Sagerunex, Software S1210 | MITRE ATT&CK®

Archived: 2026-04-05 14:33:03 UTC

Enterprise T1134 Access Token Manipulation

Sagerunex finds the `explorer.exe` process after execution and uses it to change the token of its executing thread. [1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Sagerunex communicates via HTTPS, at times using a hard-coded User Agent of `Mozilla/5.0 (compatible; MSIE 7.0; Win32)` .[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Sagerunex has archived collected materials in RAR format.[2]

Enterprise T1074 .001 Data Staged: Local Data Staging

Sagerunex gathers host information and stages it locally as a RAR file prior to exfiltration.[2] Sagerunex stores logged data in an encrypted file located at `%TEMP%/TS_FB56.tmp` during execution.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Sagerunex uses a custom decryption routine to unpack itself during installation.[2]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Sagerunex uses HTTPS for command and control communication.[1]

Enterprise T1480 Execution Guardrails

Sagerunex uses a "servicemain" function to verify its environment to ensure it can only be executed as a service, as well as the existence of a configuration file in a specified directory.[2]

Enterprise T1041 Exfiltration Over C2 Channel

Sagerunex encrypts collected system data then exfiltrates via existing command and control channels.[2]

Enterprise T1106 Native API

Sagerunex calls the `WaitForSingleObject` API function as part of time-check logic.[2]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Sagerunex has used VMProtect to pack and obscure itself.[2]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Sagerunex can be passed a reference to an XOR-encrypted configuration file at runtime.[1]

Enterprise T1057 Process Discovery

Sagerunex identifies the `explorer.exe` process on the executing system.[1]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Sagerunex is designed to be dynamic link library (DLL) injected into an infected endpoint and executed directly in memory.[2]

Enterprise T1090 Proxy

Sagerunex uses several proxy configuration settings to ensure connectivity.[2]

Enterprise T1082 System Information Discovery

Sagerunex gathers information from the infected system such as hostname.[2]

Enterprise T1016 System Network Configuration Discovery

Sagerunex will gather system information such as MAC and IP addresses.[2]

Enterprise T1102 .002 Web Service: Bidirectional Communication

Sagerunex has used virtual private servers (VPS) for command and control traffic as well as third-party cloud services in more recent variants.[2]

.003 Web Service: One-Way Communication

Sagerunex has used web services such as Twitter for command and control purposes.[2]
