Attackers Exploit DLL Hijacking to Bypass SmartScreen

socprime.com/en/news/attackers-exploit-dll-hijacking-to-bypass-smartscreen/

May 11, 2018

Delaware, USA – May 11, 2018 – DLL Hijacking technique has long been known remaining effective enough to bypass some of the security solutions, so attackers used it in new malware. ElvenPath analyzed banking trojan N40, used in a recent campaign against Chilean banks. This malware is the evolved Brazilian banking trojan used in attacks last fall. Adversaries can use it to gain access to an infected system, steal credentials and valuable data, as well as to replace bitcoin wallet in victim's clipboard. Trojan uses unusual techniques to avoid detection by security tools. To bypass Windows SmartScreen, the first stage malware drops the legitimate WMnat.exe file to the attacked system, then saves to the same folder shfolder.dll, which in fact is N40 trojan renamed and signed with a digital certificate purchased in the Black market. After that, the downloader runs WMnat.exe that loads trojan into memory, and Windows SmartScreen only detects execution of a legitimate application. Malware bypasses many signature-based anti-virus solutions, uses real-time string decoding techniques to hide in system memory and uses non-standard ports to communicate with Command & Control servers.

The researchers did not mention how the attackers spread N40 banking trojan but noted that threat actors behind this campaign are successful, and this evolved malware is efficient against standard solutions used in the banking sector. To detect exploiting of DLL Hijacking

technique, you can use ArcSight with File Hash Analytics use case, which can quickly find files with the same name, but different hashes.