RedLeaves, Software S0153 | MITRE ATT&CK®

Archived: 2026-04-05 12:50:05 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

RedLeaves can communicate to its C2 over HTTP and HTTPS if directed.[2][4]

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

RedLeaves attempts to add a shortcut file in the Startup folder to achieve persistence. If this fails, it attempts to add Registry Run keys.[1][4]

.009 Boot or Logon Autostart Execution: Shortcut Modification

RedLeaves attempts to add a shortcut file in the Startup folder to achieve persistence.[1][4]

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

RedLeaves can receive and execute commands with cmd.exe. It can also provide a reverse shell.[1][2]

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

RedLeaves can gather browser usernames and passwords.[4]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

RedLeaves has encrypted C2 traffic with RC4, previously using keys of 88888888 and babybear.[1]

Enterprise T1083 File and Directory Discovery

RedLeaves can enumerate and search for files and directories.[1][2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

RedLeaves is launched through use of DLL search order hijacking to load a malicious dll.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

RedLeaves can delete specified files.[1]

Enterprise T1105 Ingress Tool Transfer

RedLeaves is capable of downloading a file from a specified URL.[1]

Enterprise T1571 Non-Standard Port

RedLeaves can use HTTP over non-standard ports, such as 995, for C2.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

A RedLeaves configuration file is encrypted with a simple XOR key, 0x53.[1]

Enterprise T1113 Screen Capture

RedLeaves can capture screenshots.[2][4]

Enterprise T1082 System Information Discovery

RedLeaves can gather extended system information including the hostname, OS version number, platform, memory information, time elapsed since system startup, and CPU information.[1][4]

Enterprise T1016 System Network Configuration Discovery

RedLeaves can obtain information about network parameters.[1]

Enterprise T1049 System Network Connections Discovery

RedLeaves can enumerate drives and Remote Desktop sessions.[1]

Enterprise T1033 System Owner/User Discovery

RedLeaves can obtain information about the logged on user both locally and for Remote Desktop sessions.[1]
