SharkBot, Software S1055 | MITRE ATT&CK®

Archived: 2026-04-05 14:38:59 UTC

Mobile T1517 Access Notifications

SharkBot can intercept notifications to send to the C2 server and take advantage of the Direct Reply feature.[1]

Mobile T1437 .001 Application Layer Protocol: Web Protocols

SharkBot can use HTTP to send C2 messages to infected devices.[1]

Mobile T1661 Application Versioning

SharkBot initially poses as a benign application, then malware is downloaded and executed after an application update.[1]

Mobile T1407 Download New Code at Runtime

SharkBot can use the Android "Direct Reply" feature to spread the malware to other devices. It can also download the full version of the malware after initial device compromise.[1]

Mobile T1637 .001 Dynamic Resolution: Domain Generation Algorithms

SharkBot contains domain generation algorithms to use as backups in case the hardcoded C2 domains are unavailable.[1]

Mobile T1521 .001 Encrypted Channel: Symmetric Cryptography

SharkBot can use RC4 to encrypt C2 payloads.[1]

.002 Encrypted Channel: Asymmetric Cryptography

SharkBot has used RSA to encrypt the symmetric encryption key used for C2 messages.[1]

Mobile T1646 Exfiltration Over C2 Channel

SharkBot can exfiltrate captured user credentials and event logs back to the C2 server. [1]

Mobile T1630 .001 Indicator Removal on Host: Uninstall Malicious Application

SharkBot has C2 commands that can uninstall the app from the infected device.[1]

Mobile T1544 Ingress Tool Transfer

SharkBot can download attacker-specified files.[1]

Mobile T1417 .001 Input Capture: Keylogging

SharkBot can use accessibility event logging to steal data in text fields.[1]

.002 Input Capture: GUI Input Capture

SharkBot can use a WebView with a fake log in site to capture banking credentials.[1]

Mobile T1516 Input Injection

SharkBot can use input injection via Accessibility Services to simulate user touch inputs, prevent applications from opening, change device settings, and bypass MFA protections.[1]

Mobile T1406 Obfuscated Files or Information

SharkBot can use a Domain Generation Algorithm to decode the C2 server location.[1]

Mobile T1644 Out of Band Data

SharkBot can use the "Direct Reply" feature of Android to automatically reply to notifications with a message provided by C2.[1]

Mobile T1424 Process Discovery

SharkBot can use Accessibility Services to detect which process is in the foreground.[1]

Mobile T1636 .004 Protected User Data: SMS Messages

SharkBot can intercept SMS messages.[1]

Mobile T1582 SMS Control

SharkBot can hide and send SMS messages. SharkBot can also change which application is the device’s default SMS handler.[1]
