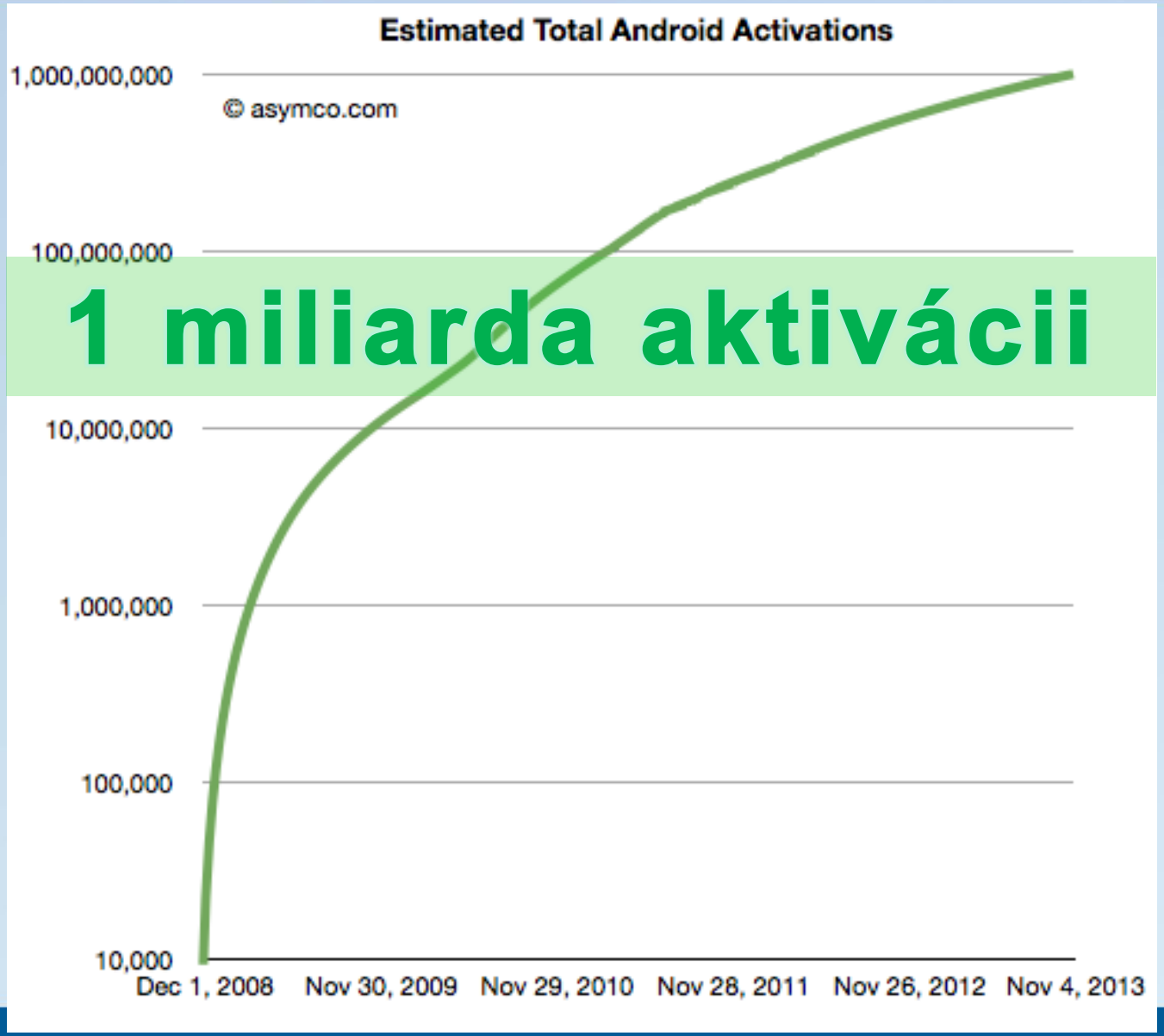
Agenti, boxeri a podvodníci vo vrecku

Ing. Gabriel Braniša

Android v roku 2013

Medzi najpopulárnejšie operačné systémy pre mobilné zariadenia patrí naďalej Android

Android v roku 2013



1 miliarda aktivácii

Android v roku 2013

2013 Q1 evidujeme

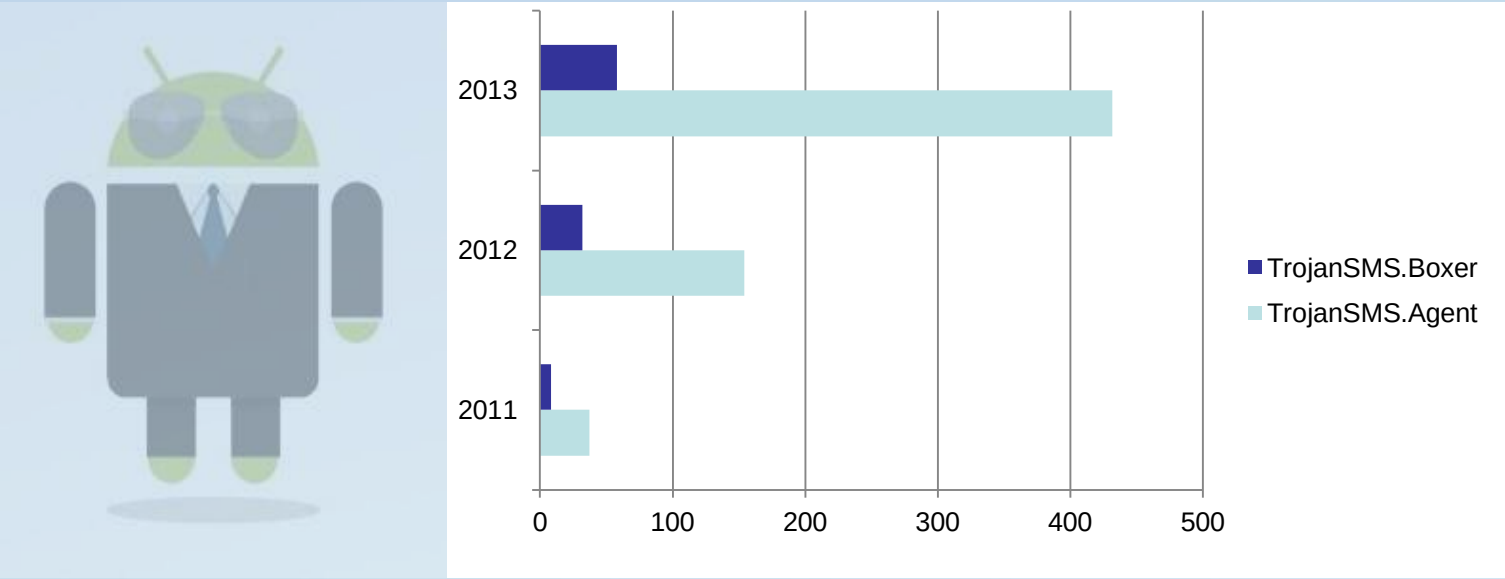
- 230+ rodín malwaru
- ~1150 odlišných variantov

Year of mobile malware

Využívanie smartphonov

- Aplikačná úroveň
- Akúkoľvek interakciu cez používateľské rozhranie je možné automatizovať
- Algoritmy ako obraz vývoja a skúseností

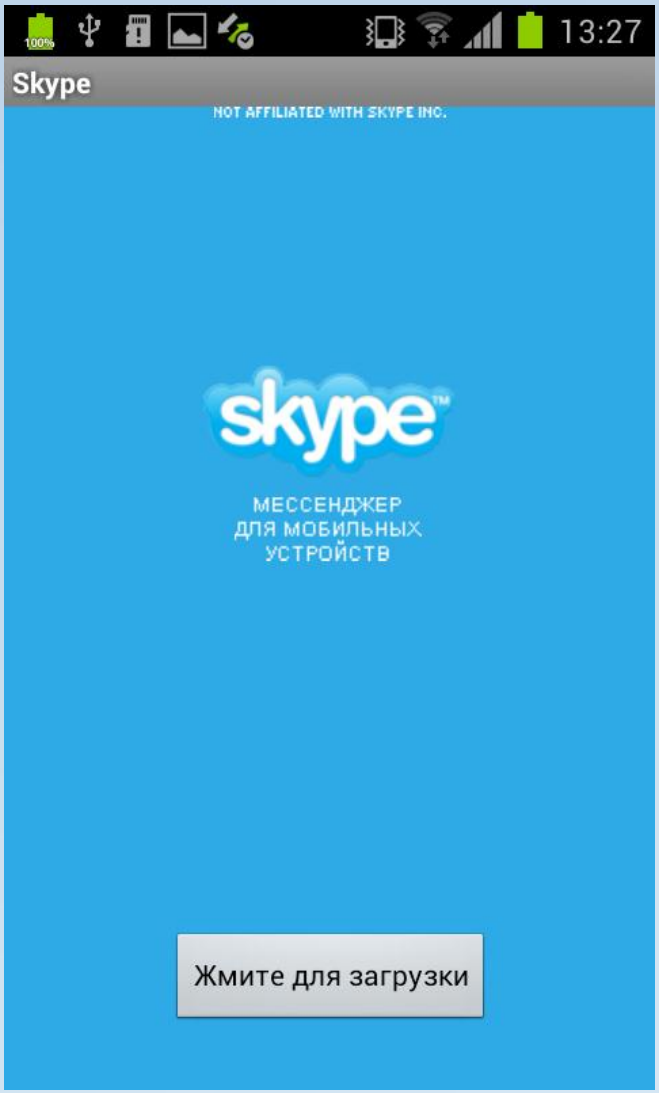
Najrozšírenejší vreckoví výtržníci

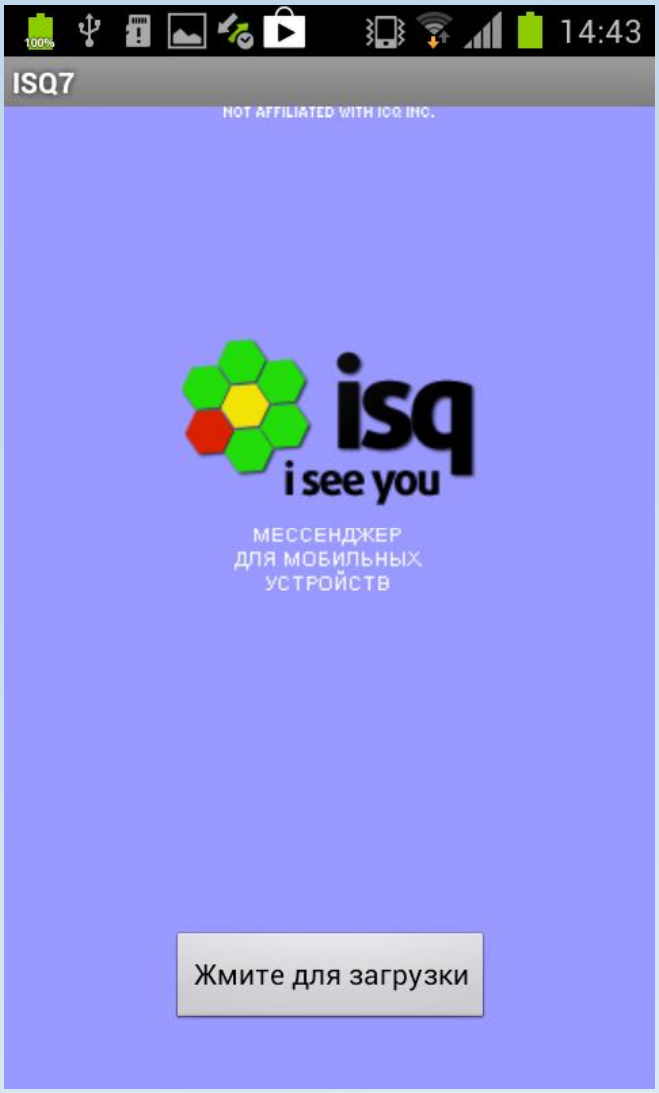


Android/TrojanSMS.Agent

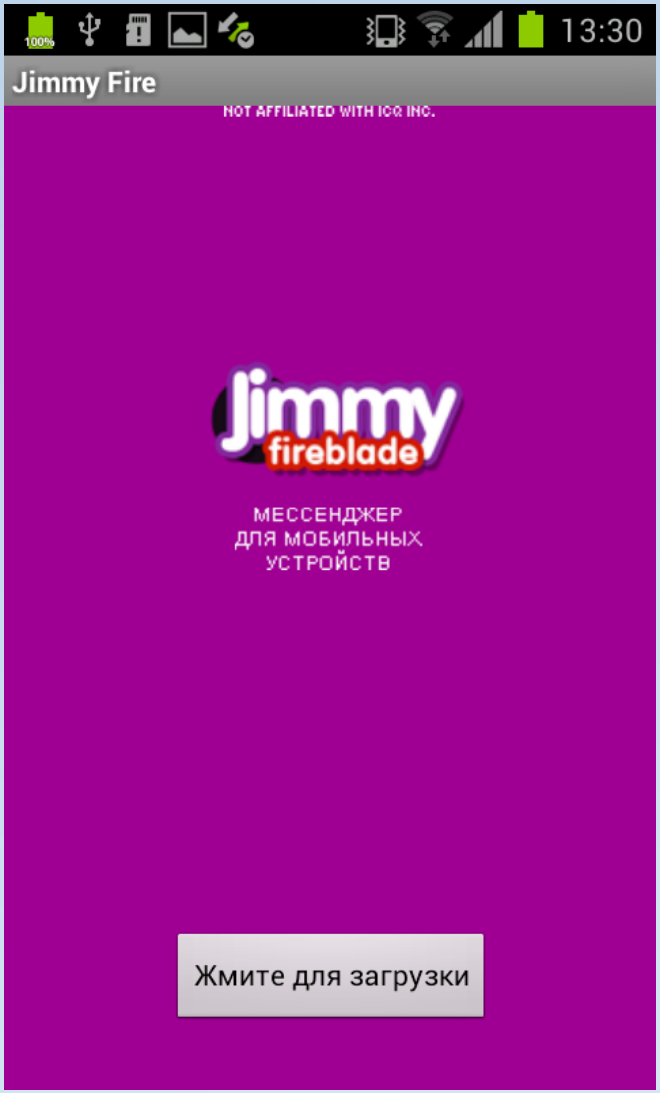
- Odosiela textové správy na spoplatnené čísla
- Kradne citlivé dáta a odosiela ich na vzdialené servery
- September 2011
- Najväčší výskyt má v Rusku, v Ukrajine a v Bielorusku
- Počet variantov ~430
- Vystupuje pod falošnou identitou známych aplikácií

Android/TrojanSMS.Agent

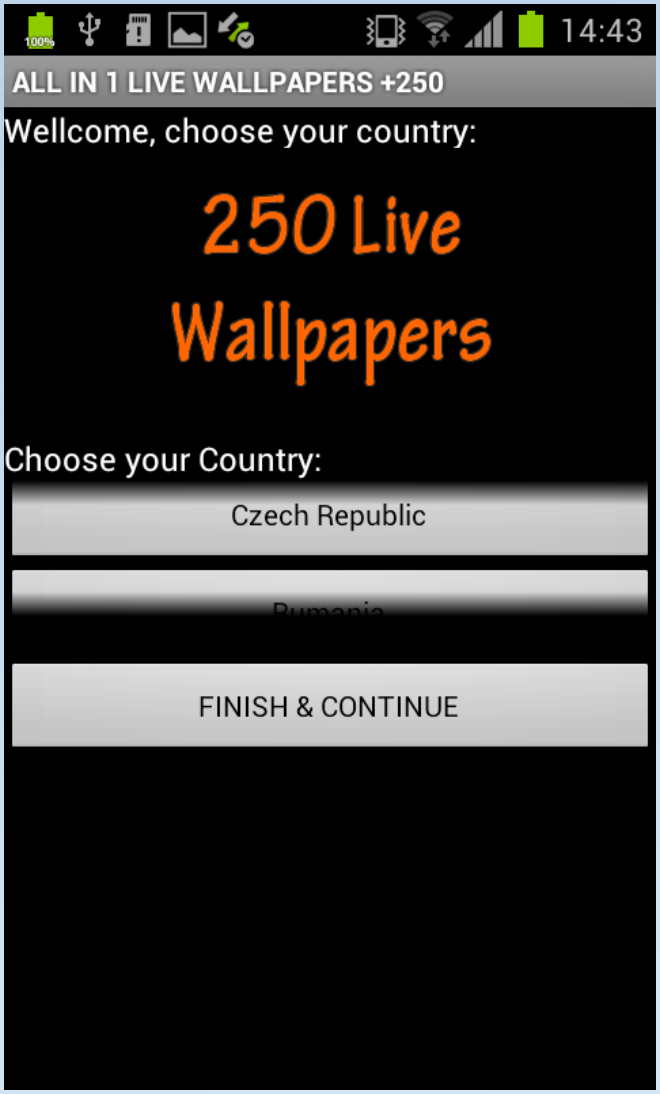


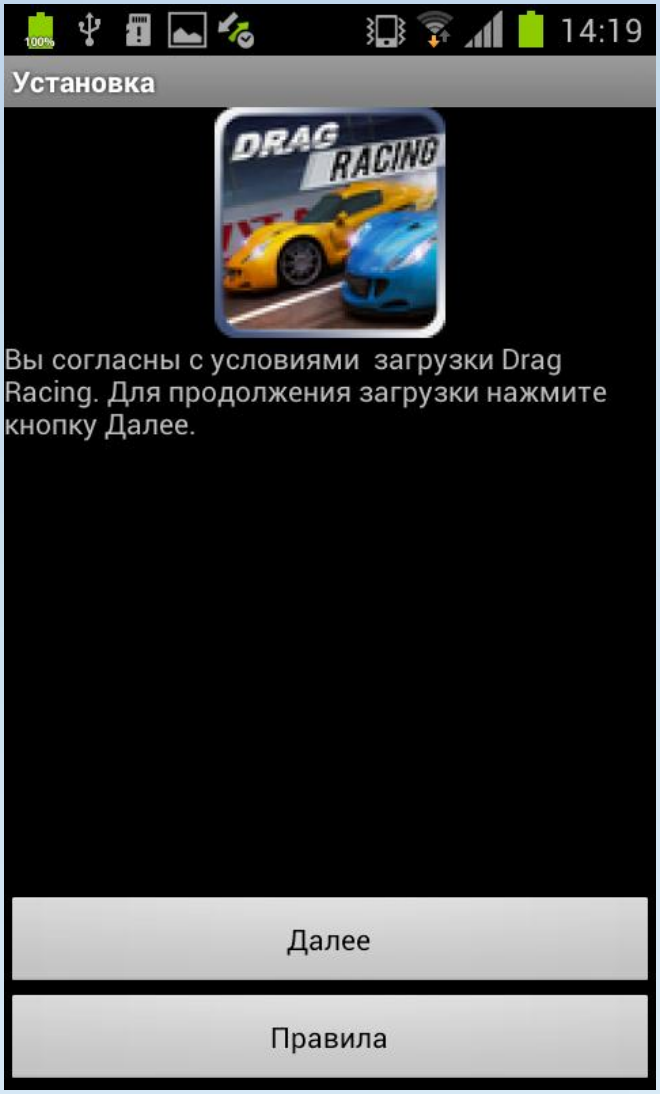


Android/TrojanSMS.Agent

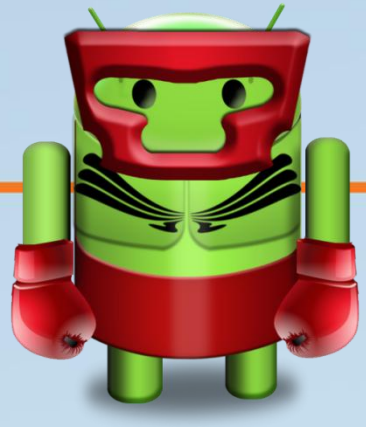


Android/TrojanSMS.Agent





Android/TrojanSMS.Boxer



- Najväčší výskyt má taktiež v Rusku, v Ukrajine a v Bielorusku
- Zisťuje krajinu a mobilného operátora obete
- Na základe týchto informácií odošle textovú správu na spoplatnené číslo danej krajiny
- Juhoafrická republika, Švédsko, Švajčiarsko, Čile, Francúzsko, Turecko, Rumunsko, **Poľsko**, Peru, Nórsko, Nový Zéland, Holandsko, Mexiko, Malajzia, Španielsko, Egypt, Dánsko, Grécko, Nemecko, **Maďarsko**, Spojené kráľovstvo, Brazília, Belgicko, Argentína, **Rakúsko**, Estónsko, **Česká republika**, Čierna Hora, Chorvátsko, Fínsko, Tchaj-wan, Slovinsko, Srbsko, Saudská Arábia, Portugalsko, Panama, Spojené arabské emiráty, Nikaragua, Moldavsko, Maroko, Macedónsko, Luxembursko, Litva, Libanon, Lotyšsko, Kirgizsko, Cyprus, Katar, Kambodža, Hongkong, Honduras, Guatemala, Bosna a Hercegovina, Bulharsko, Bielorusko, Arménsko, Alžírsko, Azerbajdžan, Kazachstan, **Ukrajina**, Ruská federácia

Android/Spy

Utajené sledovanie sa zameriava na:

- Textové a obrázkové správy
- Obrázky
- GPS
- Kontakty
- História otvorených internetových stránok
- Sledovanie obete prednou kamerou
- Odpočúvanie
- Zaznamenávanie hovoru

USSD

Unstructured Supplementary Service Data (USSD) je kód, ktorý predstavuje príkaz zaslaný mobilnému telefónu.

Information

***#44336#** Software Version Info
***#1234#** View SW Version PDA, CSC, MODEM
***#12580*369#** SW & HW Info
***#197328640#** Service Mode
***#06#** IMEI Number.
***#1234#** Firmware Version.
***#2222#** H/W Version.
***#8999*8376263#** All Versions Together.
#272*imei# Product code
#*#3264#*# RAM version
***#92782#** Phone Model
#*#9999#*# Phone/pda/csc info

Testing

***#07#** Test History
***#232339#** WLAN Test Mode
***#232331#** Bluetooth Test Mode
***#*#232331#*#*-** Bluetooth test

USSD

Štyri podmienky pre zneužitie USSD

1. Automatická realizácia USSD kódu
2. Existencia Factory Reset kódu
3. Android pracuje s URI (uniform resource identifier)

<scheme name> : <hierarchical part> [? <query>] [# <fragment>]

4. Android default internet browser realizuje URI obsah pod iframe HTML tagom

```
<HTML> <BODY>
<iframe width="1" height ="1" src="tel:*%2306%23">
</iframe>
</BODY> </HTML>
```

USSD

MITMA

- Nie každá bezdrôtová sieť je čestná a nezištná
- Útok kdekoľvek a kedykoľvek
  - Dopyt do internete
  - Vhodný názov siete

MITMA


SAMSUNG
14:57
14:57
Thu.
17/01
2 °C 2° | 0°
Petrzalka
Partly sunny
Google
Readers H
Social Hub
Maps
Play Store
Phone
Contacts
Messaging
Applications
SAMSUNG
14:57
14:57
Thu, 17 Jan
Camera
Gmail
ICQ
Facebook
Skype

MITMA - prevencia

- Host to host šifrovanie (IPsec)
- Využívať šifrovacie protokoly (SSL)
- Subneting

Odporúčania

- Kryptovanie dát
- Pripájať sa len na dôveryhodné zdroje internetu
- Šifrovať komunikáciu (internet, SMS)
- Výber aplikácií od známych developerov
- Preferovať najsťahovanejšie s vysokým hodnotením
- Uprednostniť oficiálny market
- Prehodnotiť žiadosť na pridelenie práv pri inštalácií aplikácie
- Vyhnúť sa inštalácií aplikácií z neznámeho zdroja
- Udržiavať zariadenie aktualizované
- Nainštalovať mobilný antivírus

Ďakujem za pozornosť

branisa@eset.sk