FIN6, Magecart Group 6, ITG08, Skeleton Spider, TAAL, Camouflage Tempest, Group G0037

Archived: 2026-04-05 17:42:18 UTC

Enterprise T1134 Access Token Manipulation

FIN6 has used has used Metasploit’s named-pipe impersonation technique to escalate privileges.[2]

Enterprise T1087 .002 Account Discovery: Domain Account

FIN6 has used Metasploit’s PsExec NTDSGRAB module to obtain a copy of the victim's Active Directory database.[1]

Enterprise T1560 Archive Collected Data

Following data collection, FIN6 has compressed log files into a ZIP archive prior to staging and exfiltration.[1]

.003 Archive via Custom Method

FIN6 has encoded data gathered from the victim with a simple substitution cipher and single-byte XOR using the 0xAA key, and Base64 with character permutation.[1][7]

Enterprise T1119 Automated Collection

FIN6 has used a script to iterate through a list of compromised PoS systems, copy and remove data to a log file, and to bind to events from the submit payment button.[1][7]

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

FIN6 has used Registry Run keys to establish persistence for its downloader tools known as HARDTACK and SHIPBREAD.[1]

Enterprise T1110 .002 Brute Force: Password Cracking

FIN6 has extracted password hashes from ntds.dit to crack offline.[1]

Enterprise T1059 Command and Scripting Interpreter

FIN6 has used scripting to iterate through a list of compromised PoS systems, copy data to a log file, and remove the original data files.[1][2]

.001 PowerShell

FIN6 has used PowerShell to gain access to merchant's networks, and a Metasploit PowerShell module to download and execute shellcode and to set up a local listener.[1][2][8]

.003 Windows Command Shell

FIN6 has used `kill.bat` script to disable security tools.[2]

.007 JavaScript

FIN6 has used malicious JavaScript to steal payment card data from e-commerce sites.[7]

Enterprise T1555 Credentials from Password Stores

FIN6 has used the Stealer One credential stealer to target e-mail and file transfer utilities including FTP.[8]

.003 Credentials from Web Browsers

FIN6 has used the Stealer One credential stealer to target web browsers.[8]

Enterprise T1213 .006 Data from Information Repositories: Databases

FIN6 has collected schemas and user accounts from systems running SQL Server.[8]

Enterprise T1005 Data from Local System

FIN6 has collected and exfiltrated payment card data from compromised systems.[7][9][10]

Enterprise T1074 .002 Data Staged: Remote Data Staging

FIN6 actors have compressed data from remote systems and moved it to another staging system before exfiltration.[1]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

FIN6 used the Plink command-line utility to create SSH tunnels to C2 servers.[1]

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

FIN6 has sent stolen payment card data to remote servers via HTTP POSTs.[7]

Enterprise T1068 Exploitation for Privilege Escalation

FIN6 has used tools to exploit Windows vulnerabilities in order to escalate privileges. The tools targeted CVE-2013-3660, CVE-2011-2005, and CVE-2010-4398, all of which could allow local users to access kernel-level privileges.[1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

FIN6 has deployed a utility script named `kill.bat` to disable anti-virus.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

FIN6 has removed files from victim machines.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

FIN6 has renamed the "psexec" service name to "mstdc" to masquerade as a legitimate Windows service.[2]

Enterprise T1046 Network Service Discovery

FIN6 used publicly available tools (including Microsoft's built-in SQL querying tool, osql.exe) to map the internal network and conduct reconnaissance against Active Directory, Structured Query Language (SQL) servers, and NetBIOS.[1]

Enterprise T1095 Non-Application Layer Protocol

FIN6 has used Metasploit Bind and Reverse TCP stagers.[7]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

FIN6 has used encoded PowerShell commands.[8]

Enterprise T1588 .002 Obtain Capabilities: Tool

FIN6 has obtained and used tools such as Mimikatz, Cobalt Strike, and AdFind.[4][2]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

FIN6 has used Windows Credential Editor for credential dumping.[1][2]

.003 OS Credential Dumping: NTDS

FIN6 has used Metasploit’s PsExec NTDSGRAB module to obtain a copy of the victim's Active Directory database.[1][2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

FIN6 has targeted victims with e-mails containing malicious attachments.[8]

.003 Phishing: Spearphishing via Service

FIN6 has used fake job advertisements sent via LinkedIn to spearphish targets.[4]

Enterprise T1572 Protocol Tunneling

FIN6 used the Plink command-line utility to create SSH tunnels to C2 servers.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

FIN6 used RDP to move laterally in victim networks.[1][2]

Enterprise T1018 Remote System Discovery

FIN6 used publicly available tools (including Microsoft's built-in SQL querying tool, osql.exe) to map the internal network and conduct reconnaissance against Active Directory, Structured Query Language (SQL) servers, and NetBIOS.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

FIN6 has used scheduled tasks to establish persistence for various malware it uses, including downloaders known as HARDTACK and SHIPBREAD and FrameworkPOS.[1]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

FIN6 has used Comodo code-signing certificates.[4]

Enterprise T1569 .002 System Services: Service Execution

FIN6 has created Windows services to execute encoded PowerShell commands.[2]

Enterprise T1204 .002 User Execution: Malicious File

FIN6 has used malicious documents to lure victims into allowing execution of PowerShell scripts.[8]

Enterprise T1078 Valid Accounts

To move laterally on a victim network, FIN6 has used credentials stolen from various systems on which it gathered usernames and password hashes.[1][2][8]

Enterprise T1102 Web Service

FIN6 has used Pastebin and Google Storage to host content for their operations.[2]

Enterprise T1047 Windows Management Instrumentation

FIN6 has used WMI to automate the remote execution of PowerShell scripts.[4]
