FIN13, Elephant Beetle, Group G1016

Archived: 2026-04-05 13:45:40 UTC

Enterprise T1134 .003 Access Token Manipulation: Make and Impersonate Token

FIN13 has utilized tools such as Incognito V2 for token manipulation and impersonation.[2]

Enterprise T1087 Account Discovery

FIN13 has enumerated all users and their roles from a victim's main treasury system.[1]

.002 Domain Account

FIN13 can identify user accounts associated with a Service Principal Name and query Service Principal Names within the domain by utilizing the following scripts: `GetUserSPNs.vbs` and `querySpn.vbs`.[1][2]

Enterprise T1098 .007 Account Manipulation: Additional Local or Domain Groups

FIN13 has assigned newly created accounts the sysadmin role to maintain persistence.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

FIN13 has used HTTP requests to chain multiple web shells and to contact actor-controlled C2 servers prior to exfiltrating stolen data.[1][2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

FIN13 has compressed the dump output of compromised credentials with a 7zip binary.[2]

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

FIN13 has used Windows Registry run keys such as, `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\hosts` to maintain persistence.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

FIN13 has used PowerShell commands to obtain DNS data from a compromised network.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

FIN13 has leveraged `xp_cmdshell` and Windows Command Shell to execute commands on a compromised machine. FIN13 has also attempted to leverage the ‘xp_cmdshell’ SQL procedure to execute remote commands on internal MS-SQL servers.[1][2]

.005 Command and Scripting Interpreter: Visual Basic

FIN13 has used VBS scripts for code execution on comrpomised machines.[2]

Enterprise T1136 .001 Create Account: Local Account

FIN13 has created MS-SQL local accounts in a compromised network.[2]

Enterprise T1005 Data from Local System

FIN13 has gathered stolen credentials, sensitive data such as point-of-sale (POS), and ATM data from a compromised network before exfiltration.[1][2]

Enterprise T1565 Data Manipulation

FIN13 has injected fraudulent transactions into compromised networks that mimic legitimate behavior to siphon off incremental amounts of money.[2]

Enterprise T1074 .001 Data Staged: Local Data Staging

FIN13 has utilized the following temporary folders on compromised Windows and Linux systems for their operations prior to exfiltration: `C:\Windows\Temp` and `/tmp`.[1][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

FIN13 has utilized `certutil` to decode base64 encoded versions of custom malware.[1]

Enterprise T1587 .001 Develop Capabilities: Malware

FIN13 has utilized custom malware to maintain persistence in a compromised environment.[1][2]

Enterprise T1190 Exploit Public-Facing Application

FIN13 has exploited known vulnerabilities such as CVE-2017-1000486 (Primefaces Application Expression Language Injection), CVE-2015-7450 (WebSphere Application Server SOAP Deserialization Exploit), CVE-2010-5326 (SAP NewWeaver Invoker Servlet Exploit), and EDB-ID-24963 (SAP NetWeaver ConfigServlet Remote Code Execution) to gain initial access.[1][2]

Enterprise T1133 External Remote Services

FIN13 has gained access to compromised environments via remote access services such as the corporate virtual private network (VPN).[1]

Enterprise T1083 File and Directory Discovery

FIN13 has used the Windows `dir` command to enumerate files and directories in a victim's network.[1]

Enterprise T1657 Financial Theft

FIN13 has observed the victim's software and infrastructure over several months to understand the technical process of legitimate financial transactions, prior to attempting to conduct fraudulent transactions.[2]

Enterprise T1589 Gather Victim Identity Information

FIN13 has researched employees to target for social engineering attacks.[1]

Enterprise T1590 .004 Gather Victim Network Information: Network Topology

FIN13 has searched for infrastructure that can provide remote access to an environment for targeting efforts.[1]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

FIN13 has created hidden files and folders within a compromised Linux system `/tmp` directory. FIN13 also has used `attrib.exe` to hide gathered local host information.[1][2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

FIN13 has used IISCrack.dll as a side-loading technique to load a malicious version of httpodbc.dll on old IIS Servers (CVE-2001-0507).[2]

Enterprise T1105 Ingress Tool Transfer

FIN13 has downloaded additional tools and malware to compromised systems.[1][2]

Enterprise T1056 .001 Input Capture: Keylogging

FIN13 has logged the keystrokes of victims to escalate privileges.[1]

Enterprise T1036 Masquerading

FIN13 has masqueraded staged data by using the Windows certutil utility to generate fake Base64 encoded certificates with the input file.[1][2]

.004 Masquerade Task or Service

FIN13 has used scheduled tasks names such as `acrotyr` and `AppServicesr` to mimic the same names in a compromised network's `C:\Windows` directory.[1]

.005 Match Legitimate Resource Name or Location

FIN13 has masqueraded WAR files to look like legitimate packages such as, wsexample.war, wsexamples.com, examples.war, and exampl3s.war.[2]

Enterprise T1556 Modify Authentication Process

FIN13 has replaced legitimate KeePass binaries with trojanized versions to collect passwords from numerous applications.[1]

Enterprise T1046 Network Service Discovery

FIN13 has utilized `nmap` for reconnaissance efforts. FIN13 has also scanned for internal MS-SQL servers in a compromised network.[1][2]

Enterprise T1135 Network Share Discovery

FIN13 has executed net view commands for enumeration of open shares on compromised machines.[1][2]

Enterprise T1588 .002 Obtain Capabilities: Tool

FIN13 has utilized publicly available tools such as Mimikatz, Impacket, PWdump7, ProcDump, Nmap, and Incognito V2 for targeting efforts.[2]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

FIN13 has obtained memory dumps with ProcDump to parse and extract credentials from a victim's LSASS process memory with Mimikatz.[1][2]

.002 OS Credential Dumping: Security Account Manager

FIN13 has extracted the SAM and SYSTEM registry hives using the `reg.exe` binary for obtaining password hashes from a compromised machine.[2]

.003 OS Credential Dumping: NTDS

FIN13 has harvested the NTDS.DIT file and leveraged the Impacket tool on the compromised domain controller to locally decrypt it.[2]

Enterprise T1069 Permission Groups Discovery

FIN13 has enumerated all users and roles from a victim's main treasury system.[1]

Enterprise T1572 Protocol Tunneling

FIN13 has utilized web shells and Java tools for tunneling capabilities to and from compromised assets.[2]

Enterprise T1090 .001 Proxy: Internal Proxy

FIN13 has utilized a proxy tool to communicate between compromised assets.[2]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

FIN13 has remotely accessed compromised environments via Remote Desktop Services (RDS) for lateral movement.[1]

.002 Remote Services: SMB/Windows Admin Shares

FIN13 has leveraged SMB to move laterally within a compromised network via application servers and SQL servers.[2]

.004 Remote Services: SSH

FIN13 has remotely accessed compromised environments via secure shell (SSH) for lateral movement.[1]

.006 Remote Services: Windows Remote Management

FIN13 has leveraged `WMI` to move laterally within a compromised network via application servers and SQL servers.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

FIN13 has created scheduled tasks in the `C:\Windows` directory of the compromised network.[1]

Enterprise T1505 .003 Server Software Component: Web Shell

FIN13 has utilized obfuscated and open-source web shells such as JspSpy, reGeorg, MiniWebCmdShell, and Vonloesch Jsp File Browser 1.2 to enable remote code execution and to execute commands on compromised web server.[2]

Enterprise T1082 System Information Discovery

FIN13 has collected local host information by utilizing Windows commands `systeminfo`, `fsutil`, and `fsinfo`. FIN13 has also utilized a compromised Symantex Altiris console and LanDesk account to retrieve host information.[1][2]

Enterprise T1016 System Network Configuration Discovery

FIN13 has used `nslookup` and `ipconfig` for network reconnaissance efforts. FIN13 has also utilized a compromised Symantec Altiris console and LanDesk account to retrieve network information.[1][2]

.001 Internet Connection Discovery

FIN13 has used `Ping` and `tracert` for network reconnaissance efforts.[1]

Enterprise T1049 System Network Connections Discovery

FIN13 has used `netstat` and other net commands for network reconnaissance efforts.[1]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

FIN13 has obtained administrative credentials by browsing through local files on a compromised machine.[2]

Enterprise T1550 .002 Use Alternate Authentication Material: Pass the Hash

FIN13 has used the PowerShell utility `Invoke-SMBExec` to execute the pass the hash method for lateral movement within an compromised environment.[1]

Enterprise T1078 .001 Valid Accounts: Default Accounts

FIN13 has leveraged default credentials for authenticating myWebMethods (WMS) and QLogic web management interface to gain initial access.[2]

Enterprise T1047 Windows Management Instrumentation

FIN13 has utilized `WMI` to execute commands and move laterally on compromised Windows machines.[1][2]
