جاسوس افزار Trojan/Android.Sms

احتراما به پیوست اطلاعات بد افزارTrojan/Android.Sms ارسال میگردد .

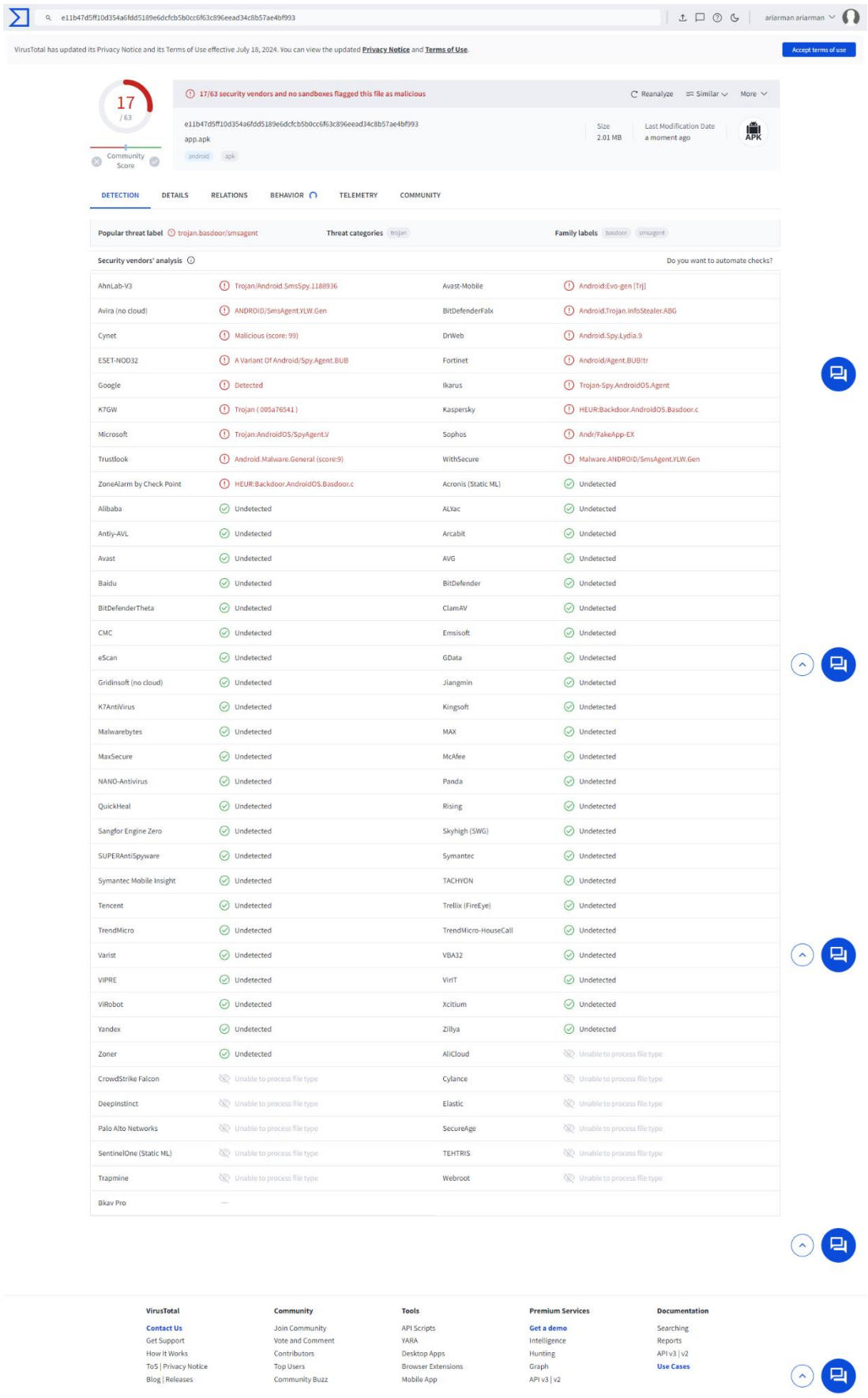
این بد افزار توسط آنتی ویروس پادویش شناسایی نمیشود و پس از اجرا در محیط ماشین مجازی توسط آنتی ویروس پادویش با آخرین بروز رسانی در تاریخ ۱۴۰۳/۰۲/۰۱ شناسایی نگردید .

در زیر اطلاعات این بد افزار که توسط سایت معتبر ویروس توتال برسی 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 بدافزار توسط آنتی ویروس پادویش



شناسایی بد افزار توسط ۱۷ آنتی ویروس معتبر

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

File system actions

Files Opened

- /data/data/com.temptation.lydia/files/PersistedInstallation-673517689tmp
- /data/data/com.temptation.lydia/files/PersistedInstallation.W0RFRkFVTFRd+MTo0NTE3NDA4MjY1NzphbmRyb2lkOmFlOTEyODdkZGQ4Njk1NTgxZjJlMjA.json
- /data/data/com.temptation.lydia/files/generatefid.lock
- /data/data/com.temptation.lydia/shared_prefs/FirebaseHeartBeatW0RFRkFVTFRd+MTo0NTE3NDA4MjY1NzphbmRyb2lkOmFlOTEyODdkZGQ4Njk1NTgxZjJlMjA.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+MTo0NTE3NDA4MjY1NzphbmRyb2lkOmFlOTEyODdkZGQ4Njk1NTgxZjJlMjA.xml.bak

Files Copied

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

/data/data/com.temptation.lydia/files/PersistedInstallation.W0RFRkFVTFRd+MTo0NTE3NDA4MjY1NzphbmRyb2lkOmFlOTEyODdkZGQ4Njk1NTgxZjJlMjA.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

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

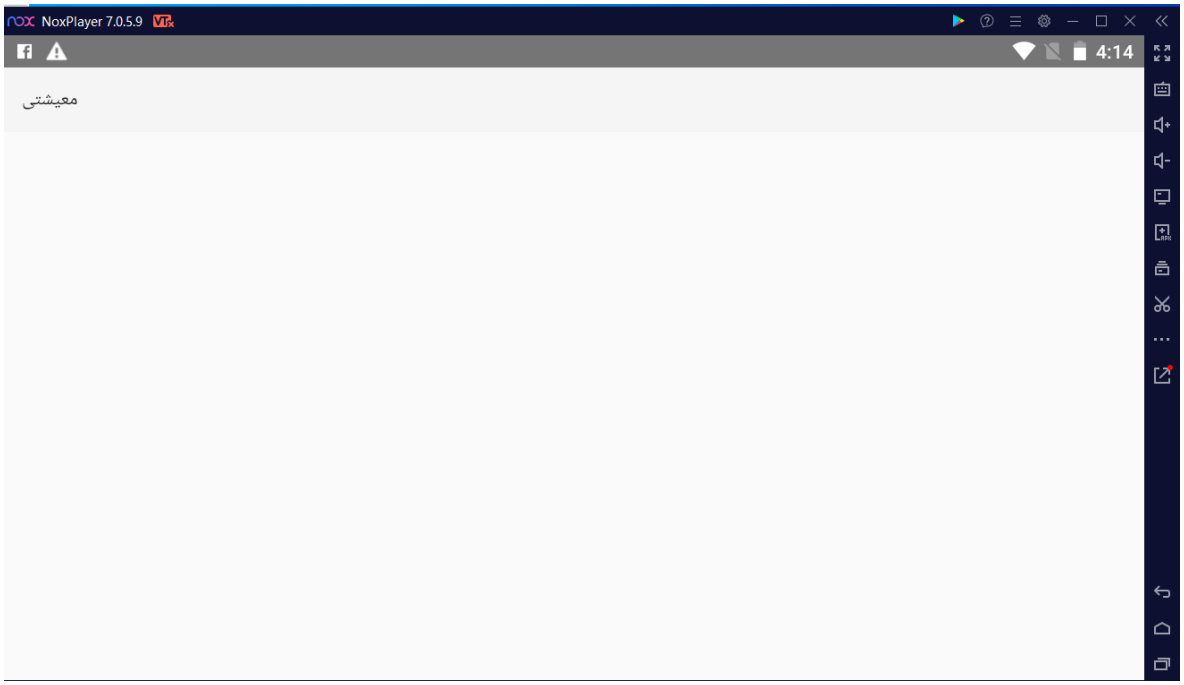
پس از باز کردن لینک ارسالی از طرف مخاطب قربانی به لینک زیر هدایت میشود .

https://meshati.com/dashbord/

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

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 برخورده است اقدام به اجرای چندین باره آن می نماید .