System Network Configuration Discovery, Technique T1422 - Mobile

Archived: 2026-04-05 17:31:23 UTC

S1061 AbstractEmu

AbstractEmu can collect device IP address and SIM information.[3]

S1214 Android/SpyAgent

Android/SpyAgent has collected device network information, such as the IMEI and the phone number.[4]

S0310 ANDROIDOS_ANSERVER.A

ANDROIDOS_ANSERVER.A gathers the device IMEI and IMSI.[5]

S0292 AndroRAT

AndroRAT collects the device's location through GPS or through network settings.[6]

G1028 APT-C-23

APT-C-23 can collect the victim's phone number, device information, IMSI, etc.[7]

S0540 Asacub

Asacub can collect various pieces of device network configuration information, such as mobile network operator. [8]

S1215 Binary Validator

Binary Validator has collected the device's phone number and IMEI.[9]

S1079 BOULDSPY

BOULDSPY can collect network information, such as IP address, SIM card information, and Wi-Fi information. [10]

S0432 Bread

Bread collects the device's IMEI, carrier, mobile country code, and mobile network code.[11]

S0529 CarbonSteal

CarbonSteal has collected device network information, including 16-bit GSM Cell Identity, 16-bit Location Area Code, Mobile Country Code (MCC), and Mobile Network Code (MNC). CarbonSteal has also called `netcfg` to get stats.[12]

S0425 Corona Updates

Corona Updates can collect device network configuration information, such as Wi-Fi SSID and IMSI.[13]

S0315 DualToy

DualToy collects the connected iOS device's information including IMEI, IMSI, ICCID, serial number and phone number.[14]

S0478 EventBot

EventBot can gather device network information.[15]

S0522 Exobot

Exobot can obtain the device's IMEI, phone number, and IP address.[16]

S0405 Exodus

Exodus One queries the device for its IMEI code and the phone number in order to validate the target of a new infection.[17]

S0509 FakeSpy

FakeSpy can collect device networking information, including phone number, IMEI, and IMSI.[18]

S1093 FlyTrap

FlyTrap can collect IP address and network configuration information.[19]

S0577 FrozenCell

FrozenCell has collected phone metadata such as cell location, mobile country code (MCC), and mobile network code (MNC).[20]

S1231 GodFather

GodFather has accessed the device's current cellular network information, including the phone number and the serial number.[21]

S0535 Golden Cup

Golden Cup can collect the device's phone number and IMSI.[22]

S0536 GPlayed

GPlayed can collect the device’s IMEI, phone number, and country.[23]

S0406 Gustuff

Gustuff gathers the device IMEI to send to the command and control server.[24]

S1077 Hornbill

Hornbill can collect a device's phone number and IMEI, and can check to see if WiFi is enabled.[25]

S0463 INSOMNIA

INSOMNIA can collect the device’s phone number, ICCID, IMEI, and the currently active network interface (Wi-Fi or cellular).[26]

S1185 LightSpy

LightSpy has collected device information such as IMEI, phone number, MAC address and IP address.[27]

S0407 Monokle

Monokle checks if the device is connected via Wi-Fi or mobile data.[28]

C0054 Operation Triangulation

During Operation Triangulation, the threat actors use the heartbeat beacons from the implant to obtain device information, such as the IMEI, MEID, and the serial number.[29]

S0316 Pegasus for Android

Pegasus for Android checks if the device is on Wi-Fi, a cellular network, and is roaming.[30]

S0291 PJApps

PJApps has the capability to collect and leak the victim's phone number, mobile device unique identifier (IMEI).[31]

S1241 RatMilad

RatMilad has collected device information such as MAC address, IMEI and phone number.[32]

S0326 RedDrop

RedDrop collects and exfiltrates information including IMEI, IMSI, MNC, MCC, nearby Wi-Fi networks, and other device and SIM-related info.[33]

S0403 Riltok

Riltok can query the device's IMEI.[34]

S0411 Rotexy

Rotexy collects the device's IMEI and sends it to the command and control server.[35]

S0313 RuMMS

RuMMS gathers the device phone number and IMEI and transmits them to a command and control server.[36]

S0324 SpyDealer

SpyDealer harvests the device phone number, IMEI, and IMSI.[37]

S0328 Stealth Mango

Stealth Mango collects and uploads information about changes in SIM card or phone numbers on the device.[38]

S1082 Sunbird

Sunbird can exfiltrate phone number and IMEI.[25]

S0329 Tangelo

Tangelo contains functionality to gather cellular IDs.[38]

S0545 TERRACOTTA

TERRACOTTA has collected the device’s phone number and can check if the active network connection is metered.[39]

S1056 TianySpy

TianySpy can check to see if Wi-Fi is enabled.[40]

S1216 TriangleDB

TriangleDB has collected and sent information on the device’s IMEI, MEID, serial number and other device information.[29]

S0427 TrickMo

TrickMo can collect device network configuration information such as IMSI, IMEI, and Wi-Fi connection state.[41]

S0506 ViperRAT

ViperRAT can collect network configuration data from the device, including phone number, SIM operator, and network operator.[42]

S0489 WolfRAT

WolfRAT sends the device's IMEI with each exfiltration request.[43]

S0318 XLoader for Android

XLoader for Android collects the device's IMSI and ICCID.[44]

S0490 XLoader for iOS

XLoader for iOS can obtain the device's IMEM, ICCID, and MEID.[44]

S0311 YiSpecter

YiSpecter has collected compromised device MAC addresses.[45]
