Crowdsourced IDS rules

HIGH 2 MEDIUM 0 LOW 3 INFO 0

- Matches rule INDICATOR-COMPROMISE Suspicious .cn dns query
- Matches rule INDICATOR-COMPROMISE Suspicious .cc dns query
- Matches rule ET DNS Query to a *.top domain - Likely Hostile
- Matches rule ET DNS Query for .cc TLD
- Matches rule INDICATOR-COMPROMISE Suspicious .top dns query

Popular threat label trojan.smsreg/andr **Threat categories** trojan adware **Family labels** smsreg andr roo

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	PUP/Android.SMSPay.670290
Alibaba	AdWare:Android/SMSreg.f422f222
Antiy-AVL	Trojan/Generic.ASMalwAD.6F0
Avast	Android:SMSreg-DDG [PUP]
Avast-Mobile	APK:RepMalware [Trj]
AVG	Android:SMSreg-DDG [PUP]
Avira (no cloud)	PUA/ANDR.SMSReg.YBR.Gen
BitDefenderFalx	Android.Trojan.Rootnik.MZ
Cynet	Malicious (score: 99)
Cyren	AndroidOS/Agent.EB.gen!Eldorado
DrWeb	Android.Triada.236.origin
ESET-NOD32	Multiple Detections
F-Secure	PotentialRisk.PUA/ANDR.SMSReg.YBR.Gen
Fortinet	Android/Agent.EE!tr
Google	Detected
Ikarus	Trojan.AndroidOS.SmsSpy
Jiangmin	RiskTool.AndroidOS.dges
K7GW	Trojan (00536a311)

Kaspersky	HEUR:Trojan-Downloader.AndroidOS.Agent.gz
Lionic	Trojan.AndroidOS.Agent.C!c
MAX	Malware (ai Score=96)
MaxSecure	Virus.AdWare.AndroidOS.Agent.cf
McAfee	Artemis!D65DCF563268
McAfee-GW-Edition	Artemis!PUP
Microsoft	Program:AndroidOS/Multiverze
NANO-Antivirus	Trojan.Android.Agent.dyqpps
QuickHeal	Android.Agent.GEN3293
Sangfor Engine Zero	PUP.Android-Script.Save.27ddfe93
Sophos	Andr/Rootnik-AI
Symantec	Trojan.Gen.MBT
Symantec Mobile Insight	Trojan:Malapp
Tencent	A.payment.MoneyThief
Trustlook	Android.PUA.Trojan
VirIT	Android.Adw.G2P.JYK
Xcitium	ApplicUnwnt@#3apll3ak1qk7y
Acronis (Static ML)	Undetected
Ad-Aware	Undetected
ALYac	Undetected
Arcabit	Undetected
Baidu	Undetected
BitDefender	Undetected
BitDefenderTheta	Undetected
Bkav Pro	Undetected
ClamAV	Undetected
CMC	Undetected
Elastic	Undetected
Emsisoft	Undetected
eScan	Undetected
GData	Undetected
Gridinsoft (no cloud)	Undetected
K7AntiVirus	Undetected
Kingsoft	Undetected
Malwarebytes	Undetected
Panda	Undetected
Rising	Undetected
SUPERAntiSpyware	Undetected
TACHYON	Undetected

Trellix (FireEye)	Undetected
TrendMicro	Undetected
TrendMicro-HouseCall	Undetected
VBA32	Undetected
VIPRE	Undetected
ViRobot	Undetected
Yandex	Undetected
Zillya	Undetected
Zoner	Undetected
CrowdStrike Falcon	Unable to process file type
Cybereason	Unable to process file type
Cylance	Unable to process file type
DeepInstinct	Unable to process file type
Palo Alto Networks	Unable to process file type
SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type
TEHTRIS	Unable to process file type
Trapmine	Unable to process file type
Webroot	Unable to process file type