# Crimson, Software S0115 | MITRE ATT&CK®

Archived: 2026-04-05 12:41:39 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Crimson can use a HTTP GET request to download its final payload.[1]

Enterprise T1123 Audio Capture

Crimson can perform audio surveillance using microphones.[2]

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

Crimson can add Registry run keys for persistence.[1][2]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Crimson has the ability to execute commands with the COMSPEC environment variable.[2]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Crimson contains a module to steal credentials from Web browsers on the victim machine.[1][2]

Enterprise T1005 Data from Local System

Crimson can collect information from a compromised host.[3]

Enterprise T1025 Data from Removable Media

Crimson contains a module to collect data from removable drives.[1][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Crimson can decode its encoded PE file prior to execution.[1]

Enterprise T1114 .001 Email Collection: Local Email Collection

Crimson contains a command to collect and exfiltrate emails from Outlook.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Crimson can exfiltrate stolen information over its C2.[3]

Enterprise T1083 File and Directory Discovery

Crimson contains commands to list files and directories, as well as search for files matching certain extensions from a defined list.[1][2][3]

Enterprise T1070 .004 Indicator Removal: File Deletion

Crimson has the ability to delete files from a compromised host.[1][2][3]

Enterprise T1105 Ingress Tool Transfer

Crimson contains a command to retrieve files from its C2 server.[1][2][3]

Enterprise T1056 .001 Input Capture: Keylogging

Crimson can use a module to perform keylogging on compromised hosts.[1][2][3]

Enterprise T1680 Local Storage Discovery

Crimson contains a command to collect disk drive information.[1][2][3]

Enterprise T1112 Modify Registry

Crimson can set a Registry key to determine how long it has been installed and possibly to indicate the version number.[1]

Enterprise T1095 Non-Application Layer Protocol

Crimson uses a custom TCP protocol for C2.[1][2]

Enterprise T1120 Peripheral Device Discovery

Crimson has the ability to discover pluggable/removable drives to extract files from.[1][2]

Enterprise T1057 Process Discovery

Crimson contains a command to list processes.[1][2][3]

Enterprise T1012 Query Registry

Crimson can check the Registry for the presence of `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\last_edate` to determine how long it has been installed on a host.[1]

Enterprise T1091 Replication Through Removable Media

Crimson can spread across systems by infecting removable media.[2]

Enterprise T1113 Screen Capture

Crimson contains a command to perform screen captures.[1][2][3]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Crimson contains a command to collect information about anti-virus software on the victim.[1][2]

Enterprise T1082 System Information Discovery

Crimson contains a command to collect the victim PC name and operating system.[1][2][3]

Enterprise T1614 System Location Discovery

Crimson can identify the geographical location of a victim host.[2]

Enterprise T1016 System Network Configuration Discovery

Crimson contains a command to collect the victim MAC address and LAN IP.[1][2]

Enterprise T1033 System Owner/User Discovery

Crimson can identify the user on a targeted system.[1][2][3]

Enterprise T1124 System Time Discovery

Crimson has the ability to determine the date and time on a compromised host.[2]

Enterprise T1125 Video Capture

Crimson can capture webcam video on targeted systems.[1][2]

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

Crimson can determine when it has been installed on a host for at least 15 days before downloading the final payload.[1]

---