USB malware goes after air-gapped computers

March 26 2016, by Nancy Owano

Credit: Peter Griffin

Uh-oh. USB malware trouble again. Earlier this week, *iTWire* and other sites reported on USB-based malware that steals data. "USB Thief" is also described as Win32/PSW.Stealer.NAI affecting computers.

ESET, created in 1992 in Bratislava, Slovakia, a malware detection and analysis company, made the discovery.

Reports among tech-watching sites described the malware as targeting air-gapped systems. What is air gapping? As computers connected to the Internet are vulnerable to outside hacking, air-gapping is a security measure. As the name suggests, the computer is given air-tight security. It is not connected to the Internet. "The malware is able to steal data from air-gapped systems (which aren't connected to the internet) by writing it to the device itself," said *The Register*'s John Leyden.

The Stack described the theft mechanism as highly cloaked. It doesn't leave any evidence on the infected computer. Users can have their data stolen without even noticing and without being online.

"It seems that this malware was created for targeted attacks on systems isolated from the internet," commented Tomas Gardon, ESET malware analyst, in *iTWire*.

Gardon, writing in *We Live Security*, the ESET information site, said the malware consists of six files. Four of them are executables and the other two contain configuration data.

"A unique data-stealing trojan has been spotted on USB devices in the wild – and it is different from typical data-stealing malware," he wrote. "Each instance of this trojan relies on the particular USB device on which it is installed and it leaves no evidence on the compromised system. Moreover, it uses a very special mechanism to protect itself from being reproduced or copied, which makes it even harder to detect."

Security watchers commenting on the news echoed the key word about this data-stealing discovery: the USB-malware is unique. The malware does not leave traces and victims are not aware their data was stolen."

Also, as Gardon in *iTWire* stated, "Another feature which makes this malware unusual is that not only it is USB-based, but it is also bound to a single USB device since it is intended that the malware shouldn't be duplicated or copied. This makes it very difficult to detect and analyze."

The code is intended to exist in the environs of a USB stick rather than attempting to replicate itself onto the host system, said *The Stack*. It resists copying to any other USB stick than the one it is found on.

Adding to the discussion of its nature, Martin Anderson, editor-in-chief of *The Stack*, said, "The malware is designed to exfiltrate data from the target system, although no details are provided regarding how it communicates with any control server that might be in play. If there is no control server, the low-network approach of USB Thief would seem to indicate a 'hands on' campaign, where the communication of the device takes place at a personal or 'insider' level."

Dan Goodin, Security Editor, *Ars Technica,* said, "There are indications that the USB Thief developers devoted a fair amount of testing to make sure the trojan worked properly under a variety of different scenarios. The malware, for instance, won't install itself in the event the target machine is running antivirus software from Kaspersky Lab or G Data, presumably because those programs either detected the malware or created performance problems."

How much harm has this malware caused? Gardon said, "As ESET's statistics shows, that malware is not very widespread. However, it possesses the ability to be used in targeted attacks – especially at computers that are not connected to the internet for security reasons."

Citation: USB malware goes after air-gapped computers (2016, March 26) retrieved 26 April

2024 from https://techxplore.com/news/2016-03-usb-malware-air-gapped.html