FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

06 JANUARY 2022

FLASH Number

MU-000160-MW

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact FBI CyWatch immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email: cywatch@fbi.gov | Phone: **1-855-292-3937**

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

FIN7 Cyber Actors Target US Businesses Through USB Keystroke Injection Attacks

Summary

This is an update to FLASH Number MI-000120-MW which was disseminated on March 26, 2020.

As recently as November 2021, the FBI has observed the cyber criminal group known as FIN7 targeting the US defense industry with a package containing a fraudulent thank you letter, counterfeit Amazon gift card, and a USB device. The enclosed USB provided by the group is a commercially available device known as a "BadUSB" or "Bad Beetle USB," typically with the logo "LilyGO." When plugged into a computer system, the USB device automatically injects a series of keystrokes in order to download and execute a malware payload. FIN7 seeks to deploy ransomware within a compromised network using a variety of tools including Metasploit, Cobalt Strike, PowerShell scripts, Carbanak, GRIFFON, DICELOADER, and TIRION for financial gain.

As early as August 2021, US businesses, especially in the transportation and insurance industries, started receiving nefarious USB devices through the mail, which were intended to deliver payloads of FIN7 malware. The USB devices are accompanied by fictitious letters purporting to

be from the US Department of Health and Human Services (HHS) and providing information on COVID-19 guidelines, or as fake gifts with forged Amazon thank you cards and counterfeit gift cards. Since at least May 2020, the packages included items such as teddy bears or gift cards and were sent to retail businesses, restaurants, and hotels.

Technical Details

In February 2020, the FBI discovered FIN7 mailed US businesses malicious USB devices which were sometimes accompanied by fraudulent emails or phone calls pressuring recipients to plug the USB devices into their computers. When the USB device was plugged into a computer system, the USB registered as a Human Interface Device (HID) Keyboard with a Vendor ID (VID) of `0x2341` and a Product ID (PID) of `0x8037`. Once the USB registration process completed, the USB device injected a series of keystroke commands, including the (Windows + R) shortcut launching the Windows Run Dialog to run a PowerShell command, which downloads and executes a malware payload from a server controlled by FIN7. The infected machine then called out to domains or IP addresses hosted by FIN7's command and control (C2) servers. The USB device still had the ability to operate on systems even with removable storage devices disabled in the local group policy editor, since the USB registers as a HID Keyboard Device when plugged into a computer.

Upon gaining access to the computer system, attackers conducted reconnaissance and moved laterally in the network until they obtained administrative privileges. 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.

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 packages were sent using the United States Postal Service and United Parcel Service. There are two variations of packages—those imitating HHS 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.

Indicators

Packages with the USB device may include letters, gift cards, and other miscellaneous items. The USB devices may also have the recipient's name written on them with a marker. The USB device, known as "BadUSB" or "Bad Beetle USB," is commonly available for purchase on the Internet. There are many types of "BadUSB" products available. Several of the received "BadUSB" devices were "LilyGO" devices, which are available for shipping to the United States from China. All of the USB devices observed by the FBI to date were silver with a swivel cover.

COVID-19 Letters Imitating HHS (Figure 1)

The first variation of the mailings contained a letter imitating HHS and referencing COVID-19 guidelines, also accompanied by a USB.

U.S.Department of Heath and Human Services

COVID-19

COVID-19 Pandemic Prevention Program

United States Department of Health and Human Services, The Centers for Disease Control and Prevention (CDC), VaccineFinder had applied new regulations for public places, government agencies, restaurants, hotels and companies.

These rules are required and concerned individuals who had been vaccinated, are about to be vaccinated and who have gone through COVID-19 disease. The instructions have been added and updated according to the official guidelines on the prevention and spread of COVID-19.

To confirm that you received the regulations and apply these instructions, you must be familiar with the regulations provided on the USB flash drive. This is required to avoid additional lockdown measures and possible fines for you and your company.

Using the USB Flash drive, go to the website https://www.hhs.gov and pass the mandatory confirmation procedure that you familiarized and applied all of these instructions.

Sincerely,
Ann C. Agnew,
Executive Secretary,
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201

Executive Secretary,
Department of Health and
Human Services

Ann C. Agnew

Figure 1. Letter imitating HHS

Decorative Packages Imitating Amazon (Figure 2)

The second variation of the mailings used a decorative box containing a fraudulent thank you letter imitating Amazon with a counterfeit gift card and a USB device.

Figure 2. Example of package imitating Amazon

LilyGO USB Device (Figure 3) and Internal Hardware of the USB Device (Figure 4)

The USB devices used PowerShell to download malware onto the victim's computer. The internal hardware of the USB device is a custom Arduino board using the ATMEGA32U4 microcontroller. The USB device is known to be registered as an Arduino Leonardo device prior to being initialized with a custom script. This type of USB device is designed to act as a virtual keyboard that registers as an I/O device when connected to a computer.

Figure 3. LilyGO USB devices

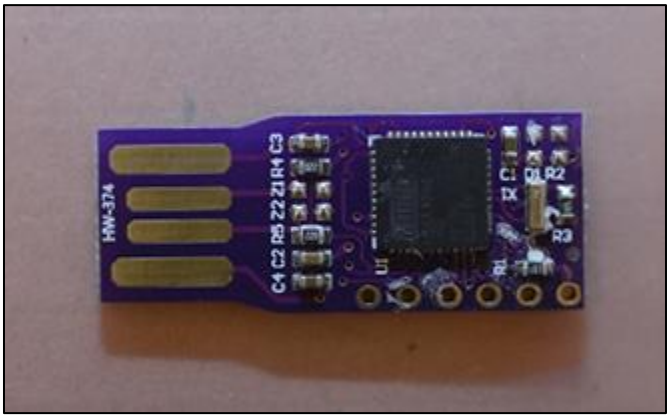

Figure 4. Internal hardware of the USB device

Information Requested:

If your organization was targeted by FIN7, the FBI is seeking information, including:

- The original mailing package sent to your organization, including all contents. Please limit the exposure of the package to a few individuals, and handle it with care to preserve DNA and fingerprints that may be obtainable from the package.
    - If the package contained a gift card, please provide identifying information.
- The mailing carrier tracking number listed on the package.
- The return address of the package.
- If the USB device was analyzed by a security or IT professional:
    - Any information about how the package and device was handled by your organization.

- A report based on your organization's findings.
- The IP address or domain the USB tried to communicate with.

- If the USB device was plugged into any computer(s), please preserve the following evidence:
  - A full memory capture of the victim computer(s).
  - A full forensic image or copy of the victim computer(s) before any remediation or deletion of files. If your organization requires assistance, please reach out to your local FBI field office.
  - Netflow or full packet capture of network communications to/from the victim computer(s).
  - Log files including event logs, DNS logs, and firewall logs from the suspected date the USB device was plugged in.

Recommended Mitigations:

While the applications, systems, and devices listed in this FLASH support legitimate purposes, threat actors can use them to aid in system compromise or exploration of a network. The FBI recommends the following security measures to protect your systems against FIN7:

- Do not plug any unknown USB devices into any computer system.
- Implement monitoring or alerts for any endpoints that plug in a USB device with a VID of `0x2341` and PID of `0x8037`.
- Update endpoints to PowerShell version 5 or higher and turn on PowerShell logging through the Group Policy Editor, including module logging, script block logging, and transcription. Organizations should also increase their PowerShell event log size to 1GB or higher to ensure logs are not quickly overwritten.
- Although it will not prevent these USB devices from operating, if feasible for your business operations and for general additional security, disable access to all removable storage in the local group policy editor, allowing only administrator access in a network environment. This can also be implemented using Group Policy Objects.
  - See Figure 5 below for configurations in Windows Registry Settings:
    - HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\RemovableStorageDevices
    - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices

- Deny_All DWORD
- (delete)=Enable
- 1 = Disable

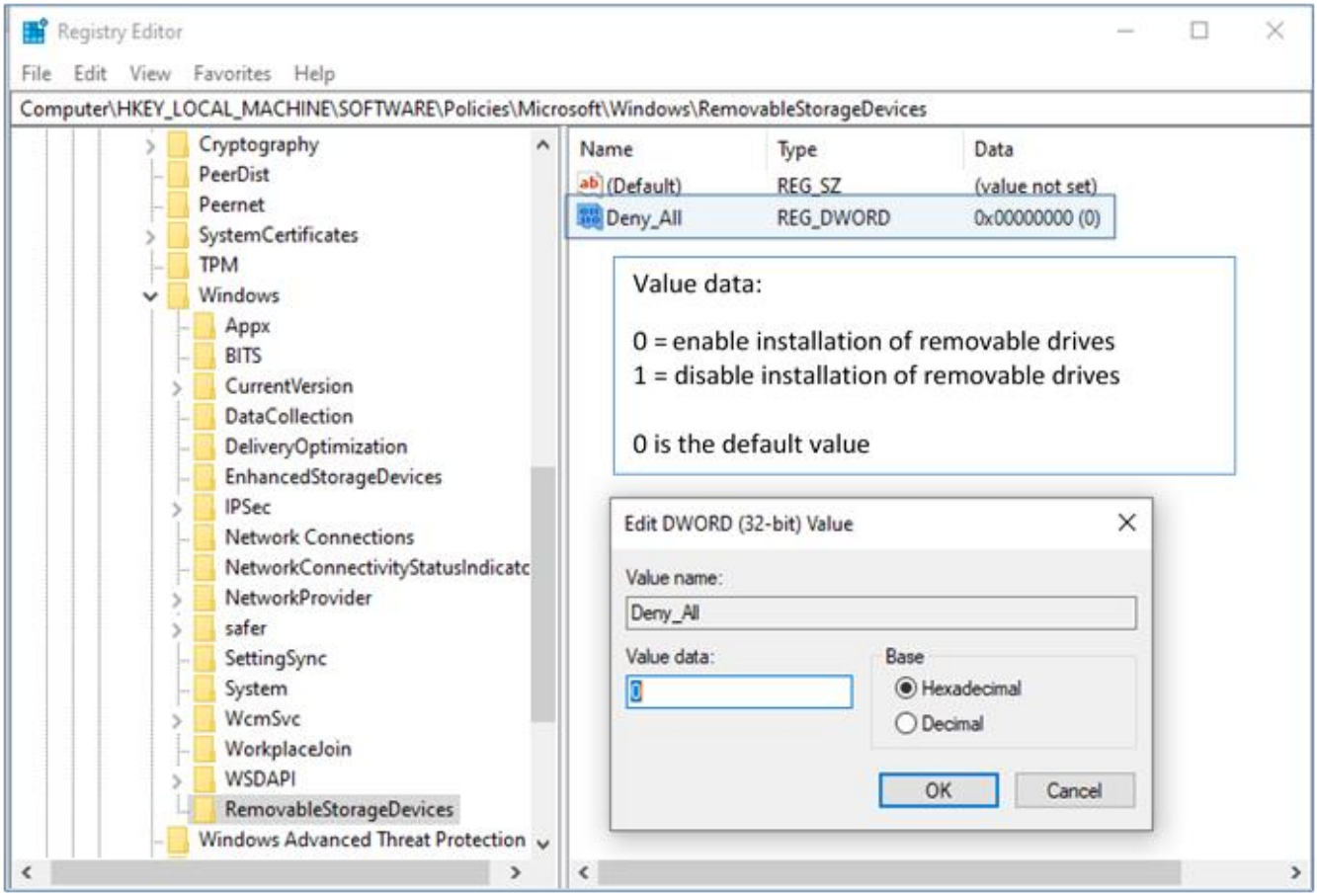

Figure 5. Windows Registry Settings

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:GREEN**. The information in this product may be shared with peers and partner organizations within your sector or community, but not via publicly accessible channels.