# FIN7 Revisited: Inside Astra Panel and SQLRat Malware

March 20, 2019

Blogs

Blog

Despite the arrests of three prominent members of the FIN7 cybercrime gang beginning in January 2018, attacks targeting businesses and customer payment card information did not cease.

*By Joshua Platt and Jason Reaves*

Despite the arrests of three prominent members of the FIN7 cybercrime gang beginning in January 2018, attacks targeting businesses and customer payment card information did not cease.

The latest evidence involves the discovery of a new administrative panel and previously unseen malware samples that Flashpoint analysts are linking to this notorious group. Activity from this campaign dates from May to July 2018, but could go back farther to January 2018.

FIN7 has been active since at least 2015, targeting more than 100 U.S.-based companies in 47 states, as well as businesses in Europe and Australia. The U.S. companies affected were operating primarily in the hospitality, restaurant, and gaming industries, according to a U.S. Department of Justice press release last Aug. 1 announcing the arrest of three Ukrainian nationals alleged to be members of FIN7. Two were arrested in January in Germany and Poland, while the third—an alleged supervisor—was arrested in June in Spain.

FIN7, which has also used a backdoor linked to Carbanak—another prolific cybercrime outfit responsible for billions in losses in the financial services industry—has stolen more than 15 million payment card records from American businesses. The group, which operated behind a front company called Combi Security, has infiltrated more than 6,500 individual point-of-sale terminals at more than 3,600 business locations, according to the DoJ.

## New Attack Panel and Malware Samples

Flashpoint analysts recently uncovered a new attack panel used by this group in campaigns they have called Astra. The panel, written in PHP, functions as a script-management system, pushing attack scripts down to compromised computers.

Analysts discovered references to the FIN7 front company Combi Security in the Astra panel's backend PHP code, connecting the group to these campaigns. According to the DoJ indictments, Combi Security purported itself as a penetration-testing and security services company based in Russia and Israel. The DoJ alleges FIN7 portrayed Combi Security as a legitimate business in order to recruit other hackers to their operation.

The attackers gain an initial foothold on targeted machines via phishing emails containing malicious attachments. The emails are often industry-specific and crafted to entice a victim to open the message and execute the attached document.

One of the documents spreads what analysts are calling SQLRat, previously unseen malware that drops files and executes SQL scripts on the host system. The use of SQL scripts is ingenious in that they don't leave artifacts behind the way traditional malware does. Once they are deleted by the attackers' code, there is nothing left to be forensically recovered. This technique has not been observed in previous campaigns associated with FIN7.

The second new malware sample discovered is a multiprotocol backdoor called DNSbot, which is used to exchange commands and push data to and from compromised machines. Primarily, it operates over DNS traffic, but can also switch to encrypted channels such as HTTPS or SSL, Flashpoint analysts discovered.

The campaigns maintain persistence on machines by creating two daily scheduled task entries. The code, meanwhile, is still controlled by the FIN7 actors and may be leveraged in future attacks by the group.

## SQLRat Technical Details

SQLRat campaigns typically involved a lure document that included an image overlayed by a VB Form trigger. The documents contained a message asking the user to “Unlock Protected Contents,” below, while showing a message box displaying “US SEC Unlock document service.”

Image 1: An image of a document used in a typical campaign.Image 1: An image of a document used in a typical campaign.
Once a user has double-clicked the embedded image, the form executes a VB setup script. The script writes files to the path %appdata%\Roaming\Microsoft\Templates\, then creates two task entries triggered to run daily.

Image 2: Executing scripts on disk.Image 2: Executing scripts on disk.
The scripts are responsible for deobfuscating and executing the main JavaScript file mspromo.dot. The file uses a character insertion obfuscation technique, making it appear to contain Chinese characters.

Image 3: Obfuscated mspromo file.Image 3: Obfuscated mspromo file.
After deobfuscating the file, the main JavaScript is easily recognizable. It contains a number of functions designed to drop files and execute scripts on a host system.

Image 4: Deobfuscated mspromo script.Image 4: Deobfuscated mspromo script.=
The SQLRat script is designed to make a direct SQL connection to a Microsoft database controlled by the attackers and execute the contents of various tables. The script retrieves an item from the bindata table and writes the file to disk. This file appears to primarily be a version of TinyMet—an open source Meterpreter stager—but the actors have the option to store and execute any binary loaded into the table.

Image 5: Code responsible for downloading from the database.Image 5: Code responsible for downloading from the database.
Files associated with the SQLRat campaigns were all SFX RAR files. The files were 32/64-bit versions of a custom-built TinyMet along with a recon.js file. The 32-bit file contained an XOR embedded .exe file. The file was decoded out using the following:

Image 6: Deobfuscate embedded “TiniMet,” a customized version of TinyMet.Image 6: Deobfuscate embedded “TiniMet,” a customized version of TinyMet.
The result is a customized version of TinyMet. This version has limited usage; it does reverse TCP, XOR decodes the data retrieved for execution of the stager, and looks for TrendMicro processes. This file calls itself TiniMet:

Image 7: TiniMet looking for TrendMicro processes.Image 7: TiniMet looking for TrendMicro processes.
Analysts also uncovered a “TinyPS” stager:

After decoding out the blob, analysts found a PowerShell script. This script was similar to what was previously documented in the Trustwave report “Operation Grand Mars: Defending Against Carbanak Cyber Attacks.” The script contained the same XOR key but does not achieve persistence. It is only intended to create the Meterpreter session. The following is the PowerShell version of TiniMet:

Image 9: TinyPS PowerShell stager snippet.Image 9: TinyPS PowerShell stager snippet.

## DNSbot Technical Details

Analysts also uncovered subsequent campaigns associated with this panel. These campaigns were similar, but leveraged a document containing an embedded JavaScript-based DNSbot. The document contained the same MsgBox display, but this time there was a single file and task. The task name is similar to “Microsoft update service,” but the obfuscated JS file is dropped in %localappdata%\Storage:

Image 10: DNSBot drop location.Image 10: DNSBot drop location.

Additionally, the same US SEC Unlock document service is displayed, though the Microsoft update service task is deleted and replaced with the DNSbot.

Image 11: DNSbot task update.Image 11: DNSbot task update.

The JavaScript is heavily obfuscated. The first variable—a—is an array of obfuscated values. The second line contains a function to deobfuscate the values, while the call to that function is the second variable, b:

Image 12: DNSbot obfuscation.Image 12: DNSbot obfuscation.

A deobfuscated version of the DNS script is:

Image 13: DNSbot deobfuscated.Image 13: DNSbot deobfuscated.

A second deobfuscated testing script also matched components of the JavaScript embedded in the ASTRA docs, demonstrating the script’s multiprotocol use. The domain stats25-google[.]com was included in a report released by FireEye earlier in the year:

Image 14: Script relation to other reporting.Image 14: Script relation to other reporting.

The ASTRA backend was installed on a Windows server with Microsoft SQL. The panel was written in PHP and managed the content in the tables. It functioned as a script management system.

## Mitigations

Image 15: ASTRA attack panel partially redacted.Image 15: ASTRA attack panel partially redacted. Image 16: FIN7 front company name.Image 16: FIN7 front company name.

Image 17: The file types that were inserted, along with a table layout of the database with partial redaction.

Image 17: The file types that were inserted, along with a table layout of the database with partial redaction.

Flashpoint recommends watching for newly added Windows tasks, specifically those with a JScript switch. Also, monitor for attempts to delete the Microsoft update service.

Flashpoint also recommends implementing host-based detections for new files in %appdata%\Roaming\Microsoft\Templates\ with a dot extension, as well as implementing host-based detections for files in %appdata%\local\Storage\.

## Attachments and Downloads

The indicators of compromise (IOCs) for ASTRA panel, SQLRat, and DNSbot are available for download **here.**