Advanced Notification of Cyber Threats against Microsoft Exchange Servers

Security Advisory	ADV-19-21	**Criticality**	High	
Advisory Released On	16 May 2019			

Impact

Exploiting the vulnerability allows hackers to have full control over everything that passes through the compromised mail server, such as editing the contents of the incoming and outgoing emails, intercepting and redirecting emails.

Attacker Profile

Turla is an advanced persistent threat group which is also known as Waterbug, VENOMOUS BEAR, Snake, WhiteBear, and Kypton. They are known or their high-profile attacks and advanced custom tools. In addition to, over the past eleven years they have been responsible for tremendous high-profile breaches.

Solution

Adhere the advices written under the recommendations section.

Affected Platforms:

- Microsoft Exchange Mail Servers

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a critical malware known as LightNeuron which creates a backdoor within Microsoft Exchange servers. The backdoor serves as a Mail Transfer Agent (MTA), and, according to researchers, is the first malware specifically designed to target Microsoft Exchange servers in many aspects such as, spying on all emails through the exchange server, and modifying or blocking any emails. As well as, executing hidden commands sent by email in the form of PDF or JPG using steganography.

Details

LightNeuron is a complex malware designed to target Microsoft Exchange servers. And it has two aspects: the first is to spy on emails while the other side is to act as a backdoor. The malware is unique in the sense that it leverages a Microsoft Exchange Transport Agent for persistence. Furthermore, the few cases that have been studied have shown that LightNeuron runs with SYSTEM privileges. Described below are the two methods that the malware leverage.

1) Mail Transfer Agent (MTA)

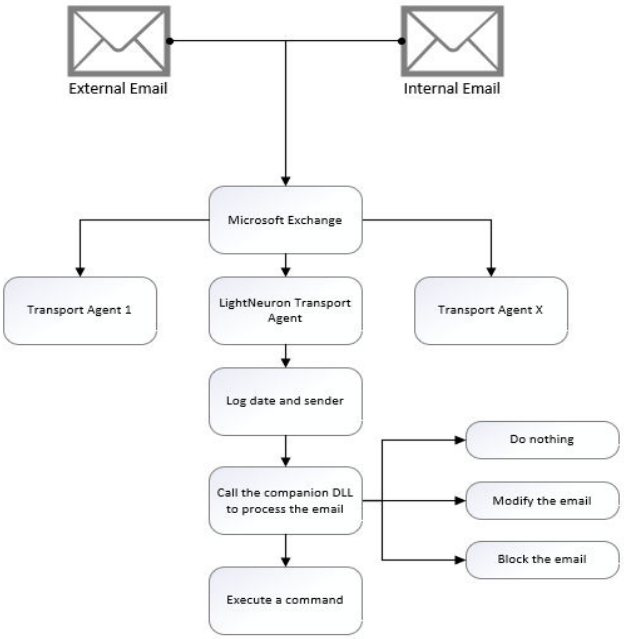
LightNeuron, employing a Transport Agent method, functions at the same trust level as security products. Initially, it starts by leveraging the Transport Agent accesses, after which it gains the capability to execute the following actions on behalf of the targets:

- Compose and send new emails.
- Read and modify any emails passing through the server.
- Block any email; in this case the original recipient would not receive the email.

This is possible due to the flexibility of modifying the XML rule file after leveraging the MTA access. For each victim, a customized file of rules been created embedded with list of handlers implemented by LightNeuron including things like changeBody, changeTo, changeSubject and etc.

The XML rules use emails that are customized for each victim; this is to target the most interesting people. The rules end with a list of handlers implemented by LightNeuron that are used to process the emails.

The following flowchart summarizes how LightNeuron functions:



2) Backdoor

The command handler for the backdoor Is unlike the one used for email modification; it is a backdoor that is controlled by emails, and uses instruction codes, with the commands hidden using steganography in the form of a specially crafted PDF document or JPG image. Some of the instruction codes, along with a brief description, are as follows:

0x01 – Write an executable. Execute it if it is an executable.
0x02 – Delete a file
0x04 – Execute a process (CreateProcess)
0x07 – Disable backdoor for x minutes

Once an email is discovered to be a command email, the command is executed and the email is thus blocked directly on the Exchange server. As such, the original recipient would not be able to view the email.

IOC

A list of the indicators of compromise are as follows:

Hashes

SHA-1 hash	ESET Detection Name
3C851E239FBF67A03E0DAE8F63EEE702B330DB6C	MSIL/Turla.A
76EE1802A6C920CBEB3A1053A4EC03C71B7E46F8	Win64/Turla.CC
FF28B53B55BC77A5B4626F9DB856E67AC598C787	MSIL/Turla.A
C1FF6804FDB8656AB08928D187837D28060A552F	Win64/Turla.CC
F9D52BB5A30B42FC2D1763BE586CEE8A57424732	MSIL/Turla.A
0A9F10925AF42DF94925D07112F303D57392C908	Win64/Turla.CC
A4D1A34FE5EFFD90CCB6897679586DDC07FBC5CD	MSIL/Turla.A

Filenames

- %tmp%\winmail.dat
- C:\Windows\ServiceProfiles\NetworkService\appdata\Local\Temp\msmocf.xml
- C:\Windows\ServiceProfiles\NetworkService\appdata\Local\Temp\msmodl.dat
- C:\Windows\serviceprofiles\networkservice\appdata\Roaming\Microsoft\Windows\814ad43-58ab-2cd3-3e68-b82a8f402fd0
- C:\Windows\serviceprofiles\networkservice\appdata\Roaming\Microsoft\Windows\42cf8a1-6e20-8c24-d35f-82c46d8b70ba
- C:\Windows\serviceprofiles\networkservice\appdata\Roaming\Microsoft\Windows\36b1f4a-82b9-eb06-7c1e-90b4b2d5c27d
- C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\thumbcache_idx.db
- C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\Windows\thumbcache_32.db

Recommendations

In order to circumvent the exploit, we highly recommend the following:

- Create dedicated accounts for the administration of Exchange servers with strong unique passwords.
- Frequently monitor the usage of these accounts
- Restrict PowerShell execution.
- Check if all the installed Transport Agents are signed by a trusted provider.

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

We Live Security - Turla LightNeuron: An email too far

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