blackpoint

THREAT PROFILE:

FIN7

ADVERSARY
BLACKPOINT CYBER
APG
PURSUIT GROUP

Table of Contents

Executive Summary 2

Description 3

Previous Targets: FIN7 5
- Previous Industry Targets
- Previous Victim HQ Regions

Known Operations: FIN7 7

Known Counter Operations: FIN7 10

Known Exploited Vulnerabilities 11

Associations: FIN7 13

Team Structure: FIN7 16

Known Tools: FIN7 20

Known Malware: FIN7 25

MITRE ATT&CK® Mappings: FIN7 30

References 36

Executive Summary

First Identified:

2012

Known Associates:

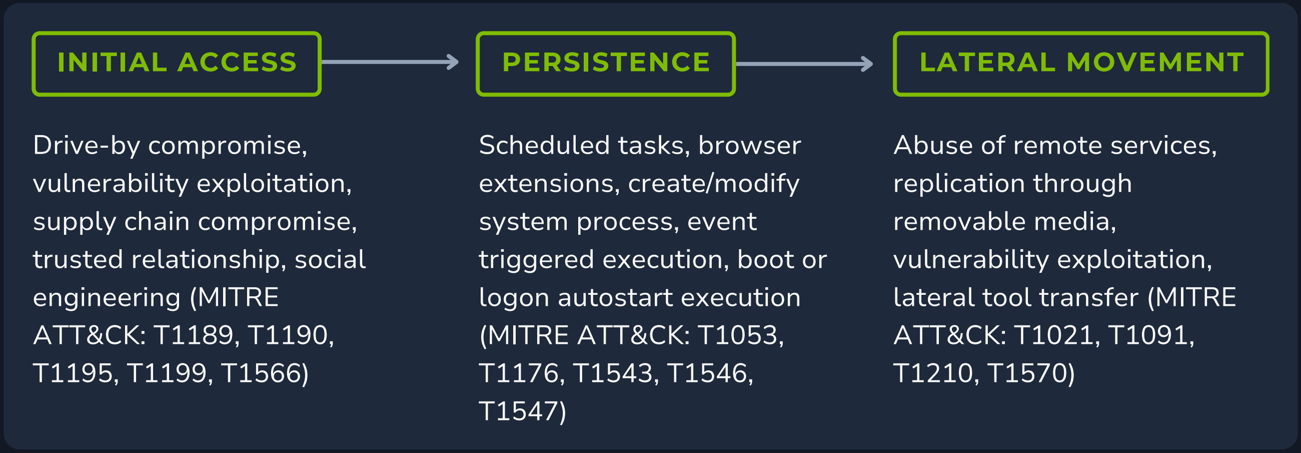
- Combi Security
- Bastion Secure
- ITG23
- Secure Cloud Tech
- Stark Industries Solutions
- UNC3381

Attributed Country:

- Russia

Also Known As:

- Anunak
- APT-C-11
- ATK 32
- Calcium
- Carbanak
- Carbon Spider
- Coreid
- Elbrus
- G0048
- Gold Niagra
- ITG14
- Magecart Group 7
- Navigator
- Sangria Tempest
- TAG-CR1
- TelePort Crew



INITIAL ACCESS

Drive-by compromise, vulnerability exploitation, supply chain compromise, trusted relationship, social engineering (MITRE ATT&CK: T1189, T1190, T1195, T1199, T1566)

PERSISTENCE

Scheduled tasks, browser extensions, create/modify system process, event triggered execution, boot or logon autostart execution (MITRE ATT&CK: T1053, T1176, T1543, T1546, T1547)

LATERAL MOVEMENT

Abuse of remote services, replication through removable media, vulnerability exploitation, lateral tool transfer (MITRE ATT&CK: T1021, T1091, T1210, T1570)

Description

FIN7 (AKA Carbon Spider, Gold Niagara, Sangria Tempest) is a financially-motivated threat group that has been active since at least 2012. The group has been most known for their targeting of organizations in the Consumer Cyclicals, Transportation, and Utilities verticals in the United States. However, the group has been observed targeting organizations worldwide in large scale campaigns and attacks. The group has been assessed to have origins in Russia; however, some members of the group have been assessed to likely reside in Ukraine and other neighboring countries.

FIN7 specialized in point-of-sale (PoS) malware for financial theft and fraud; however, the group was observed changing directions and getting involved in ransomware operations in 2020. The group has been observed as an affiliate with ransomware-as-a-service (RaaS) operations such as REvil and Conti; as well as developing and operating their own RaaS program, DarkSide and BlackMatter.

FIN7 has also been observed creating fraudulent security and tech firms – Combi Security, Bastion Secure, and Secure Cloud Tech – to add legitimacy to their attacks and purportedly used the companies as a front for their malicious activities. Additionally, the group has been observed with several user accounts on multiple cybercriminal forums – XSS, Exploit, RAMP – advertising tooling and malware for sale.

Security researchers with PRODAFT conducted an in-depth analysis of FIN& and reported the group's staff, including three members of management, a development team, pentesters, and identified affiliates. The group appears to be a vast network of members focused on financial gain.

FIN7 has been linked to Russia and has worked with a number of high profile operations, including Black Basta ransomware.

Their activities have included:

- Malware development,
- Ransomware operations,
- Acting as an initial access broker (IAB) for other threat actors; and
- Conducting large-scale PoS attacks to steal payment card details and conduct financial fraud.

FIN7 has been observed gaining initial access via multiple methods, most often relying on phishing emails with malicious attachments. The group has also been observed conducting drive-by compromise, exploiting known vulnerabilities, and conducting supply chain compromise. The group used the trusted relationship between two organizations to gain access to victim environments.

The group has been observed gaining persistence in victim networks via scheduled tasks, likely in an attempt to blend in with normal traffic. The group has also been observed creating new and modifying existing system processes, modifying Registry Run Keys, and setting up malware to run on system startup and when users log in.

Description

The group has been observed moving laterally by abusing remote services, such as RDP, using USBs laced with malware to infect devices as the USB is inserted, exploiting known vulnerabilities, and lateral tool transfer.

Multiple members of FIN7 were arrested in 2018 and 2020; while the group's activities appeared to slow, security researchers have reported that the group is active again in 2023 and 2024. It is likely that the group will continue to operate, focusing on malware development and financial gain over the next 12 months.

Previous Targets: FIN7

Previous Industry Targets

- **Academics**
- **Consumer Cyclicals**
  - Hotels & Entertainment
  - Retail
- **Consumer Non-Cyclicals**
- **Energy**
- **Financials**
- **Government**
- **Industrials**
  - Construction & Engineering
  - Transportation
- **Technology**
  - MSPs
  - Telecommunications

Previous Targets: FIN7

Previous Victim HQ Regions

- **Africa**
  - Algeria, Angola, Botswana, Burkina, Burundi, Cameroon, Chad, Congo, Egypt, Ethiopia, Gabon, Ghana, Guinea, Kenya, Libya, Madagascar, Malawi, Mali, Mauritania, Morocco, Mozambique, Namibia, Niger, Nigeria, Senegal, Sierre Leone, South Africa, Sudan, Tanzania, Togo, Tunisia, Uganda, Zaire, Zambia, Zimbabwe
- **Asia**
  - Afghanistan, Armenia, Azerbaijan, Bangladesh, Bhutan, Burma, Cambodia, China, Cyprus, Georgia, Indonesia, Iran. Iraq, Israel, Japan, Jordan, Kazakhstan, Kyrgyzstan, Laos, Lebanon, Malaysia, Mongolia, Nepal, Oman, Pakistan, Philippines, Russia, Saudi Arabia, South Korea, Sri Lanka, Syria, Taiwan, Tajikistan, Thailand, Turkmenistan, UAE, Uzbekistan, Vietnam
- **Europe**
  - Albania, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom
- **North America**
  - Bahamas, Belize, Canada, Costa Rica, Cuba, Dominican Republic, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Nicaragua, Panama, Puerto Rico, Trinidad, United States
- **Oceania**
  - Australia, Fiji, French Polynesia, New Zealand, Papua New Guinea, Samoa, Solomon Islands, Tasmania
- **South America**
  - Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Guyana, Paraguay, Peru, Suriname, Uruguay, Venezuela

Known Operations: FIN7

2017	FIN7 was attributed with conducting a spearphishing campaign that appeared to be targeting personnel involved with the United States Securities and Exchange Commission (SEC) filings at various organizations. The group reportedly used the spearphishing emails to deploy the Carbanak backdoor malware.
2017	FIN7 was attributed with two fileless malware campaigns targeting financial organizations and government entities. The group reportedly targeted more than 140 banks and used the Meterpreter tool and other known tools.
2017	FIN7 was attributed with a phishing campaign targeting organizations with emails that contained either a malicious DOCX or RTF file. The group was then observed calling the targeted organizations to ensure that the victim had received the email. The group reportedly deployed the HalfBaked malware variant.
2017	FIN7 was attributed with deploying the Bateleur malware variant to organizations, including restaurants. The malware was deployed via phishing emails with malicious attachments.
2017	FIN7 was attributed with a campaign deploying the Carabanak malware for persistent access to victim environments. The group was observed leveraging an application shim database to achieve persistence on system. The shim injected a malicious in-memory patch into the Services Control Manager process.
2018	FIN7 was attributed with targeting victims with phishing emails to deploy the SQLRat malware. The group was also observed utilizing a new malware control panel, Astra.
2018	FIN7 was attributed with targeting organizations in the Consumer Cyclicals vertical – specifically stores, hotels, and restaurants – to steal payment data.
2018	FIN7 was attributed with targeting organizations with phishing emails to deploy the Griffon implant on the victim's computers. The group was attributed with deploying the AveMaria infostealer bot, likely to steal payment data and credentials.

Known Operations: FIN7

2018	Operation CopyPaste. FIN7 was attributed with using social engineering tactics, such as typosquatting, to deploy malware that would aid the group in stealing payment details and credentials.
2019	FIN7 was attributed with deploying the BioLoad malware to deploy second-stage payloads that eventually led to the Carbanak backdoor malware.
2020	FIN7 was attributed with targeting a U.S.-based hospitality provider with a badUSB attack. The organization reportedly received an envelope containing a fake BestBuy gift card, along with a USB thumb drive. The USB drive functioned as a keyboard when connected to a computer and was used to launch automated attacks.
2020	FIN7 was attributed with working with the Ryuk ransomware operation to deliver the ransomware on victim networks.
2020	FIN7 was attributed with attempting to deploy the JSSLoader on victim networks, likely in an attempt to maintain persistent access to the compromised networks.
2021	FIN7 was attributed with using malicious Windows 11 Alpha-themed Microsoft Word documents with VBS macros being used to drop JavaScript payloads, including a backdoor malware to maintain persistent access.
2021	FIN7 was attributed with deploying multiple malware variants throughout 2021, including LoadOut, Griffon, Carbanak, PowerPlant, and more.
2023	FIN7 was attributed with exploiting CVE-2023-27532 in Veeam Backup & Replication vulnerability to gain initial access to victim environments. The group reportedly deployed the PowerTrash malware.
2023	FIN7 was attributed with partnering with ITG23 – the Conti and TrickBot syndicate – purportedly acting as a malware developer and possibly an IAB.

Known Operations: FIN7

2023 - 2024	FIN7 was attributed with targeted organizations in the automotive industry with spearphishing emails using a lure of a free IP scanning tool and targeting employees in the IT department. The group used the emails to deliver the Anunak backdoor and gain persistence on the victim environment, the group then reportedly deployed the PowerTrash malware.
2024	FIN7 was attributed with impersonating well-known brands to target victim environments. The group reportedly delivered the NetSupport RAT via MSIX app installer files.
2024	FIN7 was attributed with conducting automated SQL injection attacks for exploiting public-facing applications and using AvNeutralizer, a purportedly custom tool developed by FIN7. The group was also reportedly observed using multiple personas to advertise custom tools and malware.

Known Counter Operations: FIN7

2018	The U.S. DoJ announced that three high-ranking members of the FIN7 group operating out of Eastern Europe were arrested and facing charges. The members included Ukrainian nationals Dmytro Fedorov, 44, Fedir Hladyr, 33, and Andrii Kolpakov, 30. The members were accused of conducting highly sophisticated malware campaigns targeting more than 100 U.S. companies.
2020	The U.S. FBI arrested a member of the FIN7 cybercriminal group, Ukrainian national Denys Iarmak was reportedly extradited from Thailand and arrested in Seattle. The member was charged with multiple criminal counts, including wire fraud; conspiracy to commit computer hacking; conspiracy to commit wire and bank fraud; three counts of aggravated identity theft; three counts of accessing a protected computer in furtherance of fraud; three counts of intentional damage to a protected computer; and access device fraud and forfeiture allegations.

Known Exploited Vulnerabilities

CVE-2013-3660 (CVSS: 6.9)

Privilege Escalation Vulnerability
Product Affected: Microsoft Win32k

CVE-2017-11882 (CVSS: 7.8)

Memory Corruption Vulnerability
Product Affected: Microsoft Office

CVE-2020-0688 (CVSS: 8.8)

Static Key Vulnerability
Product Affected: Microsoft Exchange

CVE-2021-31207 (CVSS: 7.2)

Security Feature Bypass Vulnerability
Product Affected: Microsoft Exchange Server

CVE-2021-42321 (CVSS: 8.8)

RCE Vulnerability
Product Affected: Microsoft Exchange Server

CVE-2022-24521 (CVSS: 7.8)

Privilege Escalation Vulnerability
Product Affected: Windows Common Log File System Driver

CVE-2022-37969 (CVSS: 7.8)

Privilege Escalation Vulnerability
Product Affected: Windows Common Log File System Driver

Known Exploited Vulnerabilities

CVE-2023-21715 (CVSS: 7.3)

Security Features Bypass Vulnerability
Product Affected: Microsoft Publisher

CVE-2023-23376 (CVSS: 7.8)

Elevation of Privilege Vulnerability
Product Affected: Windows Common Log File System Driver

CVE-2023-27532 (CVSS: 7.5)

Missing Authentication for Critical Function Vulnerability
Product Affected: Veeam Backup & Replication Cloud Connect

CVE-2023-28252 (CVSS: 7.8)

Elevation of Privileges Vulnerability
Product Affected: Windows Common Log File System (CLFS)

ProxyLogon (CVE-2021-26855) (CVSS: 9.8)

RCE Vulnerability
Product Affected: Microsoft Exchange

ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) (CVSS: 9.8, 9.8, 7.2)

Pre-Auth Path Confusion, Privilege Escalation, Post-Auth RCE Vulnerabilities
Product Affected: Microsoft Exchange

ZeroLogon (CVE-2020-1472) (CVSS: 10)

Privilege Escalation Vulnerability
Product Affected: Netlogon

Associations: FIN7

Russia

FIN7 has been linked to Russia; however, some members of the group have been assessed to reside in Ukraine and other neighboring countries.

Anunak

FIN7 alias used by Group-IB

APT-C-11

FIN7 alias used by Group-IB

ATK 32

FIN7 alias used by Thales

Calcium

FIN7 alias used by Symantec

Carbanak

FIN7 alias used by Kaspersky

Carbon Spider

FIN7 alias used by CrowdStrike

Coreid

FIN7 alias used by Symantec

Elbrus

FIN7 alias used by Microsoft

G0046

FIN7 alias used by MITRE

Associations: FIN7

Gold Niagra

FIN7 alias used by Secureworks

ITG14

FIN7 alias used by IBM

Magecart Group 7

FIN7 alias used by RiskIQ

Navigator

FIN7 alias used by Fox-IT

Sangria Tempest

FIN7 alias used by Microsoft

TAG-CR1

FIN7 alias used by Recorded Future

TelePort Crew

FIN7 alias used by tr1adx

Combi Security

A reported front company for the FIN7 threat group. The group purportedly used the front company to provide a semblance of legitimacy to attacks and to recruit hackers to join the FIN7 group.

Bastion Security

A reported front company for the FIN7 threat group. The group purportedly used the front company to provide a semblance of legitimacy to attacks and to recruit hackers to join the FIN7 group.

Associations: FIN7

Secure Cloud Tech

A reported front company for the FIN7 threat group. The group purportedly used the front company to provide a semblance of legitimacy to attacks and to recruit hackers to join the FIN7 group.

Stark Industries Solutions

A large hosting provider that was first observed two weeks prior to Russia's invasion of Ukraine. Security researchers have reported that numerous Stark Industries IPs were solely dedicated to hosting FIN7 infrastructure.

ITG23

FIN7 has been assessed to have been hired or paid to develop a new malware for the ITG23 – a Conti and TrickBot syndicate.

UNC3381

A purported sub-group involved with the FIN7 operation.

goodsoft

A user profile on the Russian-language forum, Exploit, that has been observed offering malware and "penetration tools" for sale. The group reportedly advertised an AV killer tool for a starting price of $4,000.

lefroggy

A user profile on the Russian-language forum, XSS, that has been observed offering malware and "penetration tools" for sale. The group reportedly advertised an AV killer tool for a starting price of $15,000.

killerAV

A user profile on the cybercriminal forum, RAMP, that has been observed offering malware and "penetration tools" for sale. The group reportedly advertised an AV killer tool for a starting price of $8,000.

Stuper

A user profile on the Russian-language forum, XSS, that has been observed offering malware and "penetration tools" for sale. The group reportedly advertised an AV killer tool for a starting price of $10,000.

Team Structure: FIN7

Alex

Assessed to be a part of FIN7's management team. Alex has been assessed to be the employer and leader of the FIN7 threat group; is reportedly heavily involved in infiltration and ransomware attacks attributed to the FIN7 threat group.

Rash

AKA Corleone. Assessed to be a part of FIN7's management team. Rash has been assessed to the manager of Shepard and Roland, two of the group's pentesters. Rash is purportedly in charge of the ransomware operations attributed to the group.

Sergey-Oleg

AKA serhii. Assessed to be a part of FIN7's management team. Sergey-Oleg is reportedly an expert in tailored access operations and responsible for assigning tasks to the group's members.

Vie

Assessed to be a part of FIN7's developer team. Vie reportedly played a crucial role in FIN7's Carbanak campaign and has been assessed to be the developer behind the Checkpoint Software Loader used by FIN7.

Zergo

Assessed to be a part of FIN7's developer team.

BlackCode

Assessed to be a part of FIN7's developer team.

Kurt

Assessed to be a part of FIN7's developer team. Kurt reportedly used the username derv1sh and maintained a GitHub account that hosted a number of payloads they were responsible for maintaining for FIN7.

Shepard

Assessed to be a part of FIN7's pentester team. Shepard has been assessed to work for Rash and has provided initial access to ransomware providers and has been assessed to be located in Ukraine.

Team Structure: FIN7

Yar

Assessed to be a part of FIN7’s pentester team.

Roman

Assessed to be a part of FIN7’s pentester team.

Dalhar

Assessed to be a part of FIN7’s pentester team.

Illddd

Assessed to be a part of FIN7’s pentester team.

Andrey

Assessed to be a part of FIN7’s pentester team.

Roland

AKA seeerega, rol, soslowso. Assessed to be a part of FIN7’s pentester team. Roland has been assessed to work for Rash and has provided tailored access to ransomware providers.

Jndot

Assessed to be a part of FIN7’s pentester team.

Brilliant

Assessed to be a part of FIN7’s affiliate team.

Morgan

Assessed to be a part of FIN7’s affiliate team.

aramis.se

Assessed to be a part of FIN7’s affiliate team.

Team Structure: FIN7

srst

Assessed to be a part of FIN7’s affiliate team.

diez

Assessed to be a part of FIN7’s affiliate team.

Junior

Assessed to be a part of FIN7’s affiliate team.

Dorlan

Assessed to be a part of FIN7’s affiliate team.

ASX

Assessed to be a part of FIN7’s affiliate team.

Tranquility

Assessed to be a part of FIN7’s affiliate team.

Docker

Assessed to be a part of FIN7’s affiliate team.

Att

Assessed to be a part of FIN7’s affiliate team.

Ruben

Assessed to be a part of FIN7’s affiliate team.

fgood

Assessed to be a part of FIN7’s affiliate team.

hbonorato

Assessed to be a part of FIN7’s affiliate team

Team Structure: FIN7

Kermit

Assessed to be a part of FIN7’s affiliate team.

EQX

Assessed to be a part of FIN7’s affiliate team.

Known Tools: FIN7

7zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.
Alexa	It is used by the threat groups to evaluate analytics data including traffic size of victims' websites, likely to determine if the target is worth the cyberattack.
Amazon S3 Buckets	A service that offers object storage through a web service interface, is often used to host tools and malware.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
Atera	A remote monitoring and network discovery tool that provides a comprehensive security scan and complete view of all your end-user networks and devices.
AvNeutralizer	AKA AuKill. A specialized, custom tool used to tamper with security solutions that has been marketed on cybercriminal forums and used by multiple threat groups.
Azure Blob Storage	Microsoft's object storage solution for the cloud. It has been used to store exfiltrated data from compromised victims.
BoatLaunch	A helper module that patches PowerShell processes on the compromised systems with a 5-byte instruction sequence that results in an AMSI-bypass.
Checkmark's	A tool that automatically performs post-exploitation steps after the threat actors gain initial access.

Known Tools: FIN7

Checkpoint Software Loader	A remote access tool that has been observed being FIN7’s primary remote access tool, likely providing threat groups with persistent access to compromised environments.
cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
Core Impact	A penetration testing tool designed for exploitation activities that offers an extensive library of exploits, allows a threat actor to take control of the impacted device, and connect with the C2.
CrackMapExec	An open-source tool that leverages Mimikatz to enable users to harvest credentials and move laterally through an Active Directory environment.
Crunchbase	It is used by the threat groups to evaluate the size and profits of a potential target, likely to determine what to set as the ransom demand.
DNB	It is used by the threat groups to evaluate the size and profits of a potential target, likely to determine what to set as the ransom demand.
EasyLook	A reconnaissance that captures a wide range of data from infected systems, including operating system version, registration key, system name, username, domain information, and hardware specifications.
Google Drive	A file storage and synchronization service that threat actors have used to host malware or export stolen files to.
Google Scripts	An application development platform that has been abused by threat actors to develop and store malicious applications.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.

Known Tools: FIN7

MEGA	A cloud storage and file hosting service.
MetaSploit	A tool that can be used by threat actors to probe systematic vulnerabilities on networks and servers.
Meterpreter	Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
mshta.exe	A Windows-native binary designed to execute Microsoft HTML Application (HTA) files.
MSIX-PackageSupportFramework	A framework of tools that have been used to create their malicious MSIX files.
Mustat	It is used by the threat groups to evaluate analytics data including traffic size of victims' websites, likely to determine if the target is worth the cyberattack.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
OpenSSH	A suite of secure networking utilities based on the Secure Shell protocol. It is a connectivity tool for remote login with the SSH protocol.
Owler	It is used by the threat groups to evaluate the size and profits of a potential target, likely to determine what to set as the ransom demand.
Pastebin	A text storage site used by threat actors to host malware.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.

Known Tools: FIN7

PowerSploit

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.

PuTTY

A free and open-source terminal emulator, serial console and network file transfer application.

Rclone

A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.

RDP

A protocol that provides a user with a graphical interface to connect to another computer over a network connection.

rundll32.exe

A command line utility in Microsoft Windows used to run DLLs on the Windows operating system.

schtasks.exe

A utility used to schedule execution of programs or scripts on a Windows system to run at a specific date and time.

Similarweb

It is used by the threat groups to evaluate analytics data including traffic size of victims' websites, likely to determine if the target is worth the cyberattack.

sqlmap

An open-source penetration testing tool that can be used to automate the process of detecting and exploiting SQL injection flaws.

Tasklist

A utility that displays a list of applications and services with their Process IDs for all tasks running on either a local or a remote computer.

TeamViewer

A comprehensive, remote access, remote control and remote support solution that works with almost every desktop and mobile platform, including Windows, macOS, Android, and iOS.

TightVNC

A remote desktop software that allows users to access and control a computer over the network.

TinyMet

A Meterpreter stager that supports various transports and allows destination port and destination host setting during runtime.

Known Tools: FIN7

whoami	A command that displays user, group, and privileges information for the user who is currently logged on to the local system.
WMI	A utility that allows script languages to manage Microsoft Windows personal computers and server.

Known Malware: FIN7

7Logger	A keylogger malware that is used to collect system information and credentials that can be used for further compromise.
Astra	A malware control panel, written in PHP, that functions as a script-management system, pushing attack scripts to compromised computers.
AveMaria	An information stealer that uses AutoIT for wrapping.
BabyMetal	A tunneling malware based on the TinyMet Meterpreter tool, primarily used to execute Meterpreter reverse shell payloads.
Bateleur	A backdoor malware that used sophisticated anti-analysis and sandbox evasion techniques. The malware allows the group to maintain persistence.
BeakDrop	A malware variant observed in FIN7 campaigns around 2022. Little analysis has been done on the variant.
Bellhop	A JavaScript backdoor interpreted using the native Windows Scripting Host (WSH). The malware is capable of performing basic host information gathering and gains persistence.
BioLoad	A loader malware that is written in C++ and has been used to deploy second-stage payloads.
Birddog	AKA SocksBot, Nadrac. A malware that has the ability to enumerate processes, take screenshots, download/upload/write/execute files, create and inject into new processes, and communicate with C2 via sockets.
BirdWatch	A .NET-based downloader that retrieves payloads over HTTP, writing them to disk and then executing them. The malware uploads reconnaissance information from targeted system as well.
Black Basta Ransomware	A ransomware operation that conducts double extortion methods and maintains a data leak site where victim data is leaked if the ransom demand is not paid.
BlackMatter Ransomware	A ransomware operation that conducted double extortion methods and maintained a data leak site where victim data was leaked if the ransom demand was not paid.

Known Malware: FIN7

BoostWrite
An in-memory-only dropper that decrypts embedded payloads using an encryption key retrieved from a remote server at runtime.

Carbanak
AKA Anunak, Sekur RAT. A backdoor malware that is capable of exploiting known Windows vulnerability, CVE-2013-3660, and maintains persistent access to victim environments.

Clop Ransomware
A ransomware operation that conducts double extortion methods and maintains a data leak site where victim data is leaked if the ransom demand is not paid.

Conti Ransomware
A ransomware operation that conducted double extortion methods and maintained a data leak site where victim data was leaked if the ransom demand was not paid.

CrowView
A .NET-based loader malware that can how an embedded payload, self-delete, and support additional arguments.

CultSwap
A malware variant observed in FIN7 campaigns around 2020. Little analysis has been done on the variant.

DarkSide Ransomware
A ransomware operation that conducted double extortion methods and maintained a data leak site where victim data was leaked if the ransom demand was not paid.

DaveShell
Shellcode that functions as an in-memory dropper relying on reflective injection.

DNS Messenger
AKA TextMate. A tunneling malware that makes use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. That malware allows the threat actor to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the threat actor.

DNSbot
A multiprotocol backdoor used to exchange commands and push data to and from compromised machines.

Driftpin
A small and simple backdoor that enables the attackers to assess the victim.

Known Malware: FIN7

EugenLoader	A Windows trojan that has been used to inject Carbanak malware.
Flyhigh	A downloader, written in C using the Excel XLL SDK, but masquerades as using the Excel-DNA framework.
Gozi	AKA Snifula, Ursnif, CRM, Papras. A malware payload that is used to extract system information and steal user credentials that can be used for persistence, privilege escalation, and more.
Griffon	AKA Harpy. A lightweight JScript validator-style implant without any persistence mechanism. The malware is designed for receiving modules to be executed in-memory and sending the results to C2s.
HalfBaked	A family of malware that consists of multiple components designed to establish and maintain a foothold in victim networks, with the ultimate goal of gaining access to sensitive financial information.
IceBot	A RAT malware that allows the threat group to maintain remote access, collect system information, and connect to the C2.
JSSLoader	A RAT with multiple capabilities that were introduced over time. The malware has been used to download the DiceLoader malware.
Lizar	AKA DiceLoader, Remote System Client, Tirion. A minimal backdoor that enables a threat group to establish a C2 channel. The backdoor allows the threat actor to control the system, load additional payloads, and maintain persistent access to victim environments.
LoadOut	An obfuscated VBScript-based downloader which harvests extensive information from the infected system.
LockBit Ransomware	A ransomware operation that conducts double extortion methods and maintains a data leak site where victim data is leaked if the ransom demand is not paid.
Maze Ransomware	A ransomware operation that conducts double extortion methods and maintains a data leak site where victim data is leaked if the ransom demand is not paid.

Known Malware: FIN7

Minodo Backdoor	A backdoor malware that gathers basic system information, sends the information to the threat actor's C2, and receives an AES encrypted payload. While it has not been confirmed that FIN7 has used the malware, the group has been assessed to be the likely developer of the malware.
NetSupport RAT	A malicious version of the legitimate NetSupport Manager. The malware allows threat actors to maintain persistent access to compromised environments.
Nymaim	AKA Nymain. A downloader malware that has been observed deploying the Gozi malware variant.
Pillowmint	A PoS malware designed to capture credit card information.
Powerpipe	A malware variant observed in FIN7 campaigns around 2020. Little analysis has been done on the variant.
PowerPlant	AKA KillACK. A PowerShell-based backdoor with a breadth of capabilities, depending on which modules are delivered from the C2 server.
PowerSource	A PowerShell backdoor that obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage.
PowerTrash	A heavily obfuscated PowerShell script that is designed to reflectively load an embedded PE file in-memory.
RDF Sniffer	A payload of BoostWrite that appears to have been developed to tamper with NCR Corporation's "Aloha Command Center" client. The malware loads into the same process as the Command Center process by abusing the DLL load order of the legitimate Aloha utility.
REvil Ransomware	A ransomware operation that conducted double extortion methods and maintained a data leak site where victim data was leaked if the ransom demand was not paid.
Ryuk Ransomware	A ransomware variant used to encrypt victim networks and demand ransom payments in exchange for a decryption key.

Known Malware: FIN7

SalsaVerde.SayCheese	A malware variant observed in FIN7 campaigns around 2020. Little analysis has been done on the variant.
Simplecred	A malware variant observed in FIN7 campaigns around 2020. Little analysis has been done on the variant.
SQLRat	A RAT malware that drops files and executes SQL scripts on the host system.
SSH-based Backdoor	A backdoor malware designed to provide the threat group with persistent access to compromised devices.
StoneBoat	A .NET-based in-memory dropper which decrypts a shellcode payload embedded in it.
TakeOut	A malware variant observed in FIN7 campaigns around 2020. Little analysis has been done on the variant.
Termite	A password protected memory-only dropper that contains an encrypted shellcode payload.
ThreeDog	A malware variant observed in FIN7 campaigns around 2020. Little analysis has been done on the variant.
Wingnight	A WSF-based downloader that utilizes VBScript.

MITRE ATT&CK® Mappings: FIN7

Execution	
T1583: Acquire Infrastructure	.001: Domains .003: Virtual Private Server .006: Web Services .008: Malvertising
T1587: Develop Capabilities	.001: Malware
T1588: Obtain Capabilities	.002: Tool .003: Code Signing Certificates .004: Digital Certificates
T1608: Stage Capabilities	.001: Upload Malware .003: Install Digital Certificate .004: Drive-by Target .005: Link Target
Initial Access	
T1189: Drive-by Compromise	
T1190: Exploit Public-Facing Application	
T1195: Supply Chain Compromise	.002: Compromise Software Supply Chain
T1199: Trusted Relationship	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link .004: Spearphishing Voice
Execution	
T1047: Windows Management Instrumentation	

MITRE ATT&CK® Mappings: FIN7

Execution	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .005: Visual Basic .007: JavaScript
T1204: User Execution	.001: Malicious Link .002: Malicious File
T1559: Inter-Process Communication	.002: Dynamic Data Exchange
T1569: System Services	.002: Service Execution
Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1176: Browser Extensions	
T1543: Create or Modify System Process	.003: Windows Service
T1546: Event Triggered Execution	.011: Application Shimming
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
Defense Evasion	
T1027: Obfuscated Files or Information	.001: Binary Padding .005: Indicator Removal from Tools .010: Command Obfuscation

MITRE ATT&CK® Mappings: FIN7

Defense Evasion	
T1036: Masquerading	.003: Rename System Utilities .004: Masquerade Task or Service .005: Match Legitimate Name or Location
T1055: Process Injection	
T1070: Indicator Removal	.004: File Deletion
T1140: Deobfuscate/Decode Files or Information	
T1218: System Binary Proxy Execution	.005: Mshta .010: Regsvr32 .011: Rundll32
T1222: File and Directory Permissions Modification	.001: Windows File and Directory Permissions Modification
T1497: Virtualization/Sandbox Evasion	.001: System Checks .002: User Activity Based Checks
T1553: Subvert Trust Controls	.002: Code Signing
T1562: Impair Defenses	.004: Disable or Modify System Firewall
T1564: Hide Artifacts	.001: Hidden Files and Directories .003: Hidden Window
T1620: Reflective Code Loading	
Credential Access	
T1056: Input Capture	.003: Web Portal Capture
T1110: Brute Force	.002: Password Cracking

MITRE ATT&CK® Mappings: FIN7

Credential Access	
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers
T1558: Steal or Forge Kerberos Tickets	.003: Kerberoasting
Discovery	
T1012: Query Registry	
T1033: System Owner/User Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.002: Domain Account
T1124: System Time Discovery	
T1482: Domain Trust Discovery	
T1518: Software Discovery	.001: Security Software Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .004: SSH .005: VNC

MITRE ATT&CK® Mappings: FIN7

Lateral Movement	
T1091: Replication Through Removable Media	
T1210: Exploitation of Remote Services	
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1113: Screen Capture	
T1125: Video Capture	
T1213: Data from Information Repositories	
T1560: Archive Collected Data	
Command and Control	
T1008: Fallback Channels	
T1071: Application Layer Protocol	.004: DNS
T1090: Proxy	
T1095: Non-Application Layer Protocol	
T1105: Ingress Tool Transfer	
T1132: Data Encoding	.001: Standard Encoding

MITRE ATT&CK® Mappings: FIN7

Command and Control	
T1219: Remote Access Software	
T1571: Non-Standard Port	
T1573: Encrypted Channel	.002: Asymmetric Cryptography
T1665: Hide Infrastructure	
Exfiltration	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1486: Data Encrypted for Impact	
T1491: Defacement	.001: Internal Defacement
T1657: Financial Theft	

References

- Abdo, Bryce; Work, Zander; Teaca, Ioana; McKeague, Brendan (2022, April 04) Mandiant: “FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7.” https://cloud.google.com/blog/topics/threat-intelligence/evolution-of-fin7/
- Cocomazzi, Antonio (2024, July 17) SentinelLabs: “FIN7 Reboot | Cybercrime Gang Enhances Ops with New EDR Bypasses and Automated Attacks.” https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/
- eSentire Threat Response Unit (TRU) (2024, May 08) “FIN7 Uses Trusted Brands and Sponsored Google Ads to Distribute MSIX Payloads.” https://www.esentire.com/blog/fin7-uses-trusted-brands-and-sponsored-google-ads-to-distribute-msix-payloads
- ETDA (2024, June 18) “APT group: FIN7.” https://apt.etda.or.th/cgi-bin/showcard.cgi?g=FIN7&n=1
- Flashpoint Intel Team (2019, March 20) “FIN7 Revisited: Inside Astra Panel and SQLRat Malware.” https://flashpoint.io/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/
- Hammond, Charlotte; Villadsen, Ole (2023, April 27) Security Intelligence: “Ex-Conti and FIN7 actors collaborate with new backdoor.” https://securityintelligence.com/x-force/ex-conti-fin7-actors-collaborate-new-backdoor/
- Lambert, Tony; Bohlmann, Tyler, et. al. (2024, July 18) Red Canary: “MSIX installer malware delivery on the rise across multiple campaigns.” https://redcanary.com/blog/threat-intelligence/msix-installers/
- McWhirt, Matthew; Erickson, Jon; Palombo, DJ (2017, May 03) Mandiant: “To SDB, Or Not To SDB: FIN7 Leveraging Shim Databases for Persistence.” https://cloud.google.com/blog/topics/threat-intelligence/fin7-shim-databases-persistence/
- Misgav, Omri (2019, December 26) Fortinet: “Introducing BIOLOAD: FIN7 BOOSTWRITE’s Lost Twin.” https://www.fortinet.com/blog/threat-research/bioload-fin7-boostwrite-lost-twin
- MITRE (2024, April 17) “FIN7.” https://attack.mitre.org/groups/G0046/
- Palli, Ishita Chigilli (2020, May 27) “Another Alleged FIN7 Cybercrime Gang Member Arrested.” https://www.bankinfosecurity.com/another-alleged-fin7-cybercrime-gang-member-arrested-a-14345
- PRODAFT (2022, December) “FIN7 Unveiled: A deep dive into notorious cybercrime gang.”https://www.ledecodeur.ch/wp-content/uploads/2022/12/Prodaft-2022-FIN7-Unveiled.pdf
- Silent Push (2024, July 10) “FIN7: Silent Push unearths the largest group of FIN7 domains ever discovered. 4000+ IOFA domains and IPs found. Louvre, Meta, and Reuters targeted in massive global phishing and malware campaigns.” https://www.silentpush.com/blog/fin7/
- Singh, Neeraj; Nejad, Mohammad Kazem Hassan (2023, April 26) WithSecure Labs: “FIN7 tradecraft seen in attacks against Veeam backup servers.” https://labs.withsecure.com/publications/fin7-target-veeam-servers
- The BlackBerry Research and Intelligence Team (2024, April 17) “Threat Group FIN7 Targets the U.S. Automotive Industry.” https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry

References

- U.S. DoJ (2018, August 01) “Three Members of Notorious International Cybercrime Group “Fin7” In Custody for Role in Attacking Over 100 U.S. companies.” https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100
- U.S. DoJ (2023, May 03) “Team from Western Washington honored for investigation and prosecution of major cybercrime group Fin7.” https://www.justice.gov/usao-wdwa/pr/team-western-washington-honored-investigation-and-prosecution-major-cybercrime-group

Adversary Pursuit Group