



Csomagja érkezett Mylord!



Csizmazia-Darab István [Rambo]
IT biztonsági szakértő, ESET/Sicontact

csizmazia-darab.istvan@sicontact.hu

Linkek, letöltések, telepítések, engedélyek - Hova vezet mindez?

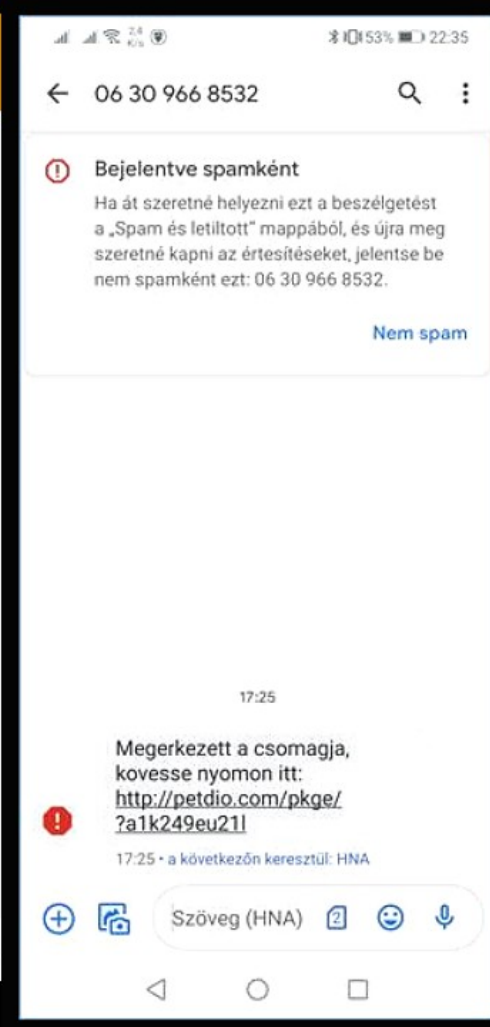
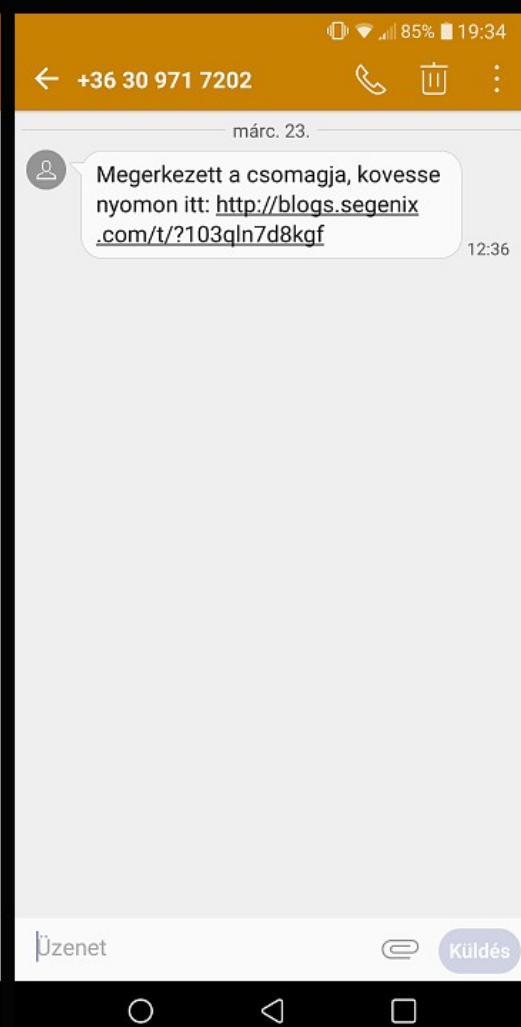
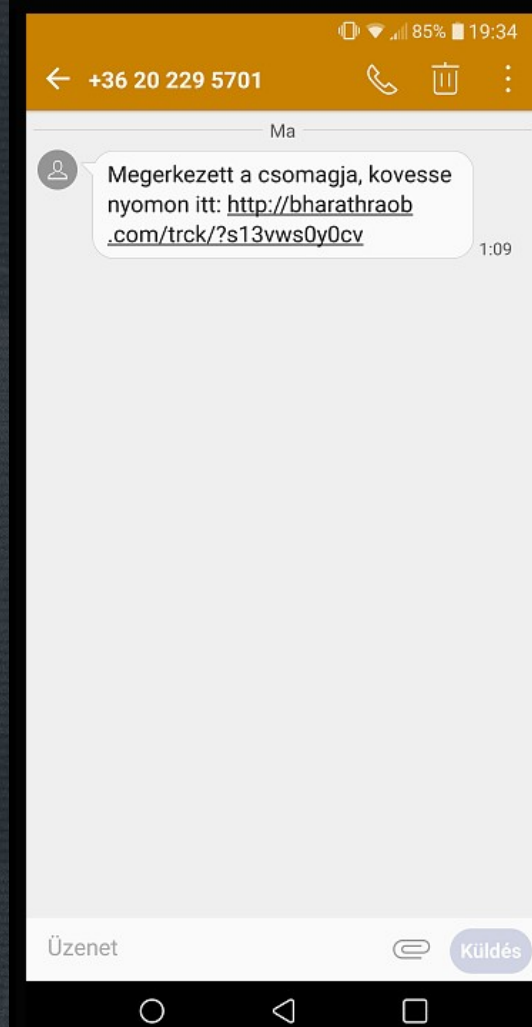


Egy nem mindennapi SMS csalás tanulságai

Az ég kék, a fű zöld, a vírusok, kártevők támadják a sebezhetőségeket.
Népi megfigyelések, amiket az ember elfogad természeti törvénynek



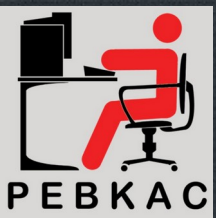
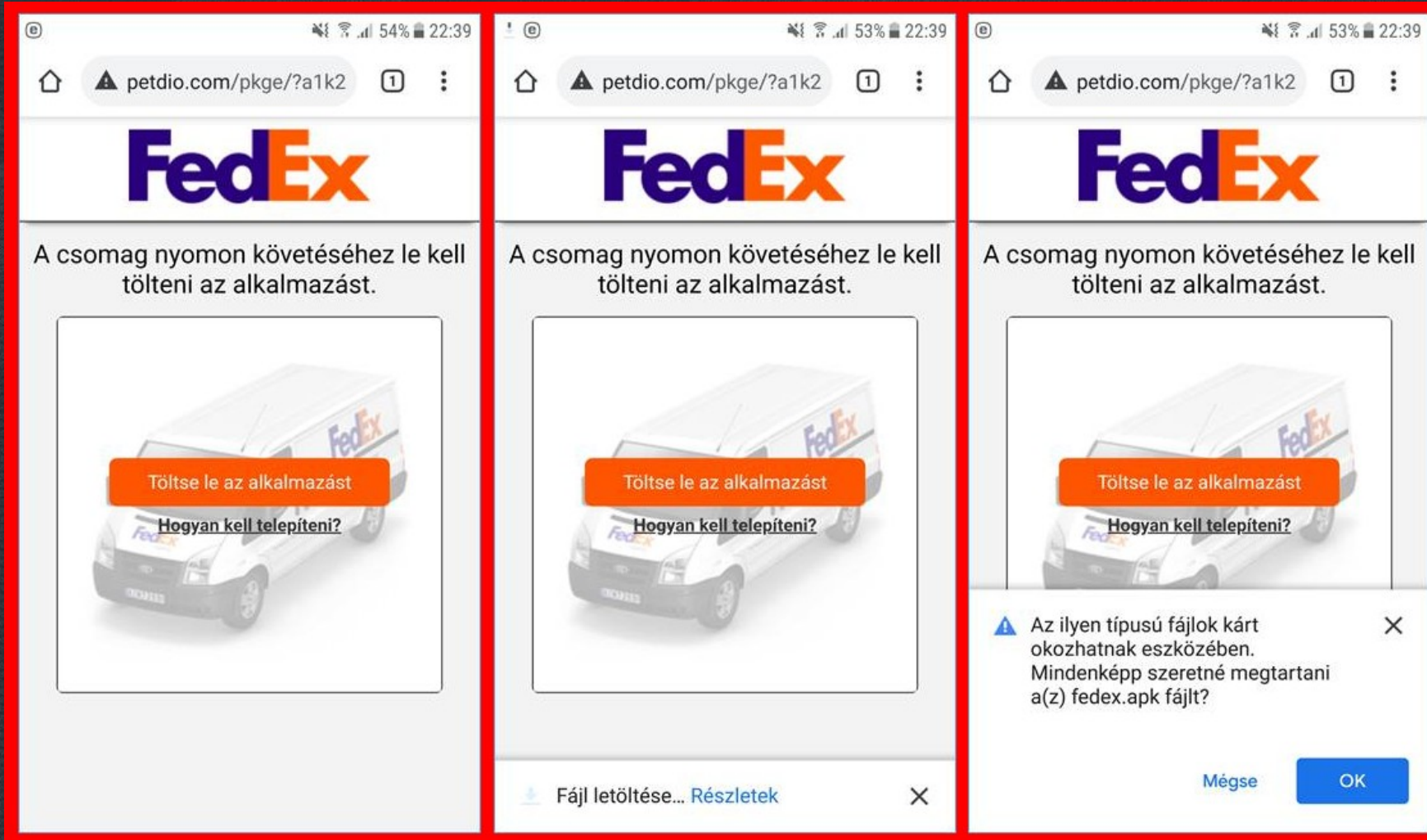
Covid miatt sokan vártunk csomagot, erre jött ez...



2021. március nemzetközi futárcég FedEx.apk app

- több százezer SMS üzenet
- magyar telefonszámokról
- csak helyi, lokális számról kapunk SMS-t
- több különböző domain, feltört Wordpress oldalak linkje (Android user agent)

- profi kártevő, nemzetközi bűnözők, titkosított C&C szerver



Problem Exists Between Keyboard And Chair

FluBot előzmények:

- 2020. november Spanyolország
- 70 ezer fertőzött telefon,
11 millió telefonszám
- 2021. március, 4 letartóztatás





A magyar kampánnyal egyidőben:

- Lengyelország



- Németország



- Olaszország



FluBot utóélet:

- Most 2021. júniusban Írország
- Felkészül:ország?



Three Ireland ✓
@Threelreland



✓ Customer notice ✓

We've been made aware of a FluBot scam text circulating. We would like to warn our customers to take the following actions if they receive a text message that looks like the one below:



Do not click on any links

Remove the text from your phone

Text Message
Today 12:18

DHL: Your parcel is arriving, track here: <http://fuzhoudaikuan.com/a/?6obk7qyn45dt>

10:57 AM · Jun 2, 2021



32



9



Copy link to Tweet

**FedEx**

Action Required

To install you must turn on the accessibility service for "FedEx".

Click "OK" to go to the settings and then scroll until you find "FedEx" and click to turn on the accessibility service.

If you do not find it click on "Downloaded / Installed services" and then click on "FedEx".

OK

Letöltés, telepítés idegen doménről - az jó lesz...

Engedélyek figyelmetlen megadása - hová vezet ez?

The following table contains the list of available FluBot commands received from the C&C server.

Command	Description
BLOCK	Block any notification
UNINSTALL_APP	Uninstall the given application via packagename
SEND_SMS	Send given text to given phone number
RUN_USSD	Running ussd code.
SMS_INT_TOGGLE	Toggle interception sms
CARD_BLOCK	Popup the credit card phishing page
DISABLE_PLAY_PROTECT	Disable play protect via accessibility
OPEN_URL	Open the given url via webview
GET_CONTACTS	Send contact list to server. Later its used for spamming
RETRY_INJECT	Retry inject to already phished application
RELOAD_INJECTS	Resend package list to server.
SOCKS	Open sockets to let the attacker connect



Sok jószándék nincs benne...

Telepítés után:



- minden telefonunkon tárolt adat
- az SMS-ek tartalma, címjegyzék, kamera, mikrofon, BT kapcsolat
- jelszavak netbankhoz, kriptovaluta tárcákhoz

Permission List
android.permission.WAKE_LOCK
android.permission.QUERY_ALL_PACKAGES
android.permission.CALL_PHONE
android.permission.READ_CONTACTS
android.permission.WRITE_SMS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECEIVE_SMS
android.permission.FOREGROUND_SERVICE
android.permission.SEND_SMS
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
android.permission.NFC
android.permission.REQUEST_DELETE_PACKAGES
android.permission.READ_PHONE_STATE
android.permission.READ_SMS
android.permission.INTERNET
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE
android.permission.BIND_ACCESSIBILITY_SERVICE

Accessibility service engedély

- akadálymentesítés fogyatékkal élőknek, vagy biztonsági alkalmazásoknál
- a védelem előtt elrejtí a futó kártékony szolgáltatást (pl. Disable PlayProtect)
- 2020. május ESET: DEFENSOR ID rogue malware app

- Magyar áldozat, 4700 SMS ($4700 \times 35 = 160$ eHUF)
- Az elküldött SMS-ek nem látszanak
- Előre beállított limit, a prepaid „megúszta”
- MyTelenor, Telekom, MyVodafone - valós forgalmi adatok....

index KORONAVÍRUS

2021. 04. 06. kedd
Vilmos, Báborka

BELFÖLD KÜLFÖLD GAZDASÁG KULT TECH-TUD SPORT VÉLEMÉNY BLOG VIDEÓ FOTÓ 24 ÓRA

BELFÖLD CSALÁS SMS KIBERVÉDELEM

A csomagküldős vírus itthon is tarolt

 METAKING
+ KÖVETÉ

2021.03.30. 20:19

Magyarországon sem kímélte az ügyfeleket a Spanyolországból indult csalóprogram. Ott 11 millió telefont fertőzött meg.

ITTHON VOLT OLYAN KÁROSULT, AKINEK 4700 SMS-T KÜLDTEK EL A TELEFONJÁRÓL, MIUTÁN LETÖLTÖTT EGY CSOMAGKÜLDŐS APPLIKÁCIÓT.

A TV és rádióbemondók köszönnek, hogy „Jó napot kívánok!”, aztán elmondják, hogy mi mindentől legyen rossz napunk, rossz kedvünk, félelmünk...

Csomagküldős csalóprogram: volt, akinek több millió forint tűnt el a bankszámlájáról

— RTL HÍRADÓ • 2021. MÁRC. 30. 16:28



Hujder Zoltán

A TELEFONNÁL:

A CSALÁSSOROZAT EGYIK ÁLDOZATA



AZ ÖSSZES PÉNZE ELTŰNT



0:29



2:30

- Magyar áldozat, akinek a bankszámláját is kifosztották

A FluBot főleg banki adatokra utazott (Prodaft Report Svájc 2021.03.05.)

The statistics page of the panel also contains details about the device manufacturers, Android version, device language, and telecommunication operator name. When FluBot successfully obtains the banking credentials, they are sent to the C&C and stored with the following Figure ²⁷ log format.

```
Bot ID: 97F5F572A0F4407B88E8B90F063A94F2
Type: INJECT:com.cajasur.android

{"user":"[REDACTED]","clave":"[REDACTED]","dob":"[REDACTED]","type_injects":"banks","exit":""}Bot ID: A3C658E0E1BF496B9E6CF0CBD3724454
Type: SMS

BBVA: BBVA: Para realizar tu operacion utiliza el codigo [REDACTED] Bot ID: 97F5F572A0F4407B88E8B90F063A94F2
Type: INJECT:com.bbva.bbvacontigo

{"login":"[REDACTED]","password":"[REDACTED]","exit":""}Bot ID: FD44C4B04BF04B1AA1F423E43B8E0BC0
Type: BAL_GRABBER:es.liberbank.cajasturapp
```

Figure 27. Victims Statistics Page

Each log entry for the infected device may contain the SMS messages, banking credentials, device contacts, and application webview text logs, all of which can be used for extracting any kind of text-based credentials from every application that uses webview panes.

KIBEV figyelmeztetés:

- MKB, K&H, Budapest Bank, OTP, UniCredit, George Magyarország
- Online Kriptotárcák: Blockchain Wallet, Coinbase, Binance, Blockchain Wallet

The image displays a Genymotion Emulator window. On the left, a mind map titled 'Flubot.xmind' is open. The central node is 'Flubot'. It has three main branches: '1 Sandbox ftw', '2 Static analysis', and '3 Dynamic analysis'. The '1 Sandbox ftw' branch further branches into 'joe' (with a URL), 'hybrid-analysis', and 'vt' (with a URL). The '2 Static analysis' branch has a sub-branch 'Cikkek' (Articles) which includes links like 'lo-sms-alware-', '30/a-lo-sms-', and 'ztas_nki.'. The '3 Dynamic analysis' branch has a sub-branch 'Resources' which includes links like 'l/frida-', 'tent/FluBot.', and 'FluBot.'. The right side of the emulator shows an Android desktop environment with a Google search bar, a clock showing 12:44, and several app icons including 'Xposed Insta..', 'Security Loc..', 'Inspeckage', 'Email', and 'Gallery'. A small video feed of a person is visible in the bottom right corner of the emulator window.

[Hackersuli] "Megérkezett a csomagod!" avagy élő FluBot analízis
2021.04.07. YouTube: Kovács Zsombor és Balázs Zoltán

Kármentés utólag #1

- FluBot Malware Uninstall (később letiltották)
- Safe mód újraindít, csak a gyári alkalmazások, így eltávolítható
- AV program teljes ellenőrzés
- Biztonsági mentés, gyári állapotra való visszaállítás



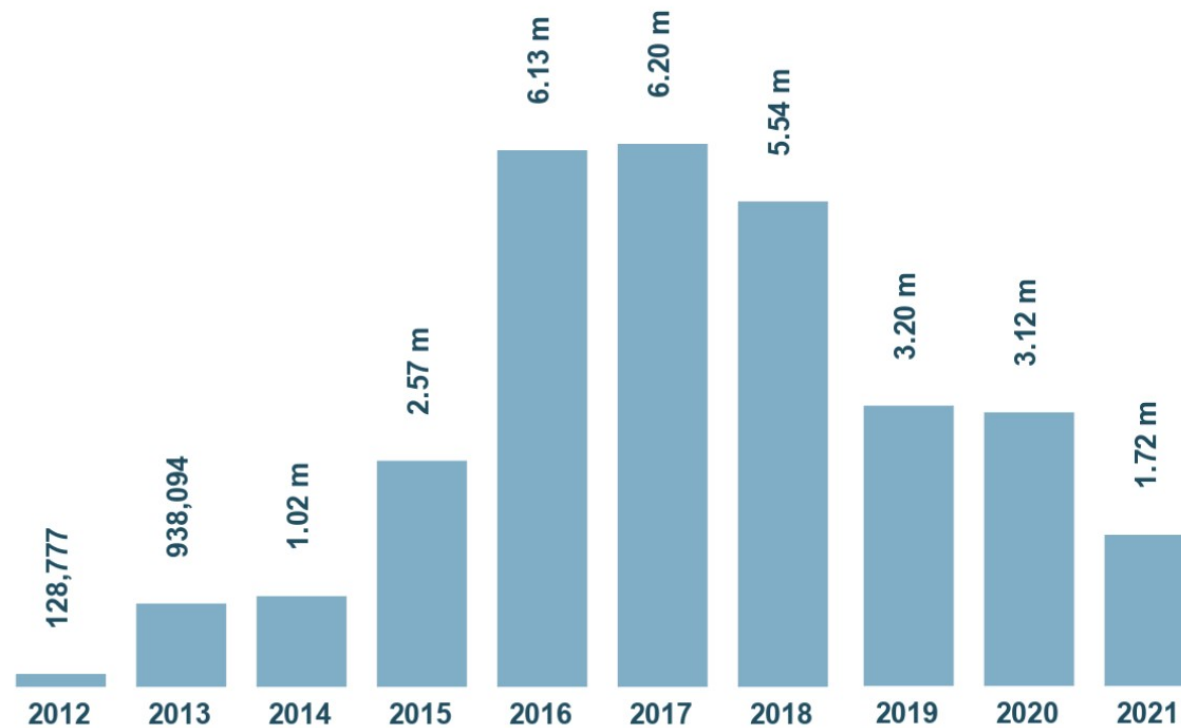
Kármentés utólag #2



- Jelszavak cseréje, beleértve a banki felületeket is
- Bank értesítése
- Akit anyagi kár ért: kiber@nni.police.hu

MINDEZ A MÁR ELLOPOTT ADATOKAT NEM HOZZA VISSZA!

Development of Android malware

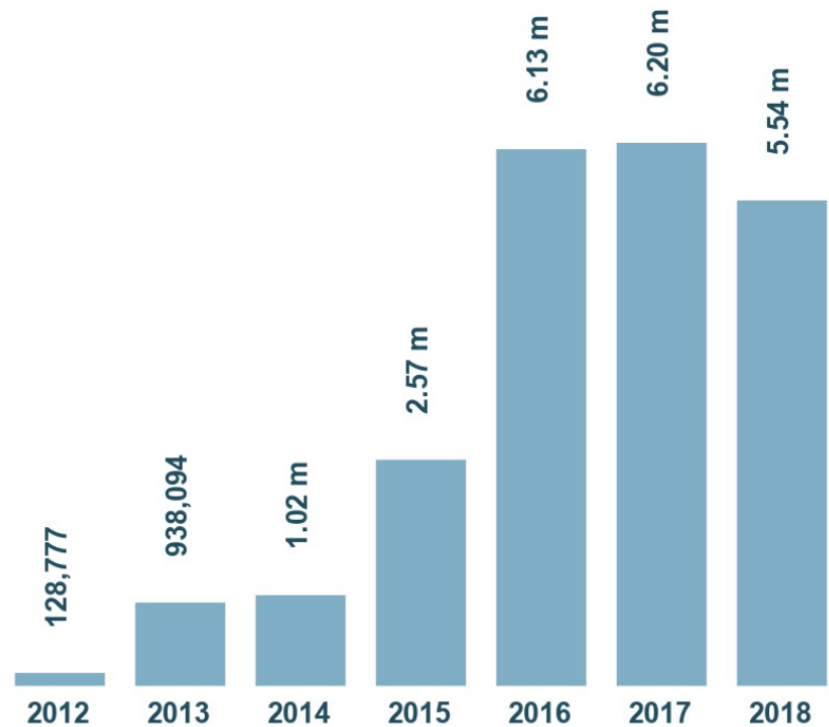


Last update: July 01, 2021

Copyright © AV-TEST GmbH, www.av-test.org

Androidos kártevő helyzet 2021. július

Development of Android malware

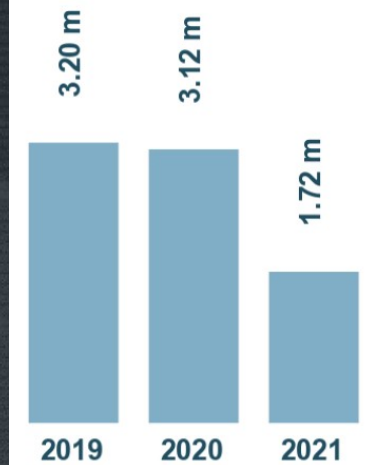


Last update: July 01, 2021

Copyright © AV-



AVTEST



-TEST GmbH, www.av-test.org

Androidos kártevő helyzet 2021. július

2017. Google Play Protect

2018. Google Play szigorítások

- aktuális Android főverzió max -1 év
- korlátozott SMS és Hívásnapló engedélyek
- Accessibility Service-t „nem rendeltetésszerű” (keylogger)
- 55%-kal több törölt, elutasított alkalmazásbeküldés
- irányelvsértés 80% visszaélésszerű fejlesztői hálózatok
- pl. új fiók, fejlesztők felvásárlása, lefizetése



A KIBEV javaslatai



ÍGY VÉDHETED MEG ANDROIDOS ESZKÖZEIDET A HACKEREKTŐL

MEGBÍZHATÓ FORRÁSBÓL

TÖLTÖD LE AZ
ALKALMAZÁSOKAT.

TELEPÍTESZ

EGY MEGBÍZHATÓ
VÍRUSIRTÓ APPOT.

KERÜLÖD

A NYILVÁNOS WI-FI
HÁLÓZATOKAT.



ELLENŐRZÖD

AZ ALKALMAZÁSOK ÁLTAL
KÉRT HOZZÁFÉRÉSI
ENGEDÉLYEKET.

GYAKRAN FRISSÍTED

AZ ALKALMAZÁSOKAT ÉS
AZ ANDROID RENDSZERT A
LEGÚJABB VERZIÓRA.

NEM KATTINTASZ

EGYBŐL A LINKEKRE,
ELŐTTE ÁTGONDOLOD,
HOGY GYANÚSAK-E.

Megelőzésdi

23:29 48%

creatagreat.com/t/?m7

Megtévesztő webhely megnyitására készül

A támadók a(z) creatagreat.com webhelyen megpróbálhatják csellel rávenni Önt például arra, hogy veszélyes szoftvert telepítsen, vagy felfedje személyes adatait (jelszavakat, telefonszámokat, bankkártyaadatokat stb). [További információ.](#)

A Chrome legmagasabb szintű biztonságának eléréséhez [kapcsolja](#)

Vissza a biztonsághoz

Részletek



22:40 53%

petdio.com/pkge/?a1k2

FedEx

eset MOBILE SECURITY

Észlelt kártevők

fedex.apk
Android/TrojanDropper.Agent.HNJ

Ez a fájl távoli hozzáférést biztosíthat a fertőzött készülékhez, bizalmas adatokat szivárogtathat ki és elérhetővé teheti azt más kártevők számára. Eltávolítása erősen javasolt.

[TOVÁBBI INFORMÁCIÓK](#) [ELTÁVOLÍTÁS](#)

fedex.apk. Megnyitás

Kommentből: "Mikor lesz már a felhasználóknak józan paraszti eszük?"

Köszönöm, hogy zavartam...
Nem akartam ;-)

