Exploit for CVE-2017-8759 detected and neutralized

Rate this article★★★★★

msft-mmpc (https://social.technet.microsoft.com/profile/msft-mmpc) September 12, 2017

The September 12, 2017 security updates from Microsoft (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8759) include the patch for a previously unknown vulnerability exploited through Microsoft Word as an entry vector. Customers using Microsoft advanced threat solutions were already protected against this threat.

The vulnerability, classified as CVE-2017-8759 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8759), was used in limited targeted attacks and reported to us by our partner, FireEye. Microsoft would like to thank FireEye for responsibly reporting this vulnerability (https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html) and for working with us to protect customers.

Customers receiving automatic updates for Microsoft products are protected from this attack without any additional action required. Customers not enjoying the benefits of automatic updates should consider immediately applying this month's updates to avoid unnecessary exposure.

Office 365 ATP and Windows Defender ATP customers protected

Customers running Microsoft advanced threat solutions such as Office 365 Advanced Threat Protection (https://products.office.com/en-us/exchange/online-email-threat-protection) or Windows Defender Advanced Threat Protection (https://www.microsoft.com/en-us/WindowsForBusiness/windows-atp) were safe from this attack without the need of additional updates. The security configuration and reduced attack surface of Windows 10 S (https://www.microsoft.com/en-us/windows/windows-10-s) blocks this attack by default.

Office 365 ATP (https://products.office.com/en/exchange/online-email-threat-protection) blocked the malicious attachments automatically in customer environments that have adopted the mail detonation and filtering solution. The attachment was blocked based on the detection of the malicious behaviors, as well as its similarity with previous exploits. SecOps personnel would see an ATP behavioral detection in Office 365's Threat Explorer page:

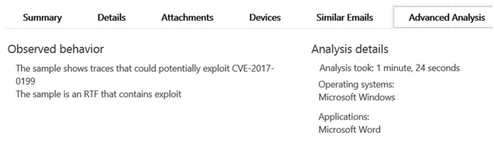

Figure 1. Block reasons for the exploit attachment as seen in Office 365 ATP console

Windows Defender ATP (https://www.microsoft.com/en-us/WindowsForBusiness/windows-atp) was also able to raise multiple alerts related to post-exploitation activities performed by this exploit using scripting engines and PowerShell. Additional alerts may also be visible for subsequent stages of the attack performed after malware installation.

In addition, Windows Defender Antivirus (https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-defender-in-windows-10) detects and blocks exploits for this vulnerability as Exploit:RTF/Fitipol.A, Behavior:Win32/Fitipol.A, and Exploit:RTF/CVE-2017-8759.A using the cloud protection service, which delivers near-real-time protection against such never-before-seen threats.

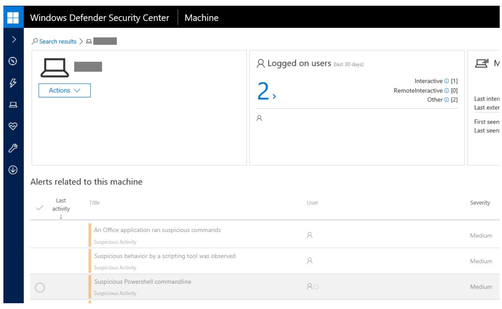

Figure 2. Windows Defender ATP alerts raised for CVE-2017-8759 zero-day exploit

Protection with Windows Defender Exploit Guard

We are also happy to share with customers testing our upcoming Windows 10 Fall Creators Update that Windows Defender Exploit Guard (https://blogs.technet.microsoft.com/mmpc/2017/06/27/whats-new-in-windows-defender-atp-fall-creators-update/) was also able to prevent this attack using one of the many Attack Surface Reduction rules and exploit protection features.

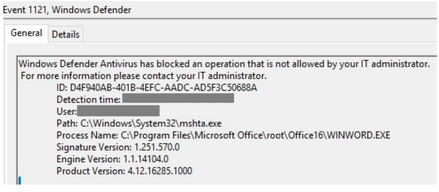

Figure 3. Example of exploit blocking event logged by Windows Defender Exploit Guard

Windows Defender Exploit Guard (https://aka.ms/wdegdocs) is part of the defense-in-depth protection in the Windows 10 Fall Creators Update (https://blogs.windows.com/business/2017/06/27/announcing-end-end-security-features-windows-10/) release.

Another zero-day leading to FinFisher

The CVE-2017-8759 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8759) vulnerability can allow remote code execution after users open a spam email, and double-click on an untrusted attachment and disable the Microsoft Office *Protected View* mode. The exploit uses Microsoft Word as the initial vector to reach the real vulnerable component, which is not related to Microsoft Office and which is responsible for certain SOAP-rendering functionalities through .NET classes.

For more information on this new campaign our partner FireEye has a good technical blog (https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html) describing the infection mechanism and the details of the exploit.

After the initial notification from FireEye, Windows Defender telemetry revealed very limited usage of this zero-day exploit. The attacker used this exploit to deploy a spyware detected as Wingbird (https://www.microsoft.com/en-us/security/portal/threat/encyclopedia/Entry.aspx?Name=Backdoor:Win32/Wingbird.A!dha) and also known to the security community as "FinFisher (https://en.wikipedia.org/wiki/FinFisher)", a commercial surveillance package often seen combined with expensive zero-day vulnerabilities and used by sophisticated actors.

Microsoft researchers believe that the adversary involved in this operation could be linked to the NEODYMIUM group (http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf), which has used similar zero-day exploits with spear-phishing attachments combined with the usage of FinFisher spyware. We previously reported about the NEODYMIUM group in the Windows Security blog (https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/) in 2016. For additional information about this new attack as well as other NEODYMIUM attacks, we encourage ATP customers to review the in-product Threat Intelligence reports on this activity group.

Elia Florio

Follow Us

(https://blogs.technet.microsoft.com/mm

Recent posts

- Exploit for CVE-2017-8759 detected and neutralized (https://blogs.technet.microsoft.com/r for-cve-2017-8759-detected-and-neutralized/)
- Ransomware 1H 2017 review: Global outbreaks reinforce the value of security hygiene (https://blogs.technet.microsoft.com/r 1h-2017-review-global-outbreaks-reinforce-the-value-of-security-hygiene/)
- Microsoft to remove WoSign and StartCom certificates in Windows 10 (https://blogs.technet.microsoft.com/r to-remove-wosign-and-startcom-certificates-in-windows-10/)
- Links in phishing-like emails lead to tech support scam (https://blogs.technet.microsoft.com/r in-phishing-like-emails-lead-to-tech-support-scam/)
- Windows Defender ATP machine learning: Detecting new and unusual breach activity (https://blogs.technet.microsoft.com/r defender-atp-machine-learning-detecting-new-and-unusual-breach-activity/)

Social

@msftmmpc (https://twitter.com/msftmmp

MMPC (https://www.facebook.com/m

Security@Microsoft (https://www.linkedin.com/gr gid=3660709&trk=myg_ugrp_

RSS (http://blogs.technet.com/b/n

Security Newsletter (http://technet.microsoft.com us/security/cc307424.aspx)

About

Windows Security

(https://blogs.technet.microsoft.com/mm

Categories

- Advanced persistent threats (https://blogs.technet.microsoft.com/r (20)
- Cloud protection (https://blogs.technet.microsoft.com/r protection/) (5)
- Device Guard (https://blogs.technet.microsoft.com/r guard/) (1)
- Exploits (https://blogs.technet.microsoft.com/r (13)
- Java malware (https://blogs.technet.microsoft.com/r malware/) (1)
- JavaScript malware (https://blogs.technet.microsoft.com/r (5)
- Macro-based malware (https://blogs.technet.microsoft.com/r malware/) (15)
- Malvertising (https://blogs.technet.microsoft.com/r campaign/) (2)
- Microsoft Edge (https://blogs.technet.microsoft.com/r edge/) (2)
- MSRT (https://blogs.technet.microsoft.com/r (38)
- Objective Criteria (https://blogs.technet.microsoft.com/r criteria/) (19)
- Office (https://blogs.technet.microsoft.com/r (5)
- Office 365 Advanced Threat Protection (https://blogs.technet.microsoft.com/r 365-advanced-threat-protection/) (3)
- Phishing (https://blogs.technet.microsoft.com/r (3)
- PowerShell (https://blogs.technet.microsoft.com/r (1)
- Ransomware (https://blogs.technet.microsoft.com/r (44)
- Rogue (https://blogs.technet.microsoft.com/r (2)
- Spam (https://blogs.technet.microsoft.com/r (13)
- Tech support scam (https://blogs.technet.microsoft.com/r (4)
- Trojan (https://blogs.technet.microsoft.com/r (26)
- Uncategorized (https://blogs.technet.microsoft.com/r (472)
- Unwanted software (https://blogs.technet.microsoft.com/r software/) (22)
- Windows 10 (https://blogs.technet.microsoft.com/r 10/) (39)
- Windows 10 Creators Update (https://blogs.technet.microsoft.com/r update/) (19)
- Windows 10 Fall Creators Update (https://blogs.technet.microsoft.com/r creators-update/) (2)
- Windows 10 S (https://blogs.technet.microsoft.com/r

Windows Defender ATP Research Team

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community (https://answers.microsoft.com/en-us/protect).

Follow us on Twitter @MMPC (https://twitter.com/msftmmpc) and Facebook Microsoft Malware Protection Center (https://www.facebook.com/msftmmpc/)

Tags CVE-2017-8759 (https://blogs.technet.microsoft.com/mmpc/tag/cve-2017-8759/) exploit (https://blogs.technet.microsoft.com/mmpc/tag/exploit/) NEODYMIUM (https://blogs.technet.microsoft.com/mmpc/tag/neodymium/) vulnerability (https://blogs.technet.microsoft.com/mmpc/tag/vulnerability/) Windows Defender Advaned Threat Protection (https://blogs.technet.microsoft.com/mmpc/tag/windows-defender-advaned-threat-protection/) Windows Defender Antivirus (https://blogs.technet.microsoft.com/mmpc/tag/windows-defender-antivirus/) Wingbird (https://blogs.technet.microsoft.com/mmpc/tag/wingbird/) zero-day exploits (https://blogs.technet.microsoft.com/mmpc/tag/zero-day-exploits/)

10-s/) (2)
- Windows Defender ATP (https://blogs.technet.microsoft.com/r defender-atp/) (29)
- Windows Defender AV (https://blogs.technet.microsoft.com/r defender/) (44)
- Windows Defender Security Intelligence (https://blogs.technet.microsoft.com/r (126)
- Windows security product tips (https://blogs.technet.microsoft.com/r (46)
- Windows security technologies (https://blogs.technet.microsoft.com/r (59)
- Worms (https://blogs.technet.microsoft.com/r (4)

Popular Tags

research (https://blogs.technet.microsoft.com/m

MSRT (https://blogs.technet.microsoft.com/m

telemetry (https://blogs.technet.microsoft.com/m

spam (https://blogs.technet.microsoft.com/m

rogue (https://blogs.technet.microsoft.com/m

Windows Defender (https://blogs.technet.microsoft.com/m defender/)

Windows 10 (https://blogs.technet.microsoft.com/m 10/)

ransomware (https://blogs.technet.microsoft.com/m

Windows Defender ATP (https://blogs.technet.microsoft.com/m defender-atp/)

malware research (https://blogs.technet.microsoft.com/m research/)

SIR (https://blogs.technet.microsoft.com/m

MMPC (https://blogs.technet.microsoft.com/m

exploits (https://blogs.technet.microsoft.com/m

guidance (https://blogs.technet.microsoft.com/m

Microsoft Security Essentials (https://blogs.technet.microsoft.com/m security-essentials/)

social engineering (https://blogs.technet.microsoft.com/m engineering/)

conference (https://blogs.technet.microsoft.com/m

Windows Defender Antivirus (https://blogs.technet.microsoft.com/m defender-antivirus/)

malware (https://blogs.technet.microsoft.com/m

Microsoft Edge (https://blogs.technet.microsoft.com/m edge/)

Archives

September 2017 (https://blogs.technet.microsoft.com/mm
August 2017 (https://blogs.technet.microsoft.com/mm
July 2017 (https://blogs.technet.microsoft.com/mm
June 2017 (https://blogs.technet.microsoft.com/mm
May 2017 (https://blogs.technet.microsoft.com/mm
April 2017 (https://blogs.technet.microsoft.com/mm
March 2017 (https://blogs.technet.microsoft.com/mm
February 2017 (https://blogs.technet.microsoft.com/mm
January 2017 (https://blogs.technet.microsoft.com/mm
All of 2017 (https://blogs.technet.microsoft.com/mm
All of 2016 (https://blogs.technet.microsoft.com/mm
All of 2015 (https://blogs.technet.microsoft.com/mm
All of 2014 (https://blogs.technet.microsoft.com/mm
All of 2013 (https://blogs.technet.microsoft.com/mm
All of 2012 (https://blogs.technet.microsoft.com/mm
All of 2011 (https://blogs.technet.microsoft.com/mm
All of 2010 (https://blogs.technet.microsoft.com/mm
All of 2009 (https://blogs.technet.microsoft.com/mm
All of 2008 (https://blogs.technet.microsoft.com/mm