

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'

**Introduction
to malware**

Classification

Sample
malware

Statistics

Mobile
malware

Means of
protection

Malware Classification

Modifiable _____
Controllable _____
Backdoor / attack vector _____
Autonomic _____

Payload



Introduction
to malware

Classification

Sample
malware

Statistics

Mobile
malware

Means of
protection

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

Introduction
to malware

Classification

Sample
malware

Statistics

Mobile
malware

Means of
protection

'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?)

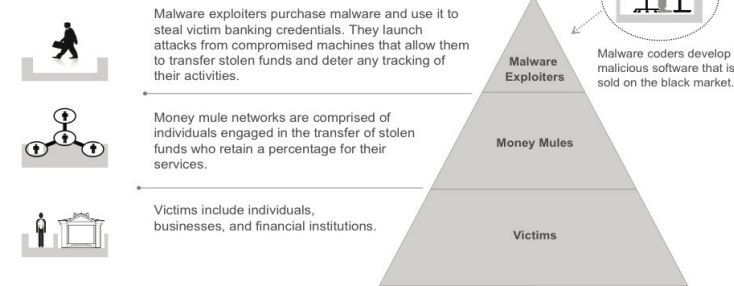
- Cost to build, four+ 0-day exploits

Introduction
to malware
Classification
**Sample
malware**
Statistics
Mobile
malware
Means of
protection

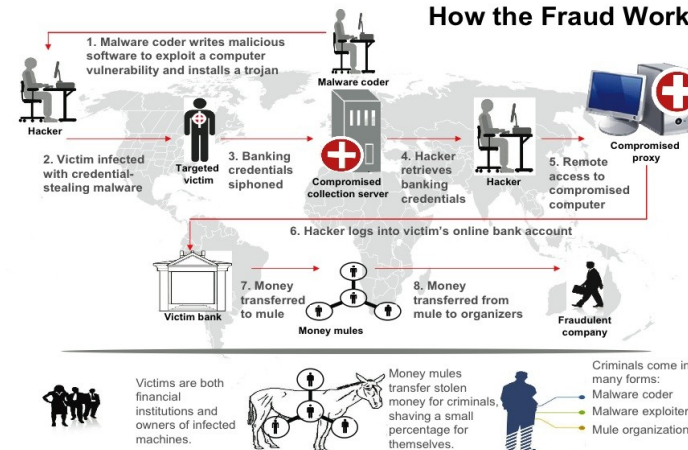
Zeus

- 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 ...

Cyber Theft Ring



How the Fraud Works



Global Reach

Diagram showing the global reach of the Cyber Theft Ring, with lines connecting victims, mule organization, and malware coder/exploiters across the world map.

Law Enforcement Response To Date:

Total FBI cases: 390
 Attempted loss: \$220 million
 Actual loss: \$70 million

United States: 92 charged and 39 arrested
 United Kingdom: 20 arrested and eight search warrants
 Ukraine: Five detained and eight search warrants

Introduction to malware
 Classification
Sample malware
 Statistics
 Mobile malware
 Means of protection

Polish Police accepts „donations”

Polizia. Biuro Służby Kryminalnej
Wydział Wsparcia Zwalczania Cyberprzestępczości

IP: ?
Kraj: Poland
Region: --
Miasto: '

UWAGA! Pańska przeglądarka została zablokowana ze względów bezpieczeństwa z wskazanych niżej przyczyn. Wszystkie działania tego komputera zostały zarejestrowane. Wszystkie pliki są szyfrowane.

Pan/Pani jest oskarżony/a w przeglądaniu/przechowywaniu i/ albo rozpowszechnieniu materiałów pornograficznych zabronionej treści (Pornografia dziecięca/Zoofilia/Zgwałcenie i tak dalej). Pan/Pani poruszył/a Światową Deklarację po walce z rozpowszechnieniem pornografii dziecięcej i jest oskarżony/a w dokonaniu przestępstwa, przewidzianego Artykułem 161 Kodeksu Kryminalnego Rzeczypospolitej Polskiej.

Artykuł 161 Kodeksu Kryminalnego Rzeczypospolitej Polskiej przewiduje w jakości ukarania pozbawienie wolności w terminie od 5 do 11 lat.

Również Pan/Pani jest podejrzanym/a w naruszeniu "Ustawy o prawach autorskich i stycznych" (ściągnięcie pirackiej muzyki, wideo, oprogramowania nielicencyjnego) i użyciu i/ albo rozpowszechnieniu kontentu, obronionego prawem autorskim. W ten sposób jest Pan/Pani podejrzanym/a w naruszeniu Artykułu 148 Kodeksu Kryminalnego Rzeczypospolitej Polskiej.

Artykuł 148 Kodeksu Kryminalnego Rzeczypospolitej Polskiej w jakości ukarania przewiduje grzywnę w wymiarze od 150 do 550 bazowych wielkości lub pozbawienie wolności w terminie od 3 do 7 lat.

Z Pańskiego komputera osobistego został zrealizowany dostęp niesankcjonowany do zamkniętej dla publicznego dostępu informacji i informacji ważności państwowej w sieci Internet.

Dostęp niesankcjonowany mógł/mogła Pan/Pani zorganizować naumyślnie z motywów korzyistnych lub dostęp niesankcjonowany mógł stać się bez Pańskiej wiedzy i zgody, ponieważ Pański komputer osobisty może być zarażony programami szkodliwymi. W ten sposób jest Pan/Pani podejrzanym/a, do przeprowadzenia śledztwa, w nieumyślnym naruszeniu Artykułu 215 Kodeksu Kryminalnego Rzeczypospolitej Polskiej ("Ustawa o niedbalym i nonszalanckim użyciu środków techniki obliczeniowej/komputera osobistego").

Pozostały czas: 47:43:07

Ukash paysafecard

Kod PIN Wartość
Wpisz kod 500

Opłacić Ukash Opłacić PaySafeCard

Gdzie mogę nabyć pieniężny voucher Ukash?

Możesz nabyć Ukash w jednym z tysięcy punktów na świecie, przez Internet, przez portfel, w kiosku oraz bankomacie.

Zakup kuponu w serwisie www.dotPay.pl

ePay - Ukash możesz kupić w wybranych sklepach z logo ePay.

PayUp - Korzystaj z Ukash w wybrany kiosk PayUp.

Apollo - Sprawdź Warunki Ukash, zanim uzyskasz kod Ukash lub użyjesz go kiosk Apollo.

Gdzie mogę nabyć pieniężny voucher PaySafeCard?

PaySafeCard możesz kupić w wielu sklepach z elektroniką

Introduction to malware
Classification
Sample malware
Statistics
Mobile malware
Means of protection

Cryptolocker – pay for your data



Introduction
to malware
Classification
**Sample
malware**
Statistics
Mobile
malware
Means of
protection

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)

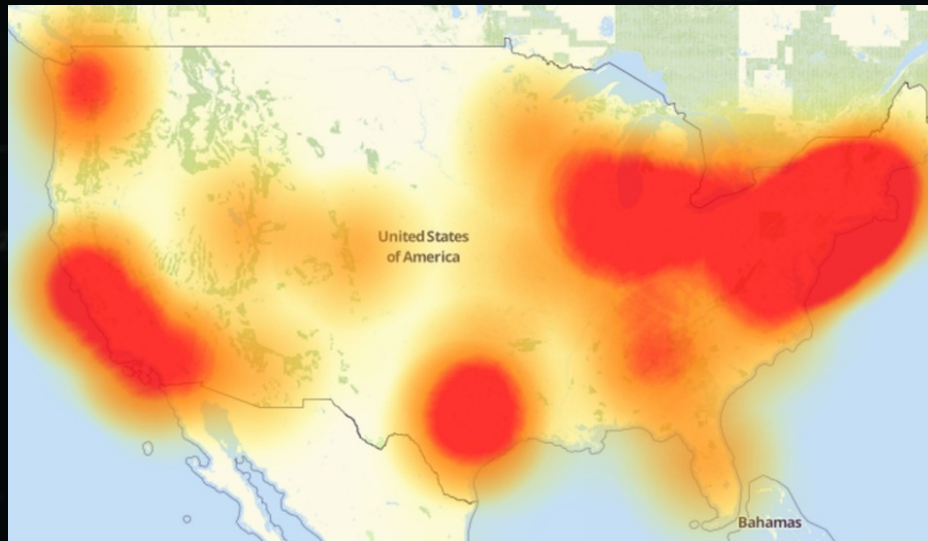
- 10-15 mln infected, 3-4 mln during the peak

Zeus (2007-)

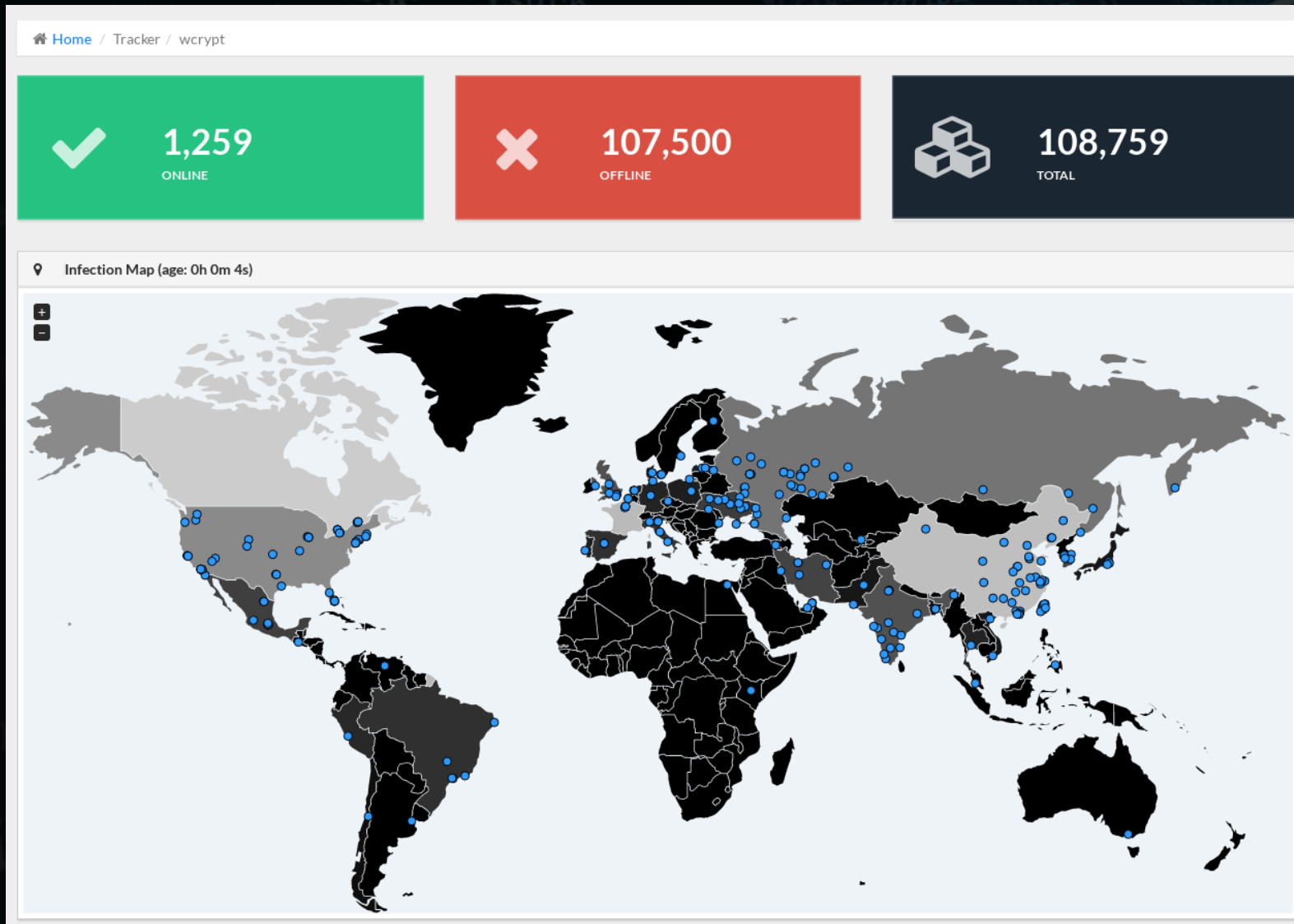
- 3+ mln PCs, focused on bank accounts

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



WannaCrypt 2017



Introduction to malware
Classification
Sample malware
Statistics
Mobile malware
Means of protection

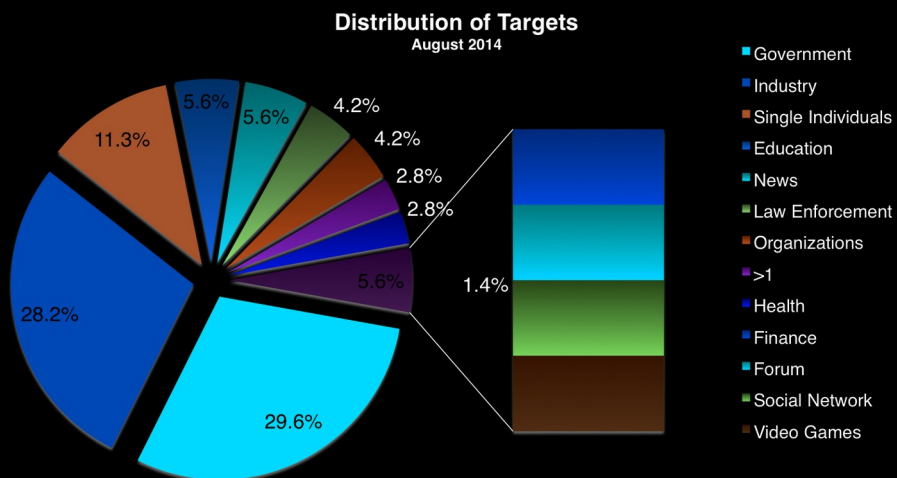
Malware statistics

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

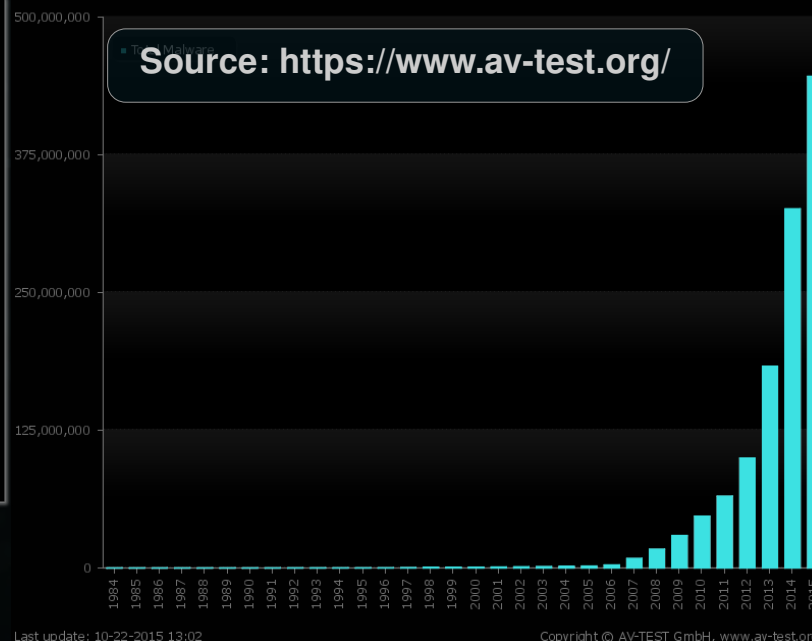
Ranking	Country	Infection Rate
1	China	47.22%
2	Taiwan	45.92%
3	Turkey	42.33%
4	Russia	41.45%
5	Bolivia	41.38%
6	Argentina	41.16%
7	Ecuador	39.47%
8	Peru	37.11%
9	El Salvador	35.02%
10	Guatemala	34.98%

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%

Introduction to malware
Classification
Sample malware
Statistics
Mobile malware
Means of protection



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



Geographical threat distribution



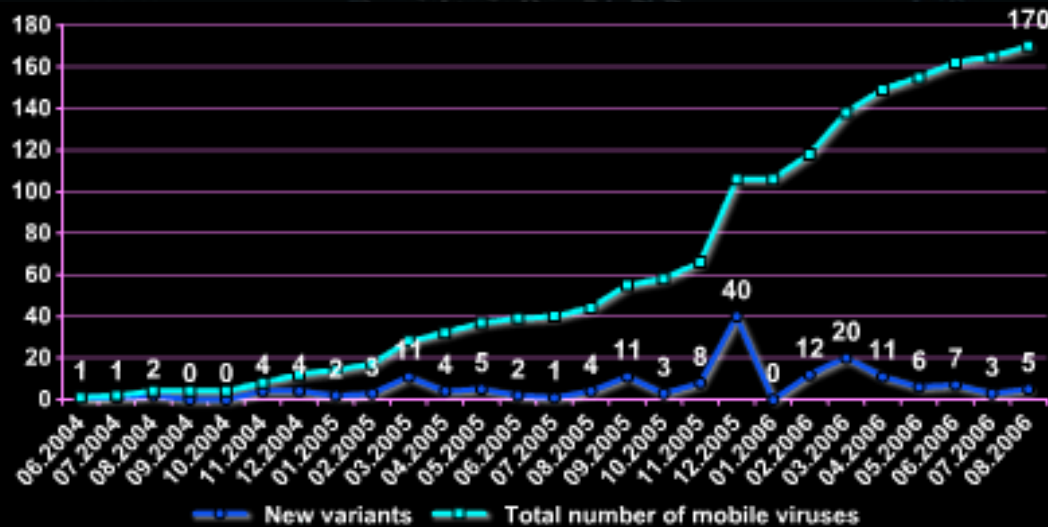
Introduction
to malware
Classification
Sample
malware
Statistics
Mobile
malware
Means of
protection

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

Introduction
to malware
Classification
Sample
malware
Statistics
**Mobile
malware**
Means of
protection

Mobile malware statistics

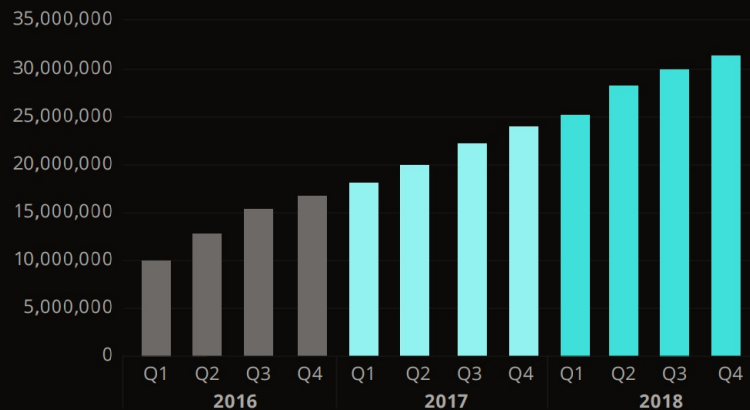


Source: securelist.com

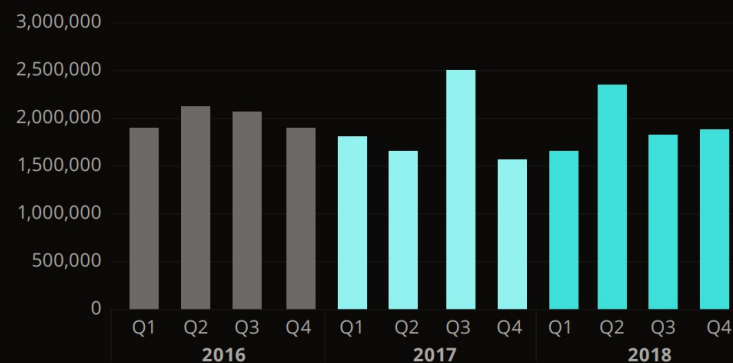
Source: www.mcafee.com

Introduction to malware
Classification
Sample malware
Statistics
Mobile malware
Means of protection

Total Mobile Malware



New Mobile Malware



MALWARE SAMPLES RECEIVED, BY APP STORE



of samples sourced from
store classed as malware

unique malware samples / total samples received



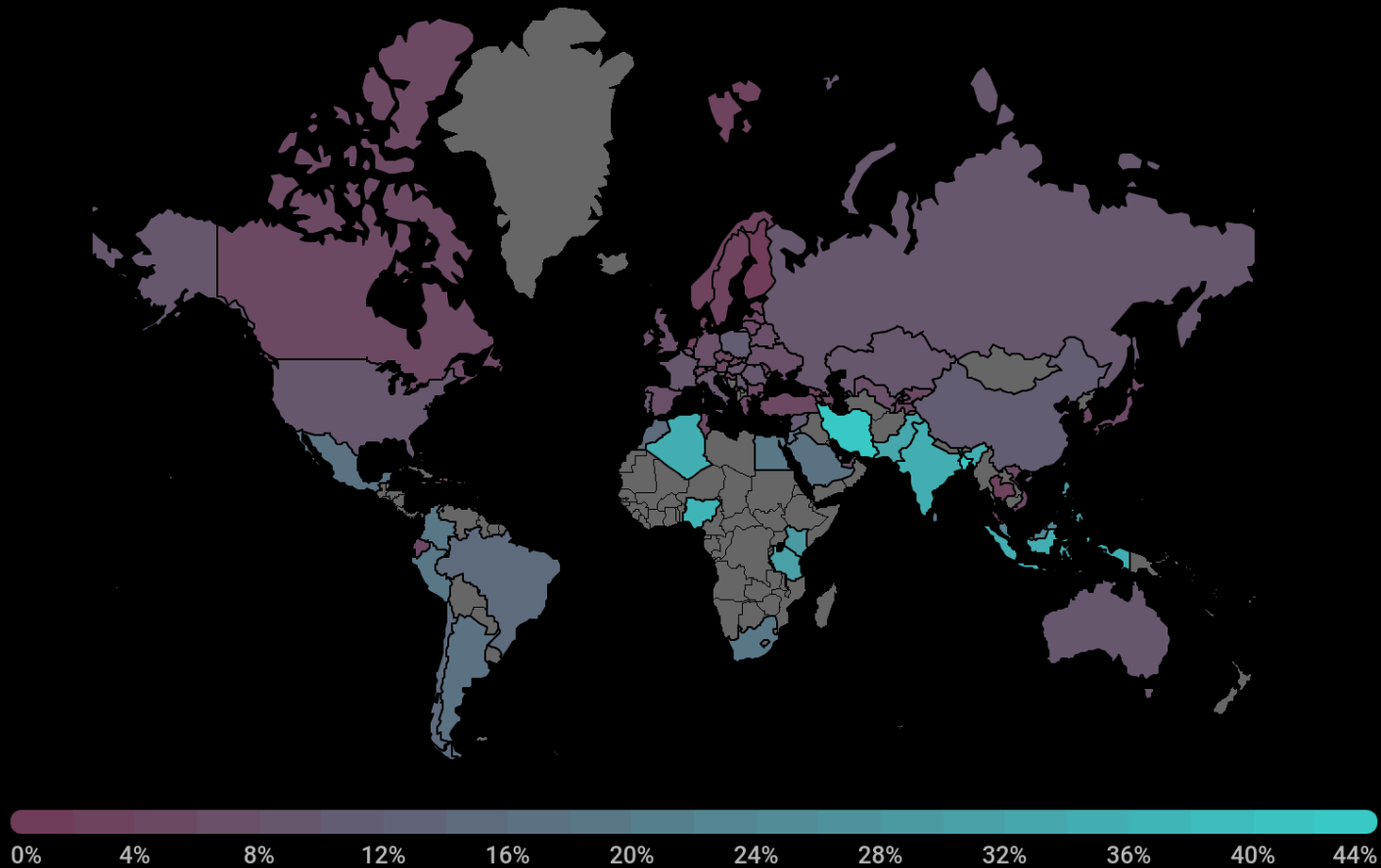
Although the number of malware for Android is significant, it doesn't mean an 'average Joe' is at risk (unless he decides to tweak his phone). The risks are associated with using the black market applications (“warez”)

Introduction
to malware
Classification
Sample
malware
Statistics
**Mobile
malware**
Means of
protection

Trends in mobile malware

- Adware and 'clickjacking' 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



KASPERSKYlab

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

Introduction
to malware
Classification
Sample
malware
Statistics
Mobile
malware
**Means of
protection**

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

Introduction
to malware
Classification
Sample
malware
Statistics
Mobile
malware
**Means of
protection**

Thank you for your attention.

Any questions?



Published
under the
following
license

Creative
Commons
Attribution
Share-Alike

Included content came from:

- Clipart – openclipart.org

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

- Presentation background, people's avatars