FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

26 March 2020

Alert Number

MI-000120-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

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.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but not via publicly accessible channels. This FLASH was coordinated with DHS CISA.

FIN7 Cyber Actors Targeting US Businesses Through USB Keystroke Injection Attacks

Summary

Since 2015, financially motivated cybercriminal groups have actively targeted businesses in the retail, restaurant, hotel, and gaming industries at an increasing rate. Recently, the cybercriminal group FIN7,[1] known for targeting such businesses through phishing emails, deployed an additional tactic of mailing USB devices via the United States Postal Service (USPS). The mailed packages sometimes include items like teddy bears or gift cards to employees of target companies working in the Human Resources (HR), Information Technology (IT), or Executive Management (EM) roles. The enclosed USB device is a commercially available tool known as a "BadUSB" or "Bad Beetle USB" device. After the USB device is plugged into a target system, the device automatically injects a series of keystrokes in order to download and execute a unique malware payload commonly known as GRIFFON malware, which is also a payload observed in several variations of FIN7 phishing emails.

[1] FIN7 is also known as the Carbanak Gang, based on their use of the Carbanak malware; and Combi Security, based on the name of their front company.

Technical Details

Recently, the FBI has observed USB devices mailed to US businesses, sometimes accompanied by the more common FIN7 phishing emails. When plugged into a target system, the USB registers as a Keyboard HID Keyboard Device with a Vendor ID (VID) of 0x2341 and a Product ID (PID) of 0x8037. The USB injects a series of keystroke commands, including the (Windows + R) shortcut to launch the Windows Run Dialog to run a PowerShell command to download and execute a malware payload from an attacker-controlled server. The USB device then calls out to domains or IP addresses that are currently located in Russia.

Once the targeted system is compromised, attackers conduct reconnaissance and move laterally until they obtain administrative privileges. FIN7's goal is to target and steal payment card data from Point of Sale (POS) systems on a compromised network. To do this, FIN7 uses a variety of tools including Metasploit, Cobalt Strike, PowerShell scripts, and the Carbanak, GRIFFON, BOOSTWRITE, and RDFSNIFFER malware.

The FBI has received reports of several packages containing items including a USB device sent to US businesses in the retail, restaurant, and hotel industry. The packages to date have been sent using the United States Postal Service (USPS). The packages are enclosed in packaging material that can be readily bought at most USPS Post Offices, including packaging material from the USPS ReadyPost® brand.

Figure 1 - ReadyPost® USPS packaging

Packages with the USB device may include other items such as teddy bears, 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 is commercially available, known as "BadUSB" or "Bad Beetle USB," and is commonly available for purchase on the Internet. There are many types of BadUSB products available. Several of the received devices were "LILYGO BadUSB" devices, which are available for shipping to the US from China. All of the USB devices the FBI has observed so far are silver with a swivel cover.

Figure 2 – BadUSB Example

The internal hardware of the USB device is a custom Arduino board using the ATMEGA24U 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 can be designed to act as a virtual keyboard that registers as an I/O device when connected to a computer.

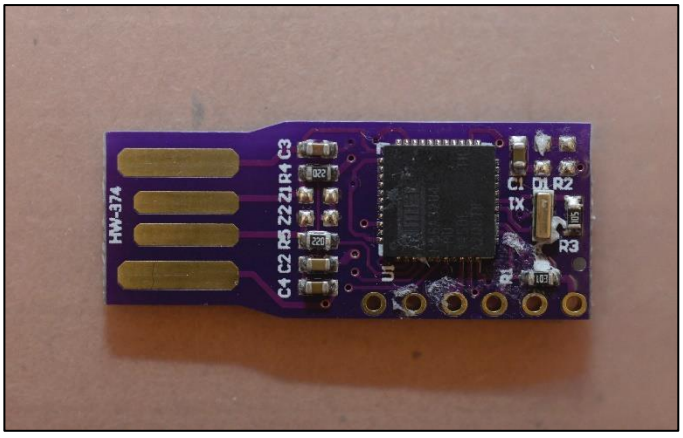

Figure 4 – Internal Hardware of the USB Device

The FBI has observed the USB device attempt to download a version of GRIFFON malware to deploy onto the target system. Once infected, FIN7 will have backdoor access to the target system to deploy additional malware with the goal of stealing payment card information from POS systems located within a compromised network.

Information Requested

If your organization is found to be a victim of FIN7, the FBI is seeking information, including:

- The original mailing package that was sent to your organization, including all of the contents. The FBI would like to request your organization limit the exposure of the package and handle it with care to preserve DNA and fingerprints that may be obtainable from the package.
- The USPS or other mailing carrier tracking number listed on the package.
- The sending 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 beacon out to.
- If the USB device was plugged into victim 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

The FBI recommends the following security measures to protect your systems against FIN7:

- Do not plug in any unknown USB devices to 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.

- This device will still operate on networks with removal storage devices disabled, since the USB registers as a Keyboard HID Keyboard Device (an I/O device) when plugged into a computer.
- Although it will not prevent these USB devices from operating, if feasible for your business operations, for general additional security you can disable access to all Removal Storage in the local group policy editor allowing only the machine administrator access to the computer in a network environment. This can also be implemented using Group Policy Objectss.
    - See below 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

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). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and 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**: Subject to standard copyright rules, **TLP: GREEN** information may be distributed to affiliated organizations or members of the same sector, but never through public channels.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.