AppleJeus, Software S0584 | MITRE ATT&CK®

Archived: 2026-04-05 17:33:32 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

AppleJeus has presented the user with a UAC prompt to elevate privileges while installing.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

AppleJeus has sent data to its C2 server via `POST` requests.[1][2]

Enterprise T1059 .004 Command and Scripting Interpreter: Unix Shell

AppleJeus has used shell scripts to execute commands after installation and set persistence mechanisms.[1][2]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

AppleJeus can install itself as a service.[1]

.004 Create or Modify System Process: Launch Daemon

AppleJeus has placed a plist file within the `LaunchDaemons` folder and launched it manually.[1][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

AppleJeus has decoded files received from a C2.[1]

Enterprise T1546 .016 Event Triggered Execution: Installer Packages

During AppleJeus's installation process, it uses `postinstall` scripts to extract a hidden plist from the application's `/Resources` folder and execute the `plist` file as a Launch Daemon with elevated permissions.[2]

Enterprise T1041 Exfiltration Over C2 Channel

AppleJeus has exfiltrated collected host information to a C2 server.[1]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

AppleJeus has added a leading `.` to plist filenames, unlisting them from the Finder app and default Terminal directory listings.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

AppleJeus has deleted the MSI file after installation.[1]

Enterprise T1027 Obfuscated Files or Information

AppleJeus has XOR-encrypted collected system information prior to sending to a C2. AppleJeus has also used the open source ADVObfuscation library for its components.[1]

Enterprise T1566 .002 Phishing: Spearphishing Link

AppleJeus has been distributed via spearphishing link.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

AppleJeus has created a scheduled SYSTEM task that runs when a user logs in.[1]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

AppleJeus has used a valid digital signature from Sectigo to appear legitimate.[1]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

AppleJeus has been installed via MSI installer.[1]

Enterprise T1082 System Information Discovery

AppleJeus has collected the victim host information after infection.[1]

Enterprise T1569 .001 System Services: Launchctl

AppleJeus has loaded a plist file using the `launchctl` command.[1]

Enterprise T1204 .001 User Execution: Malicious Link

AppleJeus's spearphishing links required user interaction to navigate to the malicious website.[1]

.002 User Execution: Malicious File

AppleJeus has required user execution of a malicious MSI installer.[1]

Enterprise T1497 .003 Virtualization/Sandbox Evasion: Time Based Checks

AppleJeus has waited a specified time before downloading a second stage payload.[1]
