# Explosive, Software S0569 | MITRE ATT&CK®

Archived: 2026-04-05 16:01:42 UTC

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | Explosive has used HTTP for communication.[1] |
| Enterprise | T1115 | | Clipboard Data | Explosive has a function to use the OpenClipboard wrapper.[1] |
| Enterprise | T1025 | | Data from Removable Media | Explosive can scan all .exe files located in the USB drive.[1] |
| Enterprise | T1573 | .001 | Encrypted Channel: Symmetric Cryptography | Explosive has encrypted communications with the RC4 method.[2] |
| Enterprise | T1564 | .001 | Hide Artifacts: Hidden Files and Directories | Explosive has commonly set file and path attributes to hidden.[1] |
| Enterprise | T1105 | | Ingress Tool Transfer | Explosive has a function to download a file to the infected system.[1] |
| Enterprise | T1056 | .001 | Input Capture: Keylogging | Explosive has leveraged its keylogging capabilities to gain access to administrator accounts on target servers.[1][2] |
| Enterprise | T1112 | | Modify Registry | Explosive has a function to write itself to Registry values.[1] |
| Enterprise | T1106 | | Native API | Explosive has a function to call the OpenClipboard wrapper.[1] |

| Domain | ID | Name | Use |
| --- | --- | --- | --- |
| Enterprise | T1082 | System Information Discovery | Explosive has collected the computer name from the infected host.[1] |
| Enterprise | T1016 | System Network Configuration Discovery | Explosive has collected the MAC address from the victim's machine.[1] |
| Enterprise | T1033 | System Owner/User Discovery | Explosive has collected the username from the infected host.[1] |

---

Source: https://attack.mitre.org/software/S0569