AL2023_20 Chinese hacking group seen using new backdoor malware (March 17, 2023)

Description

A cyber espionage group known as Mustang Panda has released a new custom backdoor malware that uses the MQTT protocol for its communication.

Details

The new malware, dubbed MQsTTang, is the new backdoor that is a part of an ongoing campaign that has been attributed to the Mustang Panda group based on the following indicators. A MQsTTang sample was found in GitHub repositories belonging to 'YanNaingOo0072022', who was seen active in a previous Mustang Panda campaign in December 2022. Researchers also founded an FTP server used by MQsTTang with a directory that contains multiple Korplug loaders and tools used in previous Mustang Panda campaigns.

The campaign was seen targeting unknown entities in Bulgaria, Australia and Taiwan. Also due to the filenames of the decoys used by the campaign, it is believed that political and governmental organizations in Europe and Asia are also being targeted.

The malware is a backdoor that allows attackers to execute commands on a victim's device. It does not use any kinds of obfuscation techniques and only has a single infection stage. The initial stage starts with the distribution of the malware through spearfishing emails, containing RAR archives with only a single executable file. The executables are given names that are diplomacy related such as embassy notes, scans of passports of members, etc. After compromising a device, the malware uses the 'CreateToolhelp32Snapshot' Windows API function to check the currently running processes for known debuggers and monitoring tools such as procmon.exe, pestudio.exe, fiddler.exe, x64dbg.exe, tcpview.exe, etc. It also uses the 'FindWindowW' Windows API function to search for Window Classes and Titles used by common analysis tools such as PROCMON_WINDOW_CLASS, OLLYDBG, WinDbgFrameClass, OllyDbg – [CPU] and Immunity Debugger – [CPU].

When executed, MQsTTang launches a copy of itself with a '1' command line argument. This clone process repeated with the argument incremented by '1' on

every run. Specific arguments are tied to specific tasks, for example if the executable is launched and reaches the command line '5', it establishes a C2 communication. The list of tasks and its command line argument are listed below:

Task number	Argument value	Task description
1	**5**	Start C&C communication.
2	**9**	Create copy and launch.
3	**32**	Create persistence copy.
4	**119**	Establish persistence.
5	**148**	Stop recursive execution.

MQsTTang uses the MQTT protocol for its C2 communication. MQTT is a standard messaging protocol used by IoT devices and are used in a wide variety of industries such as automotive, manufacturing, telecommunications, oil and gas, etc. Because MQTT communication uses a broker to receive and send messages, attackers can hide malicious communication, making it harder to detect and as such a compromised device never communicates directly with the C2 server. The MQsTTang uses the IP address '3.228.54.173' as its broker, which is a public broker operated by EMQX.

MQsTTang establishes persistence by creating a new value under the HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key. This will cause the malware to be executed on startup with a '5' argument value, meaning that the C2 communication is established.

Indicators of Compromise

For a list of SHA-1 hashes and IP addresses associated with MQsTTang, following the link below:

https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/

Remediation

To have a better chance at combating a backdoor malware like MQsTTang, we recommend the following:

1. Raise awareness of these types of attacks - Educate users of backdoors and how they work and the impacts of such malware. Follow this URL to learn more: https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/

2. Use an advanced antivirus solution - Having a proper antivirus solution may help to detect the malware before it attempts to compromise or after it may have compromised your device and help to eliminate it.
3. Be wary of phishing emails and emails containing suspicious attachments - In the case with MQsTTang, it is spread through malicious attachments in emails, therefore it is recommended to scan all attachments from emails before opening them and discard of any suspicious emails.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2023, March 2). *Chinese hackers use new custom backdoor to evade detection*. Retrieved from the BleepingComputer. https://www.bleepingcomputer.com/news/security/chinese-hackers-use-new-custom-backdoor-to-evade-detection/
- Cyr, A. (2023, March 2). *MQsTTang: Mustang Panda's latest backdoor treads new ground with Qt and MQTT*. Retrieved from welivesecurity by ESET. https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/