CERT-EU Security Advisory 2017-014

Petya-Like Malware Campaign

June 29, 2017 — v1.1

History:

- *28/06/2017 — v1.0: Initial publication*
- *29/06/2017 — v1.1: Some corrections and new information about wiping capability*

Summary

A large malware campaign broke out on Tuesday, 27/06/2017 and was widely reported in the news. The malware used – which appears to be similar to *Petya* – has been augmented with efficient local network spreading mechanisms, which resulted in a very rapid infection rate inside affected organizations. The local propagation is apparently achieved by a combination of the use of *EternalBlue* (the same exploit as the one used by *WannaCry* earlier), *EternalRomance* [8], and WMIC/`psexec` propagation vector using credentials harvested with a code similar to *Mimikatz* [1, 2].

First analysis [3, 4, 8] points to at least one likely infection vector being associated with software update systems for a Ukrainian tax accounting package called *MeDoc*. However, as among the impacted organizations there were those that did not use the software, it is likely that other infection vectors are also used. There are some reports of a watering-hole-type infection vector as well [10].

What initially looked like a fairly regular – although large – ransomware campaign, the specific targeting of Ukraine and additional disk wiping behavior detected [9, 11], indicate that money extortion was probably not the main objective of the campaign.

Technical Details

Infection Vector

Multiple sources [3, 4, 8] point to the infection vector being an infected software update system for a Ukrainian tax accounting package called *MeDoc*. Some details were provided by the Ukrainian Police on Twitter [4] (translated to English):

This software has a built-in update feature, which periodically accesses the server `http://upd.me-doc.com.ua` *with the help of the User Agent* `medoc1001189`*. The update has a hash:*

`dba9b41462c835a4c52f705e88ea0671f4c72761893ffad79b8348f57e84ba54`

Most legitimate pings *(hits to the server) are approximately 300 bytes. 27/06/2017 at 10:30, program* `M.E.doc.` *Was updated, which was approximately 333kb. After loading it, the following actions were taken:*

- *a file created:* `rundll32.exe`*;*
- *access to local IP addresses on TCP port 139 and TCP port 445;*
- *create a file:* `perfc.bat`*;*[1]
- *run* `cmd.exe` *with the following command:*

```
/c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TRCC:\Windows\system32_shutdown.exe /r /f "/ST 14:35"
```

- *another file created:* `ac3.tmp` *(* `02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f` *) and its subsequent launch.*

These details explain the observations that first infections were reported in Ukraine, and many of the companies affected worldwide had their branches in that country. Infected machines in Ukraine could then use the local network propagation mechanisms to reach across borders. Later, Kaspersky claimed that the malware had been also distributed as a watering-hole attack from `bahmut.com.us/news` [10]. There however no firm technical details related to this information.

Local Network Propagation

Once a machine is infected, malware will start attempting to spread in the local network. The malware checks if it runs on a Domain Controller (DC). If yes, than it will only scan the machines that were served IPs using DHCP [2, 8]. If the infected machine is regular one, it appears that the /24 network segment is being scanned by the malware (ports 445 and 139). Once open ports are identified, at least three separate mechanisms are used to infect other machines:

- SMB exploit *EternalBlue* – the same one used earlier by *WannaCry* – and *EternalRomance* [8],
- `psexec` for remote command execution,
- WMIC (Windows Management Instrumentation Command-Line).

EternalBlue is tried first and since the *modus operandi* is exactly the same as in case of *WannaCry*, no further details are provided in this advisory. Interested readers should refer to CERT-EU Security Advisory 2017-012. Additionally, also *EternalRomance* is tried [8]. If the system is patched for these vulnerabilities, the remaining two methods are used.

The other methods utilized are more original, although based on well-known techniques. First malware uses password dumping tools similar to *Mimikatz* [1, 2, 3, 8] to harvest credentials on the infected machine. It looks in particular for local administrator credentials. The credentials obtained are then used for remote process execution on other machines in the local network using WMI/`psexec`. The following command is used with `psexec` [3] (where `w.x.y.z` is the target IP address):

```
C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe
  C:\Windows\perfc.dat,#1
```

and the following one using WMI [3] (where `w.x.y.z` is the target IP address, and `username` / `password` are the harvested credentials):

```
Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create
  "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1"
```

[1] Please note that most sources indicate that the file name is in fact `perfc.dat` – the Ukrainian Police may have made a typo in their tweet.

Encryption Process

The malware tries to obtain administrative privileges (`SeShutdowPrivilege` and `SeDebugPrivilege`) for the current user through the Windows API `AdjustTokenPrivileges` . If successful, the ransomware will overwrite the master boot record (MBR) on the disk drive referred to as `PhysicalDrive 0` within Windows [3].

Once the malware is installed, it sets a timer for at least 10 min in the future (exact time is random) [8] to reboot the system. It appears that no data is effectively encrypted until the reboot. The malware however clears event logs using the following command [3]:

```
wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application &
  fsutil usn deletejournal /D %c:
```

Once rebooted, the malware boots from the modified MBR and shows a fake CHKDSK message [1, 6]. This message is shown during the encryption process – **if the machine is powered-down immediately, there is still a chance to recover some files before they are encrypted**. However, once a ransom message is shown [7], the files have been effectively encrypted.

Petya uses AES-128 with RSA, and a hardcoded static RSA public key. As there has been only one sample identified so far, all of the infections share the same RSA key. The AES key is randomly generated, used for the encryption, and then encrypted with the RSA key and stored in the `README.TXT` file on disk [12]. The validity of the data in this file has not been however confirmed – i.e., it is not certain that it is enough to decrypt the data even with access to the RSA private key.

Another information is than shown as a screen message [13]. This is the information that – according to the content of the message – the victim needs to provide to the attackers after paying the ransom to obtain the decryption key. However, it is interesting to notice that the value in the file [12] differs significantly from the value in the note [13]. Furthermore, it has been shown in [9] that the value shown on screen in fact is just **randomly generated** and has **nothing to do with the actual encryption key**.

Additionally, it has been recently established that the malware performs additional wiping of the first 25 sectors of the disk [11]. While the first sector (MBR) is overwritten to change the boot process (and saved elsewhere) the other 24 sectors are effectively deleted. Together the random value shown in the ransom message, **the attack seems much more to be intentionally destructive and only posing as ransomware**.

Finally, the e-mail account used to send the information about the payments has now been blocked by the provider, so there is not even a way to inform the threat actors about the payment made. All these indicate that not only there is no hope of being able to decrypt the encrypted files, but there was never even the intention to make it possible.

Kill Switch

Some researchers reported an existence of a **local** *kill switch* [1, 2]. The kill switch found is in the form of a local file that can be created on the potentially targeted system. The file should be put in `C:\WINDOWS` directory and should be named the same as the malicious library served, but without an extension. In the observed cases, the name is `perfc` . Once the malware runs, it checks for the presence of this file and stops execution in case it finds it.

There are however several issues with the way this kill switch works comparing for instance to the kill switch in case of *WannaCry*. While the *WannaCry* kill switch could have been used randomly, the local kill switch for *Petya* requires the file to be created *ahead of time* on *every* machine that could be potentially targeted. Additionally, the file name needs to be identical to the malicious library being served, which may not always be foreseen. While in observed cases, the name was always the same, it is trivial to change it in the future.

Products Affected

Majority of the infected systems are running Windows 7. The exact patch level is currently not known. Some articles – e.g., [8] indicate that Windows 10 was also impacted. There is however no definite list of impacted systems available.

Recommendations

If affected – do not pay ransom. There is currently no way to provide the threat actors with the information needed to generate the decryption key as the e-mail account used for this purpose has been closed, and the information provided by the attackers in the first place seems misleading and unusable [9]. Also, the campaign does not really seem to be focusing on money extortion, but mostly on creating chaos and destruction [9, 11], and hence the threat actors are most likely not interested in providing the decryption keys.

While it is potentially possible to use the kill switch to prevent infections, it is not very easy nor practical. Furthermore, based on the analysis of the situation, the most probably scenario for this campaign was that multiple organizations were infected simultaneously (through the MeDoc software update or using other means) and then the infection spread very quickly within these organizations. There do not appear to be new cases reported. Considering the behavior and the design of the malware – aiming at creating as much chaos and confusion rather than trying to actually extort payments – and its regional targeting – it was aimed quite specifically at Ukraine, the risk of new, identical infections is low at the moment.

While this campaign does not appear to be aiming at CERT-EU constituents, similarly to previous cases – once certain methods prove to be efficient and successful, they will most likely be re-used by other threat actors for various purposes. Hence, it is very important to implement measures that would make such attacks ineffective, and in particular:

- patching systems to avoid exploiting known vulnerabilities during the initial infection (e.g., through spear-phishing),
- ensuring good security policy preventing users from being able to elevate their privileges,
- preventing machine-to-machine connections in the local network, unless specifically necessary,
- not re-using the same local administrator passwords throughout many systems.

Some additional specific Microsoft recommendations are discussed also in [8], and specific Snort rules that may help detect/block some activities related to this type of attack have been developed by Talos in [3].

References

[1] https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html

[2] https://securingtomorrow.mcafee.com/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire/

[3] http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

[4] https://twitter.com/CyberpoliceUA/status/879772963658235904

[5] https://twitter.com/0xAmit

[6] https://zerobin.no/?f4aa14963a899169#79zg8l0TZRNJlm8diIjxAbe9ixRnT+x6NhTFjRh+ie0=

[7] https://zerobin.no/?b9c8e4a70311386d#yHG/QlLk3/3A8waWoW+Bws/1lVsBoBrxI8LzXbT1HaA=

[8] https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

[9] https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

[10] https://twitter.com/craiu/status/880011103161524224

[11] https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b

[12] https://msdnshared.blob.core.windows.net/media/2017/06/petya-readme.png

[13] https://msdnshared.blob.core.windows.net/media/2017/06/petya-ransom-note.png