Valódi veszélyt jelentenek a mobil kártevők?

Szappanos Gábor

Principal researcher

SOPHOS

SOPHOS

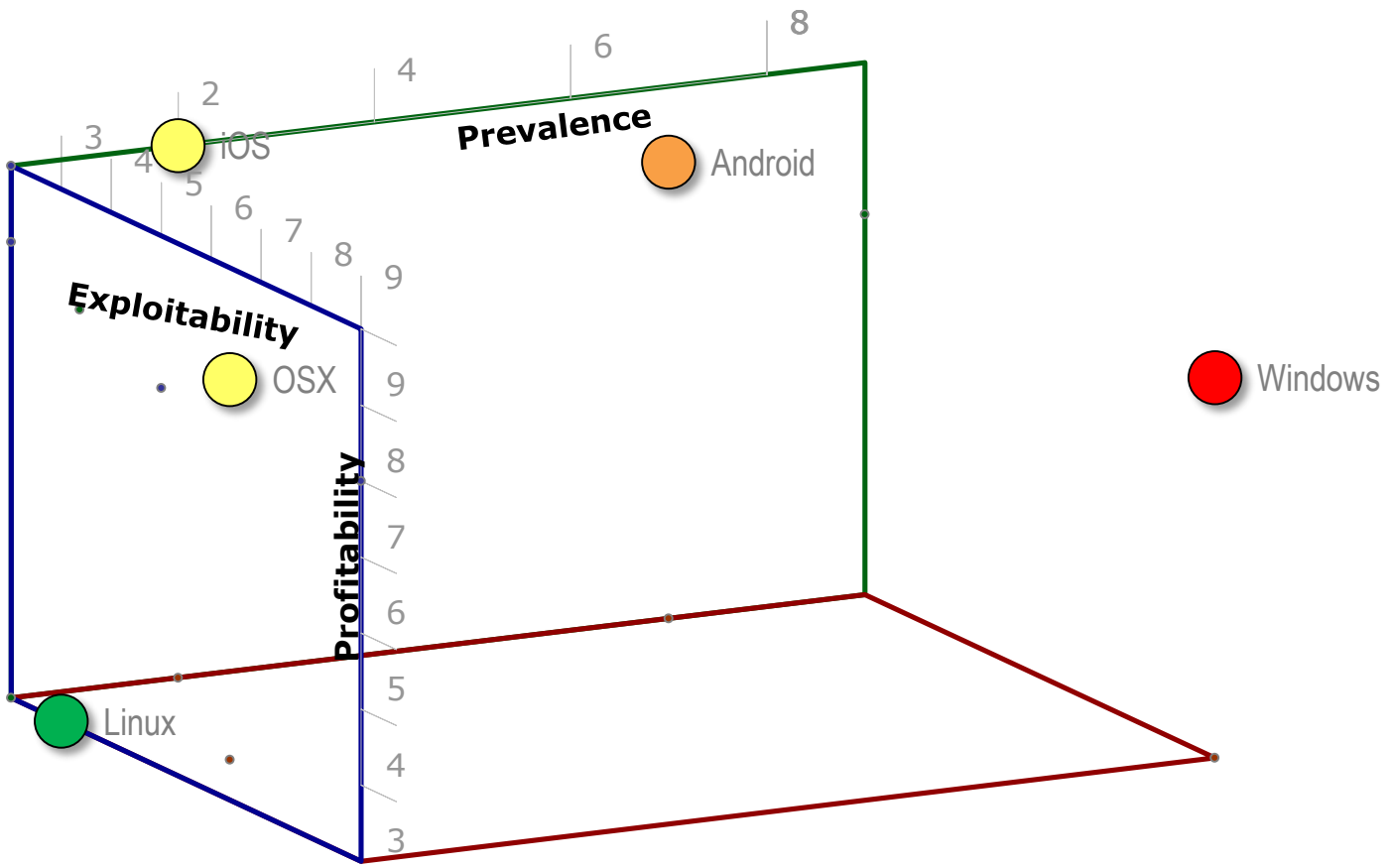
Van-e élet a Windows után?

Mi lesz a következő célpont?

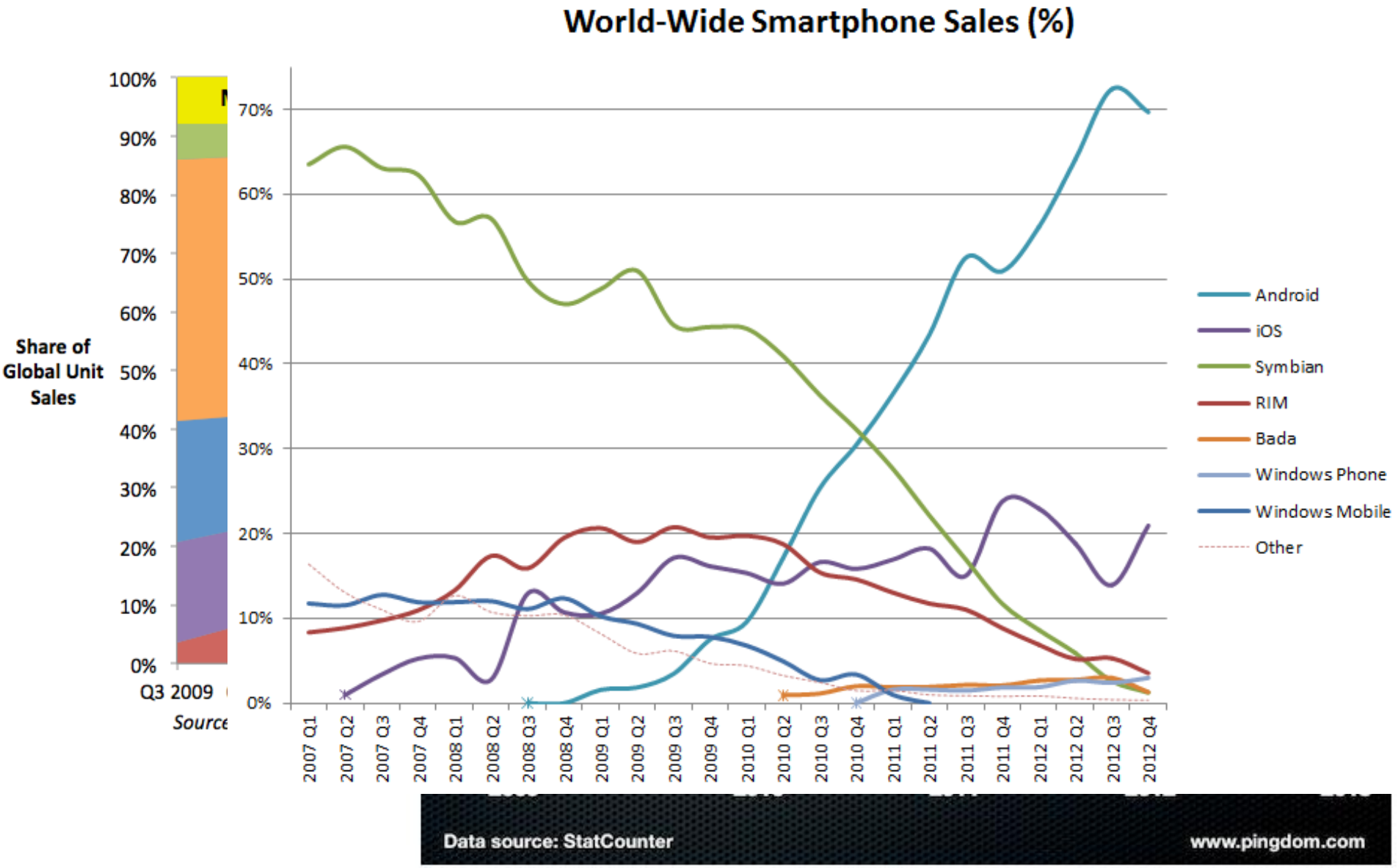
- Linux?
- Symbian?
- OSX?
- iOS?
- Android?

> “Over 100 million Android phones shipped in the second quarter of 2012 alone. In the U.S., a September 2012 survey of smartphone users gave Android a whopping 52.2% market share. Targets this large are difficult for malware authors to resist. And they aren’t resisting—attacks against Android are increasing rapidly.”

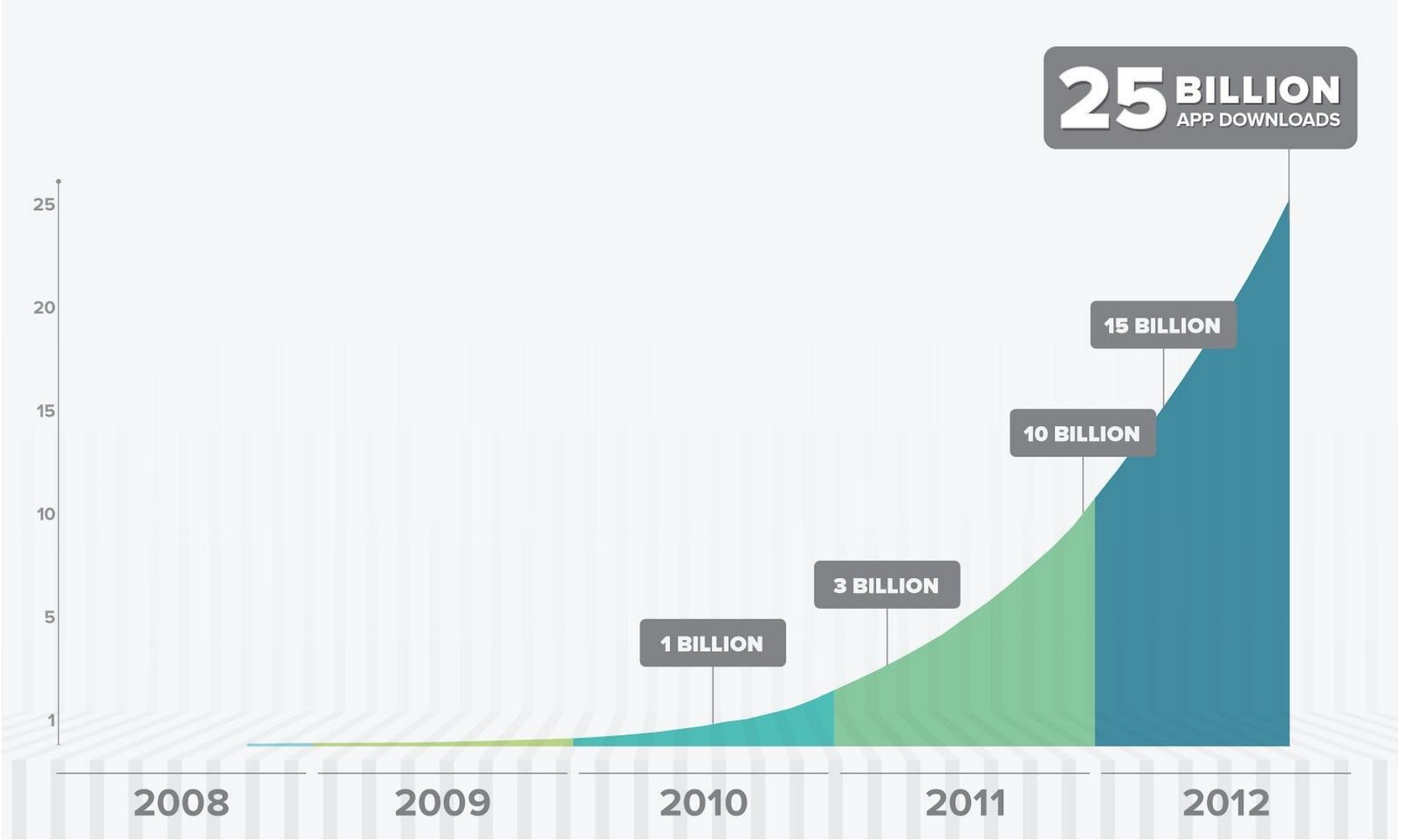
Sophos 2013 Security Threat Report


Prevalence
2
3
4
5
6
8
iOS
Android
Exploitability
6
7
8
9
OSX
Profitability
9
8
7
6
5
4
3
Linux
Windows

Mobil OS piac megoszlása



Android alkalmazás letöltések



Marketplace-en terjesztett kártevők

Fake Apple apps appear on Android

nakedse

Award-winning news, opinion, advice and r

malware mac facebook android vulne

How internet revenge by an ex-partn...

Angry Birds malware - for profiting from fake

Join thousands of others, and sign up for Na

you@example.com

by Graham Cluley on May 24, 2012 | 2 Comments

FILED UNDER: Android, Law & order, Malware, Mobile

A firm has been fined £50,000 after Trojan versions of popular Android apps secretly expensive SMS messages to premium rat numbers.

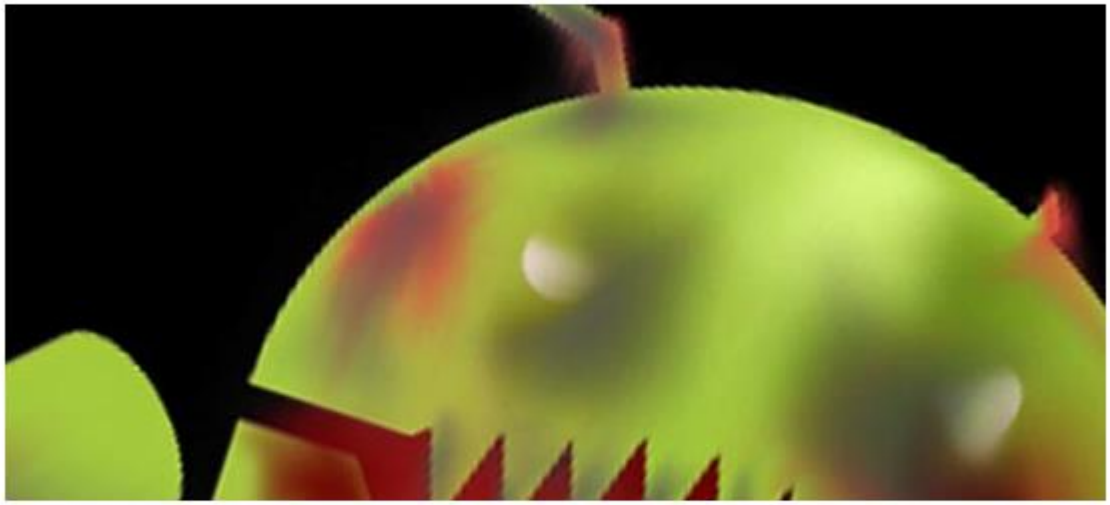
UK industry regulator PhonepayPlus unco that 1,391 mobile phone numbers in the U been stung by the scam, that targeted And owners who downloaded Trojan horse ver of popular games such as "Angry Birds", "Assassins Creed" and "Cut the Rope".

Family of "BadNews" malware in Google Play downloaded up to 9 million times

Apps steal sensitive data, push SMS app that racks up charges to pricey service.

by **Dan Goodin** - Apr 20 2013, 5:21pm CEDT

ANDROID BLACK HAT 96



greyweed

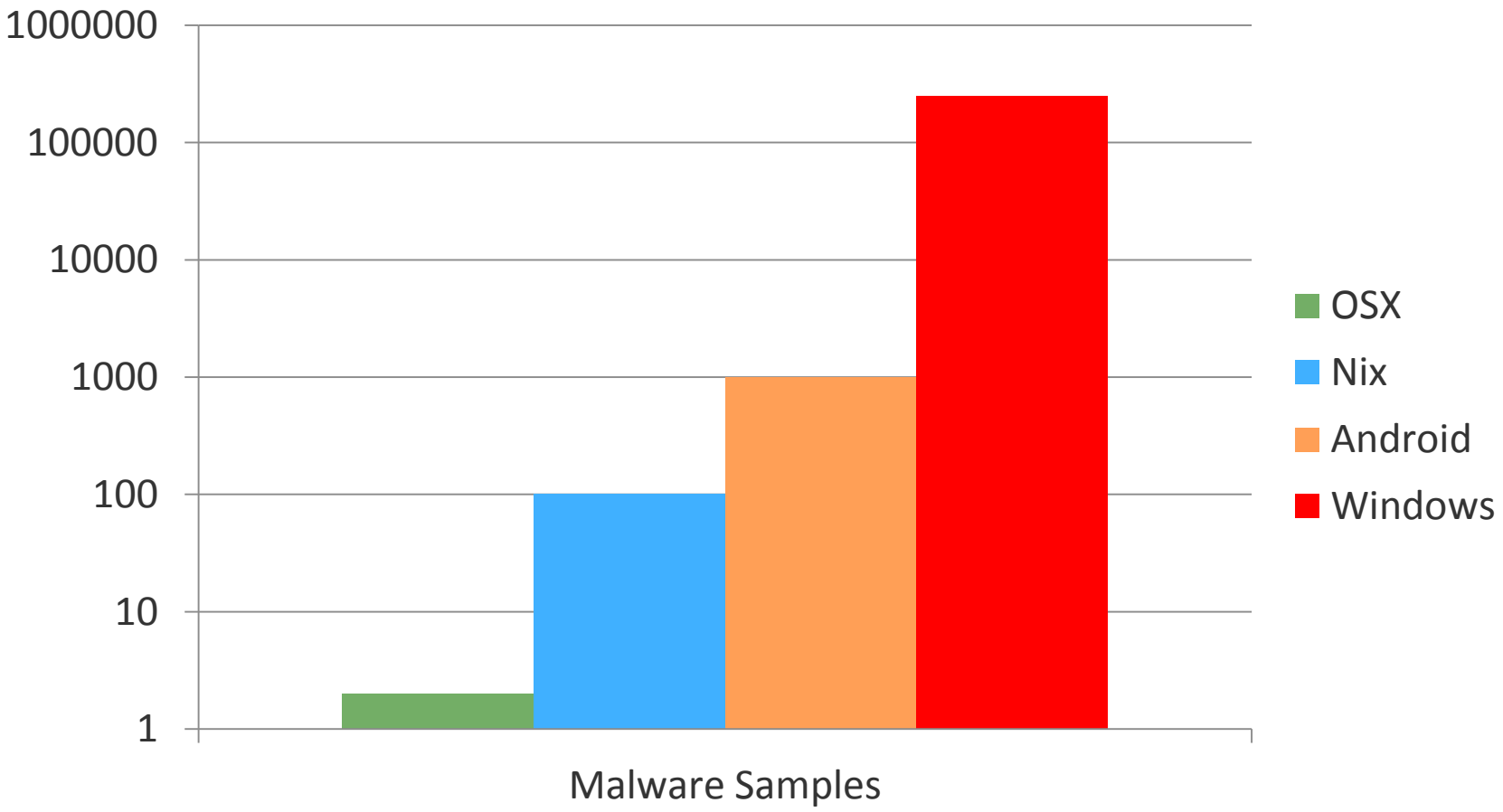
Security researchers have unearthed a family of malware for Android-based smartphones that has been downloaded as many as 9 million times from Google Play, the official distribution platform hosted on Google servers.

Garage Band

iP

Android kártevők

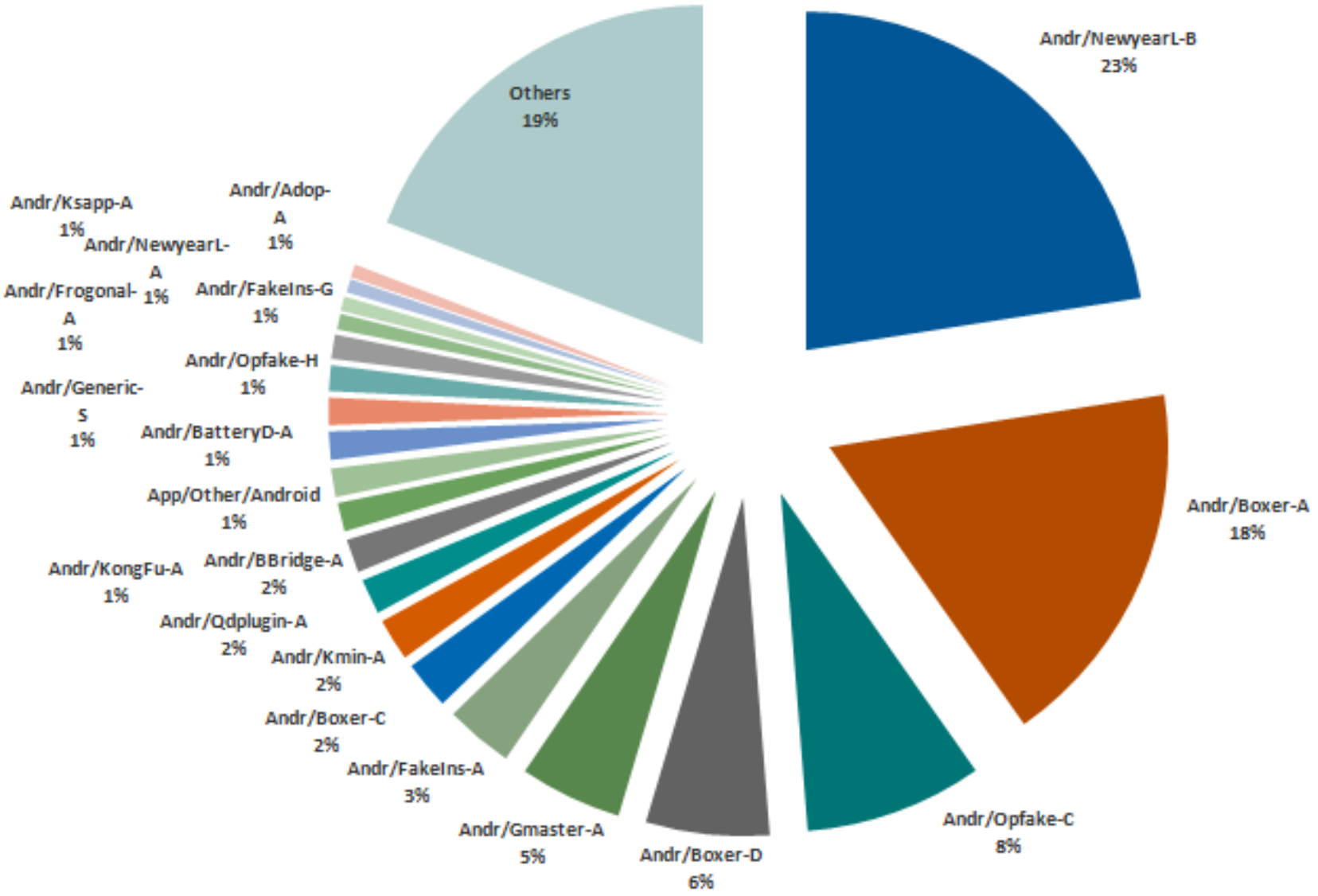
Beérkező kártevők naponta, platformonként



SOPHOS

Aktuális kártevők

Android incidensek ItW



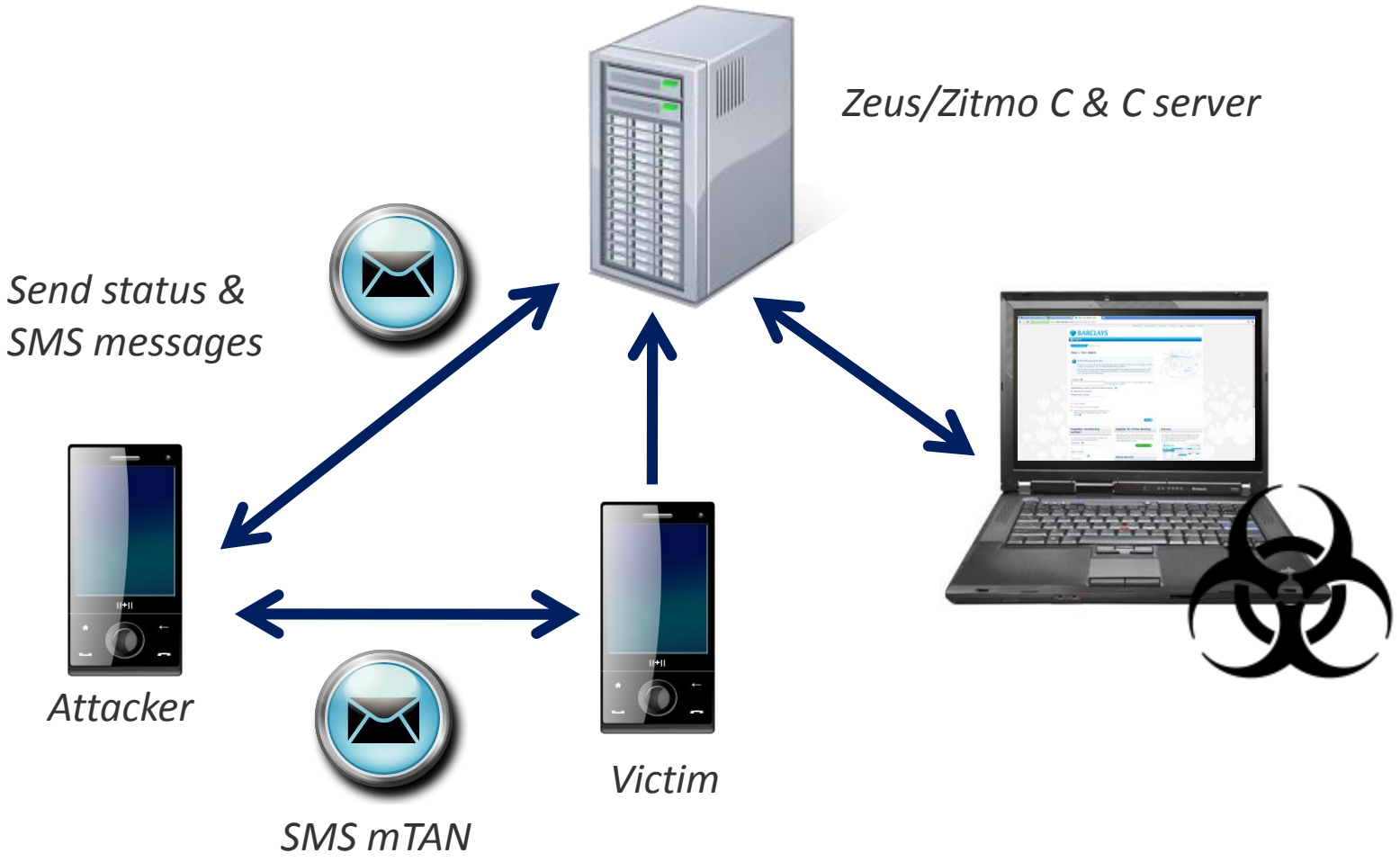
Kártevők motivációja

- Hol van a pénz? (pornó, drogok, bankok)
  - Banki információk lopása
  - Emelt díjas SMS küldés
  - Kéretlen reklám

Andr/Zitmo

- A Zeus/Zbot trójai kiegészítő komponense
- Telepítés social engineering révén
- A tranzakció a fertőzött PC-ről indul
- Egyedi tranzakciós jelszavakat tartalmazó SMS-eket figyeli, jelszót kigyűjti, továbbküldi a támadónak

Zitmo működés



Andr/Boxer

- Leggyakoribb család, az összes kártevő 1/3-a idetartozik
- Ukrajnában levő .ru domaineken terjesztik
- Célpontja Kelet-Európa
- Social engineering – kamu update-eket kínálnak (Opera, Skype) v. Fake AV fut le, és telepítést javasol
- Telepítés után emeltdíjas SMS-eket küld ki
- Kelet-Európára koncentrál (kooperatív SMS operátorok)
- INSTALL_PACKAGES jogosultággal települ, lehetővé teszi további komponensek telepítését

Andr/Boxer


update center
Обновление брау
ВНИМАНИЕ! Реком
браузера до верси
Ваша версия брауз
дальнейшая работа
некорректной и пр
ошибкам и сбоям!
Рекомендуем Вам
СКАЧАТ
Обнови свой бра
FREE
3:06
http://googleapi17.ru/l....
Anit-
Обновлено: 15-05-2012
Количество вирусов в базе: 33473
Проверок за день: 2452
Начать проверку
Возможно ваш телефон заражен и кто-то имеет доступ к вашим личным данным, таким как фото, сообщения, история звонков, контакты, история посещенных сайтов, пароли к сайтам и другое. Срочно начните проверку на вирусы!
100% гарантия защиты телефона
Проверка на вирусы
Проверка SIM вирусов:
Проверка Хранилища:
Проверка Сообщений:
Проверка Звонков:
Проверка приложений:
Проверка истории Браузера:
3:07
http://googleapi17.ru/l....
Anit-
Обновлено: 15-05-2012
Количество вирусов в базе: 33473
Проверок за день: 2452
Начать проверку
Возможно ваш телефон заражен и кто-то имеет доступ к вашим личным данным, таким как фото, сообщения, история звонков, контакты, история посещенных сайтов, пароли к сайтам и другое. Срочно начните проверку на вирусы!
100% гарантия защиты телефона
Проверка на вирусы
Проверка SIM вирусов:
Угроз не обнаружено
Проверка Хранилища:
Обнаружены угрозы! Обнаружены зараженные файлы(57)
Проверка Сообщений:
Проверка Звонков:
Android
М ДЛЯ

SOPHOS

Vírusvédelmek, tesztek

Kihívások a vírusvédelmek előtt

- Túl sok platform (Android, iOS, Windows, Blackberry, Symbian) és túl sok eszköz (telefon, tablet, TV,...) támogatása szükséges
- Kevés a memória
- Új processzor architektúrára kell portolni az engine-t, vagy új engine-t kell írni
- Hálózati kapcsolat (cloud lookup, frissítés) drága lehet

De ezeket a kezdeti problémákat a többség már leküzdötte.

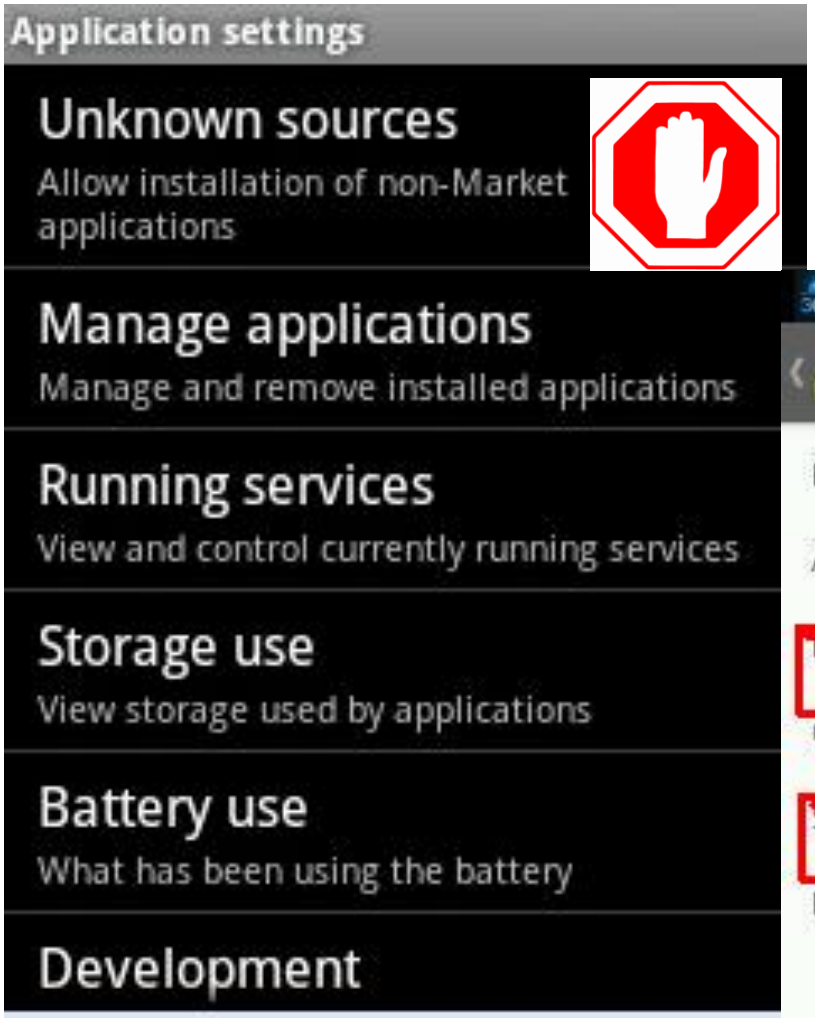
Mobil védelmi termékek tesztelése - AMTSO ajánlások

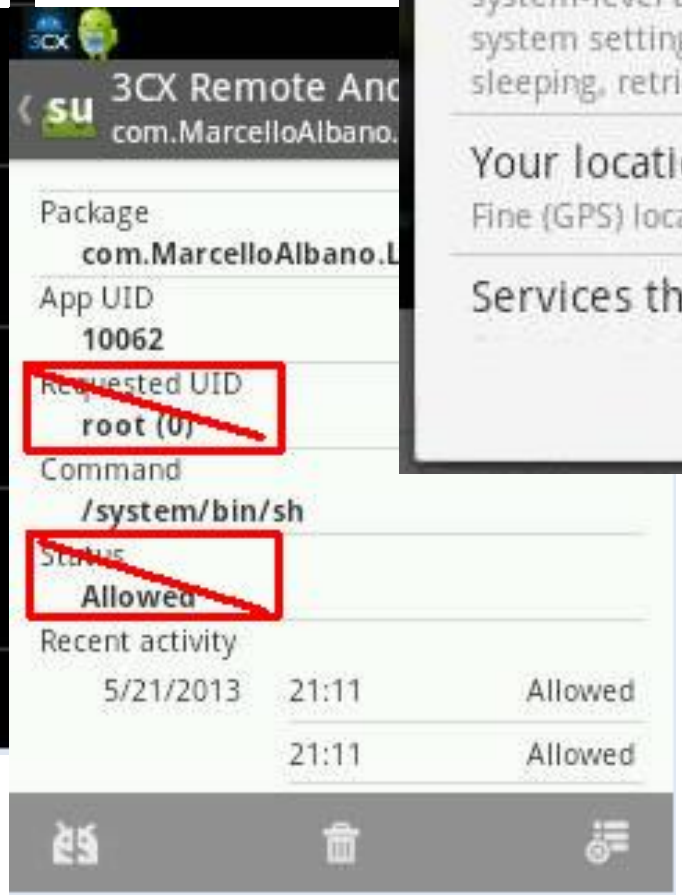
- Túl sok platform (Android, iOS, Windows, Blackberry, Symbian) és túl sok eszköz (telefon, tablet, TV,...), emuláció nehézkes
- Mobil teszt = Android teszt
- De még így is nagy a különbség az egyes mobilgyártók által adott Android telepítések között
- 3rd party marketplace-ek engedélyezése?
- Performancia (akkumulátor használat) fontos – néhány AV leáll, ha alacsony a töltés
- Sávszélesség fontos – néhány AV leáll, vagy csökkent értékű, ha nincs szélessávú elérés

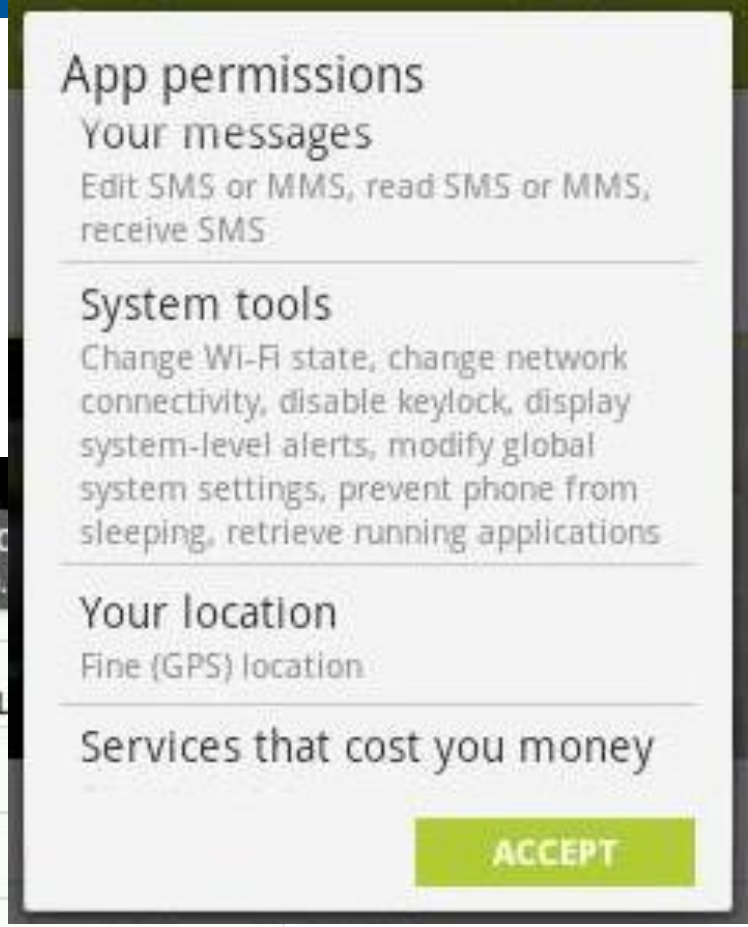
Összehasonlító tesztek

Independent Tests of
Anti-Virus Software

Első lépések a biztonság felé







Mit tegyenek a rendszergazdák?

- Biztonsági szabályozás kiterjesztése mobil eszközökre
- Rootolt eszközök kitiltása a hálózatból
- Eszköz titkotítása, lopás esetén távoli törlés biztosítása
- Automatikus redszerfrissítések
- Csak a hivatalos (Google, telefongyártó) marketplace-ek engedélyezése (ez sem 100%-os, de sokkal biztonságosabb)
- Social engineering kivédése, telepítéskori jogosultságok átvizsgálása
- Vírusvédelem telepítése

Kérdések?

SOPHOS