Microsoft Security Intelligence Report

Volume 13

January through June, 2012

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

Copyright © 2012 Microsoft Corporation. All rights reserved.

Microsoft, the Microsoft logo, Active Directory, ActiveX, AppLocker, Bing, DirectX, Forefront, Hotmail, Internet Explorer, MSDN, Outlook, PowerPoint, the Security Shield logo, SQL Server, Visual Basic, Win32, Windows, Windows Media, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Authors

Danielle Alyias
Microsoft Trustworthy Computing

Dennis Batchelder
Microsoft Protection Technologies

Joe Blackbird
Microsoft Malware Protection Center

Joe Faulhaber
Microsoft Malware Protection Center

David Felstead
Bing

Roger A. Grimes
Microsoft IT Information Security and Risk Management

Paul Henry
Wadeware LLC

Jeff Jones
Microsoft Trustworthy Computing

Jimmy Kuo
Microsoft Malware Protection Center

Marc Lauricella
Microsoft Trustworthy Computing

Jenn LeMond
Microsoft IT Security and Risk Management

Nam Ng
Microsoft Trustworthy Computing

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Anthony Penta
Microsoft Windows Safety Platform

Tim Rains
Microsoft Trustworthy Computing

David Ross
Microsoft Trustworthy Computing

David Seidman
Microsoft Trustworthy Computing

Weijuan Shi Davis
Windows Business Group

Holly Stewart
Microsoft Malware Protection Center

Matt Thomlinson
Microsoft Trustworthy Computing

Terry Zink
Microsoft Exchange Online Protection

Contributors

Doug Cavit
Microsoft Trustworthy Computing

Enrique Gonzalez
Microsoft Malware Protection Center

Heather Goudey
Microsoft Malware Protection Center

Angela Gunn
Microsoft Trustworthy Computing

Satomi Hayakawa
CSS Japan Security Response Team

Greg Lenti
CSS Security Readiness & Response Team

Le Li
Microsoft Windows Safety Platform

Ken Malcolmson
Microsoft Trustworthy Computing

Hideya Matsuda
CSS Japan Security Response Team

Takumi Onodera
Microsoft Premier Field Engineering, Japan

Kathy Phillips
Microsoft Legal and Corporate Affairs

Hilda Larina Ragragio
Microsoft Malware Protection Center

Laura A. Robinson
Microsoft Information Security & Risk Management

Richard Saunders
Microsoft Trustworthy Computing

Jasmine Sesso
Microsoft Malware Protection Center

Frank Simorjay
Microsoft Trustworthy Computing

Mark Simos
Microsoft Consulting Services

Norie Tamura
CSS Japan Security Response Team

Kurt Tonti
Microsoft Information Security & Risk Management

Henk van Roest
CSS Security EMEA

Patrik Vicol
Microsoft Malware Protection Center

Steve Wacker
Wadeware LLC

Iaan Wiltshire
Microsoft Malware Protection Center

Dan Wolff
Microsoft Malware Protection Center

The Microsoft Pass-the-Hash Working Group

Deceptive downloads: Software, music, and movies

Malware authors go to great lengths to distribute their wares, and they invest significant resources into finding victims and avoiding detection by antimalware products. Attackers experiment with different methods and mechanisms for distributing malware, ranging from exploits to pure social-engineering–based approaches. Recently, the Microsoft Malware Protection Center (MMPC) has observed a growing trend of malware infection associated with unsecure supply chains—the websites, protocols, and other channels by which software and media files are informally distributed, both legally and illegally. Unsecure distribution mechanisms range from underground sites where pirated software and media are openly exchanged, to legitimate websites that make shareware or free music files available for public download. In some cases, malware has even been discovered preinstalled on computers sold at retail.[1] Any mechanism by which untrusted parties can distribute files to a wider audience without sufficient safeguards in place is a potential vehicle for malware dissemination.

This section of the *Microsoft Security Intelligence Report* examines how attackers take advantage of these unsecure supply chains to distribute malware to victims around the world, with data and analysis about the problem based on Microsoft antimalware telemetry. It also provides guidance that computer users and administrators can use to help protect themselves from malware distributed through unsecure supply chains.

Detecting malware associated with unsecure supply chains

Through analysis of the data reported by Microsoft antimalware products running on computers that have been opted in to data collection,[2] it is possible to discern patterns of activity that show a correlation between unsecure supply chains and malware. In some cases, this correlation may simply involve malware samples that have the same names as certain files that are known to be disseminated on file-distribution sites and networks—spreading malware by claiming it is something else is a time-honored tactic used by attackers.

In other cases, a correlation can be drawn from the presence on the reporting computer of other threat families—including Win32/Keygen, Win32/Pameseg,

[1] See "Operation b70: Nitol Malware Research and Analysis," a report by the Microsoft Digital Crimes Unit, for additional details about one such incident.

[2] See "**Error! Reference source not found.**" on page 113 for links to privacy statements for the products and services that provided the data for this report.

and Win32/Gendows—that are strongly associated with file distribution activity. These indicator families were detected on 16.8 percent of all computers reporting detections in the first quarter of 2012, increasing to 17.2 percent of computers in the second quarter. Some of these indicator families are considered potentially unwanted software rather than malware, but all can be taken as evidence that file distribution activity has probably occurred. By looking at malware detected alongside the indicator families and comparing it with malware detections reported by computers that *don't* also report detections of indicator families, MMPC researchers can estimate the extent and impact of attackers' abuse of the file distribution supply chain.

Malware and unsecure software distribution

The most commonly reported threat family in 1H12 was Win32/Keygen, a detection for tools that generate keys for various software products. Software pirates often bundle a key-generator utility with a well-known application and then distribute the package using a torrent client or by uploading the package to a file distribution site. A user who downloads the package runs the key-generator utility to create a product key that will supposedly allow the software to be used illegally. Its widespread impact—of the 105 countries or regions covered in this report, 98 percent listed Keygen as one of the top 10 families detected in 1H12—and its strong association with unsecure file distribution activity make it a good indicator family to use to examine how attackers exploit such activity to distribute malware.

An examination of Keygen reports shows a diverse list of popular software products being targeted, as indicated by some of the file names used by the Keygen executable:

- keygen.exe
- Windows Loader.exe
- mini-KMS_Activator_v1.1_Office.2010.VL.ENG.exe
- AutoCAD-2008-keygen.exe
- SonyVegasPro Patch.exe
- Nero Multimedia Suite 10 - Keygen.exe
- Adobe.Photoshop.CS5.Extended.v12.0.Keymaker-EMBRACE.exe
- Call.of.Duty.4.Modern.Warfare.Full-Rip.Skullptura.7z
- Guitar Pro v6.0.7+Soundbanks+Keygen(Registered) [kk].rar
- Half Life CDkeygen.exe

Installing pirated software bears significant risks. In many cases, the distributed packages contain malware alongside (or instead of) the pirated software, which takes advantage of the download and install process to infect the computers of users who download the bundles. More than 76 percent of computers reporting Keygen detections in 1H12 also reported detections of other threat families, which is 10 percent higher than the average co-infection rate for other families. (See "Malware statistics" on page 7 for additional information.)

The tactic of bundling malware with software on unsecure file distribution sites and networks is not limited to pirated commercial software—attackers sometimes take advantage of traffic in freely distributed software as well. In 1H12, the MMPC observed 35 different threat families being distributed using the file name install_adobeflash.exe, which purports to be an installation package for the freely distributed Adobe Flash Player. Threats that make use of this technique in 1H12 included notable families such as Win32/Sirefef, Win32/Bancos, and Win32/FakeRean. (See "Threat families" beginning on page 53 for more information about these and other threats.)

Similar tactics are used by attackers who engage in so-called paid archive schemes, in which users are convinced or tricked into paying for software that might otherwise be available for free. The most commonly detected threat family in 1H12 in Russia, Ukraine, and several other countries and regions in eastern Europe and western Asia was Win32/Pameseg, a family of programs that claim to install various popular software packages. A user who launches a Pameseg installer is instructed to send an SMS text message to a premium number (typically at a cost of between 5 and 20 US dollars, although the installer usually claims that it will be free of charge) to successfully install the program. Among the top file names used by Pameseg installers in 1H12 were several that resembled the names of programs that can be legally downloaded and installed for free, in addition to paid commercial programs:

- Adobe Photoshop CS5 key-rus.exe
- avast_free.exe
- DirectX11.exe
- kb909241x.exe
- LoviVkontakte.exe
- powerpoint-setup.exe
- Skype.exe
- SkypeSetup.exe
- vksaver.exe
- willarchive.exe

For more information about Pameseg and paid archive schemes, see the following entries in the MMPC blog (blogs.technet.com/mmpc):

- Easy Money: Program:Win32/Pameseg (part one) (November 14, 2011)
- Easy Money: Program:Win32/Pameseg (part two) (November 21, 2011)

Other hacking tools that are frequently used to distribute malware with shared or pirated software include:

- Win32/Gendows. A tool that attempts to activate Windows 7 and Windows Vista operating system installations.
- Win32/Patch. A family of tools intended to modify, or "patch," programs that may be evaluation copies or unregistered versions with limited features, for the purpose of removing the limitations.
- Win32/Wpakill. A family of tools that attempt to disable or bypass WPA (Windows Product Activation), WGA (Windows Genuine Advantage) checks, or WAT (Windows Activation Technologies) by altering Windows operating system files, terminating processes, or stopping services.

Music, movies, and malware

Like software, popular movies and music are often traded on unsecure file distribution sites and networks. As with software, attackers have taken advantage of the illegal trafficking in media files to spread malware.

The ASX/Wimad family is a generic detection for malicious URL script commands found in Advanced Systems Format (ASF) (a file format used by Windows Media) that download arbitrary files. Several of the file names used by Wimad files suggest a global hit parade of popular music:

- - - 1 Alejate De Mi - Camila.mp3
- - Lady Gaga - Telephone (feat. Beyonce).mp3
- - - Alexandra Stan - - - Mr. Saxobeat.mp3
- 0 Merche - Si Te Marchas.mp3
- 09. Pitbull - Back In Time (From Men In Black III).mp3
- 09 Back In Time - Pitbull.mp3
- Oasis - Stop Crying Your Heart Out.mp3
- - - Moves Like Jagger - Maroon 5 Christina Aguilera.mp3
- עמיר בן עיון עומד בשער.mp3 [Amir Benayun, “Standing at the Gate”]
- Rumer - Slow.mp3

Current popular films are also well-represented in the list of Wimad file names:

- The Avengers 2012 720p BDRip QEBS7 AAC20 MP4-FASM.avi
- Prometheus 2012 DVDRip.avi
- Wrath of the Titans 2012 DVDRip aXXo.avi
- Battleship 2012 DVDRip.avi
- What to Expect When You're Expecting 2012.BRRip.XviD-KAZAN.avi
- The Hunger Games 2012 TRUE FRENCH DVDRIP XViD FiCTiON L S79.avi
- Sherlock.Holmes.2.A.Game.of.Shadows.2012.DVDRip.XviD-26K-0123.avi
- The Five-Year Engagement 2012 HDRip XviD-HOPE.avi
- Project X 2012 TRUE FRENCH DVDRIP XViD FiCTiON L S79.avi
- Amazing SpiderMan 2012 DVDRiP XviD.avi

Malware statistics

Computers reporting detections of the six indicator families mentioned (Keygen, Wimad, Pameseg, Wpakill, Gendows, and Patch) have a higher malware detection rate than those that don’t.[3] Figure 1 lists the families that were most commonly detected alongside the indicator families in 1H12.

[3] See “**Error! Reference source not found.**” on page 113 for information about the Microsoft

Figure 1. Threat families most commonly detected on computers displaying evidence of unsecure file distribution in 1H12, by absolute number of computers and by percentage of all computers displaying such evidence

Family	Most significant category	1Q12	1Q12 %	2Q12	2Q12 %
Win32/Autorun	Worms	849,108	10.5%	937,747	11.3%
JS/Pornpop	Adware	637,966	7.9%	661,711	8.0%
Win32/Obfuscator	Misc. Potentially Unwanted Software	515,575	6.4%	606,081	7.3%
Blacole	Exploits	561,561	7.0%	512,867	6.2%
Win32/Dorkbot	Worms	492,106	6.1%	522,617	6.3%

- 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,[4] but attackers continue to distribute malware that attempts to target it.

- JS/Pornpop is a detection for specially crafted JavaScript-enabled objects that attempt to display pop-under advertisements in users' web browsers. Initially, 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.

- Win32/Obfuscator is 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.

- Blacole is a multiplatform family of exploits that target vulnerabilities in popular products and components and are delivered through malicious or compromised webpages. (See page 23 for more information about Blacole.)

- Win32/Dorkbot is 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. Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.

See "Malware and potentially unwanted software" beginning on page 39 for more information about threat detection patterns around the world.

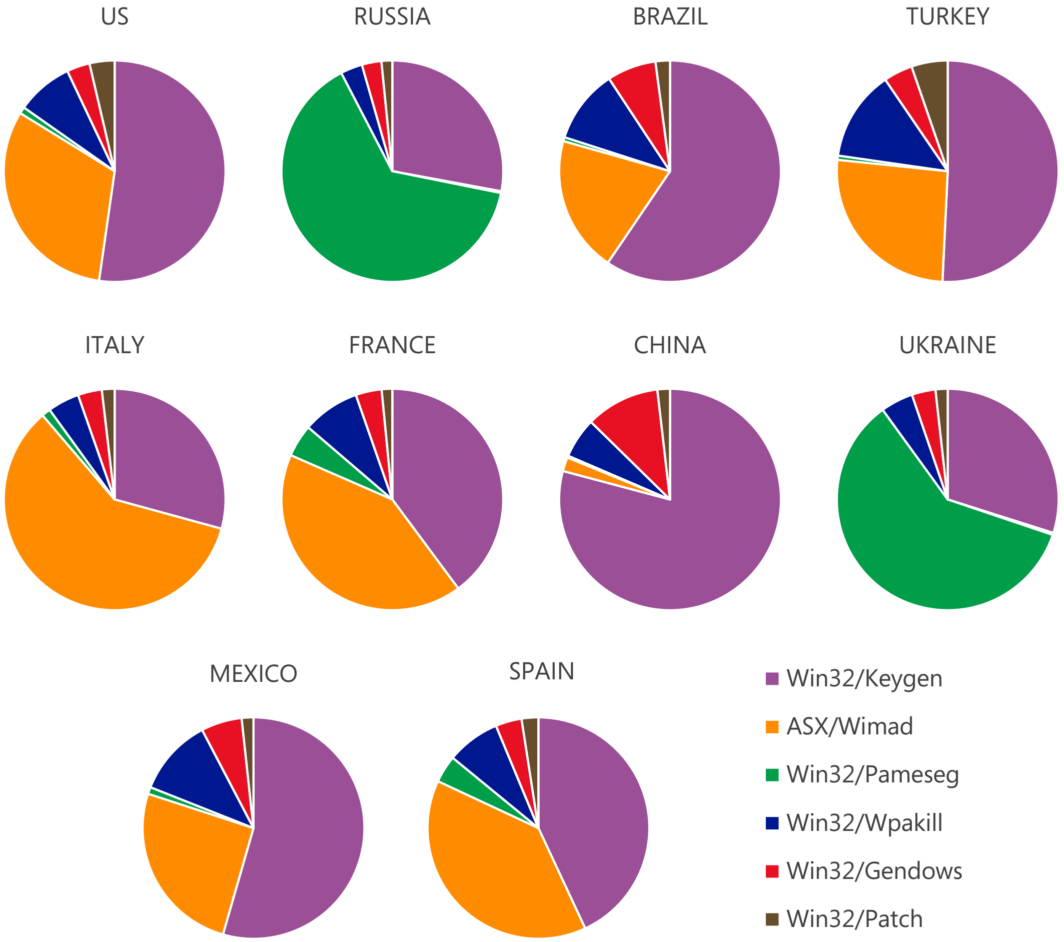
products and services that generated the telemetry used for this analysis.

[4] See support.microsoft.com/kb/971029 for more information about these changes.

Regional variations

Detections of the indicator families described in this section vary between different countries and regions. In Russia, Pameseg is detected far more often than the others; in some other locations, such as Italy and France, Wimad is in the top position. Figure 2 illustrates how these families are detected in different proportions in several different locations.

Figure 2. Relative detections of the indicator families discussed in this section in the 10 countries/regions with the most detections in 2Q12



Guidance: Defending against supply chain threats

Organizations and IT departments can use various processes and technological solutions to minimize the risk they face from malware transmitted through unsecure supply chains. Processes include the following:

- Create policies that state what constitutes acceptable and unacceptable downloading and use of third-party tools and media. Institute policies that govern the download and execution of music, movies, and game media. Create and enforce disciplinary actions for repeat policy offenders.
- Block peer-to-peer (P2P) applications from communicating into or out of the organization's internal network.
- Ensure that all new hardware is purchased by an internal procurement team. Procurement processes might include formatting computers and devices upon receipt and reinstalling the operating systems from known good images. Such images should include antimalware software, intrusion detection tools, software firewalls, monitoring and reporting tools, and other security software, all of which should be enabled by default.

Technology solutions to implement include the following:

- Use the AppLocker feature in Windows to create blacklists for potentially unsafe applications, programs, and scripts on client computers.
- On proxy servers, implement rules to block known malicious websites as well as other websites that violate the organization's acceptable media usage policy for content such as music, movies, games, shopping, pornography, and so on.
- Regularly update the organization's hardware and software standards, and limit the amount of old hardware and software. A 64-bit computer running Windows 7 and Internet Explorer 9, for example, is inherently more secure than a 32-bit computer running Windows XP and Internet Explorer 6 because of technologies such as ASLR, DEP, and SmartScreen Filter.

Vendors should use code signing and digital rights management to ensure customers can trust and confirm the authenticity of downloads.

Individual users can protect themselves by running antimalware software from a reputable vendor and keeping it up to date, and by only downloading software and content from trustworthy sources. Software updates and free software should only be obtained from the original vendors or from known, reputable sources. Using Internet Explorer with SmartScreen Filter enabled can help provide protection from malicious downloads.

TwC Next

Microsoft

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

www.microsoft.com/twcnext