Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas

Cyber Actors Targeting US Businesses Through USB Keystroke Injection Attacks

03/26/2020

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.

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.

DIR.TEXAS.GOV

Assistance/Feedback/Questions?

Office of the Chief Information Security Officer

DIRSecurity@dir.texas.gov

Texas Department of Information Resources

Transforming How Texas Government Serves Texans