UNICORN COLLEGE

Bezpečnost ve světě mobilních zařízení a aplikací

UNICORN COLLEGE OPEN

8. listopadu 2013

Marian Bartl

Marian Bartl

- Unicorn Systems, Production Manager, 2013
- Unicorn Systems, Operation Architect, 2012
- Unicorn 2012
  - Projektové řízení
  - IT Security
  - Infrastruktura

Agenda

- Úvod do problematiky
- Hrozby vs. platformy
- Mobilní hrozby a jejich rozdělení
- Odcizení zařízení
- Trojské koně a jejich varianty
- SMS hrozby
- Riskware - skutečná hrozba ?
- Pohled do budoucnosti

Bezpečnost ve světě mobilních zařízení a aplikací

UNICORN COLLEGE OPEN

Úvod do problematiky

- Počet aktivních SIM v ČR – cca. **13,5 mil.**
- Celosvětově počet zařízení prudce narůstá
- Počet zařízení v ČR „stagnuje“, přenos dat však dynamicky roste
- Online 24/7
- Nezávislost na lokalitě
- Penetrace mobilních zařízení

	2011	2012	2013	2014	2015
Smartphony	12,3	35,5	46,6	56,5	71,7
Tablety	2,9	4,7	7,2	10,0	13,0

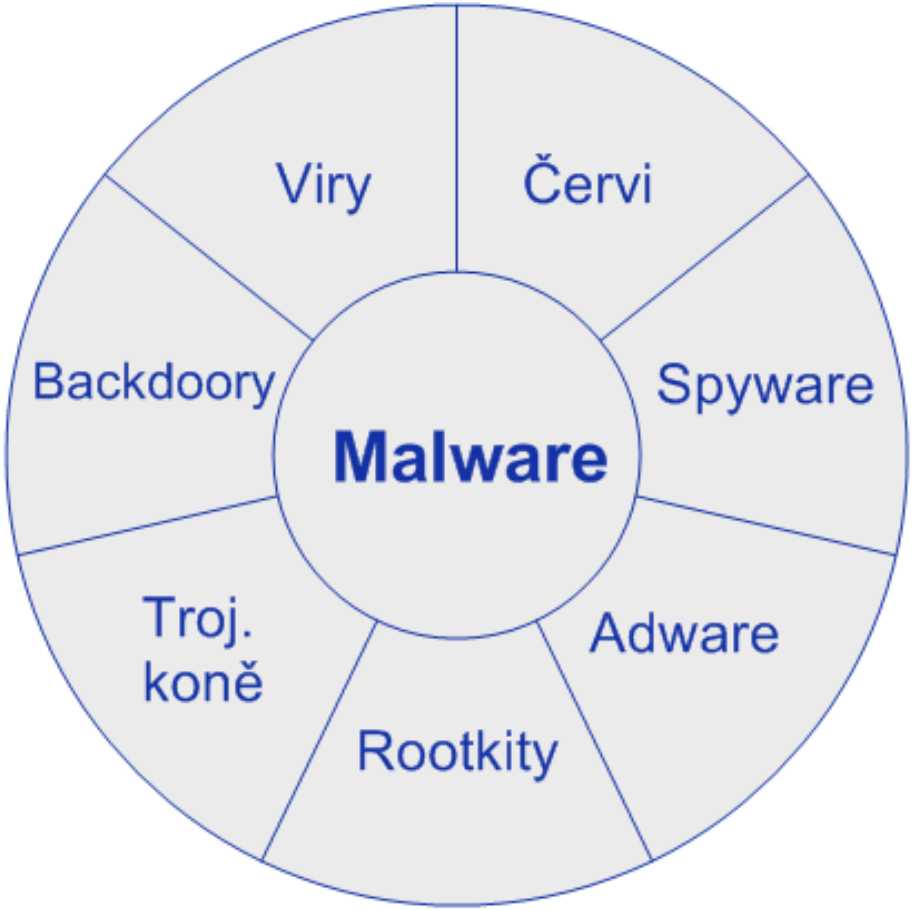
zdroj: www.mediaguru.cz

Úvod do problematiky

- **Důvěra**
- Díky stále rychlejším datovým přenosům a výkonnosti zařízení se tvůrcům malware **„vyplatí“ se zaměřit na mobilní platformy**
- V roce 2011 vzrostl počet malware o 177 %
- V období od března 2012 do března 2013 o **614 %**
- Stále sofistikovanější hrozby
- Hlavní motivací je zisk – cca. **75%** hrozeb je motivováno **ziskem**

Úvod do problematiky

- Malware = obecné označení pro škodlivý kód
  - Zahrnuje



Hrozby vs. platformy

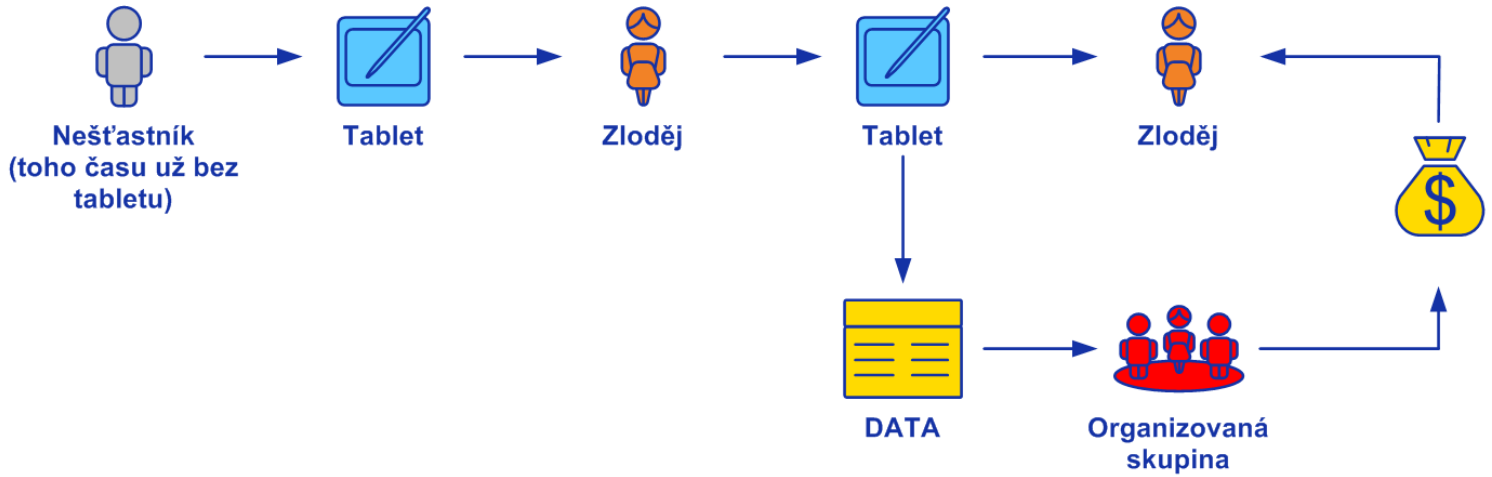
- Android
  - 92% veškerého malware
  - Pouze cca 5% zařízení má poslední verzi OS Android
- Apple iOS
  - Hrozby existují, ale nejsou zveřejňovány
  - Pro tvůrce škodlivého kódu v masivním měřítku je platforma „nezajímavá“
- Windows Phone a ostatní
  - Malé procento trhu

Mobilní hrozby a jejich rozdělení

- Odcizení zařízení
- Trojan
  - Trojan – umožňuje provádění „nechtěných“ akcí
  - Trojan-spy – sbírá data, hesla...
- Monitoring tool
- Riskware
- Adware+spyware
- Hack-tool
- Command & Controll servery

Odcizení zařízení

- Ztráta citlivých dat



- Možnost vzdáleného vyhledání a smazání zařízení
  - Sociální inženýrství – výmaz účtu neoprávněnou osobou

Trojské koně a jejich varianty

- Trojan
  - Instaluje se na zařízení pomocí legálních aplikací
  - Slouží k provedení uživatelem nevyžádaných akcí
- Trojan-spy
  - Sbírá uživatelská data
    - hesla
    - kontaktní údaje
- SMS-Trojan
  - Nenápadné odesílání „premium SMS“ útočníkům

Riskware - skutečná hrozba?

- Je legitimní SW ale má kritické funkcionality
- Malware jej může využít pro dostupnost ke kritickým funkčnostem
- Například:
  - Vzdálená správa
  - IRC klienti

Pohled do budoucnosti

- Vzestup využívání „soukromých“ mobilních zařízení ke zpracování firemních dat
- BYOD – Bring Your Own Device
- Nové hrozby!
- Zůstane do budoucna důvěra v GSM ?

Jak se bránit

- Zálohovat data
- Šifrovat data
- Používat zařízení „s rozumem“
  - Opravdu je nutné přes pracovní telefon stahovat vtipná videa nebo hry
  - Je nezbytné mít na telefonu aplikaci „svítilna“, když si aplikace žádá o přístup do adresáře a k ovládání připojení k internetu?

Shrnutí

UNICORN COLLEGE OPEN

Shrnutí

- Zabezpečit mobilní zařízení proti hrozbám je složitější
- Přichází stále nové a nebezpečnější hrozby
- Budoucnost nevypadá růžově, ale s rozumným přístupem ji lze určitě zvládnout
- Je nutné hledat kompromis mezi cenou aktiv, použitelností a paranoidním přístupem

UNICORN
COLLEGE