FIN7, GOLD NIAGARA, ITG14, Carbon Spider, ELBRUS, Sangria Tempest, Group G0046

Archived: 2026-04-05 14:45:06 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

FIN7 has used the PowerShell script 3CF9.ps1 and the executable WsTaskLoad to enumerate domain administrations by executing `net group "Domain Admins" /domain`.[12] FIN7 has also used csvde.exe, which is a built-in Windows command line tool, to export Active Directory information.

Enterprise T1583 .001 Acquire Infrastructure: Domains

FIN7 has registered look-alike domains for use in phishing campaigns.[13] Additionally, FIN7 has registered a malicious domain as `advanced-ip-sccanner[.]com` that redirected to an adversary-controlled Dropbox which contained the malicious executable.[12]

.006 Acquire Infrastructure: Web Services

FIN7 has set up Amazon S3 buckets to host trojanized digital products.[6]

Enterprise T1071 .004 Application Layer Protocol: DNS

FIN7 has performed C2 using DNS via A, OPT, and TXT records.[4]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

FIN7 malware has created Registry Run and RunOnce keys to establish persistence, and has also added items to the Startup folder.[2][4]

Enterprise T1059 Command and Scripting Interpreter

FIN7 used SQL scripts to help perform tasks on the victim's machine.[4][14][4]

.001 PowerShell

FIN7 used a PowerShell script to launch shellcode that retrieved an additional payload.[2][15][16][6][17] Additionally, FIN7 has executed a custom obfuscation of the shellcode invoker in PowerSploit called POWERTRASH.[12]

.003 Windows Command Shell

FIN7 used the command prompt to launch commands on the victim’s machine.[4][14][6] Additionally, FIN7 has used cmd.exe to open the Run dialog by sending the "Windows + R" keys through malicious USBs acting as virtual keyboards.[17]

.005 Visual Basic

FIN7 used VBS scripts to help perform tasks on the victim's machine.[4][14][5]

.007 JavaScript

FIN7 used JavaScript scripts to help perform tasks on the victim's machine.[4][14]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

FIN7 created new Windows services and added them to the startup directories for persistence.[4]

Enterprise T1486 Data Encrypted for Impact

FIN7 has encrypted virtual disk volumes on ESXi servers using a version of Darkside ransomware.[5][6] Additionally, FIN7 has deployed ransomware as the end payload during big game hunting.[12]

Enterprise T1005 Data from Local System

FIN7 has collected files and other sensitive information from a compromised network.[5]

Enterprise T1140 Deobfuscate/Decode Files or Information

FIN7 has decoded a malicious PowerShell script using `certutil -decode hex` and has decoded an XOR-obfuscated block of data with the key `qawsed1q2w3e`, which led to the installation of Lizar.[17]

Enterprise T1587 .001 Develop Capabilities: Malware

FIN7 has developed malware for use in operations, including the creation of infected removable media.[16][18]

Enterprise T1546 .011 Event Triggered Execution: Application Shimming

FIN7 has used application shim databases for persistence.[19]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

FIN7 has exfiltrated stolen data to the MEGA file sharing site.[5]

Enterprise T1190 Exploit Public-Facing Application

FIN7 has compromised targeted organizations through exploitation of CVE-2021-31207 in Exchange.[10]

Enterprise T1210 Exploitation of Remote Services

FIN7 has exploited ZeroLogon (CVE-2020-1472) against vulnerable domain controllers.[5]

Enterprise T1008 Fallback Channels

FIN7's Harpy backdoor malware can use DNS as a backup channel for C2 if HTTP fails.[20]

Enterprise T1591 Gather Victim Org Information

FIN7 has compiled a list of victims by filtering companies by revenue using Zoominfo, which is a service that provides business information.[7]

.004 Identify Roles

FIN7 has identified IT staff and employees who had higher levels of administrative rights.[12]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

FIN7 has used `attrib +h "C:\ProgramData\ssh"` to make the SSH folder hidden.[12]

.003 Hide Artifacts: Hidden Window

FIN7 has used .txt files to conceal PowerShell commands.[17]

Enterprise T1562 .004 Impair Defenses: Disable or Modify System Firewall

FIN7 has added a firewall rule to allow TCP port 59999 inbound and a rule to allow sshd.exe on TCP port 9898.[12]

Enterprise T1105 Ingress Tool Transfer

FIN7 has downloaded additional malware to execute on the victim's machine, including by using a PowerShell script to launch shellcode that retrieves an additional payload.[2][21][6][17]

Enterprise T1674 Input Injection

FIN7 has used malicious USBs to emulate keystrokes to launch PowerShell to download and execute malware from the adversary's server.[16][17]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

FIN7 spear phishing campaigns have included malicious Word documents with DDE execution.[22]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

FIN7 has created a scheduled task named "AdobeFlashSync" to establish persistence.[15]

.005 Masquerading: Match Legitimate Resource Name or Location

FIN7 has attempted to run Darkside ransomware with the filename sleep.exe.[5] Additionally, FIN7 has mimicked WsTaskLoad.exe, which is associated with the Wondershare software suite, by using a malicious executable under the same name.[12]

Enterprise T1571 Non-Standard Port

FIN7 has used port-protocol mismatches on ports such as 53, 80, 443, and 8080 during C2.[4] FIN7 has used TCP ports 59999 and 9898 for firewall rules.[12]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

FIN7 has used fragmented strings, environment variables, standard input (stdin), and native character-replacement functionalities to obfuscate commands.[23][4][5]

.016 Obfuscated Files or Information: Junk Code Insertion

FIN7 has used random junk code to obfuscate malware code.[6]

Enterprise T1588 .002 Obtain Capabilities: Tool

FIN7 has utilized a variety of tools such as Cobalt Strike, PowerSploit, and the remote management tool, Atera for targeting efforts.[6]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

FIN7 has used the command `net group "domain admins" /domain` to enumerate domain groups.[6][12]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

FIN7 sent spearphishing emails with either malicious Microsoft Documents or RTF files attached.[2][21][14][13][5]

.002 Phishing: Spearphishing Link

FIN7 has conducted broad phishing campaigns using malicious links.[5] Additionally, FIN7 has sent spearphishing emails containing a typosquatted link to "ip-sccanner[.]com."[12]

Enterprise T1057 Process Discovery

FIN7 has used the PowerShell script 3CF9.ps1 to perform process discovery by executing `tasklist /v`. Additionally, WsTaskLoad.exe executes `tasklist /v` to perform process discovery.[12]

Enterprise T1572 Protocol Tunneling

FIN7 has tunneled C2 traffic via OpenSSH.[12]

Enterprise T1620 Reflective Code Loading

FIN7 has loaded a .NET assembly into the currect execution context via `Reflection.Assembly::Load`.[17]

Enterprise T1219 Remote Access Tools

FIN7 has utilized the remote management tool Atera to download malware to a compromised system.[6]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

FIN7 has used RDP to move laterally in victim environments.[5]

.004 Remote Services: SSH

FIN7 has used SSH to move laterally through victim environments.[5]

.005 Remote Services: VNC

FIN7 has used TightVNC to control compromised hosts.[5]

Enterprise T1091 Replication Through Removable Media

FIN7 actors have mailed USB drives to potential victims containing malware that downloads and installs various backdoors, including in some cases for ransomware operations.[16] Additionally, FIN7 has used malicious USBs that acted as virtual keyboards to install malware and txt files that decode to PowerShell commands.[17]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

FIN7 malware has created scheduled tasks to establish persistence.[2][15][4][14] Specifically, FIN7 has used OpenSSH to establish persistence.[12]

Enterprise T1113 Screen Capture

FIN7 captured screenshots and desktop video recordings.[21]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

FIN7 has staged legitimate software, that was trojanized to contain an Atera agent installer, on Amazon S3.[6] FIN7 has also used an open directory web server as a staging server for payloads and other tools, such as OpenSSH and 7zip.[24]

.004 Stage Capabilities: Drive-by Target

FIN7 has compromised a digital product website and modified multiple download links to point to trojanized versions of offered digital products.[6]

.005 Stage Capabilities: Link Target

FIN7 has created a fake link that redirected to an adversary-controlled Dropbox that downloaded the malicious executable.[12]

Enterprise T1558 .003 Steal or Forge Kerberos Tickets: Kerberoasting

FIN7 has used Kerberoasting PowerShell commands such as, `Invoke-Kerberoast` for credential access and to enable lateral movement.[5][6]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

FIN7 has signed Carbanak payloads with legally purchased code signing certificates. FIN7 has also digitally signed their phishing documents, backdoors and other staging tools to bypass security controls.[3][4]

Enterprise T1195 .002 Supply Chain Compromise: Compromise Software Supply Chain

FIN7 has gained initial access by compromising a victim's software supply chain.[6]

Enterprise T1218 .005 System Binary Proxy Execution: Mshta

FIN7 has used mshta.exe to execute VBScript to execute malicious code on victim systems.[2]

.011 System Binary Proxy Execution: Rundll32

FIN7 has used `rundll32.exe` to execute malware on a compromised network.[6]

Enterprise T1082 System Information Discovery

FIN7 has used csvde.exe, which is a built-in Windows command line tool, to export system information. Additionally, WsTaskLoad has gathered system information, such as operating system and hostname.[12]

Enterprise T1033 System Owner/User Discovery

FIN7 has used the command `cmd.exe /C quser` to collect user session information.[6]

Enterprise T1569 .002 System Services: Service Execution

FIN7 has started the SSH service by executing `sc start sshd`.[12]

Enterprise T1124 System Time Discovery

FIN7 has used the PowerShell script 3CF9.ps1 to execute `net time`.[12]

Enterprise T1204 .001 User Execution: Malicious Link

FIN7 has used malicious links to lure victims into downloading malware.[5]

.002 User Execution: Malicious File

FIN7 lured victims to double-click on images in the attachments they sent which would then execute the hidden LNK file.[2][13][5] Additionally, FIN7 has used malicious Microsoft Word and Excel files and Leo VBS to distribute an updated version of JSS Loader and to distribute the Harpy backdoor.[25]

Enterprise T1078 Valid Accounts

FIN7 has harvested valid administrative credentials for lateral movement.[5]

.003 Local Accounts

FIN7 has used compromised credentials for access as SYSTEM on Exchange servers.[10]

Enterprise T1125 Video Capture

FIN7 created a custom video recording capability that could be used to monitor operations in the victim's environment.[4][21]

Enterprise T1497 .002 Virtualization/Sandbox Evasion: User Activity Based Checks

FIN7 used images embedded into document lures that only activate the payload when a user double clicks to avoid sandboxes.[2]

Enterprise T1102 .002 Web Service: Bidirectional Communication

FIN7 used legitimate services like Google Docs, Google Scripts, and Pastebin for C2.[4]

Enterprise T1047 Windows Management Instrumentation

FIN7 has used WMI to install malware on targeted systems.[13]
