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

blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

December 14, 2016

Targeted attacks are typically carried out against individuals to obtain intellectual property and other valuable data from target organizations. These individuals are either directly in possession of the targeted information or are able to connect to networks where the information resides. Microsoft researchers have encountered twin threat activity groups that appear to target individuals for reasons that are quite uncommon.

Unlike many activity groups, which typically gather information for monetary gain or economic espionage, PROMETHIUM and NEODYMIUM appear to launch campaigns simply to gather information about certain individuals. These activity groups are also unusual in that they use the same zero-day exploit to launch attacks at around the same time in the same region. Their targets, however, appear to be individuals that do not share common affiliations.

Activity group profiles

PROMETHIUM is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.

NEODYMIUM is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor's characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.

Similarly timed attacks

In early May 2016, both PROMETHIUM and NEODYMIUM started conducting attack campaigns against specific individuals in Europe. They both used an exploit for CVE-2016-4117, a vulnerability in Adobe Flash Player that, at the time, was both unknown and unpatched.

PROMETHIUM distributed links through instant messengers, pointing recipients to malicious documents that invoked the exploit code to launch Truvasys on victim computers. Meanwhile, NEODYMIUM used well-tailored spear-phishing emails with attachments that delivered the exploit code, ultimately leading to Wingbird's installation on victim computers.

While the use of the same exploit code could be attributed to coincidence, the timing of the campaigns and the geographic location of victims lend credence to the theory that the campaigns are somehow related.

Stopping exploits in Windows 10

PROMETHIUM and NEODYMIUM both used a zero-day exploit that executed code to download a malicious payload. Protected view, a security feature introduced in Microsoft Office 2010, can prevent the malicious Flash code from loading when the document is opened. Control Flow Guard, a security feature that is turned on by default in Windows 10 and Microsoft Office 365 64-bit, can stop attempts to exploit memory corruption vulnerabilities. In addition, Credential Guard, an optional feature introduced in Windows 10, can stop Wingbird's use of the system file, *lsass.exe*, to load a malicious DLL.

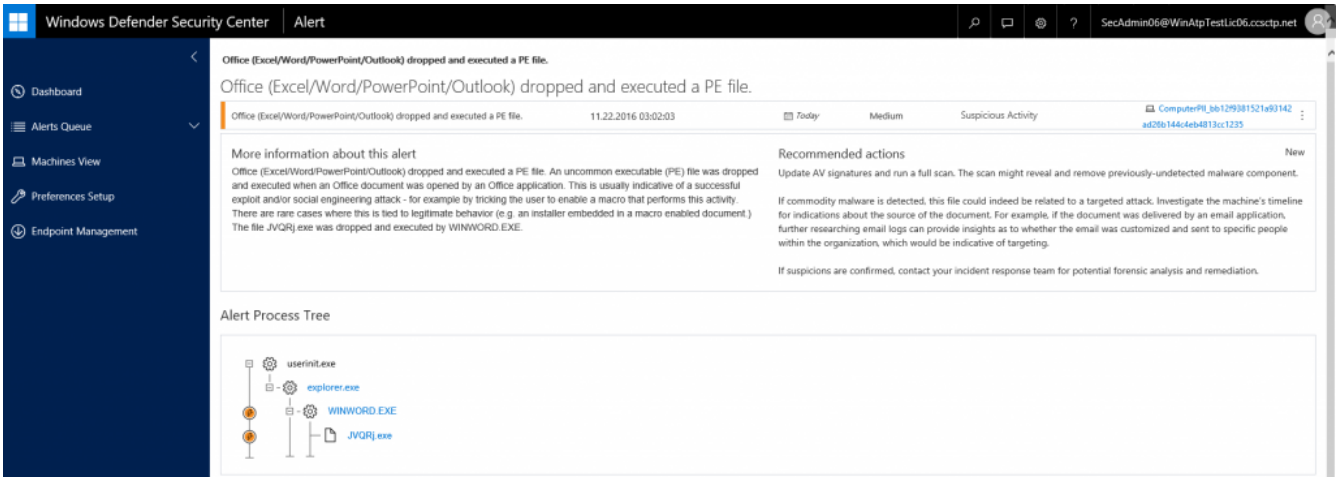
Detecting suspicious behaviors with Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection (Windows Defender ATP) is a new built-in service that ships natively with Windows 10 and helps enterprises to detect, investigate and respond to advanced targeted attacks. When activated, it captures behavioral signals from endpoints and then uses cloud-based machine learning analytics and threat intelligence to flag attack-related activities.

Wingbird, the advanced malware used by NEODYMIUM, has several behaviors that trigger alerts in Windows Defender ATP. Windows Defender ATP has multiple behavioral and machine learning detection rules that can catch various elements of the malware kill chain. As a result, it can generically detect, without any signature, a NEODYMIUM attack in the following stages:

- Zero-day exploits causing Microsoft Office to generate and execute malicious files
- Zero-day exploits attempting to grant malicious executables higher privileges
- Malicious files trying to delete themselves
- Malicious files attempting the DLL side-loading technique, in which legitimate DLLs in non-standard folders are replaced by malicious ones so that malicious files are loaded by the operating system or by installed applications
- Malicious files injecting code into legitimate processes

In the example below, Windows Defender ATP alerts administrators that something is amiss. It notifies them that an Office document has dropped an executable file in one of their computers—activity that is very likely part of an attack.



Additionally, Windows Defender ATP and Office 365 ATP leverage rules based on IOCs and threat intelligence specific to PROMETHIUM and NEODYMIUM. Alerts from these rules work alongside concise briefs and in-depth profiles provided in the Windows Defender ATP console to help administrators address breach attempts by these activity groups.

For more information about Windows Defender ATP service in Windows 10, check out its features and capabilities and read more about why a post-breach detection approach is a key component of any enterprise security stack.

Details about PROMETHIUM and NEODYMIUM along with indicators of compromise can be found in the Microsoft Security Intelligence Report volume 21.

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

Windows Defender ATP team

Talk to us

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