FIN8, Syssphinx, Group G0061 | MITRE ATT&CK®

Archived: 2026-04-05 14:30:27 UTC

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

FIN8 has used a malicious framework designed to impersonate the lsass.exe/vmtoolsd.exe token.[5][4]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

FIN8 has used HTTPS for command and control.[5]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

FIN8 has used RAR to compress collected data before exfiltration.[6]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

FIN8's malicious spearphishing payloads are executed as PowerShell. FIN8 has also used PowerShell for lateral movement and credential access.[1][5][6][4]

.003 Command and Scripting Interpreter: Windows Command Shell

FIN8 has used a Batch file to automate frequently executed post compromise cleanup activities.[6] FIN8 has also executed commands remotely via `cmd.exe`.[1][5][4]

Enterprise T1486 Data Encrypted for Impact

FIN8 has deployed ransomware such as Ragnar Locker, White Rabbit, and attempted to execute Noberus on compromised networks.[4]

Enterprise T1074 .002 Data Staged: Remote Data Staging

FIN8 aggregates staged data from a network into a single location.[6]

Enterprise T1482 Domain Trust Discovery

FIN8 has retrieved a list of trusted domains by using `nltest.exe /domain_trusts`.[5]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

FIN8 has used the Plink utility to tunnel RDP back to C2 infrastructure.[6]

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

FIN8 has used WMI event subscriptions for persistence.[5]

Enterprise T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

FIN8 has used FTP to exfiltrate collected data.[6]

Enterprise T1068 Exploitation for Privilege Escalation

FIN8 has exploited the CVE-2016-0167 local vulnerability.[2][6]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

FIN8 has cleared logs during post compromise cleanup activities.[6]

.004 Indicator Removal: File Deletion

FIN8 has deleted tmp and prefetch files during post compromise cleanup activities. FIN8 has also deleted PowerShell scripts to evade detection on compromised machines.[6][4]

Enterprise T1105 Ingress Tool Transfer

FIN8 has used remote code execution to download subsequent payloads.[2][5]

Enterprise T1112 Modify Registry

FIN8 has deleted Registry keys during post compromise cleanup activities.[6]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

FIN8 has used environment variables and standard input (stdin) to obfuscate command-line arguments. FIN8 also obfuscates malicious macros delivered as payloads.[1][6][5]

Enterprise T1588 .002 Obtain Capabilities: Tool

FIN8 has used open-source tools such as Impacket for targeting efforts.[3]

.003 Obtain Capabilities: Code Signing Certificates

FIN8 has used an expired open-source X.509 certificate for testing in the OpenSSL repository, to connect to actor-controlled C2 servers.[3]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

FIN8 harvests credentials using Invoke-Mimikatz or Windows Credentials Editor (WCE).[6]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

FIN8 has distributed targeted emails containing Word documents with embedded malicious macros.[1][2][6]

.002 Phishing: Spearphishing Link

FIN8 has distributed targeted emails containing links to malicious documents with embedded macros.[6]

Enterprise T1055 .004 Process Injection: Asynchronous Procedure Call

FIN8 has injected malicious code into a new svchost.exe process.[5]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

FIN8 has used RDP for lateral movement.[6]

.002 Remote Services: SMB/Windows Admin Shares

FIN8 has attempted to map to C$ on enumerated hosts to test the scope of their current credentials/context. FIN8 has also used smbexec from the Impacket suite for lateral movement.[6][3]

Enterprise T1018 Remote System Discovery

FIN8 has used dsquery and other Active Directory utilities to enumerate hosts; they have also used `nltest.exe /dclist` to retrieve a list of domain controllers.[6][5]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

FIN8 has used scheduled tasks to maintain RDP backdoors.[6]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

FIN8 has used Registry keys to detect and avoid executing in potential sandboxes.[6]

Enterprise T1082 System Information Discovery

FIN8 has used PowerShell Scripts to check the architecture of a compromised machine before the selection of a 32-bit or 64-bit version of a malicious .NET loader.[4]

Enterprise T1016 .001 System Network Configuration Discovery: Internet Connection Discovery

FIN8 has used the Ping command to check connectivity to actor-controlled C2 servers.[3]

Enterprise T1033 System Owner/User Discovery

FIN8 has executed the command `quser` to display the session details of a compromised machine.[4]

Enterprise T1204 .001 User Execution: Malicious Link

FIN8 has used emails with malicious links to lure victims into installing malware.[1][2][6]

.002 User Execution: Malicious File

FIN8 has used malicious e-mail attachments to lure victims into executing malware.[1][2][6]

Enterprise T1078 Valid Accounts

FIN8 has used valid accounts for persistence and lateral movement.[6]

Enterprise T1102 Web Service

FIN8 has used `sslip.io`, a free IP to domain mapping service that also makes SSL certificate generation easier for traffic encryption, as part of their command and control.[5]

Enterprise T1047 Windows Management Instrumentation

FIN8's malicious spearphishing payloads use WMI to launch malware and spawn `cmd.exe` execution. FIN8 has also used WMIC and the Impacket suite for lateral movement, as well as during and post compromise cleanup activities.[1][5][6][4]
