www.sisainfosec.com

SISA ProACT MDR Solution: Threat Group: FIN7

Threat Severity: High
Published on: 31st Jan 2023

www.sisainfosec.com

AN IN-DEPTH LOOK AT THE APT, FIN7

Overview of the Group:

FIN7 is a financially motivated threat group that has been active since 2013 primarily targeting the U.S. retail, restaurant, and hospitality sectors, often using point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. Since 2020 FIN7 shifted operations to a big game hunting (BGH) approach including use of REvil ransomware and their own Ransomware as a Service (RaaS), Darkside. FIN7 may be linked to the Carbanak Group, but there appears to be several groups using Carbanak malware and are therefore tracked separately.

TACTICS & TECHNIQUES 2022:

Initial Access

1. **Exploiting Microsoft Exchange Vulnerabilities: [CVE-2020-0688, CVE-2021-42321]**

For using exploit against Exchange vulnerability, this threat group purchases the stolen accounts of OWA on specific internet markets and developed tailored scripts to automate the exploitation process.

2. **BadUSB attacks : [T1458, T1474.002**]

Social engineering attacks which involve convincing potential victims to plug in USB flash drives containing malicious code into their computers. FIN7's BadUSB attacks, they have been known to modify their USBs to act as a keyboard and simulate keyboard strokes to invoke a malicious Powershell command
They have recently added a new SSH-based backdoor, which allows them to steal confidential files from the target system using reverse SSH connections (SFTP)

3. **Spear Phishing [T1566.001/T1566.002/T1204.002]**

The group members distribute spam e-mails by demanding payment with an attached malicious file .docm. This file has a macro script which opens a backdoor in a victim's device.

4. **Mass scale scanning**

Attackers directly scanned and exploited hundreds of Microsoft Exchange servers with Proxyshell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) vulnerabilities.
Threat actors exploit ProxyShell vulnerabilities to establish remote PowerShell sessions on the vulnerable Exchange Servers. There are several ways that attackers have used the PowerShell to create web shells.
Following vulnerabilities are observed to be exploited:

- CVE-2021-34473 : Microsoft Exchange Server Remote Code Execution(RCE) vulnerability that does not require any user action or privilege to exploit ;
- CVE-2021-34523 : Microsoft Exchange Server Elevation of Privilege Vulnerability after authentication
- CVE-2021-31207 : Microsoft Exchange Server security feature bypasses vulnerability flaw that allows attackers to gain administrative access.

5. **Auto-SQLi Module[S0225]**

In addition to the auto-exploitation of Microsoft Exchange vulnerabilities, threat actors also developed a module for the SQL Injection attacks. In cases where an attack does not meet a definitive result and cannot be proceeded within the server, the target victim is marked for scanning by SQLMap tool. Ultimately, all URLs are scanned to acquire if there are any SQL injection vulnerabilities

6. **Using compromised Remote Desktop Protocol (RDP) credentials to login to a target server[T1021]**

The following windows process chains were initiated post logon:

```
rdpinit.exe
  ↳ notepad++.exe
    ↳ cmd.exe
      ↳ powershell.exe
rdpinit.exe
  ↳ notepad++.exe
    ↳ cmd.exe
      ↳ rundll32.exe
```

Execution

1. **Carbanak [S0030/T1553.002**]

FIN7 group consistently used the multi-functional tool known as Carbanak to open backdoors on victim computers. It has capabilities such as port forwarding, RDP/VNC access, command line access, file transfer, and more

2. **Icebot, Lizar, and Tirion:**

FIN7 threat actors are currently developing this new remote access Trojan (RAT) called Icebot . This tool has similar capabilities to Carbanak, Lizar, and Tirion.

The functions of Tirion/Lizar malware are the following:

- Information Gathering
- Taking Screenshot
- List Running Processes
- Command / Code Execution
- Process Migration
- Mimikatz Execution
- Password Grabbing
- Active Directory and Network Recon

3. **Use of Dynamic Powershell Scripts [T1059.001**]

The group uses highly dynamic PowerShell scripts developed by their own development team to produce executables for the deployment of fresh instances

The deployment pack (containing scripts, along with instructions and public-private keys) used by threat actors often includes a generic dropper. Some of the file names used in these scripts **ClearTemp.ps1**

FIN7 PowerShell Execution from 2019 to 2021:

2019

- cmd.exe /c start %SYSTEMROOT%\system32\WindowsPowerShell\v1.0\powershell.exe -noni -nop -exe bypass -f <REDACTED>/ADMIN$/temp/wO9EBGmDqwdc.ps1
- powershell.exe -ex bypass -file C:\windows\temp\fdddu32.ps1

2020

- `powershell.exe -ex bypass -f c:\users\public\temp\AC-Win10w-x64.ps1`
- `powershell.exe -ex bypass -f C:\Users\Public\Videos\AC-Bot-x64.ps1`

2021

- cmd.exe /c start %SYSTEMROOT%\system32\WindowsPowerShell\v1.0\powershell.exe -noni -nop -exe bypass -f \\<REDACTED>\Admin$\c5k3fsys.3bp.ps1
- powershell.exe -ex bypass -f pkit.ps1
- powershell.exe -ex bypass -f cube.ps1

Observed payloads loaded by FIN7's POWERTRASH include CARBANAK, DICELOADER, SUPERSOFT, BEACON and PILLOWMINT. POWERTRASH is a uniquely obfuscated iteration of a shellcode invoker included in the **PowerSploit** framework available on GitHub

Collection

When the Proxyshell attack is successful, post-exploitation steps are automatically executed, including extracting all emails from Active Directory (AD) and collecting all Exchange Server information.

1. **Email Collection from Active Directory [T1114/T1119]**
2. **Collecting all Exchange Server information. [T1119]**

The team gathers information on potential victims, including their current revenue, number of employees, headquarter details, domain, and website.

Victim Prioritization

Companies with the highest revenue are prioritised to get profitable operations. The FIN7 group uses various information sources, including **Owler Data, DNB, Zoominfo, and Crunchbase** to select victims. Once they have evaluated the data obtained from services, they can target the victims accordingly. The group also uses services like **Similarweb, Mustat, and Alexa** to evaluate analytics data including traffic size of victims' websites.
FIN7 group uses a variety of Google Dorks keywords to scan the internet to find fresh targets for their attack modules.

Command and Control

1. Cobaltstrike [S0154]

Cobaltstrike payloads were often combined with PowerShell scripts for post-exploitation

2. SSH-based Backdoor [T1021.004]

FIN7 mostly uses an SSH-based Backdoor to manage the remote access and transfer files besides Cobalt Strike. The remote server acts as a proxy, allowing the FIN7 group to operate the SSH connection through an Onion domain

Exfiltration

1. Use of the rclone tool to download files to cloud storage T1537

The group members of FIN7 use the rclone tool for downloading the big files from the victim's system to cloud storage such as Mega.nz and Azure Blob Storage. The file depicts the rclone configuration found among other files owned by FIN7

Data Encryption to extract monetory compensation [T1486]

After infiltrating the victim's network, they steal and encrypt files using a stealer malware, and determine the ransom amount based on the company's revenue.

Defense Evasion

- Malicious code was interspersed **with random junk code** to evade static detections (T1001.001)
- PowerShell command obscured through custom obfuscation mechanism :

```
Text1 = "/3/3.1/2.1,7/2/2.0/3+4+5/4/2*3,7.0,7/2/2.1/4.0,6/3/3.0/3.0+5/4+5-
9/4.1+5/4/3*3,7.0,6/3/2*32723272724122923262416182523101121172621252225182524292425162614162722142027101122122323 10"
TextCrypt = Encryption(MakeCryptoText(TextUnShifter(Text1)), False)

pwsh_command = TextCrypt & FileName & ".ps1"
objWSH.Run pwsh_command, 0, True
FSO.DeleteFile FileName & ".ps1"
```

Ransomware Affiliations

As per the evidence collected, FIN7 threat group are found to be affiliated with ransomware groups such REvil, LockBit, and the Darkside Ransomware.

Once the threat actors have gained access to a victim's network, they typically install backdoors to facilitate their ransomware attacks and ensure they are able to collect ransom payments. After the attack is complete, the group may resell or reuse the access they have gained to launch additional attacks. Even if the victim takes steps to remove the initial vulnerabilities, the existing backdoors can continue to provide a means for future infections. This allows the threat actors to repeatedly target the same victim, potentially causing significant damage and disruption

Softwares Used:

AdFind

AdFind is a free command-line query tool that can be used for gathering information from Active Directory.

BOOSTWRITE

BOOSTWRITE is a loader crafted to be launched via abuse of the DLL search order of applications used by FIN7.

Carbanak
Carbanak is a full-featured, remote backdoor used by a group of the same name (Carbanak). It is intended for espionage, data exfiltration, and providing remote access to infected machines.

Cobalt Strike
Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz.

CrackMapExec
CrackMapExec, or CME, is a post-exploitation tool developed in Python and designed for penetration testing against networks. CrackMapExec collects Active Directory information to conduct lateral movement through targeted networks.

GRIFFON
GRIFFON is a JavaScript backdoor used by FIN7.

HALFBAKED
HALFBAKED is a malware family consisting of multiple components intended to establish persistence in victim networks.

JSS Loader
JSS Loader is Remote Access Trojan (RAT) with .NET and C++ variants that has been used by FIN7 since at least 2020.

Lizar
Lizar is a modular remote access tool written using the .NET Framework that shares structural similarities to Carbanak. It has likely been used by FIN7 since at least February 2021.

Mimikatz
Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.

Pillowmint
Pillowmint is a point-of-sale malware used by FIN7 designed to capture credit card information.

POWERSOURCE
POWERSOURCE is a PowerShell backdoor that is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. It was observed in February 2017 in spearphishing campaigns against personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. The malware was delivered when macros were enabled by the victim and a VBS script was dropped.

PowerSploit

PowerSploit is an open source, offensive security framework comprised of PowerShell modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration.

RDFSNIFFER

RDFSNIFFER is a module loaded by BOOSTWRITE which allows an attacker to monitor and tamper with legitimate connections made via an application designed to provide visibility and system management capabilities to remote IT techs.

Hunting Queries for FIN7:

Event Type	Event ID	Logic Used
Powershell Execution	4688	cmd.exe /c start %SYSTEMROOT%\system32\WindowsPowerShell\v1.0\powershell.exe -noni -nop -exe bypass -f <REDACTED>/ADMIN$/temp/wO9EBGmDqwdc[.]ps1
		cmd.exe /c start %SYSTEMROOT%\system32\WindowsPowerShell\v1.0\powershell.exe -noni -nop -exe bypass -f \\<REDACTED>\Admin$\c5k3fsys.3bp[.]ps1
		powershell.exe -ex bypass -f pkit.ps1
Enumeration using built-in Windows commands as well as POWERSPLOIT and Kerberoasting PowerShell modules	4688	cmd.exe /C net group "Domain Admins" /domain cmd.exe /C quser powershell.exe -c import-module C:\Users\Public\kerberoast_hex.ps1; Invoke-Kerberoast -OutputFormat HashCat > hash.txt powershell.exe -ex bypass -c import-module C:\Users\Public\kerberoast_hex.ps1; Invoke-Kerberoast -OutputFormat HashCat

		powershell.exe -ex bypass -f pkit.ps1
PowerShell command obfuscation	4103, 4104	Text1 = "/3/3.1/2.1,7/2/2.0/3+4+5/4/2*3,7.0,7/2/2.1/4.0,6/3/3.0/3.0+5/4+5-9/4.1+5/4/3*3,7.0,6/3/2*32723272724122923262416182523101121172621252225182524292425162614162722142027101122122323 10" TextCrypt = Encryption(MakeCryptoText(TextUnShifter(Text1)), False) pwsh_command = TextCrypt & FileName & ".ps1" objWSH.Run pwsh_command, 0, True FSO.DeleteFile FileName & ".ps1"
Execution of obfuscated loader	4688	powershell.exe -ex bypass -f cube.ps1
Command line used to load FIN7 TERMITE		RunDll32.* TstDll.dll,TstSec 11985756
Payloads used to Scan CVE-2020-0688		GET /owa/auth/logon.aspx?url=https%3a%2f%2f1%2fecp%2f
		GET /owa/auth/logon.aspx?url=https://1/ecp/
CVE-2021-42321		Log type= Application Source= "MSExchange Common" Entry type= Error Message= *BinaryFormatter.Deserialize*
		4 posts in a chain Source IP: Public AND agent="ExchangeServicesClient/15.01.2308.008" AND url="https://www.reddit.com/EWS/Exchange.asmx" AND method="POST"
	4688	user LIKE "%DefaultAppPool%" AND parent_process_name LIKE "%w3wp.exe%" AND process_name LIKE "%cmd%"

MITRE Map

Initial Access	Execution	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Resource Development	Command and Control	Impact
T1195.002: Compromise Software Supply Chain	T1059: Command and Scripting Interpreter	T1027: Obfuscated Files or Information	T1110.002: Password Cracking	T1012: Query Registry	T1021.001: Remote Desktop Protocol	T1113: Screen Capture	T1583.003: Virtual Private Server	T1071.001: Web Protocols	T1491.002: External Defacement
T1199: Trusted Relationship	T1059.001: PowerShell	T1027.005: Indicator Removal from Tools	T1555.003: Credentials from Web Browsers	T1033: System Owner/User Discovery	T1021.004: SSH	T1213: Data from Information Repositories	T1588.003: Code Signing Certificates	T1090: Proxy	
T1566.001: Spearphishing Attachment	T1059.003: Windows Command Shell	T1036: Masquerading	T1558.003: Kerberoasting	T1057: Process Discovery		T1560: Archive Collected Data	T1588.004: Digital Certificates	T1095: Non-Application Layer Protocol	
T1566.002: Spearphishing Link	T1059.005: Visual Basic	T1036.003: Rename System Utilities		T1069: Permission Groups Discovery			T1608.003: Install Digital Certificate	T1105: Ingress Tool Transfer	
	T1059.007: JavaScript	T1055: Process Injection		T1069.002: Domain Groups			T1608.005: Link Target	T1132.001: Standard Encoding	
	T1204.001: Malicious Link	T1070.004: File Deletion		T1082: System Information Discovery				T1573.002: Asymmetric Cryptography	
	T1204.002: Malicious File	T1140: Deobfuscate/ Decode Files or Information		T1083: File and Directory Discovery					
	T1569.002: Service Execution	T1218.010: Regsvr32		T1087: Account Discovery					
		T1218.011: Rundll32		T1087.002: Domain Account					
		T1497.001: System Checks		T1482: Domain Trust Discovery					
		T1553.002: Code Signing		T1518: Software Discovery					
		T1564.003: Hidden Window							
		T1620: Reflective Code Loading							

Indicators of Compromise:

Hashes

- 0c6b41d25214f04abf9770a7bdfcee5d
- 21f153810b82852074f0f0f19c0b3208
- 02699f95f8568f52a00c6d0551be2de5
- 0291df4f7303775225c4044c8f054360
- 0fde02d159c4cd5bf721410ea9e72ee2
- 2cbb015d4c579e464d157faa16994f86
- 3803c82c1b2e28e3e6cca3ca73e6cce7
- 5a6bbcc1e44d3a612222df5238f5e7a8
- 833ae560a2347d5daf05d1f670a40c54
- b637d33dbb951e7ad7fa198cbc9f78bc
- bce9b919fa97e2429d14f255acfb18b4
- d1d8902b499b5938404f8cece2918d3d
- edb1f62230123abf88231fc1a7190b60
- d405909fd2fd021372444b7b36a3b806
- 122cb55f1352b9a1aeafc83a85bfb165
- 936b142d1045802c810e86553b332d2d
- 23e1725769e99341bc9af48a0df64151
- 4d56a1ca28d9427c440ec41b4969caa2
- 50260f97ac2365cf0071e7c798b9edda
- 6fba605c2a02fc62e6ff1fb8e932a935
- 49ac220edf6d48680f763465c4c2771e
- 52f5fcaf4260cb70e8d8c6076dcd0157
- 78c828b515e676cc0d021e229318aeb6
- 70bf088f2815a61ad2b1cc9d6e119a7f
- 4961aec62fac8beeafffa5bfc841fab8

Domains:

- findoutcredit[.]com
- againcome[.]com
- modestoobgyn[.]com
- myshortbio[.]com
- estetictrance[.]com
- internethabit[.]com
- bestsecure2020[.]com
- chyprediction[.]com
- domenuscdm[.]com
- astara20[.]com
- coincidencious[.]com
- spontaneousance[.]com
- fashionableeeder[.]com
- incongruousance[.]com
- electroncador[.]com

SSH-based Backdoor (Active):

- xft6kit4fj5mnzsdt75ejf2spriszgaqpujclwimvfz7gtangi72suad[.]onion
- 141[.]94[.]147[.]168
- 15[.]235[.]156[.]105
- 15[.]235[.]156[.]115
- 185[.]117[.]119[.]108
- 185[.]117[.]88[.]245
- 185[.]225[.]17[.]220
- 185[.]232[.]170[.]83
- 185[.]234[.]247[.]62
- 194[.]104[.]136[.]113
- 46[.]105[.]81[.]76
- 5[.]252[.]177[.]15
- 5[.]252[.]177[.]8
- 79[.]141[.]168[.]12
- 80[.]71[.]157[.]110
- 80[.]71[.]157[.]173
- 85[.]239[.]54[.]186
- 91[.]242[.]229[.]184
- 93[.]185[.]166[.]15
- 94[.]158[.]247[.]23
- 103[.]253[.]43[.]212

SSH-based Backdoor (Early Version)

- 146[.]19[.]233[.]81
- 162[.]248[.]225[.]188
- 185[.]161[.]210[.]56
- 193[.]42[.]37[.]46
- 194[.]104[.]136[.]182
- 194[.]156[.]98[.]73
- 223[.]252[.]173[.]124
- 223[.]252[.]173[.]18
- 45[.]142[.]212[.]82
- 46[.]17[.]107[.]27
- 46[.]17[.]107[.]43
- 80[.]92[.]205[.]244
- 80[.]92[.]205[.]75
- 94[.]158[.]247[.]5
- 2cedhihsepjtcpwuwes77cle5wb6ml7e5ys6ivsb4a4ivlrw2vc4wwad[[.]]onion

Tirion/Lizar

- 138[.]124[.]180[.]193
- 138[.]124[.]183[.]50
- 138[.]124[.]183[.]85
- 138[.]124[.]183[.]90

- 176[.]103[.]62[.]29
- 176[.]103[.]63[.]104
- 176[.]103[.]63[.]198
- 178[.]33[.]111[.]73
- 185[.]161[.]209[.]161
- 185[.]174[.]101[.]186
- 185[.]174[.]101[.]216
- 185[.]174[.]102[.]183
- 185[.]174[.]102[.]37
- 185[.]250[.]151[.]126
- 185[.]250[.]151[.]134
- 185[.]82[.]217[.]21
- 195[.]149[.]87[.]118
- 195[.]2[.]71[.]90
- 37[.]252[.]4[.]131
- 45[.]133[.]216[.]194
- 45[.]133[.]216[.]89
- 45[.]142[.]213[.]56
- 45[.]142[.]215[.]132
- 45[.]87[.]152[.]64
- 51[.]254[.]149[.]31
- 54[.]38[.]123[.]229
- 74[.]119[.]194[.]129
- 91[.]134[.]14[.]26
- 94[.]158[.]244[.]18
- 94[.]158[.]244[.]200
- 94[.]158[.]244[.]209
- 94[.]158[.]244[.]91
- softowii[.]com
- red6djrs7fbkchy3[.]onion
- bgumuduxnkkecg3b[.]onion
- ba2xy52xrtagkrh3[.]onion
- fndqgtdkj4v6g4aq[.]onion
- 225ppqutwykx2or3[.]onion
- dppnmjep33rf6ct3[.]onion
- 4ktbtv54flfhs6ea[.]onion
- 4r7hlqzkxl5xtjxn[.]onion

Carbanak:

- 37[.]252[.]4[.]131
- 45[.]133[.]216[.]25
- 45[.]140[.]146[.]184
- 184[.]95[.]57[.]98
- 45[.]147[.]228[.]239
- 206[.]166[.]251[.]200

Loader Proxies:

- mozillaupdate[.]com
- milkmovemoney[.]com
- tableofcolorize[.]com
- moviedvdpower[.]com
- landscapesboxdesign9[.]com
- hawrickday[.]com
- colormiagi[.]com

Cobalt-Strike Servers

- 45[.]11[.]180[.]82
- 138[.]124[.]180[.]226
- 185[.]172[.]129[.]144

Powershell Scripts/Loaders (.ps1)

- 03402fa2054644b95d250213c83874b4696315c160b3bc9109a51ad8d8d70e5e
- 0e5a7d5b2c4a03db0c4e0e5861c0e952b940f191be767643f7ef81b89dc00f32
- 0f083aac77fb734a8e81fb9dff218f0414ac6c4c9a23b2832837fbc2c7e2031d
- 0f4f3b415558a9f6e51012e84d5c695124201cabb831feb3c6a796a7de515ed6
- 102c2ac3fed6abecc006fe3bfd686dcb210f06851352ce472eb5cedf7346211d
- 1066b89b56ea19958d3d3a2133547e964853d435a3b0cb45a8c45658d1fb2669
- 113a0233bde9933a49580eb8a4899df110b92a614bb01d6791a7cc9719482260
- 1145bb619227425efa376027a1f915b1511fda84ac4119a8c2fd5860c226c0d2
- 11c3a522322f5e9b2d3c24513bfed0735403e3643451ae8913c021f82097a2fb
- 12d9f50bac269885e66ba28a28b66afeffd8cca63f280313b49e88abd7455189
- 142825b4f37214fa1ca3fa37f74591c8f1702296a61f2a5fab7978f61daf124e
- 147aefbd27ff72eb0e77a4aa49cf5ab975046b400a682221363601ca82150f4d
- 152c72685127071e7e5b810102f0fa730a29e3b9fb61424221e0321263cf558d
- 1651b7ef2ff50ba11def006d3cf3ee68083a01a348389f72b4180d5120ab5e08
- 189f64cfb60310aefe0274f046a10e445a294f0e7573b122edce42b4392c6f66
- 1f036ce73e714170e6d11c469592ce0862b11659399a4eed04b918a20588e930
- 1fcbcc8af63bbb5d68e391f1518c1750dfcce60af7a5a852239271fed8fd354c
- 1fd44f5125590dc7e70c4112236d641cf4bc379223f1a464e5ee0cc2e420186e
- 21b06f6218981b2aa4125e72b6c24caea81ea9cb338d4d27cfb21de110f13d21
- 234c75e5c42c3fe4e9d87f5dd791ecb363f96b2ea701a5e8d13372180b95c0b6
- 243eb5ce49a3105455cfbc762d6e81e060f7d65ccc70c176c3b80f1ef226f0a8
- 249f604165b0b61860faf60459add5abcae9aca357c30a75735e512341aed063
- 287f363173683119bad58fc07eaaeac7ae3179ddac9510014da3e6db25da4167
- 2ed9284394cf9597401f6c93aa2f8e70515cb3a50d7ed75f9f4357b74ef1cb69
- 313aec1711acd5b12ddb832555fb007675d6d6a5b3986abf0cf5cdb127839a50
- 31e00424ede2b38899768686d44cc0ab4ff5808cb9996ce32d5d281a701a62bb
- 366a2cf31a56121ae3ddb7655913acce7c492e99086bca351495b6626d2c2a09
- 37cb9f0548735a00233a6a8c9910fd330712ccd57475c3110eb73ec998a3a091
- 37e5a9da84a9b73fe4c4e4da890eaef43afd971d029207c834b41ac00c9f610f
- 3b3089dd222febdfc20469c2dd6b246a8901f6653eef5ec6a687deaa8e41614a

- 3f97a1f421ec088f48851da977d291e90b13100293e8045fac40bcf297293833
- 3fe20f5c806d19665f7abd9079b2df16039566d53ed3347e42dd3e957557c797
- 4426def5168e2b00c65bfe8ff70c7e19f94f8925d20b6057e84dad169f34d328
- 4591b89fe88e210d4826f947fdac0ea6669d489e7903a8db1a8fe09d36b8eaae
- 45e3a5144f30f7a0def32452e4ca3874705ef3f808e4a756b62d773b581db1a3
- 4812f7ac410994e809f20d887c5fac300355d694f2b3ca0befe7df7bebb2818d
- 48f70181bd6aa7eeb0d1aa9a827c482fab837ae3a869f4842ee02bda58d92d48
- 4992e7f9da4343d8b9136db3b5c4640cb39196b336787bfb7651839c765a04a0
- 4ac9897d418ea3d73864e9ded58610bc387a55fdc9d9afb362066dfeb2cd1652
- 4b5a14eb9f847324a300e80ab3380f1713e0dd79ed051b9a4988ff1f7864788c
- 4eef954d91a2dea4242ec8c6d898250ae46d252a06f93a3b49b86d86e0d71674
- 50df2192220c6d9752b5cc68b44012d414441a282af72689fdcb83a779988d8d
- 519e63285fc68c5ca51fc82b7a4100b47450aadce38a5f1dbdab3ac11f07827c
- 51ac92206031f4e228333d6065e26737d707487f32e8b8b5d165220f6f4a64ce
- 525c2d5a8f95e8f457ca6437626f5e09619bdecc6f49dc8d85edf3c9437d1899
- 56bec8cfa25140ccb89cc9d8376ab90eb97bfc8831ecc89ece7f5ea930b2f164
- 5a53211bbeea5e2f19704729ab11985dc4304a04aa3581cfc762f9ef26c3f44b
- 5cabc4e2868f3ed1a7c0b437944e1e204416221b2667144e114d03937c55822a
- 5ccf66192ea9d2b6395fbb4a058d0af8409040d6d38b82b7fa1bf120371e9538
- 62b4cf54427087befe44a4081a044e9ab30f111256922730ae5b31fe5635995c
- 62ec5544d37d49ab9cef449358684f3f9d99768cb5526783598c0c0c5a1145d8
- 654d26e8abe7226d187bfa0a0470ffe8c1f388be7b0c17e86b7460acabb4b071
- 66168b2214552bd108c526f30c9a117ad5e91f764e81af9ffe640e5c8697169d
- 66aaded44e17f4ba18e95b8d10c0acc9ef4a41b6b08ed9dbcce171dc50bb9b3d
- 67e210540a9803d990b08d9367891dbb121bcea82b7d11748594daf8f60fac78
- 687aee5b9dbca6b29bf4627e806a6e7c7f4eae238651b3bbcc2fc78347e63111
- 6d61846213a454bff788196e1d0b08e8de900d7ea041931cf7d3a5d04172cc2b
- 6e8e2aaa62ec3d3605eef11a2a28b73fa6769eae49d86dc872676b36ccf6aee7
- 6f7a5ceb9362f5ce196d0b045b36a7408ce2590d9354e221fa48886d8ee5afb7
- 704181ce63a9d614bb7278cd5a608149b7bd10f8c29dece262ab986516daf9dc
- 72330db6e1fdd69316e30342f67a2dc6df443b9d9e19fef72dd4f05b6aa24939
- 76b80b1caae3573db89c0c18efe86d6d2566e0536019c1715ece7ddfeef8aaa3
- 76edd43b63a834a8bd3992f2529e41696fe69cef169898bc8fc70144ef50c14a
- 796757e7d0dc99f9544c7664628a3458778afe7e5db1a7d703933216d28ff637
- 798144bf051cb0fb3d5926a29f9e6ce93375e1bb1b259853392f72f5a1beb93b
- 7bb89b53f5de648c4bd67d317d92f6e70bc207b3a94ea661fa222ced617b4702
- 7c50cce83b56d5d0c591768590fa8d0b652c751920ca64da9c8f308759a6301b
- 7c97d38c7f852109bb55043348f21ca3ce4444d3aa928f99a120d91254d45bd5
- 7d43b6e0bb060655ec11550a48215f38df9f75a099a5435a3c7902794673980e
- 7d6de9ff0d85eb4cd6e555b38f93bc54ca381d24355999e496e723444b63fd0d
- 7e83b1656cfc054eb24b4ffcdf2701381cf9431cda64773b36d5e9521d617bcb
- 7f4361fe723bb40ea96f61366e21a92d0e59a06ad2089b63794398f33752fd51
- 8157539c61b135f80111e945c4fbafdc5bfdb86ff5f42a3334c8f87a8e70749d
- 84db02ab8e55dccd00c4c8d59f04b53ba9cc06739f14fe373fd3508468368b0b
- 86af5b326928b2c1ff88a7a840e7ab2a556caf29004ecb780be2f365e2141f3d
- 87e5fc0af403ee8e34e0ae88073c2e55d57174a8332f13d386b1c6b274532cbb

- 894c0129123266fbd2b2c4db1648c0c699a6694312a446697c8b2519da9a10e8
- 896c1d552ae040ff1bc14cb5e64bff4f662ed2c7d77478bc2b091b434bc3c2ca
- 89897c2321b28b57055d88b033edeba813db8b6365350f1fdaad503ba3886fd2
- 8ad17c2f7336668ea0a2e44a84ebf657774118db0888da7fbc1070e8d15ad039
- 8d8d2ef56247e8425da9c1c71466befeb918cdd2b1eedefa16b539abc9ff2cce
- 8dd435678c48eea256052c7edb3eb6f63e12684d811798bb07cde868d7ba3ecd
- 8f55483eeaf397df04fbca11f84c1e6b0f9248c62d78f072d25bb37501651510
- 91c5c33d3458ec7c51ecb5dfb218cee8ea949a821c7dcfcb0de65e50063f42dd
- 94c11d94d3c690c03149b9b78019027895d7a9ded4cc788b67be255d9b69e8ef
- 94dcd65e114b1b9abffbcab76ff741f3fa7c4f966ed22e79e757efb677e0991d
- 968cf5ca8774ef83fb3372072936d89c9b592c0b2680eca78c4e9e1cf7e391f7
- 987e84a12c0a8de359ba1e92eb0c8cffa882eb87b1e5da6d922a2e6c41807755
- 9b082f3cb56f9454bce695f80a0310d697bb213af34e25a0922e8db6c93d79e6
- 9b5010c4b62d2fff62f5d03bb6af2ae4da2d2fdfde2b706aac3cef162946cdd3
- 9ba1f64b6841210d5368912fcae656b5f228085f7074a82606f6257ba339d1f6
- 9bcb8259a2a535cb5eb91af699b02a79e91b41a8d0aecbd358bfbc32de4a3085
- 9ccb3dd2e872e138b7772f0d200bfa2fffe967bb509346a36aa1e179eb7d2638
- 9e359293685487ab9bf8bb016494c465720e2b41e3139e792199a4e268117255
- a5743b6744bb071c5358251690b888e8ce53acb821b4e2c11c29e6c5e0cd08ee
- a9718a216bdf9bf1778a0dd1b368289ad8463bd412b5f33b1d8a3ed099644175
- a99f60b516ee0333d39b9cf1f3685933bd2f2b2a7efdac86b06a5427e5035178
- abdbad63fb5df46b18557faba588727b3a47a4deef48735be7f7d9d050ac1098
- bad56fd5b56c7a3ed63932bfa25bd50923d1a01e5bd875981da38f8d2e22f4c7
- bdf258569c65ace982f6d78165067656794a2a3f7e76c87cdcc282de0ca36bce
- beb7bc9cce14adfc0740b34c9d1b664f0132d0fc626de13b992e639ec4024ee9
- bece44ebf63223b09c1eb6ae7d76b812915c618bad99f644a3821bb2ac9c32f7
- bf0a72eaa43ec0b955dcd963f553c440667cb9eadb4d8f0d14c26f19be435017
- c1a557ae03a36b62780ea4fc18d8d8101ff2706d955c74e84d025f36e698c478
- c58aa7860c981f988ca66154373c3f8afd8ccf0550df292104ff956a4f24882d
- c598870bce55a9c969dadb1d5164d49d0638c0557316d788beae7efb096495fa
- c6e79054bf3e8a837eaabb102f3a506bcaedbf666b8a79167e49f2483ec1c2a1
- cc0c5b39889d0ff1106aa0570943b9b22ca9274e8187f4394f59572944d1f515
- cd89163f0da49de1da3bd88068b417d6955cfb863bb2169e4742fa6e2613dc1b
- cdeb7d66af20f4026d9f7463dc02e4c6b3ea8f317a744be135af55c03902f2ff
- d06b23fcc87fbf82c945afb218b8333c056c1585db419539753e5aa4a9fa09c3
- d3199c96093db623854e2e41b2752aff74097b3ba594f1ef22b45f7cc1047ad7
- d44c4247b7516b030f5c3b5c6f18246933700447a6462531d31b06c4f0ab9112
- d73c9baedc0028945244a304367fbc2359b6284dfa7aa6943330946d4b1f8bb9
- da1cd0853f8c5a172390799492c284308f7cda3211e3168065ea1038b34dccc1
- dc4fc1de8d7c9c95bd6304df338bb3aa748502cac8a2dd3445e8464e4082d8d6
- dc9442838b464e96281a32705c9b5958e4f45dbefd1ef4a885fac9898af0a4b7
- dce8a6fb8dbd5c48c020df02cf7108b390d2c271f30c388c17be5bab8d6f2a3a
- de35b786c3c68ebefbd2ea345838c6347f219daaa5146757202330a0d1d22828
- e1283c59b22173590c75fbd1e5d5049ce6a07d17511f331d207155b5ce23ec8e
- e1b3035d6b53c7faccf2e062693836ae077cb7b3e66d1ad6534f91dee53b0916
- eb015ba9d6aaa4c26242fb38216d0ed89f98f95af9bbfde9dcf0d6ba247a3cc8

- eb95f84f22cb823fb85e81585db43fcaa1d15d9d3ab7e8f66e52f6cc52ce2b1c
- ee504ae4cef55bb0da834ee7e3e529a96f6629dbc252e30e20f699387210250f
- f15d5f8cdf45e551d039415ec53706049815cf685e9e7ccf5113158f546d88c3
- f418b680024e1ba15e40b056959122f5c05772a2e145c25b29e7a2641da7d38b
- f58c61bda2867fd5c5aefefacffc5d0fa06833f8df22a80485e24f4d9f559673
- f63c3c0347e1b4f9b13b02fd86cd7be749ab29fc313666e2047354336bd42fbf
- f6b758022358f2d915104c616fc2abeb76c797e9e60a883e9161f8bbb928b512
- f767b0dabd5fc8f3977ef02c68448dc03a8572a5bae64f85bb7bafdce9e8ba83
- f87813c2572eefdf225f075aaf0a19794273ff6904a2ec5e4df296bfc9ec6809
- f9cca8a37fe027b8f5084c34a156bbd5fd8237e6d4740622d2c17f9f9f420ada
- fa10e61e168c579058406f63bc93880f85f67333f319636623414fffd78627f1
- fcacb66e961df0eeacbc1b0a74c355c5b7a2f5dd3937a5b77c3db991c0f58922
- fcd8cd529bbe424234e65ba7daa17291d18bb19b26e10e7cb1498b3fbff07d67
- fd638aa195d9c92f40b64175a68e6b037c07d29ddcef7c5033edbe57c1b91c56
- fe84128b54ac6c29bfdb6933451060d201864b384474386f35a3dfde2afe5172

DLLs used in Reflective Injection (.dll)

- 00bce4a794d4e36ffbffb89f0c985daa85b47ebae686fc82e79f0f5f7c1c55b3
- 024787688d9cf2f3f868f7bc5115949724b6870ecf1d0e6e018a83fac534f9e6
- 057093bd4aae459eaa9b501544a035d5cbe8705158fedda6677cb28fa7197154
- 05f572ee9e0b4cbdfdccfd16ad74043d8df3dec0aefeb1e8d9dfca12e8e5e463
- 0899f0a3696e717dc46958c1079f263c9ba413051235e6bb1beb8b77f2dc6278
- 09c62bdb7826eb20401d64ebc6c391e9633cb32ecd2be88bb47d5d5efb78b1ee
- 0d43eca3777f98773314e04870bcbe76d6c5eb0694356509cd9f698d9a169f76
- 0f622acdd066ebba14487cc31ac2cd3eea44f97530b0e406e637ea05ff3b175b
- 1250e7bb1f6293dbf3ea3d6d83fdb52edfb5dc1ab006806c0ebcaaaca120f538
- 12798a2e9abead453c3b38d4b35f3ae563b06863307760d94b75b80d640c0b29
- 199a69b5863e2f8b19895b6e5f0f79dd16915459867d4d7581cc79eca0cacd01
- 1caa8424e7d9e8f6af0ae704894dd7e47bd03fab0314cf23264c4f23f00c89dd
- 1cb246b76add81b74ff746e5a9cda1a370ed21b187a59f97afde65534f6eb3f9
- 1d9b6d69de1bc5bd146c0a3c8096ba0c465c3a9fb5de6348c847c127bac0bca4
- 24b31ce7cf44cb9acc92280d24545fdbbf42b3d6c76ea62d244ca22084943879
- 377f4676bdf3c5fccae0065f828e3d774354c8f2ad3ca6401de9a89a1a22889e
- 3c36444de4c6df85ec9158b7136df7f458ba9239acfacb60b8b0d273133824af
- 3c87406df35f5fd264634d60deda9f1a32b66f22b5a56a2245129883d91c32f4
- 3ec1602b1ef9d4ac7b35171ccf7b465bb2645b66efac159125c3850660bf83e4
- 3fb04f5606bb8d556a86c5a4fe87dee200bb7a731ce226c537d318b2c493041a
- 40c4dc04a080fbd24d0164b46567265b8186e03fcb2b8a38bd9b3ba60599e81a
- 40e29b626e7656b7fc0719de41582964079170e201147c19e20afae17bdcecdc
- 444e8919a4c9bb545fcf87a412a1f1b35aa5a3b863ff378ed32bbb095b66e8d1
- 4b0484265a5d7b7864bff1de53b48d880fe6688677240de7202236d3c5a22e87
- 4c5fb53e0787ebc0bbc99d8dc079e99cfcb111ddfb040abcf8b4cb56898db7e7
- 4dd732120f265e0c430d437a3a5eac426baee3a272e18683bf45ff17ad680cbc
- 4eb4b601b0da4ad1e83a7df5d35fb852c2a57cb12bf4c618456bb70684dc3683
- 5010d230e315e3333cdc639d8fa4caed602c6073cda7a52702c148091592c3b8
- 5579e036f5769d82eca99823844bbc60ad8cf5b0e6c6a03c596c11cccc8faf34

- 575e9d1dda2e1dfec81c5a1c3b182d114f2ebac9aa91e304d5ae6dc26319f8ea
- 5b90d64969bc653a9f16e4af35425e639a1a4293083dcef0659102924abe116d
- 5cc7e55514418118f68d067a15d9496cfe867817bf0b5dfd4a061fa5851e2cca
- 5ce10299e8da54195412431333d28527d69a50ce0610d81e5c7ea985c5b3e286
- 73f98bba5806d612c8618fba09b69bf30c4004c509b3584302c8a580f8c4a241
- 769961f1ea98c57eb237c0ef75f3887adbb193820b0e84c70dc5c9ea5d2288df
- 79bcdc6a013d38c67272428b6a2a82d12937ff55894917a167662cb992007115
- 7efa90c80c564d6041cfa896708549a7a5c0311056f90e512c22b11fda7292fd
- 8327a3633ff79e1eb890d5b9b0c57e37c61f364090eb06d9d4d68492489e9e5b
- 8574d51a4bad21304283c2b8b624220657d2cfe7a26e0c072a61a74754b130aa
- 89f2442d402f1f6bb2cd250e15c69edf2ebfd35bbf835b4c4bc652595b32b055
- 8b121f75715948313f44b4fea6275dffc823a95cf4e5a1ed6e234e35197d9024
- 8cdb26386b6aa3ab8629afc3378f9dac5ecb92695f679955f438ddb4a8495f61
- 9766dca93376a8c520a6341db941783213b62596b0e0f0cde231e5894ab02210
- 97763566a162b1114a0f31753144188e40b5ea4efb03762e3bcfa2befc03d19b
- 9847b71a4a5fe4f6749ba80d403a67e06e65a9feeb244a8af19e7bf5370e9eee
- 9a5ed033c0a119e0460b6055ea175d2fe09be3d4642ce1bdbbc5f2a1d309c97b
- 9b51eca8947765e4da56111fd23dc531e7dbf85c564af2c74b7f00054116f270
- 9b8af8b48f229c79aae80013b56c83da9dd4edebc6f0fd33fb46936925737d1e
- 9e489d6e0ff151bd7ea30083edc84b49bab7d01da4c497ac201f9e7e202d6eb6
- 9f4578c75551deddcfc85411b0e8a9db2632ad497741a32ba019c162e43328f3
- 9f834177faa76ebb8d9bcf36054298492d91bcdfcec74714e76e79ffc9fc6bd9
- a2cbf90e781461674a053940930e3648c092f62463d7f1b67af72dc93e8462d8
- a3c8cf59eaa14be924c04853ae5f097d32fef703d5bde2fe0d542e989cfe6133
- a5c85435d59c10c59f719017d578e616953d36881c5f8d8c2b09ff307ff731af
- aa16c5322e9317d2c64fe9bcce45be47f0ed765c3fa26e5e29af4f0583fa36e1
- b8c9ff2c2543b5860211f0b86be9a5e0b66566247f27d1802ad06a184114995c
- b9fef960f1cef1713883f55f9ba22e34f007004eea3aa3d012e76268ef457c51
- bb10276cc6e85ff02d0dde90d20e78f4b4a3c60e01dd8c27d39e4b6fdca6227e
- bb22e8eb9439e274bf5441ee708c78e78c4e5a1988dc7ad06a98cd3545c478e8
- c6bdcfc229ba855cde5dd91043c50a8adb5b39be2db10de8b0913b260e82d467
- c6de227d06044ee65a1e434d7371d845d8b2a744dd1911fb200caa0252d395c8
- cab9613be36682d29afc24d1cf89f2a45ba76b96a087647f05b014c2033b6f57
- cfec2c71cc82479348c310c0a0b2b2d88e9496f7fab98528e300a7167ce787c3
- cff41c53068b0eaa8823ae17f288a7fc8b90475b7a39625cff034ed965d86d92
- d0ac3ee7a8493c15fee8122f292db57b648ca511f969026df244fd7a70b475b9
- d484ed62c67a46a2ddc9a6d41b76493818489ec2f697a743681f23f8b35bd94f
- d6223cc31ca3c8f5a56d4000cbd8210e0d005c3b46004f569362ec6237bb015b
- dd7c9855f75cee6375304a44ce2926110568e75386b91fab4eca438d9ffbb0ce
- de0657b9e6f165814ab501bda45db60858df7689e6eb99735683674f4dfde704
- dedbcced35c4c94589d7961fe117252114c3d4e00fe916921eded551c620daee
- f1c268bacb3879a836ec05226465b70bad27c24f2d0d5b0abd9b7fe2bbad4822
- f2be4f603293b9133e5e75be8bac8542748c880255de3fe9b2fb88b0b653a395
- f66cda08b58e96e1d39f7e548b1aa3564d80da805ba4582c5cd424545a8b472a

Backdoor Install Scripts (.bat)

- 15a0ee975e75a466f7f4cd1d8228ace7bbef5cbfc909fec5c53421fc050e7a61
- 2076398177d76b77ed32a1dbb5220d3bae873a1e736a6abab7812b50c0f0328b
- 46a842177d8765b73978d9526e3f8d287528de0e3b004d58c8ebe6f3f42f434d
- 4d27f295ba6f9f0d1691ebc910f5b1cfa2c8d60c0a1fac68cdceba7f85841d49
- 627ff24df51a94e3086596f595732ceb3ab290e067f1b039832f98af09a931b3
- 87c235bccddf0c657027b7ac0ef33b82644c92fc16e284114980e0be43396ba3
- 90ed60f5290391b8cbe70d09ce7d0831d847ecb060ac6ec3f7ed2cef180905a9
- 9a4b066ff59caac6f4c3f044b5c9c0e57ffeaaab49ad8bca76d686a4e3e77292
- 9dc250729a1fe4f5ff8e559a34299b54bf6e245803b9f03a9c8983bce7426da6
- c8df05eb7200806627aa629df9219d6140d4526ec552cdb37383b44d4f7c96c6
- ccf5f274e5930df4bf9bda2de3e8279fbcfd6679e44fd797d9e42d41f3814981
- d74a283f9bee0a871007fa92e2036997d17b1d8528ec37919c3c4d61b8fdbf13
- dc3314d6574630c4a870aa0e6025583816a4aaab569354dbfb924c320dc4219a
- de0cba17d4c1627f13edf3bcadc93ca532ae2ee39c290e4b05c6e1116997b118

Ending Note:

Throughout their evolution, FIN7 has increased the speed of their operational tempo, the scope of their targeting, and even possibly their relationships with other ransomware operations in the cybercriminal underground

Despite increased detection solutions and awareness within the targeted sectors, utilizing public exploits is a powerful approach for gaining access to the victims' systems. To this date, the FIN7 group compromised and caused monetary damage to 8,147 victims, predominantly residing in the USA (16.74%). It is essential to mention that they managed to infiltrate all those high-profile companies after scanning 1,826,508 targets. Their signature move is to thoroughly research the companies based on their revenue, employee count, headquarters and website information to pinpoint the most profitable targets.

Reference:

- https://www.prodaft.com/resource/detail/fin7-unveiled-deep-dive-notorious-cybercrime-gang
- https://www.mandiant.com/resources/blog/evolution-of-fin7
- FIN7 APT Group Updates: Incorporating Software Supply Chain Compromise, Enhancing Operations - SOC Prime
- https://www.bleepingcomputer.com/news/security/fin7-hackers-create-auto-attack-platform-to-breach-exchange-servers/
- https://github.com/horizon3ai/proxyshell
- https://screensitter.com/2021/11/23/cve-2021-42321-microsoft-exchange-rce-vulnerability-what-we-know-so-far/
- https://isc.sans.edu/diary/rss/26132

MITRE ATT&CK techniques:

ID	Name
T1059	Command and Scripting Interpreter
T1059.001	PowerShell
T1059.003	Windows Command Shell
T1059.005	Visual Basic
T1059.007	JavaScript
T1204.001	Malicious Link
T1204.002	Malicious File
T1569.002	Service Execution
T1195.002	Compromise Software Supply Chain
T1199	Trusted Relationship
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1491.002	External Defacement
T1583.003	Virtual Private Server
T1588.003	Code Signing Certificates
T1588.004	Digital Certificates
T1608.003	Install Digital Certificate
T1608.005	Link Target
T1027	Obfuscated Files or Information
T1027.005	Indicator Removal from Tools
T1036	Masquerading
T1036.003	Rename System Utilities
T1055	Process Injection
T1070.004	File Deletion
T1140	Deobfuscate/Decode Files or Information
T1218.010	Regsvr32
T1218.011	Rundll32
T1497.001	System Checks
T1553.002	Code Signing
T1564.003	Hidden Window
T1620	Reflective Code Loading
T1113	Screen Capture

T1213	Data from Information Repositories
T1560	Archive Collected Data
T1021.001	Remote Desktop Protocol
T1021.004	SSH
T1071.001	Web Protocols
T1090	Proxy
T1095	Non-Application Layer Protocol
T1105	Ingress Tool Transfer
T1132.001	Standard Encoding
T1573.002	Asymmetric Cryptography
T1012	Query Registry
T1033	System Owner/User Discovery
T1057	Process Discovery
T1069	Permission Groups Discovery
T1069.002	Domain Groups
T1082	System Information Discovery
T1083	File and Directory Discovery
T1087	Account Discovery
T1087.002	Domain Account
T1482	Domain Trust Discovery
T1518	Software Discovery
T1110.002	Password Cracking
T1555.003	Credentials from Web Browsers
T1558.003	Kerberoasting