Hive Pro

THREAT ADVISORY

New Threat Actor using Serpent Backdoor attacking French Entities	TA2022072

Threat Level	RED	Publish Date – Mar 22, 2022

Threat actors are using a new backdoor called **Serpent** through macro-enabled Microsoft Word documents attacking French entities in sectors such as construction and government. Using this backdoor the attacker could potentially enable remote administration, command & control (C2), data theft or even deliver other additional payloads.

The threat actor targets organizations using phishing mails attached with a macro-enabled Microsoft Word document masquerading as information relating to the European Union's General Data Protection Regulations (GDPR). Once the macros are enabled in the Microsoft Word, it executes a PowerShell script hidden in an image. The PowerShell script downloads, installs, and updates the **Chocolatey** installer package and repository script. Now Chocolatey installs Python including several packages and dependencies. Another image file encoded with a Python script is downloaded and saves the Python file as **MicrosoftSecurityUpdate.py**. The script then creates and executes a .bat file that in turn executes the Python script. The attack chain ends with a command to a shortened URL which redirects to the Microsoft Office help website.

The MITRE TTPs commonly seen are:
TA0011: Command and Control
TA0003: Persistence
TA0009: Collection
TA0005: Defense Evasion
T1027: Obfuscated Files or Information
T1070: Indicator Removal on Host
T1090: Proxy
T1137: Office Application Startup
T1213: Data from Information Repositories
T1573: Encrypted Channel

Indicators of Compromise (IoCs)

Type	Value
URL	http://ggfwk7yj5hus3ujdls5bjza4apkpfw5bjqbq4j6rixlogylr5x67dmid[.]onion[.]pet/index[.]html, http://mhocujuh3h6fek7k4efpxo5teyigezqkpixkbvc2mzaaprmusze6icqd[.]onion[.]pet/index[.]html, https://www[.]fhccu[.]com/images/ship3[.]jpg, https://www[.]fhccu[.]com/images/7[.]jpg, http://shorturl[.]at/qzES8
SHA-256	f988e252551fe83b5fc3749e1d844c31fad60be0c25e546c80dbb9923e03eaf2, ec8c8c44eae3360be03e88a4bc7bb03f3de8d0a298bff7250941776fcea9faab, 8912f7255b8f091e90083e584709cf0c69a9b55e09587f5927c9ac39447d6a19

References

https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain