Mis-Type, Software S0084 | MITRE ATT&CK®

Archived: 2026-04-05 13:55:59 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Mis-Type may create a file containing the results of the command `cmd.exe /c net user {Username}` .[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Mis-Type network traffic can communicate over HTTP.[1]

Enterprise T1547 Boot or Logon Autostart Execution

Mis-Type has created registry keys for persistence, including `HKCU\Software\bkfouerioyou` , `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{6afa8072-b2b1-31a8-b5c1-{Unique Identifier}` , and `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{3BF41072-B2B1-31A8-B5C1-{Unique Identifier}` .[1]

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

Mis-Type has used `cmd.exe` to run commands on a compromised host.[1]

Enterprise T1136 .001 Create Account: Local Account

Mis-Type may create a temporary user on the system named `Lost_{Unique Identifier}` .[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Mis-Type uses Base64 encoding for C2 traffic.[1]

Enterprise T1005 Data from Local System

Mis-Type has collected files and data from a compromised host.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Mis-Type has temporarily stored collected information to the files `"%AppData%\{Unique Identifier}\HOSTRURKLSR"` and `"%AppData%\{Unique Identifier}\NEWERSSEMP"` .[1]

Enterprise T1041 Exfiltration Over C2 Channel

Mis-Type has transmitted collected files and data to its C2 server.[1]

Enterprise T1008 Fallback Channels

Mis-Type first attempts to use a Base64-encoded network protocol over a raw TCP socket for C2, and if that method fails, falls back to a secondary HTTP-based protocol to communicate to an alternate C2 server.[1]

Enterprise T1105 Ingress Tool Transfer

Mis-Type has downloaded additional malware and files onto a compromised host.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Mis-Type saves itself as a file named `msdtc.exe`, which is also the name of the legitimate Microsoft Distributed Transaction Coordinator service binary.[1][2]

Enterprise T1106 Native API

Mis-Type has used Windows API calls, including `NetUserAdd` and `NetUserDel`.[1]

Enterprise T1095 Non-Application Layer Protocol

Mis-Type network traffic can communicate over a raw socket.[1]

Enterprise T1055 Process Injection

Mis-Type has been injected directly into a running process, including `explorer.exe`.[1]

Enterprise T1082 System Information Discovery

The initial beacon packet for Mis-Type contains the operating system version and file system of the victim.[1]

Enterprise T1016 System Network Configuration Discovery

Mis-Type may create a file containing the results of the command `cmd.exe /c ipconfig /all`.[1]

Enterprise T1033 System Owner/User Discovery

Mis-Type runs tests to determine the privilege level of the compromised user.[1]
