Malware:
malicious software

Marek Zachara
http://marek.zachara.name

A short history of Malware

Computer 'Viruses'

- The name originates from the analogy to their biological counterparts
- Traditionally spread by attaching themselves to executable files or infecting system partitions

Internet: the turning point

- New methods of distribution
- Remotely-controllable
- Communication with their 'master'
- No longer a virus, but an 'army of zombies'

Malware Classification

- Modifiable
- Controllable
- Backdoor / attack vector
- Autonomic

Payload

- Worms
- Distributed with other software
- Installed by convinced users
- Data storage
- Other ...

Infection method

Selected functionality:

- Eavesdroppers, password stealers
  key-loggers, screen-loggers etc.
- Hijacking of communication and config.
  M-t-B, local proxy, routing, DNS
- Distribution of mal-activity
  click stealers, spam senders, DDoS
- Use of local resources (CPU)
  BitCoin mining, password cracking
- Ransomware
- Rogue Anti-Malware
- Illegal content containers

'Famous' malware

I Love You (2000)

- Use of “social engineering”, infected approx. 10% of world PCs

Zeus (2008)

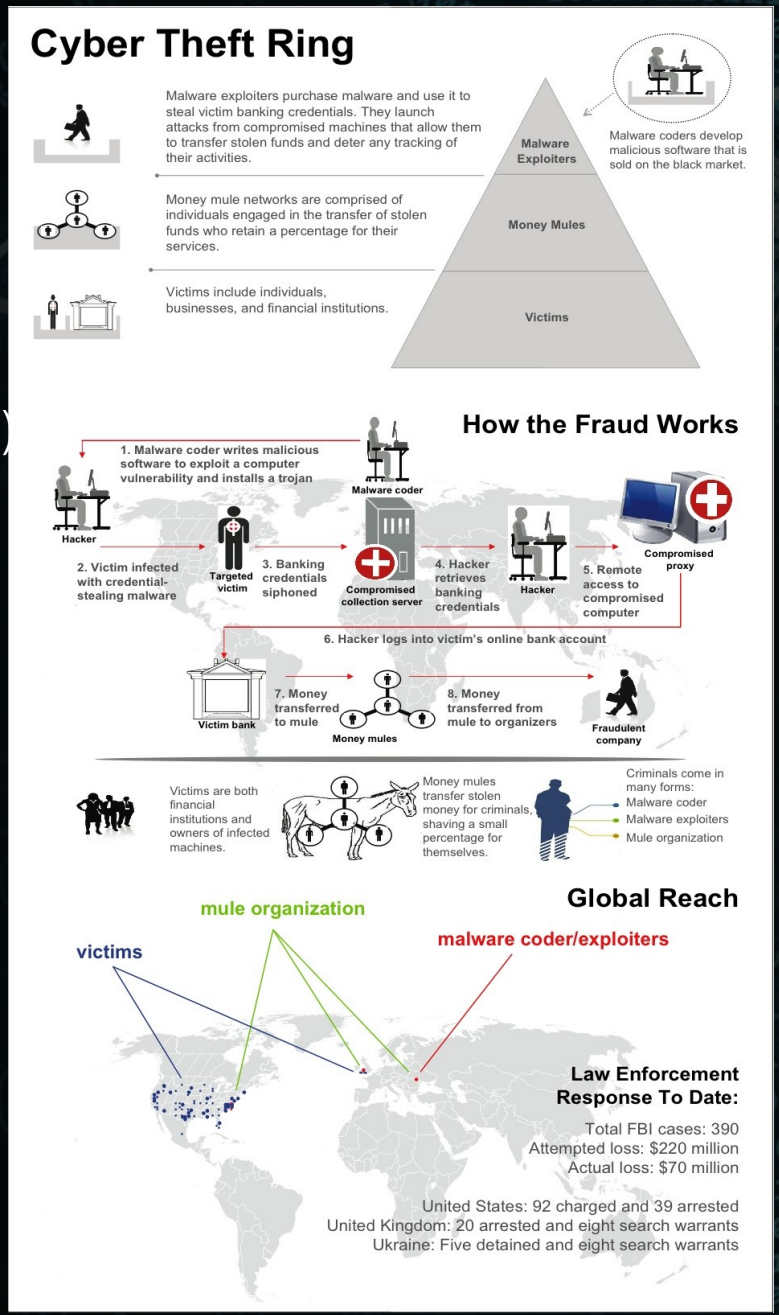
- One of the first specialized banking / password stealer

StuxNet (2005-2009?)

- Cost to build, four+ 0-day exploits

Zeus

- Export of locally stored certificates
- Retrieval of passwords from local Windows Protected Storage
- Monitoring and extraction of passwords from common protocols (POP3, FTP etc.)
- Keylogger, screenlogger
- HTML modification on-the-fly
- Extraction of SIDs and auth. tokens
- Traffic routing
- Searching for victims in LAN
- etc ...



Source: FBI / Wikimedia Commons

Polish Police accepts „donations”

Source: http://www.komputerswiat.pl, http://usunwirusa.pl

Cryptolocker – pay for your data

Source: http://cdn.arstechnica.net

Bot-nets: the next level of malware

- Organized network of 'zombies'
- Specialized, with an upgrade option

Srizbi (2008)

- 60 bln of e-mails sent daily (60-70% of world spam)

ZeroAccess (2011)

- 2 mln PCs, click-fraud / Bitcoin
  energy use comparable to 100 000 households

Conflicker / Mariposa (2008)

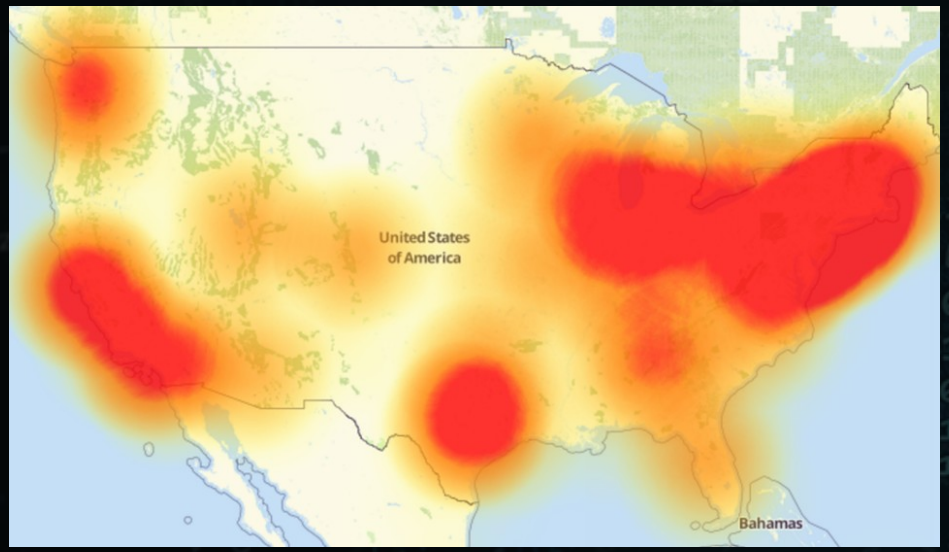
- 10-15 mln infected, 3-4 mln during the peak

Zeus (2007-)

- 3+ mln PCs, focused on bank accounts

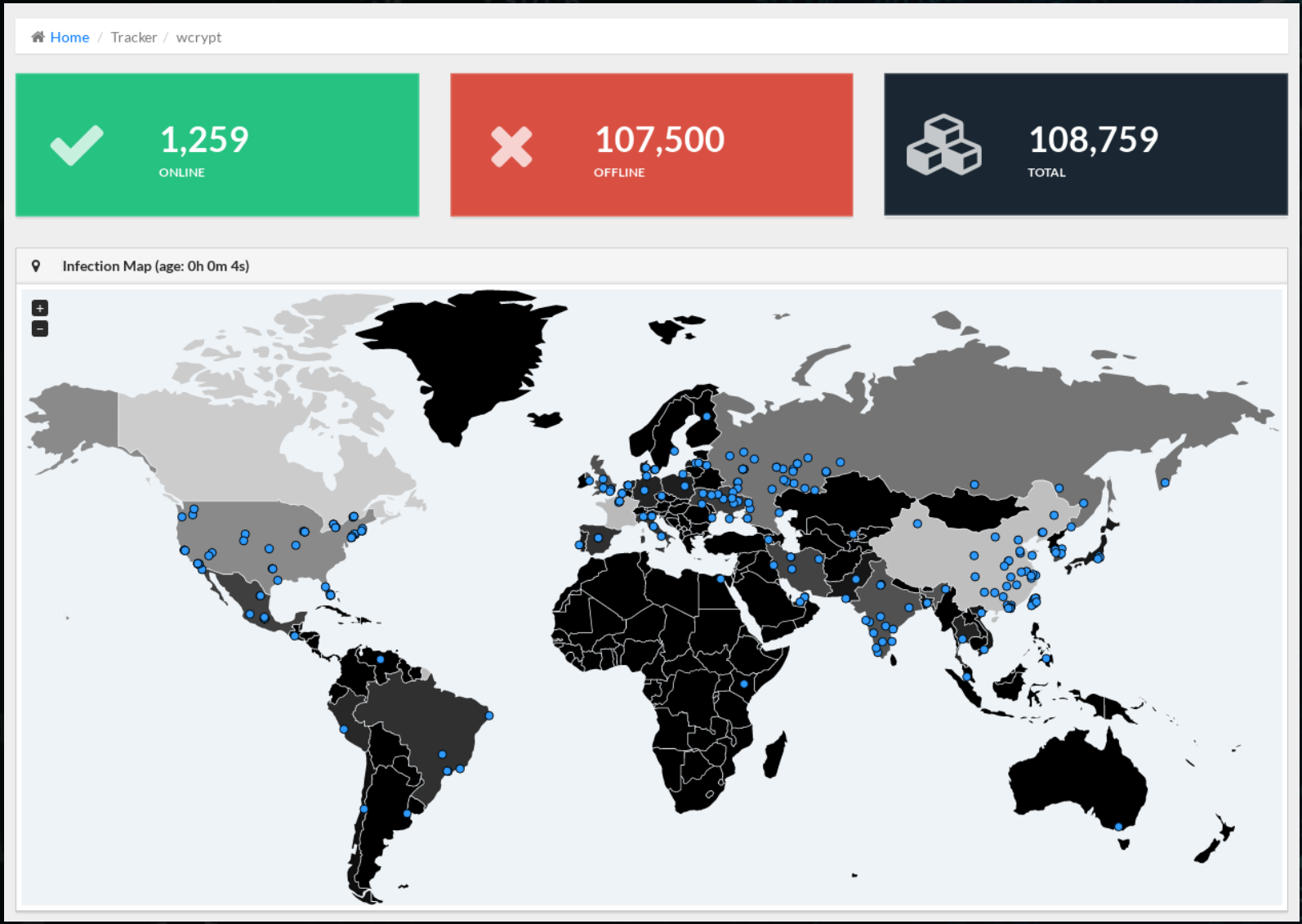
IoT- enabled massive attacks

- In Sep 2016, there were a couple of DDoS attacks performed by Mirai-controlled botnet of devices
- Over 140 000 devices participated
- Attacks reaching 1Tbps



Source: http://www.forbes.com

WannaCrypt 2017

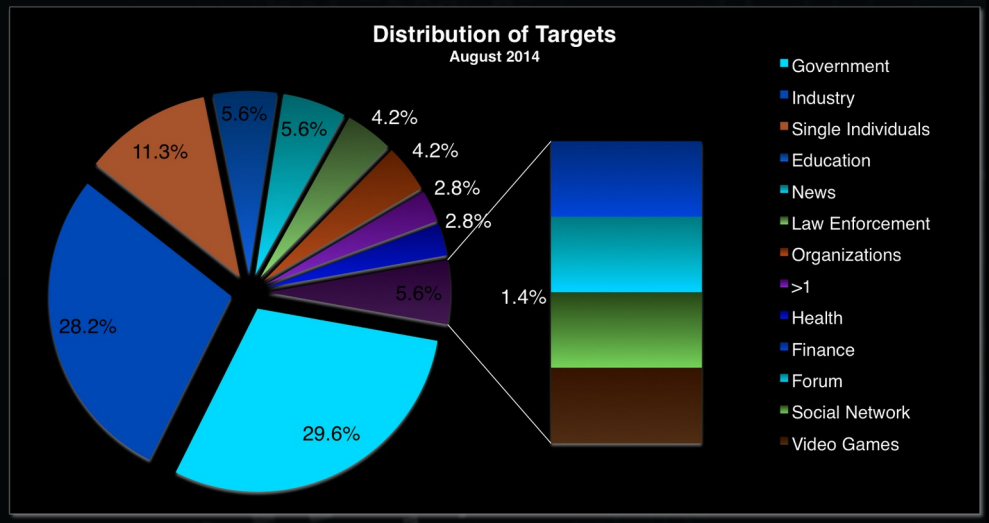


Malware statistics

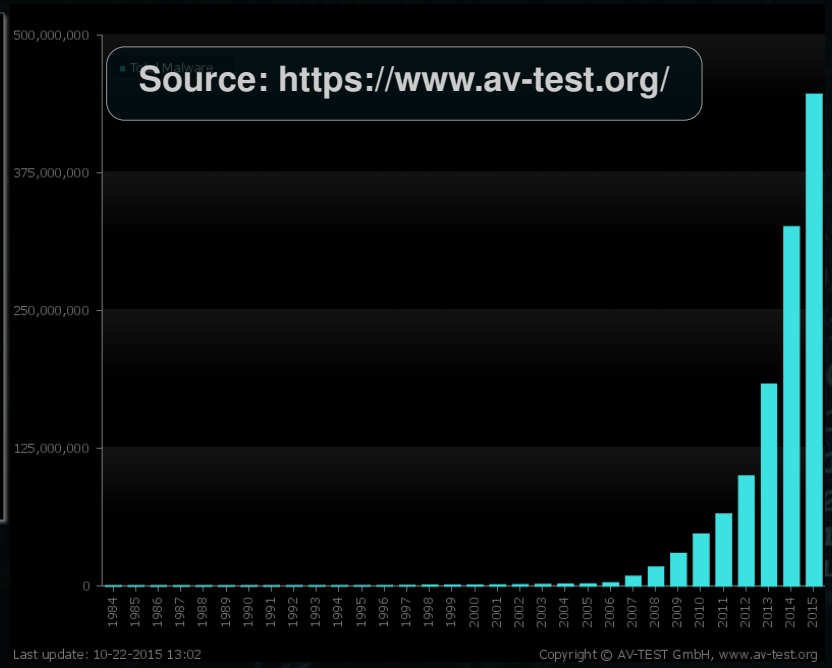
Source: http://docs.apwg.org/reports/

Ranking	Country	Infection Rate
1	China	47.22%
2	Taiwan	45.92%
3	Turkey	42.33%
4	Russia	41.45%
5	Bolivia	41.38%
6	Argentina	41.16%
7	Ecuador	39.47%
8	Peru	37.11%
9	El Salvador	35.02%
10	Guatemala	34.98%

Ranking	Country	Infection Rate
45	Switzerland	27.83%
44	Belgium	26.39%
43	Portugal	25.56%
42	Germany	24.81%
41	France	23.37%
40	UK	22.93%
39	Netherlands	22.36%
38	Japan	21.34%
37	Norway	21.02%
36	Sweden	20.07%



Source: http://www.hackmageddon.com/



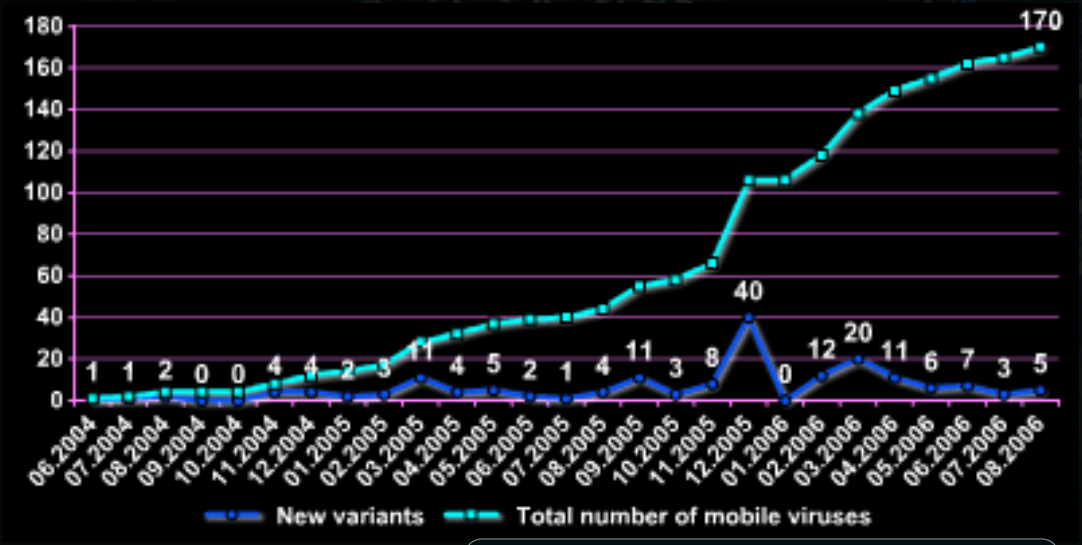
Geographical threat distribution

Source: http://www.virusbtn.com/

Malware for the mobile world

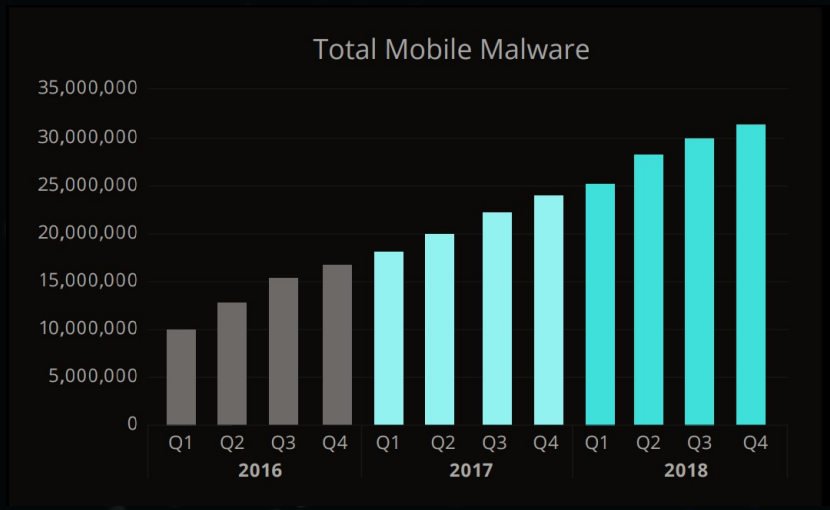
- Most of the attacks are user-targetted
- Usually distributed with applications outside official channels (stores)
- First virus (Symbian/ARM) – 2004
- First Malnets (Botnets) – active since 2012
- ZEUS and other malnets are targeting internet banking services

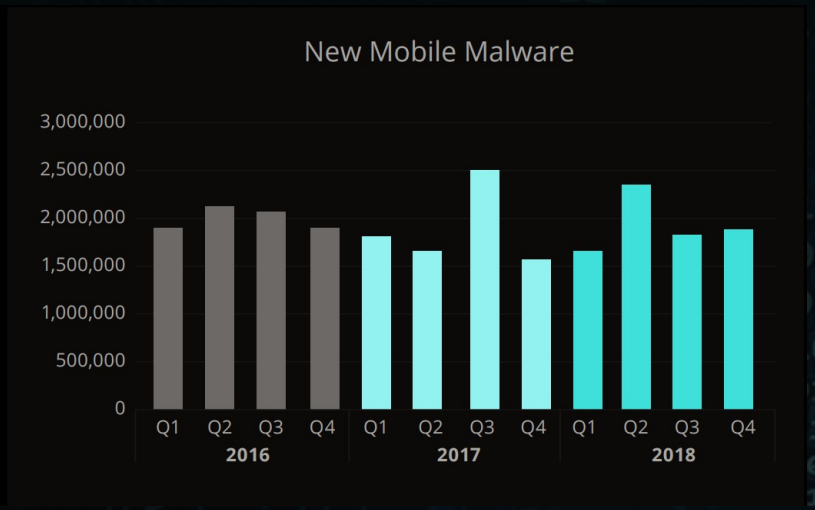
Mobile malware statistics

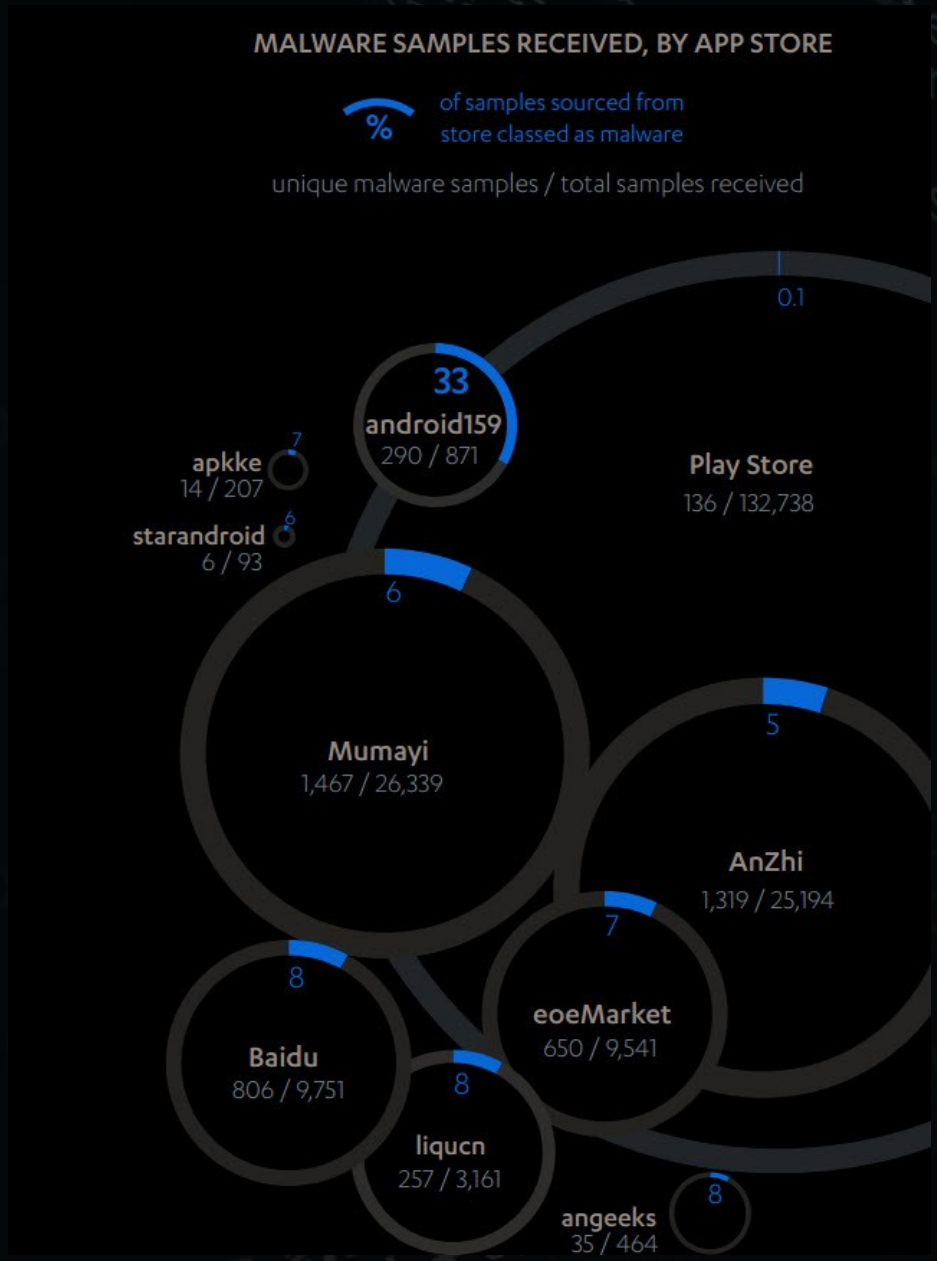


Source: securelist.com

Source: www.mcafee.com







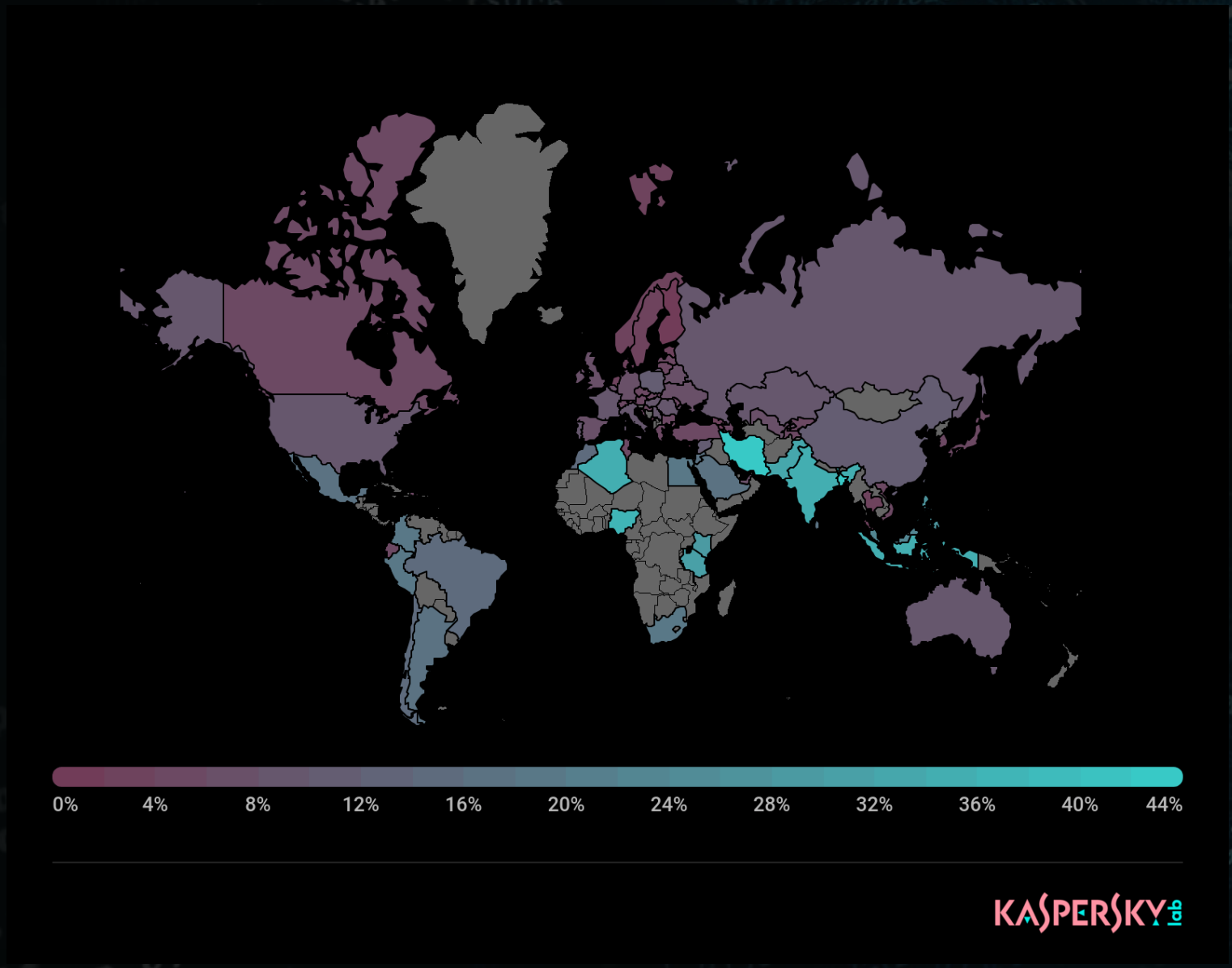
Although the number of malware for Android is significant, it doesn't mean an 'average Joe' is at risk (unless he decides to tweak his phone). The risks are associated with using the black market applications ("warez")

Source: http://forbes.com/

Trends in mobile malware

- Adware and ‘clickjaking’ treated as PHA by Google since 2018
- Malware uses active ‘sandboxing’ detection
  - Changes activities or downloads new code once installed on a user’s phone
  - Phones may become ‘adware zombies’
- Rise in mobile ‘miners’ (5x in 2018)
- Increased use of ‘droppers’
- Use of other channels to deliver apps:
  - SMS messages
  - Social platforms

Geographical distribution of mobile malware



Malware and „anti-viruses”

- Anti-virus programs are usually based on signatures – patterns identifying particular piece of malware code
- By definition they are produced after a new version of malware is identified
- As a result, there is no protection against new malware nor 'zero-day' exploits

Methods for combating Malware

Technical (including heuristics)

- Traffic analysys
- Behavior analysys

Disabling of botnets' Command Centers

Sociological

- Introduction of uniform practices and comm. preferably for the whole industry sectors
- Limit changes
- Information and training

Sept. 2013 – Symantec attacks ZeroAccess

- By exploiting a protocol vulnerability
- Approx. 0.5mln of bots disconnected

Thank you for your attention.

Any questions?

Included content came from:

- Clipart – openclipart.org

Licensed (royalty-free) content, cannot be distributed separately:

- Presentation background, people's avatars