05.13.19

Threat Report < https://www.deepwatch.com/blog_category/threat-report/>

Profile of an Adversary – FIN7

By Bryan Austin

Estimated Reading Time: 10 minutes

The majority of companies in either the Retail or Hospitality industries are [sadly] familiar with FIN7. We face many challenges in our various environments across multiple Enterprises.

Overview

This article, while focused on FIN7, is truly applicable to numerous enemies that we face. This article is aimed at defrocking a particular enemy and arming us all with better tools to defend against them.

It is also worth noting that the current syndicate attributed to FIN7 is not the same organizational composition that it once was. Thanks to **high profile arrests < https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100>** back in 2018.

Meet the Bad Guys

FIN7 has been known to be in operation since 2012 (although some estimates put them being active as far back as 2011), when TrustWave SpiderLabs first observed threat behavior that became much more prolific after 2015. Since then FIN7 has been identified by many organizations, including:

- FireEye – FIN7
- CrowdStrike – Carbon Spider
- Media – Carbanak Gang/Group

This group has suspected ties to Russian organized crime and has netted roughly $1 Billion USD in the last half-decade. Sources indicate a very loose connection with the Russian GRU.

The FIN7 group is increasingly adaptable not only to the geopolitical influences around them, but also quite capable in the environments they find themselves in. Additionally, the group has strong ties to Ukraine, where 3 members of the FIN7 group were arrested in 2018, though often times Russian cyber operations find their first deployment in Ukraine.

Targeting

The FIN7 group began by targeting banks in the Russian Federation, but in 2015 began to transition their targeting to a broader scope to include the Middle East, Europe and the United States. Currently, the group is known to target auto manufacturers, financial organizations, technology companies and innovators and hospitality, and retail organizations.

As of 2018, the main targets of this group are in the financial, retail and hospitality sectors. The US Department of Justice estimates put their intrusions at 6,500 POS terminals at 3,600 separate organizations. As a group, their targeting is clear, but at the onset of the attack it can seem less so.

Historically the group has targeted individuals who are listed in the organizations SEC

filings which can be viewed publicly by looking the business up in the **Edgar < https://www.sec.gov/edgar/searchedgar/companysearch.html>** filing database. Other individuals targeted for attack are customer service representatives who are attempting to resolve an issue they've identified from the attack.

Techniques

FIN7 begins the attack via malware delivery. This starts as a spear phishing email sent to the initial target. Generally the sentiment of the email is anger and accusations against the target's organization either due to a policy or a product. In short, the attacker is disguised as a highly dissatisfied customer.

The attacker performs a technique commonly called "amygdala hijacking" by eliciting a fear response in the target, and proceeds to reinforce the hijack by making threats and demands of the target which puts the individual on a defensive stance. Once the target responds, the actor then shifts to a deescalation tactics which eases the tension of the situation and causes the target to let their guard down in order to develop a more civil rapport with the target.

Additionally, the actor then begins to offer help to assist the target in resolving the issue which they themselves have created, thus "hooking" the target by making themselves seem to be the *hero*. The actor then begins to use the first name of the target to establish a sense of intimacy, common knowledge and familiarity.

The exchange then leads to an initial document delivery that is usually benign but possesses a tracking pixel that allows the actor to verify whether or not the target is opening attachments, and if so can provide initial visibility into the system of the target. The documents for this phase are often either blank or built for the campaign and correspond to the topic of conversation from the attacker.

The second document the attacker sends is usually the one with the actual payload. This document has either a VBA macro or an embedded OLE which persuades the target to run these in order to drop the first stage loaders. If the first stage loader is not dropped, the attacker resumes the threat tactic and escalates the issue to the target's supervisor which indicates an extensive amount of OSINT and revealing the extent the

attacker is willing to pursue a single individual.

Tools

Since FIN7 focuses on obtaining financial data, they rely heavily on malware to scrape consumer credit card information from Point Of Sale (POS) systems as well as other account information from databases in the network. The data stolen is then used to steal funds from victims and commit fraud, which is how the organization funds itself. There is also a possible connection to the 2016 SWIFT attacks, many of which have since been attributed to North Korea, however evidence of this is limited and open to interpretation.

The group typically follows a standard sequence of events: Spear phishing a target with a document loaded with a malware payload which as of May 2018 has been the Griffon payload, or a combination of SQLRat and DNSBot historically. These trends, observed by FireEye/Mandiant and Flashpoint respectively, always lead to the loading of an additional payload which is most commonly the Tinymet meterpreter payload to establish a beachhead in the network.

This begins the beaconing back to the Cobalt Strike servers. To establish persistence, the group then injects a scheduled task to reestablish the C2 connection to Cobalt Strike which historically is run twice a day. From there the adversary loads process injection tools or memory scrapers (commonly mimikatz) and pivots using tools like powersploit, RDP services, and PowerAdmin Exec.

A new development was the discovery of the Astra PHP Panel being used in conjunction with SQLRat. This discovery was posted in March 2019 from Flashpoint, was tracked back via the tie in established by the US DOJ; the Combi Security company was acting as a front and recruitment platform for the FIN7 group.

The malware most commonly associated with FIN7 is the Carbanak family, which the group gained as its common moniker. The Carbanak malware is not, however, exclusive to FIN7, nor do they use it explicitly. Currently, the group is using macro enabled word documents and spear phishing to deliver initial payloads that pull down second stage loaders like Spy. Sekur, although recently the Bateleur JavaScript

backdoor has come into fashion as of November 2017. Additionally, the group heavily targets the following CVEs:

- **CVE-2015-2545 < https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2545>**
- **CVE-2015-1701 < https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1701>**
- **CVE-2017-0199 < https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199>**

The group has begun branching out in using various malware versions and a full listing of the known IOCs for the new SQLRat and DNSBot additionally the Astra PHP panel are included at the end of this document as well as a list of links to the open source projects to allow for greater research.

Defensive Options

This adversary is persistent, capable, adaptable, and competent. That being said, there are a variety of options to begin defending your environment. The most critical aspect is detection. Due to FIN7's heavy use of spear phishing to deliver malicious MSFT Office documents to users, the most common exploits are scripts written in PowerShell or VBA and executed as macros in the documents. Blocking macro execution and enabling verbose logging from PowerShell (although storage space is expensive) is an excellent start to defend against this group and others who favor sophisticated phishing attacks.

Additionally, the usage of honey tokens in the environment can give a high-fidelity alert regarding access. In the case of FIN7, string searches can detect user credentials to a database or a fake credit card number. Tracking known indicators based on the actor's activity and setting alarms once IOCs are detected are also effective defense options.

Many organizations are able to track the activity in their environment, but taking a more proactive stance is optimal. First and foremost it is imperative to know where critical data lies. In this case, PCI/DSS scoping can act as an initial point of reference, but knowing where card data and financial data live can create a position of strength for

defenders.

Vulnerability management is also a critical piece to the holistic cyber defense. Though FIN7 does not actively exploit vulnerabilities at the time of this writing (e.g. CVE's 2545, 1701, & 0199), they can potentially begin to do so in the future. Vulnerability Management allows you to take an in depth stock of your IT assets. TTPs posted by intelligence and research groups can help prioritize patches based on exploits available for the vulnerability. However, it is important to note that many adversaries gain access to an organization not via high and critical vulnerabilities, but by chaining together a number of vulnerabilities considered to have low and medium severity.

Monitoring your systems for scheduled task changes is also critical. Be on the lookout for new scheduled tasks, especially those that use a .js file extension. If possible establish a host based detection for new files in the %appdata%\Roaming\Microsoft\Templates\ directory, particularly any with a .dot extension as well as new files in %appdata%\local\Storage\.

Ensuring that your toolsets and configurations are set up properly can not only deter threats, but also cause problems for adversaries. Properly configured EDR, script blocking can prevent things like JavaScript or macros to deploy while OS hardening guidelines modeled after groups like NIST and CIS will also cause more issues for attackers than most tools.

Finally, user education is a key component in every organization. Phishing is a highly used method for an initial foothold in organizations. According to Mimecast, 97% of breaches start with phishing. Until perfect phishing protection is created, users need to know how to recognize a malicious email, how to respond and what the company policies are for mitigating the risk. Good reporting can prevent a major campaign from being effective and can potentially cause a large portion of attacker infrastructure to be burned if reported correctly and responded to properly.

Recap of Minimum Baseline Defenses

Below is a recap of what should be considered minimum Enterprise defense and/or planning goals to reach first. The higher the number below the greater the impact to

defense, however there is typically a corresponding increase to the deployment lifecycle complexity.

1. Patch Relevant CVEs

- **CVE-2015-2545 < https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2545>**
- **CVE-2015-1701 < https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1701>**
- **CVE-2017-0199 < https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199>**

2. Log & Monitor on Enterprise Host Environment

- Task Scheduler jobs
- New Task Scheduler jobs
- %appdata%\Roaming\Microsoft\Templates\
- %appdata%\local\Storage\

3. Alert (& Groom) on the Monitored Enterprise Host Environment

- Task Scheduler jobs with .js extension
- New Task Scheduler jobs with .js extension
- %appdata%\Roaming\Microsoft\Templates*.dot
- %appdata%\local\Storage*.dot

4. Blocking macro execution in application userland with GPO

5. EDR JS and macro script blocking

Conclusion

In conclusion, FIN7 is an adversary worthy of concern with compromises resulting in the loss of up to a billion dollars. While this adversary is dangerous, basic security hygiene as outlined by both the NIST and CIS frameworks can reduce the actor’s

effectiveness in your environment as well as reduce the mean time to detection and mitigation. Additionally, knowledge of the group's tools, tactics, and processes allow defenders to more effectively predict the actions of the attacker, all of which can reduce your costs and the threats to your organization.

This tipper, as of late April 2019, contains new TTPs and IOCs that are worth a review by members. Here is the summary of those:

- Mapping the specific new malware signatures
- Mapping the specific new domains
- Astra IOC in particular
- Two years ago, FIN7 uploaded their Carbanak Malware to VirusTotal containing over 100k Lines of Code (LoC)

Indicators of Compromise (IoC)

Indicator – Payload delivery
Type – sha256
Signature – af60d8dfe30776b24823435b6e160d526ae500ce5583aee1ebbc909721d65120
Name – sqlRat

Indicator – Network activity
Type – ip-dst
Signature – 31.18.219.133
Name – N/A

Indicator – Payload delivery
Type – sha256
Signature – 151a90d31f218b91053656aa61bcdbcc98d2009b31b90de76d74fb3b163bb420
Name – sqlRat

Indicator – Network activity
Type – ip-dst

Signature – 185.117.89.134
Name – N/A

Indicator – Payload delivery
Type – sha256
Signature –
fe8f6d366546c2e935cf01aae7233e12445f10b815b28702e739e6951475f687
Name – sqlRat

Indicator – Payload delivery
Type – sha256
Signature –
d9ac4ef250a05ef8bd22c3227fd11df420cd663d5009b89a95466c1e0c301c1d
Name – sqlRat

Indicator – Payload delivery
Type – sha256
Signature – 2296e672f49cc9f8802571970a58fe86f8fafaf841fc44fe5c73e291eaa55daa
Name – sqlRat

Indicator – Network activity
Type – ip-dst
Signature – 185.15.25.79
Name – N/A

Indicator – Payload delivery
Type – sha256
Signature –
5236ec183f819c5e5cbe3d7a1f8e5b3478b23cebacc5daa501f563e1971bace5
Name – sqlRat

Indicator – Payload delivery
Type – sha256
Signature –
ee0cb9e6de83f807ccf9c3a02b384c1fb6e59f7de720f1eaf37141bf0487f5e6

Name – sqlRat

Indicator – Network activity
Type – ip-dst
Signature – 185.66.68.9
Name – N/A

Indicator – Payload delivery
Type – sha256
Signature – 860a5e83c509ec6615a722cd62ba47a506f115743eeb03cc94b3d2b03cc0ecc0
Name – DNSRat

Indicator – Network activity
Type – ip-dst
Signature – 5.10.40.54
Name – N/A

Indicator – Payload delivery
Type – sha256
Signature – 4c76e44d25c34620dc8cc019b96fd4da34d01fb4ac1e3b9f459c1ed6f80f05c4
Name – DNSRat

Indicator – Payload delivery
Type – sha256
Signature – 75a75224e81423663dd66ce20f845a58d523b0948c9d5cf135d599324512103e
Name – DNSRat

Indicator – Network activity
Type – ip-dst
Signature – 194.165.17.159
Name – N/A

Indicator – Payload delivery
Type – sha256
Signature – cfb152969e61e740fbb85c89239d3ff6a319657d5fc28a971e0592604174f4e7
Name – DNSRat

Indicator – Network activity
Type – domain
Signature – bigmoneyforus.com
Name – N/A

Indicator – Network activity
Type – domain
Signature – magicsoundmusic.com
Name – N/A

Indicator – Payload installation
Type – sha256
Signature – 3622154e566f4f3c87c81f6757d94707a7c74b1133866f8e5ebf2568f878c10f
Name – TiniMet

Indicator – Payload installation
Type – sha256
Signature – 2c73b87dbf21af4361b70b214b09cd92beb77ebcc6638be82b08e99fa564378a
Name – TiniMet

Indicator – Payload installation
Type – sha256
Signature – 6ef59d0ef5922c79bcc447c05af95de84a29e09048e12167994085eda3107a99
Name – TiniMet

Indicator – Payload installation

Type – sha256
Signature –
1439d301d931c8c4b00717b9057b23f0eb50049916a48773b173971351944424a
Name – TiniMet

Indicator – Payload delivery
Type – yara
Signature – rule astra_docs

```
{

meta:

description=ver1 of astra_docs"

author="JDP"
strings:
$header = {d0cf11e0a1b11ae1}
$a1 = "PROTECTED CONTENT" ascii wide nocase
$a11 = "CONTROL" ascii wide nocase
$b1 = "ConForm" ascii wide
$b2 = "Reanimator Extreme Edition" ascii wide nocase
$b3 = "Unlock document service." ascii wide nocase
$c1 = "Image1_DblClick" ascii wide nocase
$c2 = "img_click_DblClick" ascii wide nocase
$c3 = "img_click" ascii wide nocase
$c4 = "img_Click" ascii wide nocase
$c5 = "Forms.Image.1"

condition:
$header and all of ($a*) and 1 of ($b*) and 1 of ($c*)
}"
```

Links