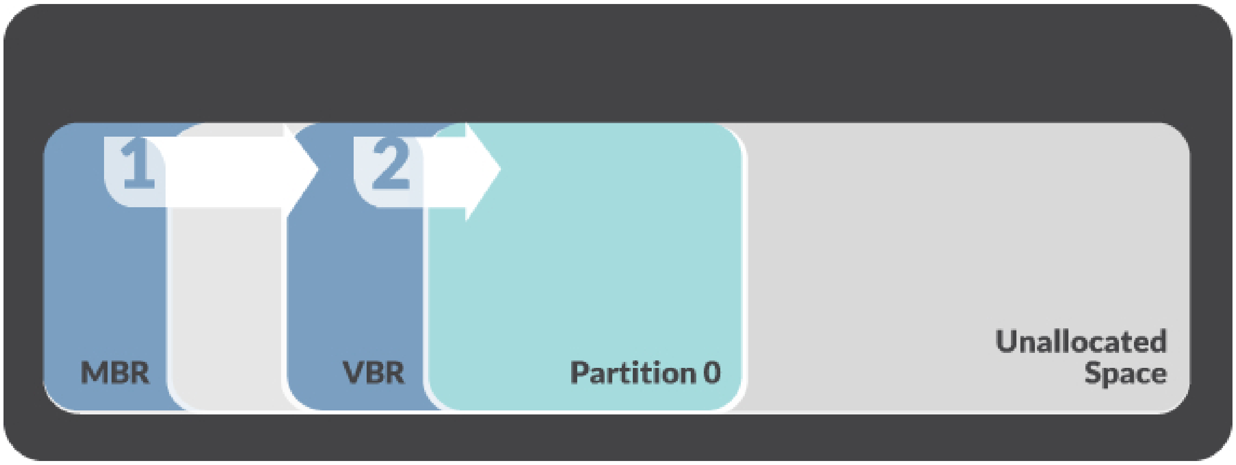
TechXplore

Sophisticated malware won't budge in simple OS re-install

December 8 2015, by Nancy Owano



Simplified normal boot process. Credit: FireEye

Security watchers had a menace on their minds Monday, and it is payment card malware dubbed Nemesis.

The malware carries the twin headache of being difficult to detect and difficult to remove. How bad a headache?

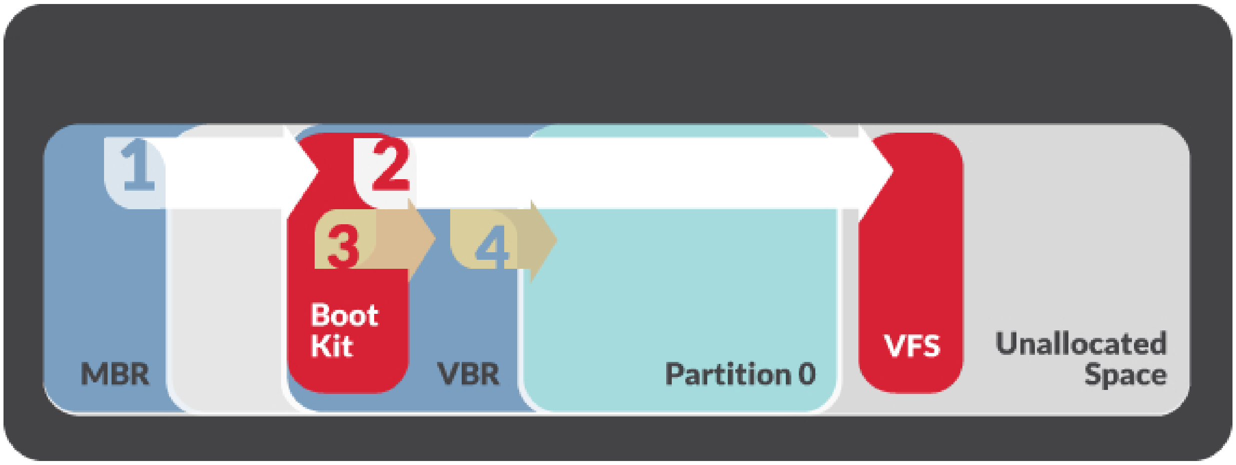
"Nemesis is a so-called bootkit. It is installed on lower-level operating system components, and even if the operating system is reinstalled, it can remain in place," said the IDG News Service's Jeremy Kirk on Monday.

Threatpost reported that FireEye and Mandiant uncovered the specialized malware this past September while carrying out an investigation at a financial organization.

On Monday, Dimiter Andonov, Willi Ballenthin, Nalani Fraser, Will Matson, Jay Taylor wrote about Nemesis in the FireEye blog headlined "Financial Threat Group Targets Volume Boot Record."

Back in September, said FireEye, Mandiant Consulting had identified a financially motivated threat group targeting payment card data. The group was reported as using sophisticated malware which executes before the operating system boots. This is a technique referred to as a 'bootkit.'

Commented FireEye: "The selective use of bootkits for persistence suggests some threat actors may have access to more sophisticated toolsets. The threat actors may selectively deploy these advanced toolsets when the victim organization is difficult to penetrate or if the targeted data is of high value and the threat actors want to ensure continued access to the compromised environment."



Simplified hijacked boot process. Credit: FireEye

Chris Brook in *Threatpost* on Monday described the malware as "a cornucopia of malware, backdoors, files, and utilities it uses to infiltrate systems and extract cardholder data." Its capabilities, include file transfer, a keylogger, screen capture, and process manipulation.

In early 2015, said FireEye, the FIN1 group updated their toolset. Included was a utility to modify the legitimate system Volume Boot Record and hijack the system boot process to begin loading Nemesis components before the Windows operating system code. "We refer to this utility as BOOTRASH."

Who is behind Nemesis? FireEye said FIN1 may be located in Russia or a Russian-speaking country based on language settings in many of their custom tools. The group, said FireEye, "is known for stealing data that is easily monetized from financial services organizations such as banks, credit unions, ATM operations, and financial transaction processing and financial business services companies."

Re-installing the operating system is considered the effective way to eradicate malware. This is different, however. "Malware with bootkit functionality can be installed and executed almost completely independent of the Windows operating system. As a result, incident responders will need tools that can access and search raw disks at scale for evidence of bootkits," said FireEye. "Similarly, re-installing the operating system after a compromise is no longer sufficient."

Their advice: "System administrators should perform a complete physical wipe of any systems compromised with a bootkit and then reload the operating system."

More information: www.fireeye.com/blog/threat-re … ets-boot-record.html

Citation: Sophisticated malware won't budge in simple OS re-install (2015, December 8) retrieved 10 April 2024 from https://techxplore.com/news/2015-12-sophisticated-malware-wont-budge-simple.html