LunarWeb, Software S1141 | MITRE ATT&CK®

Archived: 2026-04-05 15:13:34 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

LunarWeb can use `POST` to send victim identification to C2 and `GET` to retrieve commands.[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

LunarWeb can create a ZIP archive with specified files and directories.[1]

.002 Archive Collected Data: Archive via Library

LunarWeb can zlib-compress data prior to exfiltration.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

LunarWeb has the ability to run shell commands via PowerShell.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

LunarWeb can run shell commands using a BAT file with a name matching `%TEMP%\<random_9_alnum_chars>.batfile` or through cmd.exe with the `/c` and `/U` option for Unicode output.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

LunarWeb can use Base64 encoding to obfuscate C2 commands.[1]

Enterprise T1001 .002 Data Obfuscation: Steganography

LunarWeb can receive C2 commands hidden in the structure of .jpg and .gif images.[1]

Enterprise T1030 Data Transfer Size Limits

LunarWeb can split exfiltrated data that exceeds 1.33 MB in size into multiple random sized parts between 384 and 512 KB.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

LunarWeb can decrypt strings related to communication configuration using RC4 with a static key.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

LunarWeb can send AES encrypted C2 commands.[1]

.002 Encrypted Channel: Asymmetric Cryptography

LunarWeb can send short C2 commands, up to 512 bytes, encrypted with RSA-4096.[1]

Enterprise T1083 File and Directory Discovery

LunarWeb has the ability to retrieve directory listings.[1]

Enterprise T1615 Group Policy Discovery

LunarWeb can capture information on group policy settings[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

LunarWeb can self-delete from a compromised host if safety checks of C2 connectivity fail.[1]

Enterprise T1559 Inter-Process Communication

LunarWeb can retrieve output from arbitrary processes and shell commands via a pipe.[1]

Enterprise T1104 Multi-Stage Channels

LunarWeb can use one C2 URL for first contact and to upload information about the host computer and two additional C2 URLs for getting commands.[1]

Enterprise T1135 Network Share Discovery

LunarWeb can identify shared resources in compromised environments.[1]

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

The LunarWeb install files have been encrypted with AES-256.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

LunarWeb can discover local group memberships.[1]

Enterprise T1057 Process Discovery

LunarWeb has used shell commands to list running processes.[1]

Enterprise T1572 Protocol Tunneling

LunarWeb can run a custom binary protocol under HTTPS for C2.[1]

Enterprise T1090 Proxy

LunarWeb has the ability to use a HTTP proxy server for C&C communications.[1]

Enterprise T1518 Software Discovery

LunarWeb can list installed software on compromised systems.[1]

.001 Security Software Discovery

LunarWeb has run shell commands to obtain a list of installed security products.[1]

Enterprise T1082 System Information Discovery

LunarWeb can use WMI queries and shell commands such as systeminfo.exe to collect the operating system, BIOS version, and domain name of the targeted system.[1]

Enterprise T1016 System Network Configuration Discovery

LunarWeb can use shell commands to discover network adapters and configuration.[1]

Enterprise T1049 System Network Connections Discovery

LunarWeb can enumerate system network connections.[1]

Enterprise T1033 System Owner/User Discovery

LunarWeb can collect user information from the targeted host.[1]

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

LunarWeb can pause for a number of hours before entering its C2 communication loop.[1]

Enterprise T1047 Windows Management Instrumentation

LunarWeb can use WMI queries for discovery on the victim host.[1]
