INFOTA

WHERE IDEA BECOMES REALITY

gik

ORSZÁGOS GAZDASÁGINFORMATIKAI KONFERENCIA

Software vulnerablities on desktop and mobile – Social and economic effects

Horváth Attila PhD

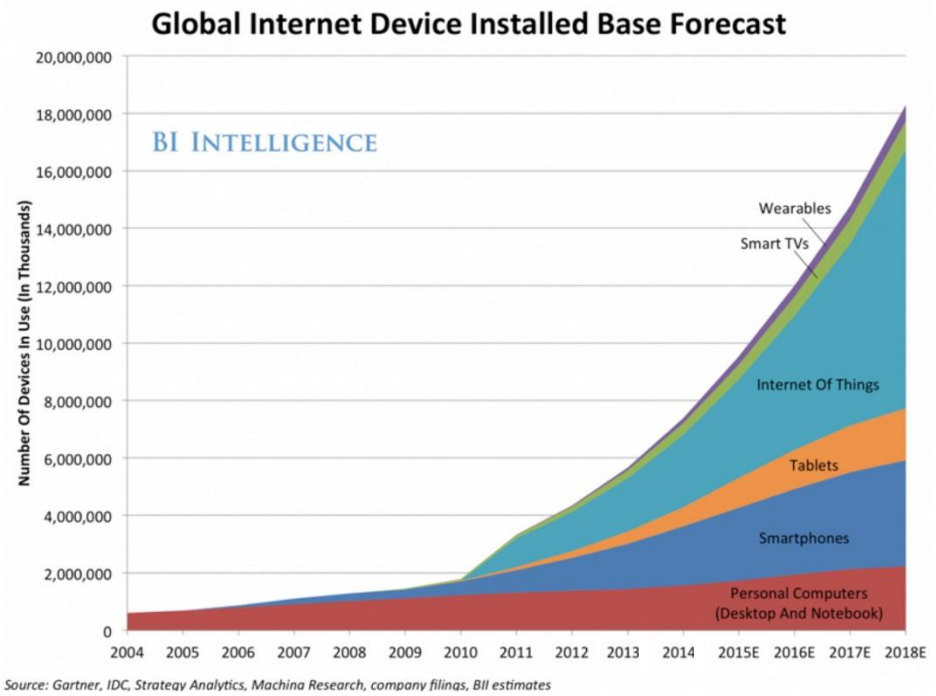
OTKA PD-109740

Summary of the project

- 2013-2016.
- Private, Corporate and Public sectors
- Software vulnerabilities
  - Monitoring since 2010
  - Over 1000 software vulnerablities analysed
  - US-Cert, NVD, CVSS, CWSS, CWE
- Financial and social effects
- Hungarian Scientific and Research Fund (OTKA)

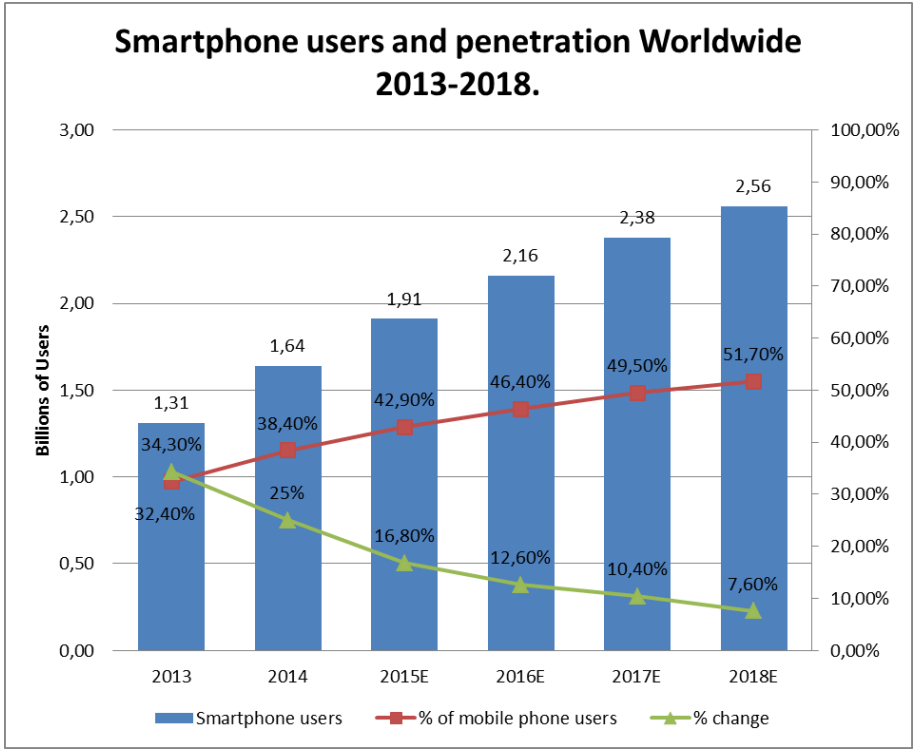
Connected devices

- 7.2 billion gadgets, multiplying five times faster than we are
- 33 billion by 2020
- Global mobile data traffic reached 2.5 exabytes (+69% y2y)
- Average of traffic per smartphone in 2014 was 819 MB (+45% y2y)
- 26% 4G → 68% traffic
- 51% video traffic

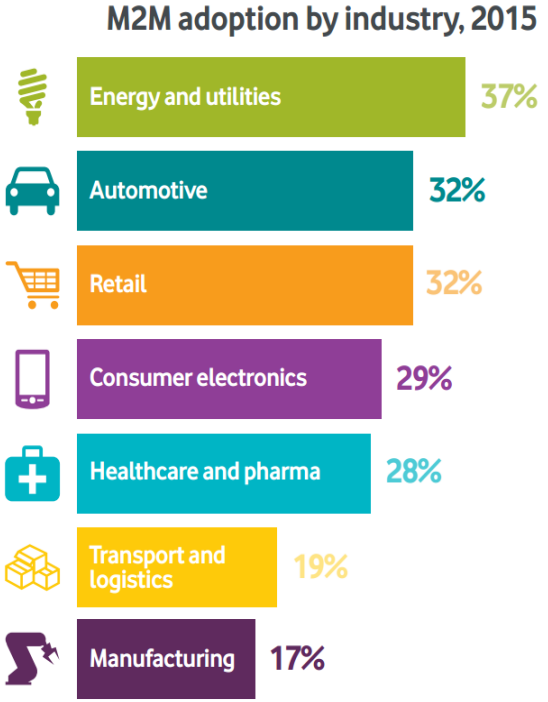


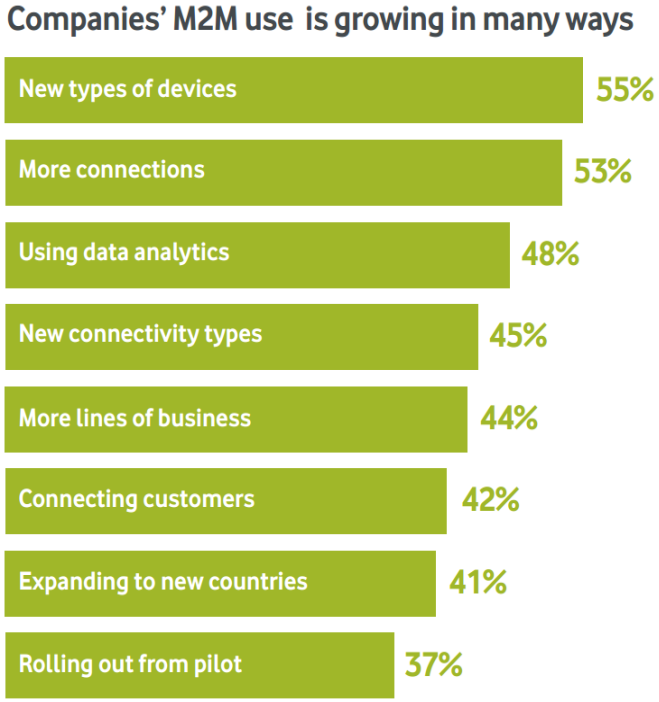
Connected users

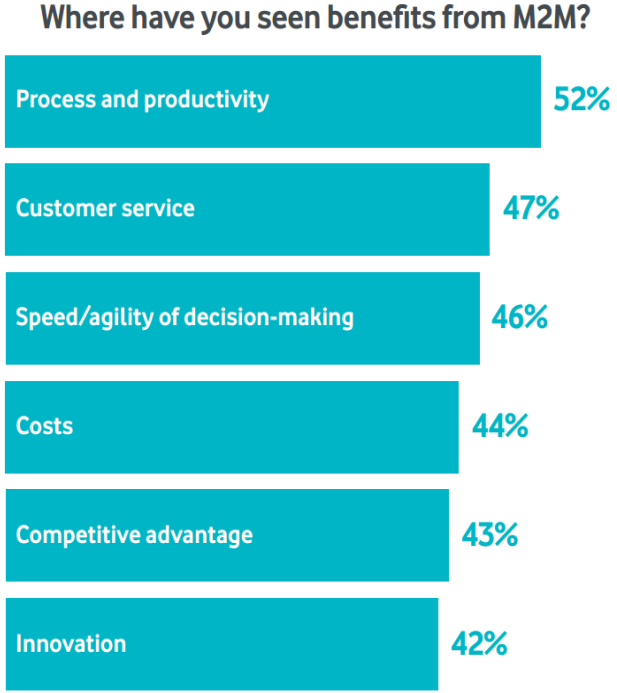
- ¼ of the global population
- China >500 million
- Russia > Japan
- India, US > 200 million
- Middle east and Africa +72%



The Internet of Things (IoT)

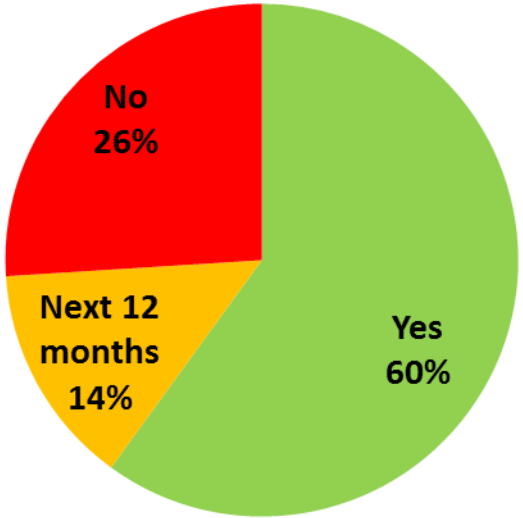




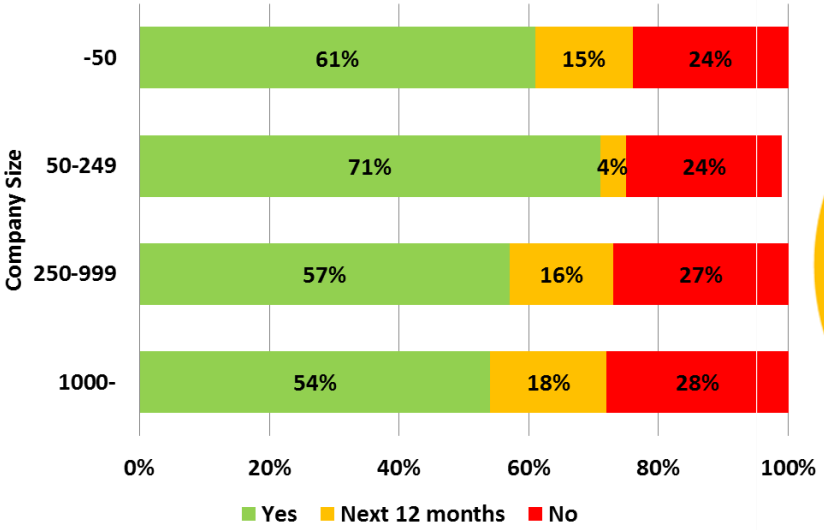


Bring Your Own Device (BYOD)

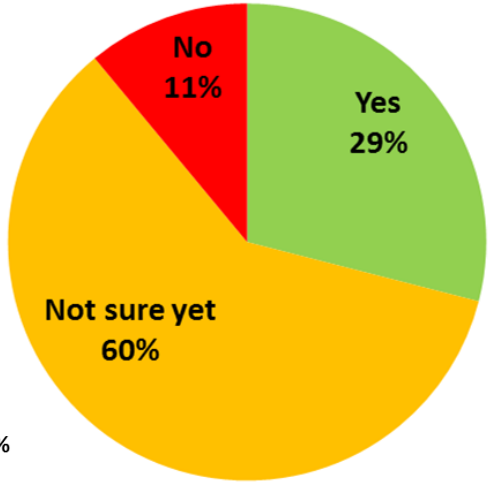
Does the company allow byod?



BYOD usage by company size



Are wearable devices part of your BYOD regulation?



Attacks already a commonplace

Devices

- IP cameras
- smart meters
- healthcare devices
- SCADA devices
- wearable devices
- smartphones/tablets

Most important security issues

- 70% contained security exposures
- 25 holes or risks of compromising the home network, on average, found for each device
- 80% did not require passwords of sufficient complexity and length
- 90% collected at least one piece of personal information
- 70% allowed an attacker to identify a valid account through account enumeration

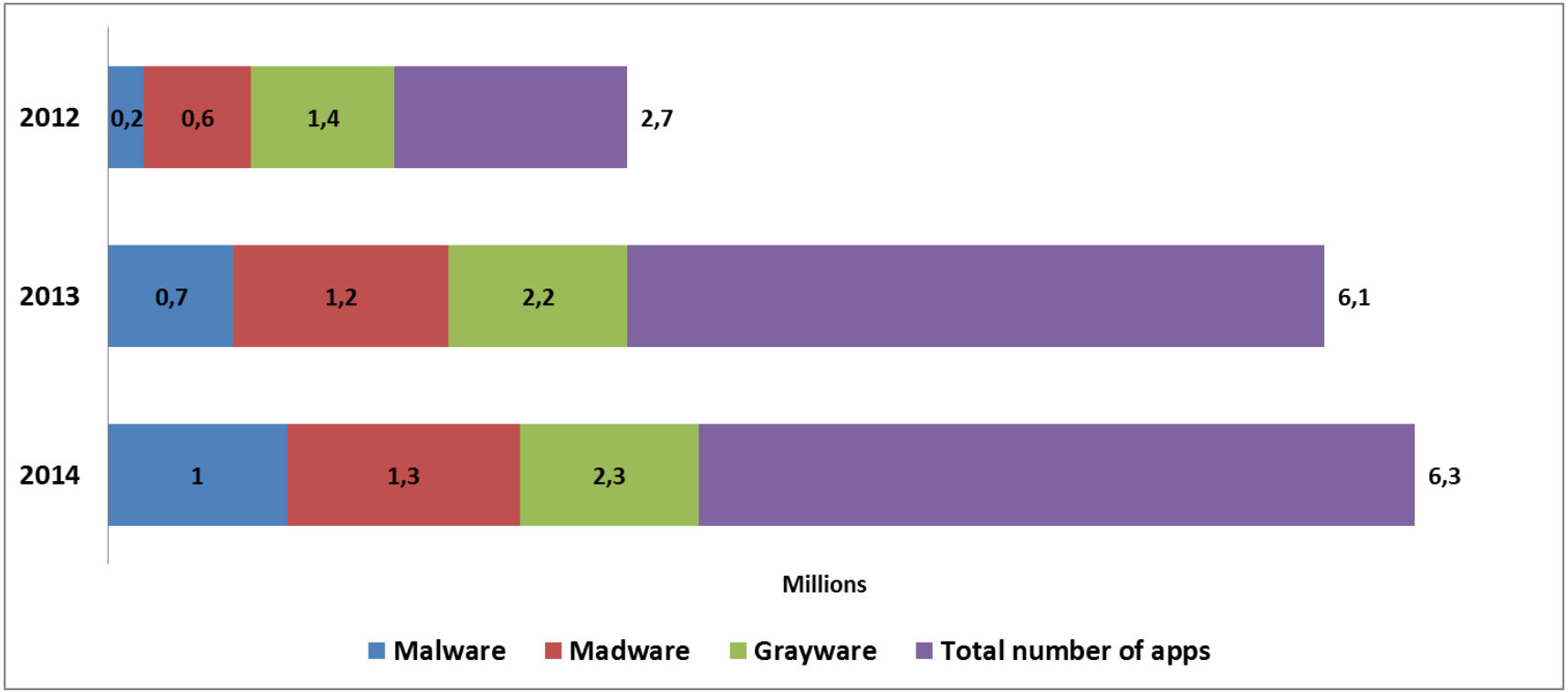
Mobile threats

- The adoption of near-field communication (NFC) for digital payments from mobile devices will likely attract cyber criminals.
- The growing availability of malware-generation kits and source code will make it easier for cybercriminals to target mobile devices.
- Dead or stale apps, which are unsupported, or simply not updated by the users any more represent a huge threat on company systems through the BYOD-philosophy.
- Over 5 million identified mobile malware in 2014, the yearly growth is over 110%

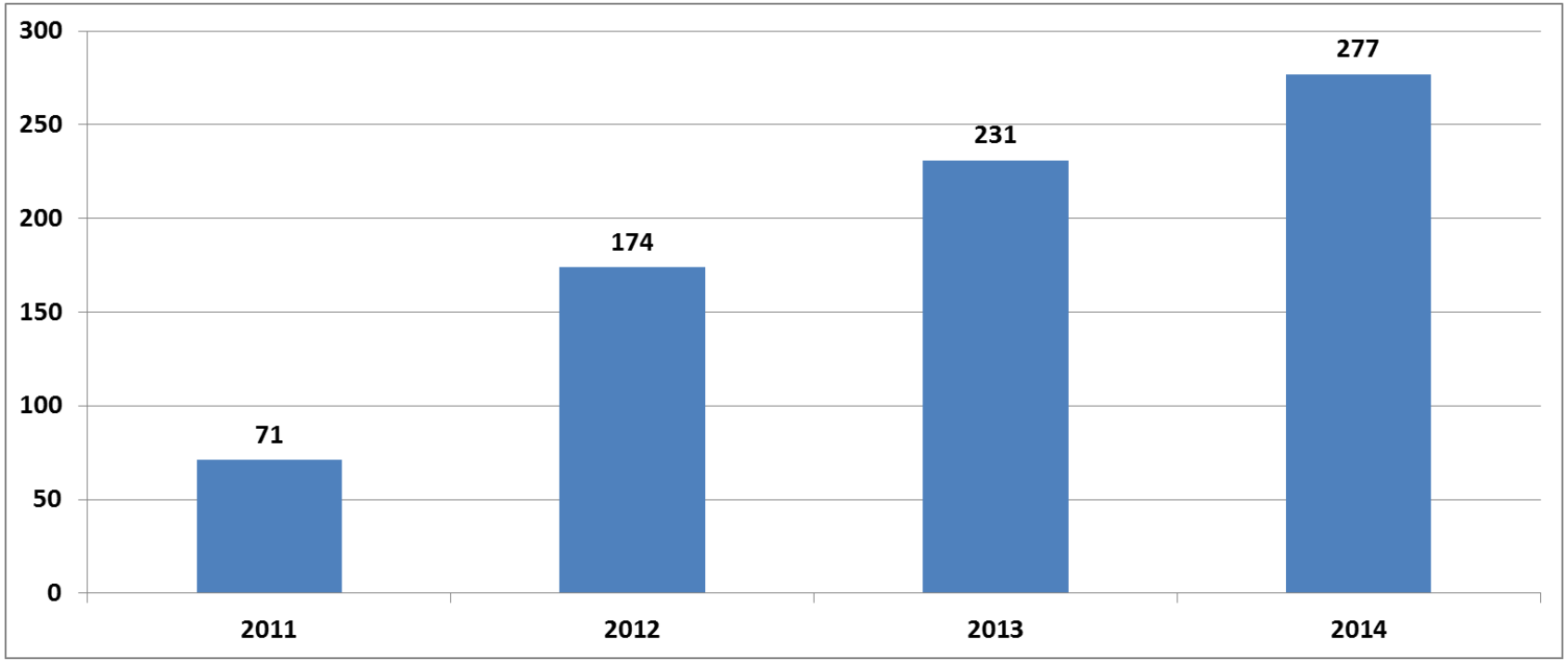
Threat cathegories

- Malware
  - Programs and files that are created to do harm. (viruses, worms, trojans, etc.)
- Grayware
  - Do not contain viruses and are not obviously malicious, but can be annoying or even harmful (hack tools, accessware, spyware, adware, dialers, and joke programs, etc.)
- Madware
  - Aggressive techniques to place advertising in your mobile device's photo albums and calendar entries and to push messages to your notification bar. Madware can even go so far as to replace a ringtone with an ad.

App analisys

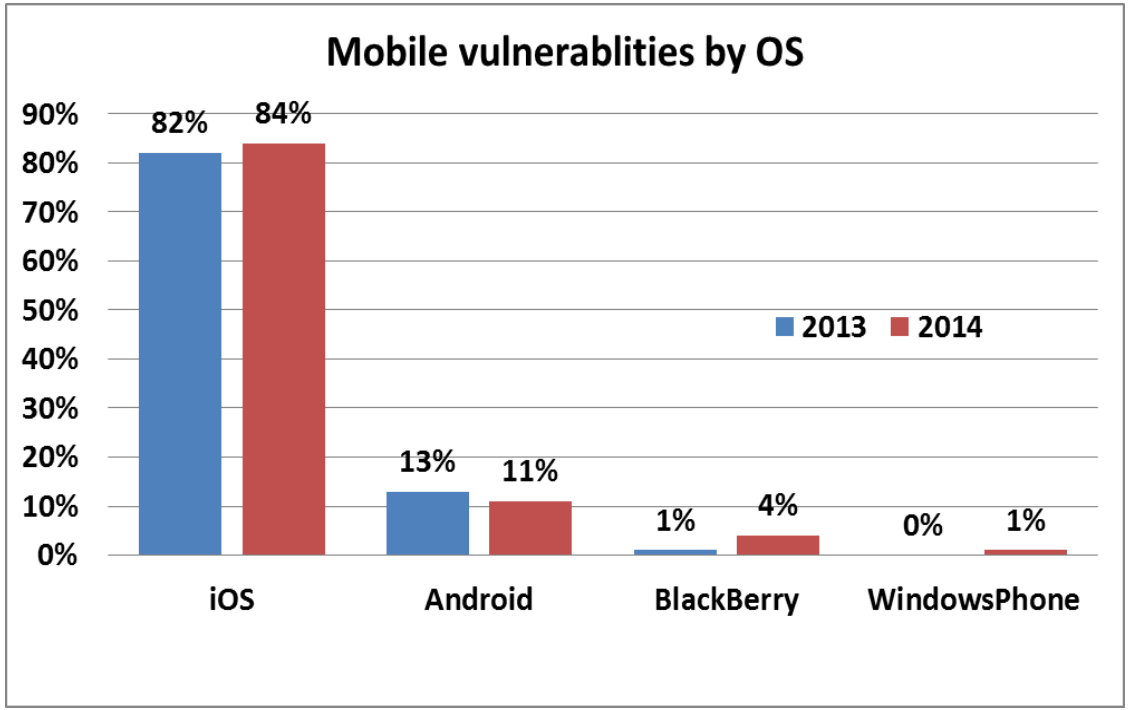


Android malware families



And iOS?

- Closed, but not invulnerable
- Weakest chain link
  - User
    - Jailbreak
  - Developer
    - XcodeGhost attack
    - 377 Apps



New types of attacks

- Multi-exploit: intelligent testing of potential vulnerablities
- Multi-effect: Data leaks, ransomware, botnet
- It is not about Windows any more:
  - Routers, TVs, industrial controllers, flight systems, critical infrastructure, mobile devices
- Eg. the Shellshock case
  - Level 10 NVD
  - 22.487 attacking IP addresses

Connected medical devices are seriously ill

Anything with an IP (>1000/hospital)

- MRIs
- X-rays
- Infusion pumps
- Medical ventillators
- CTs
- Anaesthetic machines
- Defibrillators

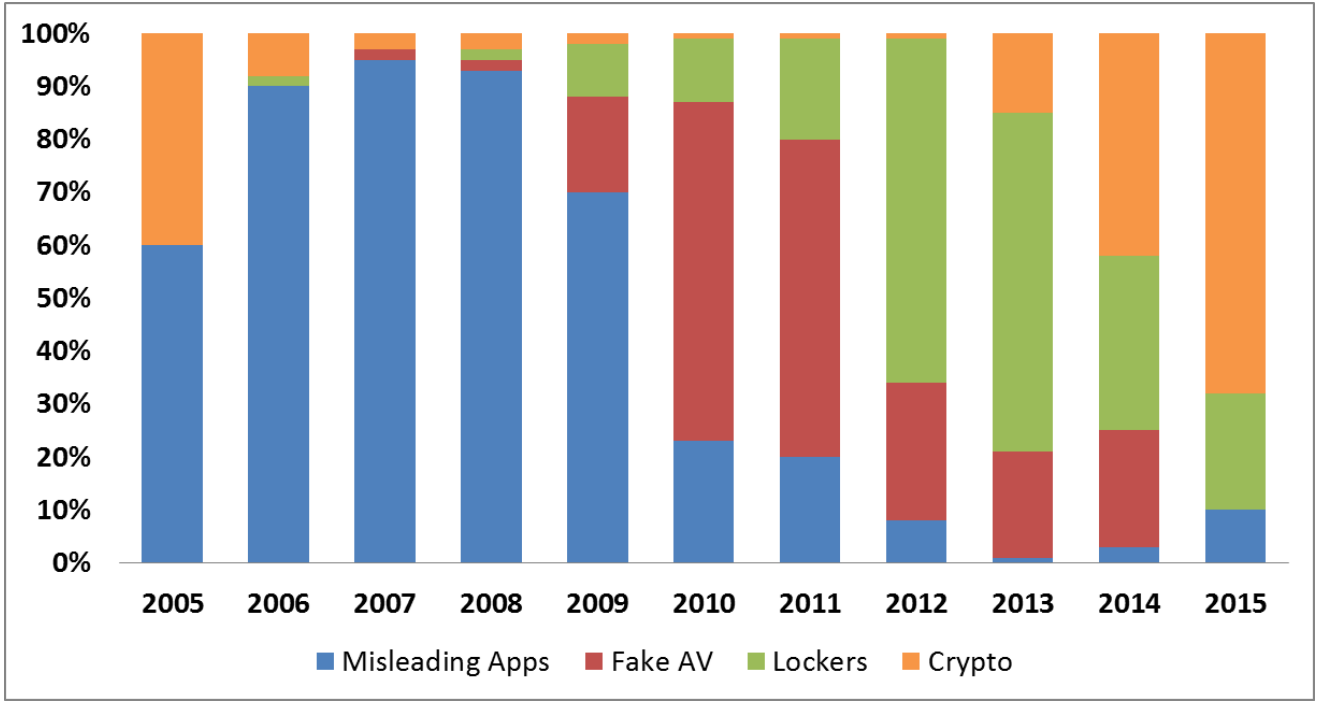
Connected medical devices are seriously ill

- Can be discovered in search engines (eg. Shodan)
- Experiment: in 6 months – 55k login attempt, 55 succesful logins, 24 explits, 299 malwares
- Hospital WIFI
- Phisically set passwords, ports, or no protection at all
- 85% of healthcare devices can be accesd by just trying common GE settings
- Data breach, botnet, targeted attack, patients!!!! (pain inhibitor)
- Windows XP – no AV

Ransomwares

- Locker (device)
- Crypto (data)

- Crucial areas:
  - Key mgmt.
  - Encryption



Ransomwares

New targets

- NAS devices
- TVs, set-top-boxes
- Routers
- Fridges, household
- Mobile, wearable
- Cars!!!

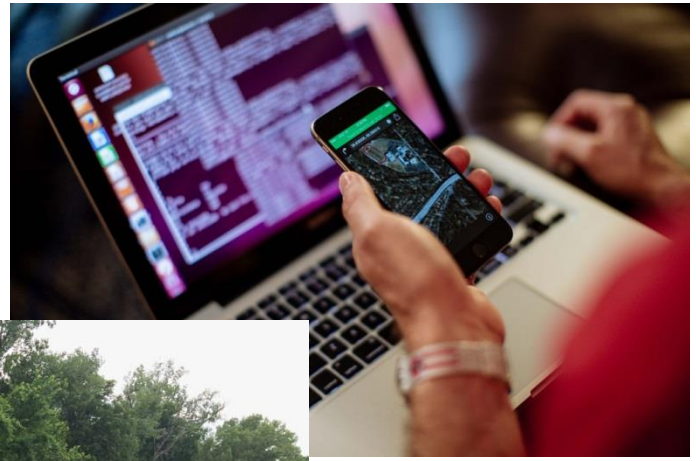
New methods

- Cyber currency (BitCoin)
- Mobile
  - Encrypt SD card
  - Set new PIN
  - Internal storage locker
  - Infect smartwatch like devices
- Dynamic pricing (20-700 USD)

IoT Case Study: Jeep Cherokee

Remotely controlled

- lights
- air circulation
- wipers
- entertainment system
- steering
- transmission
- brakes



Thank you for your attention!

Attila Horváth PhD
horvath.attila@infota.org