MITRE-ID: G0017

Name: DragonOK

Country: China

Description:

DragonOK is a threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, DragonOK is thought to have a direct or indirect relationship with the threat group Moafee. It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT.

TTPs:

1. Attacker sent user emails with attachment including the malware.
2. Attacker set the icon of the attachment files looking like a normal office use document to trick user to open it.
3. The group uses HTTP to communicate with the command-and-control server.
4. The group is known for deploying a range of sophisticated malware.
5. The group modifies the registry key to run malware when the computer starts.
6. The group store a key to use to decrypt the data during network communication.
7. The group will detect and download the key file and encrypt network communication.
8. The group uses remote server to instruct malware to execute some commonds.
9. The group uses PlugX backdoor and disguises itself as a product from Symantec.
10. The malware will install itself as a computer service and run after the computer starts by modifying the registry.
11. The FormerFirstRAT are used to transfer unencrypted HTTP over port 443.

Reference:

https://unit42.paloaltonetworks.com/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/