CYBERSECURITY
EXPERTS ON YOUR SIDE

IT Fest LUPA 2021. június 24.

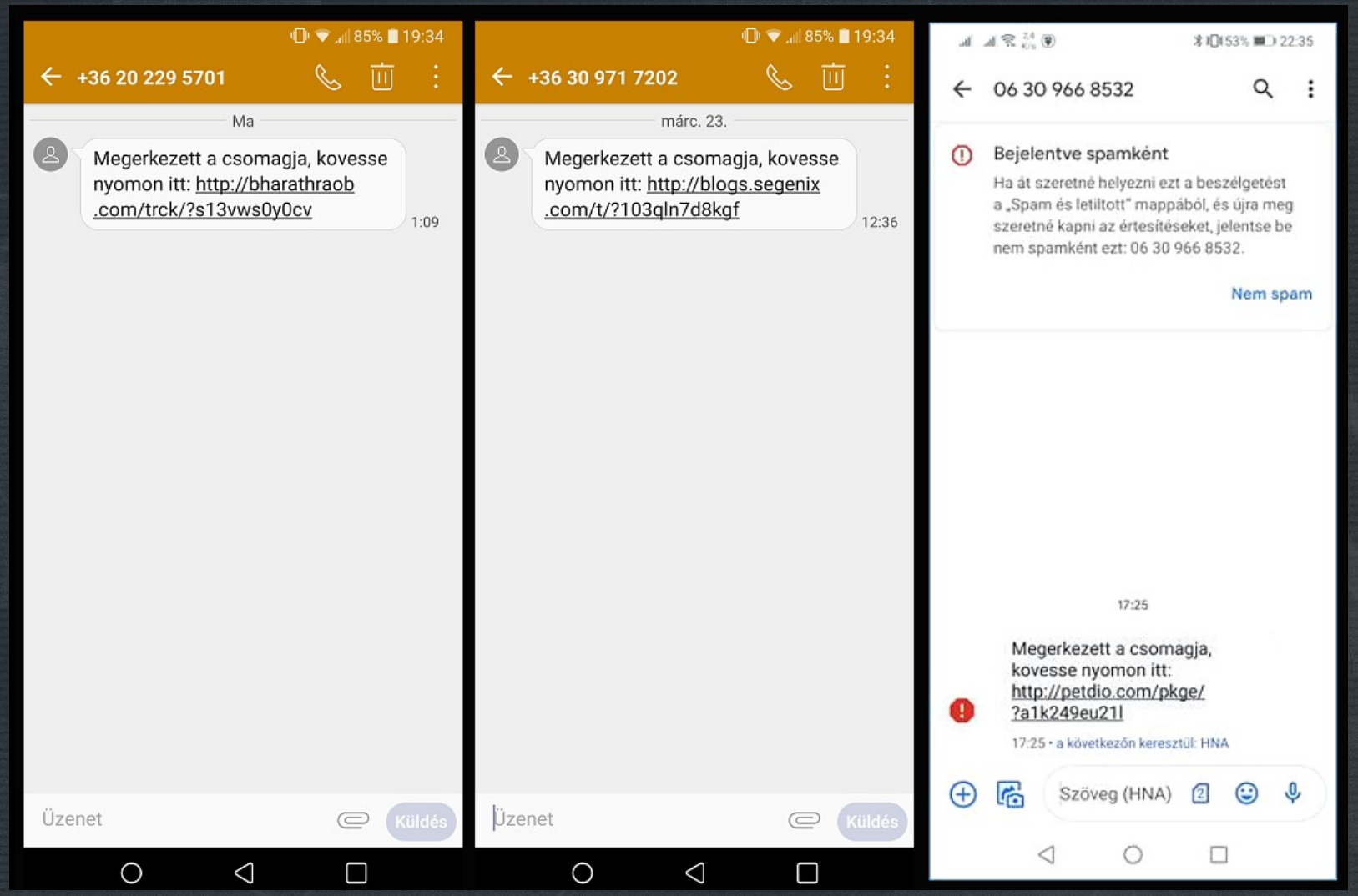
Csomagja érkezett Mylord!

Csizmazia-Darab István
IT biztonsági szakértő, ESET/Sicontact

csizmazia-darab.istvan@sicontact.hu

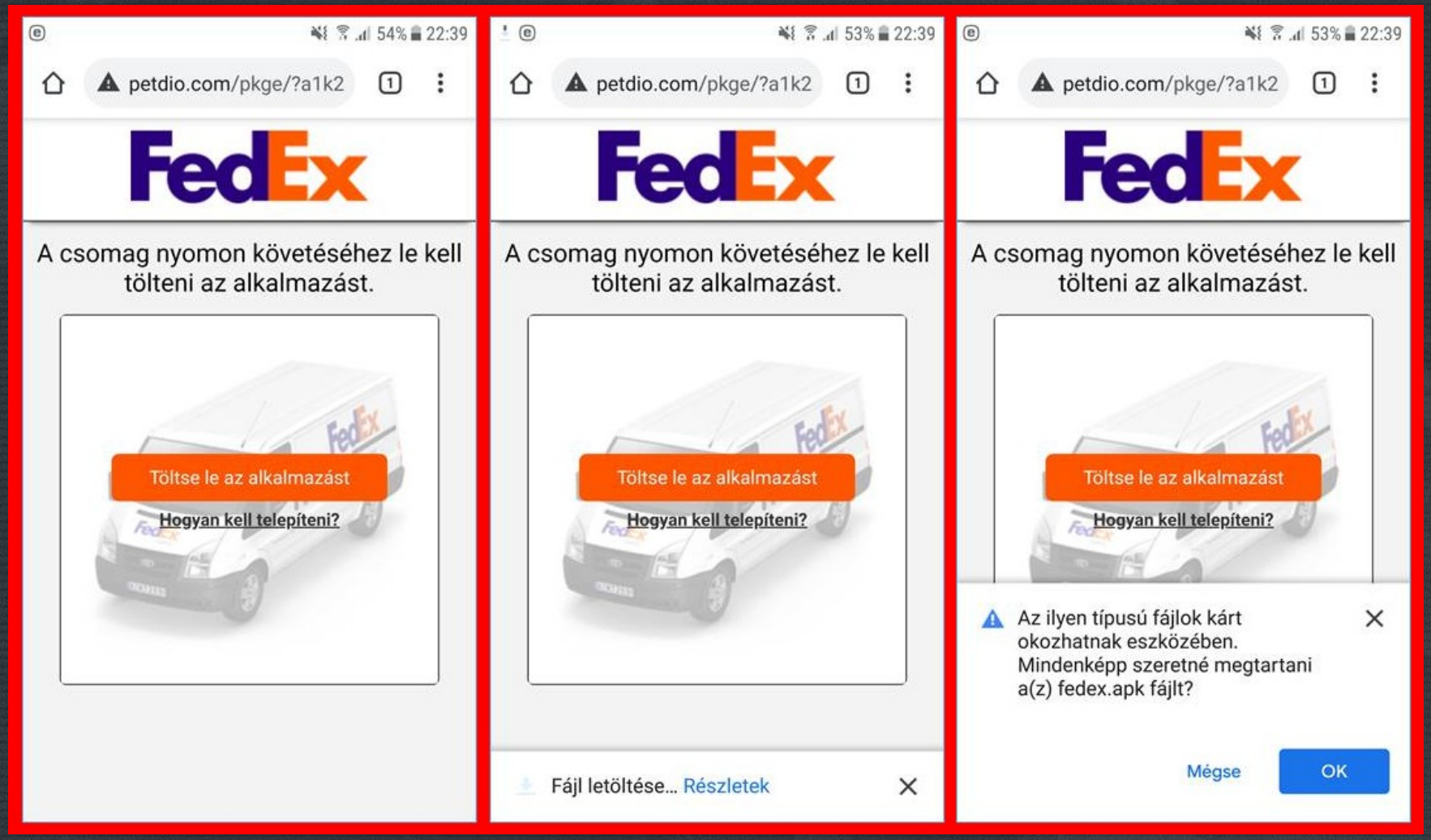
Linkek, letöltések, telepítések, engedélyek - Hova vezet mindez?

Egy nem mindennapi SMS csalás tanulságai.



2021. március
- több százezer SMS üzenet
- magyar telefonszámokról
- nemzetközi futárcég FedEx.apk app

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



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
@ThreeIreland

✅ 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:

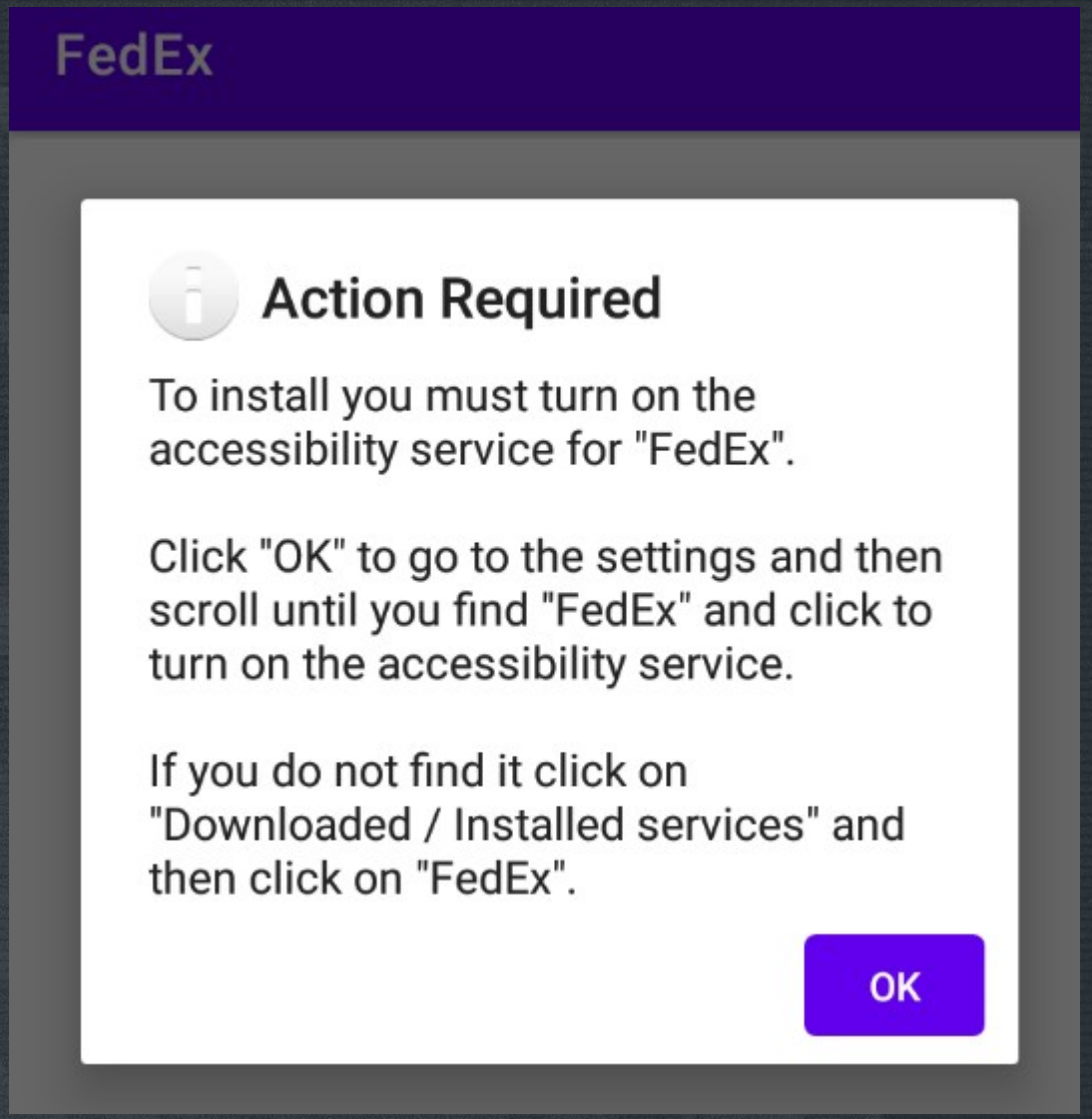
🔗 Do not click on any links
🗑️ Remove the text from your phone

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



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

Telepítés után:

- minden telefonunkon tárolt adat

- az SMS-ek tartalma, címjegyzék, kamera, mikrofon, BT kapcsolat

- jelszavak netbankhoz, kriptovaluta tárcához

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

- a védelmi programok elől elrejti a futó kártékony szolgáltatást (pl. Disable PlayProtect)

- Magyar áldozat, 4700 SMS (4700x35=160 eHUF)
- Az elküldött SMS-ek nem látszanak
- Előre beállított limit, a prepaid „megúszta”
- MyTelenor, Telekom, MyVodafone a valós forgalmi adatokkal

index KORONAVÍRUS

2021. 04. 06. kedd
Vilmos, Bíborka

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

BELFÖLD | CSALÁS | SMS | KIBERVÉDELEM

A csomagküldős vírus itthon is tarolt

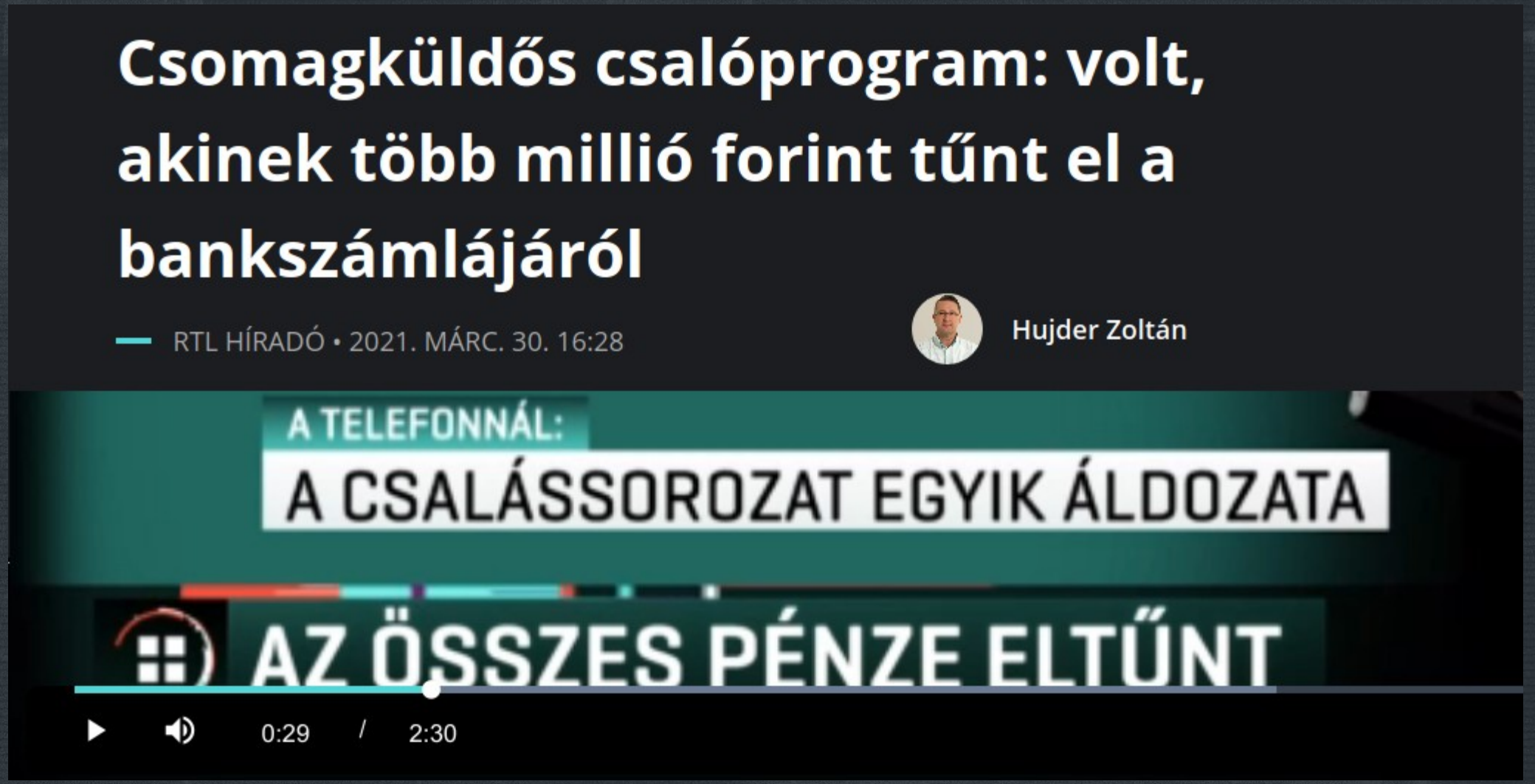
METAKING

+ 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.**



- Magyar áldozat, akinek a bankszámláját is kifosztották

- A FluBot elsősorban banki adatokra utazott (Prodaft Report 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.

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.

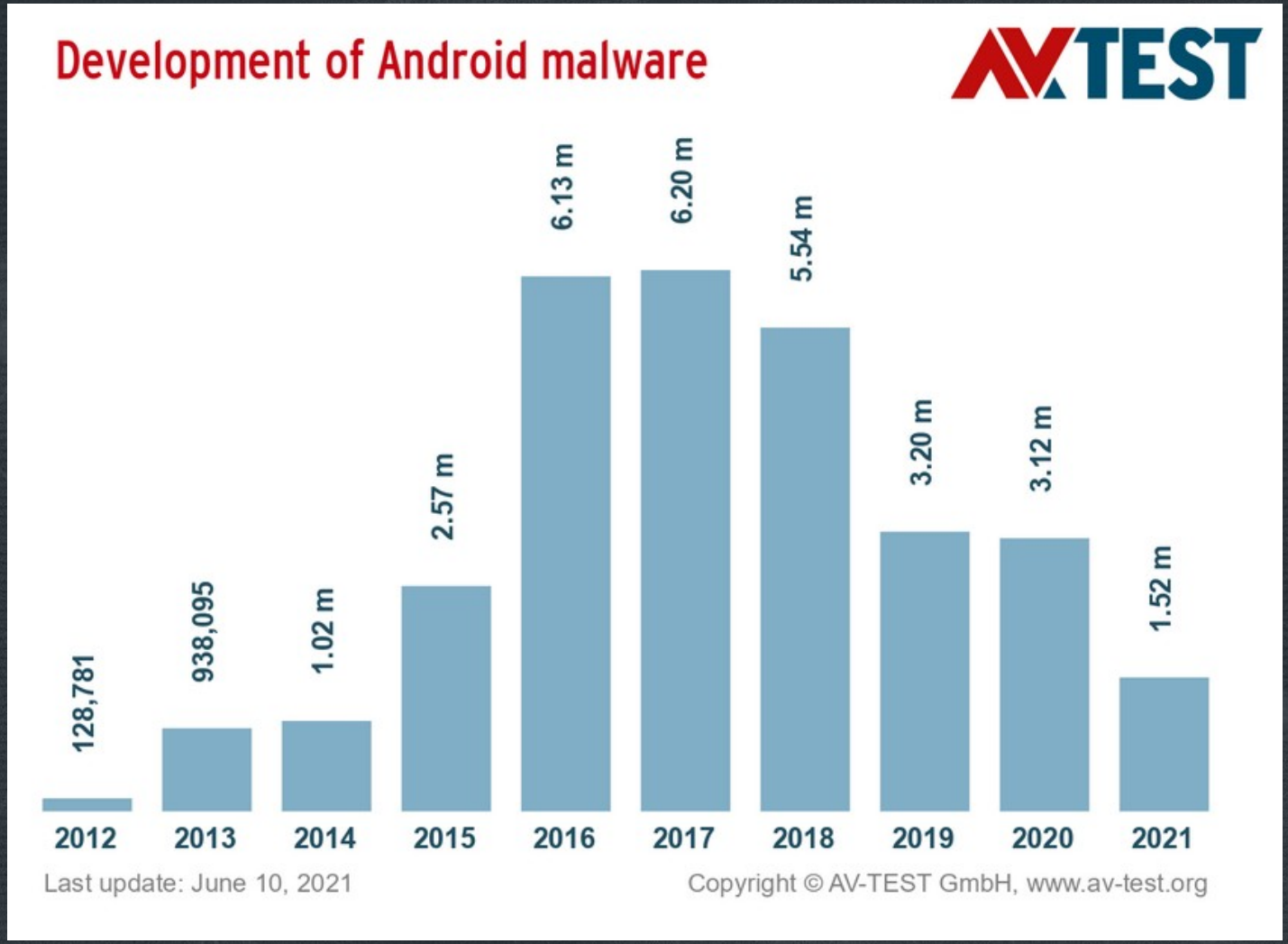
Kármentés utólag #1

- FluBot Malware Uninstall (később letiltották)
- Safe módban újraindítás, csak a gyári alkalmazások, a kártékony program eltávolítható
- AV program teljes ellenőrzés
- Adatok biztonsági mentése, gyári állapotra való visszaállítás

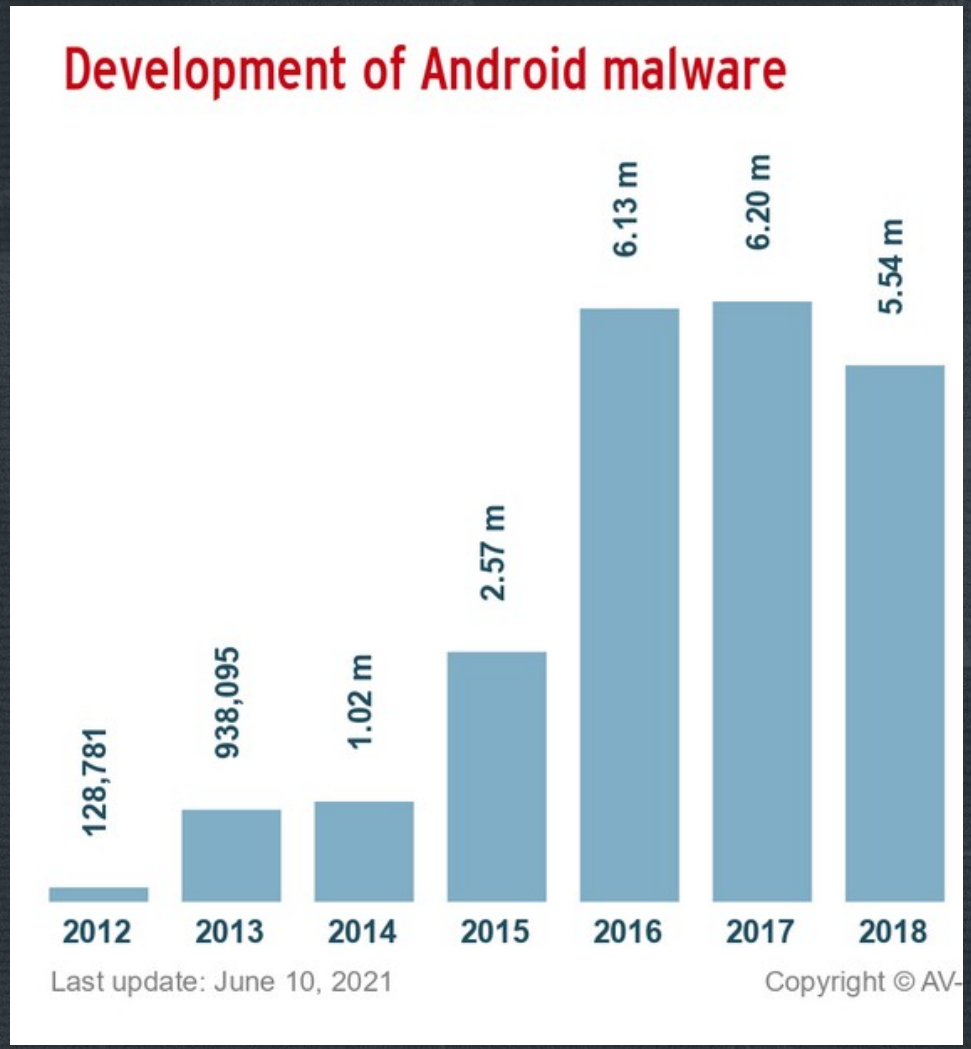
Kármentés utólag #2

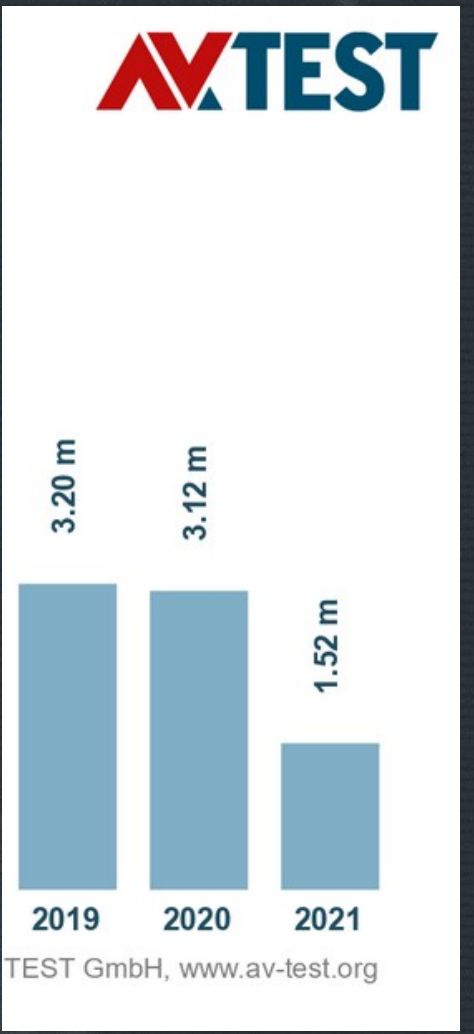
- Jelszavak cseréje, beleértve a banki felületeket is
- Bank értesítése
- Akit anyagi kár ért: kiber@nni.police.hu

MINDEZ A MÁR ELLOPOTT ADATOKAT NEM HOZZA VISSZA!

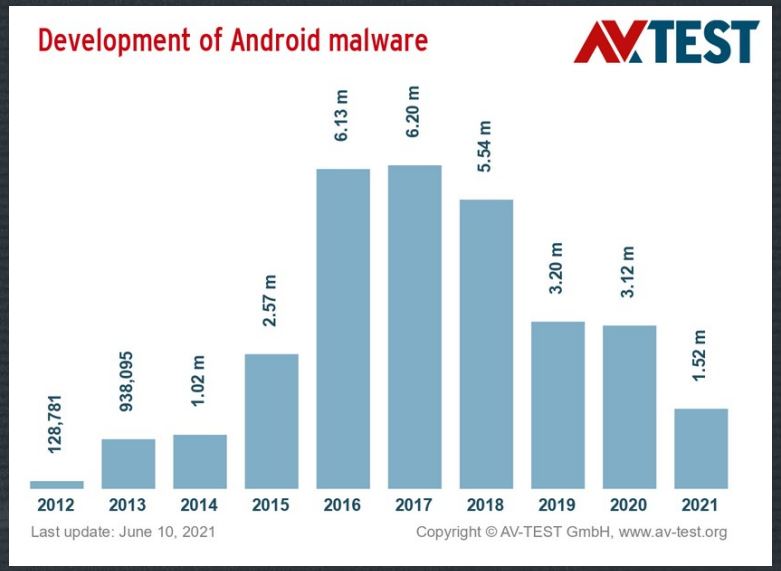


Androidos kártevő helyzet 2021. június



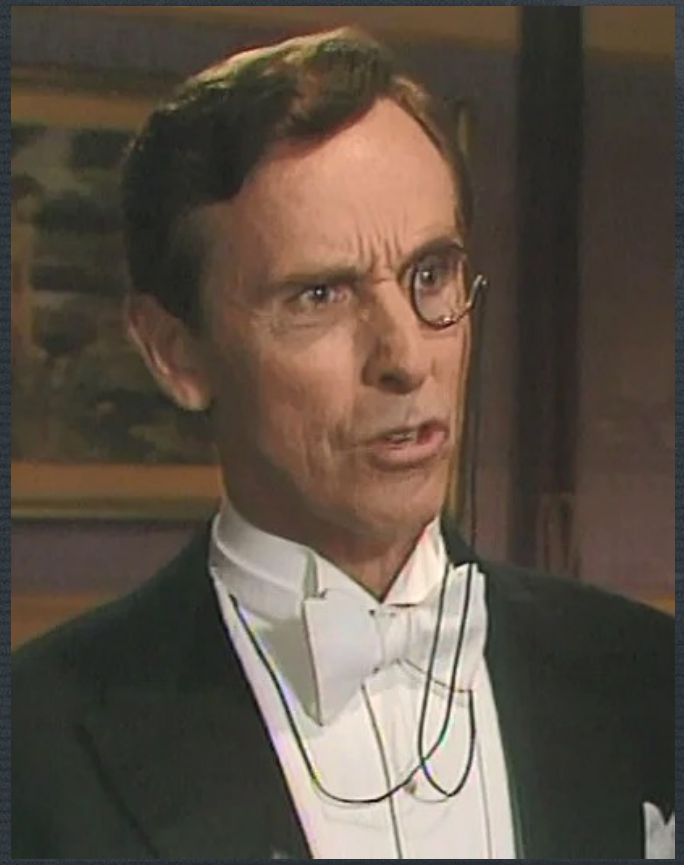


Androidos kártevő helyzet 2021. június



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.

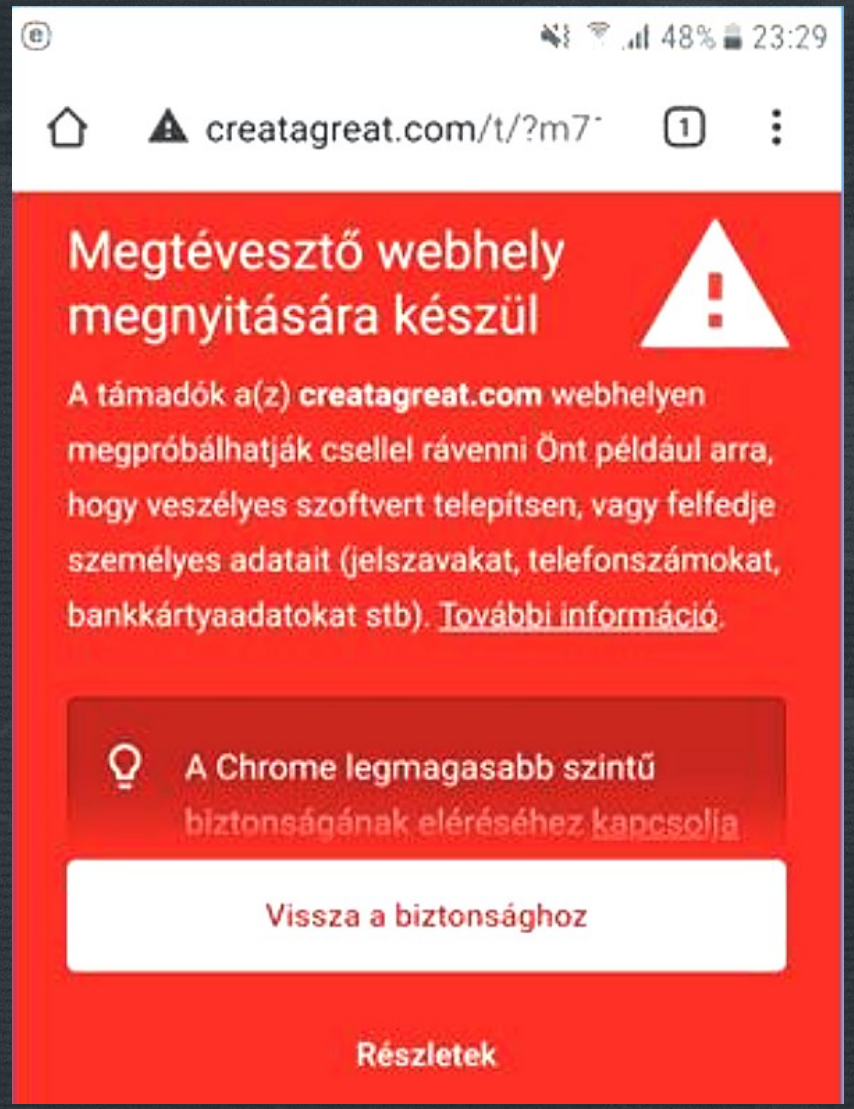
Megelőzés #1

- Figyelmesen a kéretlen üzenetekkel

- Adott szolgáltatótól jött az értesítést?

- Legitim forrásból telefonra SMS-ben internetes linket?!

Megelőzés #2



- Adathalászat: helyesírás, ékezetek, sürgetés vagy ígéret, link vagy csatolmány

- Ha az URL cím idegen

- Gyanús kikapcsoltatni a biztonsági figyelmeztetéseket

Megelőzés #3

- Idegen külső forrásból származó telepítés

- Megbízható, hivatalos forrás pl. Google Play

- Alkalmazások és OS frissítések

- Vírusvédelem, blokkolja a kártékony tartalmakat

Köszönöm a figyelmet!