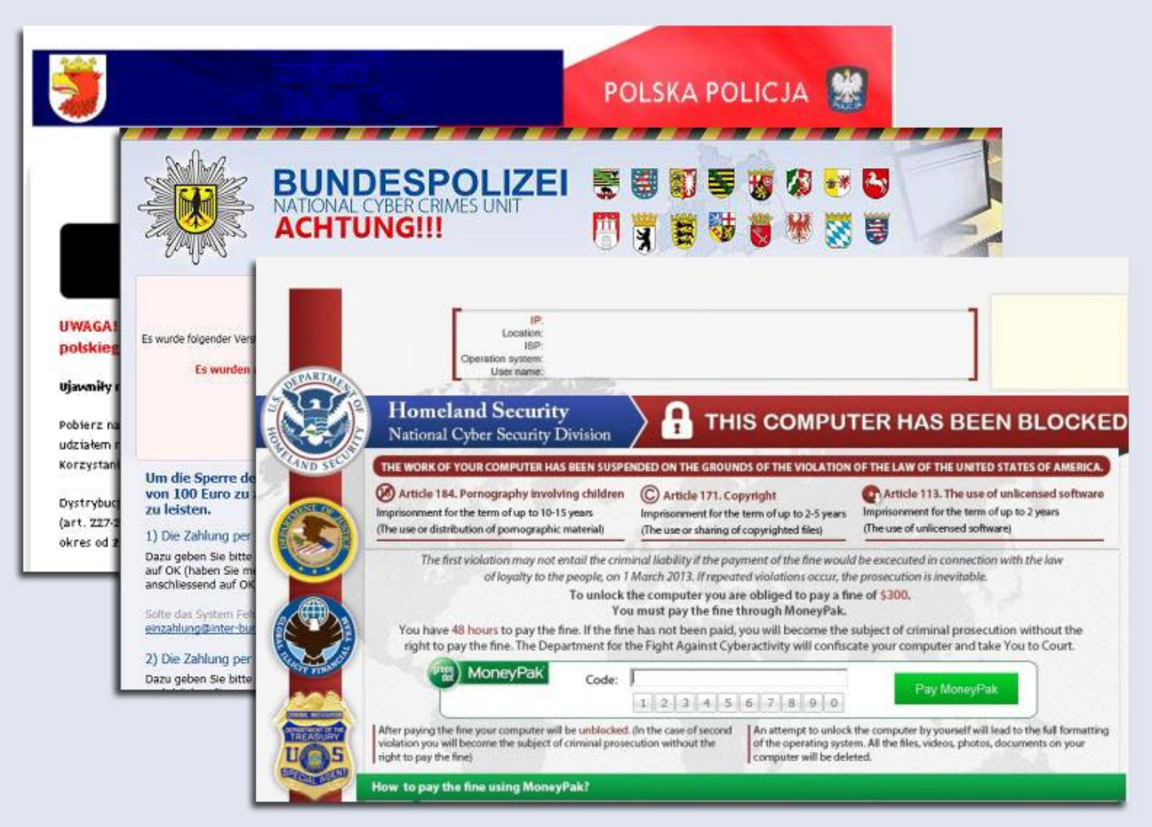
- Two exploit kits, JS/Axpergle and JS/Neclu, had particularly high encounter rates on Windows 7 SP1 and Windows 8.1 due to high adotion rates for Internet Explorer 11, which features improved detection of threats embedded in webpages, on those platforms.

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

Ransomware

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

Figure 44. Examples of the lock screens used by different ransomware families, masquerading as warnings from various national or regional police forces



Homeland Security
National Cyber Security Division

THIS COMPUTER HAS BEEN BLOCKED

THE WORK OF YOUR COMPUTER HAS BEEN SUSPENDED ON THE GROUNDS OF THE VIOLATION OF THE LAW OF THE UNITED STATES OF AMERICA.

Article 184. Pornography involving children
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic material)

Article 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

The first violation may not entail the criminal liability if the payment of the fine would be excecuted in connection with the law of loyalty to the people, on 1 March 2013. If repeated violations occur, the prosecution is inevitable.

To unlock the computer you are obliged to pay a fine of $300.
You must pay the fine through MoneyPak.

You have 48 hours to pay the fine. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer and take You to Court.

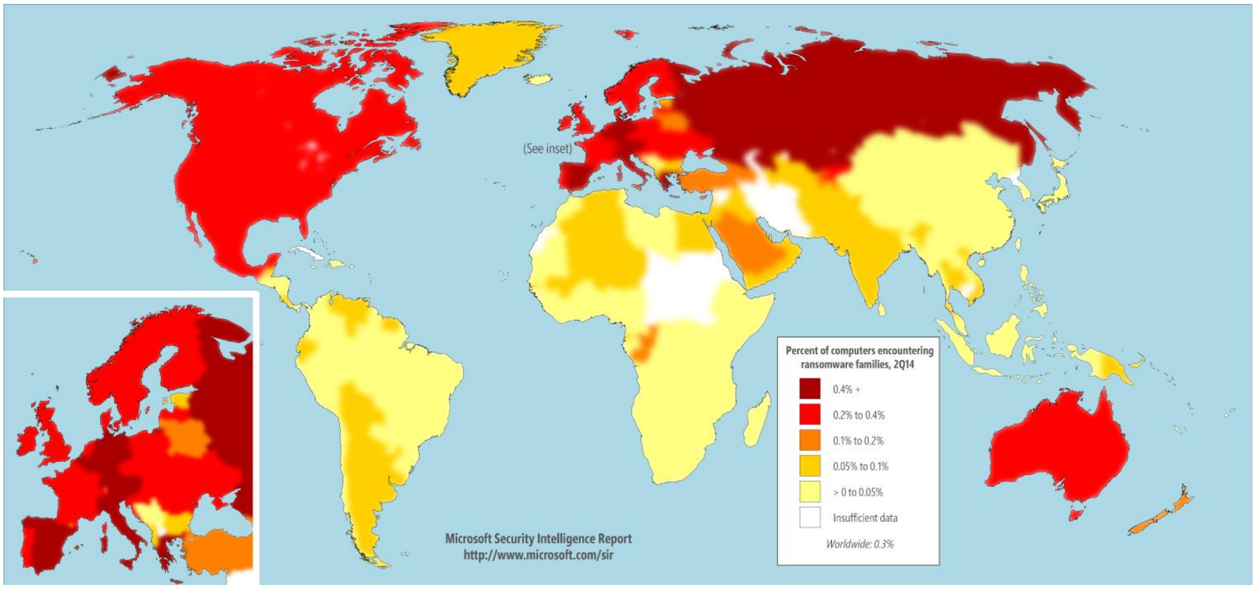
After paying the fine your computer will be unblocked. (In the case of second violation you will become the subject of criminal prosecution without the right to pay the fine)

An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.

How to pay the fine using MoneyPak?

Ransomware affects different parts of the world unequally. Figure 45 shows encounter rates for ransomware families by country and region in 2Q14.

Figure 45. Encounter rates for ransomware families by country/region in 2Q14


(See inset)
Percent of computers encountering ransomware families, 2Q14
0.4% +
0.2% to 0.4%
0.1% to 0.2%
0.05% to 0.1%
> 0 to 0.05%
Insufficient data
Worldwide: 0.3%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

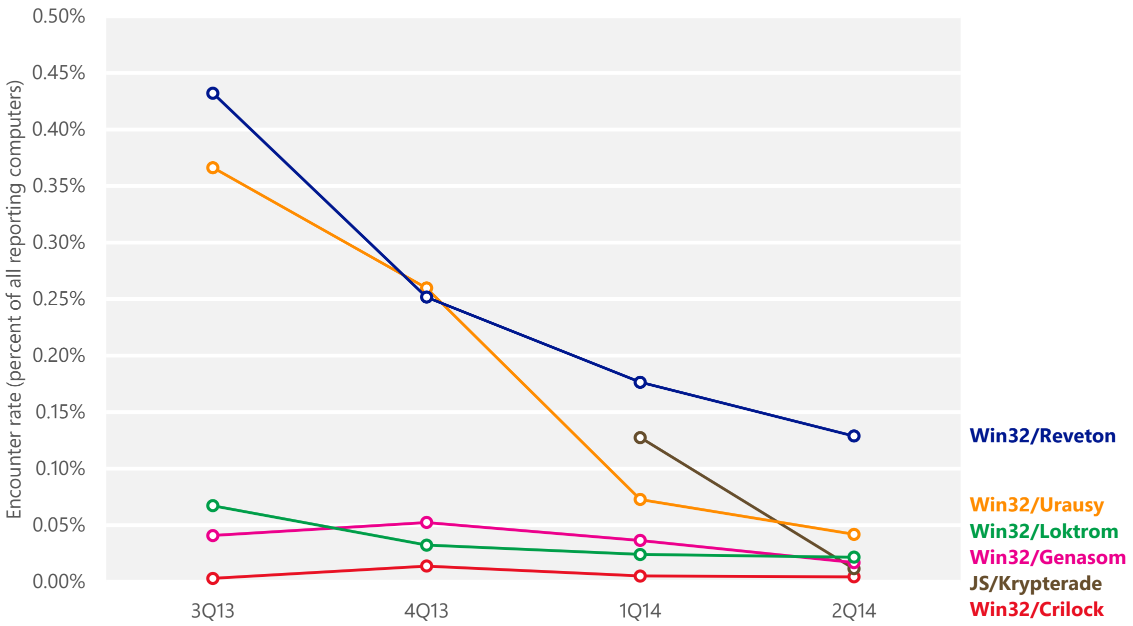
- The location with the highest ransomware encounter rate in 2Q14 was Russia (0.81 percent), followed by Italy (0.59 percent) and Kazakhstan (0.55 percent).

- Unlike with many other types of malware, the distribution of ransomware has been highly concentrated geographically, with almost all ransomware encounters taking place in Europe, western Asia, North America, and Oceania. Ransomware encounters were virtually unknown in Central and South America, Africa, the Middle East, and eastern and southern Asia.

Almost all ransomware encounters took place in Europe, western Asia, North America, and Oceania.

Figure 46 displays encounter rate trends for several of the most commonly encountered ransomware families worldwide.

Figure 46. Trends for several commonly encountered ransomware families in 1H14, by quarter



- Encounter rates for all of the most common ransomware families declined or remained stable in 1H14.

- Win32/Reveton was the most commonly encountered ransomware family worldwide in 1H14. Reveton displays behavior that is typical of many ransomware families: it locks computers, displays a webpage that covers the entire desktop of the infected computer, and demands that the user pay a fine for the supposed possession of illicit material. The webpage that is displayed and the identity of the law enforcement agency that is allegedly responsible for it are often customized, based on the user's current location. Some variants also steal passwords and transmit them to the attacker. Encounter rates for Reveton were highest in Italy (0.48 percent in 2Q14), Spain (0.33 percent), and Austria (0.32 percent).

  For additional information about Reveton, see the following entries in the MMPC blog (blogs.technet.com/mmpc):

  - Revenge of the Reveton (April 18, 2012)
  - No paysafecard needed, your passwords will pay off (May 16, 2013)

- JS/Krypterade, the second most prevalent ransomware family in 1Q14 and in the first half of the year overall, fell to fifth place in 2Q14. The highest

Krypterade encounter rates in 1Q14 were in Spain (0.74 percent), Poland (0.60 percent), and Ireland (0.58 percent).

- Win32/Urausy, the third most prevalent ransomware family worldwide in 1H14, was also most prevalent in Europe, notably in Austria (0.12 percent encounter rate in 2Q14), Belgium (0.10 percent), and Switzerland (0.10 percent).
- Win32/Crilock, also known as Cryptolocker, received significant media attention in 2013 and 2014, but was only the 10th most commonly encountered ransomware family in 1H14, with an encounter rate of 0.004 percent in 2Q14. First detected in September 2013, Crilock is often distributed as an email attachment and can spread to other computers via removable drives. After it is installed, Crilock encrypts files of certain popular types, such as photos and Microsoft Office documents, with a unique public key. It then displays a screen demanding that the computer user pay a ransom by a certain date to receive the private key that will supposedly decode the user's files. If the user does not pay by the deadline, the screen says, the attacker will delete the private key permanently.

  Because removing the Crilock infection from the computer does not decrypt the encrypted files, regular backups are the best way to avoid losing access to important files in the event of an infection from Crilock or a similar threat family. For more information, see the entry "Backup the best defense against (Cri)locked files" (November 19, 2013) on the MMPC blog at blogs.technet.com/mmpc.

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.

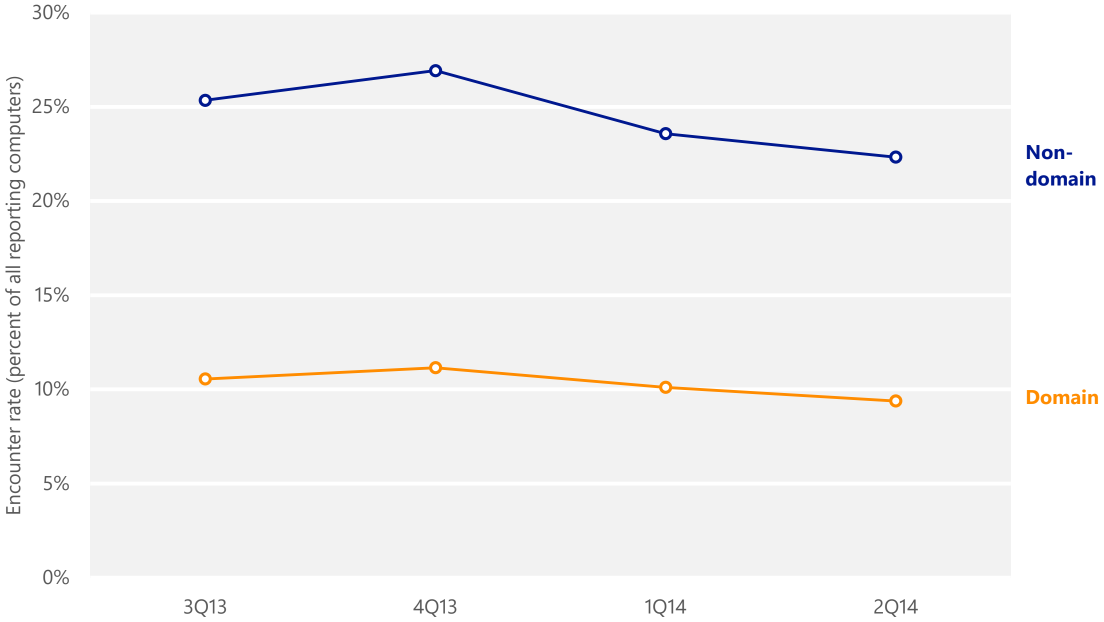
Visit www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx for more information about ransomware and how computer users can avoid being taken advantage of by this type of threat.

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.

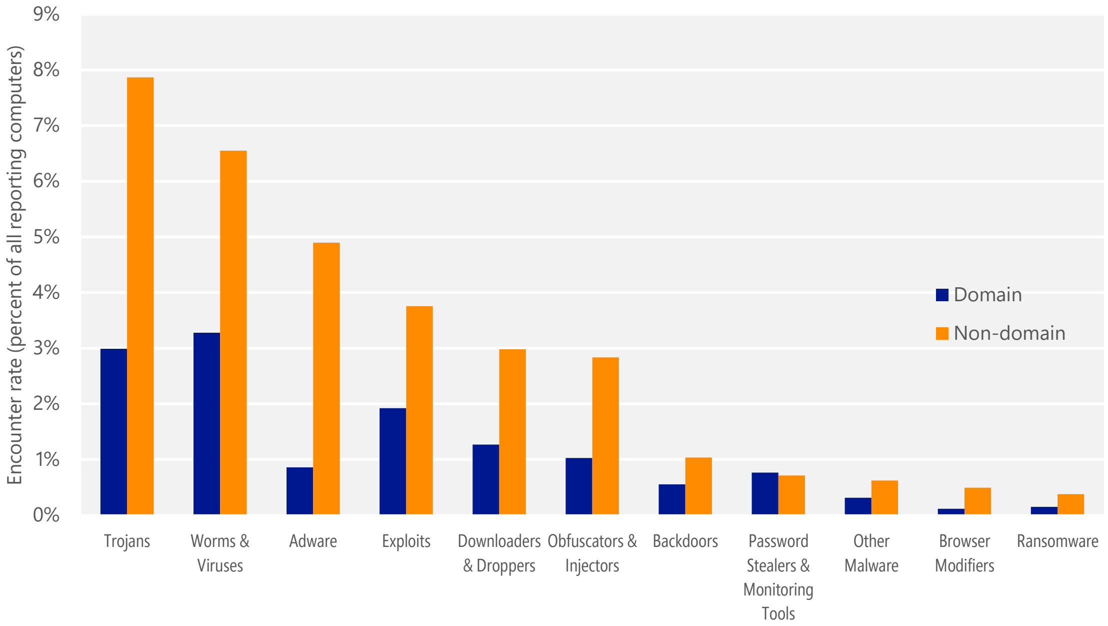
The infection telemetry data produced by Microsoft antimalware products and tools includes information about whether the infected computer belongs to an Active Directory Domain Services (AD DS) domain. Such domains are used almost exclusively in enterprise environments, and computers that do not belong 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 47. Malware encounter rates for domain-based and non-domain computers, 3Q13–2Q14



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

Figure 48. Malware encounter rates for domain-based and non-domain computers, 3Q13–2Q14, by category



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

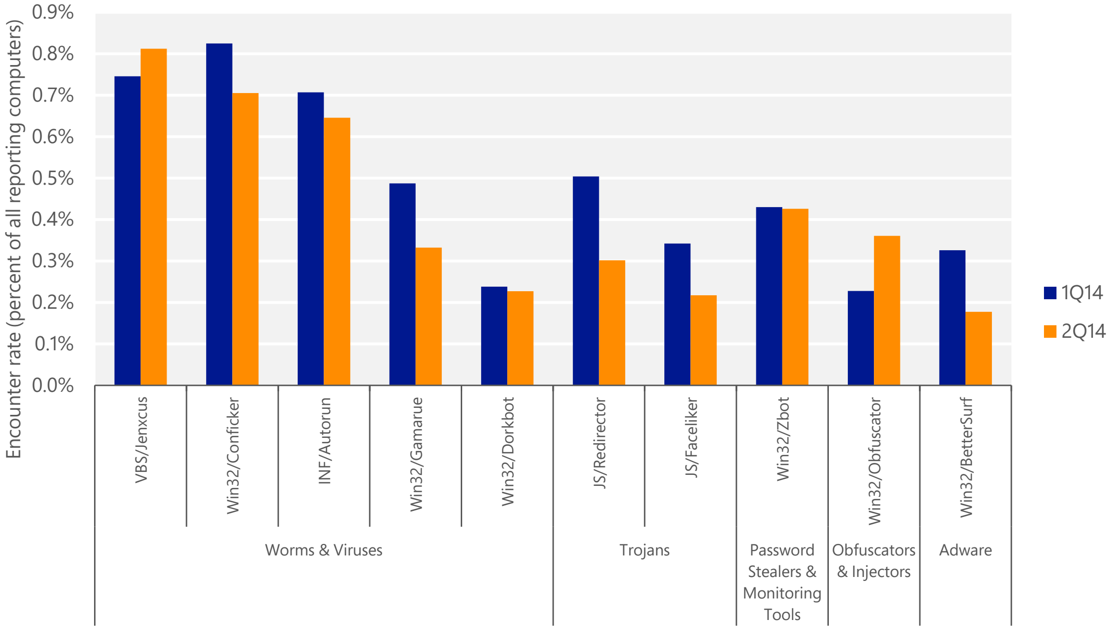
- Enterprise environments typically implement defense-in-depth measures, such as enterprise firewalls, that prevent a certain amount of malware from reaching users' computers. Consequently, enterprise computers tend to encounter malware at a lower rate than consumer computers. As Figure 47 shows, the encounter rate for consumer computers was about 2.4 times as high as the rate for enterprise computers in 1H13.

- 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 48. Non-domain computers encountered disproportionate amounts of malware in the Adware and Browser Modifiers categories, as compared to domain-based computers. Meanwhile, despite encountering less than half as much malware as non-domain computers overall, domain-based computers actually encountered slightly more Password Stealers & Monitoring Tools malware than their non-domain counterparts.

Figure 49 and Figure 50 list the top 10 malware families detected on domain-joined and non-domain computers, respectively, in 1H14.

Figure 49. Quarterly trends for the top 10 malware families detected on domain-joined computers in 1H14, by percentage of computers encountering each family

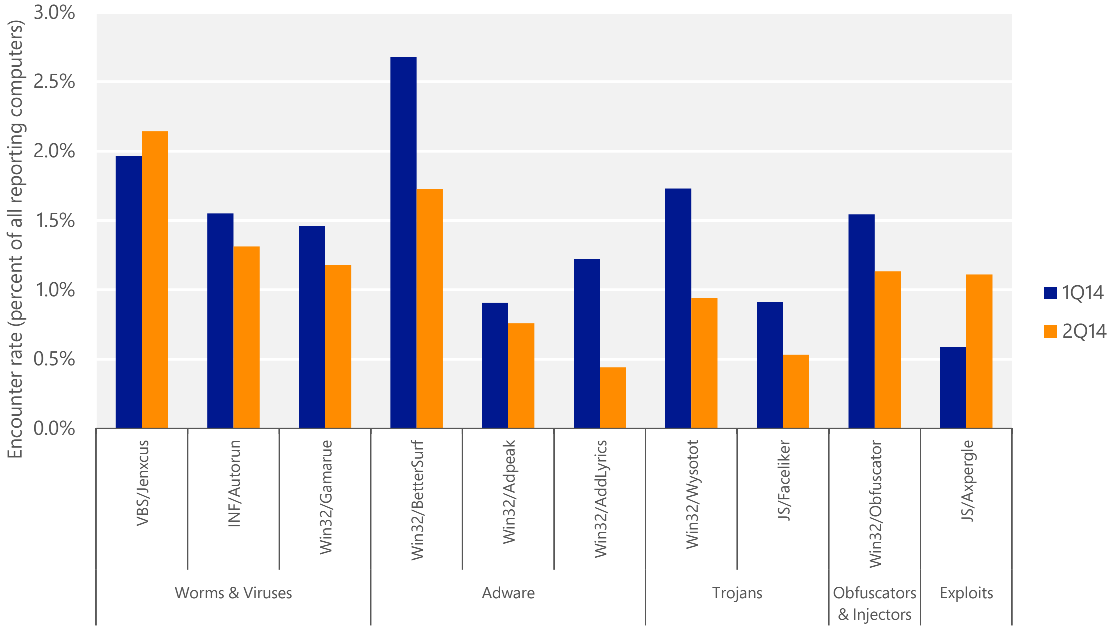
Family	Most significant category	1Q14	2Q14
VBS/Jenxcus	Worms & Viruses	0.75%	0.81%
Win32/Conficker	Worms & Viruses	0.82%	0.70%
INF/Autorun	Worms & Viruses	0.71%	0.65%
Win32/Zbot	Password Stealers & Monitoring Tools	0.43%	0.43%
Win32/Gamarue	Worms & Viruses	0.49%	0.33%
JS/Redirector	Trojans	0.50%	0.30%
Win32/Obfuscator	Obfuscators & Injectors	0.23%	0.36%
JS/Faceliker	Trojans	0.34%	0.22%
Win32/BetterSurf	Adware	0.33%	0.18%
Win32/Dorkbot	Worms & Viruses	0.24%	0.23%



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

Figure 50. Quarterly trends for the top 10 malware families detected on non-domain computers in 1H14, by percentage of computers encountering each family

Family	Most significant category	1Q14	2Q14
Win32/BetterSurf	Adware	2.68%	1.72%
VBS/Jenxcus	Worms & Viruses	1.97%	2.14%
INF/Autorun	Worms & Viruses	1.55%	1.31%
Win32/Obfuscator	Obfuscators & Injectors	1.54%	1.13%
Win32/Wysotot	Trojans	1.73%	0.94%
Win32/Gamarue	Worms & Viruses	1.46%	1.18%
JS/Axpergle	Exploits	0.59%	1.11%
Win32/Adpeak	Adware	0.91%	0.76%
Win32/AddLyrics	Adware	1.22%	0.44%
JS/Faceliker	Trojans	0.91%	0.53%



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

- Six threats—VBS/Jenxcus, INF/Autorun , Win32/Gamarue, Win32/BetterSurf, JS/Faceliker, and Win32/Obfuscator—were common to both lists. All were more frequently encountered on non-domain computers than on domain-joined computers. See "Threat families" on page 76 for more information about these families.

- Five of the top 10 malware families on domain-joined computers are worms that can spread via removable drives, which are commonly used in domain environments. Win32/Conficker and INF/Autorun can also spread via mapped network drives.
- Malware families on the list for domain-joined computers but not for non-domain computers include the worms Conficker and Win32/Dorkbot; JS/Redirector, a generic detection for trojans that redirect the browser to an unexpected web page; and Win32/Zbot, a password stealing trojan that also has backdoor functionality.
- Malware families on the list for non-domain computers but not for domain-joined computers include adware families Win32/Adpeak and Win32/AddLyrics; Win32/Wysotot, a family of trojans that change the start page of the user's web browser; and JS/Axpergle, a detection for the Angler exploit kit.

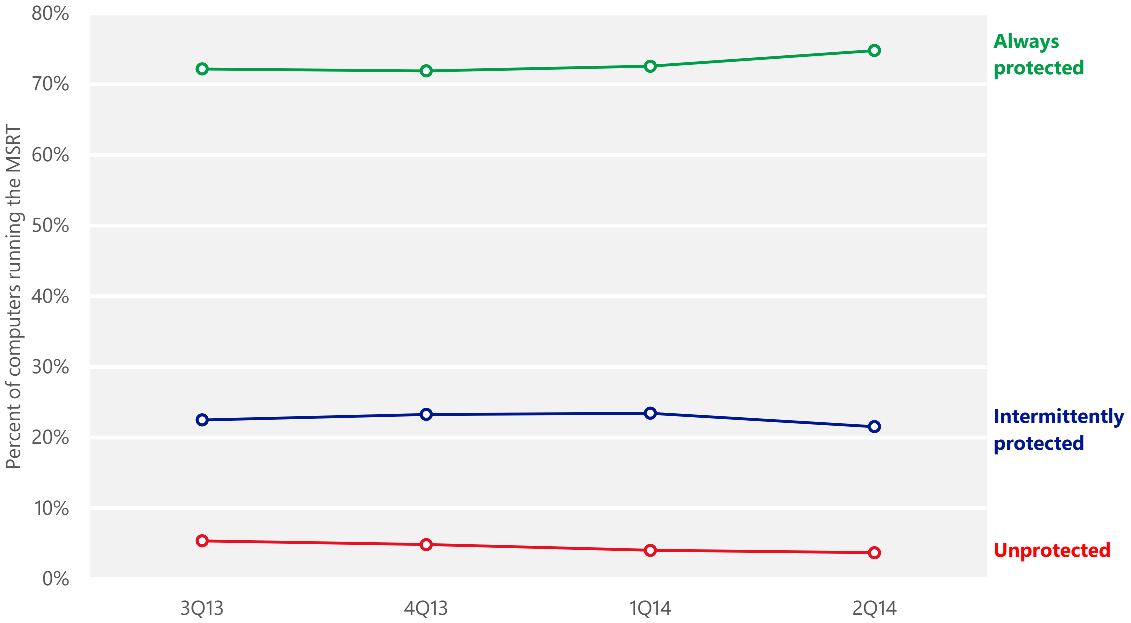
> Five of the top 10 malware families on domain-joined computers are worms that can spread via removable drives.

See "Malware at Microsoft: Dealing with threats in the Microsoft environment" on page 111 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 the 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 51 shows the percentage of computers worldwide that the MSRT found to be protected or unprotected by real-time security software each quarter in 2013.

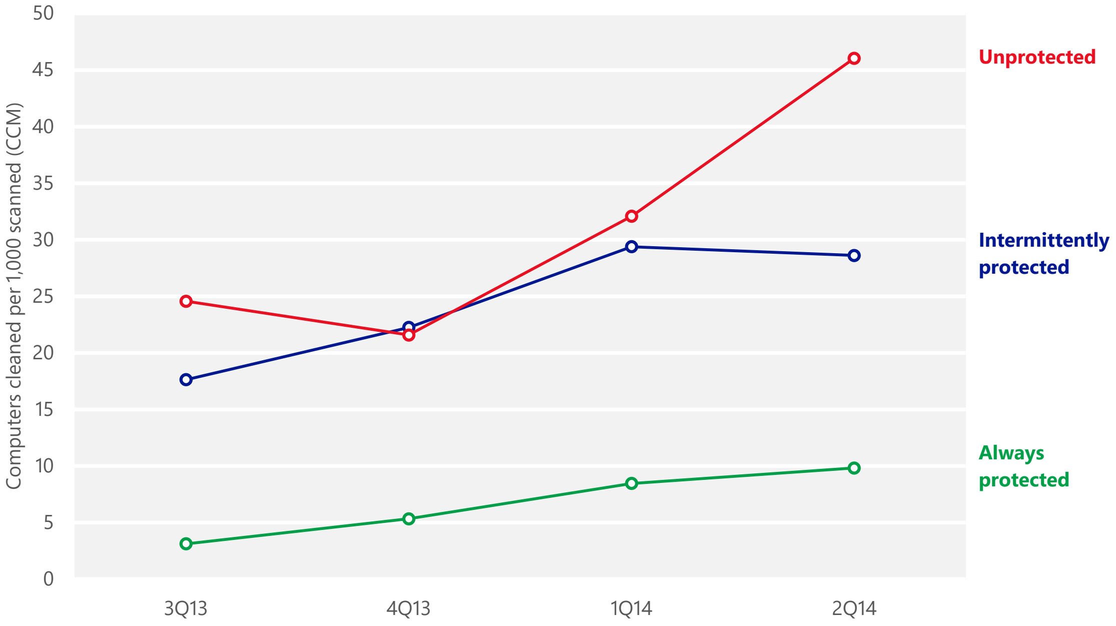
Figure 51. Percentage of computers worldwide protected by real-time security software, July 2013–June 2014



- A typical computer runs the MSRT three times each quarter, once for each monthly version of the tool that Microsoft releases. In Figure 51, "Always 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; and "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. The trend increased slightly over the four quarters, from 72.2 percent in 3Q13 to 74.8 percent in 2Q14.
- Of the computers that did not always have active protection, most were found to be running real-time security software during at least one of their three monthly MSRT executions. Intermittently protected computers accounted for between 21.5 and 23.4 percent of computers worldwide each quarter, and computers that never reported running security software accounted for between 3.7 and 5.4 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 52 compares infection rates with protection levels worldwide for each of the last four quarters.

Figure 52. Infection rates for protected and unprotected computers, July 2013–June 2014



Figures do not include Brantall, Rotbrow, and Filcout. See "The Sefnit saga: a timeline" on page 57 for more information.

- The MSRT reported that computers that were never found to be running real-time security software during 1H14 were about four 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 as likely to be infected with malware in 1H14 as computers that were always protected—a ratio nearly as great as that for computers that were always unprotected.
- 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 may disable or uninstall security software intentionally because of perceived performance issues, a belief that protection is not necessary, or a desire to run programs that would be quarantined or removed by security software. In other cases, users lose up-to-date real-time protection when

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

they don’t renew paid subscriptions for their antimalware software, which may come pre-installed with their computers as limited-time trial software. (See “The challenge of expired security software” on page 21 for more information about 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 52 illustrates.

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.

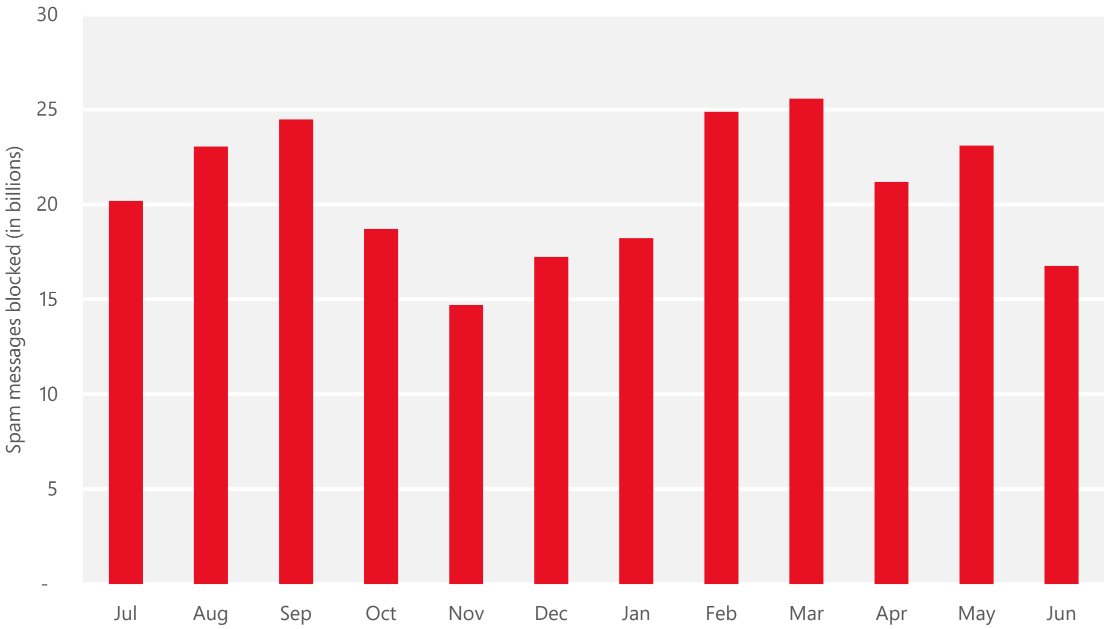
Email threats

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

Spam messages blocked

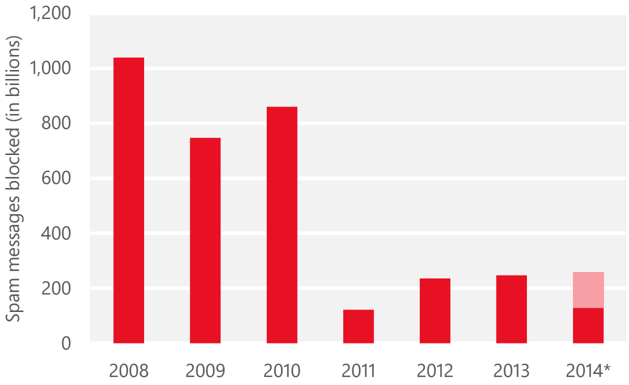
The information in this section of the *Microsoft Security Intelligence Report* is compiled from telemetry data provided by Exchange Online Protection, which provides spam, phishing, and malware filtering services. Exchange Online Protection is used by tens of thousands of Microsoft enterprise customers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

Figure 53. Messages blocked by Exchange Online Protection, July 2013–June 2014, by month



- Blocked mail volumes in 1H14 were consistent with 2H13, and remain well below levels seen prior to the end of 2010, as shown in Figure 54. The

Figure 54. Messages blocked by Exchange Online Protection each year, 2008–2014



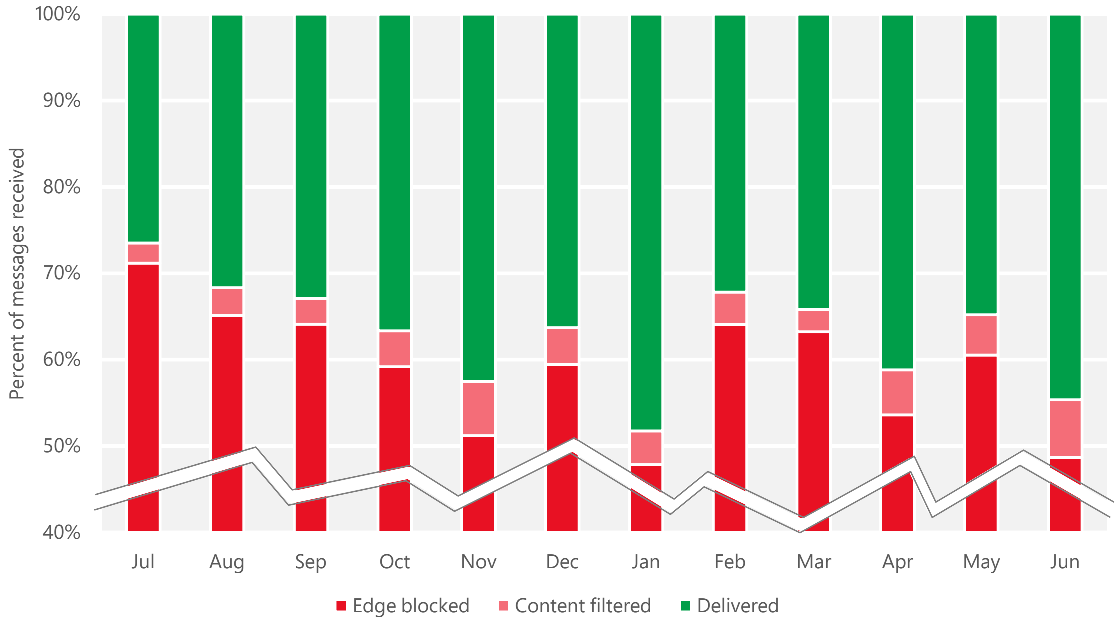
* Projected

dramatic decline in spam observed since 2010 has occurred in the wake of successful takedowns of a number of large spam-sending botnets, notably Cutwail (August 2010) and Rustock (March 2011).[32] In 1H14, Exchange Online Protection determined that about one in three email messages did not require blocking or filtering, compared to just one in 33 messages in 2010.

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

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

Figure 55. Percentages of incoming messages blocked, content filtered, and delivered, each month from July 2013 to June 2014



- Between 47.8 and 64.3 percent of incoming messages were blocked at the network edge each month in 1H14, which means that only 35.9 to 52.2 percent of incoming messages had to be subjected to the more resource-intensive content filtering process. Between 7.1 and 12.9 percent of the remaining messages (2.6 to 6.6 percent of all incoming messages) were filtered as spam each month.

Guidance: Defending against threats in email

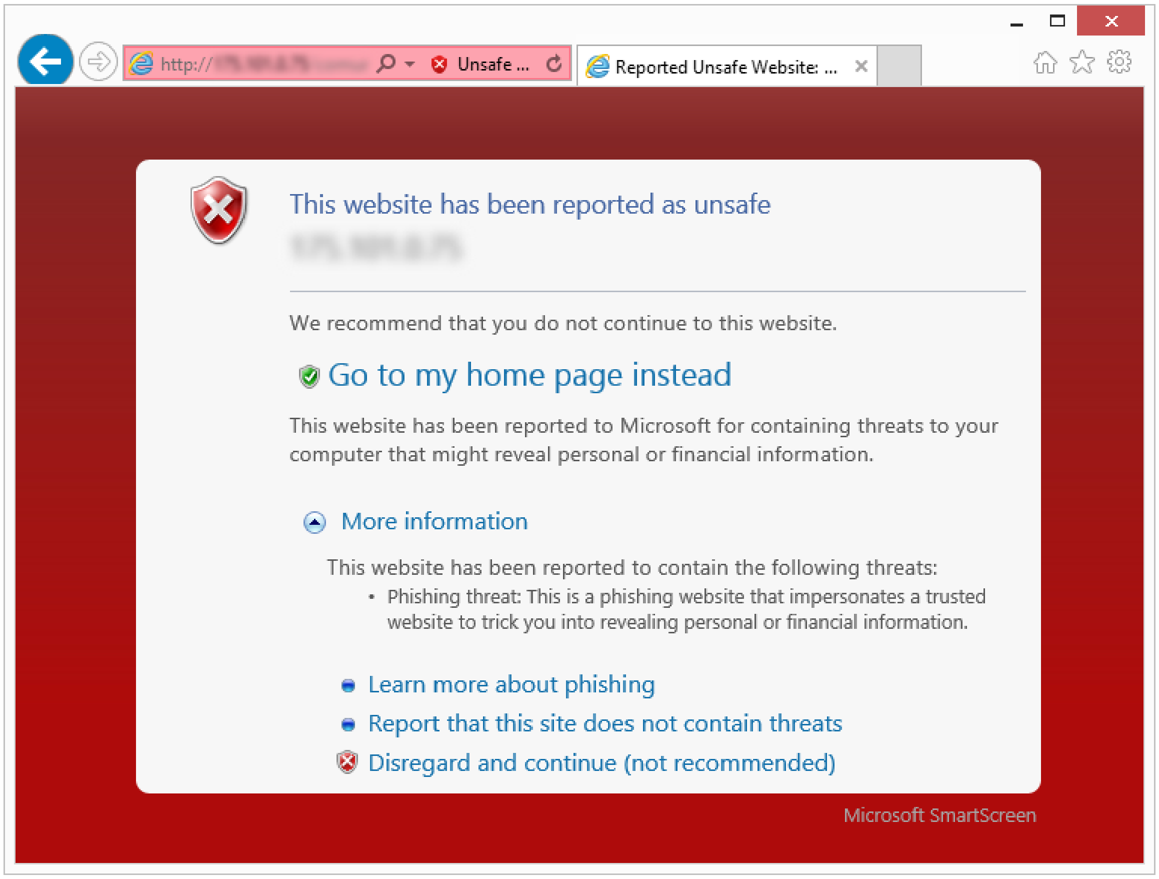
Exchange Online Protection users should see Best practices for configuring EOP at Microsoft TechNet for guidance about implementing email authentication techniques, setting anti-spam options, and other steps to reduce the risks and inconvenience of unwanted email.

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 Windows Internet Explorer versions 8 through 11) 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 127 for more information about the products and services that provided data for this report.)

Figure 56. SmartScreen Filter in Internet Explorer blocks reported phishing and malware distribution sites to protect users



This website has been reported as unsafe

[redacted]

We recommend that you do not continue to this website.

Go to my home page instead

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

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.

- Learn more about phishing
- Report that this site does not contain threats
- Disregard and continue (not recommended)

Microsoft SmartScreen

Phishing sites

Microsoft gathers information about phishing sites and impressions from *phishing impressions* that are generated by users who choose to enable the Phishing Filter or SmartScreen Filter in Internet Explorer.[33] A phishing impression is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being warned, as illustrated in Figure 57.

[33] See "Appendix B: Data sources" on page 127 for information about the products and services used to provide data for this report.

Figure 57. 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. SmartScreen Filter in Internet Explorer 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.

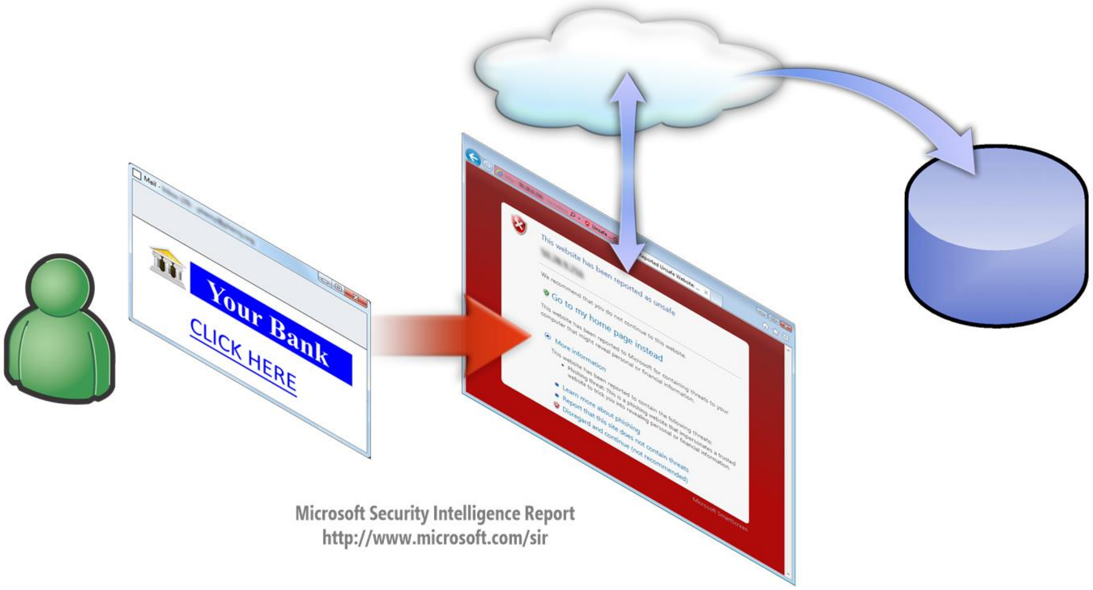
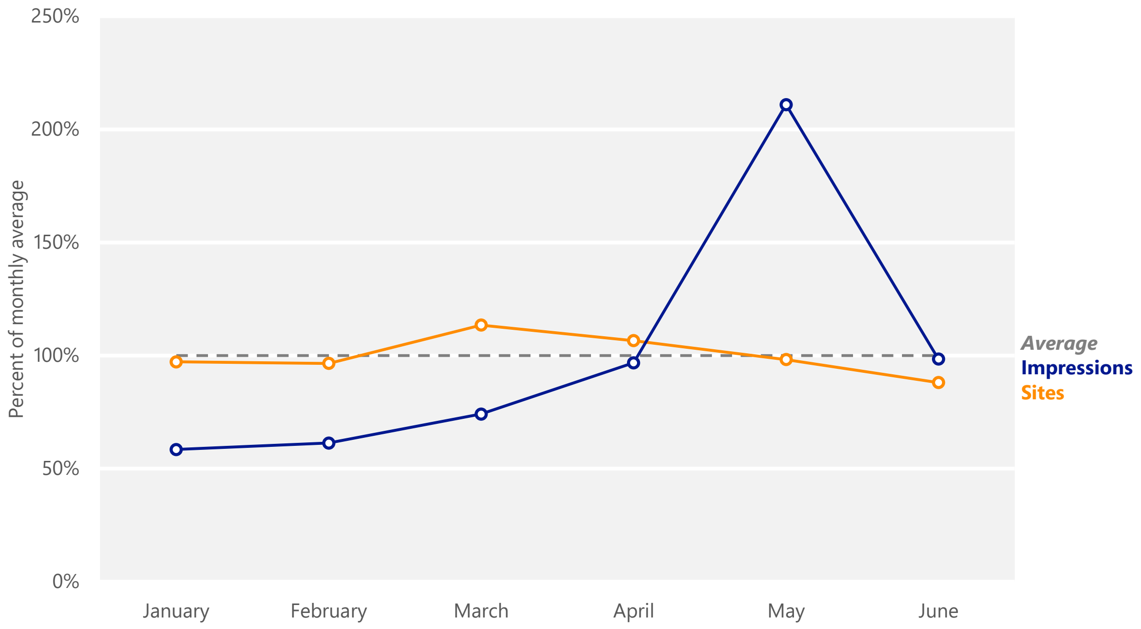

Your Bank
CLICK HERE
This website has been reported as unsafe
Go to my home page instead
More information
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Figure 58 illustrates the volume of phishing impressions tracked by SmartScreen Filter each month in 1H14 across all devices and on mobile devices running Windows Phone 8, compared to the volume of distinct phishing URLs visited.

Figure 58. Phishing sites and impressions reported by SmartScreen Filter across all devices, January–June 2014, relative to the monthly average for each



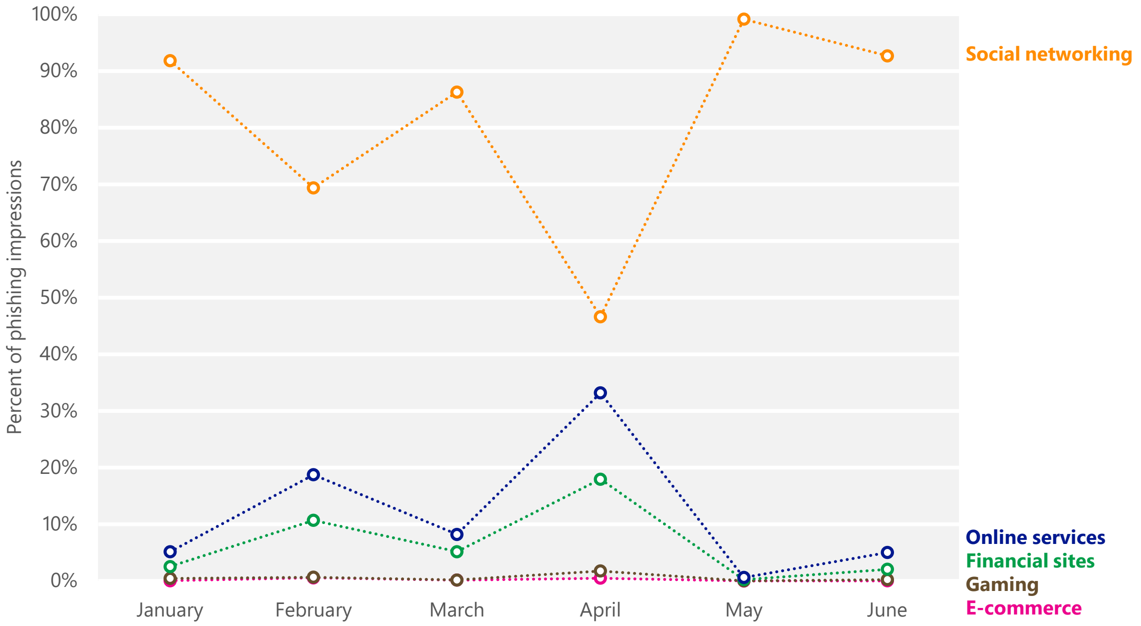
- The numbers of active phishing sites and impressions rarely correlate strongly with each other. Phishers sometimes engage in campaigns that temporarily drive more traffic to each phishing page without necessarily increasing the total number of active phishing pages they maintain at the same time. A likely example of this can be seen in May, when the number of phishing impressions briefly rose to more than twice of their overall monthly average before decreasing to more typical levels the following month. When possible, Microsoft reaches out to institutions that are targeted by significant phishing campaigns to offer advice and assistance for helping users remain protected from phishing attempts.
- At the same time, the number of active phishing sites monitored by Microsoft actually decreased slightly between April and May. Overall, phishing site counts were quite stable from month to month, never deviating from the monthly average by more than about 14 percent.

Numbers of active phishing sites and impressions rarely correlate strongly with each other.

Target institutions

Some types of sites tend to consistently draw many more impressions per site than others. Figure 59 shows the breakdown of mobile phishing impressions by category as reported by Internet Explorer running on Windows Phone 8.

Figure 59. Impressions reported by SmartScreen Filter on Windows Phone 8 for each type of phishing site, January–June 2014

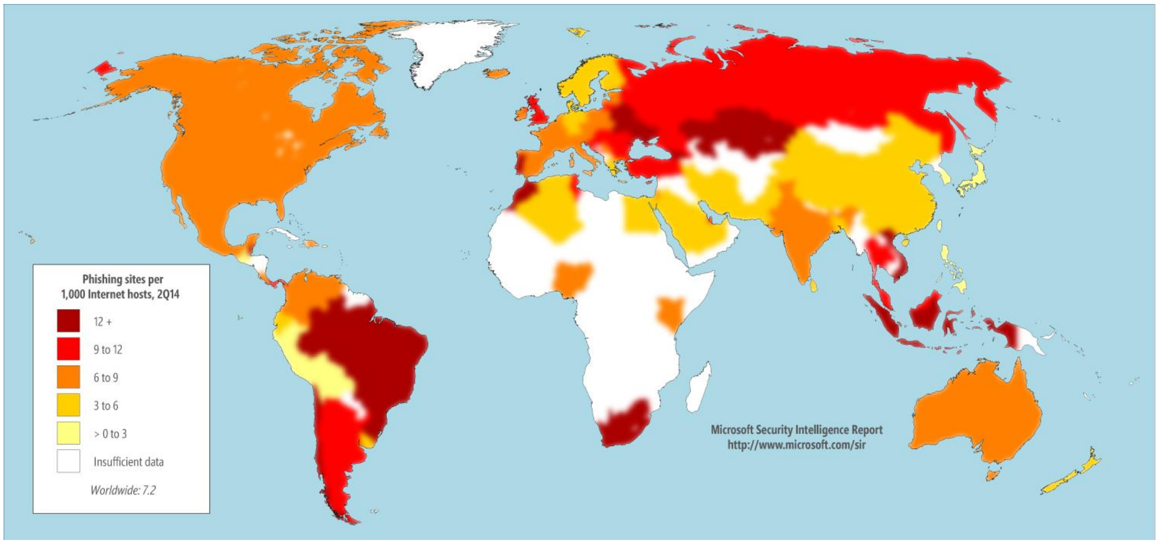


- Phishing attempts that target social networks are usually responsible for the majority of mobile phishing impressions, probably because of the popularity of such sites on mobile platforms. Social network phishing attempts accounted for more than two-thirds of Windows Phone 8 phishing impressions each month in 1H14 except April, when temporary increases in financial and online service impressions brought social network impressions to less than half of the total. In May, phishing attempts accounted for 99.2 percent of all phishing impressions on Windows Phone 8.
- Phishing sites targeting online services and financial sites accounted for the bulk of URLs visited, with all of the other categories combined accounting for less than 10 percent of the total each month.

Global distribution of phishing sites and clients

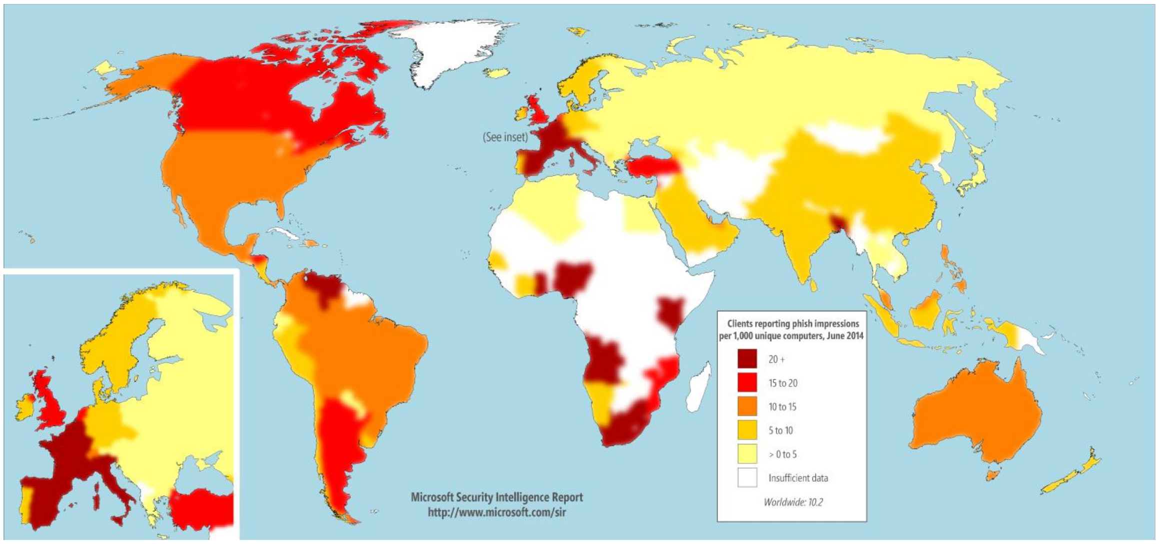
Phishing impression information from SmartScreen Filter includes anonymized information about the IP addresses of the clients making the reports, as well as the IP addresses of the phishing sites themselves. Performing geographic lookups on these addresses makes it possible to analyze patterns among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

Figure 60. Phishing sites per 1,000 Internet hosts for locations around the world in 2Q14


Phishing sites per 1,000 Internet hosts, 2Q14
12 +
9 to 12
6 to 9
3 to 6
> 0 to 3
Insufficient data
Worldwide: 7.2
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- SmartScreen Filter detected 5.8 phishing sites per 1,000 Internet hosts worldwide in 1Q14, and 7.2 per 1,000 in 2Q14.
- Locations hosting higher than average concentrations of phishing sites include Ukraine (29.9 per 1,000 Internet hosts in 2Q14), Brazil (15.8), and South Africa (13.2). Locations with low concentrations of phishing sites include Japan (1.8), Taiwan (1.8), and Korea (2.0).

Figure 61. Computers reporting phishing impressions per 1,000 unique client IP addresses in June 2014

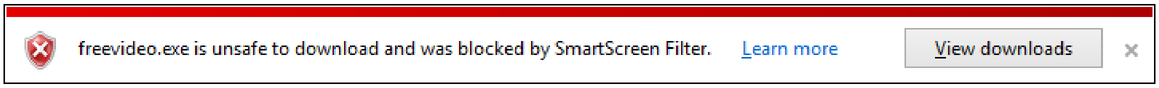

(See inset)
Clients reporting phish impressions per 1,000 unique computers, June 2014
20 +
15 to 20
10 to 15
5 to 10
> 0 to 5
Insufficient data
Worldwide: 10.2
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- SmartScreen Filter reported 10.2 phishing attempts per 1,000 unique IP addresses in June 2014.
- Computers in Western Europe were disproportionately affected by phishing attempts. Four of the 10 locations reporting more than 20 phishing impressions per 1,000 unique IP addresses in June 2014 were in Western Europe: Italy (35.0), France (27.3), Belgium (26.1), and Spain (23.4). Other locations reporting high rates of phishing impressions include Venezuela (24.9) and South Africa (22.0).
- Locations with unusually low rates of phishing impressions include Korea (0.6 impressions per 1,000 unique IP addresses in June 2014), Taiwan (1.6), and Russia (2.2).

Malware hosting sites

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

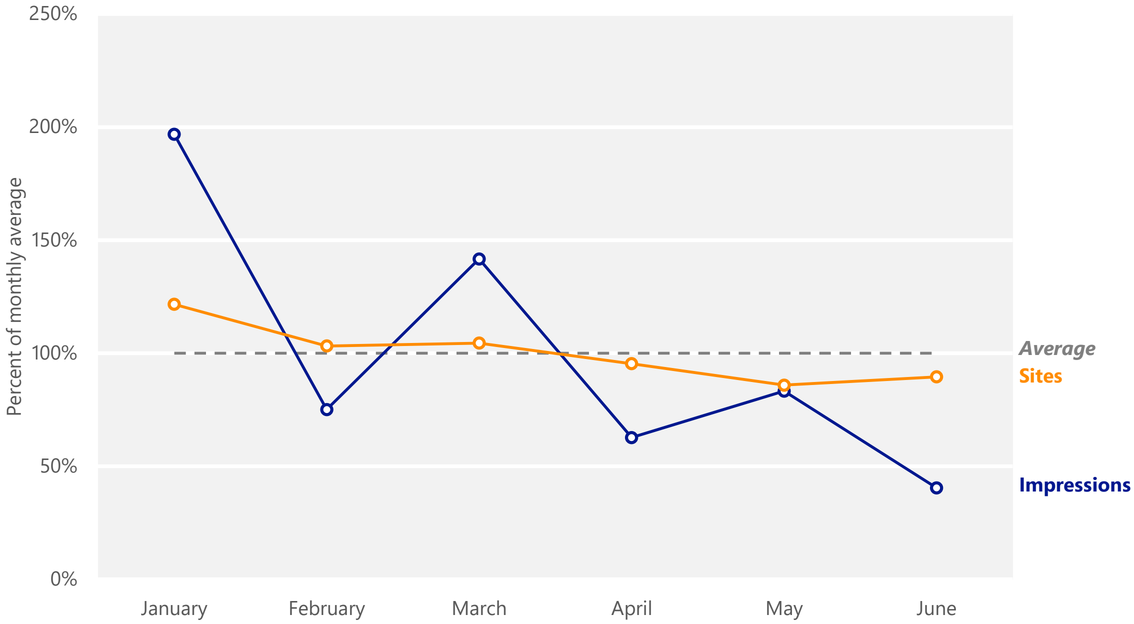
Figure 62. SmartScreen Filter in Internet Explorer displays a warning when a user attempts to download an unsafe file



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

Figure 63 compares the volume of active malware hosting sites in the Microsoft database each month with the volume of malware impressions tracked by Internet Explorer.

Figure 63. Malware hosting sites and impressions tracked each month in 1H14, relative to the monthly average for each



- As with phishing sites, malware hosting impressions don't often correlate strongly with numbers of active sites. The number of impressions generally decreased over the course of the period, but fluctuated widely from month to month; they decreased by more than half in February and April but nearly doubled in March. The number of active sites also generally decreased over the period, but month-to-month differences were much lower.

Malware categories and families

Figure 64 and Figure 65 show the types of threats hosted at URLs that were blocked by SmartScreen Filter in 1H14.

Figure 64. Categories of malware found at sites blocked by SmartScreen Filter in 1H14, by percent of all impressions

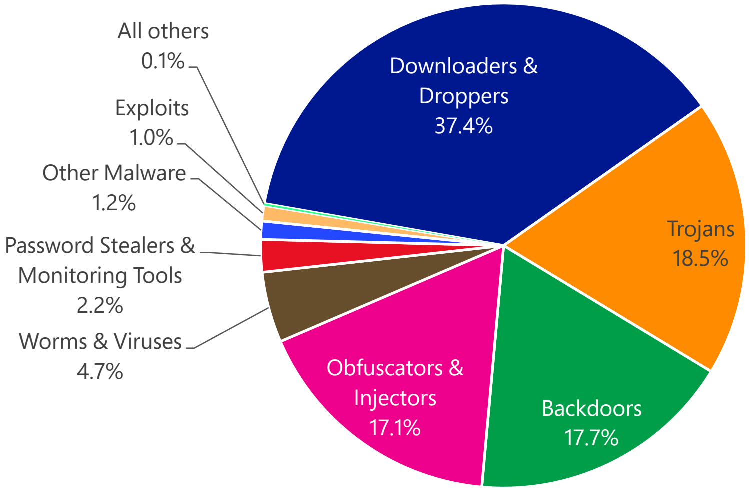


Figure 65. Top malware families found at sites blocked by SmartScreen Filter in 1H14, by percent of all malware impressions

	Family	Most significant category	% of malware impressions
1	Win32/Bdaejec	Backdoors	14.84%
2	Win32/Dowque	Downloaders & Droppers	14.66%
3	Win32/Microjoin	Downloaders & Droppers	14.33%
4	Win32/DelfInject	Obfuscators & Injectors	13.28%
5	Win32/Obfuscator	Obfuscators & Injectors	2.94%
6	Win32/Oceanmug	Downloaders & Droppers	2.86%
7	Win32/VB	Worms & Viruses	2.82%
8	Win32/Dynamer	Trojans	2.50%
9	Win32/Sisproc	Trojans	1.44%
10	Win32/Meredrop	Trojans	1.15%
11	Win32/Startpage	Trojans	1.10%
12	Win32/Bumat	Trojans	1.04%
13	Win32/Zegost	Backdoors	0.99%
14	Win32/Orsam	Trojans	0.96%
15	Win32/Banload	Downloaders & Droppers	0.90%

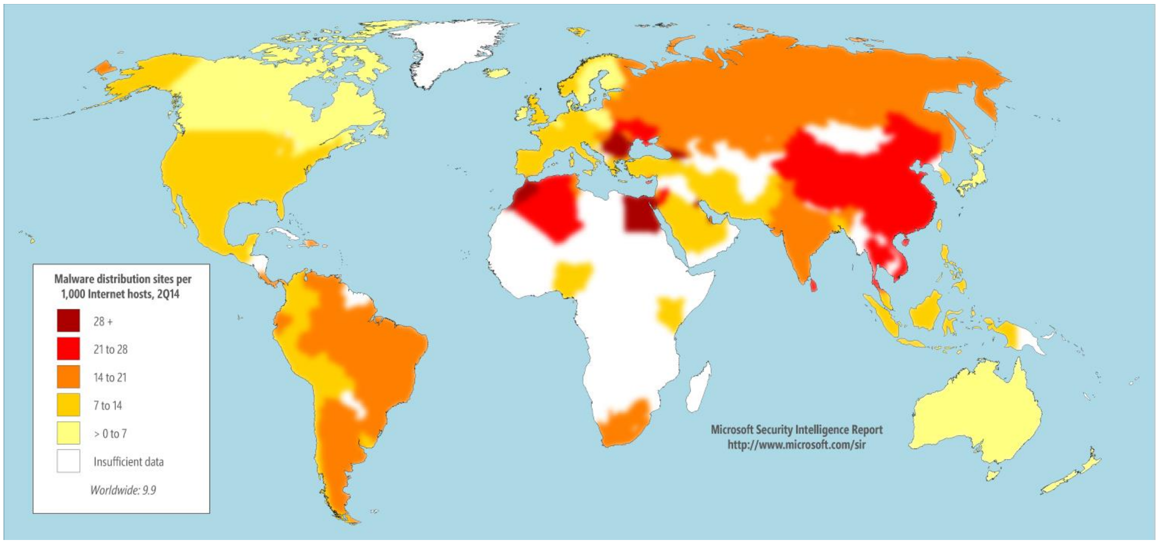
- Many of the malware families on the list are generic detections for a variety of threats that share certain identifiable characteristics.

- Win32/Bdaejec, the malware family associated with the most malware impressions in 1H14, is a trojan that allows unauthorized access and control of an affected computer, and that may download and install other programs without consent. Bdaejec was found at 14.8 percent of malware hosting sites in 1H14, down from 27.8 percent in 2H13.
- Win32/Dowque, the malware family associated with the second largest number of malware impressions in 1H14, is a generic detection for malicious files that are capable of installing other malware. Dowque ranked 7th on this list in 2H12, but did not appear on the list in 1H13 or 2H13.
- Win32/Microjoin was in third place with 14.33 percent, an increase from 8.25 percent in 2H13. Microjoin is a generic detection for tools that bundle malware files with clean files in an effort to deploy malware without being detected by security software.
- Other families that are new to the 1H14 list include Win32/VB, Win32/Sisproc, and Win32/Zegost.
- Families that were on the 2H13 list but not the 1H14 list include Win32/Delf (responsible for the second largest number of malware impressions in 2H13), Win32/Comame, AndroidOS/CVE-2011-3874, and VBS/Psyme.

Global distribution of malware hosting sites and clients

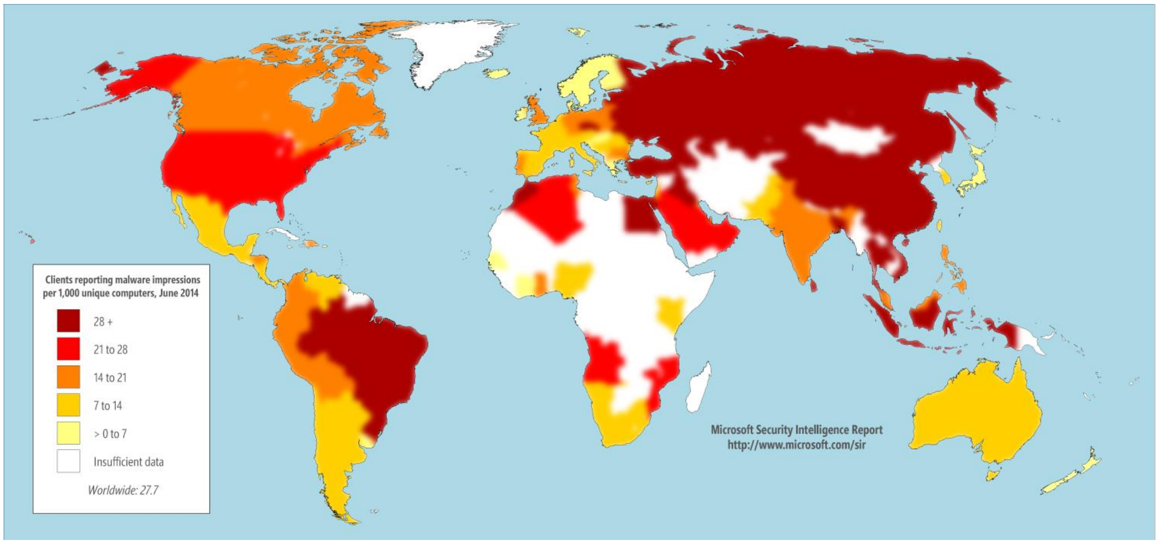
Figure 66 and Figure 67 show the geographic distribution of malware hosts and computers reporting impressions in 1H14.

Figure 66. Malware distribution sites per 1,000 Internet hosts for locations around the world in 2Q14


Malware distribution sites per 1,000 Internet hosts, 2Q14
28 +
21 to 28
14 to 21
7 to 14
> 0 to 7
Insufficient data
Worldwide: 9.9
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- SmartScreen Filter detected 12.1 malware hosting sites per 1,000 Internet hosts worldwide in 1Q14, and 9.9 per 1,000 in 2Q14.
- China, which had a lower than average concentration of phishing sites (3.2 phishing sites per 1,000 Internet hosts in 2Q14), also had a high concentration of malware hosting sites (22.6 malware hosting sites per 1,000 hosts in 2Q14). Other locations with large concentrations of malware hosting sites included Romania (31.1), Thailand (24.4), and Russia (18.9). Locations with low concentrations of malware hosting sites included Japan (4.2), Sweden (4.3), and Poland (5.7).

Figure 67. Clients reporting malware impressions per 1,000 unique client IP addresses in June 2014


Clients reporting malware impressions per 1,000 unique computers, June 2014
28 +
21 to 28
14 to 21
7 to 14
> 0 to 7
Insufficient data
Worldwide: 27.7
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

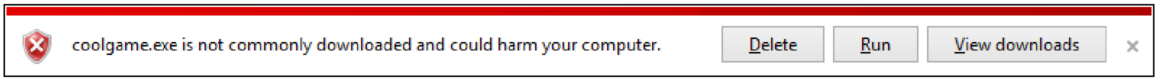
- SmartScreen Filter reported 27.7 malware impressions per 1,000 unique IP addresses in June 2014.
- Geographic patterns for malware impressions were very different from those for phishing impressions. Countries and regions in Western Europe that were heavily affected by phishing impressions, such as Italy, France, and Spain, had malware impression rates that were much lower than average. By contrast, several prominent locations that had very high malware impression rates, such as Russia, Ukraine, and Belarus, also had very low phishing impression rates.
- Locations that were heavily affected by malware impressions included Russia (106.5 malware impressions per 1,000 unique IP addresses in June 2014), Turkey (71.0), and China (54.9).

- Locations with unusually low malware impression rates included Finland (4.1), Japan (4.4), and Hungary (5.9).

Application reputation

Malware creators work hard at evading detection by conventional security measures, and attackers place a premium on threats that won't be detected by the most current signature files published by security software vendors. Therefore, in addition to blocking the download of files that are known to be harmful, SmartScreen Filter includes an application reputation feature that warns the user before downloading a program file that is not commonly downloaded.

Figure 68. SmartScreen Filter in Internet Explorer displays a warning when a user attempts to download an unknown or uncommon program



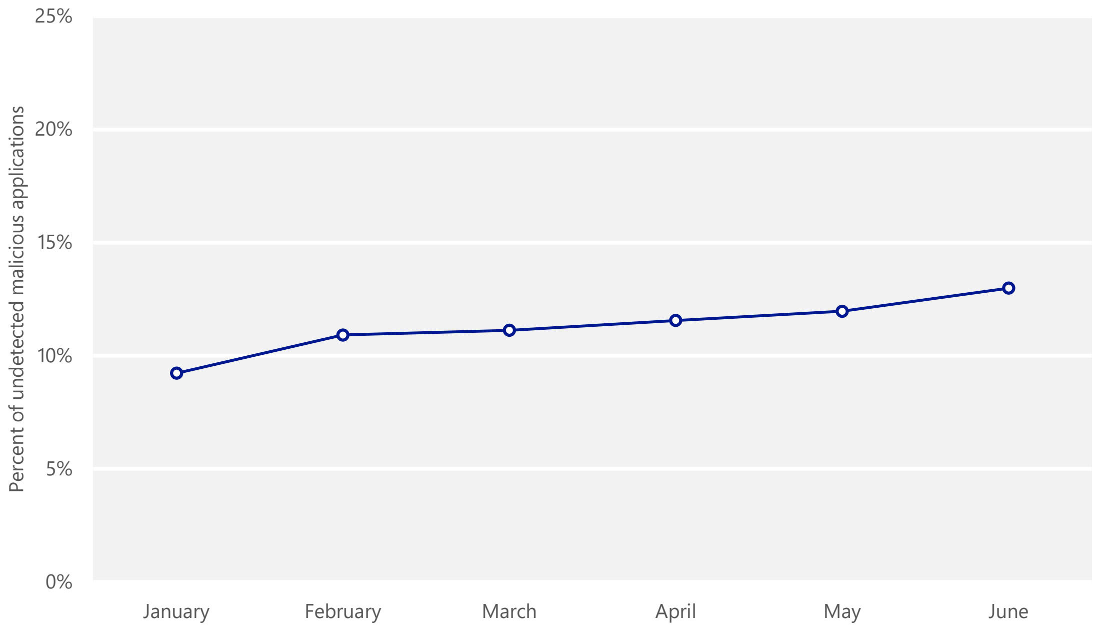
coolgame.exe is not commonly downloaded and could harm your computer.

SmartScreen Filter uses file hashes and (for signed applications) digital signatures to determine whether a given program has been widely downloaded, and displays a warning if the program is unknown or uncommon. As with reported phishing and malware hosting URLs, the hash and certificate details are recorded in a database for later analysis. If an application is determined to be malicious, SmartScreen uses the stored hash and certificate information to block additional downloads, as shown in Figure 62 on page 102. Between 20 and 40 percent of downloaded files that do not have established reputations are eventually classified as malicious, so users should give serious consideration to the application reputation warning when it appears.

Users tend to make the correct decision when faced with undetected malicious programs.

As shown in Figure 69, which illustrates user reaction to unknown and uncommon downloads that are later determined to be malicious, users tend to make the correct decision when faced with undetected malicious programs.

Figure 69. Percent of uncommon applications that were later determined to be malware that users chose to run each month in 1H14



- Warning users about unfamiliar applications has proven to be an effective way to alert users to the presence of malware. As Figure 69 shows, when confronted with a warning about an unknown or uncommonly downloaded application that was later determined to be malware, users correctly avoided downloading and running the application close to nine-tenths of the time.
- More than 89 percent of Internet Explorer users did not see any unknown application alerts in 1H14.

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.

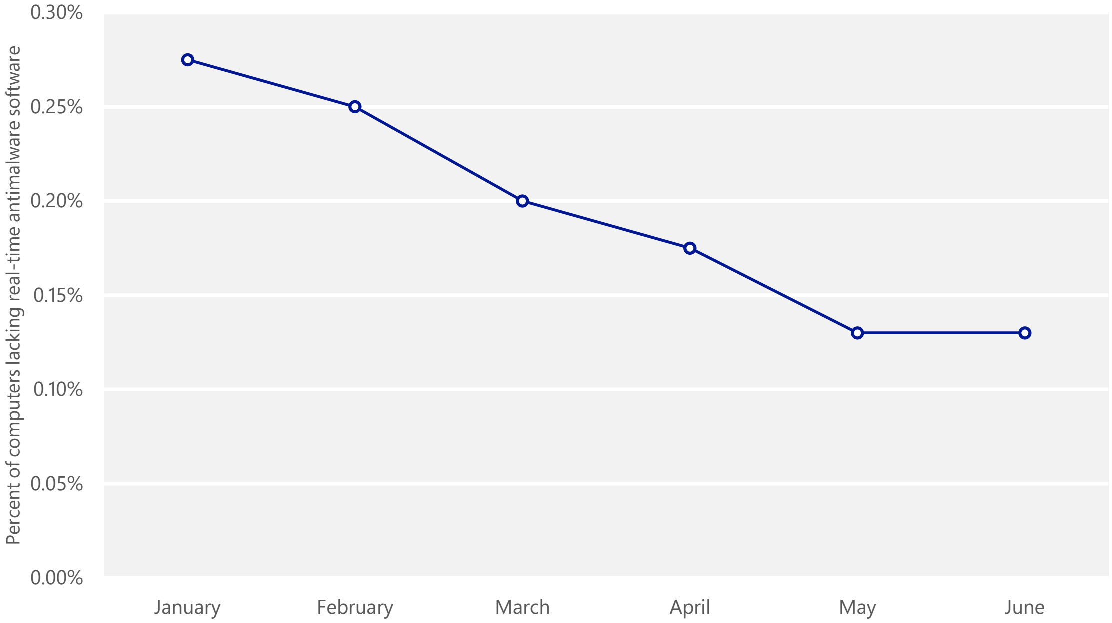
This section of the report compares the potential impact of malware to the levels of antimalware compliance from more than 500,000 workstation computers and servers managed by Microsoft IT between January and June 2014. This data is compiled from multiple sources, including System Center Endpoint Protection (SCEP), Windows Defender, Network Access Protection, DirectAccess, and manual submission of suspicious files. Comparing the nature and volume of the malware detected on these computers to the level of protection they receive can illustrate significant trends and 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) is the antimalware solution 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 client, antimalware signatures must be no more than six days old, and real-time protection must be enabled.

Figure 70 shows the level of antimalware noncompliance in the Microsoft user workstation environment for each month in 1H14.

Figure 70. Percentage of computers at Microsoft not running real-time antimalware software in 1H14



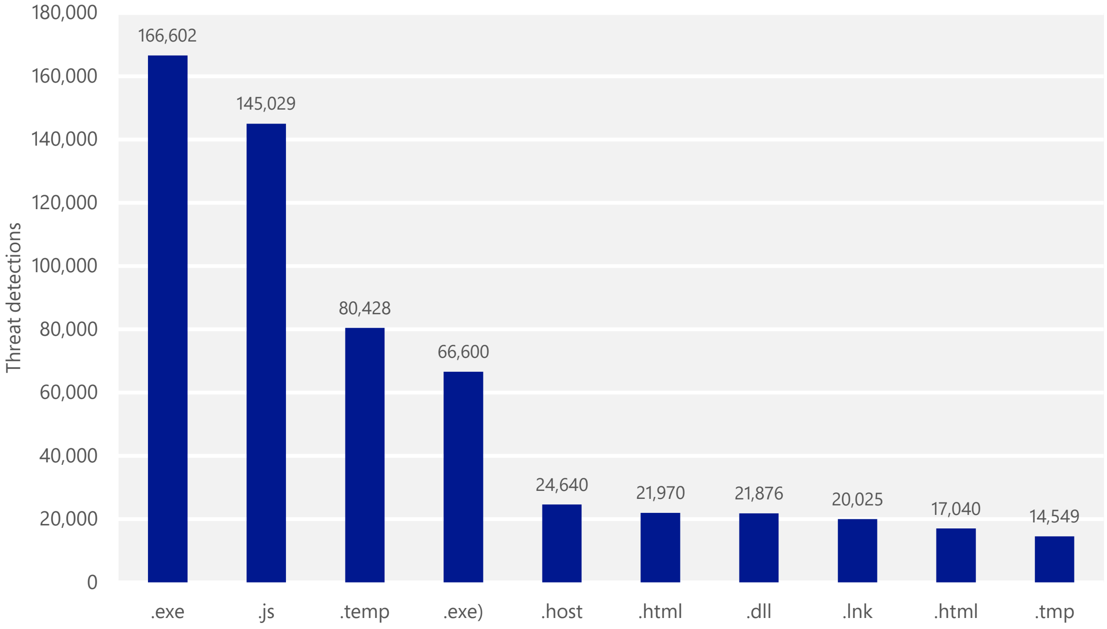
The noncompliance rate dropped by more than half during the first half of the year, from 0.28 percent in January to 0.13 percent in May and June, primarily because of continual refinement of the Microsoft IT toolset. At an average of less than one-third of one percent noncompliance during the six-month period, the antimalware compliance rate at Microsoft is very high. In any network of this size, it is almost inevitable that a small number of computers will be in a noncompliant state at any given time. In most cases, these are computers that are being rebuilt or are otherwise in a state of change when online, rather than computers that have had their antimalware software intentionally disabled. Microsoft IT believes that a compliance rate in excess of 99 percent among 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

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.)

Figure 71 shows the top 10 file types among threat detections at Microsoft in 1H14.

Figure 71. Threat detections at Microsoft in 1H14, by file type



Executable program files with the .exe extension were the most commonly detected type of malicious file at Microsoft, accounting for about 29 percent of all file detections. Malicious JavaScript files with the .js extension were the next most common type of threat, followed by .temp files. Interestingly, malicious files with the extension ".exe)" accounted for the fourth largest number of threats detected. Attackers may be using this approach to avoid being blocked by email systems that automatically block .exe files in incoming messages.

Transmission vectors

Examining the processes targeted by malware can help illustrate the methods that attackers use to propagate it. Figure 72 lists the top five transmission vectors used by the malware encountered at Microsoft in 1H14.

Figure 72. The top five transmission vectors used by malware encountered at Microsoft in 1H14

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

The transmission vector most commonly used by infection attempts detected on Microsoft computers in 1H14 involved file transfers made through Windows Explorer, followed by file transfer applications, including peer-to-peer (P2P) applications. Attempts to deliver malware through the user's web browser accounted for the third most common transmission vector, followed by non-Microsoft software and email.

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 SCEP does disinfect a computer, it is usually because its signature database has been updated to enable it to detect a threat that it did not recognize when the computer first encountered the threat. This lack of recognition may be because the threat is a new malware family, a new variant of a known family, a known variant that has been encrypted or otherwise repackaged to avoid detection, or because of some other reason. The MMPC constantly analyzes malware samples submitted to it, develops appropriate detection signatures, and deploys them to customers who use SCEP, Microsoft Security Essentials, and Windows Defender.

Figure 73 shows the top 10 file types used by malware to infect computers at Microsoft in 1H14.

Figure 73. Infections and removals at Microsoft in 1H14, by file type

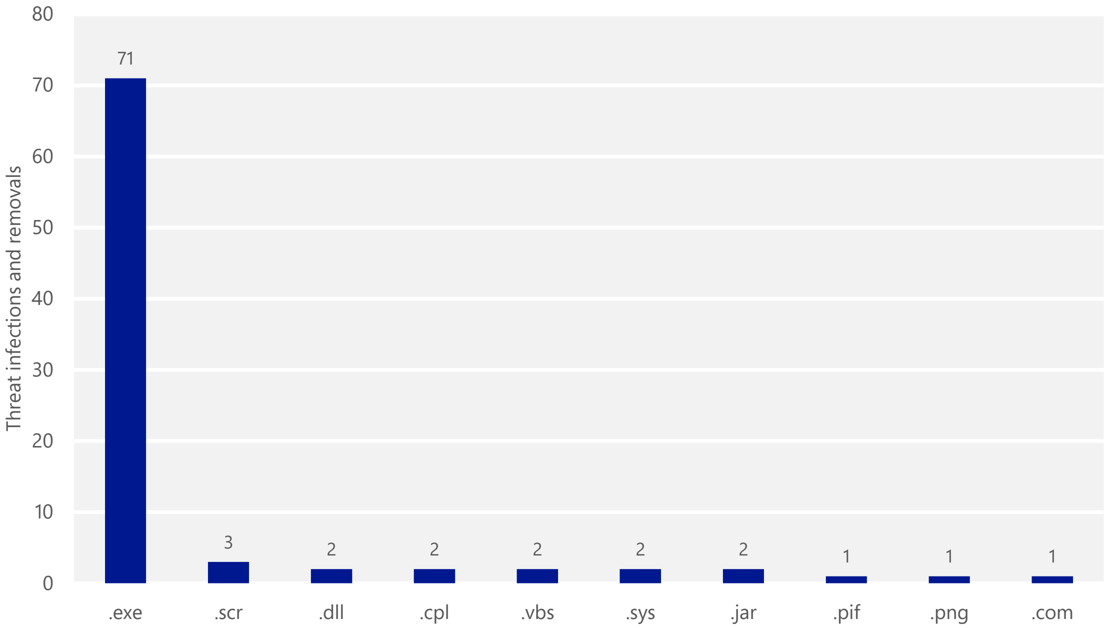


Figure 73 is important because it provides information about threats that SCEP did not detect when they were first encountered—and therefore provides a clue about the areas in which malware authors have been focusing their efforts in recent months. Seventy-one of the 87 malicious files removed from computers at Microsoft by SCEP in 1H14 had the extension .exe, used by executable program files, with nine extensions accounting for the remaining files. By contrast, the .dll extension, which denotes dynamic-link library files, was the most commonly used file type among successful infections at Microsoft in 2Q13, with .exe a distant second.

What IT departments can do to minimize these trends

- 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 and SmartScreen Filter. See Knowledge Base article KB328010 at support.microsoft.com 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.
- 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) to minimize exploitation of vulnerabilities in all manufactured software. 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.

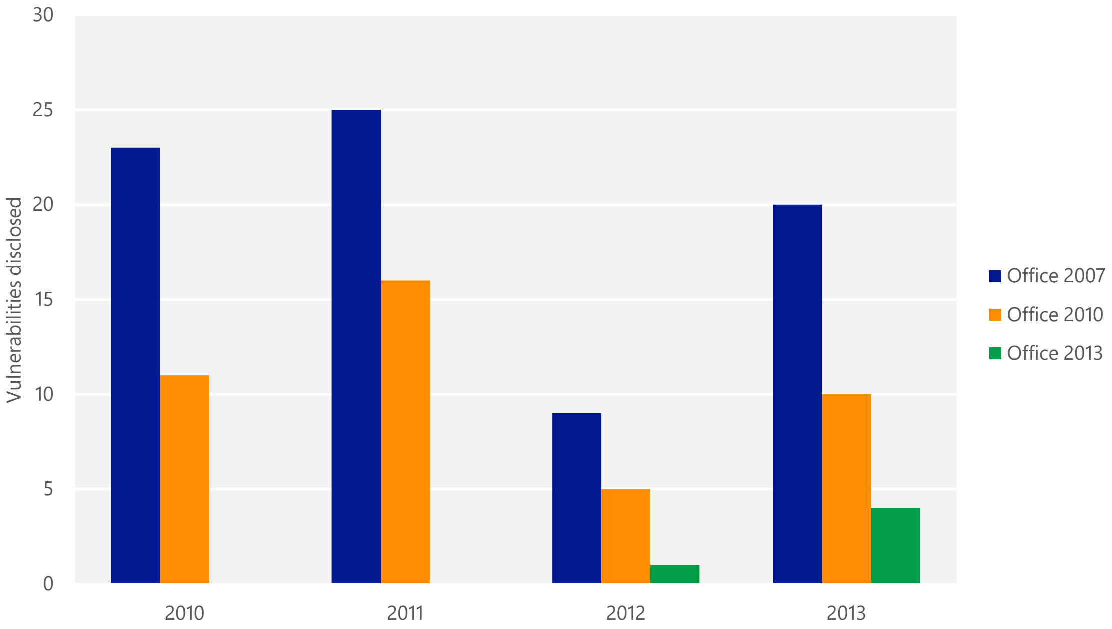
Mitigating risk with Microsoft Office

The security improvements that Microsoft has implemented in recent versions of Windows are fairly well known, but the security mitigations built into recent versions of Microsoft Office—mitigations that are just as significant in many cases as the ones added to Windows—may be less familiar to a lot of people. The goal of this section is to illustrate how customers using older versions of the Office suite of programs can improve their security posture immediately by upgrading to more recent versions. The information and statistics presented here pertain to Office programs running on x86 and x64 editions of Microsoft Windows.

Security mitigations in Microsoft Office

Customers who upgrade to Office 2013 benefit from a host of significant security improvements. Since its release, the Office 2013 suite has been affected by fewer parser vulnerabilities than any other supported version of Office by a large margin, as shown in Figure 74.

Figure 74. Parser vulnerabilities affecting different versions of Microsoft Office addressed by MSRC bulletins each year, 2010–2013



Security mitigations in Office have also evolved significantly since the release of Office 2007. Figure 75 summarizes some of the security improvements that have been added to recent Office releases.[34]

Figure 75. Security-related features in recent versions of Microsoft Office

Feature	Office 2007	Office 2010	Office 2013
Active Content Security	•	•	•
XML-based file formats	•	•	•
Trust Center	•	•	•
Trusted Locations	•	•	•
File Block	•	•	•
Document Inspector	•	•	•
Information Rights Management	•	•	•
Protected View		•	•
Office File Validation	*	•	•
Trusted Documents		•	•
Digital Signatures Improvements		•	•
Identity			•
Escrow Key			•

* Available through an add-in

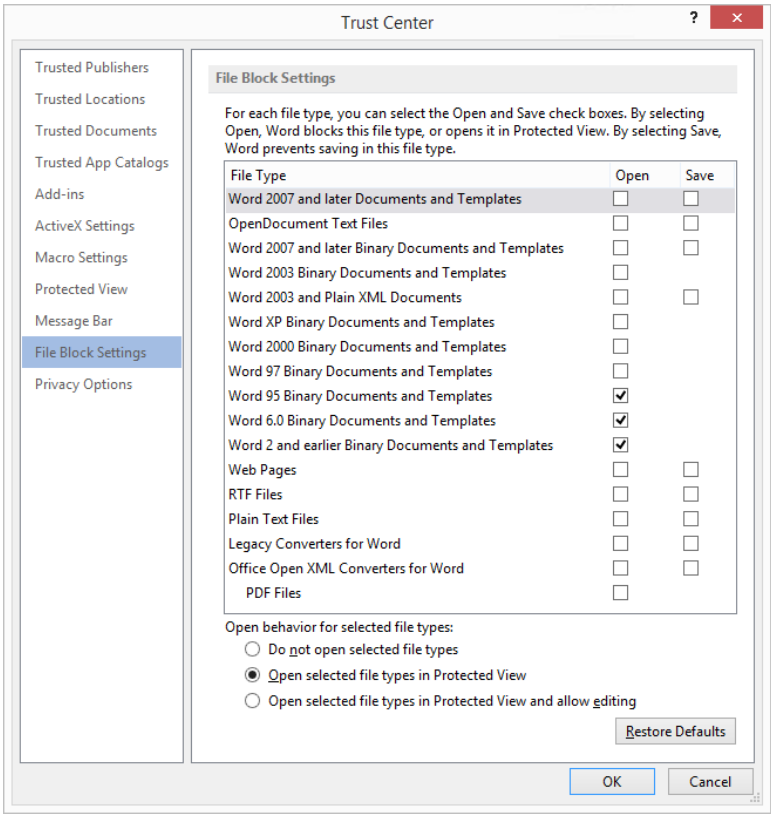
One of the most visible security improvements in Office in recent years has been the introduction of the Office Open XML (OOXML) file formats in Office 2007. The default file types used by current Office applications (including .docx, .xlsx, and .pptx) cannot contain executable macros or other embedded code, which significantly reduces the opportunities for attackers to spread malware. Macro-enabled OOXML files have their own file extensions (such as .docm, .xlsm, and .pptm), and any embedded code is disabled by default for untrusted files.

A number of security features introduced since Office 2007 enable IT departments to defend their environments against threats from malicious files, while still allowing their users to access the contents of legitimate files:

[34] See "Overview of security in Office 2013" at Microsoft TechNet for more information about these and other security mitigations.

- Embedded code is disabled. As with macro-enabled OOXML files, embedded code in binary files is disabled by default for untrusted files. The Trust Center in each Office application enables users and IT administrators to manage trusted files and locations.
- Protected View. Protected View is a secure sandbox for viewing untrusted files where editing functions are disabled. Files from potentially unsafe locations, such as the Internet, are opened in Protected View to allow the user to read the file and see its contents while reducing the risks of a malicious document harming or compromising the computer.
- File Block. Some Office applications can be configured to restrict access to files of specific types. By default, blocked file types open in Protected View and cannot be edited; the File Block feature can also be configured to allow the user to enable editing after opening the file, or to block file opening altogether. IT administrators can use Group Policy to configure and enforce File Block settings across all or part of an organization.

Figure 76. File Block settings in the Word 2013 Trust Center



File Block Settings

For each file type, you can select the Open and Save check boxes. By selecting Open, Word blocks this file type, or opens it in Protected View. By selecting Save, Word prevents saving in this file type.

File Type	Open	Save
Word 2007 and later Documents and Templates	□	□
OpenDocument Text Files	□	□
Word 2007 and later Binary Documents and Templates	□	□
Word 2003 Binary Documents and Templates	□	
Word 2003 and Plain XML Documents	□	□
Word XP Binary Documents and Templates	□	
Word 2000 Binary Documents and Templates	□	
Word 97 Binary Documents and Templates	□	
Word 95 Binary Documents and Templates	☑	
Word 6.0 Binary Documents and Templates	☑	
Word 2 and earlier Binary Documents and Templates	☑	
Web Pages	□	□
RTF Files	□	□
Plain Text Files	□	□
Legacy Converters for Word	□	□
Office Open XML Converters for Word	□	□
PDF Files	□	

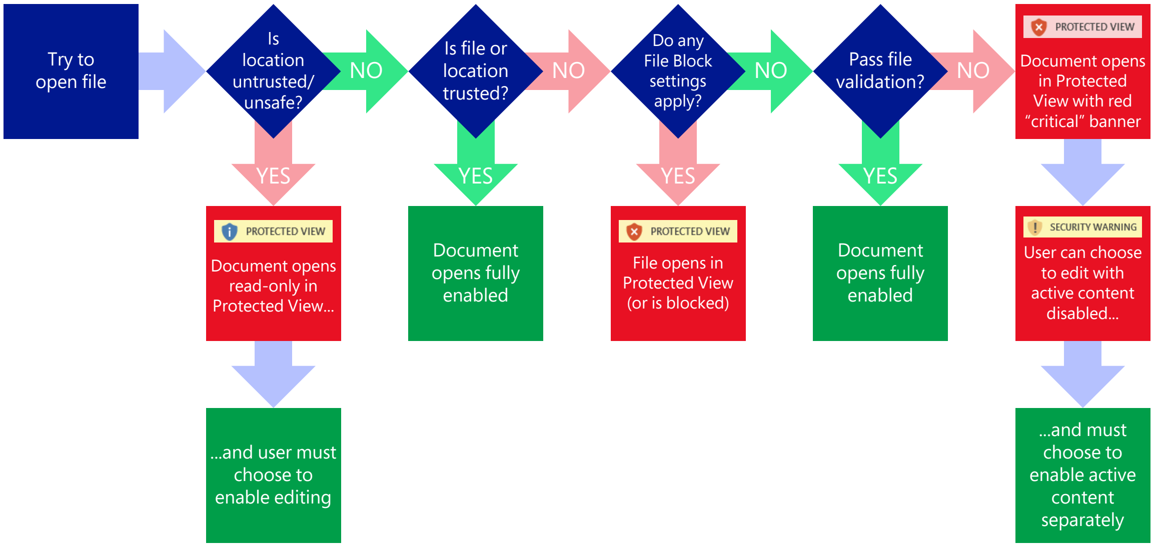
Open behavior for selected file types:

○ Do not open selected file types
● Open selected file types in Protected View
○ Open selected file types in Protected View and allow editing

Restore Defaults

- **Office File Validation**. Introduced in Office 2010 and available for earlier versions through an add-in, Office File Validation is designed to protect against undiscovered threats in Office binary files that may not be detected by security software. When an untrusted binary file is opened, Office File Validation verifies that it conforms to the designated schema for its file type. If the file fails validation, it is opened in Protected View, with a message that the file may be compromised. Administrators can use Group Policy to block the opening of files that fail validation if desired, and to otherwise configure the options users have for accessing the file and its contents.

Figure 77. Conceptual view of some of the mitigations protecting the binary file opening process in Office 2010 and Office 2013


Try to open file
Is location untrusted/ unsafe?
NO
Is file or location trusted?
NO
Do any File Block settings apply?
NO
Pass file validation?
NO
PROTECTED VIEW
Document opens in Protected View with red "critical" banner
YES
YES
YES
YES
PROTECTED VIEW
Document opens read-only in Protected View...
Document opens fully enabled
PROTECTED VIEW
File opens in Protected View (or is blocked)
Document opens fully enabled
SECURITY WARNING
User can choose to edit with active content disabled...
...and user must choose to enable editing
...and must choose to enable active content separately

Building security into Office

At Microsoft, security is considered during every step of the software lifecycle. Every employee who contributes to an Office feature or product is required to take security training and continue to learn as the industry and threats evolve. When designing a feature or product, the team is required to consider user data security and privacy from the beginning and how threats to these can be reduced by using encryption, authentication, or other methods. Their decisions are based on the environment, expected or potential exposure, and data sensitivity. The team performs multiple attack surface reviews and creates an incident response plan before an Office product is ever released.

Microsoft doesn't just rely on employees to make sure user data is safe. It also uses tools and automated quality assurance tests that fall into three general categories:

- **Functional testing.** Every piece of the user interface is verified to make sure that user input, output, and action are as intended and advertised.
- **Fuzz testing.** Large amounts of random or unexpected data are injected into the software to reveal security problems. Fuzz testing has been a big part of the testing process for all currently supported Office releases.
- **For web applications.** Dynamic or web scanning tools are used to test for potential security bugs that use techniques such as cross-site scripting (XSS) or SQL injection.

The testing never stops. The Microsoft Security Response Center (MSRC) is responsible for handling security issues that are uncovered after a product has released. This team can quickly mobilize and deliver swift fixes to customers.

Guidance: Deploying and managing Office securely

- "Guide to Office 2013 security," at Microsoft TechNet, provides links to valuable guidance for IT professionals on topics including:
  - Security threats and countermeasures for Office 2013
  - Configuring security using Group Policy and the Office Customization Tool (OCT)
  - Protecting Office file integrity
  - Using Trust Center settings to guard against external threats
- See "Group Policy Administrative Template files (ADMX, ADML) and Office Customization Tool (OCT) files for Office 2013" at Microsoft TechNet for documentation of the Group Policy settings administrators can use to manage Office 2013 security.

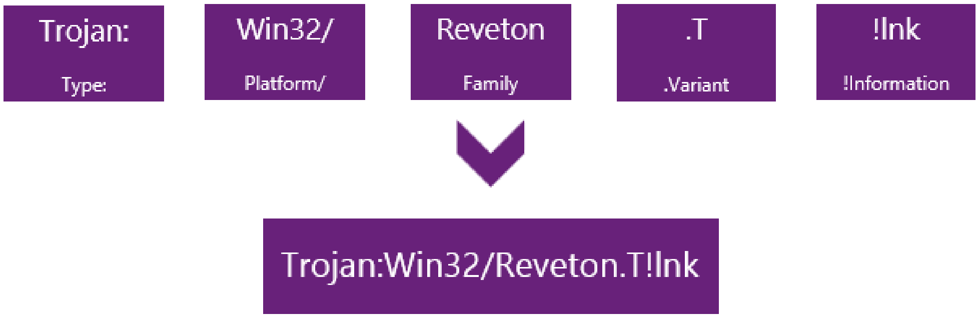
Appendixes

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 78. 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 Trojan:Win32/Reveton.T variant, as shortcut files usually use the extension .lnk.

Appendix B: Data sources

Data included in the *Microsoft Security Intelligence Report* is gathered from a wide range of Microsoft products and services 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:

- Exchange Online Protection protects the networks of tens of thousands of enterprise customers worldwide by helping to prevent malware from spreading through email. Exchange Online Protection scans billions of email messages every year to identify and block spam and malware.
- The Malicious Software Removal Tool (MSRT) is a free tool that Microsoft designed to help identify and remove 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 1H14. 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.
- 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.

- Outlook.com has more than 400 million active email users in more than 30 countries/regions around the world.
- SmartScreen Filter, a feature of 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 Internet Explorer and other Microsoft products and services. When a user attempts to visit a site in the database with the filter enabled, Internet Explorer displays a warning and blocks navigation to the page.
- Windows Defender in Windows 8 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 79. US privacy statements for the Microsoft products and services used in this report

Product or service	Privacy statement URL
Exchange Online (Office 365)	www.microsoft.com/online/legal/v2/?docid=22&langid=en-us
Internet Explorer 11	windows.microsoft.com/en-US/internet-explorer/ie11-win8-privacy-statement
Malicious Software Removal Tool	www.microsoft.com/security/pc-security/msrt-privacy.aspx
Microsoft Security Essentials	windows.microsoft.com/en-us/windows/security-essentials-privacy
Microsoft Safety Scanner	www.microsoft.com/security/scanner/en-us/privacy.aspx
Outlook.com	www.microsoft.com/privacystatement/en-us/core/default.aspx
System Center Endpoint Protection	technet.microsoft.com/en-us/library/hh508835.aspx
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 infection and encounter rates

"Malware prevalence worldwide," on page 65, explains how threat patterns differ significantly in different parts of the world. Figure 80 shows the infection and encounter rates for 1Q14 and 2Q14 for locations around the world.[35] See page 55 for information about how infection and encounter rates are calculated.

Figure 80. Encounter and infection rates for locations around the world, 1Q14–2Q14, by quarter (100,000 computers reporting minimum)

Country/Region	Encounter rate 1Q14	Encounter rate 2Q14	CCM 1Q14	CCM 2Q14
Worldwide	*21.3 %*	*19.1 %*	*10.8*	*7.2*
Afghanistan	—	—	50.8	43.5
Albania	36.8%	34.0%	42.1	32.6
Algeria	58.2%	51.9%	73.4	62.7
Angola	—	—	61.9	55.2
Argentina	31.2%	28.2%	31.1	20.7
Armenia	29.7%	32.1%	18.3	9.9
Australia	13.0%	11.7%	5.2	3.6
Austria	11.4%	12.0%	5.4	5.5
Azerbaijan	—	—	44.1	29.5
Bahamas, The	—	—	10.5	12.6
Bahrain	—	—	39.4	26.2
Bangladesh	—	52.3%	44.9	36.5
Barbados	—	—	—	8.2
Belarus	33.0%	30.9%	15.8	8.0
Belgium	16.0%	14.2%	9.3	6.8

[35] 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 1Q14	Encounter rate 2Q14	CCM 1Q14	CCM 2Q14
Bolivia	—	—	29.0	28.6
Bosnia and Herzegovina	30.5%	29.2%	19.3	19.4
Brazil	34.0%	30.5%	36.0	18.3
Brunei	—	—	—	13.5
Bulgaria	29.9%	27.3%	12.3	11.2
Cambodia	—	—	—	22.0
Cameroon	—	—	—	48.2
Canada	14.5%	12.9%	3.4	3.4
Chile	24.4%	24.2%	18.2	19.1
China	24.3%	23.1%	3.2	2.2
Colombia	34.5%	30.7%	25.2	22.5
Costa Rica	22.5%	21.0%	10.9	15.8
Côte d'Ivoire	—	—	34.8	25.4
Croatia	25.6%	23.5%	8.9	8.1
Cyprus	22.8%	20.0%	12.2	10.1
Czech Republic	16.6%	16.4%	4.7	3.4
Denmark	10.4%	8.7%	5.4	2.8
Dominican Republic	37.9%	33.4%	42.9	38.4
Ecuador	39.9%	34.2%	33.0	26.5
Egypt	49.8%	43.5%	73.1	54.4
El Salvador	—	—	18.7	21.3
Estonia	14.6%	13.5%	3.2	3.5
Finland	6.8%	5.9%	3.0	2.1
France	20.2%	16.8%	15.2	8.5
Georgia	47.5%	42.5%	38.8	26.2
Germany	13.6%	13.5%	6.9	5.7
Ghana	—	42.8%	40.3	27.4
Greece	22.8%	19.5%	12.4	10.4
Guadeloupe	—	—	21.5	13.3
Guatemala	30.5%	25.0%	20.2	19.1
Haiti	—	—	—	37.2

Country/Region	Encounter rate 1Q14	Encounter rate 2Q14	CCM 1Q14	CCM 2Q14
Honduras	—	—	25.7	24.9
Hong Kong SAR	13.4%	11.6%	4.7	4.5
Hungary	20.1%	17.4%	7.7	7.2
Iceland	—	—	3.6	2.5
India	50.5%	41.7%	42.7	30.3
Indonesia	69.1%	56.2%	44.9	31.7
Iraq	50.3%	43.1%	110.5	80.3
Ireland	12.1%	10.8%	4.9	4.8
Israel	18.5%	16.6%	16.6	8.3
Italy	25.5%	20.4%	15.2	9.4
Jamaica	—	—	21.6	16.9
Japan	7.5%	5.9%	2.4	2.8
Jordan	41.2%	37.8%	56.8	40.9
Kazakhstan	41.0%	37.3%	33.2	17.6
Kenya	—	—	31.6	20.9
Korea	29.0%	21.4%	9.2	4.9
Kuwait	—	27.7%	26.2	19.0
Kyrgyzstan	—	—	—	17.5
Latvia	18.9%	17.7%	5.0	4.6
Lebanon	—	35.5%	42.0	34.9
Libya	—	—	71.3	52.1
Lithuania	23.3%	20.1%	11.6	8.3
Luxembourg	—	—	5.0	5.5
Macao SAR	—	—	4.9	5.0
Macedonia, FYRO	32.4%	31.3%	28.4	21.1
Malaysia	35.4%	29.8%	26.2	18.9
Malta	—	—	13.1	8.3
Martinique	—	—	13.5	11.8
Mauritius	—	—	20.8	20.2
Mexico	38.6%	32.1%	39.4	24.5
Moldova	30.9%	26.6%	18.0	10.6

Country/Region	Encounter rate 1Q14	Encounter rate 2Q14	CCM 1Q14	CCM 2Q14
Mongolia	—	—	—	47.3
Montenegro	—	—	—	13.3
Morocco	43.3%	39.4%	70.7	64.4
Mozambique	—	—	—	27.7
Namibia	—	—	—	23.5
Nepal	—	—	56.1	40.6
Netherlands	12.5%	10.8%	5.4	4.3
New Caledonia	—	—	—	13.1
New Zealand	12.1%	9.8%	5.1	4.1
Nicaragua	—	—	19.3	18.1
Nigeria	41.6%	35.2%	31.7	25.7
Norway	8.2%	7.8%	3.5	2.5
Oman	—	—	38.6	33.6
Pakistan	61.5%	54.1%	70.9	52.7
Palestinian Authority	—	—	78.5	59.1
Panama	29.3%	29.3%	24.1	24.9
Paraguay	—	—	16.6	18.0
Peru	37.9%	36.8%	29.7	27.1
Philippines	47.4%	36.9%	44.5	29.5
Poland	22.3%	17.9%	27.8	12.8
Portugal	21.9%	20.1%	17.4	9.2
Puerto Rico	19.2%	16.7%	12.3	11.9
Qatar	31.1%	27.9%	22.9	16.4
Réunion	—	—	15.7	12.8
Romania	32.3%	27.9%	25.7	17.8
Russia	28.7%	26.4%	8.8	4.9
Saudi Arabia	38.6%	35.5%	48.8	33.2
Senegal	—	—	33.2	32.4
Serbia	29.7%	26.5%	13.2	15.8
Singapore	16.1%	13.6%	7.5	5.3
Slovakia	16.9%	15.9%	5.6	5.1

Country/Region	Encounter rate 1Q14	Encounter rate 2Q14	CCM 1Q14	CCM 2Q14
Slovenia	16.6%	15.2%	4.0	4.6
South Africa	26.4%	22.7%	17.4	12.3
Spain	26.1%	21.9%	17.8	13.0
Sri Lanka	39.0%	35.9%	22.9	16.4
Sweden	9.4%	7.8%	5.3	3.4
Switzerland	11.1%	10.3%	1.5	4.8
Taiwan	19.2%	16.9%	12.7	8.1
Tanzania	—	—	36.3	26.6
Thailand	38.2%	30.9%	30.7	21.8
Trinidad and Tobago	—	—	27.1	16.2
Tunisia	49.9%	45.0%	62.3	52.0
Turkey	45.7%	40.5%	45.9	26.8
Ukraine	33.2%	31.9%	14.9	7.8
United Arab Emirates	32.2%	29.2%	2.4	19.5
United Kingdom	13.5%	13.3%	2.2	4.3
United States	13.0%	12.3%	6.4	4.4
Uruguay	21.8%	19.2%	12.9	15.1
Venezuela	43.2%	43.9%	37.0	38.5
Vietnam	60.8%	52.0%	52.7	30.2
Yemen	—	—	—	60.3
Zimbabwe	—	—	—	23.0
Worldwide	*21.3 %*	*19.1 %*	*10.8*	*7.2*

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 damage a computer if a user visits a webpage that contains the malicious ActiveX control.

adware
A program that displays extra promotions that the user cannot control, and which would not appear if the adware weren't installed.

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*.

Bitcoin mining
The use of computing resources to create new bitcoins, a type of digital currency. Bitcoin mining software needs a lot of computer processing power and may slow down the computer that's running it.

bot
A malware program that joins an infected computer to a botnet.

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

browser modifier
A program that changes browser settings, such as the home page, without adequate consent. Browser modifiers include 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*.

co-owned
In the context of compromised accounts, an account that can be accessed by both the legitimate account owner and an attacker. Compare *taken over*.

credentials
See *account credentials*.

cross-site scripting
Abbreviated *XSS*. An attack technique in which an attacker inserts malicious HTML and JavaScript into a vulnerable webpage, often in an effort to distribute malware or to steal sensitive information from the website or its visitors. Despite the name, cross-site scripting does not necessarily involve multiple websites. Persistent cross-site scripting involves inserting malicious code into a database used by a web application, potentially causing the code to be displayed for large numbers of visitors.

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

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

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

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

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 unwanted software, or report detecting a specific threat or family, during a period. Also see *CCM*.

exploit
A piece of code that uses software vulnerabilities to access information on a computer or install malware.

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.

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

in the wild
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*.

Litecoin
See *Bitcoin mining*.

malware
The general name for programs that perform unwanted actions on a computer, such as stealing personal information. Some malware can steal banking details, lock the computer until a ransom is paid, or use the computer to send spam. Viruses, worms, and trojans are all types of malware. By default, Microsoft security products automatically block, quarantine, or remove malware that is determined to have a high negative impact on affected computers.

malware impression
A single instance of a user attempting to visit a page known to host malware and being blocked by SmartScreen Filter in Internet Explorer versions 8 through 11. Also see *phishing impression*.

man-in-the-middle attack
A form of eavesdropping in which a malicious hacker gets in the middle of network communications. The malicious hacker can then manipulate messages or gather information without the knowledge of users who are communicating.

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)*.

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.

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

parser vulnerability
A vulnerability in the way an application processes, or parses, a file of a particular format, which can be exploited through the use of a specially crafted file. Also see *vulnerability*.

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.

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*.

plaintext
Text that has not been encrypted or otherwise obfuscated.

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.

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 is typically used in the context of Android devices; the comparable process on iOS devices is more commonly referred to as *jailbreaking*.

salt
A string of random characters added to a password before hashing, to ensure that the same password hashes to different values for different users.

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.

Short Message Service
The standardized text messaging service implemented by most mobile phone operators.

signature
See *detection signature*.

SMS
See *Short Message Service*.

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 prompt 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.

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 computers or may use compromised computers to send spam.

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.

taken over
Said of a compromised account that the legitimate account owner can no longer access. Compare *co-owned*.

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

Tor
An open source project that provides users with a way to access Internet resources anonymously by relaying traffic through the computers of other Tor users.

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

two-factor authentication
See *multifactor authentication*.

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 in a program that could allow an attacker to compromise its integrity, availability, or confidentiality.

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.

Win32/AddLyrics. A browser add-on that displays lyrics for songs on YouTube, and displays advertisements in the browser window.

Win32/Adpeak. Adware that displays extra ads as the user browses the Internet, without revealing where the ads are coming from. It may be bundled with some third-party software installation programs.

Win32/Ardamax. A monitoring tool that captures activities such as keystrokes and may send the details to an attacker.

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 recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

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 to a remote attacker.

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

MSIL/Bepush. A family of trojans that download and install add-ons for the Firefox and Chrome browsers that post malicious links to social networking sites, track browser usage, and redirect the browser to specific websites.

Win32/BetterSurf. Adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.

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.

Win32/Brantall. A family of trojans that download and install other programs, including Win32/Sefnit and Win32/Rotbrow. Brantall often pretends to be an installer for other, legitimate programs.

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

Win32/Caphaw. A family of backdoors that spread via Facebook, YouTube, Skype, removable drives, and drive-by download. They can make Facebook posts via the user's account, and may steal online banking details.

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/Clikug. A threat that uses a computer for click fraud. It has been observed using as much as a gigabyte of bandwidth per hour.

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

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

Win32/Crilock. A ransomware family that encrypts a computer's files and displays a webpage that demands a fee to unlock them.

AndroidOS/CVE-2011-3874. A threat that attempts to exploit a vulnerability in the Android operating system to gain access to and control of the device.

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

Java/CVE-2013-0422. A detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2013-0422, addressed by an Oracle security update in January 2013.

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

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

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

Win32/Dowque. A generic detection for malicious files that are capable of installing other malware.

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

JS/Faceliker. A malicious script that "likes" content on Facebook without the user's knowledge or consent.

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

HTML/Fashack. A detection for the Safehack exploit kit, also known as Flashpack. It uses vulnerabilities in Adobe Flash Player, Java, and Silverlight to install malware on a computer.

Win32/Feven. A browser add-on for Internet Explorer, Firefox, or Chrome that displays ads on search engine results pages and other websites, and redirects the browser to specific websites.

JS/Fiexp. A detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.

Win32/Filcout. An application that offers to locate and download programs to run unknown files. It has been observed installing variants in the Win32/Sefnit family.

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 local computers and communicating with command-and-control (C&C) servers managed by attackers.

Win32/Genasom. A ransomware family that locks a computer and demands money to unlock it. It usually targets Russian-language users, and may open pornographic websites.

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 a mobile device.

Win32/Hupigon. A family of trojans that uses a dropper to install one or more backdoor files, and installs sometimes a password stealer or other malicious programs.

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

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

Win32/Kegotip. A password-stealing trojan that can steal email addresses, personal information, or user account information for certain programs.

Win32/Krypterade. Ransomware that fraudulently claims a computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.

Win32/Lecpetex. A family of trojans that steal sensitive information, such as user names and passwords. It can also use a computer for Litecoin mining, install other malware, and post malicious content via the user's Facebook account.

Win32/Loktrom. Ransomware that locks a computer and displays a full-screen message pretending to be from a national police force, demanding payment to unlock the computer.

Win32/Lollipop. Adware that may be installed by third-party software bundlers. It displays ads based on search engine searches, which can differ by geographic location and may be pornographic.

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

HTML/Meadgive. A detection for the Redkit exploit kit, also known as Infinity and Goon. It attempts to exploit vulnerabilities in programs such as Java and Silverlight to install other malware.

Win32/Meredrop. A generic detection for trojans that drop and execute multiple forms of malware on a local computer. These trojans are usually packed, and may contain multiple trojans, backdoors, or worms. Dropped malware may connect to remote websites and download additional malicious programs.

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

JS/Neclu. A detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.

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/Oceanmug. A trojan that silently downloads and installs other programs without consent.

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.

Win32/OptimizerElite. A misleading program that uses legitimate files in the Prefetch folder to claim that the computer is damaged, and offers to "fix" the damage for a price.

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

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 a file is opened.

HTML/Phish. A password-stealing malicious webpage, known as a phishing page, that disguises itself as a page from a legitimate website.

Win32/Prast. A generic detection for various password stealing trojans.

VBS/Psyme. A VBScript trojan that exploits a vulnerability addressed by Microsoft Security Bulletin MS06-014. The trojan is encountered when a user visits a malicious Web page containing the script, and it attempts to download and execute arbitrary files on the affected system.

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.

JS/Redirector. A detection for a class of JavaScript trojans that redirect users to unexpected websites, which may contain drive-by downloads.

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/Rotbrow. A trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.

Win32/Sefnit. A family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.

Win32/Sisproc. A generic detection for a group of trojans that have been observed to perform a number of various and common malware behaviors.

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

MSIL/Spacekito. A threat that steals information about the computer and installs browser add-ons that display ads.

Win32/Startpage. A detection for various threats that change the configured start page of the affected user's web browser and may also perform other malicious actions.

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

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

JS/Urntone. A webpage component of the Neutrino exploit kit. It checks the version numbers of popular applications installed on a computer, and attempts to install malware that targets vulnerabilities in the software.

Win32/VB. A detection for various threats written in the Visual Basic programming language.

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

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/Wysotot. A threat that can change the start page of the user's web browser, and may download and install other files to a computer. It is installed by software bundlers that advertise free software or games.

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

Win32/Zegost. A backdoor that allows an attacker to remotely access and control a computer.

Index

Microsoft

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