S-Type, Software S0085 | MITRE ATT&CK®

Archived: 2026-04-05 13:53:54 UTC

Enterprise T1087 .001 Account Discovery: Local Account

S-Type has run the command `net user` on a victim.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

S-Type uses HTTP for C2.[1]

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

S-Type may create a .lnk file to itself that is saved in the Start menu folder. It may also create the Registry key `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ IMJPMIJ8.1{3 characters of Unique Identifier}`.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

S-Type may create the file `%HOMEPATH%\Start Menu\Programs\Startup\Realtek {Unique Identifier}.lnk`, which points to the malicious `msdtc.exe` file already created in the `%CommonFiles%` directory.[1]

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

S-Type has provided the ability to execute shell commands on a compromised host.[1]

Enterprise T1136 .001 Create Account: Local Account

S-Type may create a temporary user on the system named `Lost_{Unique Identifier}` with the password `pond~!@6"{Unique Identifier}`.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

S-Type uses Base64 encoding for C2 traffic.[1]

Enterprise T1041 Exfiltration Over C2 Channel

S-Type has uploaded data and files from a compromised host to its C2 servers.[1]

Enterprise T1008 Fallback Channels

S-Type primarily uses port 80 for C2, but falls back to ports 443 or 8080 if initial communication fails.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

S-Type has deleted files it has created on a compromised host.[1]

.009 Indicator Removal: Clear Persistence

S-Type has deleted accounts it has created.[1]

Enterprise T1105 Ingress Tool Transfer

S-Type can download additional files onto a compromised host.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

S-Type may save itself as a file named `msdtc.exe`, which is also the name of the legitimate Microsoft Distributed Transaction Coordinator service binary.[1][2]

Enterprise T1106 Native API

S-Type has used Windows APIs, including `GetKeyboardType`, `NetUserAdd`, and `NetUserDel`.[1]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Some S-Type samples have been packed with UPX.[1]

Enterprise T1082 System Information Discovery

The initial beacon packet for S-Type contains the operating system version and file system of the victim.[1]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

S-Type has attempted to determine if a compromised system was using a Japanese keyboard via the `GetKeyboardType` API call.[1]

Enterprise T1016 System Network Configuration Discovery

S-Type has used `ipconfig /all` on a compromised host.[1]

Enterprise T1033 System Owner/User Discovery

S-Type has run tests to determine the privilege level of the compromised user.[1]

Enterprise T1007 System Service Discovery

S-Type runs the command `net start` on a victim.[1]
