Microsoft Security Intelligence Report

Volume 12

July through December, 2011

www.microsoft.com/sir

Microsoft Security Intelligence Report

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 website references, may change without notice. You bear the risk of using it.

Authors

Dennis Batchelder
Microsoft Protection Technologies

Shah Bawany
Microsoft Windows Safety Platform

Joe Blackbird
Microsoft Malware Protection Center

Eve Blakemore
Microsoft Trustworthy Computing

Joe Faulhaber
Microsoft Malware Protection Center

Sarmad Fayyaz
Bing

David Felstead
Bing

Paul Henry
Wadeware LLC

Nitin Kumar Goel
Microsoft Security Response Center

Jeff Jones
Microsoft Trustworthy Computing

Jimmy Kuo
Microsoft Malware Protection Center

Marc Lauricella
Microsoft Trustworthy Computing

Ken Malcolmson
Microsoft Trustworthy Computing

Nam Ng
Microsoft Trustworthy Computing

Mark Oram
Microsoft Trustworthy Computing

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Dave Probert
Microsoft Security Engineering Center

Tim Rains
Microsoft Trustworthy Computing

Frank Simorjay
Microsoft Trustworthy Computing

Holly Stewart
Microsoft Malware Protection Center

Matt Thomlinson
Microsoft Trustworthy Computing

Scott Wu
Microsoft Malware Protection Center

Terry Zink
Microsoft Forefront Online Protection for Exchange

Contributors

Doug Cavit
Microsoft Trustworthy Computing

Chris Compton
Microsoft Trustworthy Computing

Mike Convertino
Microsoft Trustworthy Computing

Enrique Gonzalez
Microsoft Malware Protection Center

Heather Goudey
Microsoft Malware Protection Center

Roger Grimes
Microsoft IT Information Security and Risk Management

Satomi Hayakawa
CSS Japan Security Response Team

Jenn LeMond
Microsoft IT Information Security and Risk Management

Le Li
Microsoft Windows Safety Platform

Jenner Mandel
Microsoft Trustworthy Computing

Hideya Matsuda
CSS Japan Security Response Team

Patrick Nolan
Microsoft Malware Protection Center

Takumi Onodera
Microsoft Premier Field Engineering, Japan

Anthony Penta
Microsoft Windows Safety Platform

Kathy Phillips
Microsoft Legal and Corporate Affairs

Hilda Larina Ragragio
Microsoft Malware Protection Center

Laura A. Robinson
Microsoft IT Information Security and Risk Management

Richard Saunders
Microsoft Trustworthy Computing

Jasmine Sesso
Microsoft Malware Protection Center

Adam Shostack
Microsoft Trustworthy Computing

Maarten Van Horenbeeck
Microsoft Trustworthy Computing

Henk van Roest
CSS Security EMEA

Patrik Vicol
Microsoft Malware Protection Center

Steve Wacker
Wadeware LLC

Dan Wolff
Microsoft Malware Protection Center

Table of Contents

Worldwide threat assessment 33

Appendixes 103

About this report

The *Microsoft® Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, and malicious and potentially unwanted software. Past reports and related resources are available for download at www.microsoft.com/sir. We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their organizations, software, and users.

Reporting period

This volume of the *Microsoft Security Intelligence Report* focuses on the third and fourth quarters of 2011, respectively, with trend data for the last several years 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, as in previous volumes of the report.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, where *yy* indicates the calendar year and *n* indicates the half or quarter. For example, 2H11 represents the second half of 2011 (July 1 through December 31), and 4Q11 represents the fourth quarter of 2011 (October 1 through December 31). To avoid confusion, please note the reporting period or periods being referenced when considering the statistics in this report.

Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware and potentially unwanted software. For information about this standard, see "Microsoft Malware Protection Center Naming Standard" on the MMPC website.

Trustworthy Computing: Security engineering at Microsoft

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

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

How Conficker continues to propagate

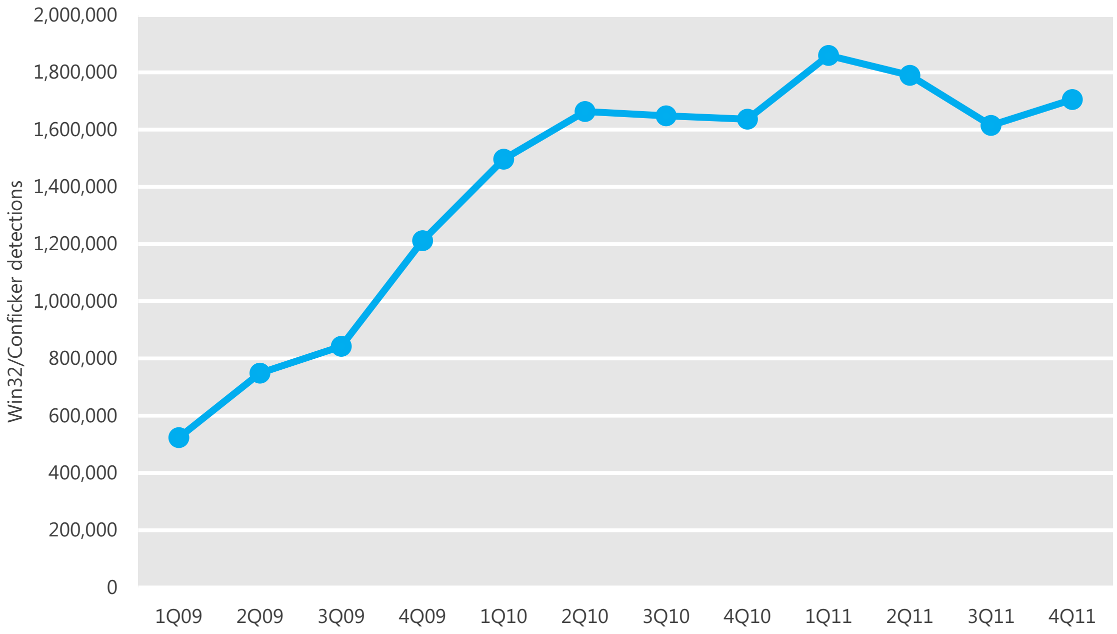
Background

In October 2008, Microsoft® released a security update (MS08-067) that addressed a software vulnerability in some versions of the Windows operating system. At that time, Microsoft recommended that customers install the update as soon as possible and warned that attackers could potentially create a worm that would affect vulnerable computers. Over the next few weeks, hundreds of millions of computers around the world received the MS08-067 update.

In November 2008, the Microsoft Malware Protection Center (MMPC) detected the emergence of the first version of Win32/Conficker, an aggressive and technically complex new family of worms. Win32/Conficker targeted the vulnerability addressed by MS08-067. Although the first version of this new threat did not spread widely, it seriously challenged security responders and others charged with ensuring the safety of the world's computer systems and data. In late December 2008—a full two months after Microsoft released the security update—a second version of Conficker was detected. This version includes additional attack vectors that help the worm to spread quickly.

Microsoft created and distributed antimalware signatures for the new threats. In addition, Microsoft worked with other members of the international security community to contain much of the damage that was caused by Conficker, and in the process established a potentially groundbreaking template for future cooperative response efforts.

Figure 1. Win32/Conficker detections by Microsoft antimalware products, 1Q09–4Q11



This section of the *Microsoft Security Intelligence Report, Volume 12* establishes that Conficker remains a threat, provides background information on why it is a serious threat, and what organizations can do to protect themselves. (For more information and deep technical details on Conficker, see the "Win32/Conficker Update" section in *Microsoft Security Intelligence Report, Volume 7 (January through June 2009)*, available at www.microsoft.com/sir.)

At its peak, Conficker infected an estimated seven million computers worldwide, according to the Conficker Working Group. Conficker was immediately recognized as dangerous because it attempts to exploit a vulnerability on Windows XP®-based systems that allows remote code execution when file sharing is enabled (CVE-2008-4250, which Microsoft had addressed in October 2008 with critical update MS08-067). In addition, Conficker disables several important system services and security products, and also downloads arbitrary files. The initial version (labeled Worm:Win32/Conficker.A by the MMPC) was not very successful at propagating, mostly because the MS08-067 security update had already been distributed and widely installed. However, the next variant, Worm:Win32/Conficker.B, uses two new propagation methods—abusing the Autorun feature on Windows XP and Windows Vista®-based computers, and guessing administrator passwords on network shares with weak or shared passwords—to quickly propagate through the Internet.

In addition to quick propagation, the newer variants of Conficker use a larger array of attack techniques than most malware families. In addition to a suite of self-defense mechanisms such as blocking access to security-related websites and disabling security software on infected computers, Conficker uses encryption and a method called *HTTP rendezvous* to protect its payload channel.[1]

Because of the way Conficker uses multiple attack vectors to maximize its reach, there was a global effort to thwart its use and to determine who would try to make use of it. Worm:Win32/Conficker.E was reported to perform some downloads of the Win32/Waledac spambot and the rogue security software family Win32/FakeSpypro (which identified itself as "SpyProtect 2009"). This variant was programmed to delete itself in May 2009.

Propagation mechanisms

Although the efforts of the Conficker Working Group and associated organizations restricted Conficker's potential for damage, the MMPC received telemetry reports of the worm infecting or attacking 1.7 million computers in 4Q11, about 100,000 computers more than in 3Q11. A detailed analysis of the MMPC telemetry can help organizations defend against Conficker variants by understanding the relative success rates of the different propagation methods that the worm uses.

Information about the propagation vectors is directly observable through data reported by Microsoft security products running on computers whose administrators or users choose to opt in to data collection. The MMPC used this data to deduce the following information about Conficker's propagation mechanisms:

- **Credential-based attacks**. This type of attack uses the credentials of the logged-in user to access local or network resources, or else attacks password-protected resources using a built-in list of common or weak passwords.[2] When the worm successfully infects a computer using this type of attack, it

[1] See page 96 of *Microsoft Security Intelligence Report, Volume 7 (January through June 2009)* for more information about this technique.
[2] See the entry for Worm:Win32/Conficker.C in the MMPC encyclopedia (www.microsoft.com/security/portal) for the list of weak passwords used by Conficker.

creates a scheduled task on the infected computer that attempts to re-infect the computer at regular intervals. Credential-based attacks can therefore be identified through the presence of such a scheduled task.

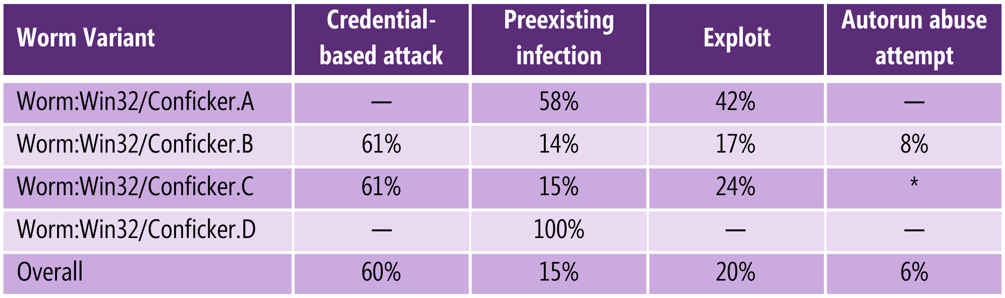
- **Autorun feature abuse attempt**. Conficker can attempt to spread to a computer by abusing the Autorun feature in Windows, through the use of a malicious autorun.ini file that links to a Conficker executable. Microsoft security software detects and blocks this file, even on computers running versions of Windows that are not at risk from this form of attack. Detection of the malicious autorun.ini file is therefore not an indication of an infected computer, but indicates that an attack has been attempted.
- **MS08-067 exploitation**. It is possible to determine this type of attack because of a detail of the worm's implementation. After successful exploitation, Conficker calls a Windows API that in turn calls the Microsoft **IOfficeAntivirus** provider, which detects and blocks the transfer of the worm's code. The telemetry includes an indicator of whether the worm was active or not, which allows excluding partially removed or broken infection attempts.
- **Preexisting infection**. Microsoft antimalware software also reports details about Conficker infections that were present on the computer before the antimalware software was installed. These pre-existing infections are indicated by the presence of a Windows service created by Conficker.

Results

Figure 2 shows an analysis of three weeks of telemetry data of active Conficker installations or installation attempts.[3]

[3] This data was collected after the February 2011 release (through Windows Update and Microsoft Update) of a security update that addressed the Autorun feature abuse technique used by Conficker, as mentioned earlier. See blogs.technet.com/b/security/archive/2011/06/27/defending-against-autorun-attacks.aspx for more information.

Figure 2. Propagation methods used by Win32/Conficker variants, by percent of all attempted attacks detected



Worm Variant	Credential-based attack	Preexisting infection	Exploit	Autorun abuse attempt
Worm:Win32/Conficker.A	—	58%	42%	—
Worm:Win32/Conficker.B	61%	14%	17%	8%
Worm:Win32/Conficker.C	61%	15%	24%	*
Worm:Win32/Conficker.D	—	100%	—	—
Overall	60%	15%	20%	6%

* Autorun files for variants B and C are identical, and accordingly are all grouped with Conficker.B in this chart.

Most of the analyzed incidents (60 percent) involved credential-based attacks, with the remaining 40 percent including all other known propagation methods. The second-greatest number of incidents in the specified timeframe (20 percent) exploited the CVE-2008-4250 vulnerability on computers that had not yet been updated with Security Bulletin MS08-067, despite the fact that the update had been released more than two years before. The third-greatest number of analyzed incidents (15 percent) involved infections that were present on the computer before the installation of the antimalware product that detected and removed the infection. Finally, only 6 percent of incidents that were observed in the specified timeframe involved abuse of the Autorun feature in Windows. The release of an update that hardened the Autorun feature in Windows XP and Windows Vista may have helped achieve this relatively low percentage.

This attack pattern suggests that improving credential policies and practices is one of the most important steps computer administrators can take to effectively combat the spread of Conficker. Domain administrators can use Active Directory® Domain Services (AD DS) to define and enforce Group Policy Objects (GPOs) that require users to create complex passwords.[4] If local passwords are used for some resources in an organization, resource owners should be required or encouraged to use strong passwords for them as well.

When considered from the perspective of the affected operating system, it becomes clearer that credential-based attacks on file shares are the primary mechanism Conficker uses to compromise computers running recent versions of the Windows operating system, as shown in Figure 3.

[4] See “Enforcing Strong Password Usage Throughout Your Organization” on Microsoft TechNet for more information and instructions.

Figure 3. Blocked Conficker infection attempts by operating system

Operating System	Credential-based attack	Exploit	Autorun abuse attempt
Windows 2003	81%	19%	1%
Windows XP	54%	43%	2%
Windows Vista	84%	—	16%
Windows 7	89%	—	11%

Windows 7 was never vulnerable to CVE-2008-4250 exploits, and although Windows Vista was vulnerable, no exploit attempts were observed in the measurement period. Network Inspection System (NIS), a feature of Microsoft Security Essentials and Microsoft Forefront® Threat Management Gateway, blocks exploit attempts on vulnerable computers running Windows Vista and other recent versions of Windows, which prevents the Conficker worm from exploiting the CVE-2008-4250 vulnerability.[5] Windows 7 was also far more difficult to attack through Autorun feature abuse, and although autorun abuse attempts were observed and blocked on 11 percent of Windows 7 systems, they would not have been successful because of the restricted Autorun policy on that platform.

The Conficker worm may or may not have had as great an effect as its creators expected, but it continues to search for new victims. Although installing all relevant security updates and hardening the Autorun feature in Windows can close off several Conficker attack vectors, this analysis of the worm's attacks shows that using weak passwords for network and local resources can still leave computers at significant risk of infection. To effectively defend against Conficker and similar malware families, responsible computer administrators should develop a multifaceted strategy that includes strong passwords, quick deployment of security updates, and the use of regularly updated, real-time antimalware software.

[5] See go.microsoft.com/fwlink/?LinkId=248183 for more information about the Network Inspection System.

Figure 4. Blocked Conficker infection attempts on enterprise computers, as detected by Microsoft Forefront Endpoint Protection

Operating System	Credential-based attack	Exploit	Autorun abuse attempt
Windows 2003	91%	9%	—
Windows 7	100%	—	—
Windows Vista	100%	—	—
Windows XP	88%	12%	—

Figure 5. Blocked Conficker infection attempts on consumer computers, as detected by Microsoft Security Essentials

Operating system	Credential-based attack	Exploit	Autorun abuse attempt
Windows 2003	77%	22%	1%
Windows 7	85%	—	15%
Windows Vista	77%	—	23%
Windows XP	46%	51%	3%

Tips to help clean up an environment in which Conficker is present

Malware such as Conficker can still pose a challenge for IT administrators, despite the fact that it is a well-known threat. Even a conscientious IT department that follows responsible practices for quickly installing security updates, installing and monitoring antimalware and intrusion detection systems, and controlling access to file shares can still encounter outbreaks of a threat such as Conficker.

Malware that uses common network protocols such as Server Message Block (SMB) to replicate can pose a threat to locked-down file shares, because an infected computer that has write privileges to the file share can pass the infection on to it. A common scenario is one in which a file share is disinfected by server-side antimalware software, but is quickly reinfected when an infected client computer connects to it. This potential for repeated reinfection gives malware that leverages open file shares, such as Conficker, staying power in data centers. Identifying the original source of the infection within the organization is therefore essential for eradicating such malware. Finding it can require a bit of agility and creativity on the part of server administrators.

Microsoft provides information to help IT administrators deal with Conficker infections at www.microsoft.com/conficker. The following list provides some additional tips that may help advanced users who possess a good understanding of computer security and Windows administration find computers that are infected with Conficker in order to minimize their attack surface.

- Create a "rogue" file share, populate it with various executable files and share the directory for full control to all. However, before sharing the folder, turn on Windows monitoring to identify computers that successfully write to the share.[6] The events captured in Windows Event Viewer with share monitoring enabled will capture enough information to identify the original source of the infection. Use this practice on several shares and systems in the environment and monitor as needed.
- On infected computers, check the device log; by default, the Windows installation places this log in *C:\Windows\inf\setupapi.dev*. The log will contain information about devices such as memory sticks or other USB hardware that has been installed on the system and will help find the original source of the infection if this method was used to install Conficker or other malware that propagates through Autorun.[7]
- The original source of the infection is often determined to be a computer inside the organization's backup infrastructure. Because of performance and other related factors, many organizations relax security controls for backup systems, which is a big mistake. It is important for the organization's IT staff to ensure that basic security practices are in place, especially for an environment in which Conficker is problematic. It isn't uncommon for malware to be stored on backup servers, because the files are usually encrypted and continuously copied back down to clean servers.
- Inside the data center, implement a server administrator file share change control process that reviews and approves file share configurations; such an approach will help minimize the attack surface for malware that uses network shares to replicate. Depending on the size of the organization, it could be a daunting task to implement such a process throughout an entire data center, but at a minimum it should be required for servers that have been identified as repeat offenders or other systems that have been deemed critical to the organization's service.

[6] For details on auditing user access, see Microsoft Knowledge Base article 310399 at support.microsoft.com.
[7] For more information about the device log, see "Troubleshooting Device Installation with the SetupAPI Log File" at the Microsoft Developer Network website (msdn.microsoft.com).

Determined Adversaries and Targeted Attacks

Introduction

Over the past two decades the internet has become fundamental to the pursuit of day-to-day commercial, personal, and governmental business. However, the ubiquitous nature of the internet as a communications platform has also increased the risk to individuals and organizations from cyberthreats. These threats include website defacement, virus and worm (or *malware*) outbreaks, and network intrusion attempts. In addition, the global presence of the internet has allowed it to be used as a significant staging ground for espionage activity directed at industrial, political, military, and civil targets.

During the past five years, one specific category of threat has become much more widely discussed. Originally referred to as *Advanced Persistent Threats (APT)* by the U.S. military — referring to alleged nation-state sponsored attempts to infiltrate military networks and exfiltrate sensitive data — the term APT is today widely used in media and IT security circles to describe any attack that seems to specifically target individual organization, or is thought to be notably technical in nature, regardless of whether the attack was actually either advanced or persistent.

In fact, this type of attack typically involves two separate components — the action(s) and the actor(s) — that may be targeted against governments, military organizations or, increasingly, commercial entities and civil society.

The *actions* are the attacks themselves, which may be IT-related or not, and are referred to as *Targeted Attacks* in this paper. These attacks are initiated and conducted by human *actors*, who are collectively referred to in this paper as *Determined Adversaries*. These definitions are important because they emphasize the point that the attacks are carried out by human actors who may use any tools or techniques necessary to achieve their goals; these attacks are not merely malicious software or exploits. Using an encompassing term such as APT can mask this reality and create the impression that all such attacks are technically sophisticated and malware-driven, making it harder to plan an effective defensive posture.

For these reasons, this paper uses Targeted Attacks and Determined Adversaries as more specific and meaningful terms to describe this category of attack.

- **Targeted Attacks**. The attackers target individuals or organizations to attack, singly or as a group, specifically because of who they are or what they represent; or to access, exfiltrate, or damage specific high-value assets that they possess. In contrast, most malware attacks are more indiscriminate with the typical goal of spreading malware widely to maximize potential profits.
- **Determined Adversaries**. The attackers are not deterred by early failures and they are likely to attack the same target repeatedly, using different techniques, until they succeed. These attackers will regroup and try again, even after their attacks are uncovered. In many cases the attacks are consciously directed by well-resourced sponsors. This provides the attackers with the resources to adapt to changing defenses or circumstances, and directly supports the persistence of attacks where necessary.

Determined Adversaries and Targeted Attacks may employ combinations of technology and tactics that enable the attacker to remain anonymous and undiscoverable, which is why these methods of attack might appeal to agencies of nation states and other entities who are involved in espionage-related activities.

Hardening the perimeters of computer networks is not a sufficient defensive strategy against these threats. Many computer security experts believe that a well-resourced and determined adversary will usually be successful in attacking systems, even if the target has invested in its defensive posture.[8]

Rather than the traditional focus on preventing compromise, an effective risk management strategy assumes that Determined Adversaries may successfully breach any outer defenses. The implementation of the risk management strategy therefore balances investment in prevention, detection, containment and recovery.[9]

Microsoft has a unique perspective on Targeted Attacks, as both a potential target of attacks and a service and solution provider to potential victims. This paper shares Microsoft's insights into the threat that Determined Adversaries and Targeted Attacks pose, identifies challenges for organizations seeking to combat this threat category and provides a context for other papers that will directly address each of those.

[8] Charney, Scott – Rethinking the Cyber Threat – A Framework and Path Forward
www.microsoft.com/download/en/details.aspx?id=747

[9] Charney, Scott – Trustworthy Computing Next
aka.ms/nextwp

Determined Adversaries

Since the beginning of history, there have been people willing to steal the possessions of others to satisfy a wide variety of motives. Targeted Attacks are simply the inevitable consequence of the digitization of previously physical processes and assets.

Determined Adversaries who deploy Targeted Attacks tend to be well funded and organizationally sophisticated. Examination of several Targeted Attacks shows that the attackers operate in a team model, to meet the requirements of a threat sponsor. The existence of the threat sponsor is critical in understanding the overall actions of Determined Adversaries. In the case of traditional cybercrime, such as attacks against on-line banking, a technically able attacker can be self-motivated. However, in other cases, such as espionage, the sponsor provides the motivation and resources for the attacker to determinedly collect the information that meets their specific requirements. Because new requirements will emerge, it is logical for the attackers to maintain persistent access to existing or potential future targets.

Detailed information about specific Determined Adversaries is often difficult to obtain. The institutions victimized by Targeted Attacks are often reluctant to share information because of the highly sensitive nature of the networks or assets that they protect.

Many of the early Targeted Attacks focused on military and defense networks,[10] which are typically among the more well-defended networks in the world. Consequently, attackers were forced to develop a wide range of technical and non-technical skills to conduct successful attacks.

Today, many of the actors involved in earlier attacks on military networks have started to put their skills to use by attacking commercial networks in order to meet a sponsor's economic goals. For this reason, security professionals consider Determined Adversaries to be among the more serious security threats that computer networks currently face.

[10] www.businessweek.com/magazine/content/08_16/b4080032218430.htm

Institutions such as military forces, defense contractors, and critical infrastructure providers have been popular targets for espionage since long before the internet existed, and they remain popular targets for Determined Adversaries. However, in a broad sense almost any institution that possesses information assets that an attacker might value can be a target.

Same old tricks, new era

The operational model often employed for human intelligence gathering will be familiar to readers of espionage novels. In this traditional espionage model, a sponsor organization or "pay master" working on their behalf provides a threat actor in the form of an intelligence officer, and requirements for the information they wish to be collected. The intelligence officer then develops operational intelligence to support the identification and recruitment of a vulnerable individual who is likely to have, or be in a position to facilitate, access to the required information. Since it may be dangerous for the intelligence officer to physically meet with the individual (or agent), they will employ a "dead drop". This is a physical location through which the intelligence officer can pass requirements to the agent, and through which in turn the agent will pass the collected information. Once the agent is established, they may then go on to recruit other agents.

The model employed by Determined Adversaries in conducting Targeted Attacks has striking similarities to this approach. The sponsor and the threat actor roles, albeit it with a different skill set, are a constant. However, the target is now a vulnerable computer system against which the attacker will employ operational intelligence to achieve compromise. Once the system is compromised, the attacker then employs a "dead drop" in the form of a command-and-control server through which information can be exchanged while protecting the identity of the attacker.

In the traditional espionage scenario, there is significant risk to both the sponsor and the threat actors of being identified. However, the same model implemented by Targeted Attacks is significantly more attractive as there is less risk of the actors being identified, detained and their activities made public.

The role of the Internet

Internet technologies provide a basis upon which to achieve huge efficiencies in communications, storage, data processing and business tractions. Given the ever-increasing use of the internet (2 billion users in 2011 with forecasts of another billion users coming online in the next four years),[11] it is no surprise that bad actors are using this near-ubiquitous communications medium for their own ends. With almost all individuals, governments, and organizations connected to one another through the internet, geography is increasingly irrelevant. Low risk attacks can be launched from locations around the world, perhaps originating in countries or regions that do not have regulations or laws governing cybercrime, or lack the resources to effectively enforce such laws.

One observation of this trend is the trickle-down effect on attack techniques and technology. Ten years ago, attackers had to build bespoke capabilities to conduct many forms of attack. Today there are kits available in illicit online marketplaces that let prospective attackers achieve the same results with much less effort and expertise. The same trickle-down effect can be observed in the evolution of financially motivated attacks employing techniques that originated with Targeted Attacks. For example, the operational model and techniques employed in the targeting of a company's payment system to facilitate online banking fraud can be similar to those used in espionage orientated Targeted Attacks.

Understanding this change in threat, and reflecting it in consideration of an organization's risk profile is now essential. For example, a luxury fashion manufacturer might think that a potential attacker would spend significant resources to acquire military or state secrets, but not to target the company's product designs. It is worth reiterating that this assumption no longer holds because cybercriminals are using the same attack knowledge and tools that were previously focused exclusively on espionage to support the traditional criminal activity of counterfeiting goods. However, in many cases, organizations are simply not prepared for this shift in the threat environment.

[11] www.mckinsey.com/Features/Sizing_the_internet_economy.aspx

Targeted Attacks

Although attackers have used computer networks to enable espionage for several decades, the widespread recognition of Targeted Attacks as a distinct class of security threat is a relatively recent development. Attacks of this type became publicly known in the mid-2000s following a number of security incidents that were believed to have been perpetrated by, or on behalf of, national governments or other state actors. More recently, reports of similar attacks waged by non-state actors against commercial and government targets for profit, intelligence gathering, or other reasons have increased.

Although Targeted Attacks may be perceived as an evolution of conventional malware activity to more sophisticated levels, it is more accurate to characterize them as the evolution of conventional espionage techniques to target individuals and non-state organizations to a degree not commonly seen in the past. This holds true even where the motive may be purely financial.

Targeted Attacks are technically opportunistic and technology agnostic; the attacker has the resources to use whatever techniques or technologies work. Although Targeted Attacks are sometimes characterized as highly advanced attacks that exploit previously unknown vulnerabilities in software, the reality is often more mundane.[12] Attackers often attempt to leverage the target's operational weaknesses, such as exploiting long out-of-date software, or unpatched vulnerabilities to gain access to a target. After the target is compromised, the attacker attempts to secure additional footholds within the network by compromising authentication systems, disabling audit capabilities, and even manipulating patch management/deployment servers, in an effort to become stealthier, maintain their position, and better exfiltrate data. Attackers have been observed to expand the scope of such attacks by remotely turning on webcams and telephones in conference rooms to eavesdrop on confidential communications in real time.

Although purely technical attacks are not unknown, most Targeted Attacks use an element of social engineering to gain access to information and sensitive resources

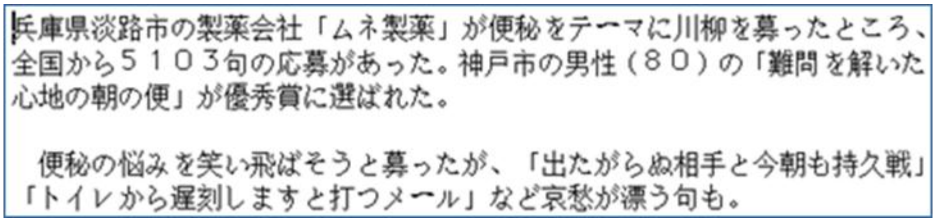
[12] www.microsoft.com/security/sir/story/default.aspx#!0day

more easily than a purely technical approach would allow. The highly targeted nature of these attacks makes it possible for a patient and thorough attacker to successfully trick even a vigilant target. Many such tactics can be considered updated versions of traditional confidence tricks in which an attacker gains the trust of the victim by appealing to basic human emotions and drives, such as curiosity, greed, compassion, and anger. Common tactics can include masquerading as a trusted party or authority figure on the telephone or in instant messenger communications in an effort to obtain the victim's network credentials, as well as customized and personalized versions of standard phishing attacks that are called *spear phishing* attacks.

In a typical spear phishing attack, the victim may receive a seemingly legitimate email that includes a malicious attachment or directs the victim to a malicious web page, in an effort to capture logon credentials or to use a browser exploit to download malware to the victim's computer. Spear phishing web pages often resemble legitimate pages on the victim's corporate intranet or externally hosted sites designed for legitimate activities, such as reviewing health insurance or employee benefit information. If the victim is accustomed to receiving internal communications about these kinds of sites, it can be difficult to distinguish between links to legitimate external sites and malicious copies.

One spear phishing technique that is often used in Targeted Attacks is the *content type attack*, in which an attacker sends an employee of the targeted organization an email message with a file attachment that contains an exploit. The attacker can individually tailor the email message to lure the recipient, making content type attacks particularly effective. Microsoft has received content type attack samples from all over the world, written in many different languages, such as the example in the following figure which announces the winner of a competition run by a pharmaceutical company.

Figure 6: Example of a lure message in Japanese

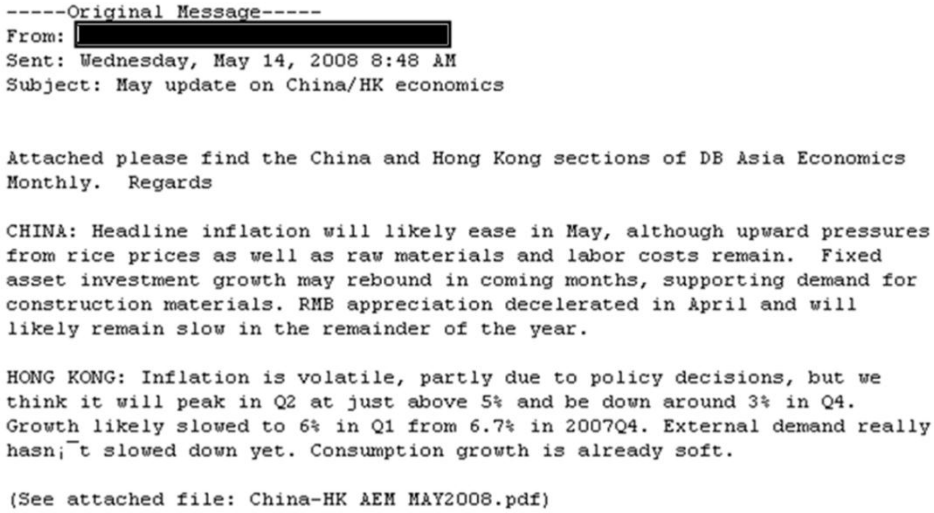


兵庫県淡路市の製薬会社「ムネ製薬」が便秘をテーマに川柳を募ったところ、全国から５１０３句の応募があった。神戸市の男性（８０）の「難問を解いた心地の朝の便」が優秀賞に選ばれた。

　便秘の悩みを笑い飛ばそうと募ったが、「出たがらぬ相手と今朝も持久戦」「トイレから遅刻しますと打つメール」など哀愁が漂う句も。

The goal of the lure email message is to trick the recipient into opening the malicious file attached to the message, and attackers use a variety of psychological tactics to accomplish this goal. Lures often masquerade as internal communications from superiors or other trusted parties, such as a trusted lawyer or business partner. A popular tactic is to represent the malicious file as containing sensitive information that the recipient might not be entitled to know, such as salary information for all of the employees in the company or department—the temptation presented by such “forbidden fruit” is often too great for recipients to resist. Another tactic is for the attacker to research the prospective recipient in advance, and then create a customized lure that appeals to the recipient’s interests, as shown in the following figure.

Figure 7: An example of a lure tailored to its recipient



```
-----Original Message-----
From: [redacted]
Sent: Wednesday, May 14, 2008 8:48 AM
Subject: May update on China/HK economics


Attached please find the China and Hong Kong sections of DB Asia Economics
Monthly.  Regards

CHINA: Headline inflation will likely ease in May, although upward pressures
from rice prices as well as raw materials and labor costs remain.  Fixed
asset investment growth may rebound in coming months, supporting demand for
construction materials. RMB appreciation decelerated in April and will
likely remain slow in the remainder of the year.

HONG KONG: Inflation is volatile, partly due to policy decisions, but we
think it will peak in Q2 at just above 5% and be down around 3% in Q4.
Growth likely slowed to 6% in Q1 from 6.7% in 2007Q4. External demand really
hasn¡¯t slowed down yet. Consumption growth is already soft.

(See attached file: China-HK AEM MAY2008.pdf)
```

In this case, the attacker determined that the recipient was someone who worked in finance and who would be especially interested in news about financial markets in Asia. Attackers sometimes send several benign messages before any malicious ones, in an effort to build a trust relationship with the recipient.

File attachments to such messages contain malicious code that attempts to exploit a vulnerability in the application which parses the information, such as a word processor or a document reader, when the file is opened. The exploit itself is typically used to install additional malware on the computer, which performs actions such as stealing or destroying files, or connecting to other network resources. As previously stated, in most cases the malicious code attempts to exploit a vulnerability that the software vendor has already addressed, which highlights the importance of keeping all software up to date.[13]

In early Targeted Attacks, the *payload*, or the actions conducted by the malware, was often performed by a trojan[14] that was specially crafted to search for specific files or types of files, and then upload them to servers controlled by the attacker. For example, one trojan used in a Targeted Attack was designed to search for computer-aided design (CAD) files, which often contain sensitive design diagrams. More recently, Targeted Attacks have been observed to use malware that allows the attacker to connect to the controlled computer, and then dynamically issue new commands, often using custom communications protocols designed to hide the traffic from detection by network monitoring software.[15]

A complicating factor in responding to Targeted Attacks is the difficulty in identifying that activity among the myriad of other cyberthreats that organizations may encounter on a daily basis. According to volume 12 of the *Microsoft Security Intelligence Report (SIR)*,[16] more than 700 million pieces of malware were detected on computers around the world in the second half of 2011. Identifying specific Targeted Attacks within this large threat ecosystem can be challenging for several reasons:[17]

- There are many different malicious actors.
- These actors have many different motives.
- The attacks can look similar, so the nature of the attack does not always help to identify the actor and the motive.
- The internet is a shared and integrated domain, where it is not easy to distinguish well-meaning and malicious network activity.

Attributing a Targeted Attack that has been successfully detected is central to many of these challenges. In some countries, law enforcement, the military, intelligence agencies and the private sector therefore attempt to cooperate in building a picture of the threat environment. Conclusive evidence of the “who” and “why” is often though unavailable when a system is under attack, which can

[13] blogs.technet.com/b/security/archive/2011/09/28/targeted-attacks-and-the-need-to-keep-document-parsers-updated.aspx
[14] www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx#t
[15] blogs.technet.com/b/security/archive/2011/09/28/targeted-attacks-and-the-need-to-keep-document-parsers-updated.aspx
[16] www.microsoft.com/sir
[17] Charney, Scott – Rethinking the Cyber Threat – A Framework and Path Forward www.microsoft.com/download/en/details.aspx?id=747

make appropriate national and organizational level responses challenging. For example, the attackers usually demonstrate operational sophistication and sometimes operate in shifts, aligning their operations to the time-zone in which the target organization or individual is located. Some attackers have even observed the same public holidays as their targets, regardless of their own physical location. Without additional information, the use of attack timing to locate the attackers can therefore have limited benefit and may even be used to mislead.

However, while attribution may never be perfect, improved categorization of specific attacks, supported by effective sharing of that information between effected parties, can help inform what an appropriate response might be. Being aware of whether the aim of a specific attack is financial crime or the theft of intellectual property, even if the actors remain unknown, will have a meaningful impact on how an organization defends itself.

Challenges in defending against Targeted Attacks

For many organizations the risks posed by the existence of Determined Adversaries presents a novel challenge. It is therefore vital for organizations to develop and implement plans that consider the possibility of Targeted Attacks. Every organization would be wise to closely evaluate their existing risk management programs, and make necessary adjustments to help reduce their overall level of vulnerability by making balanced investments in prevention, detection, containment and recovery.

The risk management challenge

Over the past 25 years, IT and information security have become more commoditized and based on a common security model, in which the focus is on infrastructure rather than asset protection. As internet technology has become cheaper and accepted as the industry standard, the emphasis has been on commercial off-the-shelf, easily deployable security mitigations to address generic threats on an enterprise wide basis. Such an approach was largely sufficient for non-military organizations 10 years ago, but during the last five years, the number of Targeted Attacks reported in industry has generally increased. And while the implementation of uniform commoditized security solutions is an important component in addressing opportunistic threats, enhanced risk management practices are more important than ever to ensure the adoption of appropriate mitigation measures to counter the more sophisticated attacks which will focus on specific assets.

However, while risk management is a well understood discipline, the most commonly taken approach has challenges when applied to addressing cyber risks, including Targeted Attacks. Since the threat environment is constantly changing, past successes in managing cyber risks are not reliable indicators of actual security and the sole basis for future planning. Additionally, many organizations have determined which risks should be managed by elevating various concerns to senior management. Managers then considered these concerns and evaluated them relative to each other, before ultimately allocating resources appropriately across the risks. According to Aon's 2011 Global Risk Management Survey, many organizations still use this method. "Senior management's intuition and experience remains the primary method used by survey respondents to identify and assess major risks facing their organizations."[18]

This intuitive approach is bound to fail, because senior management cannot possibly understand and assess the full breadth and depth of today's cyber risks. It is also the case that, unlike many corporate risk assessments relating to security, the question of probability is a moot point. For most organizations some degree of internal compromise of computer systems is inevitable.

Considerations of the appropriate in-depth approaches to risk management are beyond the scope of this paper. It is though worth noting that regardless of the analysis and assessment models employed, addressing Targeted Attacks does specifically require that digital assets are identified, the potential business impacts of their compromise is understood and that the potential motivations and capabilities of Determined Adversaries are reflected in the deployment of countermeasures.

Prevention

Despite the high likelihood of compromise, prevention continues to be a priority in ensuring effective risk management. Commodity security solutions, such as firewalls and antimalware products, continue to offer wide ranging protection against a variety of generic threats and are essential in ensuring network hygiene.

Research has though shown that poorly configured systems—those that do not have security settings applied correctly, or those that do not have security updates applied in a timely manner—continue to be exploited in attacks. For example, volume 9 of the *Microsoft Security Intelligence Report (SIR)* contains analysis of a sample set of attacks involving exploitation of vulnerabilities in document parsing software, such as Microsoft Office. This analysis shows that—in the sample set examined—the targeted systems were compromised by exploiting software vulnerabilities after the software vendor had released a security update to address them. In some cases, the security update had been available for more than five years.

[18] www.aon.com/risk-services/thought-leadership/reports-pubs_2011_grms.jsp

Many organizations develop their own software applications and some of these, particularly when internet facing, can be a vector through which to compromise associated databases and other internal systems. Such organizations should therefore consider adoption and implementation of proactive mitigations, including the use of a software security assurance process, such as the Microsoft Security Development Lifecycle (SDL).[19]

It is also worth noting that the cumulative effect of effective detection, containment and recovery measures also provide a protective effect. This is because as target organizations increase their own capabilities, the likelihood of the Targeted Attack being successful is reduced. Combined with increased information sharing between organizations this can alter the risk reward equation for the attacker, who may then become more selective as to who is targeted.

Detection

Even well protected environments will be targeted by Determined Adversaries who are technology agnostic and undeterred by traditional defenses.[20] However, the deployment of intrusion detection and advanced analytics solutions that observes the real-time health of networks involves more than traditional network monitoring. In addition to security data from intrusion detection systems, organizations can also use information provided by IT assets such as routers, hosts, and proxy servers to evaluate operational and security status. The large amounts of monitoring and audit data generated by these solutions must ultimately be turned into insights that can be used to inform more effective cyber security responses. Such responses may be operational, as discussed later in this section, or they can be more strategic and involve changes in policies, controls, and oversight measures. They can also result in combinations of both, with operational incidents informing longer-term decisions.

Regardless, for this to happen, organizations must have the right data, and analyze that data in context for that data to drive action. Fusing together disparate data from a variety of organizations and systems to create a common operational picture is challenging. And building the analytic capabilities (for example, correlation) to derive valuable insights is even more difficult and is as dependent

[19] www.microsoft.com/sdl

[20] Charney, Scott – Rethinking the Cyber Threat – A Framework and Path Forward www.microsoft.com/download/en/details.aspx?id=747

upon the application of human skills as it is on technology. These skills still scarce and the recruitment of suitably skilled individuals is a significant challenge.

Containment

In many cases, the initial compromise of an environment will not immediately result in the attacker achieving their ultimate goal. Instead they will often need to reconnoiter the environment and compromise multiple additional systems. Effective operational security designs and utilization of native security features can help. For example, if the targeted organization has configured its environment with this potential threat in mind, it is possible to contain the attacker's activities and thereby buy time to detect, respond to, and mitigate the attack. In most cases, the security features required to contain attacks already exists. Existing environments, however, are often architected to mitigate opportunistic rather than Targeted Attacks. To contain an attack, consideration should therefore be given to architecting domain administration models that limit the availability of administrator credentials and applying available technologies such as IPsec based network encryption to restrict unnecessary interconnectivity on the network.

Recovery

The purpose and challenge of recovery is to mitigate the range of harmful impacts that may result from a successful compromise of critical assets.

Because of this possibility, the best approach is to be prepared with a well-conceived recovery plan, supported by suitably skilled response capability. Where many organizations fail in this regard is due to the separation of business, security, and IT operations groups—these teams must work together to ensure the highest, most effective degree of recovery capability. It is therefore advisable to maintain a "crisis committee" to set business recovery priorities and engage in desktop and other exercises to test the organization's ability to recover from different attack scenarios.

The exact capabilities required by organizations may differ, and may need to be reinforced with external expertise. In general though, the capabilities required should cover IT operations, investigations, effected business units, legal counsel and communications.

Maintaining customer confidence immediately following a breach through clear and timely messaging is also extremely important in protecting brands, as well as mitigating the direct impact on customers.

Communication and Information Sharing

The challenges to effective risk management in relation to Targeted Attacks have already been stated. The ability for risk management processes to effectively inform the operational needs for protection, detection, containment and recovery is made even more difficult if the necessary information is unavailable. Establishing sources of actionable information, whether through public sources or through specific relationships, is therefore vital.

Communicating openly about what happened to a victim organization can help other similar organizations take appropriate measures to avoid the same fate. However, it is not enough to simply share information. The key to successful information sharing is to be clear about the practical outcome. For example, an organization may share the internet address of a system that is attacking it so that other organizations can block that same address, or an organization may want to share their analysis of an event to see if other organizations have seen similar patterns of attack.

Sharing information about Targeted Attacks is very hard. This is in part because sharing information on these attacks might have consequences for an organization's brand, regulatory compliance, shareholder concern, and its bottom line. Selective sharing between private organizations is though possible, and has been demonstrated to have a high level of effectiveness and is worth the investment.

The Role of Governments

Besides the protection of their own systems, an important role for governments is to create environments in which their constituents (organizations and individuals) can most effectively protect themselves from Targeted Attacks. The following efforts by governments can help constituents protect themselves:

- Clearly communicate the realities of the threat environment to citizens, companies and investors so that organizations are more comfortable reporting the key aspects of breaches. This reporting can encourage learning from previous incidents and bolster specific defenses to protect key assets in the future.

- Making an organization aware that there is reason to believe they may be the target of a Determined Adversary is a critical first step in protecting their critical assets. Governments may have sources of attribution and expertise in threat assessment that provide valuable insights into the intents, motivations and capabilities of Determined Adversaries. This information, which is distinct from the technical data associated with a specific attack, should be communicated to those organizations considered to be at threat to inform their risk management decisions.

- Create a climate that encourages the exchange of technical data (at the unclassified level as much as possible) between public and private organizations to enable meaningful outcomes, with rules and mechanisms that permit both sides to protect sensitive data. This approach represents a shift from past practices that viewed information sharing as an objective itself, as opposed to a tool. It must be a two-way sharing process, in which targeted organizations share details of attacks that take place against them with governments, and governments share intelligence about the current threat environment and potential future threats. To be an effective tool against Targeted Attacks, analysis of security logs, alerts, and other intelligence information needs to take place in near-real time, which will require the establishment of solid public/private partnerships.[21]

- Some governments believe that their national security is dependent on economic security. They may therefore sponsor, or tacitly condone through inaction, the use of Targeted Attacks for stealing intellectual property to support indigenous industries. This approach is ultimately nearsighted because it inhibits the development of indigenous innovation. Governments therefore have a responsibility to address their philosophical differences and use the tools at their disposal, such as diplomacy and national policy, to establish appropriate international norms of behavior.[22]

[21] Written Testimony of Scott Charney Before the Senate Committee on Homeland Security and Governmental Affairs, February 2012 www.hsgac.senate.gov/download/?id=63aa804a-eb21-45fc-8cb1-014439327fdd

[22] Charney, Scott – Rethinking the Cyber Threat – A Framework and Path Forward www.microsoft.com/download/en/details.aspx?&id=747

Conclusion

Targeted Attacks carried out by Determined Adversaries are not a new phenomenon; political, military, and even commercial espionage has existed in some form for hundreds of years. Over the past three decades, the global connectivity of the internet, together with the lack of traceability and the ability to remain anonymous online, has opened up new attack vectors.

Successfully combatting such threats requires coordinated action between the public and private sectors, and an increased focus on risk management and incident response in regard to Targeted Attacks. The following summarizes these calls to action:

- **Establish a culture that promotes information exchange**. Fast, comprehensive information sharing is vital to help address the threat of Targeted Attacks. Such information sharing requires establishing a climate in which victims are sufficiently confident to share details of the attacks against them, and to enable governments to share details of the evolving threat ecosystem from their perspectives. Governments should work toward the creation and harmonization of global laws that protect cyberspace, and enable information sharing (including technical information about the Targeted Attacks and threat assessments about the Determined Adversaries) across international boundaries. How individual countries do this domestically might differ, but the desired outcome is a shared objective.
- Make risk management a key strategy for organizations, businesses, and governments seeking to prevent, detect, contain and respond to the threat of Targeted Attacks. A key element of risk management strategies must be the assumption that the organization either will be - or already has been - compromised. Another key is to create action plans that thoroughly analyze what the bad actors will do if they compromise an organization's high value assets. The goal is effective risk management; risk elimination is not possible.
- **Make creation and active operation of an analytical security enterprise a priority.** Even well protected environments will be targeted by determined adversaries, who are technology agnostic and persistent. The deployment of

intrusion detection and advanced analytics solutions that observe the real-time health and security condition of networks involves more than traditional network monitoring. In addition to security data from intrusion detection systems, organizations can also use information provided by IT assets such as routers, hosts, and proxy servers to evaluate operational and security status. The large amounts of monitoring and audit data generated by these solutions must ultimately be turned into insights that can be used to inform more effective cyber security responses.

- **Make establishing a solid incident management and response function a vital activity**, at an organizational level and at an international level. Organizations should ensure that they have the capability to react appropriately to an attack when detected, contain the attacker, and then recover from the attack. Response plans should include robust communications plans (internal and external) to help ensure that speculation and assumption do not cause additional damage. Internationally, adequate response capability and capacity needs to be built in to countries around the world. Organizations and governments should establish points of contact that are available 24 hours a day, 7 days a week to help facilitate the response process. It would be prudent for these points of contact to be established before an attack takes place.

Worldwide threat assessment

Vulnerabilities

Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of the software or the data that it processes. Some of the worst vulnerabilities allow attackers to exploit the compromised system by causing it to run malicious code without the user's knowledge.

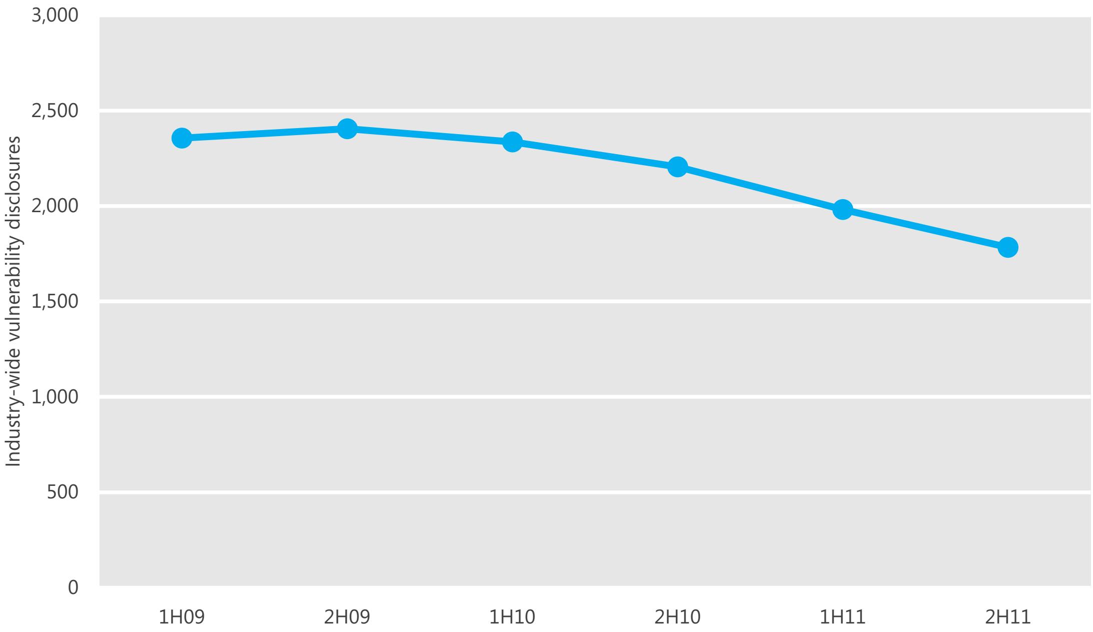
Industry-wide vulnerability disclosures

A *disclosure*, as the term is used in the *Microsoft Security Intelligence Report*, is the revelation of a software vulnerability to the public at large. It does not refer to any type of private disclosure or disclosure to a limited number of people. Disclosures can come from a variety of sources, including the software vendor, 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.nist.gov), the U.S. government repository of standards-based vulnerability management. It represents all disclosures that have a CVE (Common Vulnerabilities and Exposures) identifier.

Figure 8 illustrates the number of vulnerability disclosures across the software industry for each half-year period since 1H09. (See "About this report" on page vi for an explanation of the reporting period nomenclature used in this report.)

Figure 8. Industry-wide vulnerability disclosures, 1H09–2H11

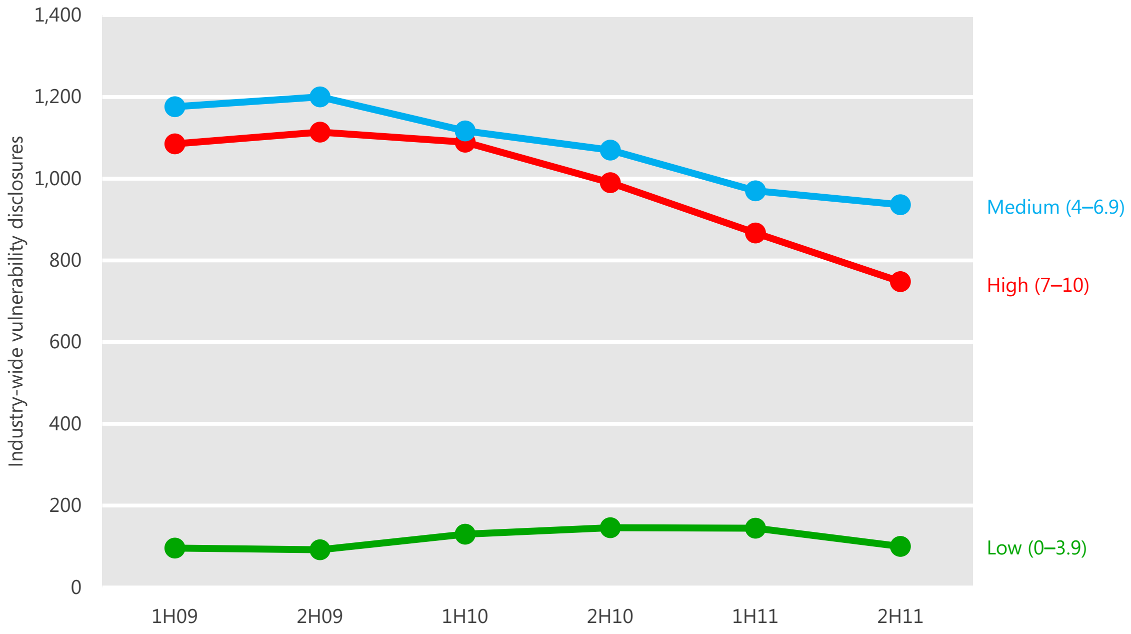


- Vulnerability disclosures across the industry in 2H11 were down 10.0 percent from 1H11, and down 24.3 percent from 1H09.
- This decline continues an overall trend of moderate declines since 2006. This trend is likely because of better development practices and quality control throughout the industry, which results in more secure software and fewer vulnerabilities from major vendors, who are most likely to have their vulnerabilities associated with a distinct CVE identifier. (See Protecting Your Software in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website for additional details and guidance about secure development practices.)

Vulnerability severity

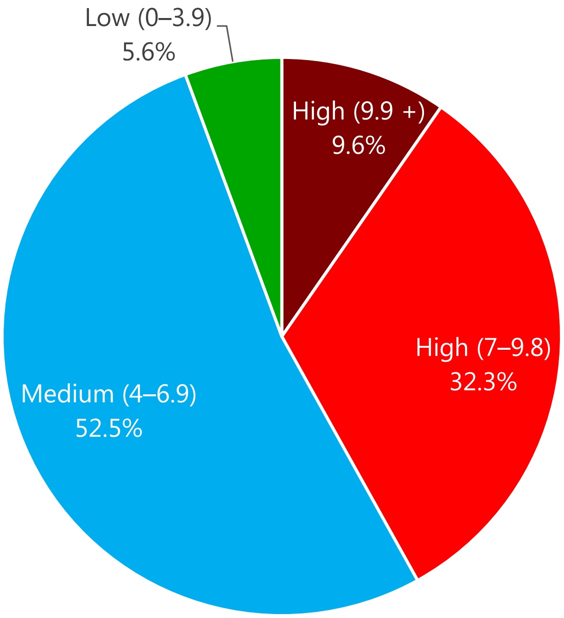
The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities. The CVSS base metric assigns a numeric value between 0 and 10 to vulnerabilities according to severity, with higher scores representing greater severity. (See Vulnerability Severity at the *Microsoft Security Intelligence Report* website for more information.)

Figure 9. Industry-wide vulnerability disclosures by severity, 1H09–2H11



- The overall vulnerability severity trend has been a positive one. All three CVSS severity classifications decreased between 1H11 and 2H11, with the Medium and High-severity classifications continuing a trend of declining disclosures in every period since 2H09.
- Medium-severity vulnerabilities again accounted for the largest number of disclosures at 936, a 3.5 percent decrease from 1H11.
- High-severity vulnerabilities decreased 31.0 percent from 1H11, continuing a near-constant rate of decline since 1H10.
- Low-severity vulnerabilities, which had increased slightly over the past several periods, decreased 13.7 percent from 1H11.
- Mitigating the most severe vulnerabilities first is a security best practice. High-severity vulnerabilities that scored 9.9 or greater represent 9.6 percent of all vulnerabilities disclosed in 2H11, as Figure 10 illustrates. This figure was down from 10.6 percent of all vulnerabilities in 1H11.

Figure 10. Industry-wide vulnerability disclosures in 2H11, by severity

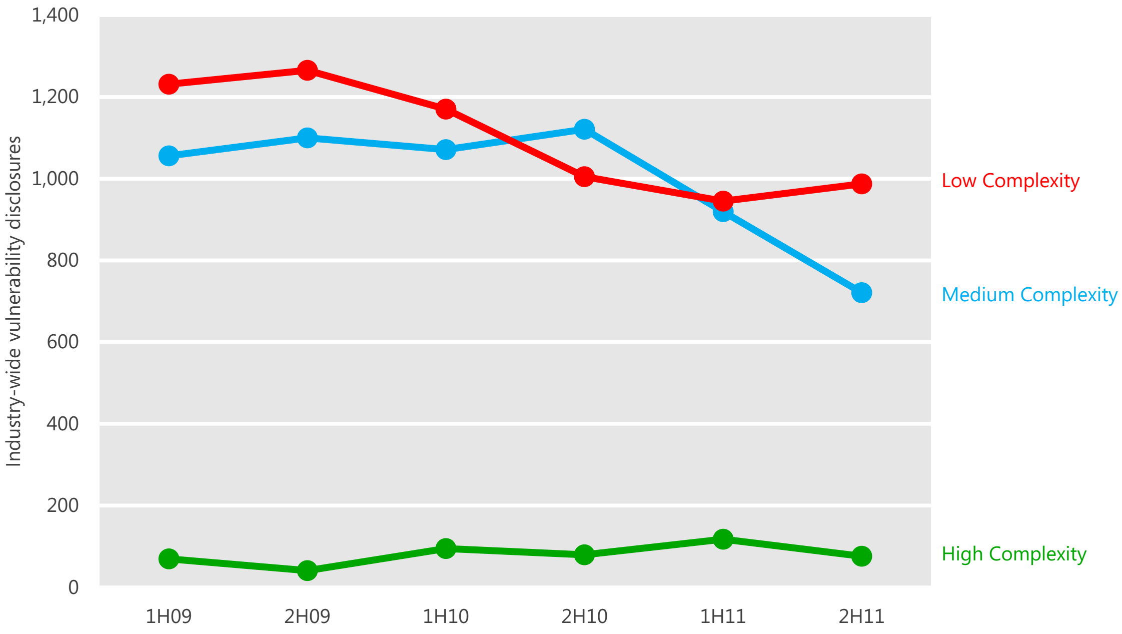


Vulnerability complexity

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

The CVSS assigns each vulnerability a complexity ranking of Low, Medium, or High. (See Vulnerability Complexity at the *Microsoft Security Intelligence Report* website for more information about the CVSS complexity ranking system.) Figure 11 shows complexity trends for vulnerabilities disclosed since 1H09. Note that Low complexity indicates greater risk, just as High severity indicates greater risk in Figure 9.

Figure 11. Industry-wide vulnerability disclosures by access complexity, 1H09–2H11

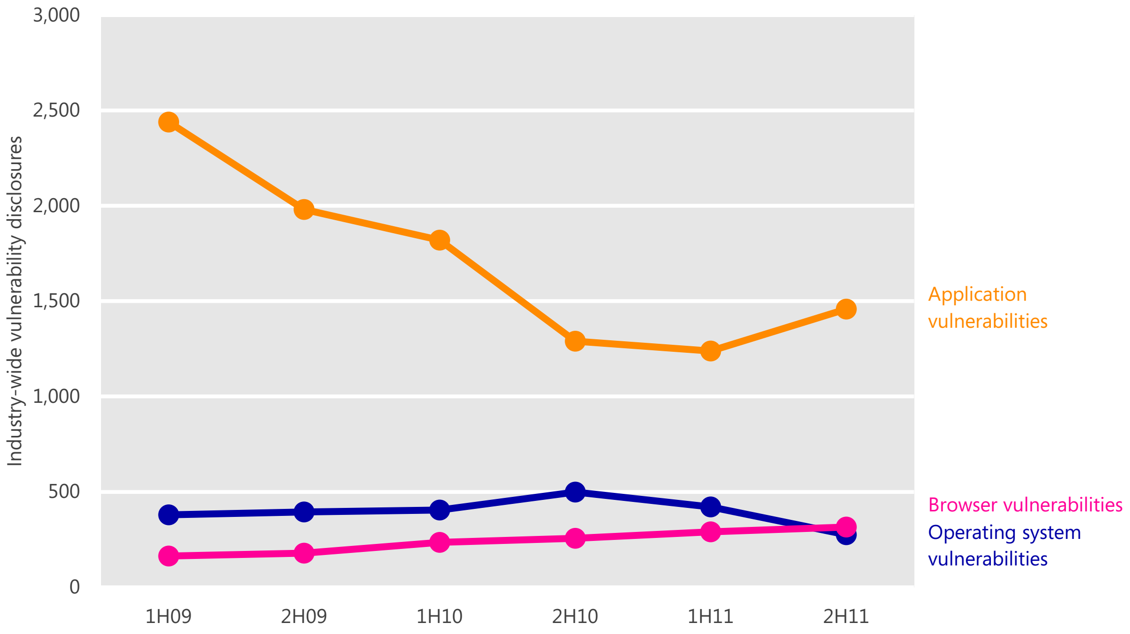


- Low-complexity vulnerabilities—those that are the easiest to exploit—accounted for 55.3 percent of all disclosures in 2H11. A total of 987 Low-complexity vulnerabilities were disclosed in 2H11, an increase from 945 in 1H11 but less than the 1,005 disclosed in 2H10.
- Medium-complexity vulnerabilities amounted for 40.4 percent of disclosures in 2H11. Disclosures of Medium-complexity vulnerabilities have decreased significantly over the past year, from 1,121 in 2H10 to 721 in 2H11.
- High-complexity vulnerability disclosures declined slightly to 76 in 2H11, a decrease from 118 in 1H11. Disclosures of High-complexity vulnerabilities have been stable or slightly increasing over the past several years, but still only account for 4.3 percent of all vulnerabilities disclosed in 2H11.

Operating system, browser, and application vulnerabilities

Figure 12 shows industry-wide vulnerabilities for operating systems, browsers, and applications since 1H09. (See Operating System, Browser, and Application Vulnerabilities at the *Microsoft Security Intelligence Report* website for an explanation of how operating system, browser, and application vulnerabilities are distinguished.)

Figure 12. Industry-wide operating system, browser, and application vulnerabilities, 1H09–2H11

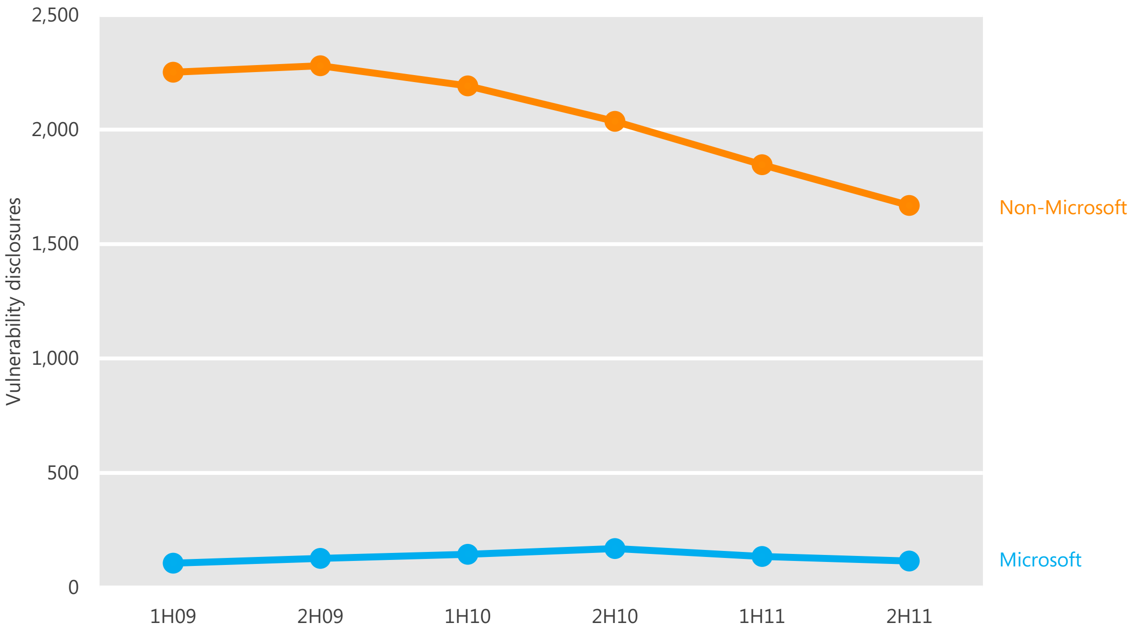


- Disclosures of application vulnerabilities increased 17.8 percent in 2H11, halting a trend of declining disclosures that extends back several periods. In all, applications accounted for 71.2 percent of all vulnerability disclosures in 2H11.
- Operating system vulnerability disclosures decreased 34.7 percent in 2H11, and ranked below browser vulnerability disclosures for the first time since at least 2003.
- Disclosures of vulnerabilities in web browsers increased 8.6 percent in 2H11, continuing a trend of small increases over each of the last several periods.

Microsoft vulnerability disclosures

Figure 13 charts vulnerability disclosures for Microsoft and non-Microsoft products since 1H09.

Figure 13. Vulnerability disclosures for Microsoft and non-Microsoft products, 1H09–2H11



- Vulnerabilities in Microsoft products accounted for 6.4 percent of all vulnerabilities disclosed in 2H11, a decrease from 6.8 percent in 1H11.
- Vulnerability disclosures for Microsoft products have generally remained stable over the past three years, though Microsoft's percentage of all disclosures industry-wide has increased slightly, primarily because of the overall decline in vulnerability disclosures across the industry.

Guidance: Developing secure software

The Security Development Lifecycle (www.microsoft.com/sdl) is a 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 vulnerabilities in the software and help manage vulnerabilities that might be found after deployment. (For more in-depth information about the SDL and other techniques developers can use to secure their software, see Protecting Your Software in the "Managing Risk" section of the *Microsoft Security Intelligence Report* website.)

Exploits

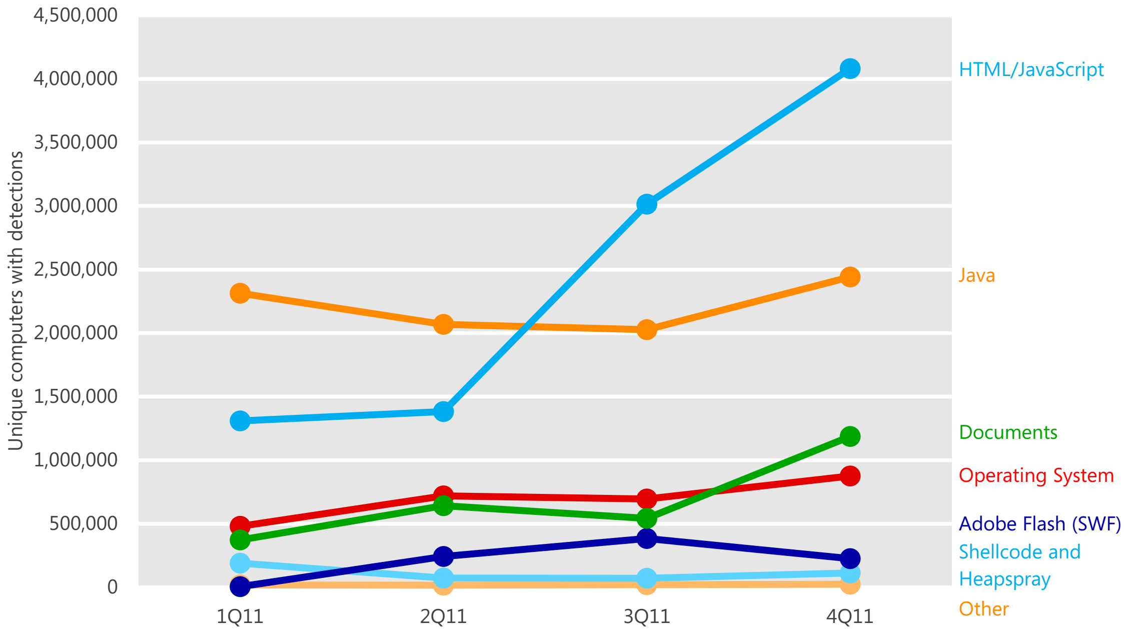
An *exploit* is malicious code that takes advantage of software vulnerabilities to infect, disrupt, or take control of a computer without the user's consent and usually without the user's knowledge. Exploits target vulnerabilities in operating systems, web browsers, applications, or software components that are installed on the computer. In some scenarios, targeted components are add-ons that are pre-installed by the computer manufacturer before the computer is sold. A user may not even use the vulnerable add-on or be aware that it is installed. 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.

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.[23]

Figure 14 shows the prevalence of different types of exploits detected by Microsoft antimalware products each quarter in 2011, by number of unique computers affected.[24] (See "Appendix B: Data sources" on page 107 for more information about the products and services that provided data for this report.)

[23] See www.microsoft.com/technet/security/Current.aspx to search and read Microsoft Security Bulletins.
[24] In previous volumes of the *Microsoft Security Intelligence Report*, individual attack counts, rather than unique computers, were often used to report exploit data. Comparison of the exploit figures in this volume with corresponding figures in previous volumes is not appropriate.

Figure 14. Unique computers reporting exploits each quarter in 2011, by targeted platform or technology



- The number of computers reporting exploits delivered through HTML or JavaScript increased steeply in the second half of 2011, due primarily to the emergence of JS/Blacole, a family of exploits used by the so-called "Blackhole" exploit kit to deliver malicious software through infected web pages. Prospective attackers buy or rent the Blacole kit on hacker forums and through other illegitimate outlets. It consists of a collection of malicious web pages that contain exploits for vulnerabilities in versions of Adobe Flash Player, Adobe Reader, Microsoft Data Access Components (MDAC), the Oracle Java Runtime Environment (JRE), and other popular products and components. When the attacker installs the Blacole kit on a malicious or compromised web server, visitors who don't have the appropriate security updates installed are at risk of infection through a drive-by download attack. (See page 100 for more information about drive-by download attacks.)

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

  - Get gamed and rue the day (October 25, 2011)
  - Disorderly conduct: localized malware impersonates the police (December 19, 2011)

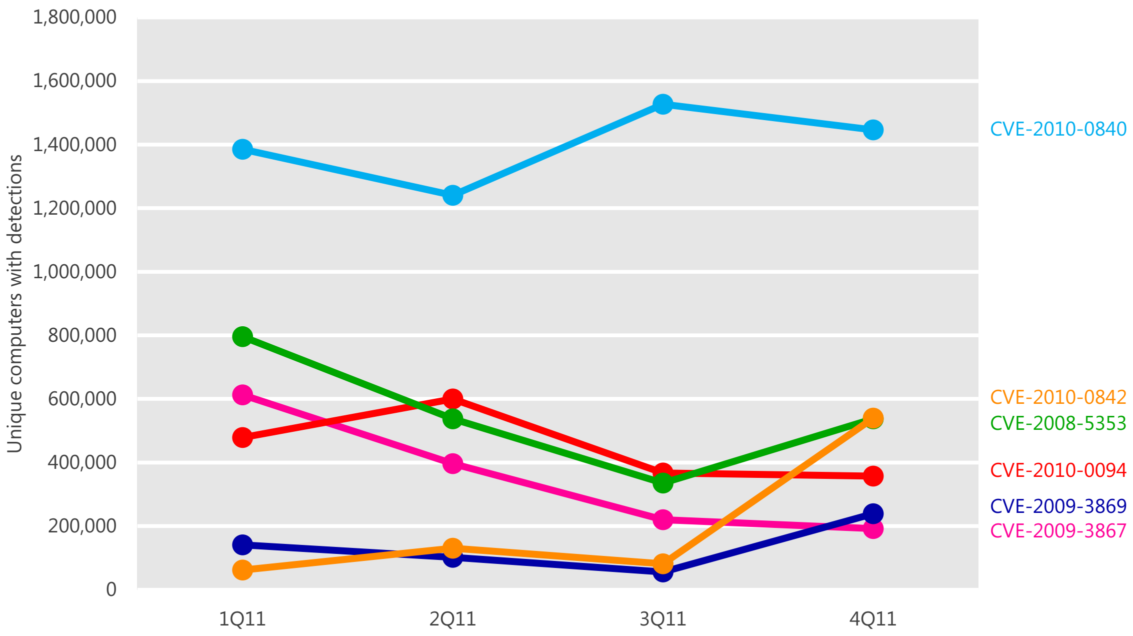
  - Plenty to complain about with faux BBB spam (January 12, 2012)

- Java exploits, formerly the most commonly observed type of exploits, were relegated to second place in 3Q11 and 4Q11 because of the rise in HTML/JavaScript exploits; despite this, the number of computers reporting Java exploit detections remained at a high level during 3Q11 and 4Q11, and actually increased overall from the first half of the year.
- Detections of exploits that target vulnerabilities in document readers and editors increased in 4Q11, making them the third most commonly detected type of exploit during the quarter, due primarily to a rise in exploits that target older versions of Adobe Reader.

Java Exploits

Figure 15 shows the prevalence of different Java exploits by quarter.

Figure 15. Unique computers reporting Java exploits each quarter in 2011



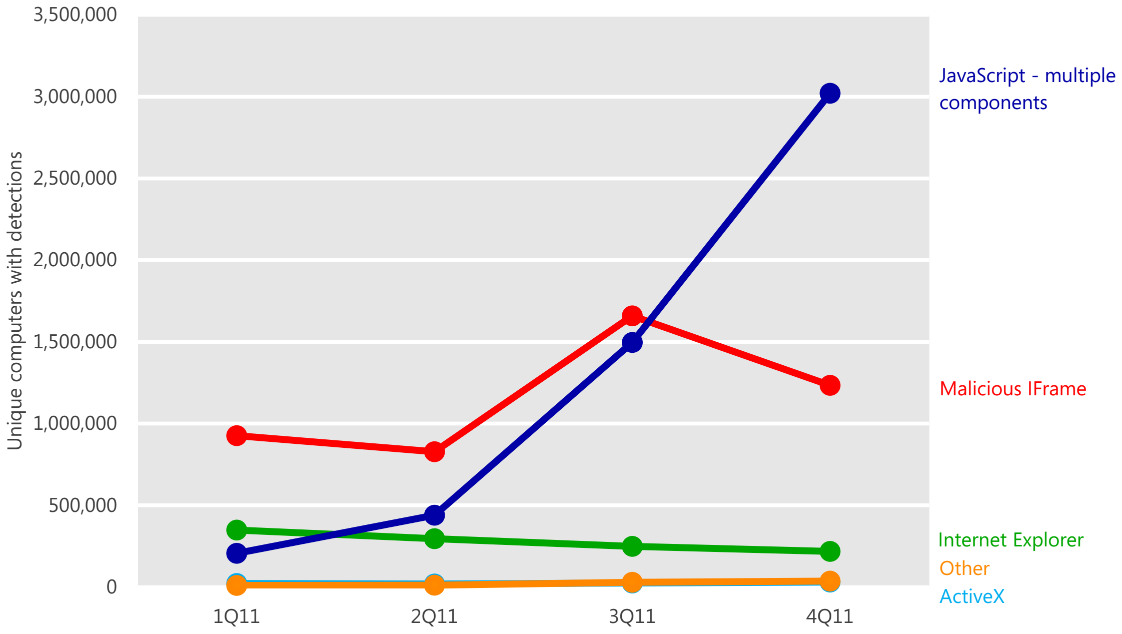
- As in previous periods, many of the more commonly exploited Java vulnerabilities are several years old, as are the security updates that have been released to address them.

- The most commonly exploited Java vulnerability throughout 2011 was CVE-2010-0840, a Java Runtime Environment (JRE) vulnerability first disclosed in March 2010 and addressed with an Oracle security update the same month. The CVE-201-0840 vulnerability is exploited by the JS/Blacole exploit kit andthe trojan downloader family Java/OpenConnection.
- CVE-2010-0842, which saw significantly increased exploitation beginning in 4Q11, is also associated with the Blacole kit.
- CVE-2008-5353, the third most commonly exploited Java vulnerability in 3Q11 and 4Q11, was first disclosed in December 2008. This vulnerability affects JVM version 5 up to and including update 22, and JVM version 6 up to and including update 10. It allows an unsigned Java applet to gain elevated privileges and potentially have unrestricted access to a host system, outside its "sandbox" environment. Sun Microsystems released a security update that addressed the vulnerability on December 3, 2008.
- CVE-2010-0094 was the second most commonly exploited Java vulnerability in 2Q11, but declined to fourth by 4Q11. This vulnerability was first disclosed in December 2009, and affects JRE versions up to and including update 18 of version 6. CVE-2010-0094 allows an unsigned Java applet to gain elevated privileges and potentially have unrestricted access to a host system, outside its sandbox environment. Oracle released a security update that addressed the vulnerability in March 2010.

HTML and JavaScript exploits

Figure 16 shows the prevalence of different types of HTML and JavaScript exploits during each of the four most recent quarters.

Figure 16. Types of HTML and JavaScript exploits detected and blocked by Microsoft antimalware products each quarter in 2011

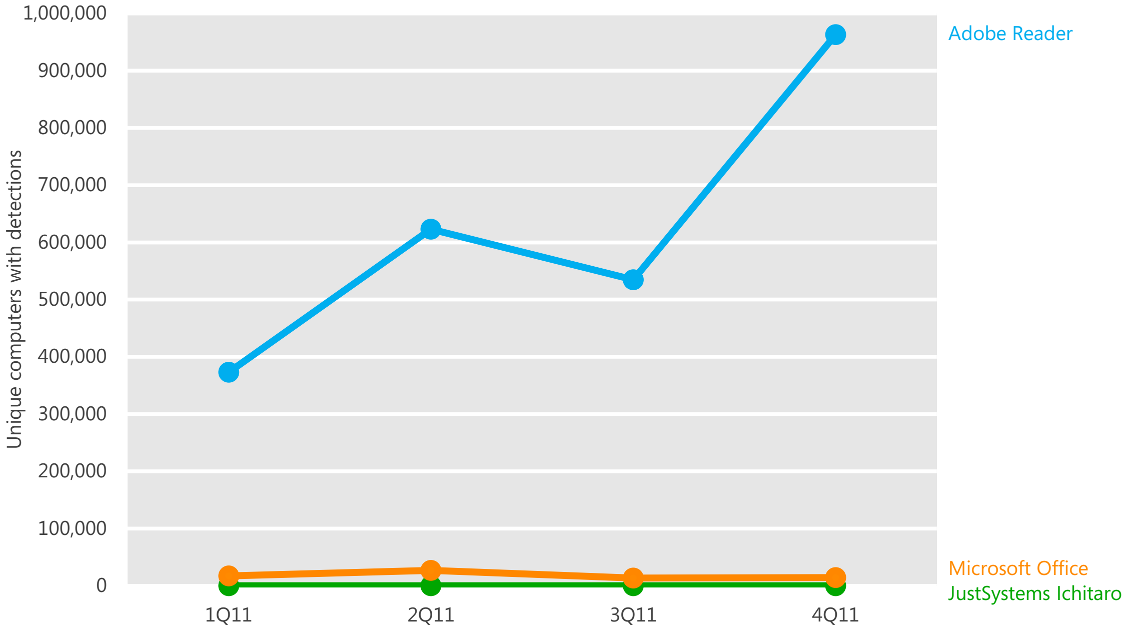


- The use of malicious JavaScript code designed to exploit one or more web-enabled technologies increased significantly in the second half of 2011, due primarily because of JS/Blacole.A, a malicious script that attempts to load a number of exploits associated with the Blacole exploit kit.
- Exploits that involve malicious HTML inline frames (IFrames) increased in the second half of 2011, although detections in 4Q11 were down from 3Q11. These exploits are typically generic detections of inline frames that are embedded in web pages and link to other pages that host malicious web content. These malicious pages use a variety of techniques to exploit vulnerabilities in browsers and plugins; the only commonality is that the exploit can be delivered through an inline frame. The exact exploit delivered and detected by one of these signatures may be changed frequently.
- Detections for specific Windows® Internet Explorer® exploits declined slowly throughout 2011.
- ActiveX® and other types of browser exploitation remain comparatively low.

Document parser exploits

Document parser exploits are exploits that target vulnerabilities in the way a document editing or viewing application processes, or parses, a particular file format. Figure 17 shows the prevalence of different types of document parser exploits during each of the four most recent quarters.

Figure 17. Types of document parser exploits detected and blocked by Microsoft antimalware products each quarter in 2011

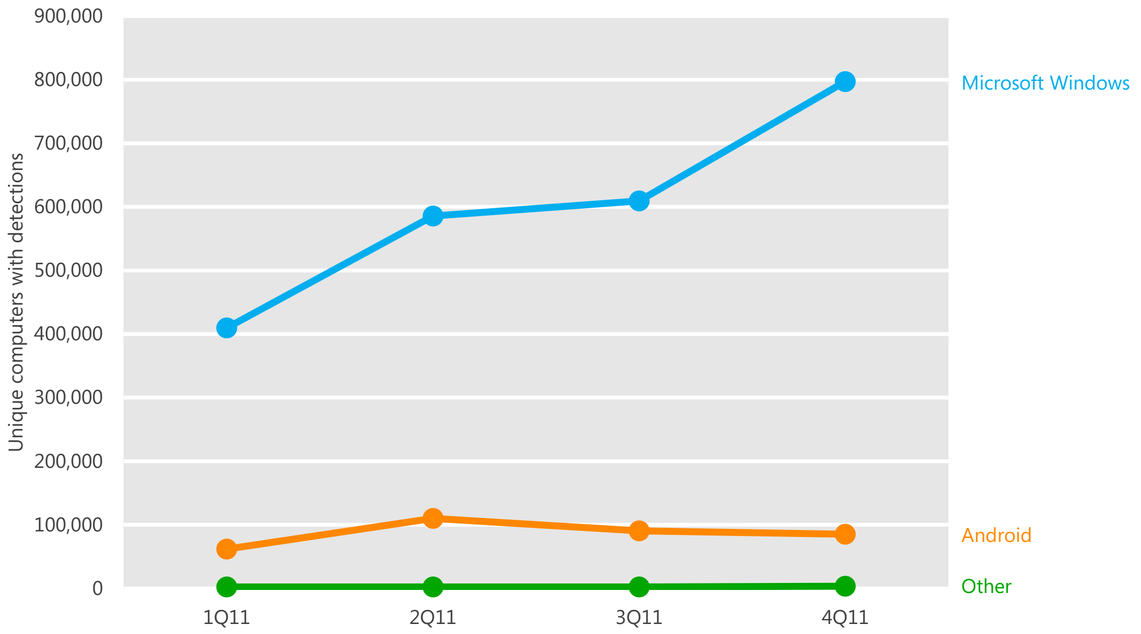


- Exploits that affect Adobe Reader and Adobe Acrobat accounted for most document format exploits detected throughout the last four quarters. Most of these exploits were detected as variants of the generic exploit family Win32/Pdfjsc. As with many of the exploits discussed in this section, Pdfjsc variants are known to be associated with the JS/Blacole exploit kit. In most cases, the vulnerabilities targeted by these exploits had been addressed with security updates or new product versions several months or years earlier.
- Exploits that affect Microsoft Office and Ichitaro, a Japanese-language word processing application published by JustSystems, accounted for a small percentage of exploits detected during the period.

Operating system exploits

Although most operating system exploits detected by Microsoft security products are designed to affect the platforms on which the security products run, computer users sometimes download malicious or infected files that affect other operating systems. Figure 18 shows the prevalence of different exploits against operating system vulnerabilities that were detected and removed by Microsoft antimalware products during each of the past four quarters.

Figure 18. Exploits against operating system vulnerabilities detected and blocked by Microsoft antimalware products each quarter in 2011

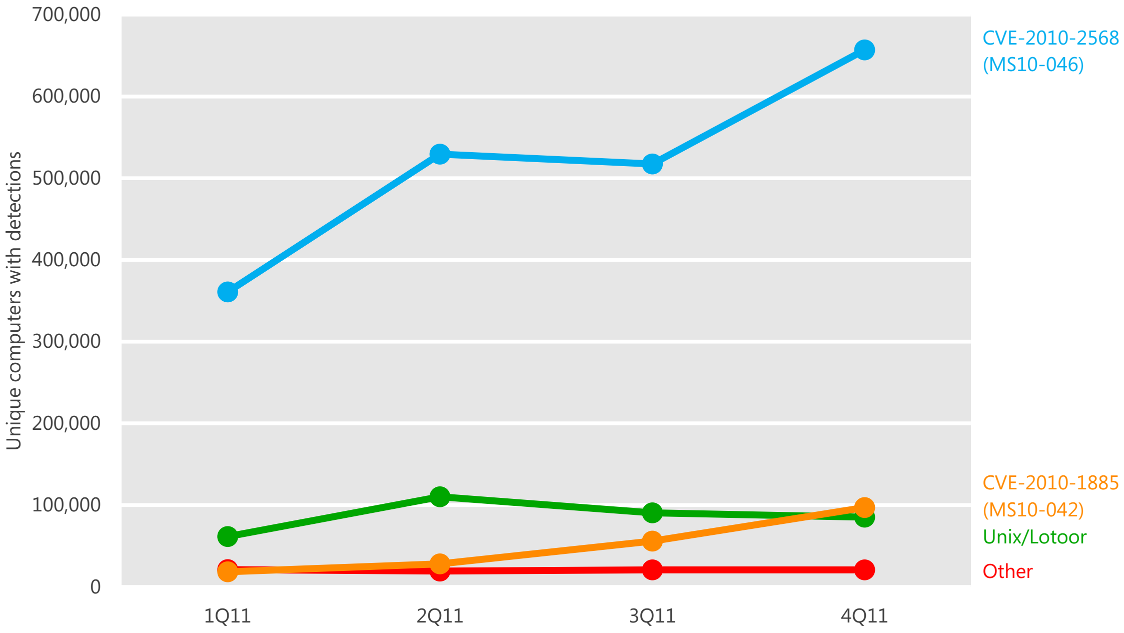


- Exploits that target Windows increased throughout 2011, almost entirely because of an increase in detections of exploit attempts that target CVE-2010-2568, a vulnerability in Windows Shell addressed by Microsoft Security Bulletin MS10-046. See Figure 19 on page 49 for more information about these exploits. Exploits that affect the Android mobile operating system published by Google and the Open Handset Alliance were detected in significant volume throughout 2011. Microsoft security products detect these threats when Android users download infected or malicious programs to their computers before transferring the software to their devices. The increase in

Android-based threats has been driven primarily by Unix/Lotoor, a detection for programs that attempt to exploit certain vulnerabilities in order to gain root access to the device. Lotoor is dropped by the trojan family AndroidOS/DroidDream, which often masquerades as a legitimate Android application. Google published a security update in March 2011 that addressed the vulnerability.

For another perspective on these exploits and others, Figure 19 shows trends for the individual exploits most commonly detected and blocked or removed in 2011.

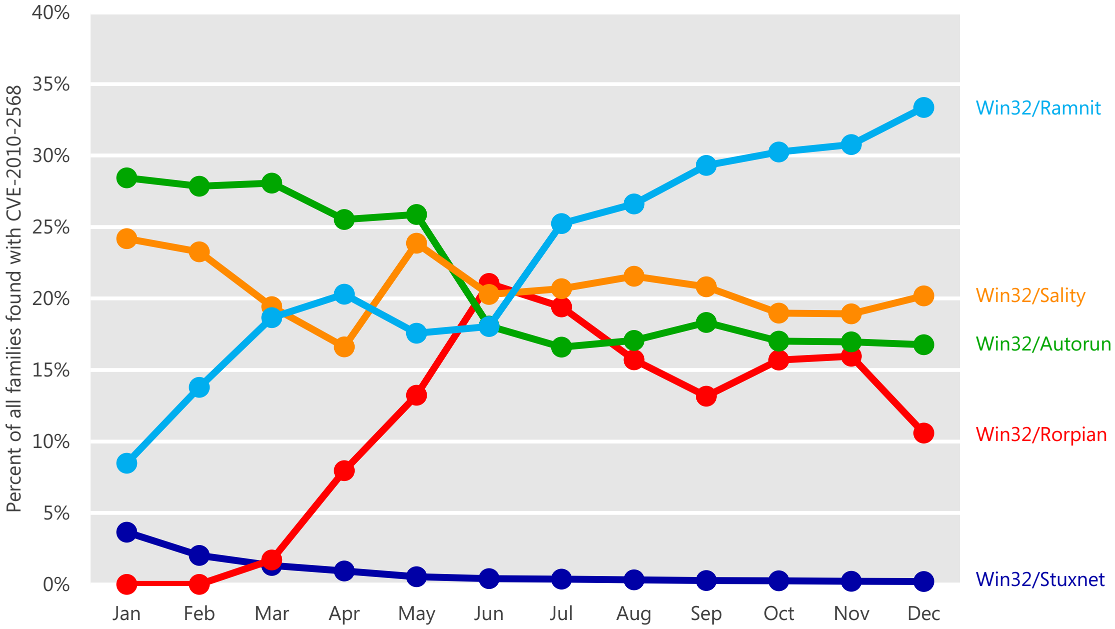
Figure 19. Individual operating system exploits detected and blocked by Microsoft antimalware products each quarter in 2011, by number of unique computers exposed to the exploit



- Exploits that target CVE-2010-2568, a vulnerability in Windows Shell, increased significantly throughout 2011, and were responsible for nearly the entire increase in Windows exploit detections seen throughout the year. Microsoft issued Security Bulletin MS10-046 in August 2010 to address the vulnerability.

  An attacker exploits 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. 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.

Figure 20. Families commonly found with CVE-2010-2568 in 2011

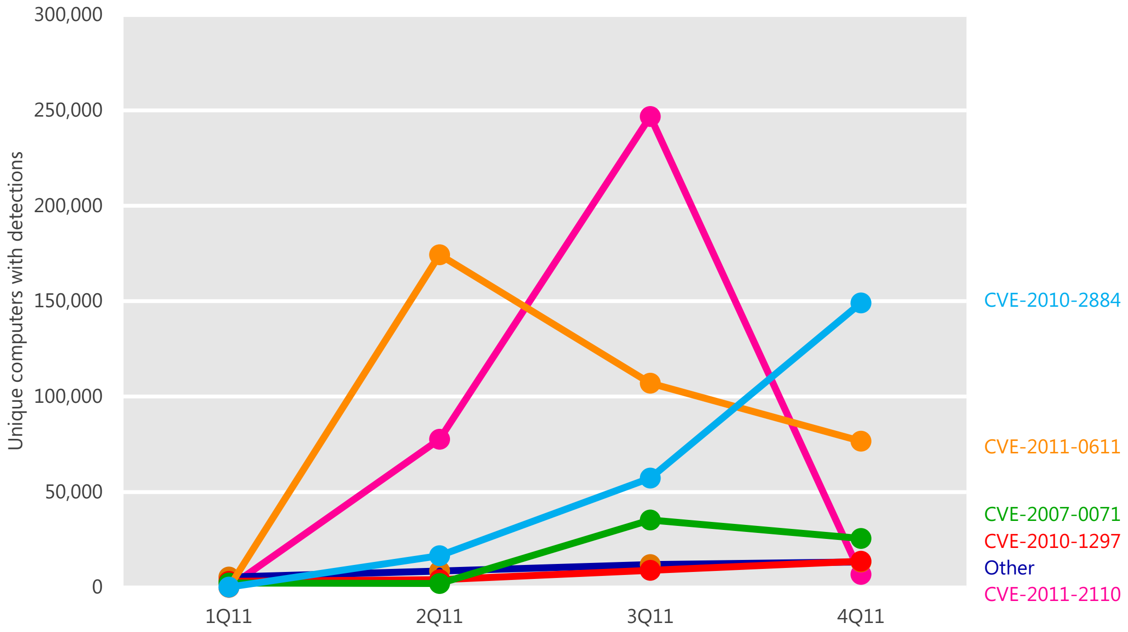


- Exploits targeting CVE-2010-1885, a vulnerability that affects the Windows Help and Support Center in Windows XP and Windows Server 2003, declined to a low level in 1Q11 after dominating for much of 2010, then increased gradually throughout 2011. Microsoft issued Security Bulletin MS10-042 in July 2010 to address the issue.

Adobe Flash Player exploits

Figure 21 shows the prevalence of different Adobe Flash Player exploits by quarter.

Figure 21. Adobe Flash Player exploits detected and blocked by Microsoft antimalware products each quarter in 2011, by number of unique computers exposed to the exploit



- Exploitation of Adobe Flash Player vulnerabilities increased significantly between 1Q11 and 3Q11, which can be attributed to two zero-day vulnerabilities discovered in the second quarter, CVE-2011-0611 and CVE-2011-2110. Detections of both exploits decreased in 4Q11, while detections of exploits targeting an older vulnerability, CVE-2010-2884, increased.
- CVE-2011-0611 was discovered in April 2011 when it was observed being exploited in the wild, typically in the form of malicious .zip files attached to spam email messages that purported to contain information about the Fukushima Daiichi nuclear disaster in Japan. Adobe released Security Bulletin APSB11-07 on April 15 and Security Bulletin APSB11-08 on April 21 to address the issue. On the same day the security update was released, attacks that targeted the vulnerability skyrocketed and remained high for several days, most of which were detected on computers in Korea. About a month later, a second increase in attacks was observed, affecting multiple locations. After peaking in 3Q11, detections of CVE-2011-0611 exploits declined to negligible levels in the fourth quarter.
- CVE-2011-2110 was discovered in June 2011, and Adobe released Security Bulletin APSB11-18 on June 15 to address the issue. As with CVE-2011-0611,

attacks that targeted the vulnerability spiked after the security update was released, again with most of the targeted computers located in Korea. CVE-2011-2110 is also exploited by the JS/Blacole exploit kit, which explains its continued prevalence in 2011.

- CVE-2010-2884 was discovered in the wild in September 2010 as a zero-day vulnerability, and Adobe released Security Bulletin APSB10-22 on September 20 to address the issue. As with CVE-2011-0611 and CVE-2011-2110, significant exploitation of the vulnerability began in 2Q11, which suggests that exploit kits may be responsible for the increase.

Exploit effectiveness with the Enhanced Mitigation Experience Toolkit

Recent versions of Windows, including Windows Vista® and Windows 7, include security enhancements that make vulnerabilities significantly harder to exploit than in older releases. Similarly, recent releases of many popular software programs offer security features that make those releases much less vulnerable to successful exploitation. Microsoft recommends using the most recent versions of Windows and applications when practical, to take advantage of the built-in security functionality they offer.[25]

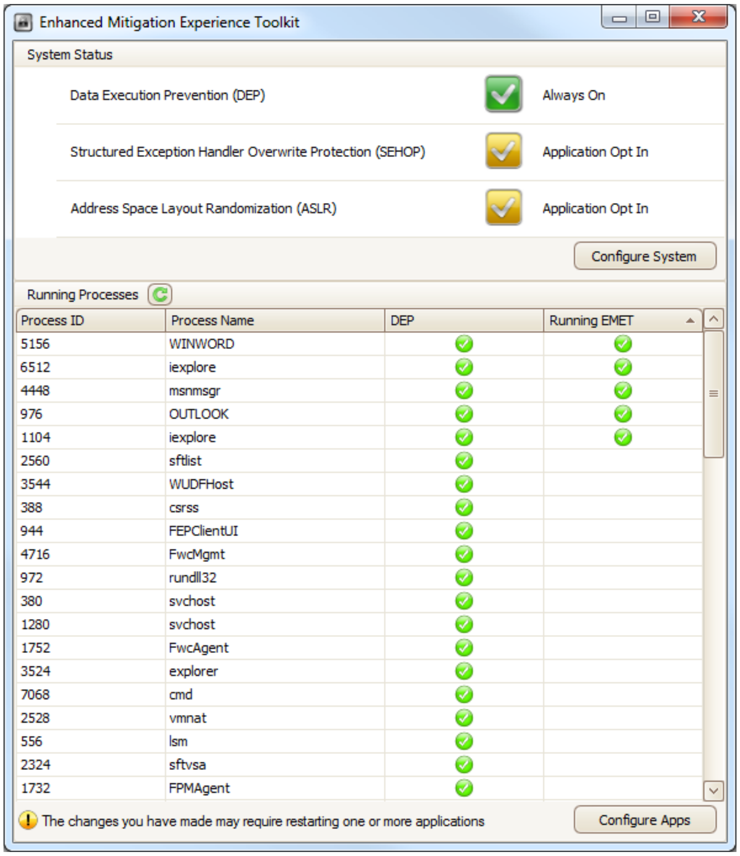
In some cases, though, individuals and organizations cannot deploy recent software versions for a variety of reasons, or want to take advantage of modern security improvements in advance of a planned upgrade. For these customers, as well as for users of the latest software versions who want to take advantage of additional security improvements, Microsoft offers the Enhanced Mitigation Experience Toolkit (EMET) at no charge from the Microsoft Download Center (www.microsoft.com/download).

EMET provides system administrators with the ability to deploy security mitigation technologies such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), Structured Exception Handler Overwrite Protection (SEHOP), and others to selected installed applications. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited. However,

[25] For more information about some of the security features in Windows and other Microsoft products, see "Mitigating Software Vulnerabilities," available from the Microsoft Download Center.

they make exploitation more difficult. EMET 2.1 is compatible with supported versions of Windows XP, Windows Vista, Windows 7, Windows Server® 2003, Windows Server 2008, and Windows Server 2008 R2.

Figure 22. The Enhanced Mitigation Experience Toolkit (EMET), version 2.1



Enhanced Mitigation Experience Toolkit

System Status

Data Execution Prevention (DEP)	✓	Always On
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In

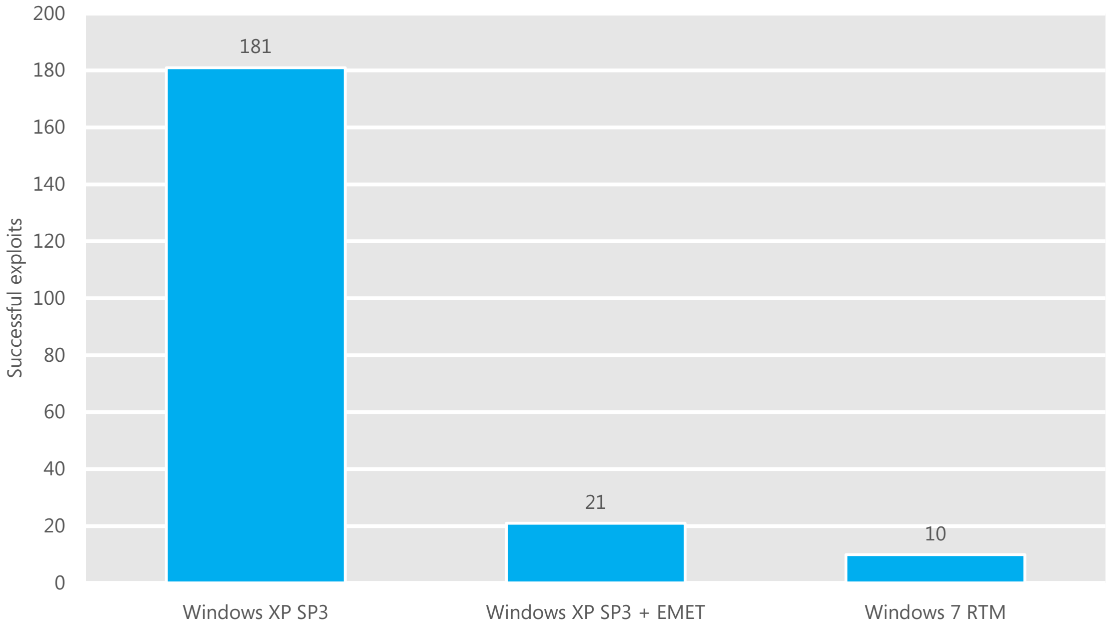
Running Processes

Process ID	Process Name	DEP	Running EMET
5156	WINWORD	✓	✓
6512	iexplore	✓	✓
4448	msnmsgr	✓	✓
976	OUTLOOK	✓	✓
1104	iexplore	✓	✓
2560	sftlist	✓	
3544	WUDFHost	✓	
388	csrss	✓	
944	FEPClientUI	✓	
4716	FwcMgmt	✓	
972	rundll32	✓	
380	svchost	✓	
1280	svchost	✓	
1752	FwcAgent	✓	
3524	explorer	✓	
7068	cmd	✓	
2528	vmnat	✓	
556	lsm	✓	
2324	sftvsa	✓	
1732	FPMAgent	✓	

The changes you have made may require restarting one or more applications

To assess the effectiveness of EMET in addressing a number of commonly exploited vulnerabilities, Microsoft researchers collected a sample of 184 application exploits that had been sent to Microsoft from customers worldwide. All exploits targeted vulnerabilities in popular applications running on one or more versions of Windows. The researchers tested each exploit against Windows XP SP3 in an out-of-the-box configuration, Windows XP SP3 with EMET deployed, and the release-to-manufacturing (RTM) version of Windows 7 in an out-of-the-box configuration. Figure 23 shows the results of these tests.

Figure 23. The effectiveness of 184 exploits for popular applications on Windows XP, Windows XP with EMET deployed, and Windows 7



- By a large margin, the highest success rates for the exploits tested involved Windows XP without EMET installed. All but three of the 184 exploits tested succeeded on Windows XP in this configuration.
- Deploying EMET drastically reduces the effectiveness of exploits on Windows XP. Only 21 of 184 exploits succeeded on Windows XP with EMET deployed.
- Ten of the 184 exploits tested succeeded on Windows 7 RTM.

It should be recognized that the results of an exercise such as this one are influenced by the specific exploits being actively used in the wild at the time the exercise is conducted. Nevertheless, the data suggests that system administrators can significantly reduce their attack surface now by upgrading to the latest versions of their operating system and application software by deploying EMET, or both.

Malware and potentially unwanted software

Except where specified, the information in this section was compiled from telemetry data that was generated from more than 600 million computers worldwide and some of the busiest services on the Internet. (See "Appendix B: Data sources" on page 107 for more information about the telemetry used in this report.)

Global infection rates

The telemetry data generated by Microsoft security products from administrators or users who choose to opt in to data collection includes information about the location of the computer, as determined by IP geolocation. This data makes it possible to compare infection rates, patterns, and trends in different locations around the world.[26]

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

Figure 24. The locations with the most computers reporting detections and removals by Microsoft desktop antimalware products in 2H11

	Country/Region	3Q11	4Q11	Chg. 3Q to 4Q
1	United States	10,293,718	10,122,222	-1.7% ▼
2	Brazil	3,969,106	3,810,308	-4.0% ▼
3	Russia	1,808,380	2,323,182	28.5% ▲
4	France	2,254,527	2,053,267	-8.9% ▼
5	Germany	1,477,340	1,926,096	30.4% ▲
6	China	2,179,211	1,814,082	-16.8% ▼
7	Korea	1,684,479	1,741,551	3.4% ▲
8	Turkey	1,359,815	1,591,529	17.0% ▲
9	United Kingdom	1,669,737	1,568,287	-6.1% ▼
10	Italy	1,206,092	1,382,590	14.6% ▲

- In absolute terms, the locations with the most computers reporting detections tend to be ones with large populations and large numbers of computers.

- Detections in Germany increased 30.4 percent from 3Q11 to 4Q11, primarily because of significantly increased detections of Win32/EyeStye, a family of trojans that attempt to steal sensitive data and send it to an attacker. Detection signatures for EyeStye were added to the MSRT in October 2011; within the first 10 days thereafter, more than half of the EyeStye infections detected and removed by the MSRT were in Germany. Germany also saw increased detections of the exploit family JS/Blacole and the generic detection Win32/Keygen.

- Detections in Russia increased 28.5 percent from 3Q11 to 4Q11. Families contributing to the increase include Win32/Pameseg, a potentially unwanted software program with a Russian language user interface; Win32/Vundo, a family of trojans that display out-of-context advertisements; and the Blacole exploit family.

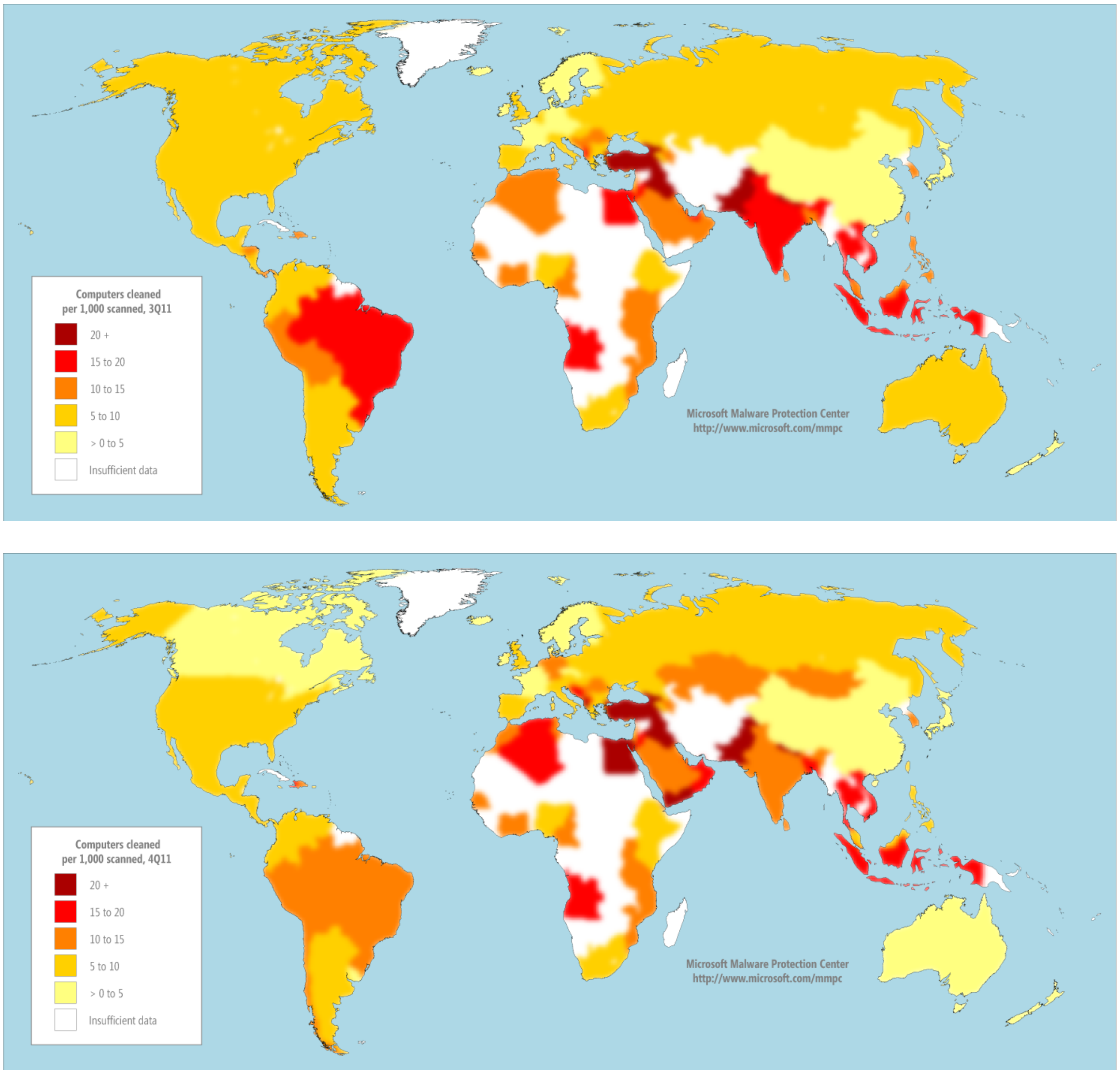
- Detections in Turkey increased 17.0 percent from 3Q11 to 4Q11, driven by small increases in a number of widespread families, including Keygen, JS/Pornpop, Win32/Sality, and Win32/Autorun.

- Detections in Italy increased 14.6 percent from 3Q11 to 4Q11, with increases in EyeStye, Keygen, and Win32/Zbot.

- Detections in France decreased 8.9 percent from 3Q11 to 4Q11, primarily because of fewer detections of a number of adware and adware-related families, including Win32/ClickPotato, Win32/Hotbar, Win32/Zwangi, Win32/ShopperReports, Win32/OfferBox, and Win32/OpenCandy.
- Detections in China decreased 16.8 percent from 3Q11 to 4Q11. This decrease follows a 15.7 percent increase from 2Q11 to 3Q11, driven by a large increase in detections of the adware family Win32/Rugo. Detections of Rugo then dropped in the fourth quarter, explaining much of the overall decrease.

For a different perspective on infection patterns worldwide, Figure 25 shows the infection rates in locations around the world in *computers cleaned per mille* (CCM), which represents the number of reported computers cleaned for every 1,000 executions of the Microsoft Malicious Software Removal Tool (MSRT). (See the *Microsoft Security Intelligence Report* website for more information about the CCM metric.)

Figure 25. Infection rates by country/region in 3Q11 (top) and 4Q11 (bottom), by CCM


Computers cleaned per 1,000 scanned, 3Q11
20 +
15 to 20
10 to 15
5 to 10
> 0 to 5
Insufficient data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc
Computers cleaned per 1,000 scanned, 4Q11
20 +
15 to 20
10 to 15
5 to 10
> 0 to 5
Insufficient data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Detections and removals in individual countries/regions can vary significantly from quarter to quarter. Increases in the number of computers with detections can be caused not only by increased prevalence of malware in that location, but also by improvements in the ability of Microsoft antimalware solutions to detect malware. Large numbers of new antimalware product or tool installations in a location also typically increase the number of computers cleaned in that location.

The next three figures illustrate infection rate trends for specific locations around the world, relative to the trends for all locations with at least 100,000 MSRT executions each quarter in 2H11.

Figure 26. Trends for the five locations with the highest infection rates in 4Q11, by CCM (100,000 MSRT executions minimum)

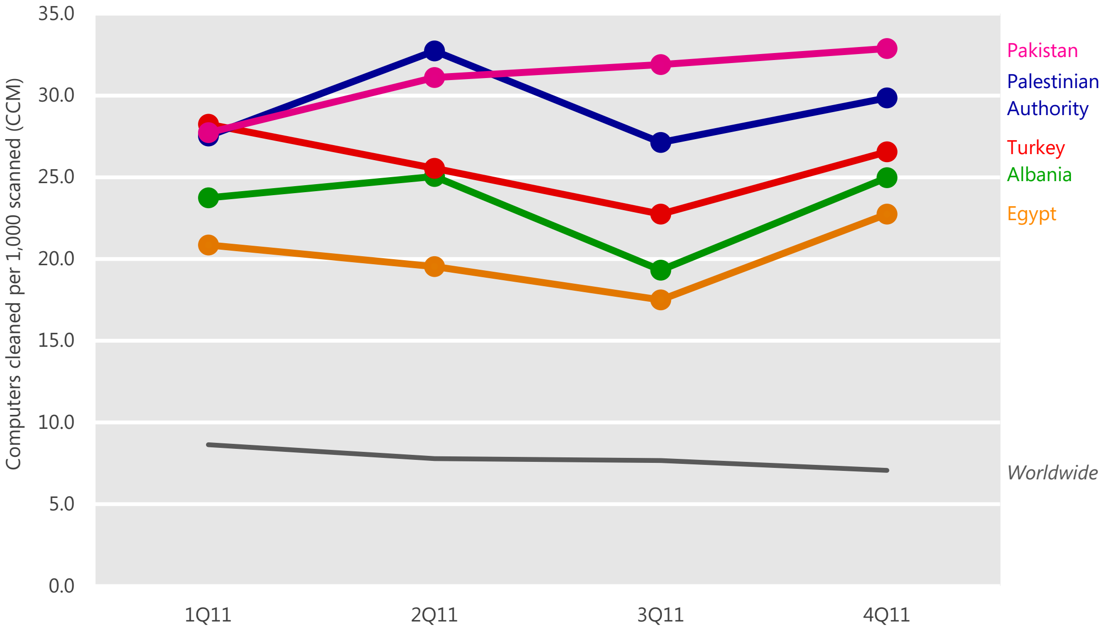
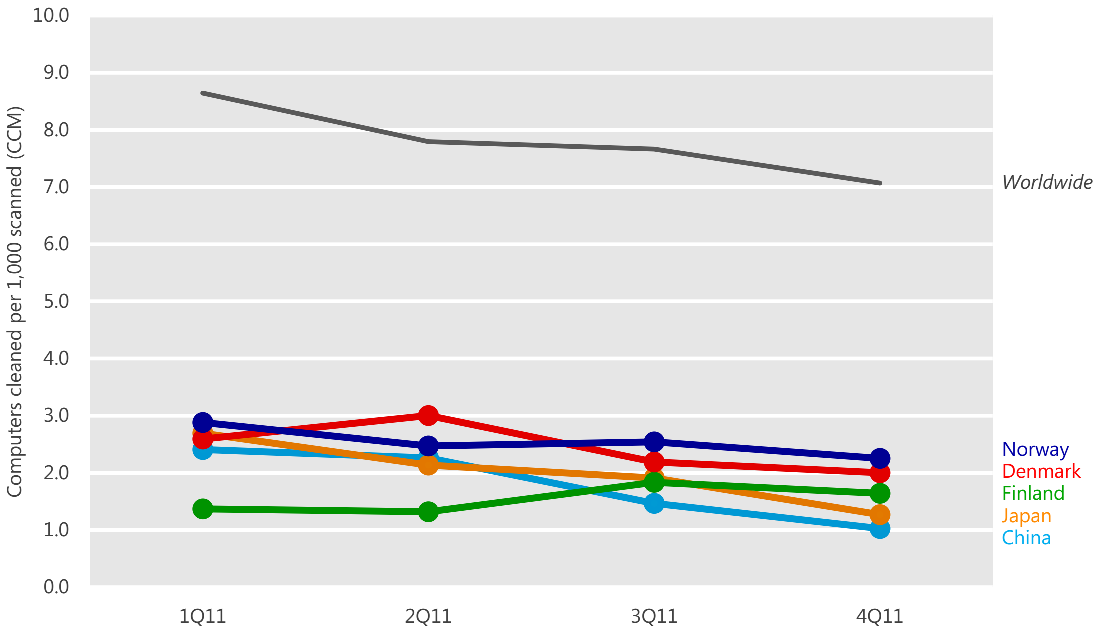


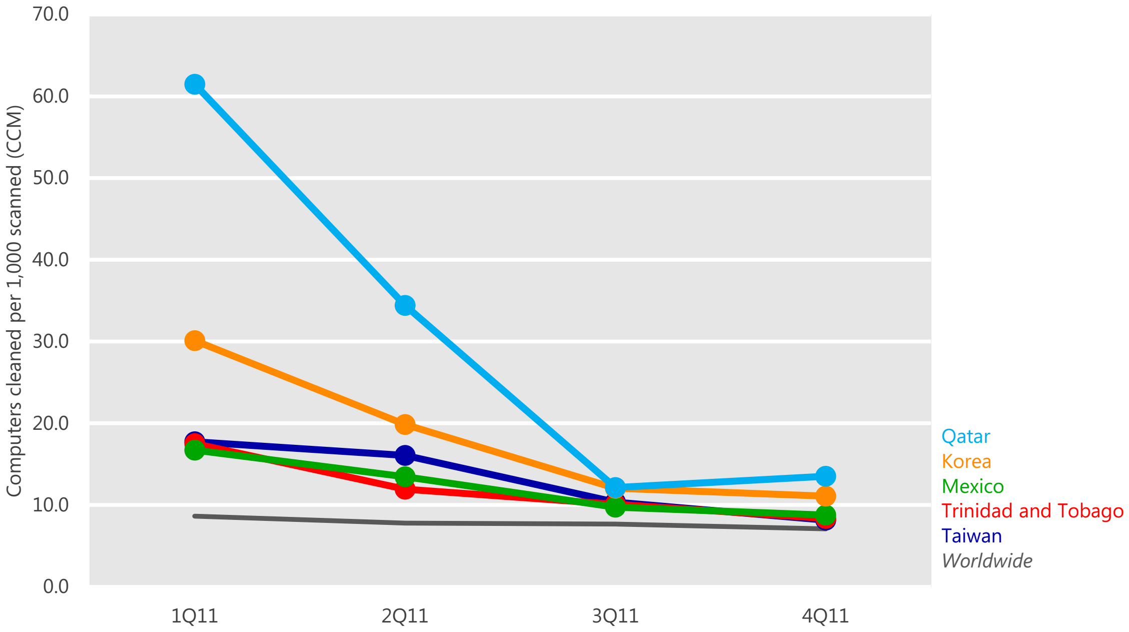
Figure 27. Trends for the five locations with the lowest infection rates in 4Q11, by CCM (100,000 MSRT executions minimum)



- The five locations with the highest infection rates in 4Q11 each had a CCM between 22.7 and 32.9, compared to a worldwide 4Q11 CCM of 7.1. Pakistan, the Palestinian territories, and Turkey were also among the five most infected locations in 2Q11, while Albania and Egypt are new to the top five.
  - Pakistan has seen significant increases in a pair of file infectors, Win32/Ramnit and Win32/Sality. Ramnit detections in Pakistan increased by more than 900 percent between 1Q11 and 4Q11, while detections of Sality more than doubled.
  - Albania and Egypt also saw an increase in Sality detections, along with increases in a number of worms, notably Win32/Rimecud, Win32/Autorun, Win32/Helompy, and Win32/Conficker. Detections of Win32/Dorkbot also increased significantly in Albania during the second half of the year.
- Four of the five locations with the lowest infection rates in 4Q11 were also on the list in 2Q11, with Denmark taking the place of Sweden. All five had 4Q11 infection rates between 1.3 and 2.3, compared to the worldwide average of 7.1.

- Historically, Nordic countries such as Denmark, Norway, and Finland have typically had some of the lowest infection rates in the world. Japan also usually experiences a low infection rate.
- Although China is one of the locations with the lowest infection rates worldwide as measured by CCM, a number of factors that are unique to China are important to consider when assessing the state of computer security there. The malware ecosystem in China is dominated by a number of Chinese-language threats that are not prevalent anywhere else. The CCM figures are calculated based on telemetry data from the MSRT, which tends to target malware families that are prevalent globally. As a result, many of the more prevalent threats in China are not represented in the data used to calculate CCM. For a more in-depth perspective on the threat landscape in China, see the "Regional Threat Assessment" section of the *Microsoft Security Intelligence Report* website.

Figure 28. Trends for five locations with significant infection rate improvements in 2H11, by CCM (100,000 MSRT executions minimum per quarter)



- Qatar exhibited the most dramatic improvement, from 61.5 in 1Q11 to 13.5 in 4Q11. Qatar as well as Trinidad and Tobago both have relatively few computers overall and are therefore prone to display large statistical variances of this sort from time to time. For Qatar, much of the reduction is the result of steep declines in detections of the worm family Win32/Rimecud, which was responsible for the relatively high CCM in 1Q11. Trinidad and Tobago experienced a general decline in a number of prevalent adware families, including Win32/OpenCandy, Win32/ClickPotato, and Win32/ShopperReports.

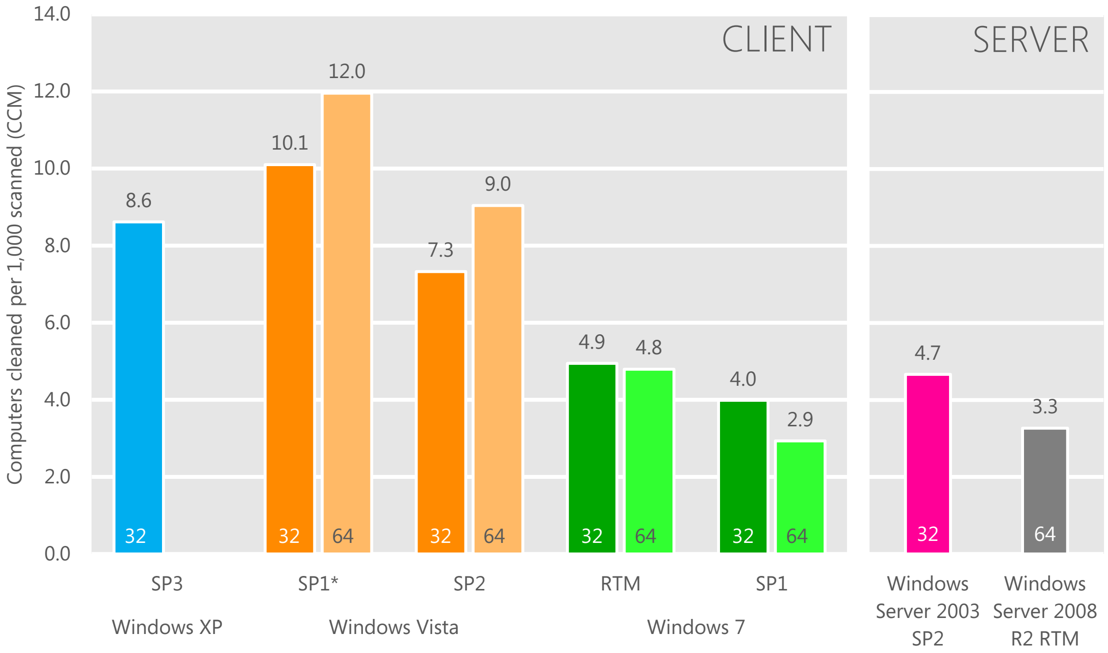
- Among populous countries and regions, Korea improved the most, going from 30.1 in 1Q11 to 11.1 in 4Q11. Significant decreases in detections of Rimecud, Win32/Frethog, and Win32/Parite were responsible for much of this improvement.
- Mexico improved from 16.7 in 1Q11 to 8.8 in 4Q11, with significant declines in detections of OpenCandy, Rimecud, and JS/Pornpop.
- Taiwan improved from 17.7 in 1Q11 to 8.2 in 4Q11, with significant declines in detections of Frethog, OpenCandy, Win32/Taterf, and Win32/Agent.

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

Operating system infection rates

The features and updates that are available with different versions of the Windows operating system, along with the differences in the way people and organizations use each version, affect the infection rates for the different versions and service packs. Figure 29 shows the infection rate for each currently supported Windows operating system/service pack combination that accounted for at least 0.1 percent of total MSRT executions in 4Q11.

Figure 29. Infection rate (CCM) by operating system and service pack in 4Q11



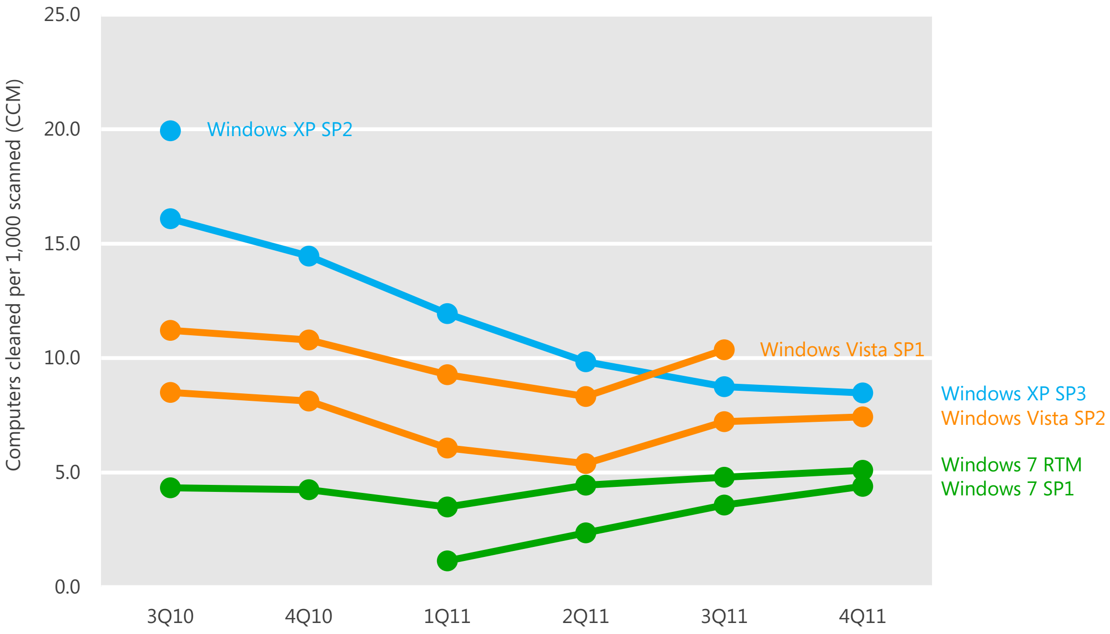
"32" = 32-bit edition; "64" = 64-bit edition. SP = Service Pack. RTM = release to manufacturing.
Operating systems with at least 0.1 percent of total executions in 4Q11 shown. *Service pack not supported in 4Q11.

- This data is normalized: the infection rate for each version of Windows is calculated by comparing an equal number of computers per version (for example, 1,000 Windows XP SP3 computers to 1,000 Windows 7 RTM computers).

- As in previous periods, infection rates for more recently released operating systems and service packs tend to be lower than earlier ones, for both client and server platforms. Windows 7 SP1 and Windows Server 2008 R2, the most recently released Windows client and server versions, respectively, have the lowest infection rates on the chart. The exception is Windows XP SP3, which displayed a lower infection rate than the 32- and 64-bit editions of Windows Vista SP1 and the 64-bit edition of Windows Vista SP2. As the user base of Windows XP continues to decline in favor of newer versions of Windows, malware writers may be refocusing their efforts away from the older platform as well, which could be a factor in this discrepancy.

- Infection rates for the 64-bit editions of Windows Vista and Windows 7 have increased since the first half of 2011. For the first time, infection rates for the 64-bit editions of Windows Vista SP1 and SP2 were higher than for the corresponding 32-bit versions of those platforms in 2H11, and infection rates for both the 32- and 64-bit editions of Windows 7 RTM were almost identical. This data may indicate the increasing acceptance of 64-bit platforms by mainstream users. In the past, 64-bit computing tended to appeal to a more technically savvy audience than the mainstream, and the infection rates for 64-bit platforms were typically much lower than for their 32-bit counterparts, perhaps because 64-bit users tended to follow safer practices and keep their computers more up-to-date than the average user. Over the past several years, 64-bit computing has become more mainstream, and the infection rates for 64-bit platforms have increased at the same time. Malware authors may also be targeting 64-bit platforms more as they become more popular, which could affect infection rates.

Figure 30. Infection rate trends for currently and recently supported 32-bit version of Windows XP, Windows Vista, and Windows 7, 3Q10–4Q11



- This chart shows infection rates for supported versions of Windows only. Support for Windows XP SP2 was retired on July 13, 2010. Support for Windows Vista SP1 was retired on July 12, 2011.
- Infection rates for all of the supported 32-bit versions of Windows increased slightly during the second half of the year except for Windows XP, for which the infection rate decreased slightly. Microsoft added signatures for a number

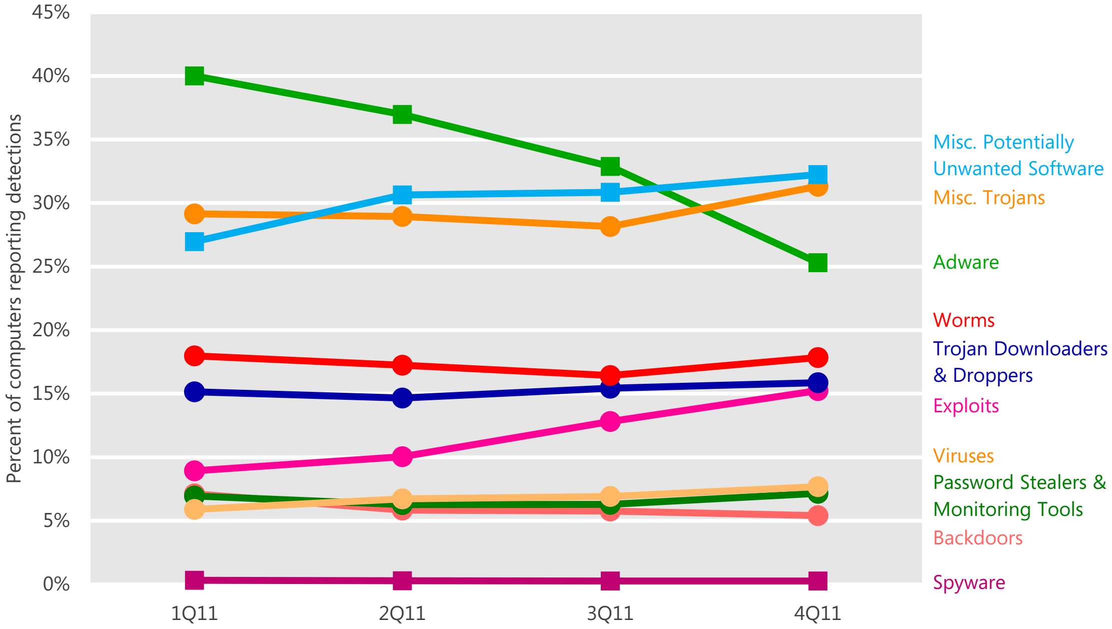
of prevalent malware families to the MSRT in 2H11, including Win32/Tracur (July 2011), Win32/Bamital (September 2011), and Win32/EyeStye (October 2011). Detections of these families increased significantly on all of the supported platforms after MSRT coverage was added, which contributed to the higher infection rates seen in 3Q11 and 4Q11. On Windows XP, however, the increase was offset by decreased detections of families that abuse the Autorun feature in Windows, following the February 2011 release of a security update that changed the way Autorun works on Windows XP and Windows Vista to match its functionality in Windows 7. (For more information about this change, see "Defending Against Autorun Attacks" (June 27, 2011) on the Microsoft Security Blog at blogs.technet.com/security.)

- Windows 7 RTM and SP1 have consistently shown lower infection rates than other platforms since their introduction, although increased detections of EyeStye, Bamital, Tracur, and a few other families have contributed to a rise in the infection rate on Windows 7 computers, as with other platforms.

Threat categories

The Microsoft Malware Protection Center (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 10 categories based on similarities in function and purpose.

Figure 31. Detections by threat category each quarter in 2011, by percentage of all computers reporting detections



Round markers indicate malware categories; square markers indicate potentially unwanted software categories.

- Totals for each time period may exceed 100 percent because some computers report more than one category of threat in each time period.
- Adware, the most commonly detected category during the first three quarters, fell to 3rd in 4Q11, continuing a year-long trend of decline. Decreased detections of several highly prevalent adware families, notably Win32/OpenCandy, Win32/ClickPotato, and Win32/ShopperReports, were chiefly responsible for the decline. (See “Threat families” on page 68 for more information.)
- Miscellaneous Potentially Unwanted Software rose from 3rd in 1Q11 to 1st in 4Q11, led by the generic detection Win32/Keygen, a tool that generates keys for illegally obtained versions of various software products.
- Exploits increased from 8.9 percent of computers with detections in 1Q11 to 15.3 percent in 4Q11, partially because of increased detections of exploits associated with the JS/Blacole exploit kit, a malicious JavaScript that loads a series of other exploits to deliver a payload. If a vulnerable computer browses a compromised website that contains the exploit kit, various malware may be downloaded and run.

Threat categories by location

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

Figure 32 shows the relative prevalence of different categories of malware and potentially unwanted software in several locations around the world in 4Q11.

Figure 32. Threat category prevalence worldwide and in 10 individual locations in 4Q11

Category	World	US	Brazil	Russia	France	Germany	Chiuna	Korea	Turkey	UK	Italy
Adware	37.0%	30.9%	18.5%	5.4%	53.0%	18.8%	9.9%	57.5%	36.6%	32.3%	34.4%
Misc. Potentially Unwanted Software	30.6%	19.6%	36.4%	57.2%	28.4%	23.4%	48.3%	21.1%	33.9%	23.8%	31.2%
Misc. Trojans	28.9%	38.5%	25.3%	39.1%	16.8%	40.8%	29.5%	33.7%	27.8%	34.8%	25.7%
Worms	17.2%	5.7%	22.0%	17.2%	8.6%	7.2%	12.1%	10.4%	34.1%	6.2%	12.7%
Trojan Downloaders & Droppers	14.7%	20.8%	26.1%	14.3%	9.1%	9.4%	12.8%	17.2%	11.9%	13.2%	10.5%
Exploits	10.0%	26.3%	9.7%	17.4%	6.6%	16.7%	13.9%	13.9%	6.6%	23.1%	14.0%
Viruses	6.7%	2.3%	9.3%	6.4%	2.2%	2.0%	8.7%	4.5%	16.6%	5.3%	2.3%
Password Stealers & Monitoring Tools	6.3%	5.2%	20.4%	4.2%	3.8%	8.5%	4.4%	3.8%	6.1%	5.3%	11.0%
Backdoors	5.8%	6.3%	5.0%	4.3%	2.8%	4.3%	6.6%	2.9%	4.6%	4.0%	4.1%
Spyware	0.3%	0.3%	0.1%	0.3%	0.1%	0.2%	1.8%	0.2%	0.1%	0.2%	0.1%

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

- Within each row of Figure 32, 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 24 on page 56,the locations in the table are ordered by number of computers reporting detections in 2H11.
- The United States and the United Kingdom, two predominantly English-speaking locations that also share a number of other cultural similarities, have similar threat mixes in most categories.
- In Russia, the Miscellaneous Potentially Unwanted Software category is especially prevalent, led by Win32/Pameseg and Win32/Keygen. Pameseg is a family of installers that require the user to send a text message to a premium number to successfully install certain programs, some of which are otherwise available for free. Currently, most variants target Russian speakers.
- Brazil has long had higher-than-average detections of Password Stealers & Monitoring Tools because of the prevalence of malware that targets customers of Brazilian banks, especially Win32/Bancos and Win32/Banker.
- Worms were especially prevalent in Turkey in 4Q11 due to Win32/Helompy, which was detected on more than five times as many computers in Turkey in 4Q11 as in any other individual location. Helompy is a worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or services, including Facebook and Gmail. The worm contacts a remote host to download arbitrary files and to upload stolen details.

See “Appendix C: Worldwide infection rates” on page 109 for more information about malware around the world.

Threat families

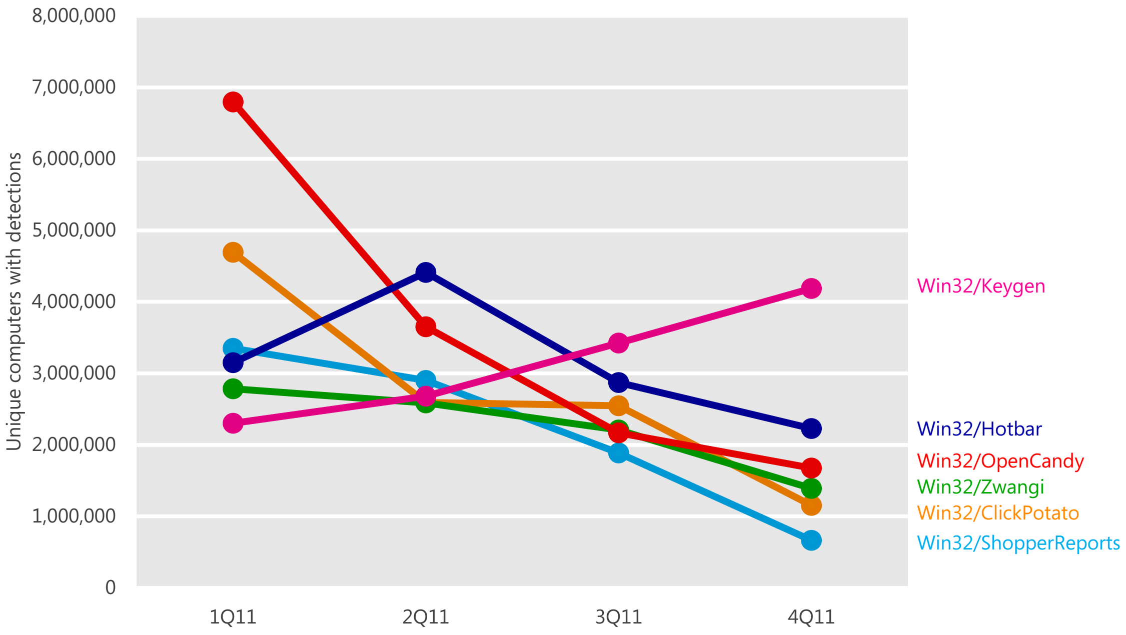
Figure 33 lists the top 10 malware and potentially unwanted software families that were detected on computers by Microsoft antimalware products in the second half of 2011.

Figure 33. Quarterly trends for the top 10 malware and potentially unwanted software families detected by Microsoft antimalware products in 3Q11 and 4Q11, shaded according to relative prevalence

Family	Most Significant Category	1Q11	2Q11	3Q11	4Q11
Win32/Keygen	Misc. Potentially Unwanted Software	2,299,870	2,680,354	3,424,213	4,187,586
JS/Pornpop	Adware	4,706,968	4,330,510	3,944,489	3,906,625
Win32/Autorun	Worms	3,718,690	3,677,588	3,292,378	3,438,745
Win32/Hotbar	Adware	3,149,677	4,411,501	2,870,465	2,226,173
Win32/Sality	Viruses	1,502,172	1,686,745	1,728,966	1,951,118
Win32/Conficker	Worms	1,859,498	1,790,035	1,614,368	1,704,736
Win32/OpenCandy	Adware	6,797,012	3,652,658	2,166,625	1,676,753
Win32/Zwangi	Misc. Potentially Unwanted Software	2,785,111	2,586,630	2,207,208	1,388,938
Win32/ClickPotato	Adware	4,694,442	2,592,125	2,545,842	1,153,203
Win32/ShopperReports	Adware	3,348,949	2,902,430	1,886,696	662,632

For a different perspective on some of the changes that have taken place throughout the year, Figure 34 shows the detection trends for a number of families that increased or decreased significantly in 2011.

Figure 34. Detection trends for a number of notable families in 2011



- Win32/Keygen was the most commonly detected family in 4Q11, and one of only two families in the top 10 with more detections in the fourth quarter of the year than in the first. Keygen is a generic detection for tools that generate keys for illegally obtained versions of various software products.

- JS/Pornpop, the second most commonly detected family in 4Q11, is a detection for specially crafted JavaScript-enabled objects that attempt to display pop-under advertisements in users' web browsers. Initially, JS/Pornpop appeared exclusively on websites that contained adult content; however, it has since been observed to appear on websites that may contain no adult content whatsoever. First detected in August 2010, it grew quickly to become one of the most prevalent families in the world.

- Keygen, Win32/Autorun, and Win32/Sality were the only families in the top ten with more detections in 4Q11 than in 3Q11. Sality is a family of polymorphic file infectors that target executable files with the extensions .scr or .exe. Win32/Autorun is a generic detection for worms that spread between mounted volumes using the Autorun feature of Windows. Recent changes to the feature in Windows XP and Windows Vista have made this technique less effective, but attackers continue to distribute malware that attempts to target it.

- Detections of Win32/OpenCandy, the most commonly detected family in 1Q11, declined steeply thereafter; it ranked seventh in 4Q11. OpenCandy is an adware program that may be bundled with certain third-party software installation programs, for which detection was first added in February 2011. Some versions of the OpenCandy program send user-specific information without obtaining adequate user consent, and these versions are detected by Microsoft antimalware products. Detections have declined as third-party software developers have increased their use of versions that do not exhibit these behaviors.

- Other families that declined in the second half of the year include the adware families Win32/Hotbar, Win32/ClickPotato, and Win32/ShopperReports, and the potentially unwanted software family Win32/Zwangi. Hotbar, ClickPotato, and ShopperReports are three related families that are often found together, and which display targeted advertisements to users based on browsing habits.

Rogue security software

Rogue security software has become one of the most common methods that attackers use to swindle money from victims. Rogue security software, also known as *scareware*, is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure users into participating in fraudulent transactions. These programs typically mimic the general look and feel of legitimate security software programs and claim to detect a large number of nonexistent threats while urging users to pay for the "full version" of the software to remove the threats. Attackers typically install rogue security software programs through exploits or other malware, or use social engineering to trick users into believing the programs are legitimate and useful. Some versions emulate the appearance of the Windows Security Center or unlawfully use trademarks and icons to misrepresent themselves. (See www.microsoft.com/security/resources/videos.aspx for an informative series of videos designed to educate a general audience about rogue security software.)

Figure 35. False branding used by a number of commonly detected rogue security software programs

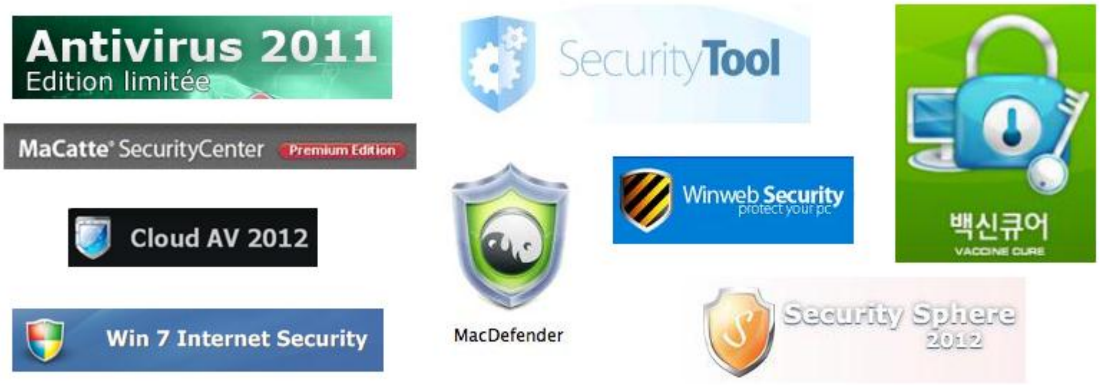
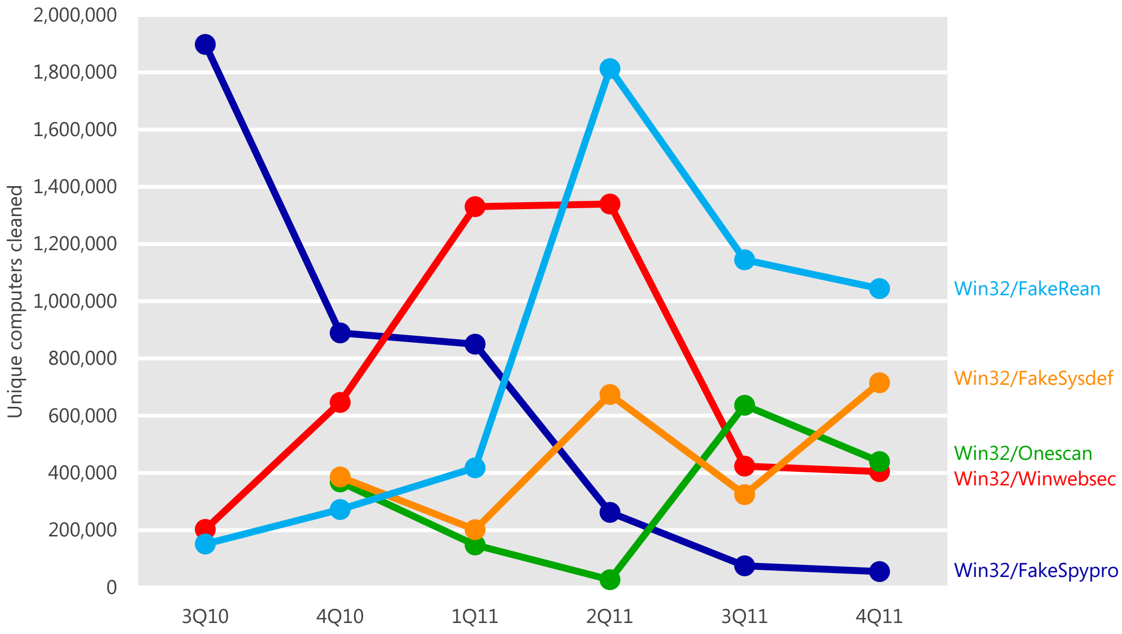


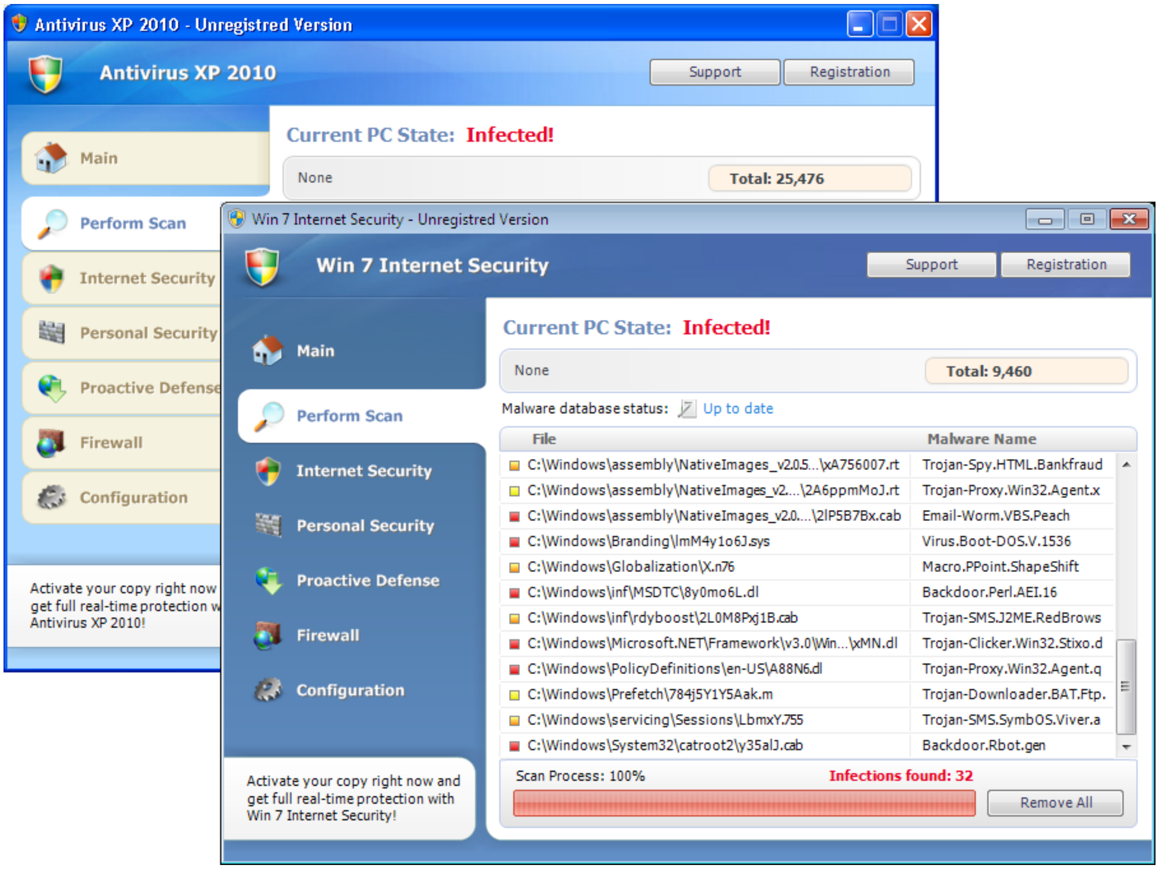
Figure 36 shows detection trends for the most common rogue security software families detected in 2H11.

Figure 36. Trends for the most common rogue security software families detected in 2H11, by quarter



- Detections of Win32/FakeRean decreased significantly after 2Q11, but it remained the most commonly detected rogue security software program during the third and fourth quarters of the year. FakeRean has been distributed with several different names. The user interface and some other details vary to reflect each variant's individual branding. Current variants of FakeRean choose a name at random, from a number of possibilities determined by the operating system of the affected computer. Signatures for FakeRean were added to the MSRT in August 2009.

Figure 37. Typical Win32/FakeRean variants on Windows XP and Windows 7



Current PC State: Infected!

None — Total: 25,476

Activate your copy right now get full real-time protection w Antivirus XP 2010!

Current PC State: Infected!

None — Total: 9,460

Malware database status: Up to date

File	Malware Name
🟧 C:\Windows\assembly\NativeImages_v2.0.5...\xA756007.rt	Trojan-Spy.HTML.Bankfraud
🟨 C:\Windows\assembly\NativeImages_v2....\2A6ppmMoJ.rt	Trojan-Proxy.Win32.Agent.x
🟥 C:\Windows\assembly\NativeImages_v2.0....\2lP5B7Bx.cab	Email-Worm.VBS.Peach
🟥 C:\Windows\Branding\lmM4y1o6J.sys	Virus.Boot-DOS.V.1536
🟧 C:\Windows\Globalization\X.n76	Macro.PPoint.ShapeShift
🟥 C:\Windows\inf\MSDTC\8y0mo6L.dl	Backdoor.Perl.AEI.16
🟧 C:\Windows\inf\rdyboost\2L0M8Pxj1B.cab	Trojan-SMS.J2ME.RedBrows
🟥 C:\Windows\Microsoft.NET\Framework\v3.0\Win...\xMN.dl	Trojan-Clicker.Win32.Stixo.d
🟥 C:\Windows\PolicyDefinitions\en-US\A88N6.dl	Trojan-Proxy.Win32.Agent.q
🟨 C:\Windows\Prefetch\784j5Y1Y5Aak.m	Trojan-Downloader.BAT.Ftp.
🟧 C:\Windows\servicing\Sessions\LbmxY.755	Trojan-SMS.SymbOS.Viver.a
🟥 C:\Windows\System32\catroot2\y35alJ.cab	Backdoor.Rbot.gen

Scan Process: 100%   Infections found: 32

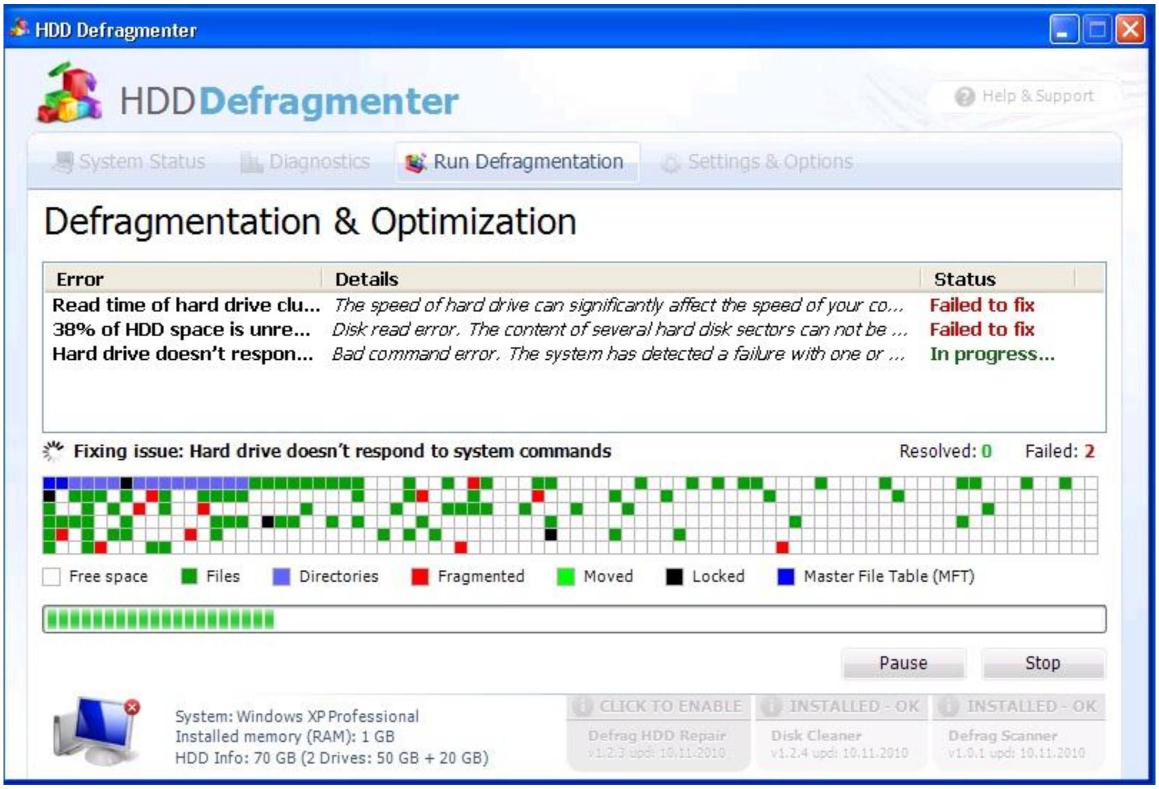
Activate your copy right now and get full real-time protection with Win 7 Internet Security!

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

- Win32/FakeRean and MSRT (August 11, 2009)
- Win32/FakeRean is 33 rogues in 1 (March 9, 2010)
- When imitation isn't a form of flattery (January 29, 2012)

- Win32/FakeSysdef, the second most commonly detected rogue security software program in 4Q11, was first detected in late 2010, and signatures for the family were added to the MSRT in August 2011. Unlike most rogue security software families, FakeSysdef does not claim to detect malware infections. Instead, it masquerades as a performance utility that falsely claims to find numerous hardware and software errors such as bad hard disk sectors, disk fragmentation, registry errors, and memory problems. Like other rogue security software families, it claims that the user must purchase additional software to fix the nonexistent problems.

Figure 38. Win32/FakeSysdef pretends to find computer problems and offers to fix them for a fee



Defragmentation & Optimization

Error	Details	Status
Read time of hard drive clu...	*The speed of hard drive can significantly affect the speed of your co...*	Failed to fix
38% of HDD space is unre...	*Disk read error. The content of several hard disk sectors can not be ...*	Failed to fix
Hard drive doesn't respon...	*Bad command error. The system has detected a failure with one or ...*	In progress...

Fixing issue: Hard drive doesn't respond to system commands

Resolved: 0 Failed: 2

System: Windows XP Professional
Installed memory (RAM): 1 GB
HDD Info: 70 GB (2 Drives: 50 GB + 20 GB)

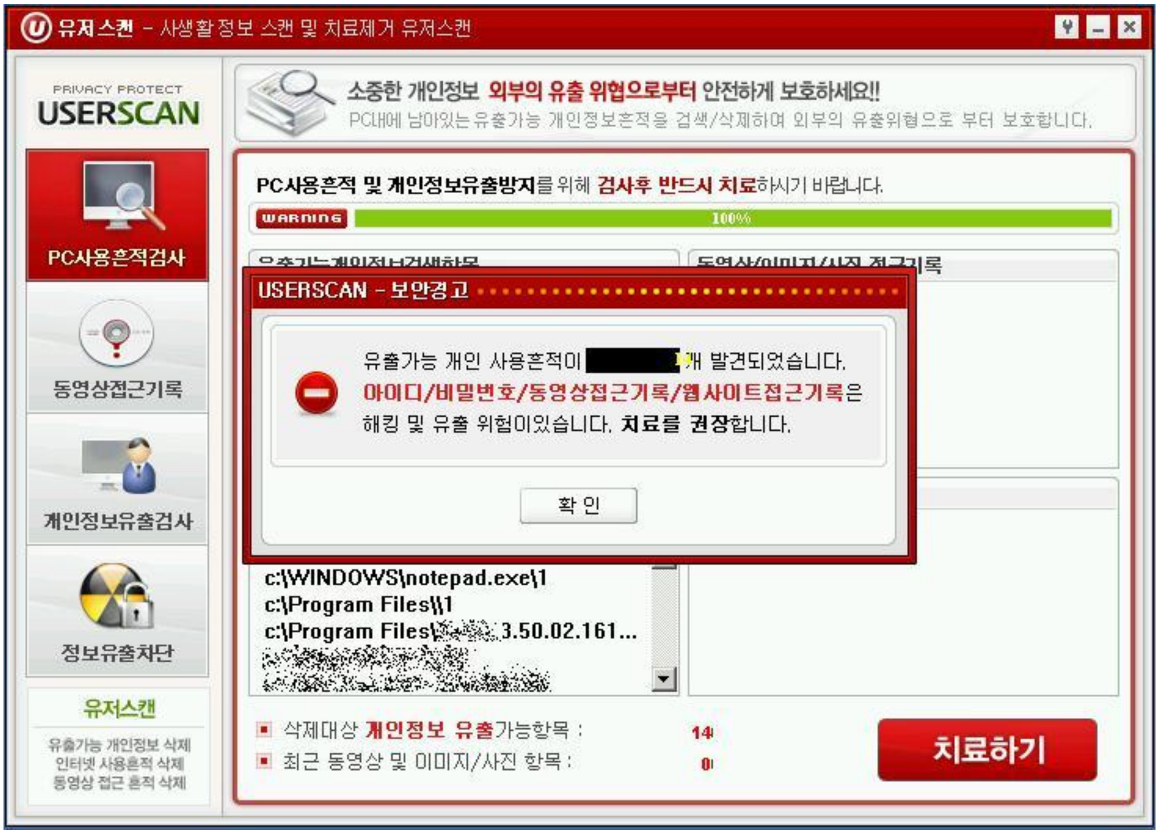
Like FakeRean, FakeSysdef uses a large number of aliases, which are often tailored to the operating system version it is running on.

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

- FakeSysdef: We can defragment that for you wholesale! / Diary of a scamware (December 1, 2010)
- How to defang the Fake Defragmenter (March 19, 2011)
- MSRT August '11: FakeSysdef (August 10, 2011)

- Detections of Win32/Onescan increased from the first half of the year to the second. Onescan is a Korean-language rogue security software distributed under a variety of names, brands, and logos. The installer selects the branding randomly from a defined set, apparently without regard to the operating system version.

Figure 39. Win32/Onescan, a Korean-language rogue security software program



소중한 개인정보 외부의 유출 위협으로부터 안전하게 보호하세요!!

PC내에 남아있는 유출가능 개인정보흔적을 검색/삭제하여 외부의 유출위협으로 부터 보호합니다.

PC사용흔적 및 개인정보유출방지를 위해 검사후 반드시 치료하시기 바랍니다.

유출가능 개인 사용흔적이 [redacted]개 발견되었습니다.
아이디/비밀번호/동영상접근기록/웹사이트접근기록은
해킹 및 유출 위험이있습니다. 치료를 권장합니다.

```
c:\WINDOWS\notepad.exe\1
c:\Program Files\\1
c:\Program Files\3.50.02.161...
```

- 삭제대상 개인정보 유출가능항목 : 14
- 최근 동영상 및 이미지/사진 항목 : 0

- Detections of Win32/Winwebsec declined significantly in 3Q11, although it remains one of the more widely detected rogue security software programs worldwide. Winwebsec has also been distributed under many names, with the user interface and other details varying to reflect each variant's individual branding. These different distributions of the trojan use various installation methods, with filenames and system modifications that can differ from one variant to the next. The attackers behind Winwebsec are also believed to be responsible for MacOS_X/FakeMacdef, the highly publicized "Mac Defender" rogue security software program for Apple Mac OS X that first appeared in May 2011. Detections for Winwebsec were added to the MSRT in May 2009.

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 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 40 and Figure 41 list the top 10 families detected on domain-joined and non-domain computers, respectively, in 4Q11.

Figure 40. Top 10 families detected on domain-joined computers in 4Q11, by percentage of domain-joined computers reporting detections

	Family	Most Significant Category	1Q11	2Q11	3Q11	4Q11
1	Win32/Conficker	Worms	17.8%	15.8%	14.7%	13.5%
2	Win32/Autorun	Worms	11.7%	11.1%	9.3%	8.5%
3	JS/Blacole	Exploits	—	—	2.3%	6.4%
4	Win32/Keygen	Misc. Potentially Unwanted Software	2.9%	3.5%	4.6%	5.0%
5	Win32/Dorkbot	Worms	0.0%	0.6%	2.9%	3.7%
6	Win32/Zbot	Password Stealers & Monitoring Tools	1.8%	1.7%	2.2%	3.6%
7	Win32/RealVNC	Misc. Potentially Unwanted Software	4.5%	4.4%	4.1%	3.4%
8	JS/Redirector	Misc. Trojans	0.9%	0.9%	1.5%	3.3%
9	JS/Pornpop	Adware	4.4%	3.9%	3.5%	3.2%
10	Java/CVE-2010-0840	Exploits	3.3%	3.1%	4.1%	3.2%

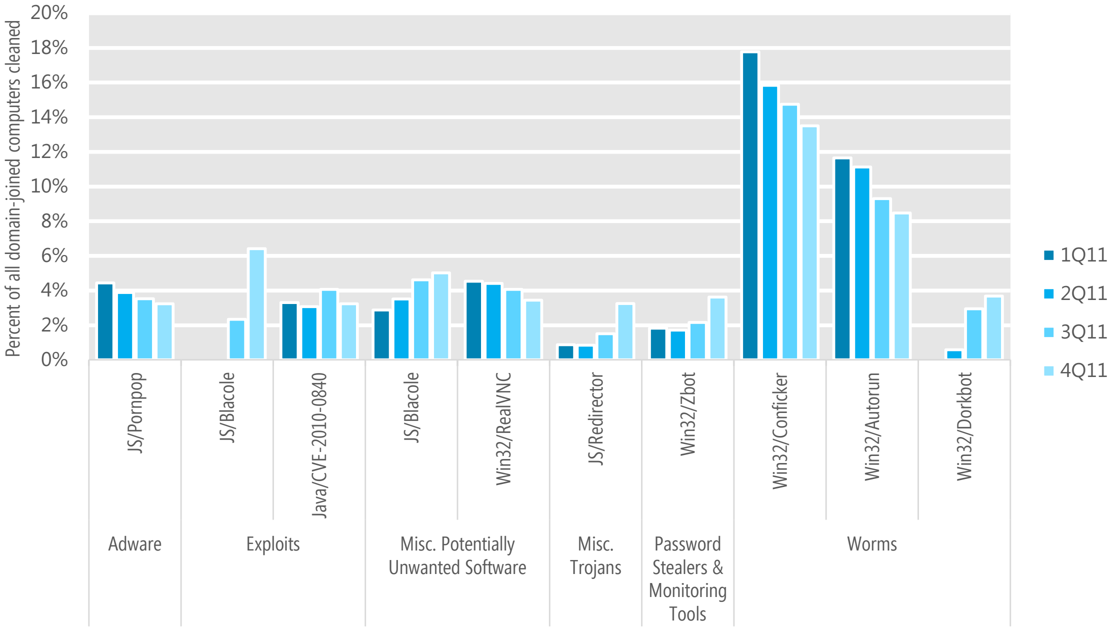
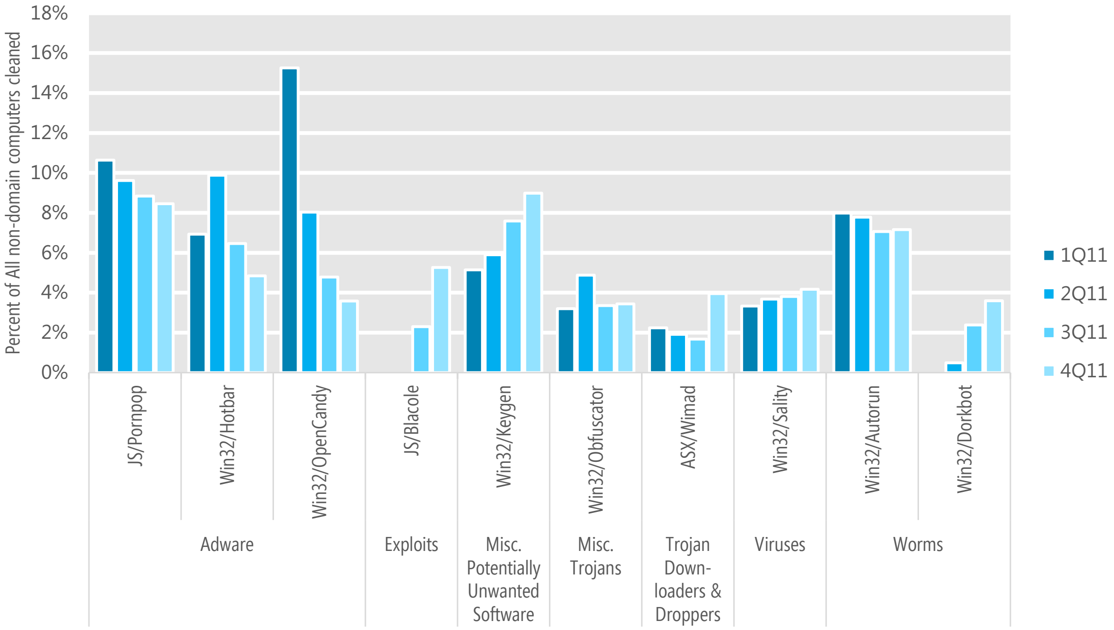


Figure 41. Top 10 families detected on non-domain computers in 4Q11, by percentage of non-domain computers reporting detections

	Family	Most Significant Category	1Q11	2Q11	3Q11	4Q11
1	Win32/Keygen	Misc. Potentially Unwanted Software	5.1%	5.9%	7.6%	9.0%
2	JS/Pornpop	Adware	10.6%	9.6%	8.8%	8.5%
3	Win32/Autorun	Worms	8.0%	7.8%	7.1%	7.2%
4	JS/Blacole	Exploits	0.0%	0.0%	2.3%	5.3%
5	Win32/Hotbar	Adware	6.9%	9.9%	6.5%	4.8%
6	Win32/Sality	Viruses	3.3%	3.7%	3.8%	4.2%
7	ASX/Wimad	Trojan Downloaders & Droppers	2.2%	1.9%	1.7%	4.0%
8	Win32/Dorkbot	Worms	0.0%	0.5%	2.4%	3.6%
9	Win32/OpenCandy	Adware	15.3%	8.0%	4.8%	3.6%
10	Win32/Obfuscator	Misc. Potentially Unwanted Software	3.2%	4.9%	3.4%	3.4%



- Five families are common to both lists, notably the generic families Win32/Keygen and Win32/Autorun and the exploit family JS/Blacole.
- Other families that were prevalent on domain-joined computers during at least one quarter in 2011 included the worm family Win32/Rimecud, the generic detection Win32/Obfuscator, and the adware family

Win32/OpenCandy. Families that were prevalent on non-domain computers during at least one quarter included the potentially unwanted software family Win32/Zwangi and the adware family Win32/ClickPotato.

- The worm family Win32/Dorkbot, ranked fifth on domain-joined computers and eighth on non-domain computers in 4Q11, affected both types of computers about equally during the third and fourth quarters. Dorkbot is an IRC-based botnet family with rootkit capability and password stealing functionality. For more information, see the entry "MSRT March 2012: Breaking bad" (March 13, 2012) on the MMPC blog at blogs.technet.com/mmpc.
- Detections of worm family Win32/Conficker, the most commonly detected family on domain-joined computers during each quarter in 2011, declined slowly throughout the year. After being detected on 17.8 percent of domain-joined computers reporting detections in 1Q11, Conficker detections declined in each successive quarter, to a low of 13.5 percent in 4Q11. (See "How Conficker continues to propagate" on page 1 for more information.) Similarly, detections of the generic family Win32/Autorun decreased on domain-joined computers during each quarter in 2011.
- Families that were significantly more prevalent on domain-joined computers include Conficker, the botnet family Win32/Zbot, and the potentially unwanted software program Win32/RealVNC. RealVNC is a program that enables a computer to be controlled remotely, similar to Remote Desktop Services. It has a number of legitimate uses, but attackers have also used it to gain control of users' computers for malicious purposes.
- Java/CVE-2010-0840, an exploit that targets a vulnerability in older versions of Oracle Java SE and Java for Business, was the tenth most commonly detected threat on domain-joined computers. See "Java Exploits" on page 44 for more information about this exploit.
- Detections on non-domain computers have historically tended to be dominated by adware, but a decline in detections of a number of prevalent adware families has led to a more diverse mix of threat categories during the second half of the year. The adware families ClickPotato and Win32/ShopperReports are among the families that no longer appear on the top-10 list for non-domain computers.
- Families that were significantly more prevalent on non-domain computers include the adware families JS/Pornpop and Win32/Hotbar and the generic detection ASX/Wimad. Wimad is a detection for malicious files in the Advanced Stream Redirector (ASX) format used by Windows Media® Player.

Guidance: Defending against malware

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

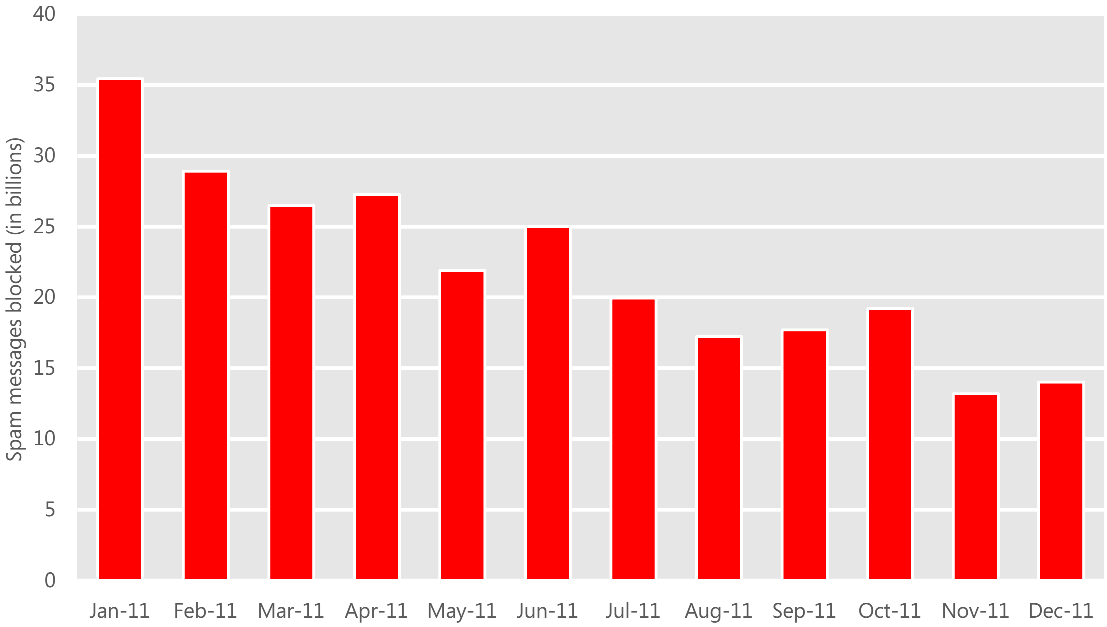
Email threats

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 Microsoft Forefront® Online Protection for Exchange (FOPE), which provides spam, phishing, and malware filtering services for thousands of Microsoft enterprise customers that process tens of billions of messages each month.

Figure 42. Messages blocked by FOPE each month in 2011

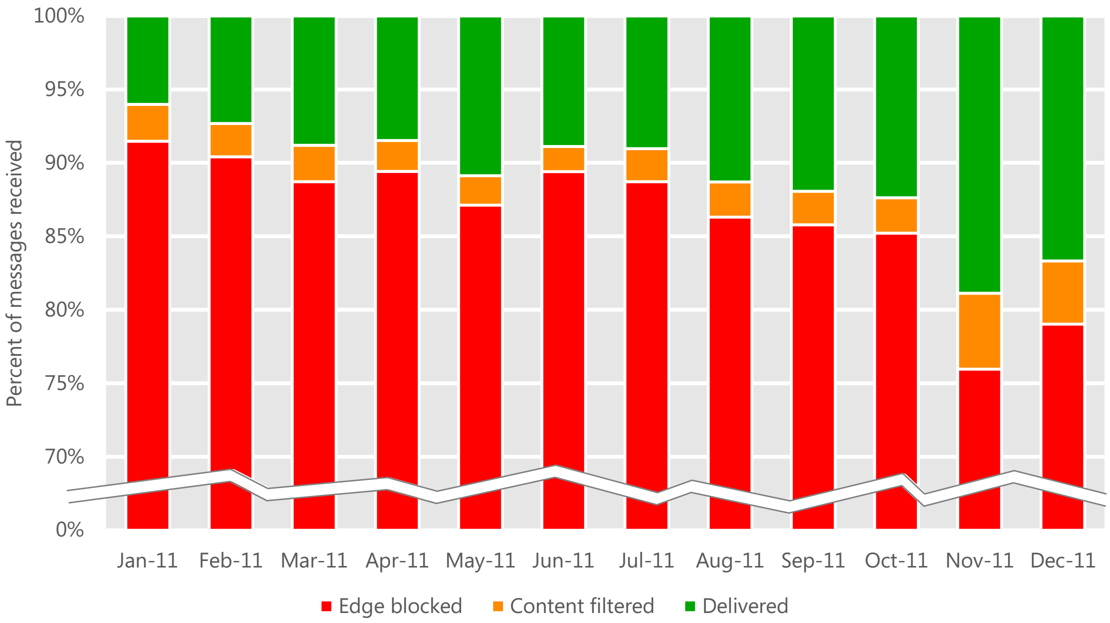


- FOPE blocked 14.0 billion messages in December 2011, less than half of the amount blocked in January. The significant decline in blocked messages seen throughout 2011 is likely attributable to several factors, including the following:
  - Takedown actions waged against a number of high-volume botnets, including the Rustock botnet in March and the Kelihos botnet in September, seem to have had a significant impact on the ability of spammers to distribute their messages to wide audiences. (For more information about the Rustock takedown, see "Battling the Rustock Threat," available from the Microsoft Download Center at www.microsoft.com/download.)
  - As filtering improvements and high-profile takedowns have made it more difficult for spammers to get their messages out, they have adapted their methods in a continual effort to stay one step ahead of spam fighters. Many spammers have shifted from botnet-based delivery to a method some call *snowshoe spam*, whereby spam is distributed in lower volumes from a wider range of IP addresses in an effort to avoid detection. Snowshoe spam is often sent from IP addresses that the spammers have leased legitimately from commercial Internet service providers (ISPs), and

can be difficult for automated blocks and filters to distinguish from legitimate bulk email, such as opt-in newsletters and mailing lists.[27]

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

Figure 43. Percentage of incoming messages blocked by FOPE using edge-blocking and content filtering in 2011



- Between 76 and 92 percent of incoming messages were blocked at the network edge each month, which means that only 8 to 24 percent of incoming messages had to be subjected to the more resource-intensive content filtering process.
- The overall decline in spam blocked between January and December, shown in Figure 42, has disproportionately affected spam blocked at the network edge. Overall, the total volume of content-filtered spam decreased for most of the year, even as the share of content-filtered spam increased relative to edge-blocked spam. This trend reversed in October, as the total volume of content-

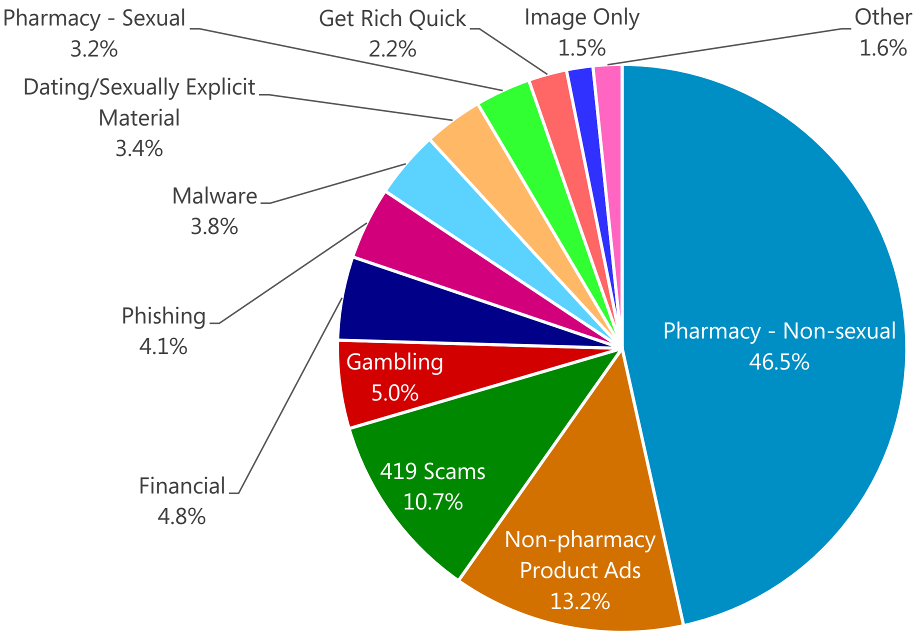
[27] See blogs.msdn.com/b/tzink/archive/2011/11/22/what-snoeshow-spam-looks-like.aspx for more information about snowshoe spam and related concepts.

filtered spam began to increase, possibly in response to the takedown of the Kelihos botnet in September and to the overall trend in favor of more snowshoe spam.

Spam types

The FOPE content filters recognize several different common types of spam messages. Figure 44 shows the relative prevalence of the spam types that were detected in 2H11.

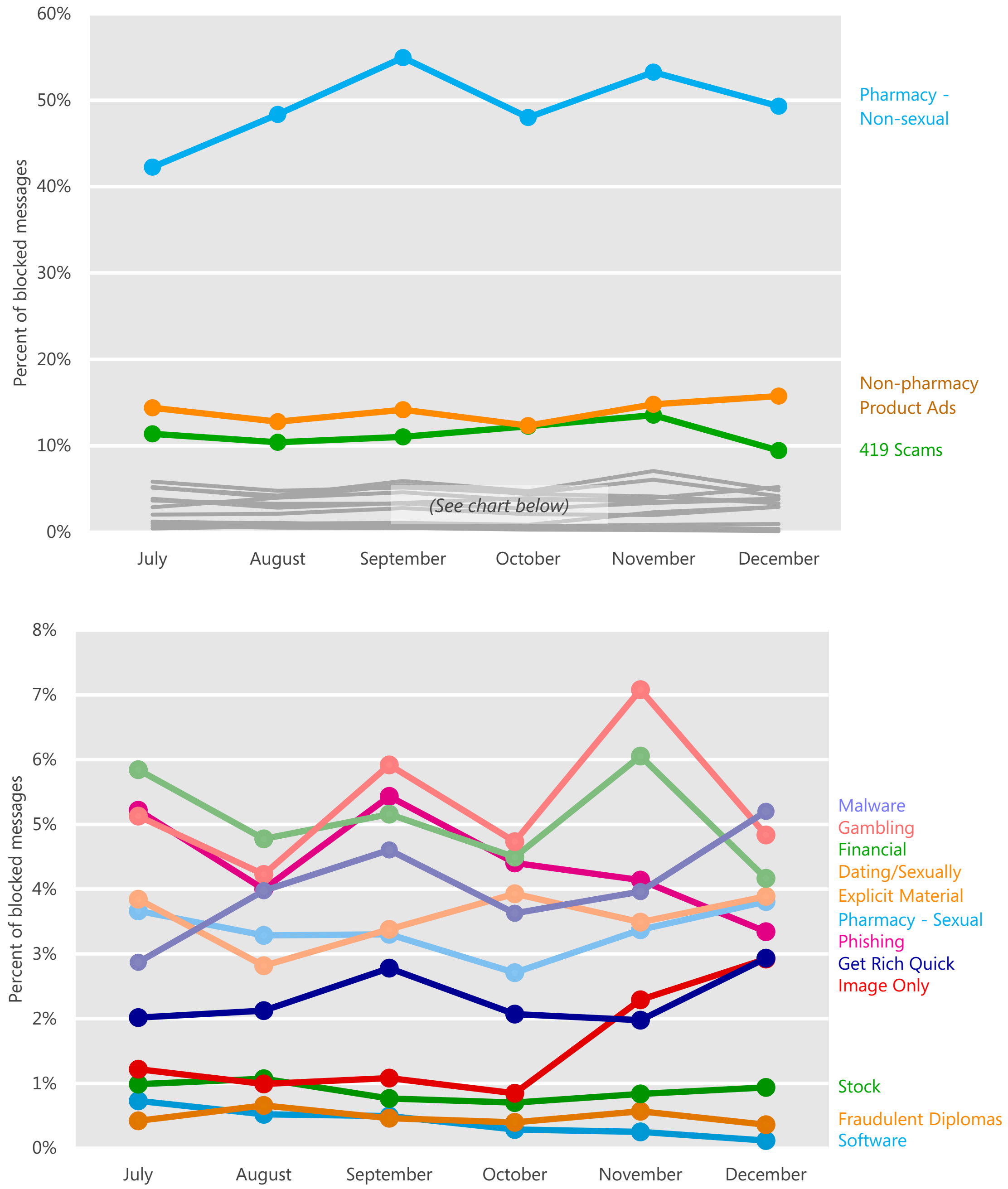
Figure 44. Inbound messages blocked by FOPE filters in 2H11, by category



- Advertisements for pharmaceutical products accounted for almost half of the spam blocked by FOPE content filters in 2H11. The largest total category of spam by a wide margin involved nonsexual pharmaceutical products at 46.5 percent of the total, an increase from 28.0 percent in 1H11. Sexually related pharmaceutical advertisements accounted for 3.2 percent of the total, a decrease from 3.8 percent in 1H11.

- Advertisements for non-pharmaceutical products accounted for an additional 13.2 percent of messages blocked, a decrease from 17.2 percent in 1H11.
- Spam messages associated with advance-fee fraud (so-called "419 scams") accounted for 10.7 percent of messages blocked, a decrease from 13.2 percent in 1H11. An advance-fee fraud is a common confidence trick in which the sender of a message purports to have a claim on a large sum of money, but is unable to access it directly for some reason, typically involving bureaucratic red tape or political corruption. The sender asks the prospective victim for a temporary loan to be used for bribing officials or for paying fees to get the full sum released. In exchange, the sender promises the target a share of the fortune amounting to a much larger sum than the original loan, but does not deliver.

Figure 45. Inbound messages blocked by FOPE content filters each month in 2011, by category



- Advertisements for non-sexual pharmaceutical products accounted for 46.5 percent of the spam messages blocked by FOPE content filters in 2H11.

- Together, non-pharmaceutical product advertisements (13.2 percent) and advertisements for non-sexual pharmaceutical products accounted for the majority of the spam messages blocked by FOPE content filters in 2H11. Along with 419 scams (10.7 percent), these categories accounted for more than 70 percent of the spam messages that were blocked during the period.
- In an effort to evade content filters, spammers sometimes send messages that consist only of one or more images, with no text in the body of the message. Image-only spam messages decreased to 1.5 percent of the total in 2H11 overall, from 3.1 percent in 1H11 and 8.7 percent in 2010. However, image-only spam increased from 0.8 percent in October to 2.1 percent in November and 2.9 percent in December, suggesting that the recent lull may have been temporary.
- Other spam categories that showed significant month-to-month increases in 2H11 included gambling advertisements and financial spam, both of which displayed moderate spikes in November. In both cases, however, the magnitude of the increase was not significantly larger than the month-to-month fluctuations observed throughout the period.

Guidance: Defending against threats in email

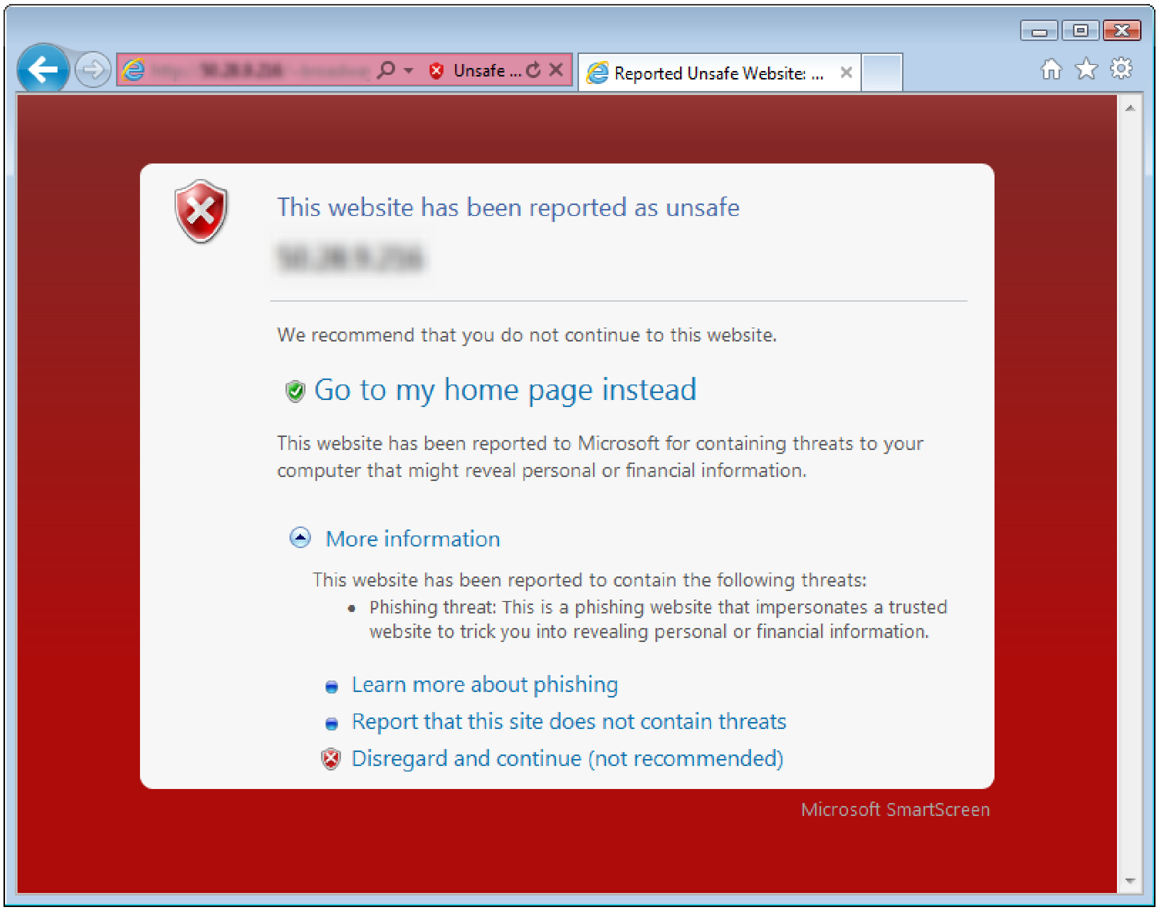
In addition to using a filtering service such as FOPE, organizations can take a number of steps to reduce the risks and inconvenience of unwanted email. Such steps include implementing email authentication techniques and observing best practices for sending and receiving email. For in-depth guidance,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

Malicious websites

Attackers often use websites to conduct phishing attacks or distribute malware. Malicious websites typically appear completely legitimate and often provide no outward indicators of their malicious nature, even to experienced computer users. To help protect users from malicious webpages, Microsoft and other browser vendors have developed filters that keep track of sites that host malware and phishing attacks and display prominent warnings when users try to navigate to them.

The information in this section is compiled from a variety of internal and external sources, including telemetry data produced by SmartScreen® Filter (in Windows Internet Explorer 8 and 9), 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 107 for more information about the products and services that provided data for this report.)

Figure 46. SmartScreen Filter in Internet Explorer 8 and 9 blocks reported phishing and malware distribution sites to protect the user



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* generated by users who choose to enable the Phishing Filter or SmartScreen Filter in Internet Explorer. A phishing impression is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being blocked, as illustrated in Figure 47.

Figure 47. How Microsoft tracks phishing impressions

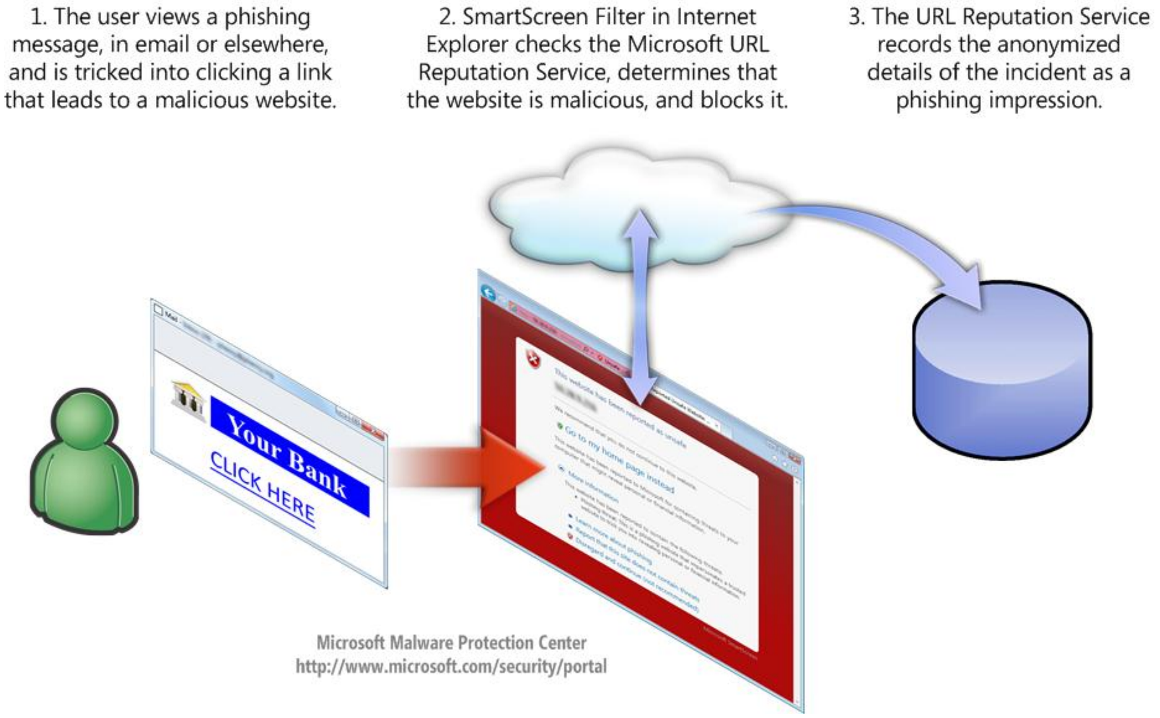
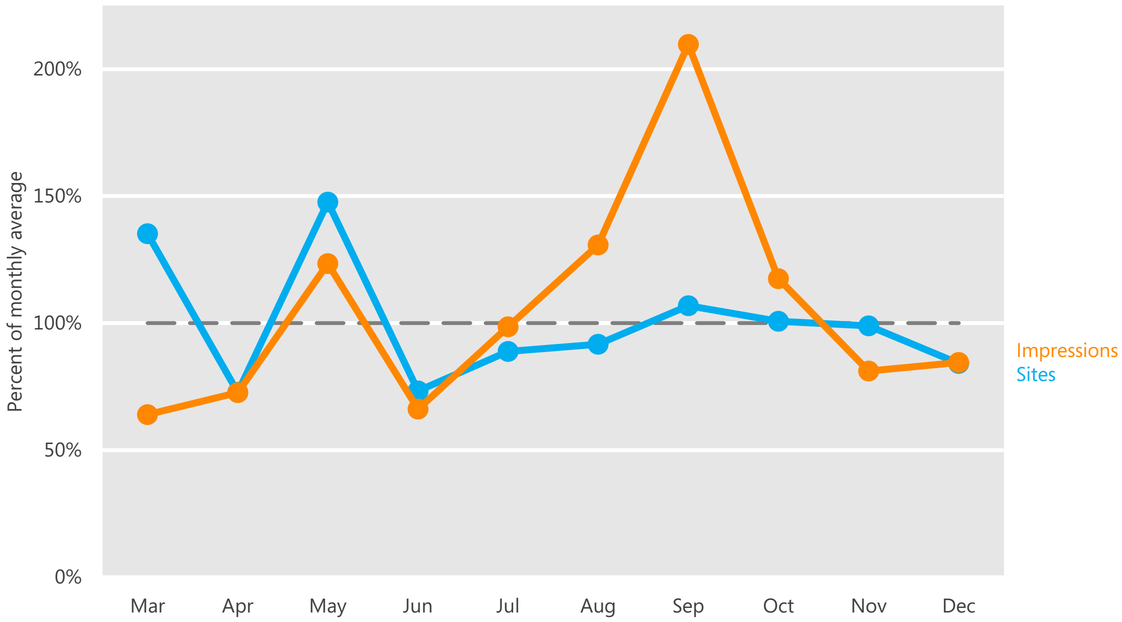

1. The user views a phishing message, in email or elsewhere, and is tricked into clicking a link that leads to a malicious website.
2. SmartScreen Filter in Internet Explorer checks the Microsoft URL Reputation Service, determines that the website is malicious, and blocks it.
3. The URL Reputation Service 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 Malware Protection Center
http://www.microsoft.com/security/portal

Figure 48 compares the volume of active phishing sites in the Microsoft URL Reputation Service database each month with the volume of phishing impressions tracked by Internet Explorer.

Figure 48. Phishing sites and impressions tracked each month from March to December 2011 relative to the monthly average for each



- Phishers often engage in discrete campaigns that are intended to drive more traffic to each phishing page, without necessarily increasing the total number of active phishing pages they maintain at the same time. A large spike in impressions was observed in September, when the number of impressions rose to more than twice the monthly average for the period, primarily because of a small number of very effective campaigns targeting social networks. At the same time, the number of active phishing sites tracked did not increase significantly.
- Most phishing sites only last a few days, and attackers create new ones to replace older ones as they are taken offline, so the list of known phishing sites is prone to constant change without significantly affecting overall volume. This phenomenon can cause significant fluctuations in the number of active phishing sites being tracked, like the one seen between March and June.

Target institutions

Figure 49 and Figure 50 show the percentage of phishing impressions and active phishing sites, respectively, recorded by Microsoft during each month from August to December 2011 for the most frequently targeted types of institutions.

Figure 49. Impressions for each type of phishing site each month from August to December 2011, as reported by SmartScreen Filter

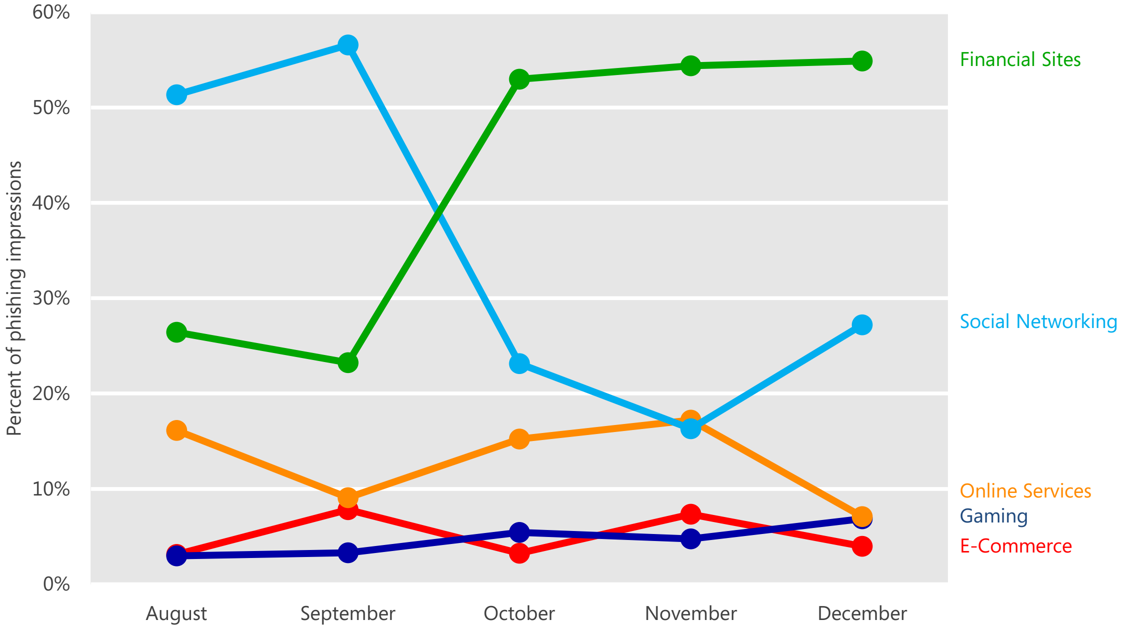
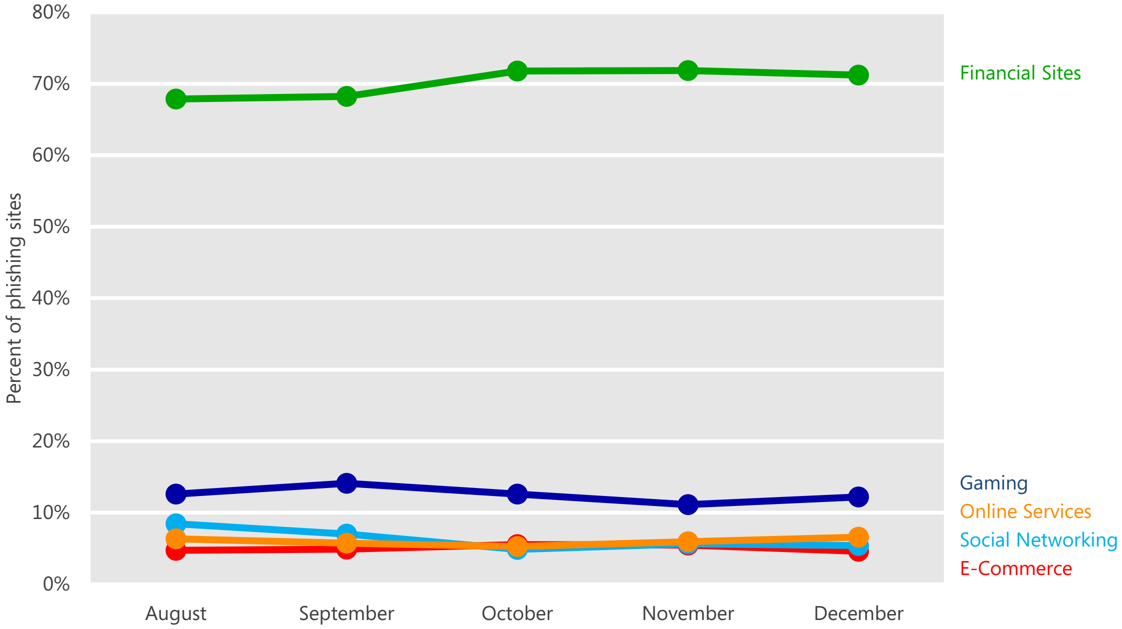


Figure 50. Active phishing sites tracked each month from August to December 2011, by type of target

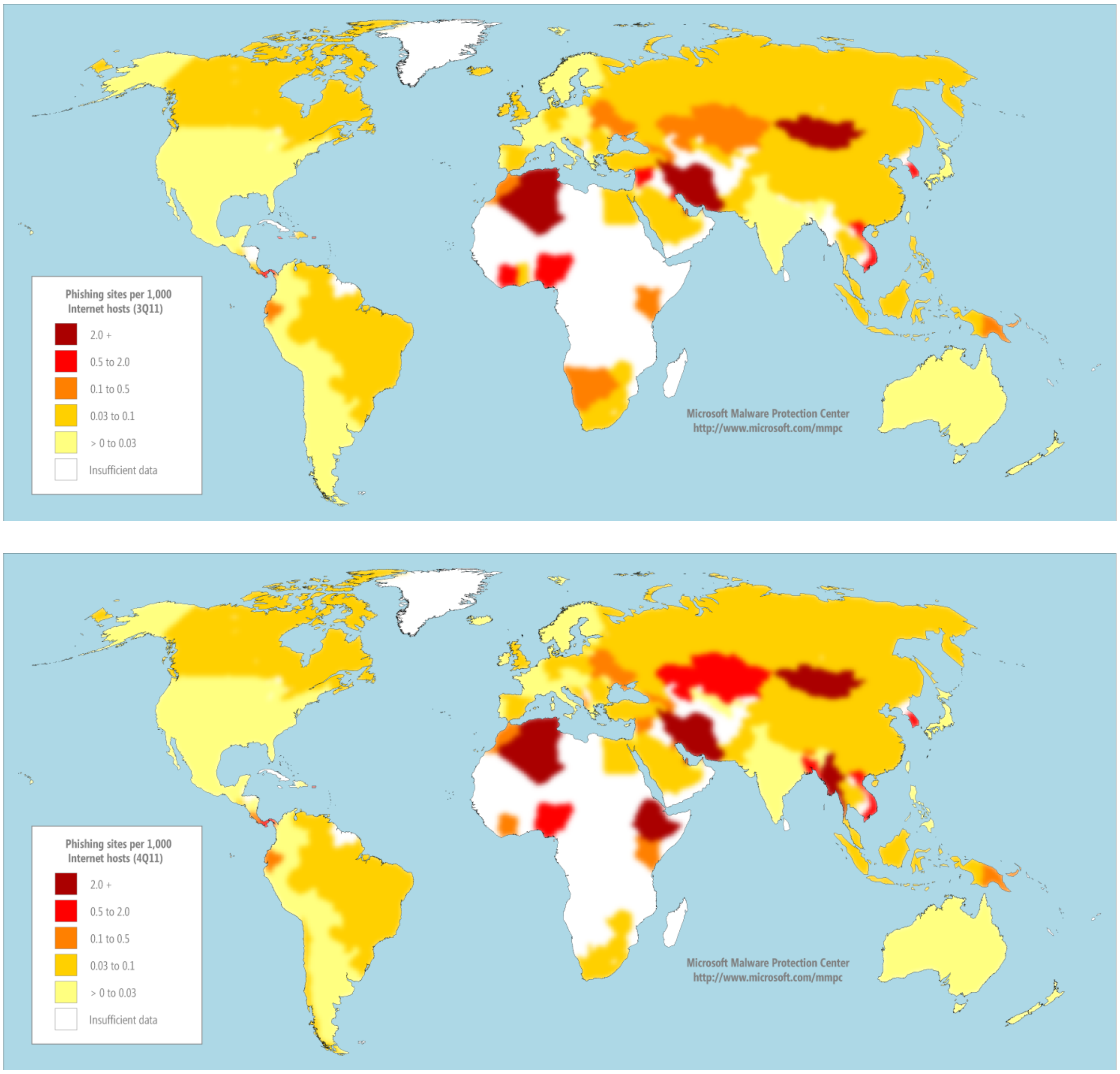


- Impressions by category tend to fluctuate more between successive months than do sites, because of the aforementioned campaign effect, in which phishers sometimes engage in short periods of intense activity designed to drive traffic to a small number of sites.
- Phishing sites that targeted financial institutions accounted for an average of 70.4 percent of active phishing sites tracked from August to December 2011, although they accounted for just 34.8 percent of impressions. Financial institutions are relatively inefficient targets for phishers, because the number of possible institutions to target can number in the hundreds or more even within a relatively small population of Internet users. Nevertheless, the potential for direct illicit access to victims' bank accounts make financial institutions a tempting target for many criminals, and they continue to receive the largest or second-largest number of impressions each month.
- By contrast, the number of popular social networking sites is much smaller, so phishers who target social networks can effectively target many more people per site. Social networks accounted for just 6.1 percent of phishing sites between August and December 2011 on average, but garnered 43.7 percent of impressions. Much of this traffic was because of a period of increased phishing activity in September targeting social networks, as mentioned on page 91.
- This phenomenon also occurs on a smaller scale with online services and gaming sites. A small number of online services account for most traffic to such sites, so phishing sites that targeted online services garnered 12.0 percent of impressions with just 6.0 percent of sites. Online gaming traffic tends to be spread out among a larger number of sites, so phishing sites that targeted online gaming destinations accounted for 12.5 percent of active sites but gained just 4.1 percent of impressions.

Global distribution of phishing sites

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

Figure 51. Phishing sites per 1,000 Internet hosts for locations around the world in 3Q11 (top) and 4Q11 (bottom)

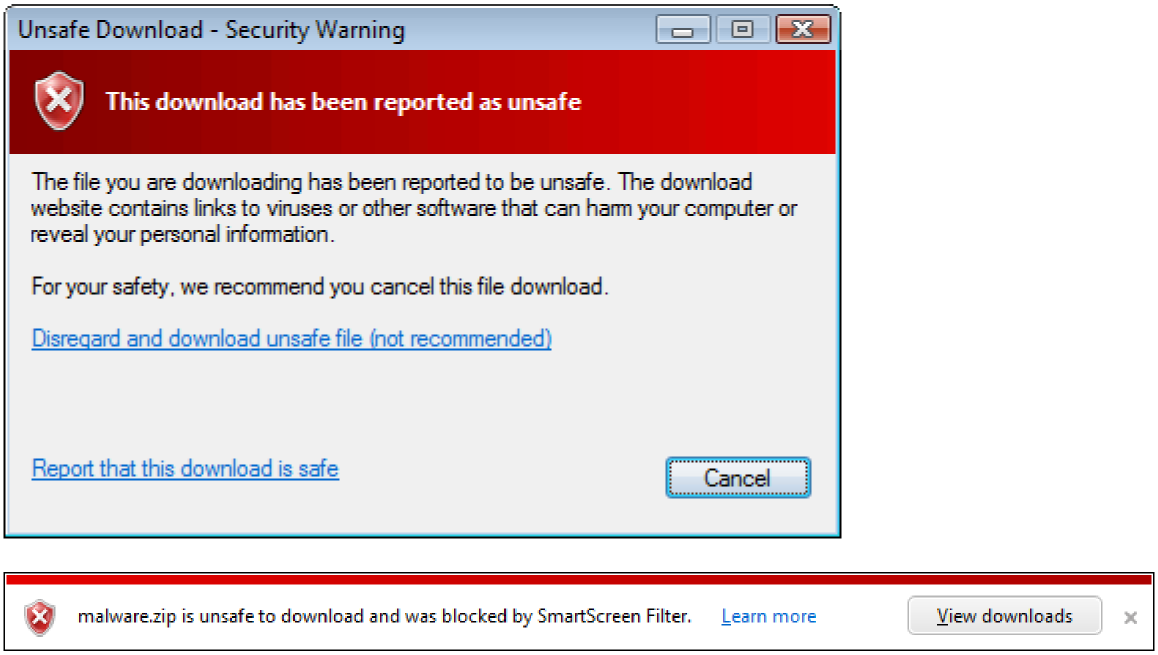

Phishing sites per 1,000 Internet hosts (3Q11)
2.0 +
0.5 to 2.0
0.1 to 0.5
0.03 to 0.1
> 0 to 0.03
Insufficient data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc
Phishing sites per 1,000 Internet hosts (4Q11)
2.0 +
0.5 to 2.0
0.1 to 0.5
0.03 to 0.1
> 0 to 0.03
Insufficient data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

- Locations with smaller populations and fewer Internet hosts tend to have higher concentrations of phishing sites, although in absolute terms most phishing sites are located in large, industrialized countries/regions with large numbers of Internet hosts.
- Significant locations with unusually high concentrations of phishing sites include Mongolia, with 5.6 phishing sites per 1,000 hosts in 4Q11; Iran, with 2.4; and Korea, with 0.6.

Malware hosting sites

SmartScreen Filter in Internet Explorer 8 and 9 helps provide protection against sites that are known to host malware, in addition to phishing sites. SmartScreen Filter uses URL reputation data and Microsoft antimalware technologies to determine whether those sites distribute unsafe content. As with phishing sites, Microsoft keeps track of how many people visit each malware hosting site and uses the information to improve SmartScreen Filter and to better combat malware distribution.

Figure 52. SmartScreen Filter in Internet Explorer 8 (top) and Internet Explorer 9 (bottom) displays a warning when a user attempts to download an unsafe file



Unsafe Download - Security Warning

This download has been reported as unsafe

The file you are downloading has been reported to be unsafe. The download website contains links to viruses or other software that can harm your computer or reveal your personal information.

For your safety, we recommend you cancel this file download.

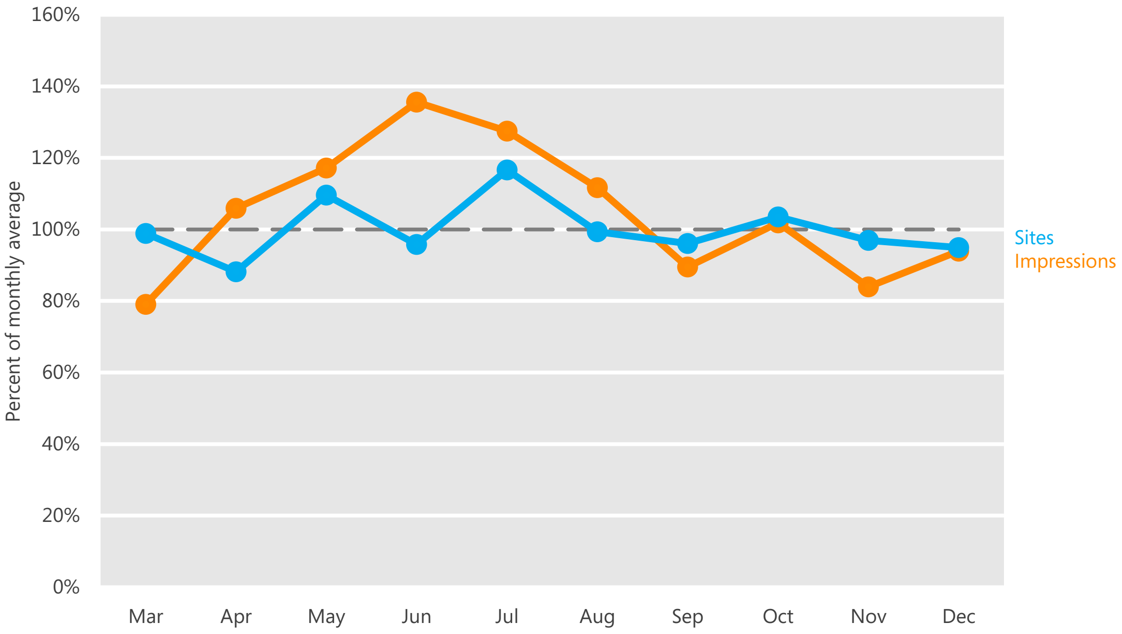
Disregard and download unsafe file (not recommended)

Report that this download is safe

malware.zip is unsafe to download and was blocked by SmartScreen Filter.

Figure 53 compares the volume of active malware hosting sites in the Microsoft URL Reputation Service database each month with the volume of malware impressions tracked by Internet Explorer.

Figure 53. Malware hosting sites and impressions tracked each month from March to December 2011, relative to the monthly average for each



- As with phishing, malware hosting impressions and active sites rarely correlate strongly with each other, and months with high numbers of sites and low numbers of impressions (or vice versa) are not uncommon.

Malware categories

Figure 54 and Figure 55 show the types of threats hosted at URLs that were blocked by SmartScreen Filter in 2H11.

Figure 54. Categories of malware found at sites blocked by SmartScreen Filter in 2H11, by percent of all malware impressions

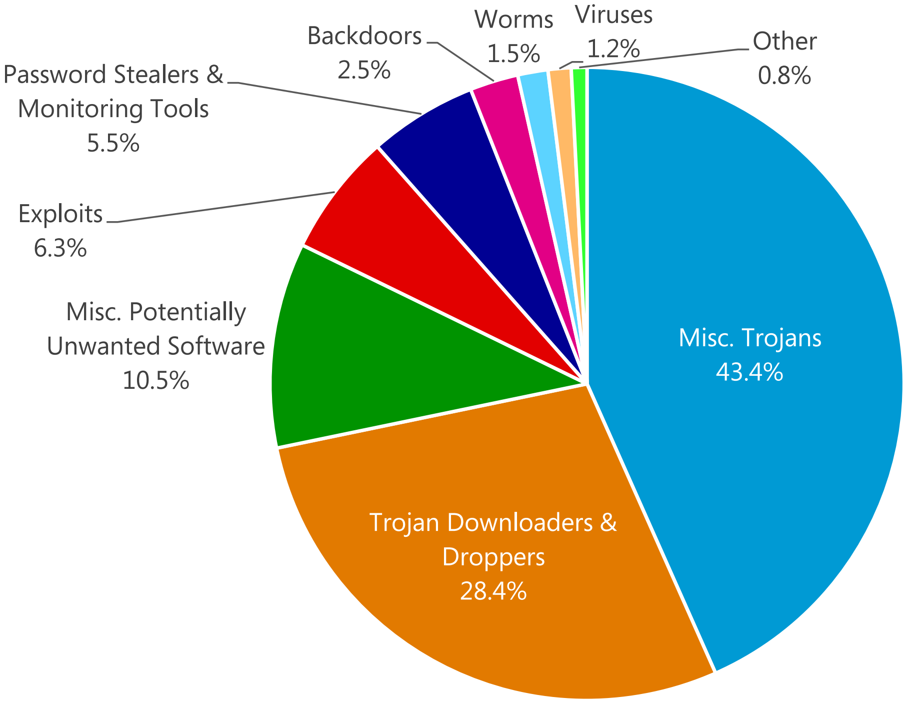


Figure 55. Top families found at sites blocked by SmartScreen Filter in 2H11, by percent of all malware impressions

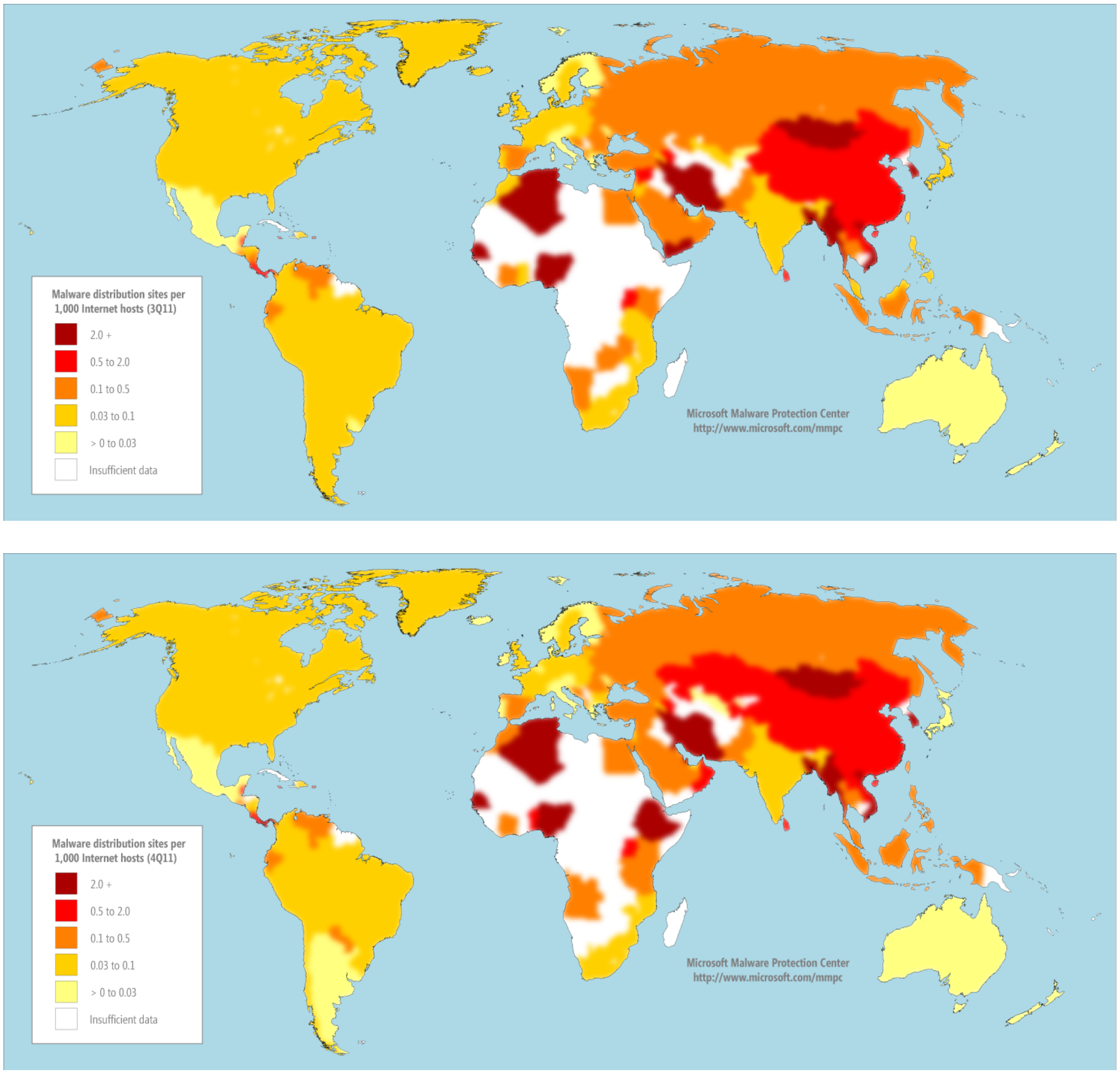
	Family	Most Significant Category	Percent of Malware Impressions
1	Win32/Startpage	Misc. Trojans	15.7%
2	Win32/Swisyn	Trojan Downloaders & Droppers	10.4%
3	Win32/Banload	Trojan Downloaders & Droppers	5.8%
4	Win32/Dynamer	Misc. Trojans	5.1%
5	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.5%
6	JS/ShellCode	Exploits	3.9%
7	Win32/Microjoin	Trojan Downloaders & Droppers	2.1%
8	Win32/Malf	Trojan Downloaders & Droppers	2.0%
9	Win32/VB	Worms	1.9%
10	Win32/Sisproc	Misc. Trojans	1.8%
11	Win32/Meredrop	Misc. Trojans	1.8%
12	Win32/Delf	Trojan Downloaders & Droppers	1.6%
13	Win32/Pdfjsc	Exploits	1.4%
14	Win32/Agent	Misc. Trojans	1.4%
15	Win32/BaiduSobar	Misc. Potentially Unwanted Software	1.4%
16	Win32/Bulilit	Trojan Downloaders & Droppers	1.3%
17	Win32/Sirefef	Misc. Trojans	1.3%

- Most of the families on the list are generic detections for a variety of threats that share certain identifiable characteristics.
- Win32/Startpage, the family responsible for the most malware impressions in 2H11, is a generic detection for malware that changes the home page of an affected user's web browser without consent.
- Win32/Swisyn, in second place, is a family of trojans that drops and executes files on an infected computer. These files may be embedded as resource files, and are often bundled with legitimate files in an effort to evade detection.

Global distribution of malware hosting sites

Figure 56 shows the geographic distribution of malware hosting sites reported to Microsoft in 2H11.

Figure 56. Malware distribution sites per 1,000 Internet hosts for locations around the world in 3Q11 (top) and 4Q11 (bottom)


Malware distribution sites per 1,000 Internet hosts (3Q11)
2.0 +
0.5 to 2.0
0.1 to 0.5
0.03 to 0.1
> 0 to 0.03
Insufficient data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc
Malware distribution sites per 1,000 Internet hosts (4Q11)
2.0 +
0.5 to 2.0
0.1 to 0.5
0.03 to 0.1
> 0 to 0.03
Insufficient data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

- As with phishing sites, locations with smaller populations and fewer Internet hosts tend to have higher concentrations of phishing sites, although in absolute terms most phishing sites are located in large, industrialized countries/regions with large numbers of Internet hosts.

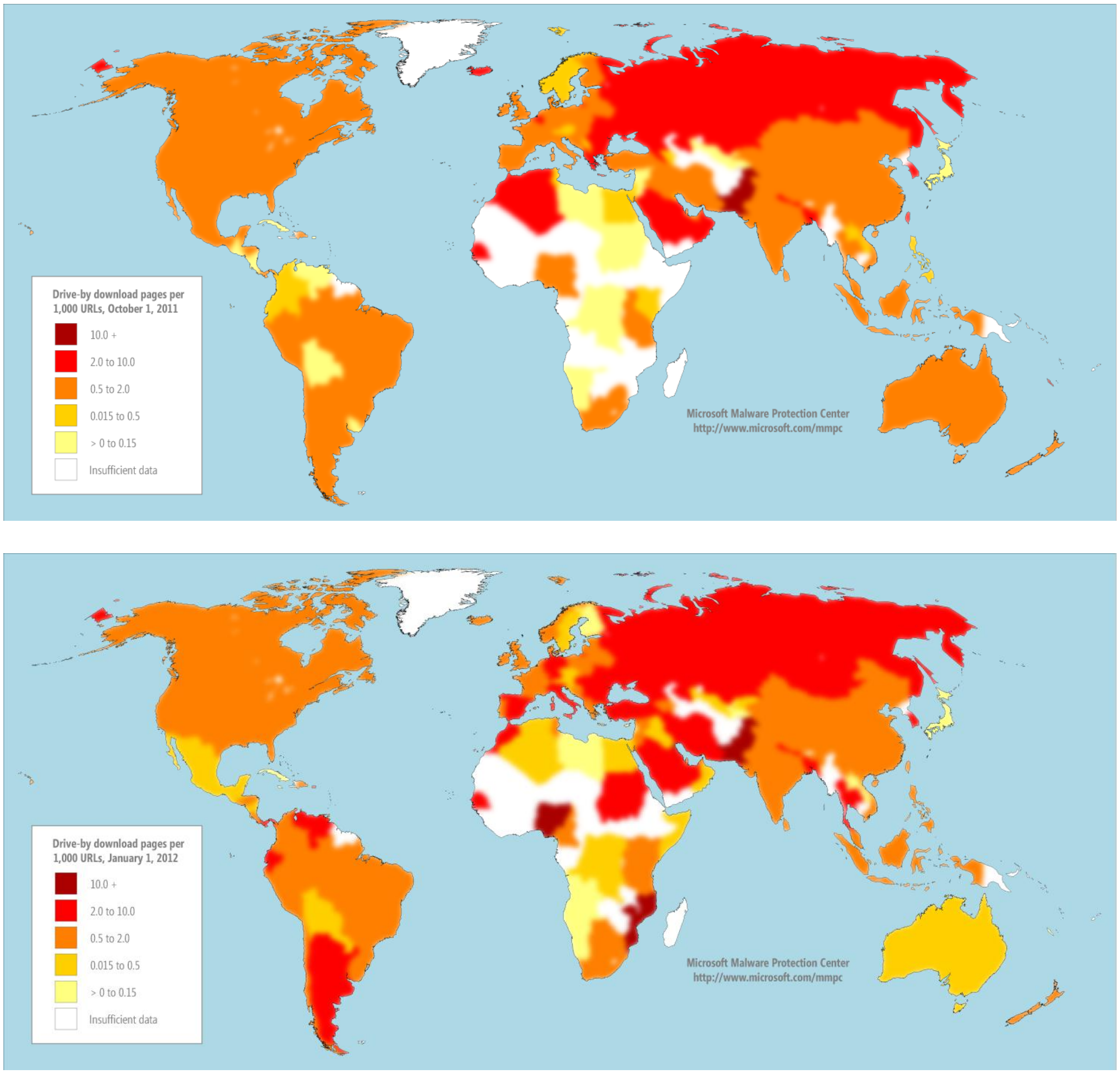
Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything.

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

Figure 57 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 3Q11 and 4Q11, respectively.

Figure 57. Drive-by download pages indexed by Bing.com at the end of 3Q11 (top) and 4Q11 (bottom), per 1000 URLs in each country/region



Drive-by download pages per 1,000 URLs, October 1, 2011
10.0 +
2.0 to 10.0
0.5 to 2.0
0.015 to 0.5
> 0 to 0.15
Insufficient data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc
Drive-by download pages per 1,000 URLs, January 1, 2012
10.0 +
2.0 to 10.0
0.5 to 2.0
0.015 to 0.5
> 0 to 0.15
Insufficient data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

- Each map shows the concentration of drive-by download URLs tracked by Bing in each country or region on a reference date at the end of the associated quarter, expressed as the number of drive-by download URLs per every 1,000 URLs hosted in the country/region. This snapshot approach contrasts with the accumulative approach used to report drive-by downloads in previous volumes of the *Microsoft Security Intelligence Report*, which accounted for every drive-by URL detected at any point during the relevant period. This new approach is intended to more accurately reflect the short-lived nature of most drive-by URLs; however, comparisons between the data presented here and data presented in previous volumes is not appropriate and should be avoided.

- Significant locations with unusually high concentrations of drive-by download URLs in both quarters include Pakistan, with 5.8 drive-by URLs for every 1,000 URLs tracked by Bing at the end of 4Q11; Saudi Arabia, with 3.3; Romania, with 2.7; and Korea, with 2.1.

Guidance: Protecting users from unsafe websites

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

- Promoting Safe Browsing
- Protecting Your People

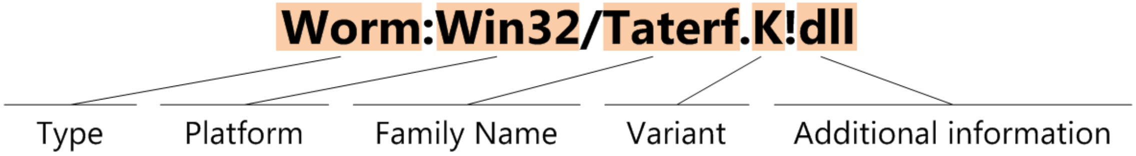
Appendixes

Appendix A: Threat naming conventions

The MMPC malware naming standard is derived from the Computer Antivirus Research Organization (CARO) Malware Naming Scheme, originally published in 1991 and revised in 2002. Most security vendors use naming conventions that are based on the CARO scheme, with minor variations, although family and variant names for the same threat can differ between vendors.

A threat name can contain some or all of the components seen in Figure 58.

Figure 58. The Microsoft malware naming convention



The *type* indicates the primary function or intent of the threat. The MMPC assigns each individual threat to one of a few dozen different 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 10 categories. For example, the TrojanDownloader and TrojanDropper types are combined into a single category, called Trojan Downloaders & Droppers.

The *platform* indicates the operating environment in which the threat is designed to run and spread. For most of the threats described in this report, the platform is listed as “Win32,” for the Win32 API used by 32-bit and 64-bit versions of Windows desktop and server operating systems. (Not all Win32 threats can run on every version of Windows, however.) Platforms can include programming languages and file formats, in addition to operating systems. For example, threats in the ASX/Wimad family are designed for programs that parse the Advanced Stream Redirector (ASX) file format, regardless of operating system.

Groups of closely related threats are organized into *families,* which are given unique names to distinguish them from others. The family name is usually not related to anything the malware author has chosen to call the threat. Researchers use a variety of techniques to name new families, such as excerpting and modifying strings of alphabetic characters found in the malware file. Security vendors usually try to adopt the name used by the first vendor to positively identify a new family, although sometimes different vendors use completely different names for the same threat, which can happen when two or more vendors discover a new family independently. The MMPC Encyclopedia (www.microsoft.com/mmpc) lists the names used by other major security vendors to identify each threat, when known.

Some malware families include multiple components that perform different tasks and are assigned different types. For example, the Win32/Frethog family includes variants designated PWS:Win32/Frethog.C and TrojanDownloader:Win32/Frethog.C, among others. In the *Microsoft Security Intelligence Report*, the category listed for a particular family is the one that Microsoft security analysts have determined to be the most significant category for the family (which, in the case of Frethog, is Password Stealers & Monitoring Tools).

Malware creators often release multiple *variants* for a family, typically in an effort to avoid being detected by security software. Variants are designated by letters, which are assigned in order of discovery—A through Z, then AA through AZ, then BA through BZ, and so on. A variant designation of "gen" indicates that the threat was detected by a generic signature for the family rather than as a specific variant. Any additional characters that appear after the variant provide comments or additional information.

In the *Microsoft Security Intelligence Report,* a threat name that consists of a platform and family name (for example, "Win32/Taterf") is a reference to a family. When a longer threat name is given (for example, "Worm:Win32/Taterf.K!dll"), it is a reference to a more specific signature or to an individual variant. To make the report easier to read, family and variant names have occasionally been abbreviated in contexts where confusion is unlikely. Thus, Win32/Taterf would be referred to simply as "Taterf" on subsequent mention in some places, and Worm:Win32/Taterf.K simply as "Taterf.K."

Appendix B: Data sources

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

- Bing, the search and decision engine from Microsoft, contains technology that performs billions of webpage scans per year to seek out malicious content. After such content is detected, Bing displays warnings to users about it to help prevent infection.
- Windows Live Hotmail has hundreds of millions of active email users in more than 30 countries/regions around the world.
- Forefront Online Protection for Exchange (FOPE) protects the networks of thousands of enterprise customers worldwide by helping to prevent malware from spreading through email. FOPE scans billions of email messages every year to identify and block spam and malware.
- Microsoft Forefront Endpoint Protection is a unified product that provides protection from malware and potentially unwanted software for enterprise desktops, laptops, and server operating systems. It uses the Microsoft Malware Protection Engine and the Microsoft antivirus signature database to provide real-time, scheduled, and on-demand protection.
- Windows Defender is a program that is available at no cost to licensed users of Windows that provides real-time protection against pop-ups, slow performance, and security threats caused by spyware and other potentially unwanted software. Windows Defender runs on more than 100 million computers worldwide.
- The Malicious Software Removal Tool (MSRT) is a free tool that Microsoft designed to help identify and remove prevalent malware families from customer computers. The MSRT is primarily released as an important update through Windows Update, Microsoft Update, and Automatic Updates. A version of the tool is also available from the Microsoft Download Center. The MSRT was downloaded and executed more than 600 million times each

month on average in 2H11. The MSRT is not a replacement for an up-to-date antivirus solution because of its lack of real-time protection and because it uses only the portion of the Microsoft antivirus signature database that enables it to target specifically selected, prevalent malicious software.

- Microsoft Security Essentials is a free real-time protection product that combines an antivirus and antispyware scanner with phishing and firewall protection.
- 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.
- SmartScreen Filter, a feature in Internet Explorer 8 and 9, 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.

Figure 59. US privacy statements for the Microsoft products and services used in this report

Product or Service	Privacy Statement URL
Bing	privacy.microsoft.com/en-us/bing.mspx
Windows Live Hotmail	privacy.microsoft.com/en-us/fullnotice.mspx
Forefront Online Protection for Exchange	https://admin.messaging.microsoft.com/legal/privacy/en-us.htm
Windows Defender	www.microsoft.com/windows/products/winfamily/defender/privacypolicy.mspx
Malicious Software Removal Tool	www.microsoft.com/security/pc-security/msrt-privacy.aspx
Forefront Endpoint Protection	www.microsoft.com/download/en/details.aspx?id=23308
Microsoft Security Essentials	windows.microsoft.com/en-US/windows/products/security-essentials/privacy
Microsoft Safety Scanner	www.microsoft.com/security/scanner/en-us/Privacy.aspx
Windows Internet Explorer 9	windows.microsoft.com/en-US/internet-explorer/products/ie-9/windows-internet-explorer-9-privacy-statement

Appendix C: Worldwide infection rates

"Global infection rates," on page 55, explains how threat patterns differ significantly in different parts of the world. Figure 60 shows the infection rates in locations with at least 100,000 quarterly MSRT executions in 2011, as determined by geolocation of the IP address of the reporting computer. [28] CCM is the number of computers cleaned for every 1,000 executions of MSRT. See the *Microsoft Security Intelligence Report* website for more information about the CCM metric and how it is calculated.

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

Figure 60. Infection rates (CCM) for locations around the world in 2011, by quarter

Country/Region	1Q11	2Q11	3Q11	4Q11
Albania	23.7	25.0	19.3	25.0
Algeria	20.8	16.2	14.2	17.3
Angola	21.4	20.1	18.6	16.1
Argentina	11.4	11.1	8.3	8.3
Armenia	9.2	8.0	6.9	6.8
Australia	5.3	4.6	5.3	4.6
Austria	4.6	3.4	3.9	8.4
Azerbaijan	11.4	10.6	10.3	11.7
Bahamas, The	17.4	14.3	12.0	10.6
Bahrain	16.5	19.2	18.0	15.6
Bangladesh	13.0	13.7	14.9	16.9
Barbados	7.5	6.4	5.4	4.6

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

Country/Region	1Q11	2Q11	3Q11	4Q11
Belarus	6.0	6.0	6.3	5.6
Belgium	6.4	5.6	6.1	4.7
Bolivia	13.3	14.3	13.9	13.0
Bosnia and Herzegovina	18.4	16.4	13.4	15.8
Brazil	19.2	18.8	17.2	14.0
Brunei	14.4	12.9	9.6	9.1
Bulgaria	13.9	10.7	8.3	9.0
Cambodia	9.2	12.0	12.4	11.5
Cameroon	15.3	11.3	11.3	12.8
Canada	4.4	5.2	5.8	4.3
Chile	15.4	10.8	7.9	13.9
China	2.4	2.3	1.5	1.0
Colombia	11.8	11.5	8.7	7.8
Costa Rica	11.8	8.9	6.4	5.8
Côte d’Ivoire	15.3	12.7	12.9	13.3
Croatia	14.5	10.9	8.1	10.0
Cyprus	15.1	10.9	9.6	8.0
Czech Republic	5.2	2.9	2.6	2.3
Denmark	2.6	3.0	2.2	2.0
Dominican Republic	18.9	16.7	14.8	14.0
Ecuador	14.2	11.2	9.0	8.6
Egypt	20.9	19.5	17.5	22.7
El Salvador	13.6	10.7	8.1	6.5
Estonia	6.6	4.9	4.8	4.0
Ethiopia	10.2	10.9	9.8	9.2
Finland	1.4	1.3	1.8	1.6
France	6.0	5.0	4.2	3.8
Georgia	22.7	21.6	20.1	21.6
Germany	3.6	3.2	3.3	11.0
Ghana	13.7	11.5	10.5	11.6
Greece	13.0	10.1	9.5	8.5
Guadeloupe	14.8	13.0	9.7	9.1
Guatemala	12.4	10.7	8.8	7.1

Country/Region	1Q11	2Q11	3Q11	4Q11
Haiti	—	—	14.6	17.6
Honduras	15.0	12.4	10.2	9.4
Hong Kong SAR	8.9	7.9	5.6	4.4
Hungary	8.7	6.9	5.9	5.1
Iceland	6.8	4.7	4.4	3.7
India	15.2	15.9	15.0	13.8
Indonesia	16.2	18.4	18.7	18.6
Iran	9.1	10.0	10.0	10.6
Iraq	13.1	18.0	20.5	22.0
Ireland	5.9	4.7	4.8	3.8
Israel	15.1	12.1	9.2	9.5
Italy	7.8	6.4	5.2	9.0
Jamaica	16.2	12.5	9.0	9.1
Japan	2.7	2.1	1.9	1.3
Jordan	17.6	18.5	15.3	16.0
Kazakhstan	10.1	8.8	7.9	10.2
Kenya	13.0	11.4	10.5	9.5
Korea	30.1	19.8	12.0	11.1
Kuwait	17.0	15.5	12.8	12.0
Latvia	11.9	9.2	7.0	6.8
Lebanon	15.4	15.8	12.7	12.3
Lithuania	13.5	10.7	7.9	7.7
Luxembourg	4.2	3.2	3.2	3.1
Macao SAR	6.9	5.8	4.6	3.0
Macedonia, FYRO	20.2	14.4	12.5	15.1
Malaysia	13.4	12.0	10.2	9.0
Malta	8.7	6.0	5.6	4.5
Martinique	13.5	10.3	8.4	7.7
Mauritius	12.0	12.1	10.8	9.2
Mexico	16.7	13.5	9.7	8.8
Moldova	7.4	6.7	6.0	6.5
Mongolia	10.7	10.8	9.2	11.2
Morocco	14.4	13.1	12.0	12.3

Country/Region	1Q11	2Q11	3Q11	4Q11
Mozambique	18.1	14.3	12.6	12.0
Nepal	18.9	23.7	24.0	22.4
Netherlands	4.6	5.3	6.6	13.1
New Zealand	5.7	5.1	4.8	3.8
Nicaragua	11.6	9.2	6.7	5.7
Nigeria	13.1	10.6	9.3	8.5
Norway	2.9	2.5	2.5	2.3
Oman	19.3	18.1	14.4	15.5
Pakistan	27.7	31.1	31.9	32.9
Palestinian Authority	27.5	32.7	27.1	29.9
Panama	15.8	12.8	10.8	9.6
Paraguay	8.9	7.7	6.7	6.3
Peru	16.8	13.7	10.3	10.0
Philippines	11.7	11.0	10.3	9.6
Poland	14.1	11.4	8.7	8.9
Portugal	11.5	9.8	8.9	8.9
Puerto Rico	13.4	10.7	8.0	6.9
Qatar	61.5	34.4	12.1	13.5
Reunion	11.9	11.1	7.9	7.4
Romania	16.5	15.3	14.0	13.8
Russia	6.7	6.0	6.1	7.2
Saudi Arabia	16.4	16.2	14.3	14.1
Senegal	15.1	13.0	10.1	10.4
Serbia	16.0	15.6	13.3	14.4
Singapore	12.6	9.0	6.9	5.7
Slovakia	9.6	6.1	4.2	3.6
Slovenia	9.0	6.3	5.0	4.6
South Africa	13.4	10.6	9.4	8.1
Spain	13.2	11.4	6.9	7.6
Sri Lanka	11.3	12.0	11.3	10.8
Sudan	14.8	16.7	16.6	16.3
Sweden	2.8	2.4	2.7	2.5
Switzerland	3.5	2.8	2.8	2.3

Country/Region	1Q11	2Q11	3Q11	4Q11
Syria	11.2	14.0	15.9	15.9
Taiwan	17.7	16.1	10.4	8.2
Tanzania	17.6	13.6	11.6	10.2
Thailand	18.0	19.6	19.4	17.9
Trinidad and Tobago	17.5	11.9	10.1	8.4
Tunisia	16.0	13.6	11.2	13.2
Turkey	28.2	25.5	22.7	26.6
Uganda	16.9	15.0	12.0	11.6
Ukraine	7.4	6.6	6.3	7.1
United Arab Emirates	18.9	16.7	15.1	16.0
United Kingdom	5.1	5.1	5.5	5.1
United States	5.6	5.6	9.4	5.5
Uruguay	6.1	6.1	5.3	4.0
Venezuela	9.8	8.5	7.5	7.1
Vietnam	12.8	15.8	16.3	16.5
Yemen	20.4	21.7	—	20.5

Glossary

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

419 scam
See *advance-fee fraud*.

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

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

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

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

ASLR
See *Address Space Layout Randomization (ASLR)*

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

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

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 MSRT. For example, if 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).

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

Data Execution Prevention (DEP)
A security technique designed to prevent buffer overflow attacks. DEP enables the system to mark areas of memory as non-executable, preventing code in those memory locations from running.

definition
A set of signatures that antivirus, antispyware, or antimalware products can use to identify malware. Other vendors may refer to definitions as DAT files, pattern files, identity files, or antivirus databases.

DEP
See *Data Execution Prevention (DEP)*

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

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

downloader/dropper
See *trojan downloader/dropper*.

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

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

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

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

in the wild
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.

Internet Relay Chat (IRC)
A distributed real-time Internet chat protocol that is designed for group communication. Many botnets use the IRC protocol for C&C.

keylogger
A program that sends keystrokes or screen shots to an attacker. Also see *password stealer (PWS)*.

malware
Any software that is designed specifically to cause damage to a user's computer, server, or network. Viruses, worms, and trojans are all types of malware.

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 8 or 9. Also see *phishing impression.*

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)*.

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

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

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

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

phishing impression
A single instance of a user attempting to visit a known phishing page with Internet Explorer 7, 8, or 9, and being blocked by the Phishing Filter or SmartScreen Filter. Also see *malware impression*.

polymorphic
A characteristic of malware that can mutate its structure to avoid detection by antimalware programs, without changing its overall algorithm or function.

pop-under
A webpage that opens in a separate window that appears beneath the active browser window. Pop-under windows are commonly used to display advertisements.

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

remote control software
A program that provides access to a computer from a remote location. Such programs are often installed by the computer owner or administrator and are only a risk if unexpected.

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.

rootkit
A program whose main purpose is to perform certain functions that cannot be easily detected or undone by a system administrator, such as hiding itself or other malware.

SEHOP
See *Structured Exception Handler Overwrite Protection (SEHOP)*.

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

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

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

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

Structured Exception Handler Overwrite Protection (SEHOP)
A security technique designed to prevent exploits from overwriting exception handlers to gain code execution. SEHOP verifies that a thread's exception handler list is intact before allowing any of the registered exception handlers to be called.

tool
Software that may have legitimate purposes but may also be used by malware authors or attackers.

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

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

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

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

wild
See *in the wild*.

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

Threat families referenced in this report

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

Win32/Agent. A generic detection for a number of trojans that may perform different malicious functions. The functionality exhibited by this family is highly variable.

Win32/Autorun. A family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

Win32/BaiduSobar. A Chinese-language web browser toolbar that delivers pop-up and contextual advertisements, blocks certain other advertisements, and changes the Internet Explorer search page.

Win32/Bamital. A family of malware that intercepts web browser traffic and prevents access to specific security-related websites by modifying the Hosts file. Bamital variants may also modify specific legitimate Windows files in order to execute their payload.

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

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

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

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 containing the exploit pack, various malware may be downloaded and run.

Win32/Bulilit. A trojan that silently downloads and installs other programs without consent. Infection could involve the installation of additional malware or malware components to an affected computer.

Win32/ClickPotato. A program that displays pop-up and notification-style advertisements based on the user's browsing habits.

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.

Java/CVE-2010-0840. A detection for a malicious and obfuscated Java class that exploits a vulnerability described in CVE-2010-0840. Oracle Corporation addressed the vulnerability with a security update in March 2010.

Win32/Delf. A detection for various threats written in the Delphi programming language. The behaviors displayed by this malware family are highly variable.

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

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

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

Win32/EyeStye. A trojan that attempts to steal sensitive data using a method known as *form grabbing*, and sends it to a remote attacker. It may also download and execute arbitary files and use a rootkit component to hide its activities.

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

Win32/FakeRean. A rogue security software family distributed under a variety of randomly generated names, including Win 7 Internet Security 2010, Vista Antivirus Pro, XP Guardian, and many others.

Win32/FakeSpypro. A rogue security software family distributed under the names Antivirus System PRO, Spyware Protect 2009, and others.

Win32/FakeSysdef. A rogue security software family that claims to discover nonexistent hardware defects related to system memory, hard drives, and overall system performance, and charges a fee to fix the supposed problems.

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

Win32/Helompy. A worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or online services, including Facebook and Gmail.

Win32/Hotbar. Adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of web-browsing activity.

Win32/Keygen. A generic detection for tools that generate product keys for illegally obtained versions of various software products.

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

Win32/Malf. A generic detection for malware that drops additional malicious files.

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.

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/OfferBox. A program that displays offers based on the user's web browsing habits. Some versions may display advertisements in a pop-under window. Win32/OfferBox may be installed without adequate user consent by malware.

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

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

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

Win32/Parite. A family of viruses that infect .exe and .scr executable files on the local file system and on writeable network shares.

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

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

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

Win32/RealVNC. A management tool that allows a computer to be controlled remotely. It can be installed for legitimate purposes but can also be installed from a remote location by an attacker.

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

Win32/Rimecud. A family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

Win32/Rugo. A program that installs silently on the user's computer and displays advertisements.

Win32/Rustock. A multi-component family of rootkit-enabled backdoor trojans that were first developed around 2006 to aid in the distribution of spam email.

Win32/Sality. A family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.

JS/ShellCode. A generic detection for JavaScript-enabled objects that contain exploit code and may exhibit suspicious behavior. Malicious websites and malformed PDF documents may contain JavaScript that attempts to execute code without the affected user's consent.

Win32/ShopperReports. Adware that displays targeted advertising to affected users while browsing the Internet, based on search terms entered into search engines.

Win32/Sirefef. A rogue security software family distributed under the name Antivirus 2010 and others.

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

Win32/Taterf. A family of worms that spread through mapped drives to steal login and account details for popular online games.

Win32/Tracur. A trojan that downloads and executes arbitrary files, redirects web search queries to a malicious URL, and may also install other malware.

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

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

ASX/Wimad. A detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.

Win32/Winwebsec. A rogue security software family distributed under the names Winweb Security, System Security, and others.

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

Win32/Zwangi. A program that runs as a service in the background and modifies web browser settings to visit a particular website.

TwC Next

Microsoft®

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

www.microsoft.com/twcnext