Empire, Software S0363 | MITRE ATT&CK®

Archived: 2026-04-05 16:19:09 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

Empire includes various modules to attempt to bypass UAC for escalation of privileges.[2]

Enterprise T1134 Access Token Manipulation

Empire can use PowerSploit's `Invoke-TokenManipulation` to manipulate access tokens.[2]

.002 Create Process with Token

Empire can use `Invoke-RunAs` to make tokens.[2]

.005 SID-History Injection

Empire can add a SID-History to a user if on a domain controller.[2]

Enterprise T1087 .001 Account Discovery: Local Account

Empire can acquire local and domain user account information.[2]

.002 Account Discovery: Domain Account

Empire can acquire local and domain user account information.[2][4]

Enterprise T1557 .001 Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay

Empire can use Inveigh to conduct name service poisoning for credential theft and associated relay attacks.[2][5]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Empire can conduct command and control over protocols like HTTP and HTTPS.[2]

Enterprise T1560 Archive Collected Data

Empire can ZIP directories on the target system.[2]

Enterprise T1119 Automated Collection

Empire can automatically gather the username, domain name, machine name, and other information from a compromised system.[6]

Enterprise T1020 Automated Exfiltration

Empire has the ability to automatically send collected data back to the threat actors' C2.[6]

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

Empire can modify the registry run keys `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` and `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` for persistence.[2]

.005 Boot or Logon Autostart Execution: Security Support Provider

Empire can enumerate Security Support Providers (SSPs) as well as utilize PowerSploit's `Install-SSP` and `Invoke-Mimikatz` to install malicious SSPs and log authentication events.[2]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Empire can persist by modifying a .LNK file to include a backdoor.[2]

Enterprise T1217 Browser Information Discovery

Empire has the ability to gather browser data such as bookmarks and visited sites.[2]

Enterprise T1115 Clipboard Data

Empire can harvest clipboard data on both Windows and macOS systems.[2]

Enterprise T1059 Command and Scripting Interpreter

Empire uses a command-line interface to interact with systems.[2]

.001 PowerShell

Empire leverages PowerShell for the majority of its client-side agent tasks. Empire also contains the ability to conduct PowerShell remoting with the `Invoke-PSRemoting` module.[2][1]

.003 Windows Command Shell

Empire has modules for executing scripts.[2]

Enterprise T1136 .001 Create Account: Local Account

Empire has a module for creating a local user if permissions allow.[2]

.002 Create Account: Domain Account

Empire has a module for creating a new domain user if permissions allow.[2]

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

Empire can utilize built-in modules to modify service binaries and restore them to their original state.[2]

Enterprise T1555 .001 Credentials from Password Stores: Keychain

Empire uses the command `/usr/bin/security dump-keychain -d` to read the keychain credential.[7]

.003 Credentials from Password Stores: Credentials from Web Browsers

Empire can use modules that extract passwords from common web browsers such as Firefox and Chrome.[2]

Enterprise T1484 .001 Domain or Tenant Policy Modification: Group Policy Modification

Empire can use `New-GPOImmediateTask` to modify a GPO that will install and execute a malicious Scheduled Task/Job.[2]

Enterprise T1482 Domain Trust Discovery

Empire has modules for enumerating domain trusts.[2]

Enterprise T1114 .001 Email Collection: Local Email Collection

Empire has the ability to collect emails on a target system.[2]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Empire can use TLS to encrypt its C2 channel.[2]

Enterprise T1546 .008 Event Triggered Execution: Accessibility Features

Empire can leverage WMI debugging to remotely replace binaries like sethc.exe, Utilman.exe, and Magnify.exe with cmd.exe.[2]

Enterprise T1041 Exfiltration Over C2 Channel

Empire can send data gathered from a target through the command and control channel.[2][6]

Enterprise T1567 .001 Exfiltration Over Web Service: Exfiltration to Code Repository

Empire can use GitHub for data exfiltration.[2]

.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Empire can use Dropbox for data exfiltration.[2]

Enterprise T1068 Exploitation for Privilege Escalation

Empire can exploit vulnerabilities such as MS16-032 and MS16-135.[2]

Enterprise T1210 Exploitation of Remote Services

Empire has a limited number of built-in modules for exploiting remote SMB, JBoss, and Jenkins servers.[2]

Enterprise T1083 File and Directory Discovery

Empire includes various modules for finding files of interest on hosts and network shares.[2]

Enterprise T1615 Group Policy Discovery

Empire includes various modules for enumerating Group Policy.[2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Empire contains modules that can discover and exploit various DLL hijacking opportunities.[2]

.004 Hijack Execution Flow: Dylib Hijacking

Empire has a dylib hijacker module that generates a malicious dylib given the path to a legitimate dylib of a vulnerable application.[2]

.007 Hijack Execution Flow: Path Interception by PATH Environment Variable

Empire contains modules that can discover and exploit path interception opportunities in the PATH environment variable.[2]

.008 Hijack Execution Flow: Path Interception by Search Order Hijacking

Empire contains modules that can discover and exploit search order hijacking vulnerabilities.[2]

.009 Hijack Execution Flow: Path Interception by Unquoted Path

Empire contains modules that can discover and exploit unquoted path vulnerabilities.[2]

Enterprise T1070 .006 Indicator Removal: Timestomp

Empire can timestomp any files or payloads placed on a target machine to help them blend in.[2]

Enterprise T1105 Ingress Tool Transfer

Empire can upload and download to and from a victim machine.[2]

Enterprise T1056 .001 Input Capture: Keylogging

Empire includes keylogging capabilities for Windows, Linux, and macOS systems.[2]

.004 Input Capture: Credential API Hooking

Empire contains some modules that leverage API hooking to carry out tasks, such as netripper.[2]

Enterprise T1106 Native API

Empire contains a variety of enumeration modules that have an option to use API calls to carry out tasks.[2]

Enterprise T1046 Network Service Discovery

Empire can perform port scans from an infected host.[2]

Enterprise T1135 Network Share Discovery

Empire can find shared drives on the local system.[2]

Enterprise T1040 Network Sniffing

Empire can be used to conduct packet captures on target hosts.[2]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Empire has the ability to obfuscate commands using `Invoke-Obfuscation`.[2]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Empire contains an implementation of Mimikatz to gather credentials from memory.[2]

Enterprise T1057 Process Discovery

Empire can find information about processes running on local and remote systems.[2][6]

Enterprise T1055 Process Injection

Empire contains multiple modules for injecting into processes, such as `Invoke-PSInject`.[2]

Enterprise T1021 .003 Remote Services: Distributed Component Object Model

Empire can utilize `Invoke-DCOM` to leverage remote COM execution for lateral movement.[2]

.004 Remote Services: SSH

Empire contains modules for executing commands over SSH as well as in-memory VNC agent injection.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Empire has modules to interact with the Windows task scheduler.[2]

Enterprise T1113 Screen Capture

Empire is capable of capturing screenshots on Windows and macOS systems.[2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Empire can enumerate antivirus software on the target.[2]

Enterprise T1558 .001 Steal or Forge Kerberos Tickets: Golden Ticket

Empire can leverage its implementation of Mimikatz to obtain and use golden tickets.[2]

.002 Steal or Forge Kerberos Tickets: Silver Ticket

Empire can leverage its implementation of Mimikatz to obtain and use silver tickets.[2]

.003 Steal or Forge Kerberos Tickets: Kerberoasting

Empire uses PowerSploit's `Invoke-Kerberoast` to request service tickets and return crackable ticket hashes.[2]

Enterprise T1082 System Information Discovery

Empire can enumerate host system information like OS, architecture, domain name, applied patches, and more.[2] [6]

Enterprise T1016 System Network Configuration Discovery

Empire can acquire network configuration information like DNS servers, public IP, and network proxies used by a host.[2][6]

Enterprise T1049 System Network Connections Discovery

Empire can enumerate the current network connections of a host.[2]

Enterprise T1033 System Owner/User Discovery

Empire can enumerate the username on targeted hosts.[6]

Enterprise T1569 .002 System Services: Service Execution

Empire can use PsExec to execute a payload on a remote host.[2]

Enterprise T1127 .001 Trusted Developer Utilities Proxy Execution: MSBuild

Empire can use built-in modules to abuse trusted utilities like MSBuild.exe.[2]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

Empire can use various modules to search for files containing passwords.[2]

.004 Unsecured Credentials: Private Keys

Empire can use modules like `Invoke-SessionGopher` to extract private key and session information.[2]

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

Empire can perform pass the hash attacks.[2]

Enterprise T1125 Video Capture

Empire can capture webcam data on Windows and macOS systems.[2]

Enterprise T1102 .002 Web Service: Bidirectional Communication

Empire can use Dropbox and GitHub for C2.[2]

Enterprise T1047 Windows Management Instrumentation

Empire can use WMI to deliver a payload to a remote host.[2]
