September 12, 2017

Exploit for CVE-2017-8759 detected and neutralized

Microsoft Defender ATP Research Team

The September 12, 2017 security updates from Microsoft 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, 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 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 or Windows Defender Advanced Threat Protection were safe from this attack without the need of additional updates. The security configuration and reduced attack surface of Windows 10 S blocks this attack by default.

Office 365 ATP 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:

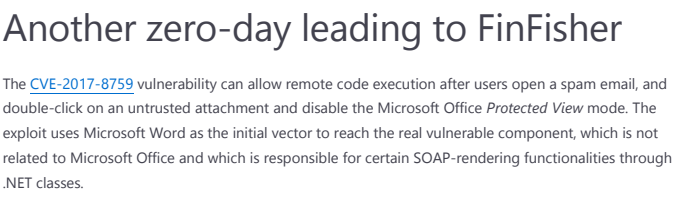

Figure 1. Block reasons for the exploit attachment as seen in Office 365 ATP console

Windows Defender ATP 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.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

In addition, Windows Defender Antivirus 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.

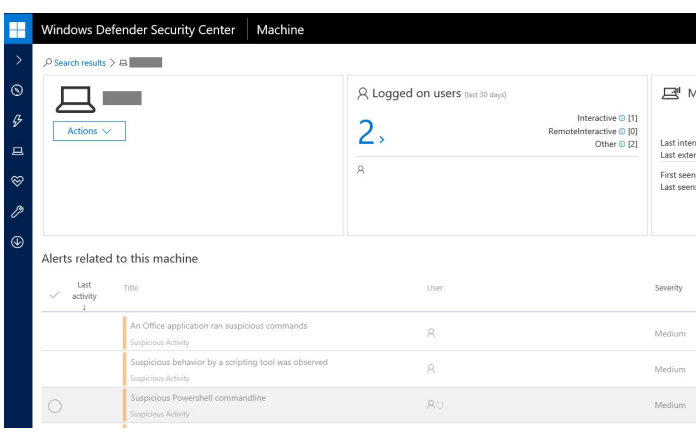

Figure 2. Windows Defender ATP alerts raised for CVE-2017-8759 zero-day exploit

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 was also able to prevent this attack using one of the many Attack Surface Reduction rules and exploit protection features.

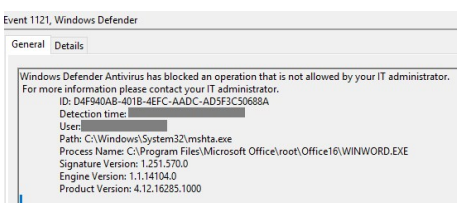

Figure 3. Example of exploit blocking event logged by Windows Defender Exploit Guard

Windows Defender Exploit Guard is part of the defense-in-depth protection in the Windows 10 Fall Creators Update release.

Another zero-day leading to FinFisher

The 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 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 and also known to the security community as "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, 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 in 2016. For additional information about this new attack as well as other NEODYMIUM attacks, we encourage Windows Defender ATP customers to review the in-product Threat Intelligence reports on this activity group.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

Elia Florio

Windows Defender ATP Research Team

Related blog posts

Office 365 Advanced Threat Protection defense for corporate networks against recent Office exploit attacks

Twin zero-day attacks: PROMETHIUM and NEODYMIUM target individuals in Europe

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.

Follow us on Twitter @WDSecurity and Facebook Windows Defender Security Intelligence.

Filed under:

Cybersecurity, Security Response, Zero Trust

You may also like these articles

Welcoming more women into cybersecurity: the power of mentorships
Read more ›

Secured-core PCs: A brief showcase of chip-to-cloud security against kernel attacks
Read more ›

Behavioral blocking and containment: Transforming optics into protection
Read more ›