

Machete, Software S0409 | MITRE ATT&CK®

Archived: 2026-04-05 17:30:40 UTC

Enterprise [T1071 .001 Application Layer Protocol: Web Protocols](#)

[Machete](#) uses HTTP for Command & Control. [\[1\]\[4\]\[3\]](#)

[.002 Application Layer Protocol: File Transfer Protocols](#)

[Machete](#) uses FTP for Command & Control. [\[1\]\[4\]\[3\]](#)

Enterprise [T1010 Application Window Discovery](#)

[Machete](#) saves the window names. [\[1\]](#)

Enterprise [T1560 Archive Collected Data](#)

[Machete](#) stores zipped files with profile data from installed web browsers. [\[1\]](#)

[.003 Archive via Custom Method](#)

[Machete](#)'s collected data is encrypted with AES before exfiltration. [\[1\]](#)

Enterprise [T1123 Audio Capture](#)

[Machete](#) captures audio from the computer's microphone. [\[2\]\[4\]\[3\]](#)

Enterprise [T1020 Automated Exfiltration](#)

[Machete](#)'s collected files are exfiltrated automatically to remote servers. [\[1\]](#)

Enterprise [T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder](#)

[Machete](#) used the startup folder for persistence. [\[2\]\[4\]](#)

Enterprise [T1217 Browser Information Discovery](#)

[Machete](#) retrieves the user profile data (e.g., browsers) from Chrome and Firefox browsers. [\[1\]](#)

Enterprise [T1115 Clipboard Data](#)

[Machete](#) hijacks the clipboard data by creating an overlapped window that listens to keyboard events. [\[1\]\[2\]](#)

Enterprise [T1059 .006 Command and Scripting Interpreter: Python](#)

[Machete](#) is written in Python and is used in conjunction with additional Python scripts. [\[1\]\[2\]\[3\]](#)

Enterprise [T1555 .003 Credentials from Password Stores: Credentials from Web Browsers](#)

[Machete](#) collects stored credentials from several web browsers.^[1]

Enterprise [T1132 .001 Data Encoding: Standard Encoding](#)

[Machete](#) has used base64 encoding.^[2]

Enterprise [T1005 Data from Local System](#)

[Machete](#) searches the File system for files of interest.^[1]

Enterprise [T1025 Data from Removable Media](#)

[Machete](#) can find, encrypt, and upload files from fixed and removable drives.^{[4][1]}

Enterprise [T1074 .001 Data Staged: Local Data Staging](#)

[Machete](#) stores files and logs in a folder on the local drive.^{[1][4]}

Enterprise [T1140 Deobfuscate/Decode Files or Information](#)

[Machete](#)'s downloaded data is decrypted using AES.^[1]

Enterprise [T1573 .001 Encrypted Channel: Symmetric Cryptography](#)

[Machete](#) has used AES to exfiltrate documents.^[1]

[.002 Encrypted Channel: Asymmetric Cryptography](#)

[Machete](#) has used TLS-encrypted FTP to exfiltrate data.^[4]

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[Machete](#)'s collected data is exfiltrated over the same channel used for C2.^[1]

Enterprise [T1052 .001 Exfiltration Over Physical Medium: Exfiltration over USB](#)

[Machete](#) has a feature to copy files from every drive onto a removable drive in a hidden folder.^{[1][2]}

Enterprise [T1008 Fallback Channels](#)

[Machete](#) has sent data over HTTP if FTP failed, and has also used a fallback server.^[1]

Enterprise [T1083 File and Directory Discovery](#)

[Machete](#) produces file listings in order to search for files to be exfiltrated.^{[1][4][3]}

Enterprise [T1564 .001 Hide Artifacts: Hidden Files and Directories](#)

[Machete](#) has the capability to exfiltrate stolen data to a hidden folder on a removable drive.^[1]

Enterprise [T1070 .004 Indicator Removal: File Deletion](#)

Once a file is uploaded, [Machete](#) will delete it from the machine.^[1]

Enterprise [T1105 Ingress Tool Transfer](#)

[Machete](#) can download additional files for execution on the victim's machine.^[1]

Enterprise [T1056 .001 Input Capture: Keylogging](#)

[Machete](#) logs keystrokes from the victim's machine.^{[1][2][4][3]}

Enterprise [T1036 .004 Masquerading: Masquerade Task or Service](#)

[Machete](#) renamed task names to masquerade as legitimate Google Chrome, Java, Dropbox, Adobe Reader and Python tasks.^[1]

[.005 Masquerading: Match Legitimate Resource Name or Location](#)

[Machete](#) renamed payloads to masquerade as legitimate Google Chrome, Java, Dropbox, Adobe Reader and Python executables.^{[1][2]}

Enterprise [T1027 .002 Obfuscated Files or Information: Software Packing](#)

[Machete](#) has been packed with NSIS.^[1]

[.010 Obfuscated Files or Information: Command Obfuscation](#)

[Machete](#) has used pyobfuscate, zlib compression, and base64 encoding for obfuscation. [Machete](#) has also used some visual obfuscation techniques by naming variables as combinations of letters to hinder analysis.^{[4][1]}

Enterprise [T1120 Peripheral Device Discovery](#)

[Machete](#) detects the insertion of new devices by listening for the WM_DEVICECHANGE window message.^[1]

Enterprise [T1057 Process Discovery](#)

[Machete](#) has a component to check for running processes to look for web browsers.^[1]

Enterprise [T1053 .005 Scheduled Task/Job: Scheduled Task](#)

The different components of [Machete](#) are executed by Windows Task Scheduler.^{[1][2]}

Enterprise [T1029 Scheduled Transfer](#)

[Machete](#) sends stolen data to the C2 server every 10 minutes.^[1]

Enterprise [T1113 Screen Capture](#)

[Machete](#) captures screenshots. ^{[1][2][4][3]}

Enterprise [T1082 System Information Discovery](#)

[Machete](#) collects the hostname of the target computer. ^[1]

Enterprise [T1016 System Network Configuration Discovery](#)

[Machete](#) collects the MAC address of the target computer and other network configuration information. ^{[1][3]}

[.002 Wi-Fi Discovery](#)

[Machete](#) uses the `netsh wlan show networks mode=bssid` and `netsh wlan show interfaces` commands to list all nearby WiFi networks and connected interfaces. ^[1]

Enterprise [T1552 .004 Unsecured Credentials: Private Keys](#)

[Machete](#) has scanned and looked for cryptographic keys and certificate file extensions. ^[1]

Enterprise [T1125 Video Capture](#)

[Machete](#) takes photos from the computer's web camera. ^{[2][4][3]}

Source: <https://attack.mitre.org/software/S0409/>