FIN10

Anatomy of a Cyber Extortion Operation

PRIMARY GOAL TO STEAL: BUSINESS DATA, FILES, RECORDS, CORRESPONDENCE AND CUSTOMER PII

100-500
REQUESTED RANSOMS RANGED FROM 100 TO 500 BITCOINS

TARGETING CASINOS AND MINING ORGANIZATIONS IN NORTH AMERICA, WITH A FOCUS ON CANADA

100 = $124,000
BITCOIN RANSOM DEMAND
AS OF MID-APRIL 2017

SPECIAL REPORT

FireEye

CONTENTS

INTRODUCTION

FireEye has identified a set of financially motivated intrusion operations being carried out by an actor we have dubbed FIN10.

Within these clusters of activity, the attacker(s) have compromised organizations' networks and sought to monetize this illicit access by exfiltrating sensitive data and extorting victim organizations. We have observed FIN10 targeting organizations in North America, predominately in Canada.

FIN10 primarily relies on publicly-available software, scripts and techniques to gain a foothold into victims' networks. The threat group then posts proof of the stolen data on publicly accessible websites. Failure to pay the threat group could result in the public release of stolen data and potential disruption or destruction of the victim's information assets and systems.

In this report, we describe FIN10's activities and tactics, techniques and procedures (TTPs), and provide a glimpse into how they execute their operations.

TARGETING CASINOS AND MINING ORGANIZATIONS IN NORTH AMERICA, WITH A FOCUS ON CANADA

Background

FireEye has observed multiple targeted intrusions occurring in North America — predominately in Canada — dating back to at least 2013 and continuing through at least 2016, in which the attacker(s) have compromised organizations' networks and sought to monetize this illicit access by exfiltrating sensitive data and extorting victim organizations. In some cases, when the extortion demand was not met, the attacker(s) destroyed production Windows systems by deleting critical operating system files and then shutting down the impacted systems. Based on near parallel TTPs used by the attacker(s) across these targeted intrusions, we believe these clusters of activity are linked to a single, previously unobserved actor or group that we have dubbed FIN10.

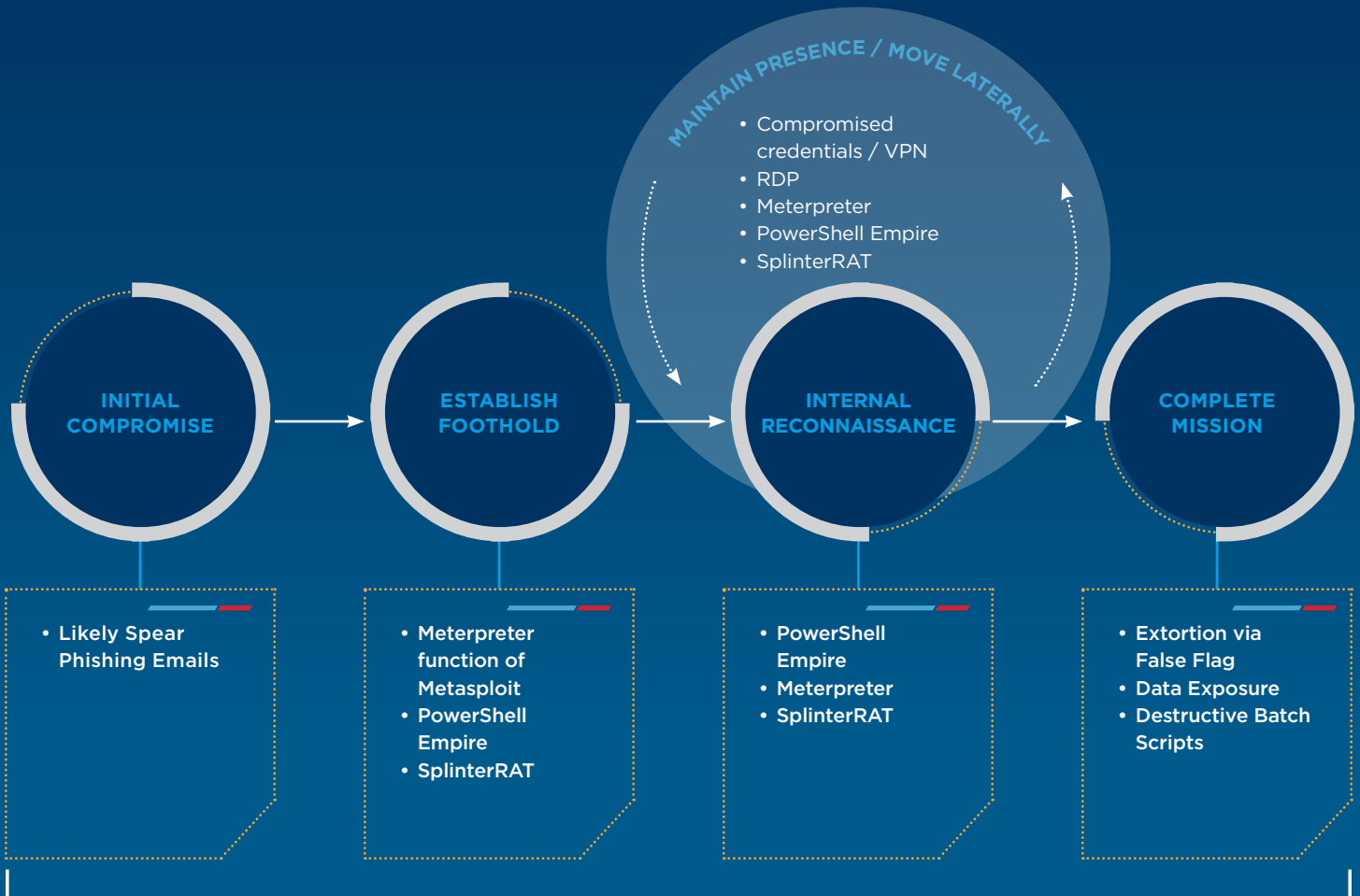
Targeting

Beginning as early as 2013 and continuing through at least 2016, we have observed FIN10 target organizations based in North America – predominately in Canada. Targeted organizations have primarily been casinos and mining organizations.

FIN10 Tactics, Techniques and Procedures

The following sections correspond to the attackers' TTPs and are organized by the stages of the targeted attack lifecycle (See Figure 1).

Figure 1. TTPs as organized by targeted attack lifecycle model



Initial Compromise

In the majority of intrusions attributed to FIN10, there was insufficient evidence to determine the initial infection vector. However, in at least two intrusions, FIN10 leveraged spear phishing emails with malicious attachments, making it plausible that this methodology was used across all breaches.

- In both instances where the initial compromise was identified, the attacker(s) used social engineering and specifically crafted lures to entice victims to click on a link that directed them to a FIN10-controlled server. The server hosted malicious artifacts that ultimately executed code on one or more systems. In these instances, the malicious code were downloaders that beaconed out to attacker-controlled infrastructure.
- In one intrusion, the phishing email referenced an updated holiday schedule for organizational staff. The embedded URL pointed to a malicious HTML Application (HTA) file.
- In another intrusion, a phishing email referenced an employee questionnaire. The embedded URL pointed to a Word Open XML Macro-Enabled Document file (DOCM) file.
- Of note, FIN10 likely uses LinkedIn — among other social media and public data sources — to support the crafting of phishing emails that appear legitimate.

Early Stage Malware

The attacker(s) primarily relied on publicly-available software, scripts and techniques to gain a foothold into victims' networks.

Meterpreter

FIN10 used Meterpreter as the primary method of establishing an initial foothold within victim environments. However, in one case, we also observed the group use Splinter Remote Access Trojan (SplinterRAT).

Meterpreter, short for the Meta-Interpreter, is an advanced payload included in the Metasploit Framework. It provides functionality that would otherwise be difficult to implement in assembly by allowing developers to write their own extensions in the form of DLL files that can be uploaded and injected post exploitation. Meterpreter and most of its extensions are executed in memory, thus largely evading detection by standard anti-virus. Due to its public availability, FireEye iSIGHT Intelligence has observed multiple threat actor groups use Meterpreter in targeted attacks across various industries.

PowerShell

Threat actors often use PowerShell to write their own malicious utilities, which typically decrease chance of detection by popular endpoint security controls. When scripts are executed with PowerShell, the scripts run inside powershell.exe (locally) or wsmprovhasost.exe (remotely), both of which are often trusted processes. PowerShell provides threat actors with the ability to create scripts that exceed the capabilities of a standard Windows shell, batch files and VBS files.

In the majority of cases, we observed FIN10 leveraging PowerShell Empire (a pen-testing tool that utilizes PowerShell) for **elevated persistence**, mainly by utilizing the Registry and Scheduled Task options; however, in at least one intrusion, we observed FIN10 use **S4U tasks** for this purpose, although this method was likely abandoned in favor of PowerShell Empire once it was released.

In at least one instance, PowerShell Empire was used to install a randomly named service that executed a Meterpreter PowerShell script, which in turn executed malicious .bat files. The created batch scripts typically contained PowerShell commands for 32-bit and 64-bit operating systems and upon execution could connect to an attacker command and control (C2) server.

We have also observed FIN10 using PowerShell to load Metasploit Meterpreter stagers into memory.

Lateral Movement and Internal Reconnaissance
FIN10 routinely leverages Windows Remote Desktop Protocol (RDP) to access systems within the environment. More specifically, attacker(s) leveraged RDP to authenticate to internal systems that were configured to allow ingress RDP connections from systems residing outside organizational firewall perimeters. Similarly, we have observed FIN10, in at least two instances, use single-factor protected VPN to connect remotely to victim networks after stealing credentials.

In multiple events, FIN10 also leveraged functionality within the PowerShell script Meterpreter backdoor to perform internal reconnaissance and move laterally throughout the environment. Further analysis found the attacker(s) used Meterpreter functionality to enumerate users on remote systems and execute additional PowerShell functionality. In at least one network compromise, attacker(s) moved laterally using the Local Administrator account and deployed Metasploit Meterpreter stagers and SplinterRAT instances on targeted systems. SplinterRAT is an open-source red team collaboration framework. It is a Java-based framework that was publicly available and relatively easy to implement with limited knowledge. In addition, SplinterRAT provides capabilities such as file system browsing, file upload and download, execution of shell commands and beaconing in case of communication issues with a C2 server. Both the Metasploit related backdoors and SplinterRAT instances were programmed to connect to attacker-controlled C2 servers.

We have regularly observed FIN10 use scheduled tasks as a persistence mechanism. For example, in at least one intrusion we observed FIN10 create a scheduled task named **"C:\Windows\System32\Tasks\Updater"**, which executed a PowerShell script encoded in the Windows registry. The script was configured to communicate with attacker-controlled C2 infrastructure.

System Disruption
FIN10 routinely deploys destructive batch scripts intended to delete critical system files and shutdown network systems. Network degradation activity typically consisted of the attacker(s) creating scheduled tasks on multiple systems within the targeted network environment to disrupt the normal operations of those systems by rendering their operating systems unusable. In at least two instances, FIN10 created a scheduled task that used the command shown in Figure 2 to delete the Windows directory using the Microsoft robocopy tool on critical systems within the environment.

```
mkdir "C:\emptydir"
robocopy "C:\emptydir" "C:\windows\system32"/MIR | shutdown /s /t 1800
```

Figure 2. Example of scheduled task created to disrupt normal operations

While this TTP could potentially be viewed as an attempt by FIN10 to obfuscate malicious activity, the resulting effects of these scheduled tasks were easily detected, suggesting that these activities were intended to lend credence to the perceived threat.

End-Stage Operations

We believe the primary goal of this threat group is to steal corporate business data, files, records, correspondence and customer PII, and then to extort victim organizations for non-release of the stolen data. The threat group posts proof of the stolen data on publicly accessible websites. Failure to pay the threat group could result in the public release of stolen data and potential disruption or destruction of the victim's information assets and systems.

Extortion

In all but one targeted intrusion we have attributed to FIN10, the attacker(s) demanded a variable sum payable in Bitcoin for the non-release of sensitive data obtained during network reconnaissance stages (See Appendix for sample extortion email).

- Requested sums ranged from 100 to 500 Bitcoins (roughly $124,000 to $620,000 as of mid-April 2017).
- Notably, we identified at least two victims who were issued the same Bitcoin address.
- In the first incident Mandiant investigated that was attributed to FIN10, the attacker(s) did not extort the targeted organization. However, it is plausible that the group was still in the process of honing its TTPs.

Data Exposure

FIN10 likely uses a combination of copy tools and file transfer utilities to both harvest and stage sensitive data. Data exposure is accomplished routinely using openly-accessible websites such as "pastebin.com," "justpaste.it," and "thepiratebay.se." We have also observed the group using popular cloud file sharing/storage solutions, such as Dropbox, to receive stolen data in extortion attempts

Links to the leaked data are initially kept private and provided solely to the victim organization as proof of the authenticity of the compromise. We have seen FIN10 heavily leverage the "justpaste.it" service for these purposes.

Narrative & Messaging

Attacker(s) in all instances utilized a false flag — a term used to describe covert operations that are designed to deceive in such a way that activities appear as though they are being carried out by entities, groups or nations other than those who actually planned and executed them.

- Based on open-source reporting, the attacker(s) in at least one intrusion self-identified as the "Angels_Of_Truth," and claimed the attacks on the victim were in reciprocity for Canada-imposed economic sanctions on Russia. The quality of the Russian-language posts, however, was considerably poor and very similar to output obtained from online translating solutions, making it likely the attacker(s) are not native Russian speakers and were using this narrative to mislead attribution attempts.
- The attacker(s) more commonly used a moniker associated with a Serbian hacktivist group dubbed "Tesla Team." Given the vast differences in external targeting calculus — targeted industry verticals by FIN10 as compared to political organizations, non-governmental organizations and websites of anti-Serb organizations targeted by Tesla Team — and inconsistencies in tradecraft, we doubt that the Serbian hacktivist group Tesla Team (previously active in 2013) is associated with FIN10.
  - In at least one intrusion, we observed the group abandon the moniker Tesla Team in the group's last correspondence to the targeted victim and adopt the moniker "Anonymous Threat Agent."
- Emphasis in regional targeting of North American-based organizations could possibly suggest the attacker(s) familiarity with the region.

FIN10 also seeks to increase its leverage by sending multiple emails to staff and board members of the victim organizations, notifying them of the breach and potential consequences for nonpayment. FIN10 also informs open-source blogs about breaches in a likely effort to publicly expose these breaches and apply additional pressure on affected organizations to acquiesce to extortion demands. Alternatively, it is just as plausible FIN10 does this to simply maximize exposure for victims who do not pay. Notably, we have also observed the group engage local journalists to publicize these breaches.

Outlook

500 = $620,000
BITCOIN RANSOM DEMAND
AS OF MID-APRIL 2017

100-500
REQUESTED RANSOMS RANGED FROM 100 TO 500 BITCOINS

The relative degree of operational success enjoyed by FIN10 makes it highly probable the group will continue to conduct similar extortion-based campaigns at least in the near term. Notably, we already have some evidence to suggest FIN10 has targeted additional victims beyond currently confirmed targets.

Furthermore, while FIN10 is predominantly financially motivated, as evidenced by its preferred monetization technique (i.e., extortion), it is plausible the group is also motivated, at least in part, by ego. For instance, the group's willingness to contact cyber security bloggers is likely the result of at least two motivational factors:

1	2
To further the groups operational objectives, likely by putting increased pressure on targeted victims to acquiesce to now public extortion demands	To gain some degree of notoriety and public exposure of the group's campaigns

While the secondary motivation may be a necessary byproduct of the first, more primary objective, desire to gain notoriety could potentially influence the group's decision-making calculus.

Lastly, while FIN10 has seemingly only targeted organizations within two industry verticals, it is possible the group has previously or will in the future expand their regional and industry-specific targeting. Historically, we have seen this type of threat activity — cyber attacks resulting in the theft or compromise of sensitive data to be leveraged in extortion plots — affect multiple targeted verticals.

Lessons Learned

from investigating FIN10 and other disruptive breaches

Responding to disruptive breaches such as FIN10 is challenging and not easy to plan for given the dynamic nature of these attacks and the attacker(s). Unlike breaches where a containment plan may be able to stop an attacker from stealing more information, in these disruptive instances the damage may have already been done by the time the attacker(s) contacts the victim organization. Therefore, a different response to these incidents might be required. The following ten lessons from our incident response engagements may help organizations deal with disruptive attacks, including those from groups such as FIN10:

1

CONFIRM THERE IS A BREACH

Just because someone claimed they hacked you doesn't necessarily make it true. Empty extortion attempts are not uncommon. Examine your environment for evidence of compromise before considering to pay the ransom. Usually FIN10 provides data as proof (see the 'Data Exposure' section), so confirm that the data is real and determine if it came from your environment.

2

REMEMBER THAT YOU'RE DEALING WITH A HUMAN ADVERSARY

Humans can be unpredictable and they may react out of emotion. Carefully consider how an attacker will react to your action or inaction. They can become more aggressive if they get upset. They may back down and allow for more time if they believe you are trying to meet their demands.

3

TIMING IS CRITICAL

You need to validate and scope the breach as quickly as possible. This may require the team working nights and weekends, so be careful of fatigue and burnout. You may need to approve emergency change requests within short order.

4

STAY FOCUSED

It's easy to get distracted. Evaluate whether the tasks you are taking on will help mitigate, detect, respond to or contain the attack. Remember that you're racing against the clock. Focus on the must-haves instead of the nice-to-haves and understand that you may need to deploy a number of temporary solutions to address the attack.

5

CAREFULLY EVALUATE WHETHER TO ENGAGE WITH THE ATTACKER(S)

Attackers do not always expect a response. If you decide to respond, limit the interactions and carefully consider everything you say. Consider involving law enforcement and legal counsel in all communications.

PRIMARY GOAL TO STEAL:
BUSINESS DATA, FILES, RECORDS, CORRESPONDENCE AND CUSTOMER PII

6
ENGAGE THE EXPERTS BEFORE A BREACH

You will need forensic, legal and public relations support to get through a disruptive breach. Identify partners before the breach and get them on retainer.

7
CONSIDER ALL OPTIONS WHEN ASKED TO PAY A RANSOM

Understand that paying the ransom may be the right option, but there are no guarantees the attacker(s) won't come back for more money or simply leak the data anyway. Include experts in the decision-making process and understand the risks associated with all options.

8
ENSURE STRONG SEGMENTATION AND CONTROLS OVER YOUR BACKUPS

Most organizations have mature backup policies so they can recover quickly in the event of a system failure. However, it's common for the systems containing backups to be part of the same environment compromised by the attacker. Tighten access to your backup environment to mitigate the risk of an attacker accessing the system using compromised credentials and destroying your backups.

9
AFTER THE INCIDENT HAS BEEN HANDLED, IMMEDIATELY FOCUS ON BROADER SECURITY IMPROVEMENTS

Regardless of the outcome, you should ensure that attackers such as FIN10 cannot come back in and do more damage. You also don't want a second attacker targeting you because they think you are willing to pay a ransom. Ensure you understand the full extent of the breach and implement both tactical and strategic actions to prevent future attackers from gaining access.

10
IF YOU KICK THEM OUT, THEY MAY TRY TO COME BACK IN A DIFFERENT WAY

Don't forget to operationalize and enhance the temporary solutions that were deployed to immediately address the attack. Conduct penetration testing and Red Team assessments to validate your security controls, identify vulnerabilities and fix them immediately.

Conclusion

Although FireEye has observed FIN10 primarily targeting casinos and mining organizations in North America (with a focus on Canada), all organizations from around the world must be prepared to detect and respond to threats from this group and other bad actors.

We believe the primary goal of FIN10 is to steal corporate business data, files, records, correspondence and customer PII for the purposes of extorting victim organizations for the non-release of the stolen data. Enterprises that are contacted by a group claiming to have their data will want to carefully assess if an incident has actually occurred. In the case of FIN10, we have observed them posting proof of the stolen data on publicly accessible websites.

When dealing with these types of extortion-based attacks, we strongly recommend that organizations work quickly, stay focused, consider all options and potentially involve forensic, legal, law enforcement and public relations experts before taking any actions or communicating with the threat actor. Strong segmentation and controls over backups will help organizations to quickly recover from a breach. Additionally, when the incident has been resolved organizations should focus on broader security improvements and ensuring the threat actor cannot come back in a different way.

Appendix – Sample Extortion Email

The text below is a redacted email that FIN10 sent to one of their victims.

At this point your company has two options:

1. Meet our demand and pay the one time price of 500 BTC (Bitcoin)
   -all of the stolen data is permanently deleted, none of it gets posted on the internet, your computer network will remain safe and functional and your organization wont be bothered again.
   -Bitcoin transactions are anonymous no one will know you cooperated

2. Refuse to pay and let the deadline pass:
. if payment is not received in 10 days or less the first data dump of your company/patrons data will be posted all over the internet for the world to see. we will also send emails to each one of your customers/patrons directing them to see their leaked data on the internet.
. if still after another 72 hours payment isnt received, a 2nd data dump will happen, and every 72 hours after that until all other data listed above along with much more will be leaked and available for download on both the dark web and on torrent sites to anyone who wants to download it.
. Your computer network will be taken down in a large scale attack and will require weeks if not months to get functional again.

It is not our goal to cripple your company, our goal is simply to receive 500 BTC (Bitcoin). Calling the authorities might seem like an obvious choice. However realize that they will not be able to help you in this case as they have no jurisdiction where we are. And bringing it to them makes your sensitive situation that much more public.
make the right choice.

-TeslaTeam

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.