FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS

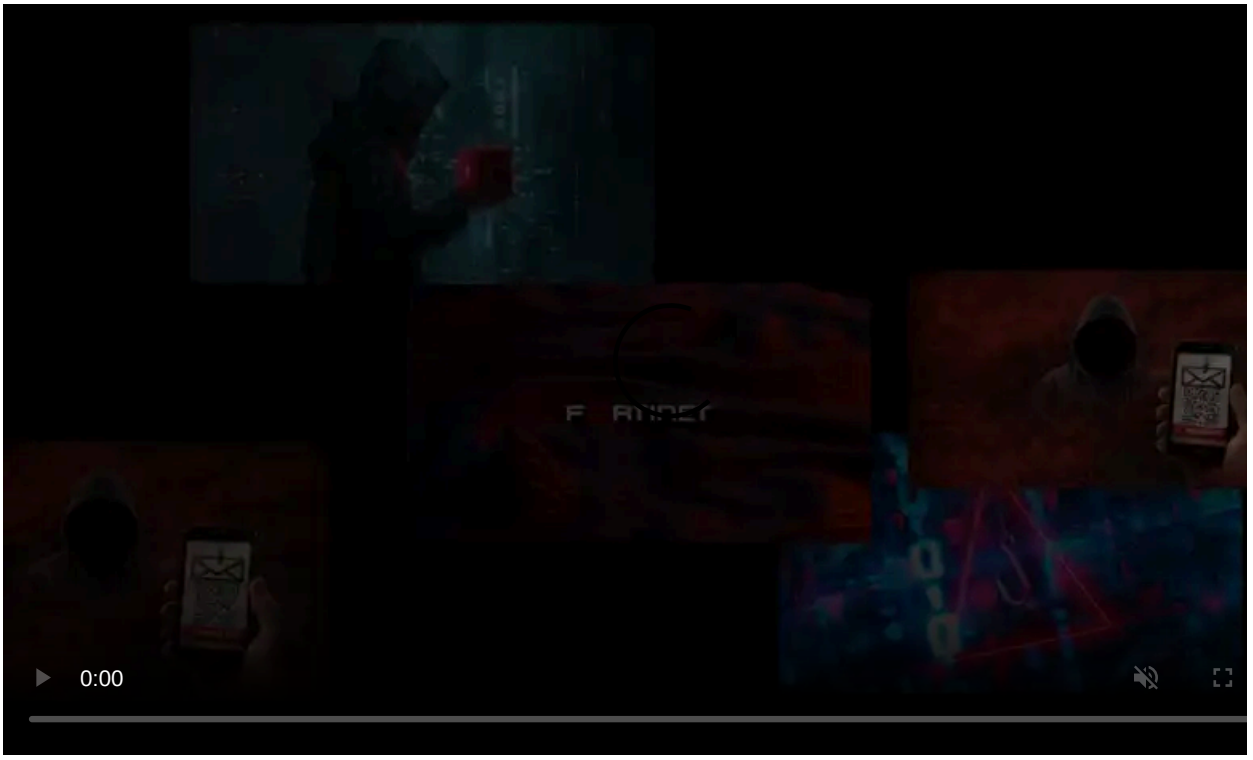
By Ionut Ilascu

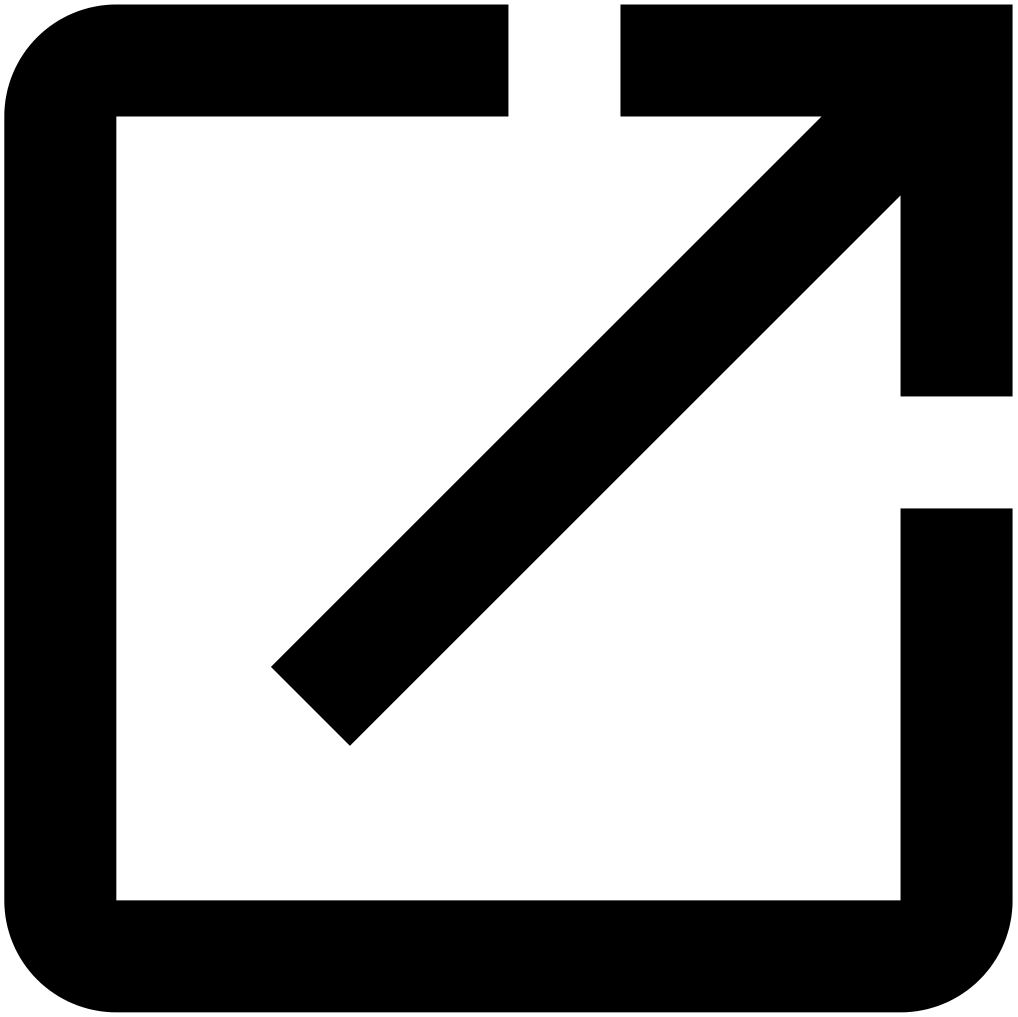
Published: 2020-03-27 · Archived: 2026-04-06 00:55:06 UTC

Hackers from the FIN7 cybercriminal group have been targeting various businesses with malicious USB devices acting as a keyboard when plugged into a computer. Injected commands download and execute a JavaScript backdoor associated with this actor.

In a FLASH alert on Thursday, the FBI warns organizations and security professionals about this tactic adopted by FIN7 to deliver GRIFFON malware.

The attack is a variation of the “lost USB” ruse that penetration testers have used for years in their assessments quite successfully and one incident was analyzed by researchers at Trustwave.


0:00



One client of the cybersecurity company received a package, allegedly from Best Buy, with a loyalty reward in the form of a $50 gift card. In the envelope was a USB drive claiming to contain a list of products eligible for purchase using the gift card.

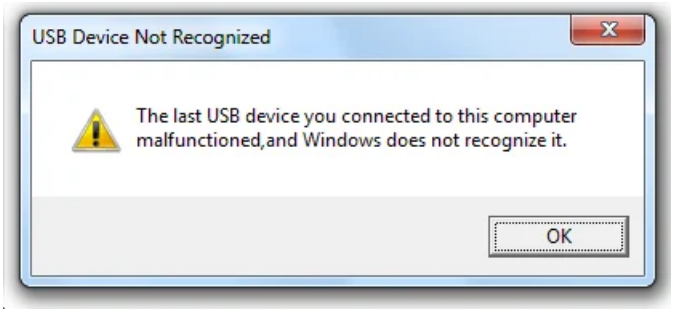
This is not a one-off incident, though.

The FBI warns that FIN7 has mailed these packages via USPS to numerous businesses (retail, restaurant, hotel industry) where they target employees in human resources, IT, or executive management departments. These packages sometimes include "gifts" like teddy bears or gift cards.

These USB drives are configured to emulate keystrokes that launch a PowerShell command to retrieve malware from server controlled by the attacker. Then, the USB device contacts domains or IP addresses in Russia.

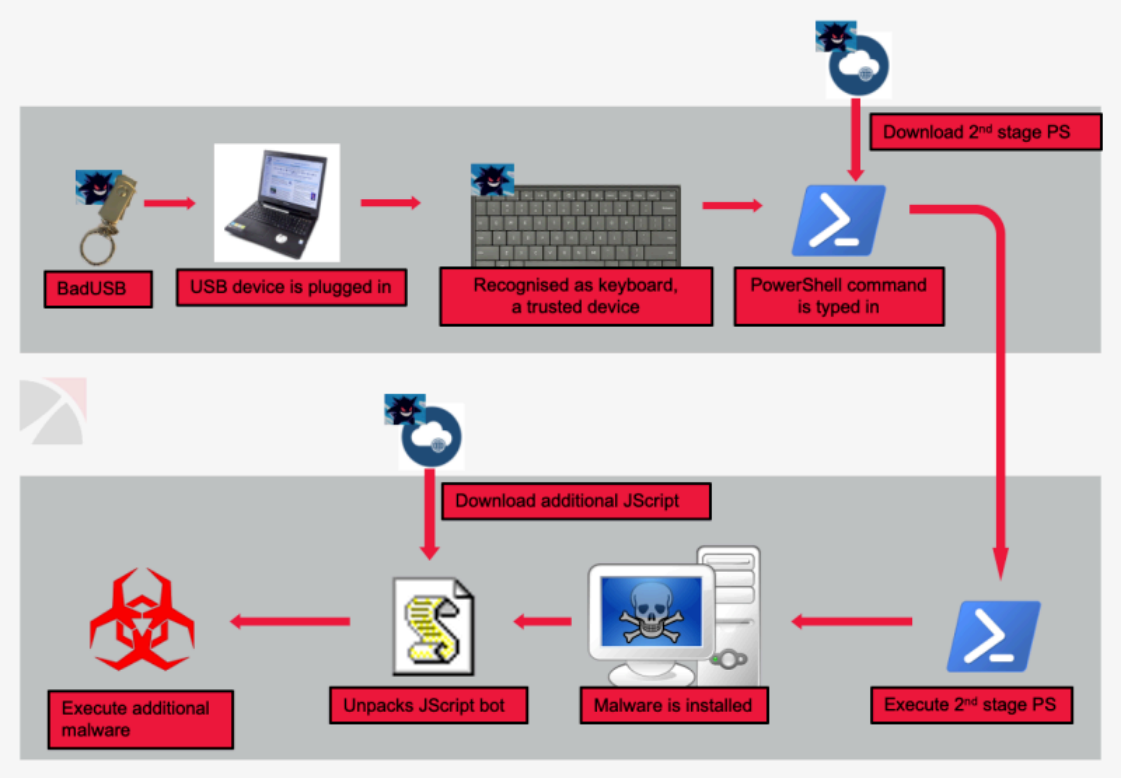
The days when USB flash drives were just for storage are long gone. Several development boards (Teensy, Arduino) are now available for programming to emulate a human interface device (HID) such as keyboards and mice and launch a pre-configured set of keystrokes to drop malicious payloads. These are called HID or USB drive-by attacks are easy to pull and don't cost much.

Trustwave analyzed this malicious USB activity and noticed two PowerShell commands that lead to showing a fake error for the thumb drive and ultimately to running third-stage JavaScript that can collect system information and downloading other malware.



To better summarize the attack flow, the researchers created the image below, which clarifies the stages of the compromise that lead to deploying malware of the attacker's choice.

The alert from the FBI informs that after the reconnaissance phase the threat actor starts to move laterally seeking administrative privileges.



FIN7's uses multiple tools to achieve their goal; the list includes Metasploit, Cobalt Strike, PowerShell scripts, Carbanak malware, Griffon backdoor, Boostwrite malware dropper, and RdfSniffer module with remote access capabilities.

BadUSB attacks, demonstrated by security researcher Karsten Nohl in 2014, are now common in penetration testing and multiple alternatives exist these days. The more versatile ones sell for $100.

FIN7 went with a simple and cheap version, though, that costs between $5-$14, depending on the supplier and the shipping country. The FBI notes in its alert that the microcontroller is an ATMEGA24U, while the one seen by Trustwave had ATMEGA32U4.

However, both variants had "HW-374" printed on the circuit board and are identified as an Arduino Leonardo, which is specifically programmed to act as a keyboard/mouse out of the box. Customizing the keystrokes and mouse movements is possible using the the Arduino IDE.

Connecting unknown USB devices to a workstation is a well-known security risk but it is still disregarded by many users.

Organizations can take precautions against attacks via malicious USB drives by allowing only vetted devices based on their hardware ID and denying all others.

Furthermore, updating PowerShell and enabling logging (the larger the log size, the better) can help determining the attack vector and the steps leading to compromise.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
