

جاسوس افزار Trojan/Android.Sms

احتراما به پیوست اطلاعات بد افزار Trojan/Android.Sms ارسال میگردد .

این بد افزار توسط آنتی ویروس پادویش شناسایی نمیشود و پس از اجرا در محیط ماشین مجازی توسط آنتی ویروس پادویش با آخرین بروز رسانی در تاریخ ۱۴۰۳/۰۲/۰۱ شناسایی نگردید .

در زیر اطلاعات این بد افزار که توسط سایت معتبر ویروس توتال بررسی گردیده است ارسال میگردد .

<https://www.virustotal.com/gui/file/e11b47d5ff10d354a6fdd5189e6dcfcb5b0cc6f63c896eead34c8b57ae4bf993?nocache=1>

لینک اسکن بد افزار در وب سایت ویروس توتال



اسکن بد افزار در محیط ماشین مجازی توسط آنتی ویروس پادویش و عدم شناسایی این بد افزار توسط آنتی ویروس پادویش

VirusTotal has updated its Privacy Notice and its Terms of Use effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

Accept terms of use

17
/ 63

Community Score

17/63 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

e11b47d5f10d354a6dd5189e6dcfb5b0cc6f3c896eed34c8b57ae4bf993

app.apk

Size2.01 MB

Last Modification Datea moment ago

APK

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY

Popular threat label
trojan.basdoor/umsagent

Threat categories
trojan

Family labels
basdoor umsagent

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan.Android.SmsSpy.1188936	Avast-Mobile	Android:Evo-gen [Tj]
Avira (no cloud)	ANDROID!SmsAgent.YLW.Gen	BitDefenderFalk	Android.Trojan.InfoStealer.ABG
Cynet	Malicious (score: 99)	DrWeb	Android.Spy.Lydia.9
ESET-NOD32	A Variant Of Android/Spy.Agent.BUB	Fortinet	Android.Agent.LBUB!tr
Google	Detected	Ikarus	Trojan.Spy.AndroidOS.Agent
K7GW	Trojan (005a76541)	Kaspersky	HEUR.Backdoor.AndroidOS.Basdoor.c
Microsoft	Trojan.AndroidOS/SpyAgent.LV	Sophos	Andri/TalkApp-EX
Trustlook	Android.Malware.General (score:9)	WithSecure	Malware.ANDROID!SmsAgent.YLW.Gen
ZoneAlarm by Check Point	HEUR.Backdoor.AndroidOS.Basdoor.c	Acronis (Static ML)	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	ClamAV	Undetected
CMC	Undetected	Emsisoft	Undetected
eScan	Undetected	GData	Undetected
Gridinsoft (no cloud)	Undetected	Jiangmin	Undetected
KTAntiVirus	Undetected	Kingsoft	Undetected
Malwarebytes	Undetected	MAX	Undetected
MaxSecure	Undetected	McAfee	Undetected
NANO-Antivirus	Undetected	Panda	Undetected
QuickHeal	Undetected	Rising	Undetected
Sangfor Engine Zero	Undetected	Skyhigh (SWG)	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
Symantec Mobile Insight	Undetected	TACHYON	Undetected
Tencent	Undetected	Trellix (FireEye)	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
Varist	Undetected	VBA32	Undetected
VIPRE	Undetected	VirtT	Undetected
ViRobot	Undetected	Xcitium	Undetected
Vandex	Undetected	Zillya	Undetected
Zoner	Undetected	AllCloud	Unable to process file type
CrowdStrike Falcon	Unable to process file type	Cylance	Unable to process file type
DeepInstinct	Unable to process file type	Elastic	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
Bkav Pro	—		

VirusTotal

Contact Us
Get Support
How It Works
ToS | Privacy Notice
Blog | Releases

Community

Join Community
Vote and Comment
Contributors
Top Users
Community Buzz

Tools

API Scripts
YARA
Desktop Apps
Browser Extensions
Mobile App

Premium Services

Get a demo
Intelligence
Hunting
Graph
API v3 | v2

Documentation

Searching
Reports
API v3 | v2
Use Cases

شناسایی بد افزار توسط ۱۷ آنتی ویروس معتبر

۲

Behavior Tags

Crowdsourced IDS rules

Matches rule (eth) truncated ethernet header at Snort registered user ruleset

misc-activity

Matches rule SURICATA STREAM Packet with invalid ack at Suricata

Generic Protocol Command Decode

Matches rule SURICATA STREAM SHUTDOWN RST invalid ack at Suricata

Generic Protocol Command Decode

Unique rule identifier:

This rule belongs to a private collection.

Network Communication

IP Traffic

- TCP 142.251.173.188:5228

Behavior Similarity Hashes

VirusTotal Droidy

[0185dfe1384f902861a9dd58ad202454](https://www.virustotal.com/gui/file/0185dfe1384f902861a9dd58ad202454)

File system actions

Files Opened

- /data/data/com.temptation.lydia/files/PersistedInstallation-673517689tmp
- /data/data/com.temptation.lydia/files/PersistedInstallation.W0RFRkFVTFRd+MTo0NTE3NDA4MjY1NzphbmRyb2lkOmFIOTEyODdkZGQ4Njk1NTgxZjJlMjA.json
- /data/data/com.temptation.lydia/files/generatefid.lock
- /data/data/com.temptation.lydia/shared_prefs/FirebaseHeartBeatW0RFRkFVTFRd+MTo0NTE3NDA4MjY1NzphbmRyb2lkOmFIOTEyODdkZGQ4Njk1NTgxZjJlMjA.xml
- /data/misc/keychain/pins

Files Written

- /data/data/com.temptation.lydia/files/PersistedInstallation-673517689tmp
- /data/data/com.temptation.lydia/no_backup/com.google.android.gms.appid-no-backup

Files Deleted

- /data/data/com.temptation.lydia/files/PersistedInstallation-673517689tmp

- /data/data/com.temptation.lydia/shared_prefs/FirebaseHeartBeatW0RFRkFVTFRd+MT00NTE3NDA4MjY1NzphbmRyb2lkOmFIOTEyODdkZGQ4Njk1NTgxZjJlMjA.xml.bak

Files Copied

/data/data/com.temptation.lydia/files/PersistedInstallation-673517689tmp

/data/data/com.temptation.lydia/files/PersistedInstallation.W0RFRkFVTFRd+MT00NTE3NDA4MjY1NzphbmRyb2lkOmFIOTEyODdkZGQ4Njk1NTgxZjJlMjA.json

Process and service actions

Permissions Checked

com.google.android.c2dm.permission.SEND

com.google.android.gms

Shell Commands

- su

Services Opened

- com.google.android.partnersetup.RlzPingIntentService (com.google.android.partnersetup)

Activities Started

- com.temptation.lydia.aapp (com.temptation.lydia)

Modules loaded

Invoked Methods

- android.net.NetworkInfo\$State.values
- com.temptation.lydia.main._globals
- com.temptation.lydia.main.initializeProcessGlobals
- com.temptation.lydia.starter._service_create
- com.temptation.lydia.starter._service_start

Highlighted actions

Calls Highlighted

- android.telephony.TelephonyManager.getNetworkOperatorName
- android.util.Base64.encode

Encoding Algorithms Observed

- base64

Decoded Text

- 1:45174082657:android:ae91287ddd8695581f2e20

- [DEFAULT]

Dataset actions

System Property Lookups

- config.disable_media
- debug.force_rtl
- debug.layout
- debug.second-display.pkg
- gsm.operator.alpha
- persist.sys.timezone
- viewroot.profile_rendering

Shared Preferences Sets

fire-count

1

last-used-date

2024-04-17

سلام معیشتی 3 میلیونی نگرفتی بگیر:
meshati.com

سامانه معیشتی دولت

meshati.com

نمونه پیامک ارسالی پس از هک شدن گوشی کاربر به لیست مخاطبین

پس از باز کردن لینک ارسالی از طرف مخاطب قربانی به لینک زیر هدایت میشود .

<https://meshati.com/dashbord/>



کمک معیشتی دولت

نام و نام خانوادگی

نام کامل خود را وارد کنید

شماره تلفن

۰۹۱۲۰۰۰۰۰۰۰۰

کد ملی

کد ملی خود را وارد کنید

وضعیت تاهل: ☐ خیر ☐ بله

پیگیری

صفحه باز شده که از کاربر اطلاعات شخصی را دریافت نموده تا به صفحه بعد انتقال یابد .

نتیجه کمک معیشتی دولت به شرح زیر می باشد

وضعیت
دریافت نشده

مبلغ کمک معیشتی شما در سال جاری
۳,۵۶۰,۰۰۰ تومان

دریافت کمک معیشتی
امکان پذیر

مراحل دریافت

- نصب اپلیکیشن سامانه کمک معیشتی
- ورود با شماره تلفن همراه
- تکمیل فرم و دریافت

مراجعه کننده عزیز برای دریافت کمک معیشتی خود شما باید اپلیکیشن سامانه کمک معیشتی را از طریق دکمه زیر دانلود و اقدام به نصب آن کنید سپس بعد از نصب میتوانید از طریق اپلیکیشن اقدام به دریافت کمک معیشتی خود کنید

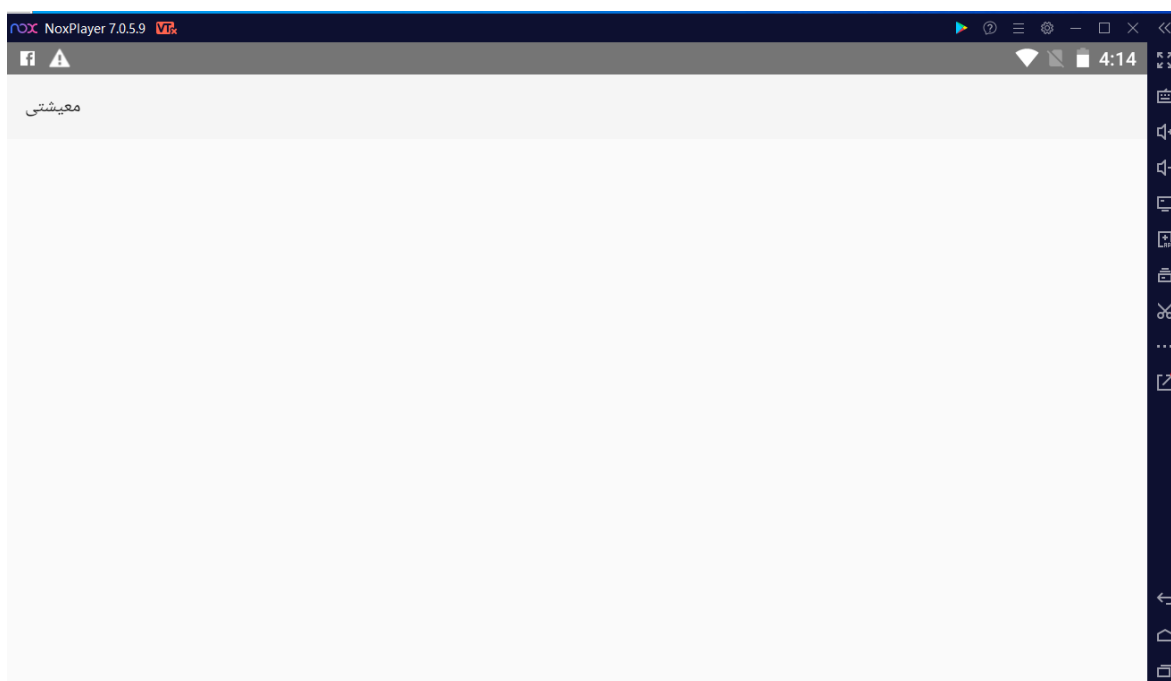
برای نصب دکمه زیر را بفشارید

دانلود اپلیکیشن سامانه کمک معیشتی

پس از نمایش اعتبار سنجی کد ملی که بصورت جعلی میباشد . کاربر به صفحه دانلود نرم افزار اندرویدی وارد میشود .



پس از نصب نرم افزار بر روی گوشی قربانی آیکن برنامه به صفحه اصلی گوشی اضافه شده و اقدام به ارسال پیامک به لیست مخاطبین نموده .



اجرای نرم افزار بر روی **ماشین مجازی** و اجرای نرم افزار و بسته شدن خودکار برنامه

نرم افزار در پس زمینه در حال ارتباط با سرور خود بوده (**TCP 142.251.173.188:5228**) و اقدام به سرقت اطلاعات کاربر مینماید . و کاربر به خیال اینکه گوشی یا نرم افزار به مشکل برخوردده است اقدام به اجرای چندین باره آن می نماید .