FBI warns US companies to avoid malicious USB devices

By Brandon Rochat, issued by Cybereason

18 Jan 2022

Cybercriminals constantly evolve the tactics, techniques, and procedures they use to execute attacks to find innovative ways to bypass or circumvent security controls. Sometimes the best strategy is the simplest one, though, and may succeed in catching targets off guard. A new warning from the FBI cautions US companies to be on alert for an old tactic that is apparently being used again - tricking users into connecting a malicious USB device.

Brandon Rochat

Malicious USB campaign

According to the FBI, threat actors targeted companies in the defense, transportation, and insurance industries in the last half of 2021 by sending USB thumb drives to intended targets.

The attackers — identified as the FIN7 cybercrime group by the FBI—used the US Postal Service and UPS to send letters and packages that claimed to be from the Department of Health and Human Services (HHS), or — in some cases — Amazon. The deliveries included a USB thumb drive containing malicious software, such as BadUSB.

Information shared by the FBI indicates that the packages were designed to seem like legitimate thank you notes or gifts. If the threat actors are smart, they presumably also did at least a little homework to improve the odds of success by tailoring the message to the organisation or individual it was sent to.

Threat actors from FIN7 have also been known to follow up — calling or emailing recipients to reinforce the con and pressure them into actually connecting the malicious device to their PC.

BadUSB

BadUSB is a particularly sinister piece of malware that immediately registers the device on the system as a Human Interface Device (HID) Keyboard. This little trick enables the malicious USB device to operate even if the system has a policy in place that disables the use of removable storage devices.

The malicious USB uses its designation as a “keyboard” to inject keystrokes on the system to install other exploits and malicious payloads on the compromised system. A report from BleepingComputer explains, “FIN7's end goal in such attacks is to access the victims' networks and deploy ransomware (including BlackMatter and REvil) within a compromised network using various tools, including Metasploit, Cobalt Strike, Carbanak malware, the Griffon backdoor, and PowerShell scripts.”

Gaining a foothold

This attack vector may be an attempt to exploit the work-from-home trend. Delivering USB flash drives directly to someone's home, for example, there are fewer guard rails and an increase in the likelihood a user will plug the computer into a work computer, or to their home network to which their work computer is also connected.

It is also possible that there are organisations or departments that routinely employ USB thumb drives — where people are more likely to use a USB storage device without finding it suspicious. That would make this tactic more effective.

The bottom line is that if the attackers are able to gain a foothold — even if it's not an admin account — they can escalate privileges or conduct reconnaissance from the inside, which may aid in gaining access to other systems.

Smoke and mirrors

This all sounds highly suspicious, though, and makes me wonder if this is a misdirection or distraction from a different or broader attack.

This is an old tactic. Even average users should know better than to use an unknown USB drive that gets delivered to them.

It does depend to some extent on how convincing the attack is, though. IT and cybersecurity professionals are well trained to not plug in devices such as found or free flash drives from unknown sources, but the average person may not be as cautious.

This is even more true if the person is convinced the package is from a credible source, or if an offer such as a free gift card triggers an emotional response which short-circuits rational thought processes.

Still, there are a variety of more effective attack vectors that don't rely on a potentially traceable and high-touch campaign like this. it is hard to imagine a reasonable scenario under which most people would use a USB stick they received in the mail. If the attackers sent a device like a USB mouse or some other type of gadget, that would probably have much higher success just by virtue of being novel.

Look for the big picture

FIN7 is a sophisticated threat actor — which is why this all feels like a big misdirection.

You should obviously never insert an unknown USB device into your PC — whether it's one you receive randomly in the mail, or even a USB device that you just don't know when or where it was used last.

Beyond that, though, you need to pay attention to the big picture when it comes to cyberattacks. Whether attackers succeed in gaining a foothold using a malicious USB drive, or use the delivery of a malicious USB drive as a distraction from a different attack vector, you need to be able to view the entire malicious operation — or MalOp™ — across your environment and recognise Indicators of Behaviour (IOBs) that enable you to quickly identify and stop malicious activity.

ABOUT THE AUTHOR

Brandon Rochat is Cybereason sales director for Africa.

- **FBI warns US companies to avoid malicious USB devices** 18 Jan 2022
- **Cybereason 2022 trends and predictions** 29 Nov 2021
- **Cybereason Exposes Chinese Threat Actors Compromising Telecommunications Providers for Cyber Espionage** 3 Aug 2021
- **Cybereason acquires empow to enhance XDR offerings** 20 Jul 2021
- **Cybereason Secures $275 Million in Crossover Financing to Extend Global Leadership in XDR** 14 Jul 2021