INSOMNIA, Software S0463 | MITRE ATT&CK®

Archived: 2026-04-05 14:36:41 UTC

Mobile T1437 .001 Application Layer Protocol: Web Protocols

INSOMNIA communicates with the C2 server using HTTPS requests.[1]

Mobile T1634 .001 Credentials from Password Store: Keychain

INSOMNIA can extract the device's keychain.[2]

Mobile T1533 Data from Local System

INSOMNIA can collect application database files, including Gmail, Hangouts, device photos, and container directories of third-party apps.[2]

Mobile T1456 Drive-By Compromise

INSOMNIA has utilized malicious JavaScript and iframes to exploit WebKit running on vulnerable iOS 12 devices.[1]

Mobile T1404 Exploitation for Privilege Escalation

INSOMNIA exploits a WebKit vulnerability to achieve root access on the device.[1]

Mobile T1430 Location Tracking

INSOMNIA can track the device's location.[2]

Mobile T1509 Non-Standard Port

INSOMNIA has communicated with the C2 using HTTPS requests over ports 43111, 43223, and 43773.[1]

Mobile T1406 Obfuscated Files or Information

INSOMNIA obfuscates various pieces of information within the application.[1]

Mobile T1631 .001 Process Injection: Ptrace System Calls

INSOMNIA grants itself permissions by injecting its hash into the kernel's trust cache.[2]

Mobile T1636 .002 Protected User Data: Call Log

INSOMNIA can retrieve the call history.[2]

.003 Protected User Data: Contact List

INSOMNIA can collect the device's contact list.[2]

.004 Protected User Data: SMS Messages

INSOMNIA can retrieve SMS messages and iMessages.[2]

Mobile T1418 Software Discovery

INSOMNIA can obtain a list of installed non-Apple applications.[2]

Mobile T1426 System Information Discovery

INSOMNIA can collect the device's name, serial number, iOS version, total disk space, and free disk space.[2]

Mobile T1422 System Network Configuration Discovery

INSOMNIA can collect the device's phone number, ICCID, IMEI, and the currently active network interface (Wi-Fi or cellular).[2]

.001 Internet Connection Discovery

INSOMNIA can collect the device's phone number, ICCID, IMEI, and the currently active network interface (Wi-Fi or cellular).[2]

.002 Wi-Fi Discovery

INSOMNIA can collect the device's phone number, ICCID, IMEI, and the currently active network interface (Wi-Fi or cellular).[2]
