Written by Marco Attard
11 July 2019

The Microsoft Defender Advanced Threat Protection (ATP) team tells all about Astaroth, a particularly sneaky strain of malware with a fileless nature making it particularly difficult to detect.

Named after no one other than the Great Duke of Hell, Astaroth has been in circulation around S. America and Europe since at least late 2017. It is used to steal sensitive data via phishing attacks launched through spear-phishing. That sounds typical enough, but Astaroth is uniquely nasty since it does not need to install an executable on the target machine. As Microsoft puts it, Astaroth "lives off the land," running legitimate system tools through a complex attack chain involving multiple steps and various fileless techniques.

How does an Astaroth attack take place? Typically, a user opens a malicious link in a spear-phishing email leading to a .LNK file. If the file is opened, the WMIC tool is executed with the "/Format" parameter allowing the downloading and execution of a JavaScript code. In turn, the JavaScript pulls and runs two DLL files able to log and upload victim information, all while disguised as a system process. The result is an attack able to avoid traditional signature-based

detection tools, since it involves no downloads or installs other than the DLL files.

"This technique is called living off the land-- using legitimate tools that are already present on the target system to masquerade as regular activity," Microsoft says. "The attacker can then use stolen data to try moving laterally across networks, carry out financial theft, or sell victim information in the cybercriminal underground."

However being fileless does not mean invisible or undetectable. The Microsoft security researchers managed to detect the Astaroth attack through a spike in the use of the WMIC tool running XSL Script, a flag in a potential fileless attack. Further analysis detected Astaroth as it attempted to run a backdoor directly on memory.

Thus, Microsoft says AV tools need to start keeping a close eye on the WMIC command-line code, and start applying rules for the download of DLL files, such as checking the age of the file and blocking the running of newly-created DLLs. Ultimately, one simply needs to know what they are looking for if they are to stop this ne attack technique.

Go Dismantling a Fileless Campaign: Microsoft Defender ATP Next-Gen Protection Exposes Astaroth Attack