Havoc, Software S1229 | MITRE ATT&CK®

Archived: 2026-04-05 13:58:20 UTC

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

Havoc has a module capable of token impersonation.[1]

Enterprise T1087 Account Discovery

Havoc can identify privileged user accounts on infected systems.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Havoc can use HTTP/S listeners to establish and maintain C2 communications. [1][3][2][4]

.002 Application Layer Protocol: File Transfer Protocols

Havoc can use an SMB listener for C2 communication.[1][3][4]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Havoc can facilitate the execution of PowerShell commands.[4]

.003 Command and Scripting Interpreter: Windows Command Shell

Havoc can execute commands via `cmd.exe`.[1][4]

Enterprise T1005 Data from Local System

Havoc can download files from the victim's computer.[1][4]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Havoc can send an AES encrypted check-in request to the C2 server.[3][2]

Enterprise T1083 File and Directory Discovery

The Havoc interface can display a file explorer view of the compromised host.[1]

Enterprise T1105 Ingress Tool Transfer

Havoc has the ability to upload files to infected systems.[1][4]

Enterprise T1559 Inter-Process Communication

The Havoc SMB demon can use named pipes for communication through a parent demon.[1]

Enterprise T1570 Lateral Tool Transfer

Havoc has the ability to copy files from one location to another.[1]

Enterprise T1106 Native API

Havoc can use `NtAllocateVirtualMemory` and `NtCreateThreadEx` to aid process injection.[1]

Enterprise T1566 .002 Phishing: Spearphishing Link

Havoc has been distributed through ClickFix phishing campaigns.[2]

Enterprise T1057 Process Discovery

Havoc can enumerate processes on targeted hosts.[1][3][2]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Havoc has DLL spawn and injection modules.[1]

.002 Process Injection: Portable Executable Injection

Havoc has itself injected into `C:\\Windows\\System32\\Werfault.exe` on targeted systems.[1]

Enterprise T1090 Proxy

Havoc has the ability to route HTTP/S communications through designated proxies.[1]

Enterprise T1018 Remote System Discovery

Havoc features a module capable of host enumeration.[1]

Enterprise T1113 Screen Capture

Havoc can capture screenshots.[1][3][4]

Enterprise T1082 System Information Discovery

Havoc can gather system information including hostname, domain, and OS details.[2]

Enterprise T1016 System Network Configuration Discovery

Havoc has a module for network enumeration including determining IP addresses.[1]

.001 Internet Connection Discovery

The Havoc demon can check for a connection to the C2 server from the target machine.[3]

Enterprise T1033 System Owner/User Discovery

Havoc can trigger exection of `whoami` on the target host to display the current user.[3][2]

Enterprise T1204 .004 User Execution: Malicious Copy and Paste

The Havoc infection chain has been initiated via ClickFix lures in phishing emails.[2]

Enterprise T1497 .003 Virtualization/Sandbox Evasion: Time Based Checks

The Havoc demon agent can be set to sleep for a specified time.[1][3]
