# TSCookie, Software S0436 | MITRE ATT&CK®

Archived: 2026-04-02 10:57:30 UTC

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | TSCookie can multiple protocols including HTTP and HTTPS in communication with command and control (C2) servers.[2][1] |
| Enterprise | T1059 | .003 | Command and Scripting Interpreter: Windows Command Shell | TSCookie has the ability to execute shell commands on the infected host.[1] |
| Enterprise | T1555 | .003 | Credentials from Password Stores: Credentials from Web Browsers | TSCookie has the ability to steal saved passwords from the Internet Explorer, Edge, Firefox, and Chrome browsers.[1] |
| Enterprise | T1140 | | Deobfuscate/Decode Files or Information | TSCookie has the ability to decrypt, load, and execute a DLL and its resources.[1] |
| Enterprise | T1573 | .001 | Encrypted Channel: Symmetric Cryptography | TSCookie has encrypted network communications with RC4.[1] |
| Enterprise | T1083 | | File and Directory Discovery | TSCookie has the ability to discover drive information on the infected host.[1] |
| Enterprise | T1105 | | Ingress Tool Transfer | TSCookie has the ability to upload and download files to and from the infected host.[1] |
| Enterprise | T1095 | | Non-Application Layer Protocol | TSCookie can use ICMP to receive information on the destination server.[2] |

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1057 | | Process Discovery | TSCookie has the ability to list processes on the infected host.[1] |
| Enterprise | T1055 | | Process Injection | TSCookie has the ability to inject code into the svchost.exe, iexplorer.exe, explorer.exe, and default browser processes.[2] |
| Enterprise | T1090 | | Proxy | TSCookie has the ability to proxy communications with command and control (C2) servers.[2] |
| Enterprise | T1016 | | System Network Configuration Discovery | TSCookie has the ability to identify the IP of the infected host.[1] |
| Enterprise | T1204 | .001 | User Execution: Malicious Link | TSCookie has been executed via malicious links embedded in e-mails spoofing the Ministries of Education, Culture, Sports, Science and Technology of Japan.[1] |

Source: https://attack.mitre.org/software/S0436