RatMilad, Software S1241 | MITRE ATT&CK®

Archived: 2026-04-05 14:07:25 UTC

Mobile T1437 .001 Application Layer Protocol: Web Protocols

RatMilad has used HTTP POST requests for communicating with its C2 server.[1]

Mobile T1429 Audio Capture

RatMilad has captured audio from the device.[1]

Mobile T1414 Clipboard Data

RatMilad has collected clipboard content.[1]

Mobile T1662 Data Destruction

RatMilad has deleted files on the device.[1]

Mobile T1533 Data from Local System

RatMilad has listed files and pictures on the device starting from `/mnt/sdcard/`.[1]

Mobile T1407 Download New Code at Runtime

RatMilad has used a fake application to request permissions and to download itself.[1]

Mobile T1646 Exfiltration Over C2 Channel

RatMilad has exfiltrated collected data to the C2.[1]

Mobile T1420 File and Directory Discovery

RatMilad has listed files and pictures on the device starting from `/mnt/sdcard/`.[1]

Mobile T1430 Location Tracking

RatMilad has collected the device's last known location.[1]

Mobile T1660 Phishing

RatMilad has concealed itself behind variants of a phone number spoofing application, which was distributed through links on social media and communication platforms.[1]

Mobile T1636 .002 Protected User Data: Call Log

RatMilad has accessed the device's call log.[1]

.003 Protected User Data: Contact List

RatMilad has accessed the device's contact list.[1]

.004 Protected User Data: SMS Messages

RatMilad has accessed the device's SMS messages, including messages that were in the inbox, sent, draft, outbox, failed, and queued.[1]

.005 Protected User Data: Accounts

RatMilad has collected account names and their types from the compromised device.[1]

Mobile T1418 Software Discovery

RatMilad has collected package names.[1]

Mobile T1426 System Information Discovery

RatMilad has collected device information such as model, brand, buildId, Android version and manufacturer.[1]

Mobile T1422 System Network Configuration Discovery

RatMilad has collected device information such as MAC address, IMEI and phone number.[1]

Mobile T1512 Video Capture

RatMilad has taken photos and videos using the device's camera.[1]
