vb2023 LONDON

4 - 6 October, 2023 / London, United Kingdom

TURLA AND SANDWORM COME FILELESSLY

Alexander Adamov

NioGuard Security Lab, Sweden

ada@nioguard.com

ABSTRACT

In July 2023, CERT-UA [1] and *Microsoft* [2] reported Turla's attack against the defence sector of Ukraine, where a new .NET backdoor called CAPIBAR (called DeliveryCheck by *Microsoft*, GAMEDAY by *Mandiant*) had been launched using fileless execution techniques. These include, for instance, loading the .NET backdoor by the PowerShell script stored in the Managed Object Format (MOF) file [2].

A year prior to that, another Russian intelligence group, Sandworm, also used a reflective DLL injection technique (T1620) [3], within the WhisperGate operation [4], to load a .NET DLL into the memory. This later writes WhisperGate's file wiper into *Microsoft*'s 'InstallUtil.exe' process [5] with the help of a process hollowing technique (T1055.012) [6].

Moreover, according to *Microsoft*'s recently published taxonomy of fileless threats [7], writing to MBR is also considered a fileless threat. Thus, another WhisperGate disk wiper that was written to the MBR on 13 January 2022 can be also seen as an example of a fileless attack [6].

Whereas *Microsoft* stated that fileless threats can be mitigated with the Anti-Malware Scan Interface (AMSI), behaviour monitoring, memory scanning, boot sector protection, and even machine learning [8], we still see fileless techniques being used by state-owned hacking groups nowadays.

In this talk, we will present the detailed analysis of fileless malware execution techniques employed by Russian intelligence groups (Turla and Sandworm) in operations against the government services and defence sector of Ukraine, as well as the rationale behind the usage of such techniques.

REFERENCES

[1] CERT-UA. Targeted Turla attacks (UAC-0024, UAC-0003) using CAPIBAR and KAZUAR malware (CERT-UA#6981). 18 July 2023. https://cert.gov.ua/article/5213167.

[2] https://twitter.com/MsftSecIntel/status/1681695399084539908.

[3] Reflective Code Loading: https://attack.mitre.org/techniques/T1620/.

[4] Microsoft. Destructive malware targeting Ukrainian organizations. 15 January 2022. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

[5] Microsoft. Installutil.exe (Installer Tool). https://learn.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool.

[6] NioGuard Security Lab. Analysis of WhisperGate. 26 January 2022. https://www.nioguard.com/2022/01/analysis-of-whispergate.html.

[7] Microsoft. Microsoft 365 Defender. https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/fileless-threats.

[8] Microsoft. Microsoft 365 Defender. https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/fileless-threats?view=o365-worldwide#defeating-fileless-malware.

(This is a last-minute presentation; no paper available.)