Bundlore, Software S0482 | MITRE ATT&CK®

Archived: 2026-04-05 13:36:04 UTC

Enterprise T1098 .004 Account Manipulation: SSH Authorized Keys

Bundlore creates a new key pair with `ssh-keygen` and drops the newly created user key in `authorized_keys` to enable remote login.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Bundlore uses HTTP requests for C2.[1]

Enterprise T1059 .002 Command and Scripting Interpreter: AppleScript

Bundlore can use AppleScript to inject malicious JavaScript into a browser.[1]

.004 Command and Scripting Interpreter: Unix Shell

Bundlore has leveraged /bin/sh and /bin/bash to execute commands on the victim machine.[1]

.006 Command and Scripting Interpreter: Python

Bundlore has used Python scripts to execute payloads.[1]

.007 Command and Scripting Interpreter: JavaScript

Bundlore can execute JavaScript by injecting it into the victim's browser.[1]

Enterprise T1543 .001 Create or Modify System Process: Launch Agent

Bundlore can persist via a LaunchAgent.[1]

.004 Create or Modify System Process: Launch Daemon

Bundlore can persist via a LaunchDaemon.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Bundlore has used `openssl` to decrypt AES encrypted payload data. Bundlore has also used base64 and RC4 with a hardcoded key to deobfuscate data.[1]

Enterprise T1189 Drive-by Compromise

Bundlore has been spread through malicious advertisements on websites.[1]

Enterprise T1048 Exfiltration Over Alternative Protocol

Bundlore uses the `curl -s -L -o` command to exfiltrate archived data to a URL.[2]

Enterprise T1222 .002 File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification

Bundlore changes the permissions of a payload using the command `chmod -R 755` .[2]

Enterprise T1564 Hide Artifacts

Bundlore uses the `mktemp` utility to make unique file and directory names for payloads, such as `TMP_DIR=`mktemp -d -t x` .[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Bundlore can change browser security settings to enable extensions to be installed. Bundlore uses the `pkill cfprefsd` command to prevent users from inspecting processes.[1][2]

Enterprise T1105 Ingress Tool Transfer

Bundlore can download and execute new versions of itself.[1]

Enterprise T1056 .002 Input Capture: GUI Input Capture

Bundlore prompts the user for their credentials.[1]

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

Bundlore has disguised a malicious .app file as a Flash Player update.[1]

Enterprise T1027 Obfuscated Files or Information

Bundlore has obfuscated data with base64, AES, RC4, and bz2.[1]

Enterprise T1057 Process Discovery

Bundlore has used the `ps` command to list processes.[1]

Enterprise T1518 Software Discovery

Bundlore has the ability to enumerate what browser is being used as well as version information for Safari.[1]

Enterprise T1176 .001 Software Extensions: Browser Extensions

Bundlore can install malicious browser extensions that are used to hijack user searches.[1]

Enterprise T1082 System Information Discovery

Bundlore will enumerate the macOS version to determine which follow-on behaviors to execute using `/usr/bin/sw_vers -productVersion` .[1][2]

Enterprise T1204 .002 User Execution: Malicious File

Bundlore has attempted to get users to execute a malicious .app file that looks like a Flash Player update.[1]
