Microsoft Security Intelligence Report

Volume 18 | July through December, 2014

Featured Intelligence

Authors

Dennis Batchelder
Microsoft Malware Protection Center

Joe Blackbird
Microsoft Malware Protection Center

Patti Chrzan
Microsoft Digital Crimes Unit

Elia Florio
Microsoft Malware Protection Center

Chad Foster
Bing

Paul Henry
Wadeware LLC

Jeff Jones
Corporate Communications

Marianne Mallen
Microsoft Malware Protection Center

Nam Ng
Worldwide Cybersecurity & Data Protection

Niall O'Sullivan
Microsoft Digital Crimes Unit

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Ina Ragragio
Microsoft Malware Protection Center

Tim Rains
Worldwide Cybersecurity & Data Protection

Paul Rebriy
Bing

Holly Stewart
Microsoft Malware Protection Center

Jerome Stewart
Microsoft Digital Crimes Unit

Todd Thompson
Microsoft IT Information Security and Risk Management

David "dwizzle" Weston
Operating Systems Group

Contributors

Chun Feng
Microsoft Malware Protection Center

Tanmay Ganacharya
Microsoft Malware Protection Center

Cristin Goodwin
Microsoft Trustworthy Computing

Roger Grimes
Microsoft IT

Satomi Hayakawa
CSS Japan Security Response Team

Ben Hope
Microsoft Malware Protection Center

Yurika Kakiuchi
CSS Japan Security Response Team

Marc Lauricella
Corporate Communications

Jenn LeMond
Microsoft IT

Scott Molenkamp
Microsoft Malware Protection Center

Dolcita Montemayor
Microsoft Malware Protection Center

Daric Morton
Microsoft Services

Cody Nicewanner
Operating Systems Group

Hamish O'Dea
Microsoft Malware Protection Center

Jeong Wook Oh
Microsoft Malware Protection Center

Dmitriy Pletnev
Microsoft Malware Protection Center

Laura A. Robinson
Microsoft IT

Jasmine Sesso
Microsoft Malware Protection Center

Norie Tamura
CSS Japan Security Response Team

Steve Wacker
Wadeware LLC

Vladimir Zubko
Microsoft Malware Protection Center

Table of contents

About this report

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

Reporting period

This volume of the *Microsoft Security Intelligence Report* focuses on the third and fourth quarters of 2014, with trend data for the last several quarters presented on a quarterly basis. Because vulnerability disclosures can be highly inconsistent from quarter to quarter and often occur disproportionately at certain times of the year, statistics about vulnerability disclosures are presented on a half-yearly basis.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, in which *yy* indicates the calendar year and *n* indicates the half or quarter. For example, 1H14 represents the first half of 2014 (January 1 through June 30), and 4Q13 represents the fourth quarter of 2013 (October 1 through December 31). To avoid confusion, please note the reporting period or periods being referenced when considering the statistics in this report.

Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware. For information about this standard, see "Appendix A: Threat naming conventions" on page 105 of the full report. In this report, any threat or group of threats that share a common unique base name is considered a family for the sake of presentation. This consideration includes threats that may not otherwise be considered families according to common industry practices, such as generic detections. For the purposes of this report, a "threat" is defined as a malware or unwanted software family or variant that is detected by the Microsoft Malware Protection Engine.

Foreword

As I look at the latest data in this volume of the *Microsoft Security Intelligence Report* I can clearly see the threat landscape evolving in at least a few important ways.

First, vulnerability disclosures across the entire industry increased precipitously in the second half of 2014, increasing 56 percent from the first half of the year. 4,512 vulnerabilities were disclosed during the second half of 2014, representing the largest number of vulnerabilities disclosed in any six month period since the Common Vulnerabilities and Exposures system was launched in 1999. This increase is predominantly the result of work performed by the Computer Emergency Response Team (CERT) Coordination Center (CERT/CC) finding almost 1,400 individual CVEs affecting thousands of different publishers of Android apps and code libraries (more details can be found in this report).

Secondly, commercial exploit kits continue to be popular tools among some attackers. The speed at which we see newly discovered exploits get incorporated into commercial exploit kits has accelerated. The timespan between the availability of a security update and when an exploit for the vulnerability is integrated into a commercial exploit kit was significantly reduced in the second half of 2014. It used to take weeks or months for new exploits to appear in exploit kits, but in the second half of 2014 we saw that time period decrease to ten days or less in several cases.

Thirdly, attackers have focused on attacking vulnerabilities in Oracle Java for many years. But that trend changed in the second half of 2014 when Microsoft deployed a new feature in Internet Explorer that blocks the use of out-of-date Java. This helped to blunt the high volume of exploitation attempts on out-of-date Java installations and protect many, many consumers and organizations from these attacks.

The last highlight I'll mention is that newer versions of Windows operating systems are performing better than older versions at mitigating malware and threats. Windows 8.1 and Windows Server 2012 R2 have some of the lowest malware infection rates we have seen and are providing clear security benefits to those people and organizations using them.

You'll get plenty of other insights in this volume of the *Microsoft Security Intelligence Report* and I hope you get real value from the data.

Tim Rains
Chief Security Advisor
Worldwide Cybersecurity & Data Protection

Featured intelligence

The life and times of an exploit

The CVE-2014-6332 vulnerability, a memory corruption issue in Windows OLE, was a focus for attackers in the last quarter of 2014. Initially released by an independent security researcher as a proof-of-concept exploit with fully operational code, it was quickly repurposed by both targeted attack groups and criminal exploit kits alike, despite the availability of a security update addressing the vulnerability.

This section focuses on the details of this exploit, its use by both criminals and targeted attack groups, and the material impact of this and other released exploits. It illustrates how attackers can move quickly to take advantage of newly disclosed vulnerabilities even after they've been addressed with security updates, and demonstrates how swiftly testing and applying updates as they are released remains one of the best ways individuals and organizations can protect themselves from attack.

Disclosure and spread

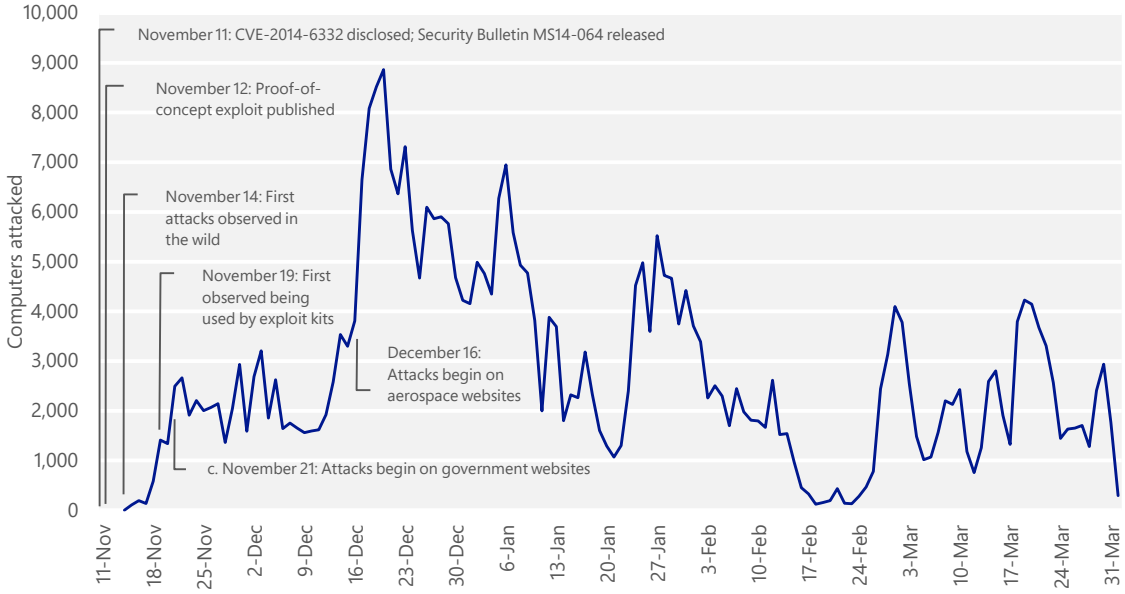
On November 11, 2014, Microsoft released Security Bulletin MS14-064 as part of its regular scheduled monthly security bulletin release (colloquially called "Patch Tuesday.") One of the vulnerabilities addressed by this security bulletin was CVE-2014-6332, a vulnerability in Windows Object Linking and Embedding (OLE) that was privately reported to Microsoft by Robert Freeman of IBM's X-Force security research team. The vulnerability has a CVSS severity score of 9.3 (categorized as "High") and an access complexity score of Medium. (See "Vulnerabilities" beginning on page 13 of the full report for more information about vulnerability severity and complexity.) Although it is not a vulnerability in Internet Explorer, a remote attacker could use Internet Explorer to attempt to exploit CVE-2014-6332 on the computer. (If Internet Explorer is in protected mode, which is enabled by default for Internet websites, the exploit requires that the user grant the Windows-based script host permission to run it in order to succeed.) Applying Security Bulletin MS14-064 resolves the issue.

November 12: Initial proof-of-concept exploit released

The day after the security bulletin was released, November 12, an independent security researcher in China published a fully-weaponized proof-of-concept exploit targeting CVE-2014-6332. This exploit was particularly notable because it was the first one known to make use of an exploitation technique developed and published by several different security researchers earlier in 2014.

Dubbed "God Mode" for its supposed resemblance to a video game cheat code, this technique could be used to bypass most memory mitigations by setting a single byte in the Internet Explorer script engine on a compromised computer. Using this technique, the exploit is capable of bypassing exploit mitigations on most versions of Windows—creating a tempting opportunity for both malware creators and targeted attackers.

Figure 1. Number of computers reporting CVE-2014-6332 exploit attempts each day, November 2014–March 2015



November 14: Watering hole attacks

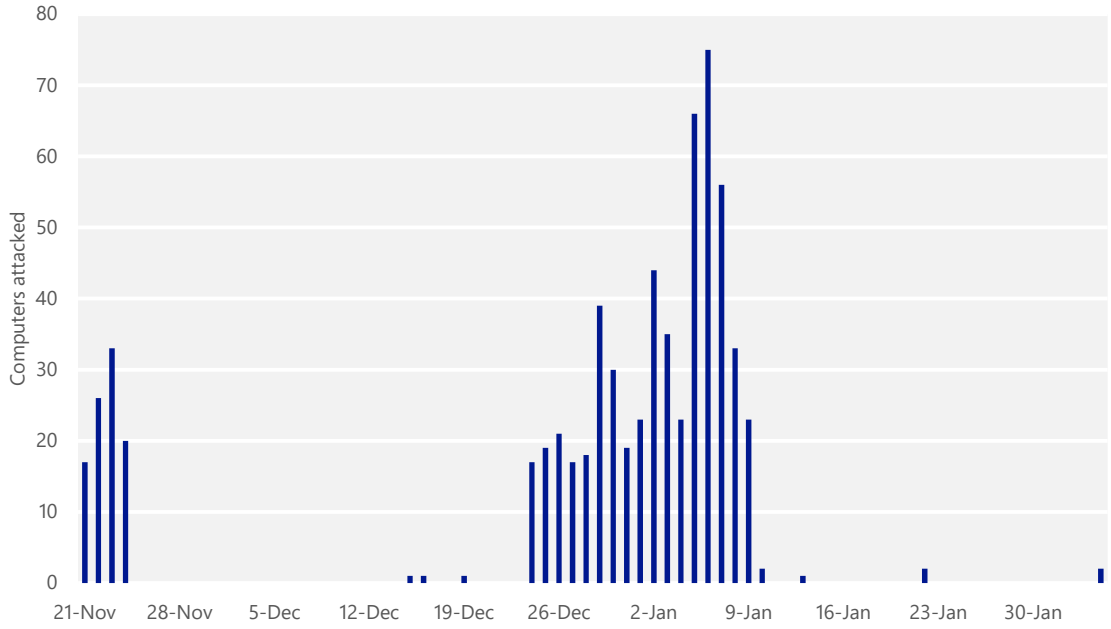
On November 14, Microsoft began receiving data that showed the CVE-2014-6332 vulnerability and exploit being used in the wild. A review of internal telemetry suggested that several active campaigns were using the exploit in *watering hole attacks* that targeted specific industries and demographic groups by compromising websites used in those communities. Targeted groups

included ethnic groups, users of certain government websites, democracy activist organizations, and university-based communities.

Late November: Attacks detected against government and aerospace websites

Microsoft identified an additional targeted attack campaign using CVE-2014-6332 that started in late November with attacks on government websites and spread to aerospace websites the following month. (See page 8 for more information about these attacks.)

Figure 2. Number of computers detected being attacked each day in the campaign against government and aerospace websites, November 2014–February 2015



Late November: CVE-2014-6332 added to exploit kits

CVE-2014-6332 exploits began appearing in exploit kits at around the time of the government website attacks. (See page 25 of the full report for more information on exploit kits.) Figure 3 lists the exploit kits that have been observed to include exploits for CVE-2014-6332.

Figure 3. Exploit kits known to target CVE-2014-6332

Exploit kit	Microsoft primary detection name	Date CVE-2014-6332 exploits first observed
Sweet Orange	Win32/Anogre	2014-11-19
Neutrino	JS/Neutrino	2014-11-20
Archie	Win32/Archost	2014-11-24
Flash	JS/Fashack	2014-12-13
Rig	JS/Meadgive	2014-12-18
Angler	JS/Axpergle	2014-12-27
Fiesta	JS/Fiexp	*Unknown*
Kaixin	JS/DonxRef	*Unknown*
Nuclear	JS/Neclu	*Unknown*
Magnitude	HTML/Pangimop	*Unknown*

The reliability of the CVE-2014-6332 exploit has made it one of the primary tools used by attackers, and Microsoft has observed significant variability in the obfuscation schemes attackers use to package the exploit in an effort to avoid detection by security software.

Analysis of CVE-2014-6332 targeted attacks

The script uses the memory corruption vulnerability to modify the property that normally prevents unsafe ActiveX controls from loading.

The CVE-2014-6332 vulnerability involves a bug in the way the VBScript engine in Internet Explorer handles array resizing. A successful exploit of the vulnerability results in memory corruption and enables the attacker to execute certain actions that VBScript is normally prevented from performing in the browser.[1]

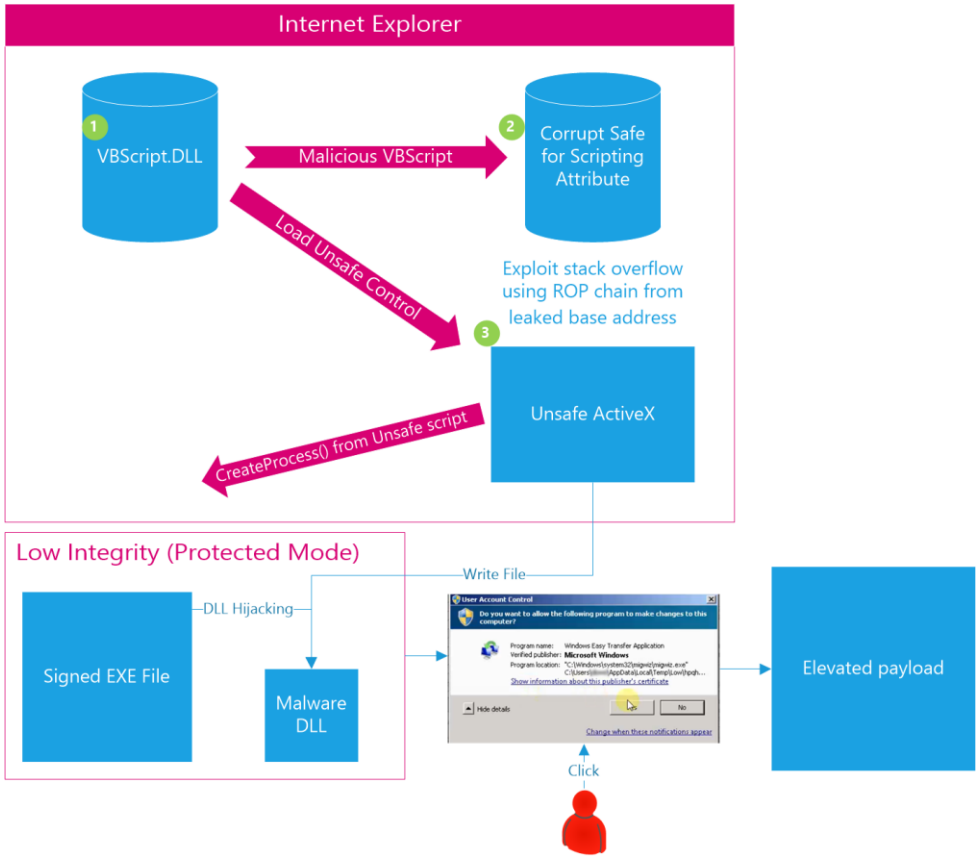
In a typical scenario, the attacker adds a malicious script based on the proof-of-concept code to a compromised webpage. When a user of a vulnerable computer visits the webpage using Internet Explorer, the script uses the memory corruption vulnerability to modify the "Safe for Scripting" property in

[1] Although VBScript is no longer supported in the Internet Explorer 11 document mode, web pages can still be written to use IE5, IE7, IE8, IE9, or IE10 document modes, and the CVE-2014-6332 vulnerability still applies to those document modes. The upcoming Microsoft Edge browser does not use VBScript or binary extensions, and is not susceptible to VBScript vulnerabilities.

memory, which typically prevents unsafe ActiveX controls from loading.

Disabling this property enables the attacker to load the Wscript.Shell ActiveX control in Internet Explorer. This control, which enables certain shell operations in VBScript, typically cannot be loaded by scripts on remote web pages because of the potential for abuse, but exploiting CVE-2014-6332 enables the attacker to bypass this restriction. The attacker can now use Wscript.Shell to perform a number of actions in Windows—including creating and executing files—without having to bypass additional exploit mitigations.

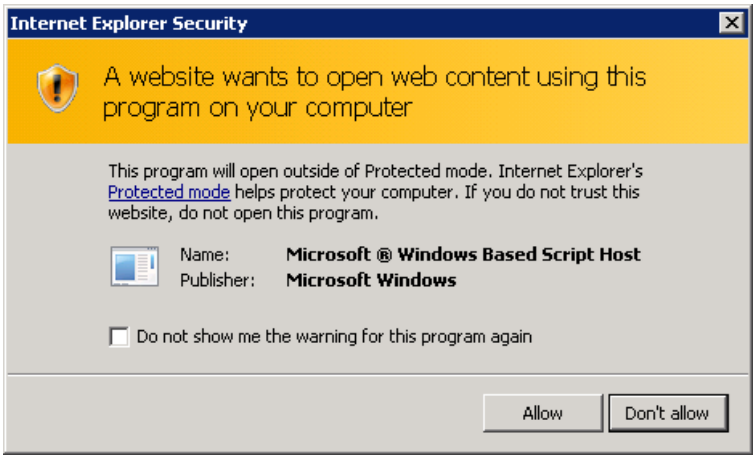
Figure 4. Mechanics of the CVE-2014-6332 exploit



To help improve the attacker's chance of remaining undetected, the exploit writes the payload to an inconspicuous directory on the user's computer, such as C:\ProgramData\Microsoft\Windows\DRM\, and executes the file. Because Internet Explorer's protected mode prevents untrusted webpages from running programs locally, a standard dialog box prompts the user for permission to open the program outside of protected mode. If the user does not grant this permission, the Internet Explorer sandbox prevents the malware from executing.

If the user does grant permission, however, the malware will launch at the user's privilege level, thereby "escaping" the sandbox.

Figure 5. The warning dialog that appears when the exploit attempts to launch from Internet Explorer's protected mode



The malware then attempts to connect to a command & control (C&C) server that security researchers have connected to a known espionage group.[2] A different C&C server observed by Microsoft was used in previous watering hole attacks, and has been connected to a different targeted attack group.[3]

Promptly installing security updates remains one of the best ways to defend against newly discovered threats.

The attack can also be packaged in other ways. In the attack on the government and aerospace websites, the CVE-2014-6332 exploit was repackaged within an Adobe Flash file, possibly in an attempt to avoid detection by security software. Interestingly, the exploit author within this campaign also chose to substitute the original "Safe-for-scripting" attack with an Adobe Flash-based return-oriented programming (ROP) exploit payload. The malicious Flash file used to package the exploit strongly resembles one used in a zero-day exploit distributed on forbes.com at around the same time that targeted CVE-2014-

[2] Gavin O'Gorman and Geoff McDonald, "The Elderwood Project," Symantec Corporation, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf.

[3] Jen Miller-Osborn and Ryan Olsen, "Recent Watering Hole Attacks Attributed to APT Group 'th3bug' Using Poison Ivy," Palo Alto Networks, September 19, 2014, http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/.

9163,[4] a vulnerability in Adobe Flash addressed by Adobe Security Bulletin APSB14-27. The two files share many of the same variable names and display a high degree of code reuse, suggesting that they may have been created by the same malware author, or that the two attacks are connected in some other way.

Guidance: Defending against exploits

The events surrounding the disclosure and exploitation of the CVE-2014-6332 vulnerability demonstrate the risks that computer users worldwide face when updates are not applied quickly and fully working exploits are released to the public. In this case, both targeted attackers and opportunistic criminals quickly took advantage of freely available vulnerability and technique information to infect thousands of unpatched computers by compromising a number of high-profile websites.

In addition, CVE-2014-6332 serves as a reminder that promptly installing all relevant security updates as soon as is practical remains one of the best ways to help defend users and systems against newly discovered threats. Microsoft issued Security Bulletin MS14-064 to address the vulnerability before any exploits targeting the vulnerability were discovered in the wild; computer users and administrators who applied the security update the day it was released faced no risk from any of the subsequently discovered exploits. In fact, most exploit kits rely heavily on vulnerability exploits for which security updates have been available for months or even years—they target computers that do not have the appropriate updates installed, and therefore remain at risk.

Additional steps users can take to reduce their risk from CVE-2014-6332 exploits and others include the following:

- System warnings. Pay close attention to security messages provided by Internet Explorer and Windows. Research has suggested that most successful attacks, such as the one described above, require some user interaction to be successful.
- Antimalware. Most popular antimalware products, including Microsoft Security Essentials, Windows Defender, and System Center Endpoint Protection (SCEP), have updated their signature files to detect and block the exploitation techniques described here. Running real-time security software

[4] Dan Goodin, "Pwned in 7 seconds: Hackers use Flash and IE to target Forbes visitors," *Ars Technica*, February 11, 2015, http://arstechnica.com/security/2015/02/11/pwned-in-7-seconds-hackers-use-flash-and-ie-to-target-forbes-visitors/.

from a reputable vendor and ensuring that its signature files are updated regularly is one of the best ways to defend against exploits and other types of malware.

- Browser. Users should keep their browser updated for the best security protection, and upgrade to the latest version of Internet Explorer to ensure that they will continue receiving security updates. Enabling Enhanced Protected Mode can help prevent exploits and malicious scripts from gaining unauthorized access to other parts of the computer, such as modifying system settings or writing to the Documents folder. Users running 64-bit editions of Windows can also enable 64-bit processes for Enhanced Protected Mode to apply an additional level of security.
- Applications. Whenever possible, use the newest available versions of applications to take advantage of the latest security fixes and improvements.

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