ESET SECURITY DAYS 2013

PREČO SA ÚTOKY NA PC PRENIESLI DO MOBILNÝCH PRÍSTROJOV

Gabriel Braniša

Čo je Android

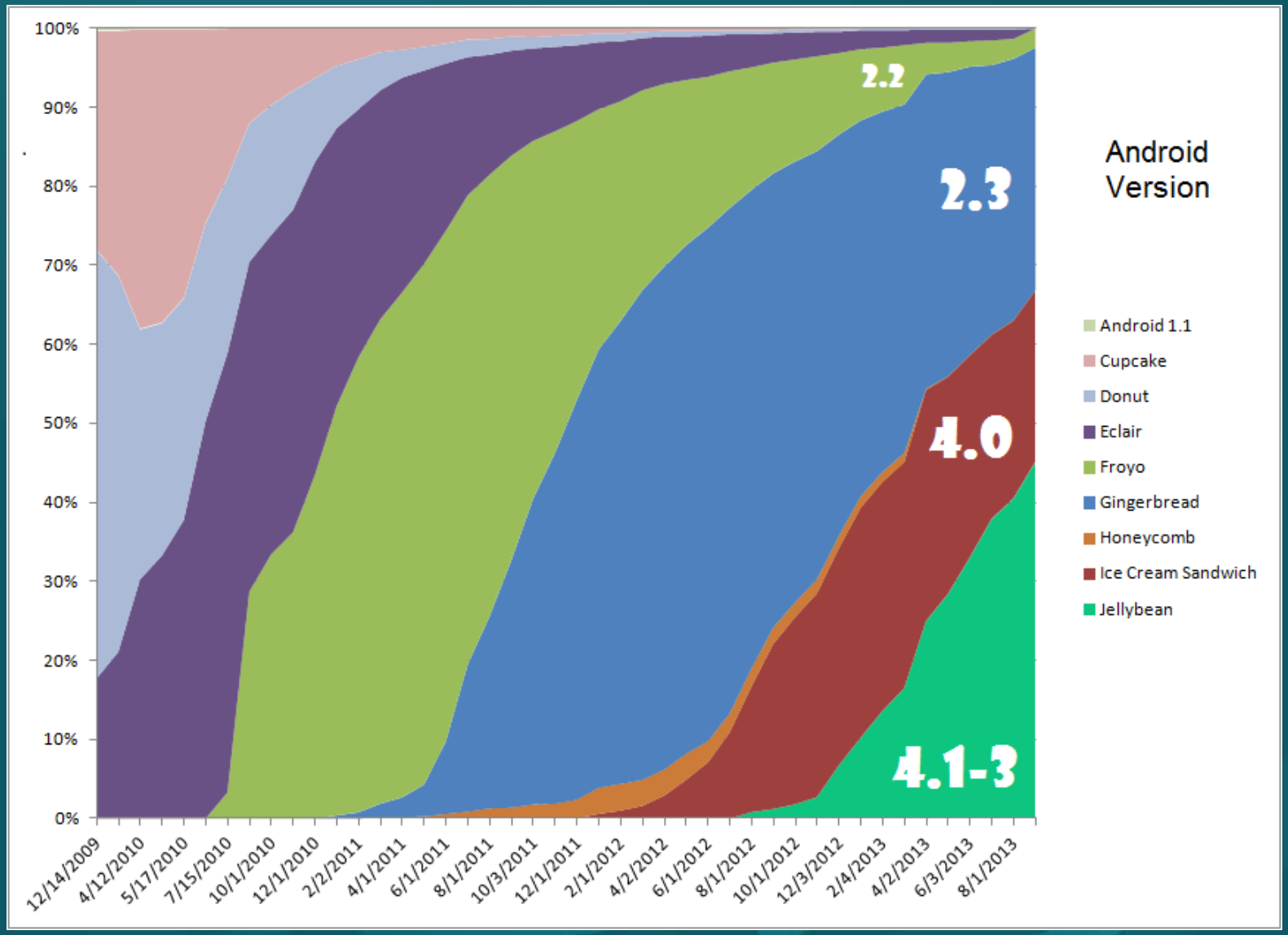
Operačný system pre mobilné zariadenia

Mobilné zariadenia od rôznych výrobcov

Android

Android 1.0	23.09.2008
Android 1.5 Cupcake	27.04.2009
Android 1.6 Donut	15.09.2009
Android 2.0 Eclair	26.10.2009
Android 2.2 Froyo	20.05.2010
Android 2.3 Gingerbread	06.12.2010
Android 3.0 Honeycomb	22.02.2011
Android 4.0 Ice Cream Sandwich	19.10.2011
Android 4.1 Jelly Bean	27.06.2012
Android 4.3 Jelly Bean	**24.07.2013**

Android


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
12/14/2009
4/12/2010
5/17/2010
7/15/2010
10/1/2010
12/1/2010
2/2/2011
4/1/2011
6/1/2011
8/1/2011
10/3/2011
12/1/2011
2/1/2012
4/2/2012
6/1/2012
8/1/2012
10/1/2012
12/3/2012
2/4/2013
4/2/2013
6/3/2013
8/1/2013
2.2
2.3
4.0
4.1-3
Android Version
Android 1.1
Cupcake
Donut
Eclair
Froyo
Gingerbread
Honeycomb
Ice Cream Sandwich
Jellybean

Prečo Android

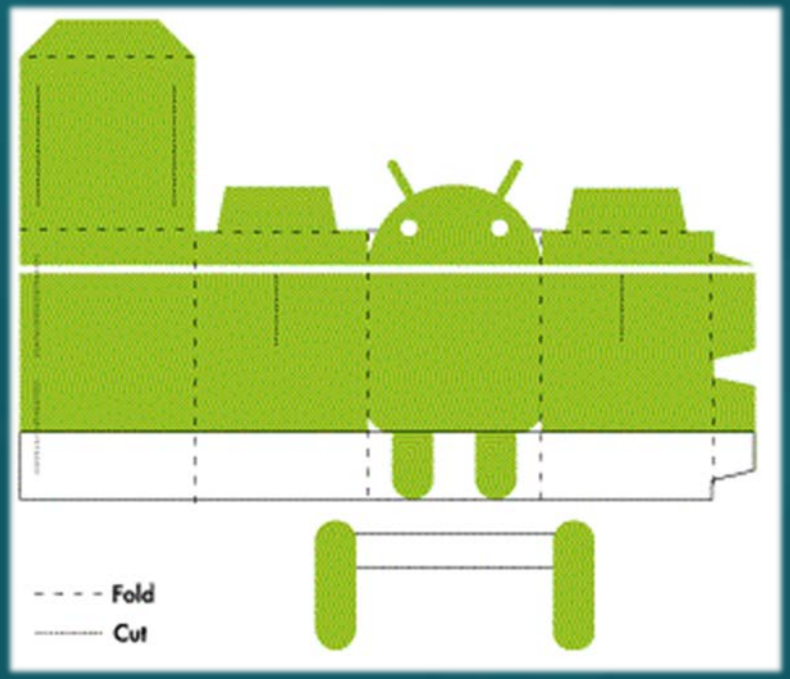
Prečo Android

Prečo Android

Prečo Android

Prečo Android

AOSP – Android Open Source Project



http://source.android.com/

Prečo Android

Prečo Android

Prečo Android

Prečo Android

Developerský poplatok

Prečo Android

Je založený na známych technológiách

Linux

C/C++

JAVA

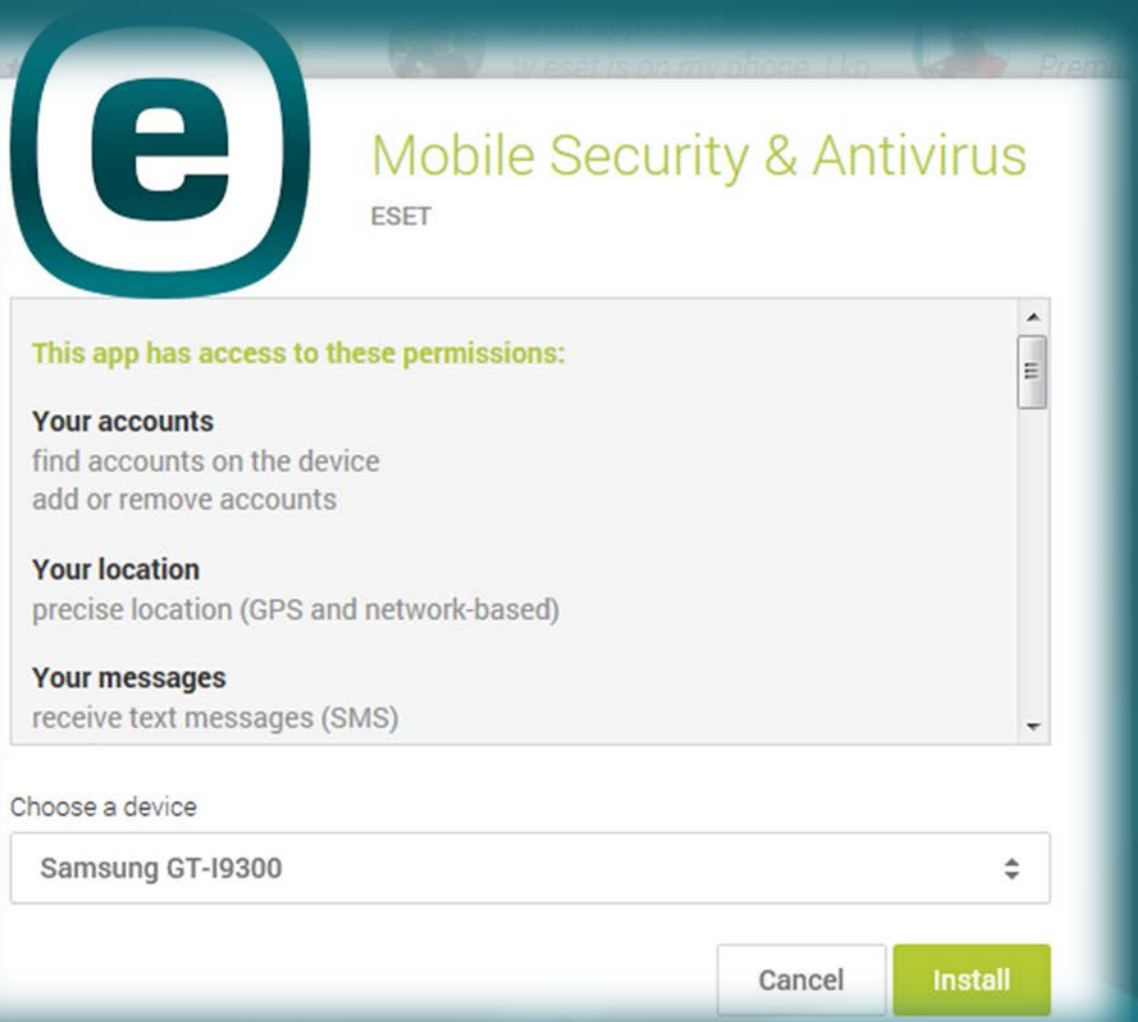
Architektúra

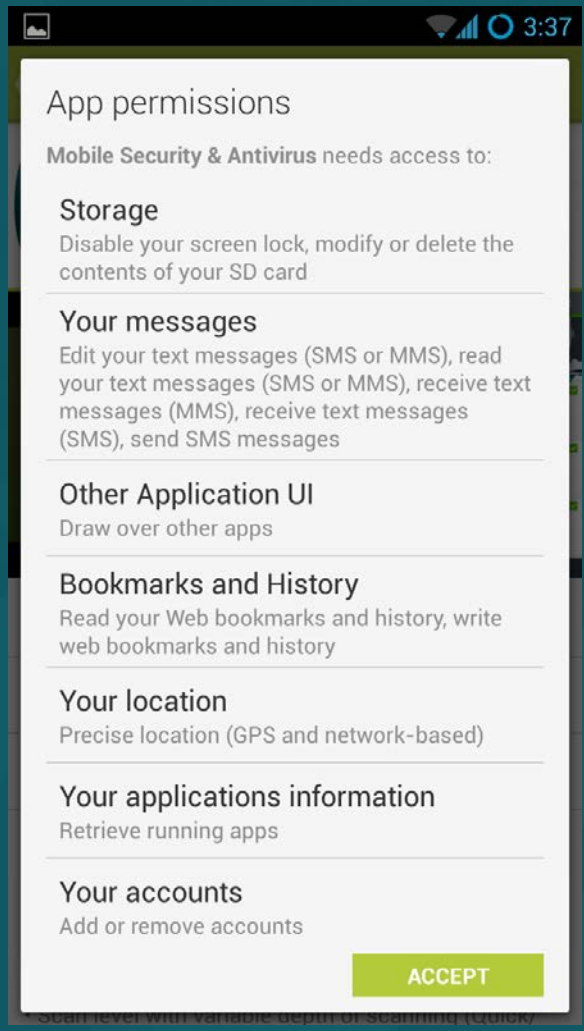
Bezpečnostné prvky

Podpisovanie aplikacií

Permissions

Permissions





Android malware všeobecne

Android malware všeobecne

Kategórie zločinu:

a) Základná

Bežní „vreckoví zločinci“

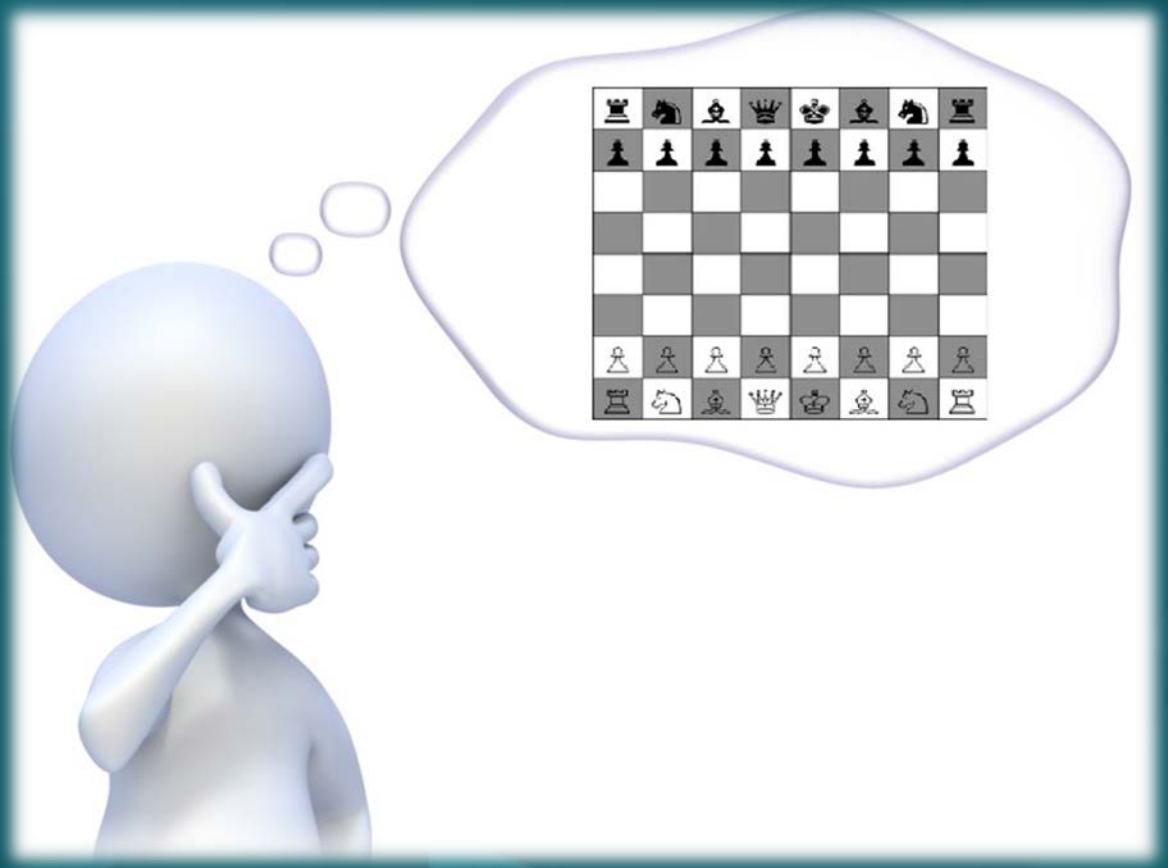
b) Pokročilá

Organizovaný zločin, obete sú lákané a usmerňované do pasce

c) Profesionálna

Účely národnej bezpečnosti a iných spoločenských zoskupení. Poľudšťovaním a moralizovaním postupov tohto zločinu sa stáva v spoločnosti neviditeľným

Spôsob infiltrácie



Spôsob infiltrácie

Spôsob infiltrácie

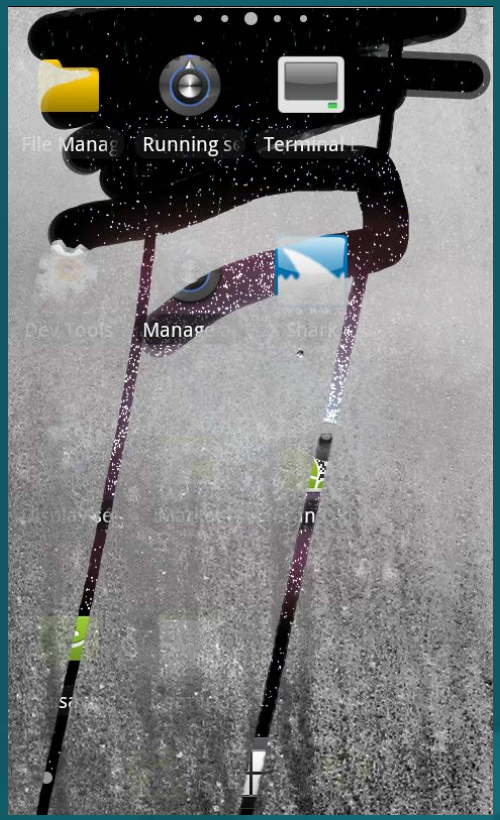
Spôsob infiltrácie

Cesty a ciele malwaru

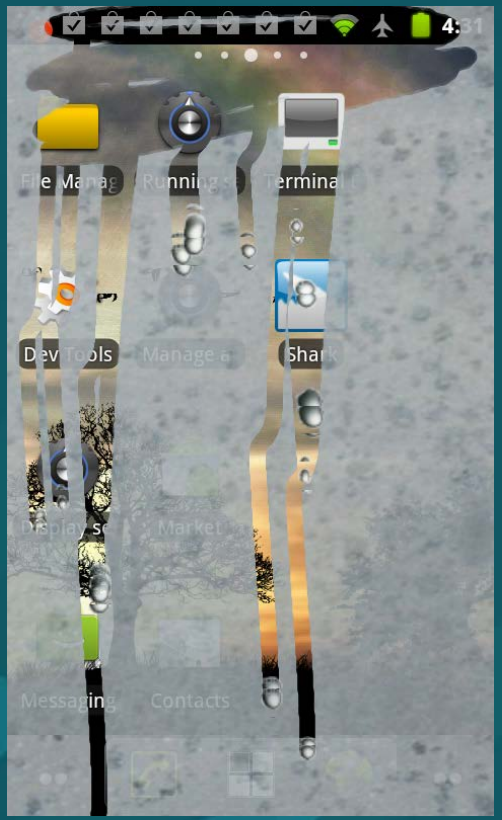
Techniky sociálneho inžinierstva

- napríklad napodobňovanie známych aplikácií

Originál



Malware

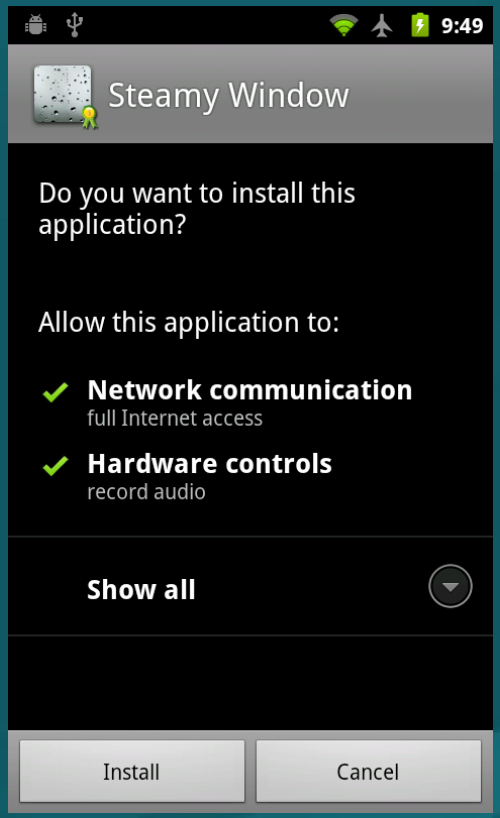


Cesty a ciele malwaru

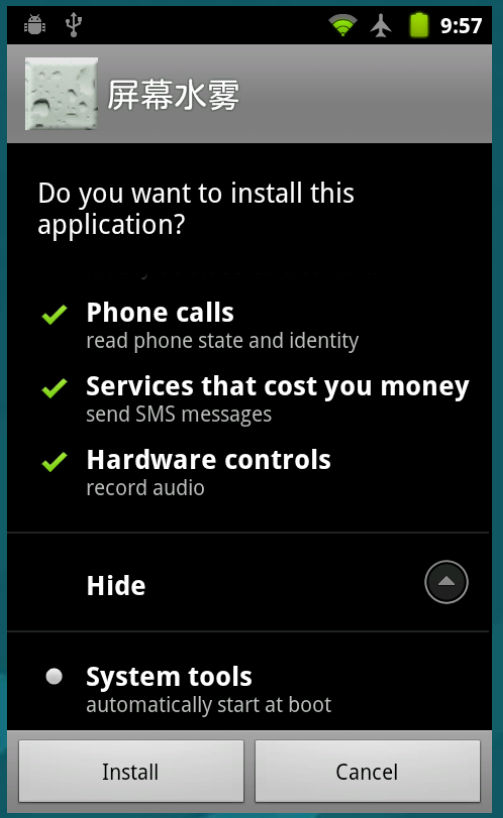
Pridelenie oprávnení

- vyžiadanie väčších právomocí

Originál



Malware



Cesty a ciele malwaru

Totožnosť developera v každej aplikácii

- zneužitie identity

Prístup na internet

- únik citlivých dát

Spoplatnené služby mobilných operátorov

- neoprávnené obohacovanie sa

Android malware

2013 Q3 evidujeme

- 250+ rodín malwaru
- ~1250 odlišných variantov

Year of mobile malware

Kategórie a typy Android malwaru

Trojan, Backdoor, Downloader, Dropper

Adware

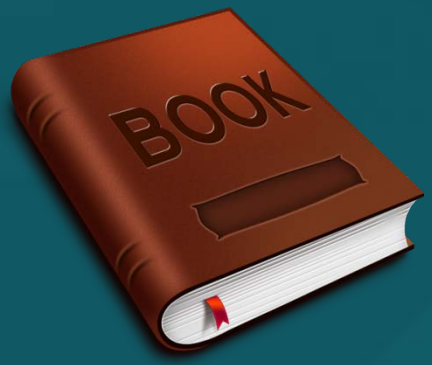
TrojanSMS

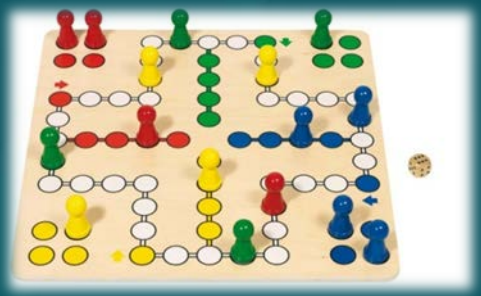
Spyware

Ransomware

Exploits

Ads





Ads

Analýza

Aplikácie (5 chýb)

Systémové zložky (3 chyby)

Tie ohrozuje treba riešiť

NA STIAHNUTIE

Ads

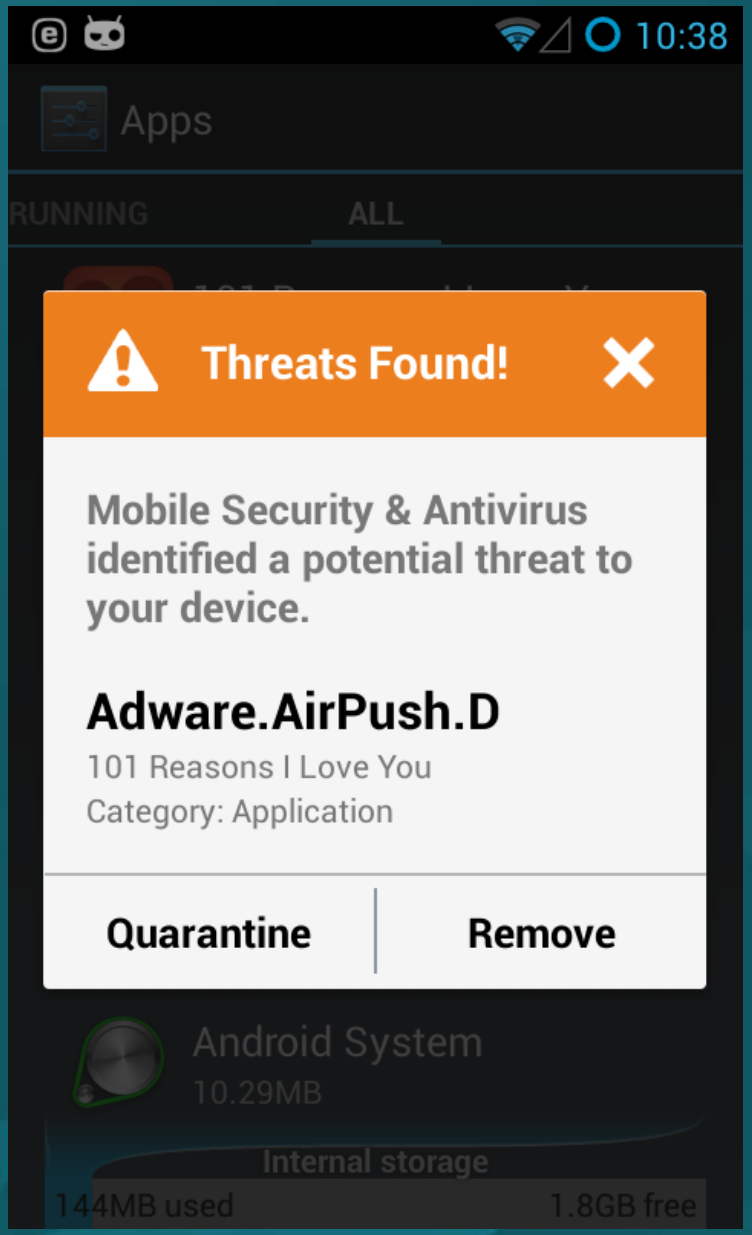
People

Google Play

Mobile Ads

Business

Adware


10:38
Apps
RUNNING
ALL
Threats Found!
Mobile Security & Antivirus identified a potential threat to your device.
Adware.AirPush.D
101 Reasons I Love You
Category: Application
Quarantine
Remove
Android System
10.29MB
Internal storage
144MB used
1.8GB free

Adware

Android/Adware.Waps

- Zobrazovanie nevyžiadanej reklamy
- Odosiela informácie na vzdialený počítač
  - IMEI / IMSI číslo
  - MAC adresu
  - Názov, typ a verziu zariadenia
  - Telefónne číslo
  - Polohu používateľa

TrojanSMS

Android/FakePlayer

- Prvý Android **SMS trójsky kôň**
- August 2010
- Rozšírený prevažne v Rusku

- Využíva bežné triky sociálneho inžinierstva
  - Prezentuje sa ako codec/media prehrávač

- Odosiela SMS správy na spoplatnené čísla

Spyware

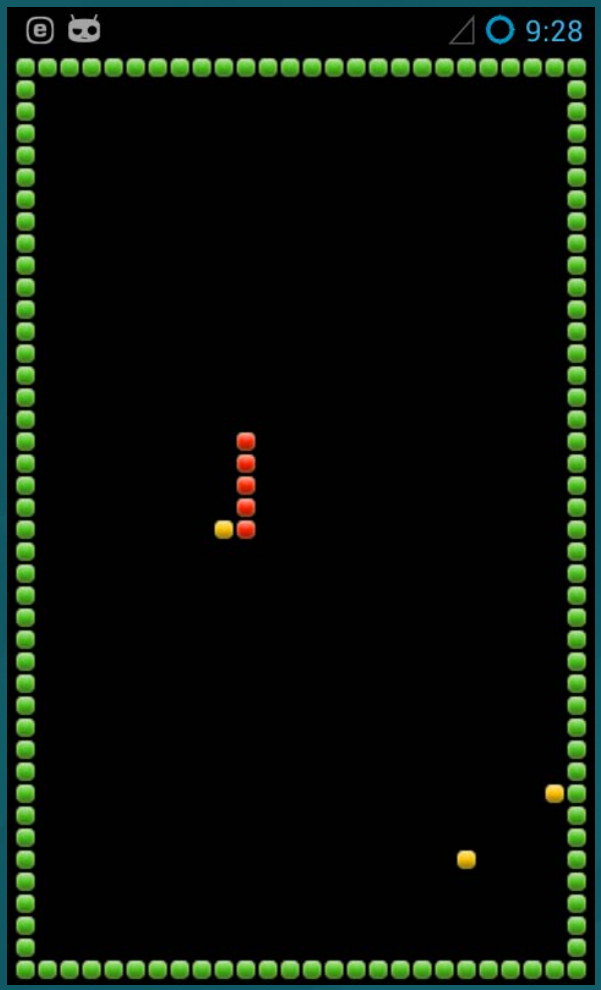
Utajené sledovanie sa zameriava na:

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

Spyware

Android/Spy.GPSpy.A

- Musí byť manuálne nainštalovaný – sociálne inžinierstvo
- Zisťuje polohu používateľa
- Zhromaždené informácie odosiela na vzdialený počítač



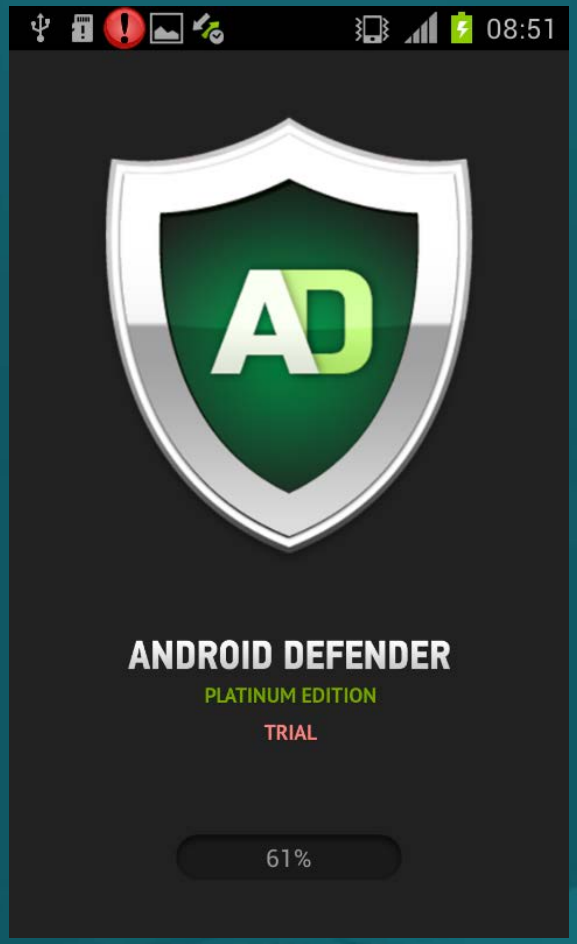
Ransomware

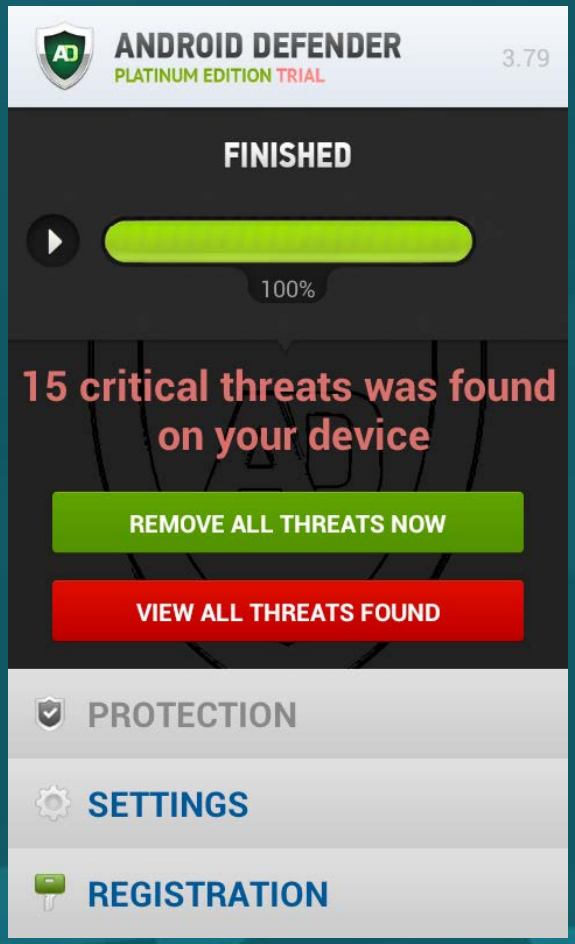
Android/FakeAV

- Prvý Android ransomware, vydieranie
- Jún 2013
- Tvári sa ako AV
- Pokúša sa získať administrátorské práva k zariadeniu
- Snaží sa získať od používateľa informácie o platobnej karte
- Agresívne blokuje mobilné zariadenie

Ransomware

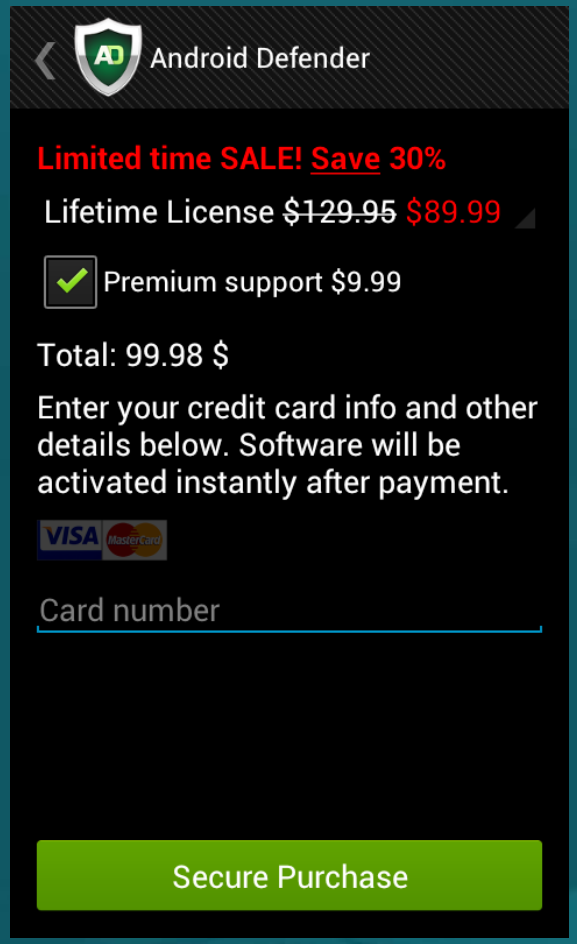
Android/FakeAV

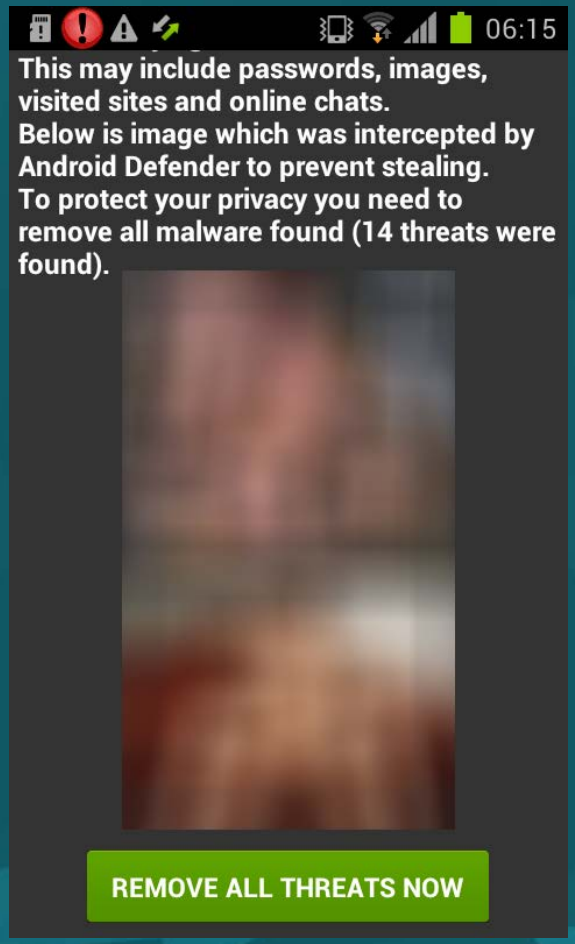




Ransomware

Android/FakeAV





Exploits

@Trojan.Android/Exploit.CVE-2013-4787.A

- Bug 8219321 & Bug 9695860
- Oficiálny patch 10 júla 2013
- Zneužitie „Android Master Key“
- 99% Android zariadení
  - Od verzie 1.6 Android Donut

Novinky

NFC - Near field communication

Bezdotykové načítanie informácií o platobnej karte

NFC - Near field communication

Najčastejší Android malware

1
Zneužitie platených služieb

2
Únik citlivých dát

3
Agresívna reklama

Zneužitie USSD

Štyri podmienky pre zneužitie USSD

1. Automatická realizácia USSD kódu
2. Existencia Factory Reset kódu
3. Android pracuje so schémou 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>
```

Zneužitie USSD

Sieťové útoky

INTERNET

Sieťové útoky

INTERNET

3G

Sieťové útoky

Zraniteľnosti sieťovej komunikácie

- Nie každá bezdrôtová sieť je čestná a nezištná
- Útočník vytvorí, sleduje a modifikuje sieťovú komunikáciu
- K útokom sú vhodné aj voľné bezdrôtové siete vo verejných priestoroch
- Útok kdekoľvek a kedykoľvek
  - Dopyt po internete
  - Vhodný názov siete

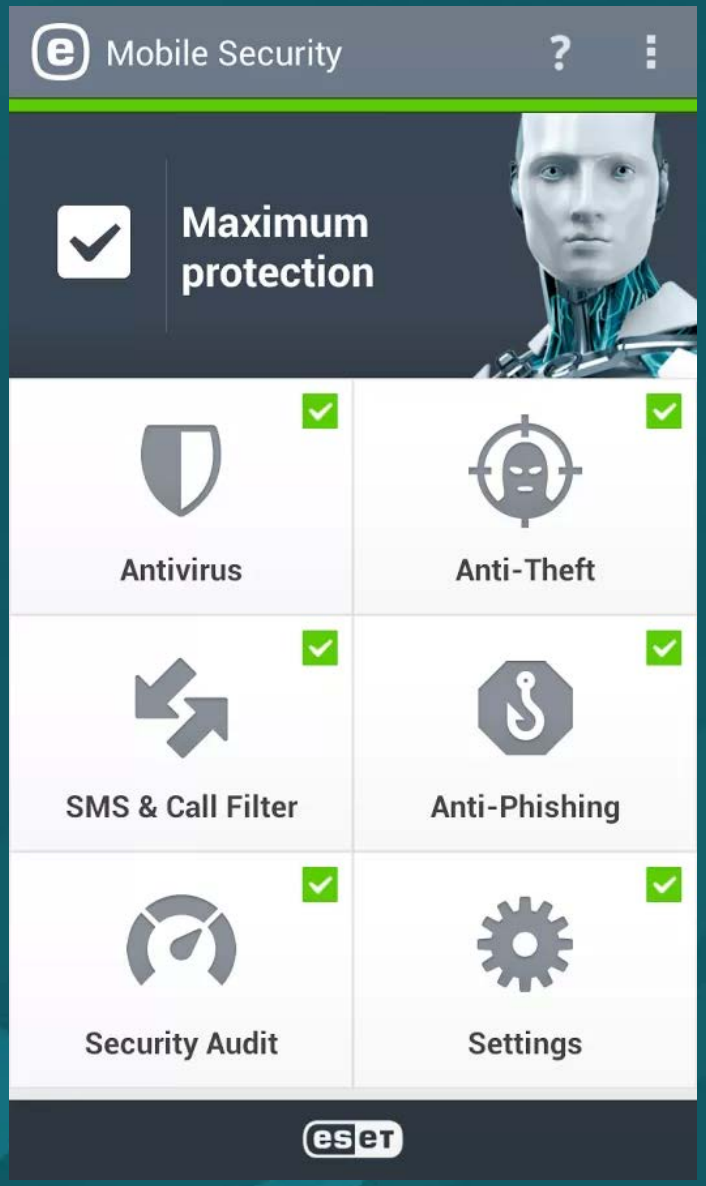
Sieťové útoky

Prevencia

- Využívať šifrovacie protokoly (SSL)
- Host to host šifrovanie (L2TP/IPsec)
- Subnetting

ESET Mobile Security

- Dostupné cez Google Play
- Skontrolujte si bezplatne svoje zariadenie



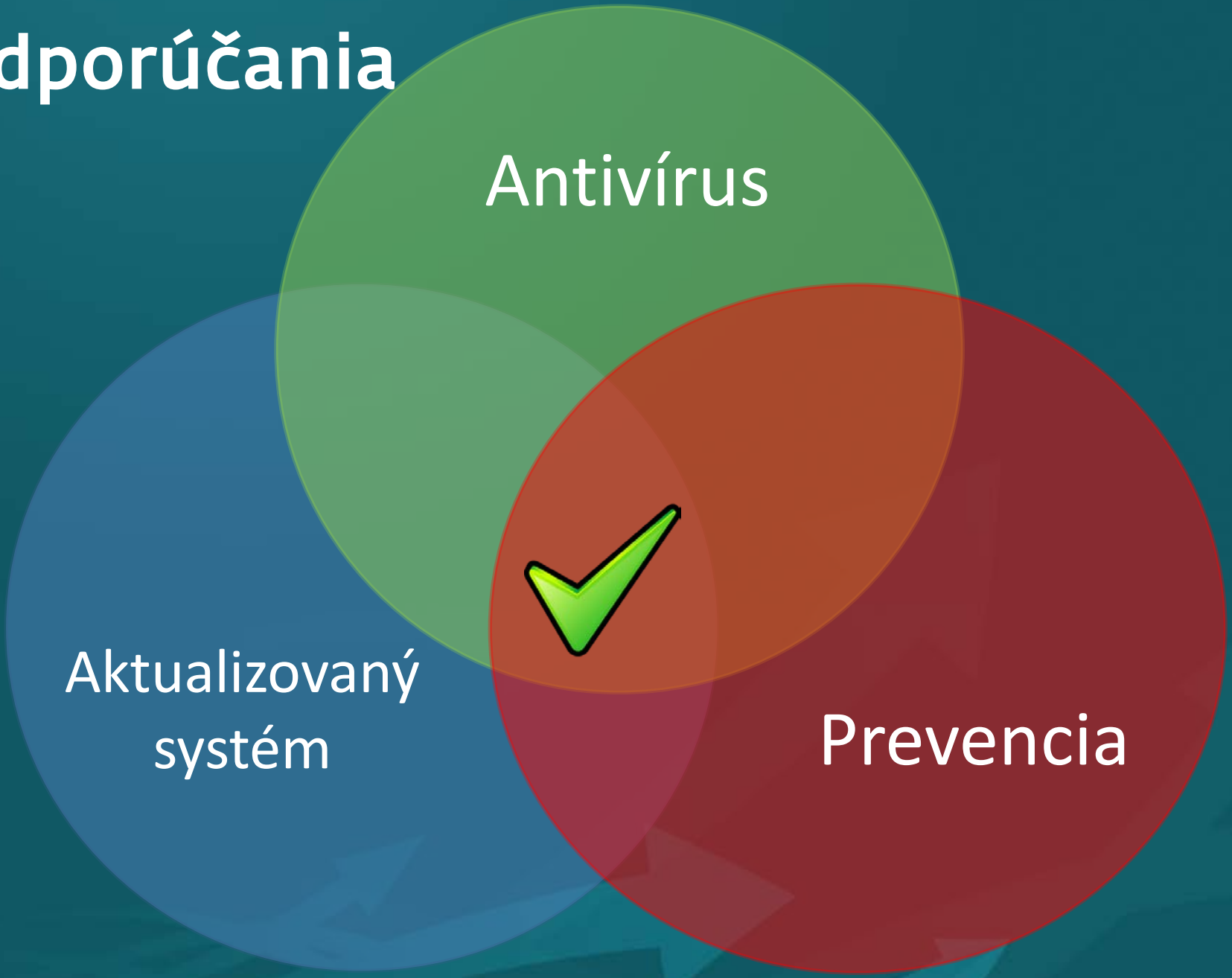
Odporúčania

- Používať „silné“ heslá
- Šifrovať dáta
- Pripájať sa len na dôveryhodné zdroje internetu
- Šifrovať komunikáciu (internet, SMS)
- Voliť aplikácie od známych vývojárov
- Preferovať najsťahovanejšie s vysokým hodnotením

Odporúčania

- Uprednostňovať oficiálny market
- Prehodnotiť požadované práva pri inštalácií aplikácie
- Vyhnúť sa inštalácii aplikácií z neznámych zdrojov
- Udržiavať software aktualizovaný
- Nainštalovať mobilný antivírus

Odporúčania



Ďakujem...

branisa@eset.sk