AppleSeed, Software S0622 | MITRE ATT&CK®

Archived: 2026-04-05 17:04:50 UTC

Enterprise T1134 Access Token Manipulation

AppleSeed can gain system level privilege by passing `SeDebugPrivilege` to the `AdjustTokenPrivilege` API.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

AppleSeed has the ability to communicate with C2 over HTTP.[1][2]

Enterprise T1560 Archive Collected Data

AppleSeed has compressed collected data before exfiltration.[2]

.001 Archive via Utility

AppleSeed can zip and encrypt data collected on a target system.[1]

Enterprise T1119 Automated Collection

AppleSeed has automatically collected data from USB drives, keystrokes, and screen images before exfiltration.[2]

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

AppleSeed has the ability to create the Registry key name `EstsoftAutoUpdate` at `HKCU\Software\Microsoft/Windows\CurrentVersion\RunOnce` to establish persistence.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

AppleSeed has the ability to execute its payload via PowerShell.[1]

.007 Command and Scripting Interpreter: JavaScript

AppleSeed has the ability to use JavaScript to execute PowerShell.[1]

Enterprise T1005 Data from Local System

AppleSeed can collect data on a compromised host.[1][2]

Enterprise T1025 Data from Removable Media

AppleSeed can find and collect data from removable media devices.[1][2]

Enterprise T1074 .001 Data Staged: Local Data Staging

AppleSeed can stage files in a central location prior to exfiltration.[1]

Enterprise T1030 Data Transfer Size Limits

AppleSeed has divided files if the size is 0x1000000 bytes or more.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

AppleSeed can decode its payload prior to execution.[1]

Enterprise T1041 Exfiltration Over C2 Channel

AppleSeed can exfiltrate files via the C2 channel.[1]

Enterprise T1567 Exfiltration Over Web Service

AppleSeed has exfiltrated files using web services.[2]

Enterprise T1008 Fallback Channels

AppleSeed can use a second channel for C2 when the primary channel is in upload mode.[1]

Enterprise T1083 File and Directory Discovery

AppleSeed has the ability to search for .txt, .ppt, .hwp, .pdf, and .doc files in specified directories.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

AppleSeed can delete files from a compromised host after they are exfiltrated.[1]

Enterprise T1056 .001 Input Capture: Keylogging

AppleSeed can use `GetKeyState` and `GetKeyboardState` to capture keystrokes on the victim's machine.[1][2]

Enterprise T1036 Masquerading

AppleSeed can disguise JavaScript files as PDFs.[1]

.005 Match Legitimate Resource Name or Location

AppleSeed has the ability to rename its payload to ESTCommon.dll to masquerade as a DLL belonging to ESTsecurity.[1]

Enterprise T1106 Native API

AppleSeed has the ability to use multiple dynamically resolved API calls.[1]

Enterprise T1027 Obfuscated Files or Information

AppleSeed has the ability to Base64 encode its payload and custom encrypt API calls.[1]

.002 Software Packing

AppleSeed has used UPX packers for its payload DLL.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

AppleSeed has been distributed to victims through malicious e-mail attachments.[1]

Enterprise T1057 Process Discovery

AppleSeed can enumerate the current process on a compromised host.[1]

Enterprise T1113 Screen Capture

AppleSeed can take screenshots on a compromised host by calling a series of APIs.[1][2]

Enterprise T1218 .010 System Binary Proxy Execution: Regsvr32

AppleSeed can call regsvr32.exe for execution.[1]

Enterprise T1082 System Information Discovery

AppleSeed can identify the OS version of a targeted system.[1]

Enterprise T1016 System Network Configuration Discovery

AppleSeed can identify the IP of a targeted system.[1]

Enterprise T1124 System Time Discovery

AppleSeed can pull a timestamp from the victim's machine.[1]

Enterprise T1204 .002 User Execution: Malicious File

AppleSeed can achieve execution through users running malicious file attachments distributed via email.[1]
