FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware

By Catalin Cimpanu

Published: 2023-01-17 · Archived: 2026-04-05 16:00:08 UTC

The US Federal Bureau of Investigation says that FIN7, an infamous cybercrime group that is behind the Darkside and BlackMatter ransomware operations, has sent malicious USB devices to US companies over the past few months in the hopes of infecting their systems with malware and carrying out future attacks.

"Since August 2021, the FBI has received reports of several packages containing these USB devices, sent to US businesses in the transportation, insurance, and defense industries," the Bureau said in a security alert sent yesterday to US organizations.

"The packages were sent using the United States Postal Service and United Parcel Service," the agency added.

"There are two variations of packages—those imitating HHS [US Department of Health and Human Services] are often accompanied by letters referencing COVID-19 guidelines enclosed with a USB; and those imitating Amazon arrived in a decorative gift box containing a fraudulent thank you letter, counterfeit gift card, and a USB."

In both cases, the packages contained LilyGO-branded USB devices.

Some BadUSB attacks lead to ransomware

But the FBI says that if recipients plugged the USB thumb drives into their computers, the devices would execute a BadUSB attack, where the USB drive would register itself as a keyboard instead and send a series of preconfigured automated keystrokes to the user's PC.

These keystrokes would run PowerShell commands that downloaded and installed various malware strains that acted as backdoors for the attackers into the victims' networks.

In cases investigated by the FBI, the agency said it has seen the group obtain administrative access and then move laterally to other local systems.

"[The] FIN7 actors then used a variety of tools—including Metasploit, Cobalt Strike, PowerShell scripts, Carbanak, GRIFFON, DICELOADER, TIRION—and deployed ransomware, including **BlackMatter** and **REvil**, on the compromised network," the agency added.

US defense company also targeted

In the most recent case of these attacks, the group also targeted a US defense industry company as recently as November 2021, using the Amazon thank-you letter trick detailed above.

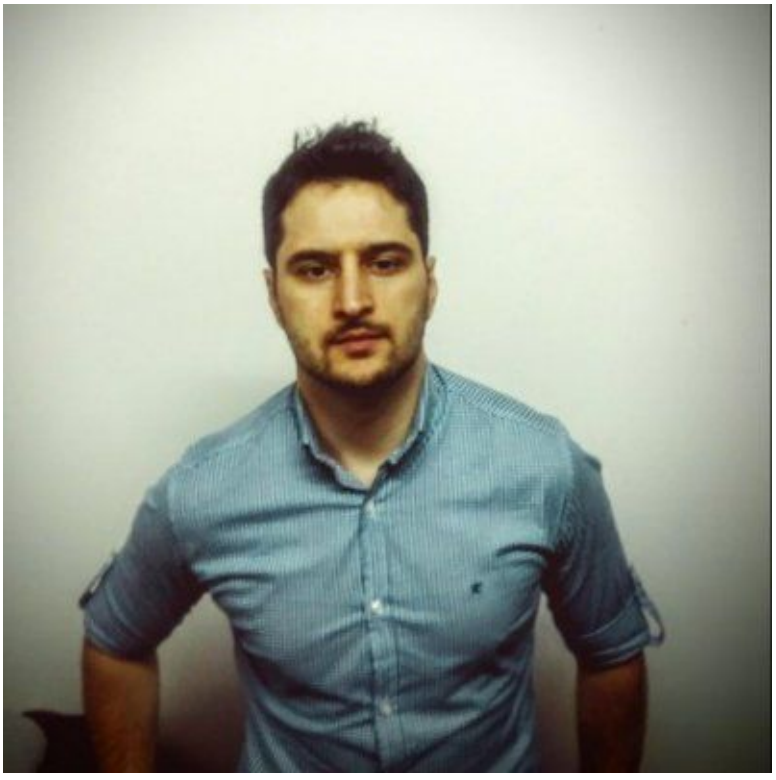
This marks the second alert the FBI has sent about FIN7 mailing malicious USB devices to US companies.

The FBI sent the first one in March 2020, after security firm Trustwave found one of the malicious BadUSB devices sent to one of its customers, a US hospitality provider.

Images of the Amazon thank-you letter, the HHS COVID-19 alert, and of the LilyGO-branded BadUSB device are included in the FBI alert, which, we cannot reproduce here. US companies can register on the InfraGard portal to gain access to the alert and learn more about FIN7's latest BadUSB attacks.

No previous article

No new articles



Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
