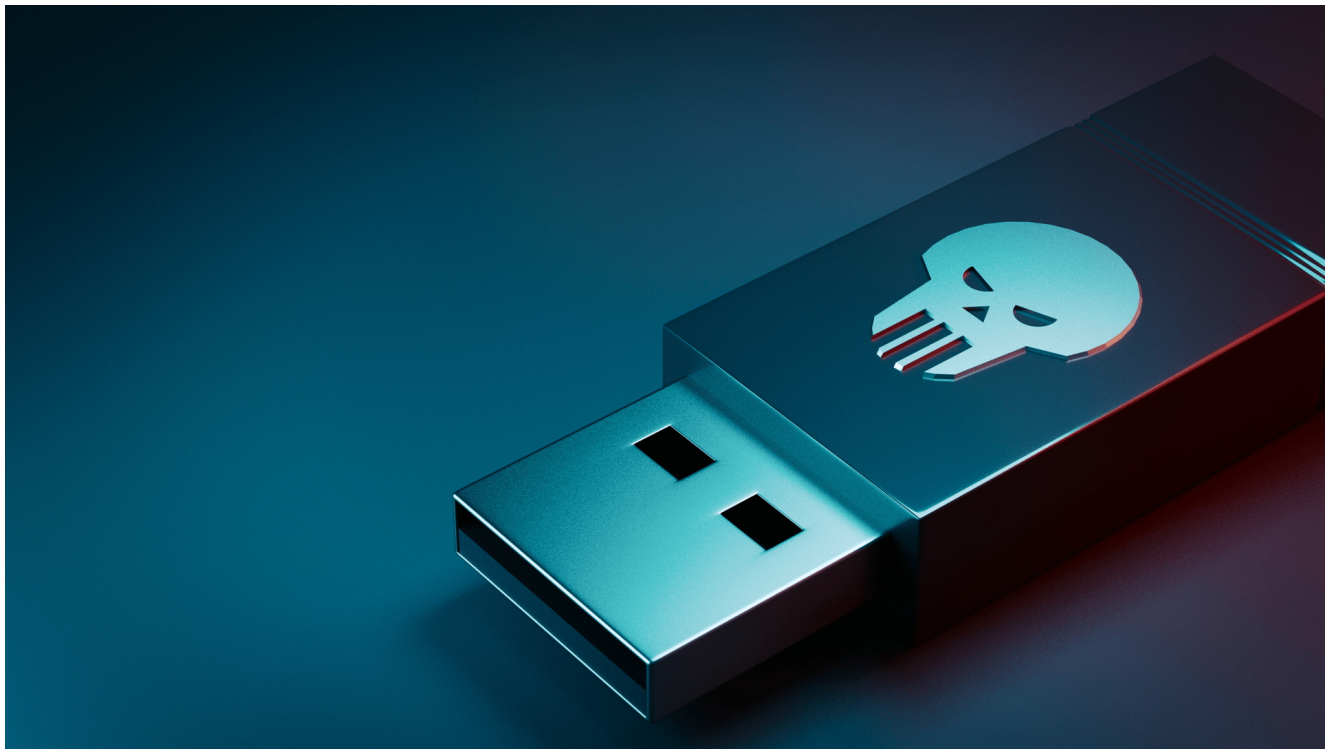
FIN7 Uses Flash Drives to Spread Remote Access Trojan

geminiadvisory.io/fin7-flash-drives-spread-remote-access-trojan/

January 13, 2022



01/13/2022

Executive Summary

Recorded Future analysts continue to monitor the activities of the FIN7 group as they adapt and expand their cybercrime operations. Gemini has conducted a more in-depth investigation into these types of attack after a Gemini source provided analysts with the file “sketch_jul31a.ino”, which was linked to FIN7’s BadUSB attacks. The file had the extension (.INO), indicating it contained the source code for an Arduino “sketch” (the Arduino term for a program). BleepingComputer also recently released a public report on FIN7’s use of the “BadUSB” attack method, outlining the activity around this type of attack.

The Arduino platform provides a common set of software utilities and libraries for constructing programs to run on platform-compatible microcontrollers. The platform uses a simplified version of the C++ programming language and provides foundational libraries, an integrated development environment for constructing the sketch, a compiler, and a means of uploading the compiled sketch to a device with a compatible microcontroller. In the Arduino ecosystem, the microcontroller executes the compiled sketch, making it operating system (OS) agnostic.

Hackers have leveraged the Arduino platform to create trojanized USB devices that emulate keyboards and inject keystrokes. In most cases, the sketches on these trojanized devices connect to a malicious actor’s file repository, download additional software, and install it on the

victim system. In March 2020, security analysts from Trustwave SpiderLabs reported that FIN7 targeted a US company by sending one of its employees a USB device trojanized with keystroke injection malware.

Key Findings

- FIN7 used an Arduino sketch file called “sketch_jul31a.ino” to install malware on USB devices as part of BadUSB attacks.
- FIN7 uses the trojanized USB devices to ultimately load the IceBot Remote Access Trojan (RAT), resulting in FIN7 gaining unauthorized remote access to systems within victims’ networks.
- We identified 9 IP addresses that host FIN7’s malicious payloads and 3 FIN7 command-and-control (C2) servers, one of which contains a control panel for managing infected systems. The control panel displayed a list of systems infected with the IceBot RAT and pertinent information about each installation.

Attack Analysis

Gemini specialists conducted the analysis of the file “sketch_jul31a.ino”. “.INO” is a file extension associated with the Arduino microcontroller programming platform, while “sketch” is the platform’s term for a program. Malicious actors have taken advantage of the Arduino platform and its support for microcontrollers installed on USB devices to install malware. When a USB is maliciously used as a virtual keyboard, the attack is called a “keystroke injection”, “BadUSB”, or “Rubber Ducky” attack.

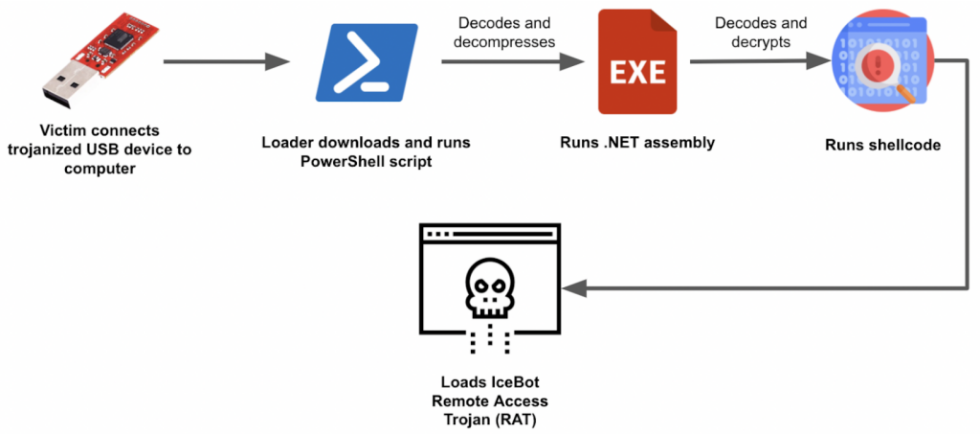


Figure 1: *The attack flow of the Fin7 USB attack (Source: Recorded Future)*

This attack’s use of keyboard injection capitalizes on Microsoft Windows’ default behavior of automatically trusting USB keyboards. It uses Arduino-compatible microcontrollers that are hidden in what appear to be typical USB devices but are actually programmed to function as virtual keyboards (usually based on ESP8266, Atmega32u4, or ATtiny85 microcontrollers). The sketch sends keystrokes to activate a shell and execute additional commands on the victim system.

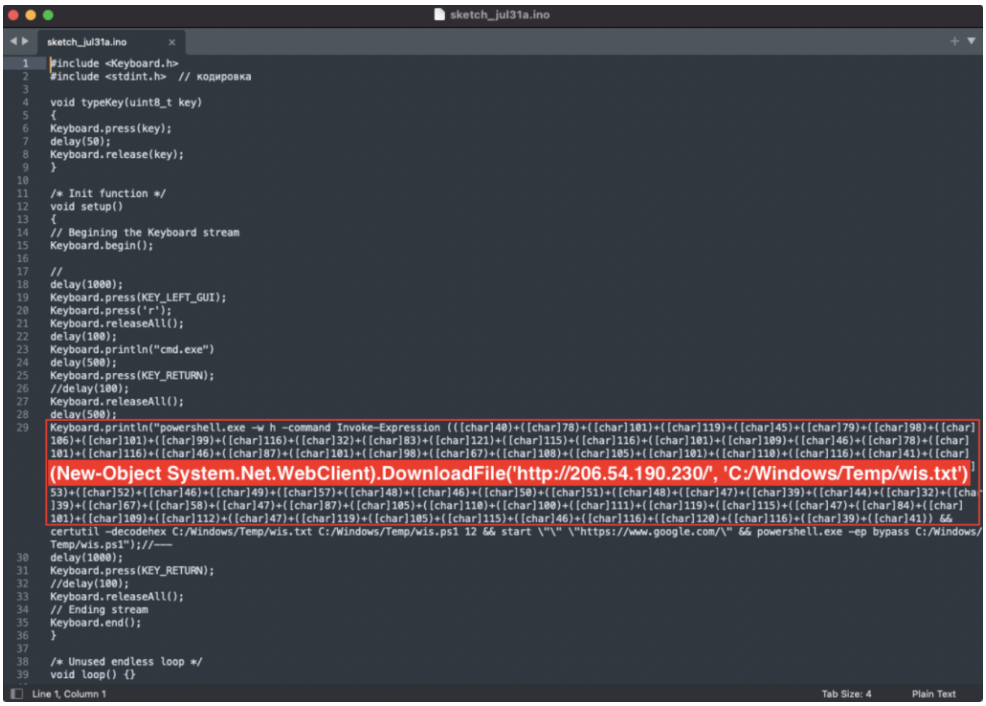


Figure 2: *Arduino sketch source code from the file "sketch_jul31a.ino" (Source: Recorded Future)*

The "sketch_jul31a.ino" file (Figure 2) contains the source code for an Arduino sketch designed to run scripts on a Windows system. First, the sketch opens the "Run" dialog by sending the "Windows" + "R" keys. Next, it sends the keystrokes for "cmd.exe" to the "Run" dialog to execute a command prompt. The sketch then sends keystrokes to execute "powershell.exe -w h -command Invoke-Expression", which runs the PowerShell interpreter in a hidden window and executes a script that is passed in-line. This script downloads and installs malware from the IP address 206.54.190[.]230. As shown in the table below, further analysis revealed 8 additional IP addresses used to host FIN7's malicious payload.

IP Address	First Seen	Last Seen
138.124.180[.]127	2021-07-29 12:26:10	2021-08-10 12:03:34
185.232.170[.]24	2021-07-29 9:21:31	2021-10-21 13:03:42
185.233.80[.]149	2021-07-29 9:50:26	2021-10-21 14:38:00
185.53.46[.]100	2021-07-29 13:47:48	2021-11-20 10:08:13
206.54.191[.]37	2021-07-29 12:37:53	2021-10-21 16:13:58
37.1.213[.]194	2021-07-29 10:48:31	2021-08-10 9:26:01
45.142.215[.]148	2021-10-21 15:17:31	2021-10-21 15:17:31
5.252.177[.]215	2021-07-29 14:18:09	2021-10-21 11:20:57

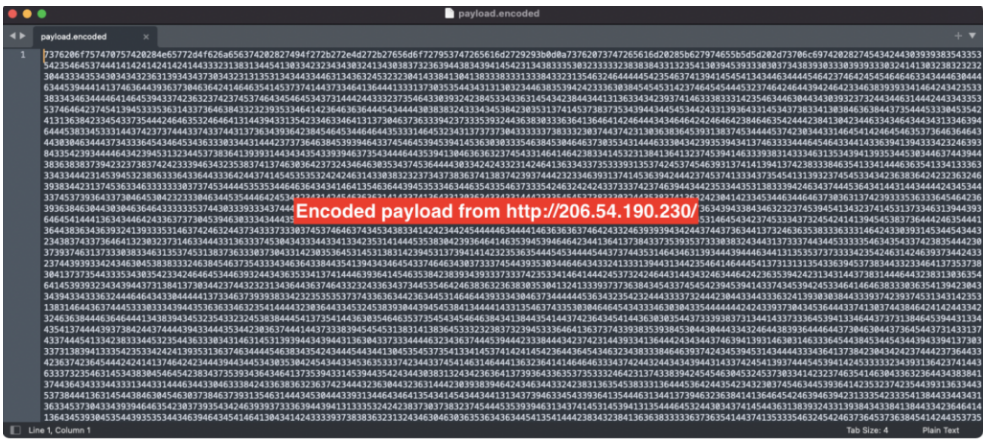


Figure 3: *Contents of the downloaded file wis.txt (Source: Recorded Future)*

After downloading the file “wis.txt” from the malicious server, the PowerShell script decodes the file via the command “certutil -decode hex”, a command-line program and routine that is part of Microsoft Windows Certificate Services. The decoding results in another PowerShell script, saved to “C:\windows\temp\wis.ps1”.

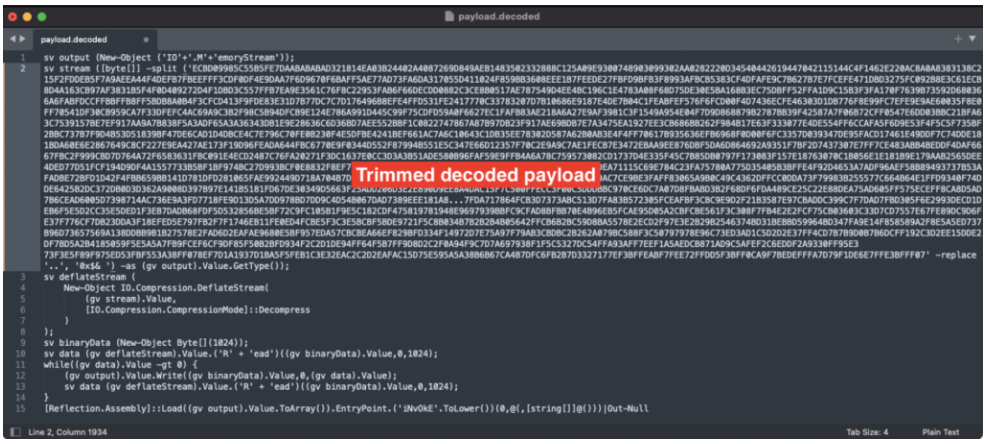


Figure 4: *Result of hex-decoding wis.txt into wis.ps1 (Source: Recorded Future)*

This script contains a large block of compressed data, which the script decompresses using the PowerShell IO.Compression.DeflateStream routine. The result is a .NET assembly (executable module), which the script loads into the current execution context through a call to Reflection.Assembly::Load.

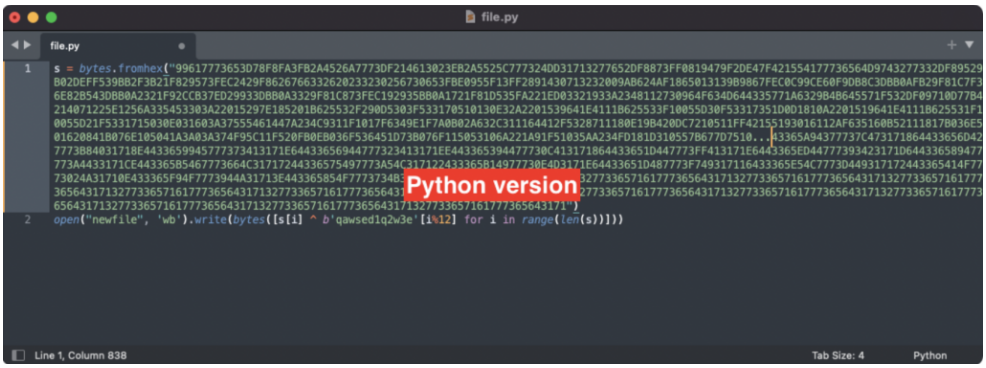


Figure 5: *The function for decoding and decrypting the reflective loader shellcode, rewritten to Python. (Source: Recorded Future)*

Once loaded, the .NET assembly decodes a block of data that has been XOR-obfuscated with the key “qawsed1q2w3e”. The result is a reflective loader shellcode that installs the IceBot Remote Access Trojan (RAT), previously known as Lizar, Tirion, and Diceloader.

Remote Access Trojan Analysis

The RAT executable dropped by “sketch_jul31a.ino” contains 2 command-and-control (C2) addresses: 199.80.55[.]66 and 207.246.92[.]213. Analysis of the fingerprints for these 2 IP addresses reveals an additional C2 server hosted on IP 185.250.151[.]126, and we were able to view the C2 control panel.

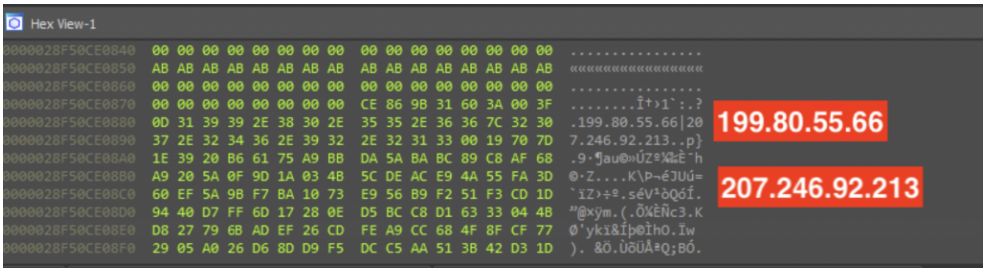


Figure 6*: Hex View snapshot of IceBot showing C2 IP addresses (Source: Recorded Future)*

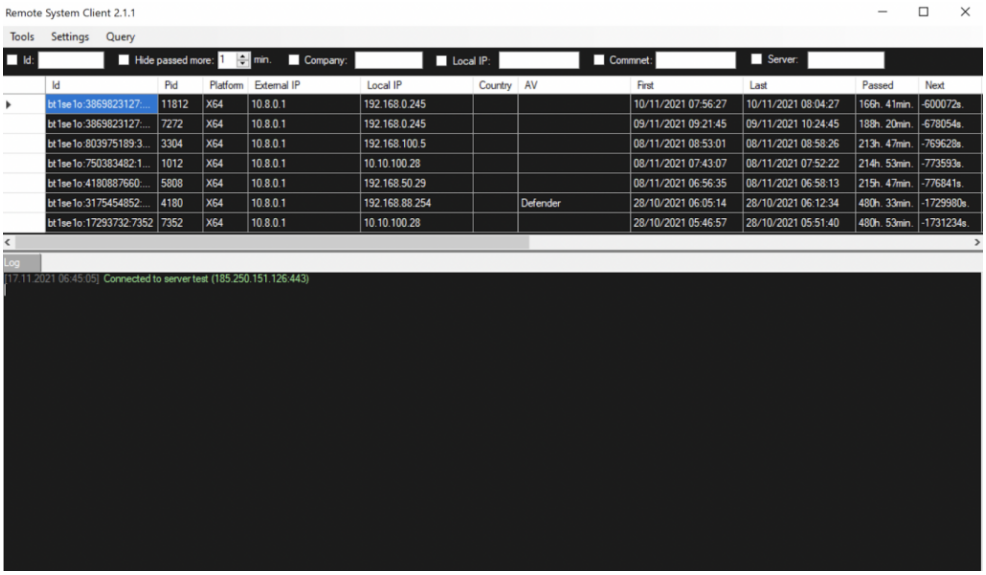


Figure 7: *The main window of the control panel of IceBot version 2.1.1. The IP address of the C2 server is 185.250.151[.]126:443. (Source: Recorded Future)*

The control panel displays a list of systems infected with the RAT, along with pertinent information about each installation, such as IP address, OS, process identifier (PID), antivirus software, communication history, and next update interval.

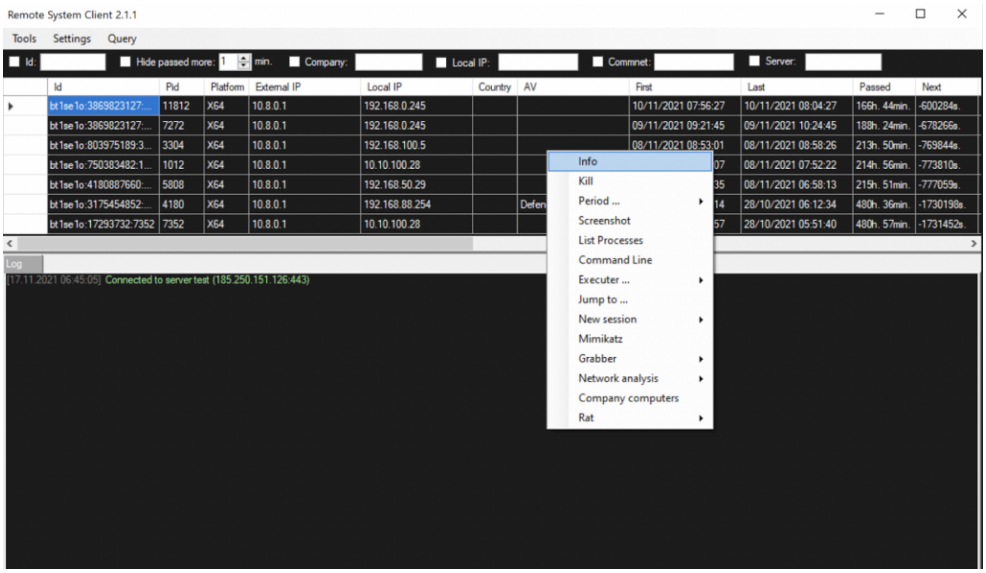


Figure 8: *The list of commands for the control panel of the RAT (Source: Recorded Future)*

Selecting an infected system and bringing up a context menu allows the threat actor to interact with the RAT and execute commands. As can be seen in Figure 8, several commands are available for managing and accessing information about the infected systems.

The IOCs for physical and in-memory files used in this attack are depicted in the table below.

File	SHA-256

sketch_jul31a.ino	f778dccfe13b8597a0a9cbb61a204c03f8e166d7f7d5a21dfcf03d56bd2505c3
wis.ps1	136095f5f529a891eabd8e04693c182f0701716fe051fa04825b5d2e0c85d1ae
.NET assembly	6a3912016f3b41c8cb67a2bc3a6fb2597065d065a809f33288fe838693b7f9a0
Shellcode	0a23ad00d0c62dccae0a759ad4853cd514abd176cfa85ba2665e30f7bdc8bcc0
RAT	09189108547ebf046c47f01f4645667e6816a126355ee963d5ad7b91167e4290

Outlook and Conclusions

The use of trojanized USB devices for keystroke injection is not a new technique, even for FIN7. Typically the attack targets specific persons with access to the computer systems of the intended victim company. As FIN7 has recently ventured into ransomware, it makes sense for them to look for alternative avenues of infecting computers that are monitored by layers of protective systems, such as firewalls, email scanners, proxy servers, and endpoint security. The tactics and techniques involved in trojanized USB attacks enable FIN7 actors to avoid many of these network-level and endpoint protections by dispensing with malware transmission over the network, minimizing the use of files on disk and employing multiple layers of encoding of the malware's scripts and executable code.

Pertinently, FIN7 recently created "Bastion Secure", a fake information security company, and employed system administrators to unknowingly assist in system exploitation. It is possible that trojanized USBs are being constructed and used by these administrators for penetration testing. Alternatively, they might also be providing trojanized USBs to clients or prospective clients through some form of ruse (for example, telling the client it contains documentation on the fake company's services). In either case, the clients or prospective clients could become victims of a trojanized USB attack, resulting in FIN7 gaining unauthorized remote access to systems within victims' networks.

Gemini Advisory Mission Statement

Gemini Advisory, a Recorded Future company, provides actionable fraud intelligence to the largest financial organizations in an effort to mitigate ever-growing cyber risks. Our proprietary software utilizes asymmetrical solutions in order to help identify and isolate assets targeted by fraudsters and online criminals in real-time.