



SUMMARY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

☒ Display grouped sandbox reports

☒ VirusTotal Droidy 0 0 3 0 0 1

☒ Zenbox 0 6 0 0 0 7

Activity Summary

Download Artifacts ▾

Full Reports ▾

Help ▾

Detections

NOT FOUND

Mitre Signatures

14 INFO

IDS Rules

3 LOW

Sigma Rules

NOT FOUND

Dropped Files











NOT FOUND

Network comms

1 DNS 6 IP 1 JA3

Behavior Tags ⓘ

checks-gps reflection telephony

MITRE ATT&CK Tactics and Techniques— **Command and Control** TA0011 Application Layer Protocol T1071
Uses HTTPS Encrypted Channel T1573
Uses HTTPS— **Credential Access** TA0031 Capture SMS Messages T1412
Queries SMS data— **Discovery** TA0032 System Network Connections Discovery T1421
Checks an internet connection is available System Information Discovery T1426
Queries the unique device ID (IMEI, MEID or ESN) Location Tracking T1430
Queries the phones location (GPS)
Has permission to query the current location— **Impact** TA0034 Carrier Billing Fraud T1448
Has permission to send SMS in the background— **Collection** TA0035 Capture SMS Messages T1412
Queries SMS data Location Tracking T1430
Queries the phones location (GPS)
Has permission to query the current location Network Information Discovery T1507
Checks an internet connection is available
Scans for WIFI networks— **Network Effects** TA0038



Exploit SS7 to Redirect Phone Calls/SMS T1449

Has permission to send SMS in the background

Crowdsourced IDS rules ⓘ

- ⚠ Matches rule (eth) truncated ethernet header
- ⚠ Matches rule SURICATA STREAM Packet with invalid ack
- ⚠ Matches rule SURICATA STREAM SHUTDOWN RST invalid ack

Network Communication ⓘ**DNS Resolutions**

— growth-pa.googleapis.com

142.251.143.138

142.251.143.202

142.251.143.106

142.251.143.170

IP Traffic

- 142.251.143.131:443 (TCP)
- 142.251.143.132:443 (UDP)
- 142.251.143.142:443 (TCP)
- 142.251.143.164:443 (TCP)
- 142.251.143.174:443 (TCP)
- 66.102.1.188:5228 (TCP)

JA3 Digests

cd08e31494f9531f560d64c695473da9

Memory Pattern Domains

- schemas.android.com
- www.apache.org

Memory Pattern Urls

- http://schemas.android.com/apk/res/android
- http://www.apache.org/licenses/LICENSE-2.0

Behavior Similarity Hashes ⓘ

VirusTotal Droidy c69920486653226127d698c3292d537d

Zenbox

2822a68c1eecfedf41af339665430439

Process and service actions ⓘ**Services Opened**com.google.android.gms.games.service.GamesIntentService
(com.google.android.gms)com.google.android.gms.people.service.bg.PeopleBackgroundTasks
(com.google.android.gms)com.nuvsoft.android.scanner.ScannerService
(com.nuvsoft.android.scanner)**Activities Started**

com.nuvsoft.android.scanner.Scanner (com.nuvsoft.android.scanner)

Modules loaded ⓘ**Invoked Methods**

android.database.sqlite.SQLiteConnectionPool\$AcquiredConnectionSta

Dataset actions ⓘ**System Property Lookups**

db.log.slow_query_threshold



debug.force_rtl



debug.layout



debug.second-display.pkg



debug.sqlite.journalmode



debug.sqlite.journalsize-limit



debug.sqlite.pagesize



debug.sqlite.syncmode



debug.sqlite.wal.autocheckpoint



persist.sys.ui.hw

