# CORESHELL, Software S0137 | MITRE ATT&CK®

Archived: 2026-04-05 18:26:02 UTC

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | CORESHELL can communicate over HTTP for C2.[1][4] |
| | | .003 | Application Layer Protocol: Mail Protocols | CORESHELL can communicate over SMTP and POP3 for C2.[1][4] |
| Enterprise | T1547 | .001 | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | CORESHELL has established persistence by creating autostart extensibility point (ASEP) Registry entries in the Run key and other Registry keys, as well as by creating shortcuts in the Internet Explorer Quick Start folder.[4] |
| Enterprise | T1132 | .001 | Data Encoding: Standard Encoding | CORESHELL C2 messages are Base64-encoded.[1] |
| Enterprise | T1573 | .001 | Encrypted Channel: Symmetric Cryptography | CORESHELL C2 messages are encrypted with custom stream ciphers using six-byte or eight-byte keys.[1] |
| Enterprise | T1105 | | Ingress Tool Transfer | CORESHELL downloads another dropper from its C2 server.[1] |
| Enterprise | T1680 | | Local Storage Discovery | CORESHELL collects the volume serial number from the victim and sends the information to its C2 server.[1] |

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1027 | | Obfuscated Files or Information | CORESHELL obfuscates strings using a custom stream cipher.[1] |
| | | .016 | Junk Code Insertion | CORESHELL contains unused machine instructions in a likely attempt to hinder analysis. [1] |
| Enterprise | T1218 | .011 | System Binary Proxy Execution: Rundll32 | CORESHELL is installed via execution of rundll32 with an export named "init" or "InitW." [4] |
| Enterprise | T1082 | | System Information Discovery | CORESHELL collects hostname and OS version data from the victim and sends the information to its C2 server.[1] |