OSEC

IoT: Internet of Threats

Dariusz Puchalak

IoT – definition.

IoT - definition

„The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.” - Wikipedia

IoT - definition

„The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.” - Oxford dictionary

IoT – Internet of Threats.

DDoS on Krebs

- wrzesień 2016
- 620-665 Gbps
- wg Akamai poprzedni duży atak jaki widzieli miał aż 363Gbps
- zaatakowały go kamery, routery i rejestratory

DDoS on OVH

- październik 2016
- ataki dochodzące do 1Tbps
- jeden z udokumentowanych 93 MMps and 799 Gbps
- „145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS” - Octave Klaba OVH

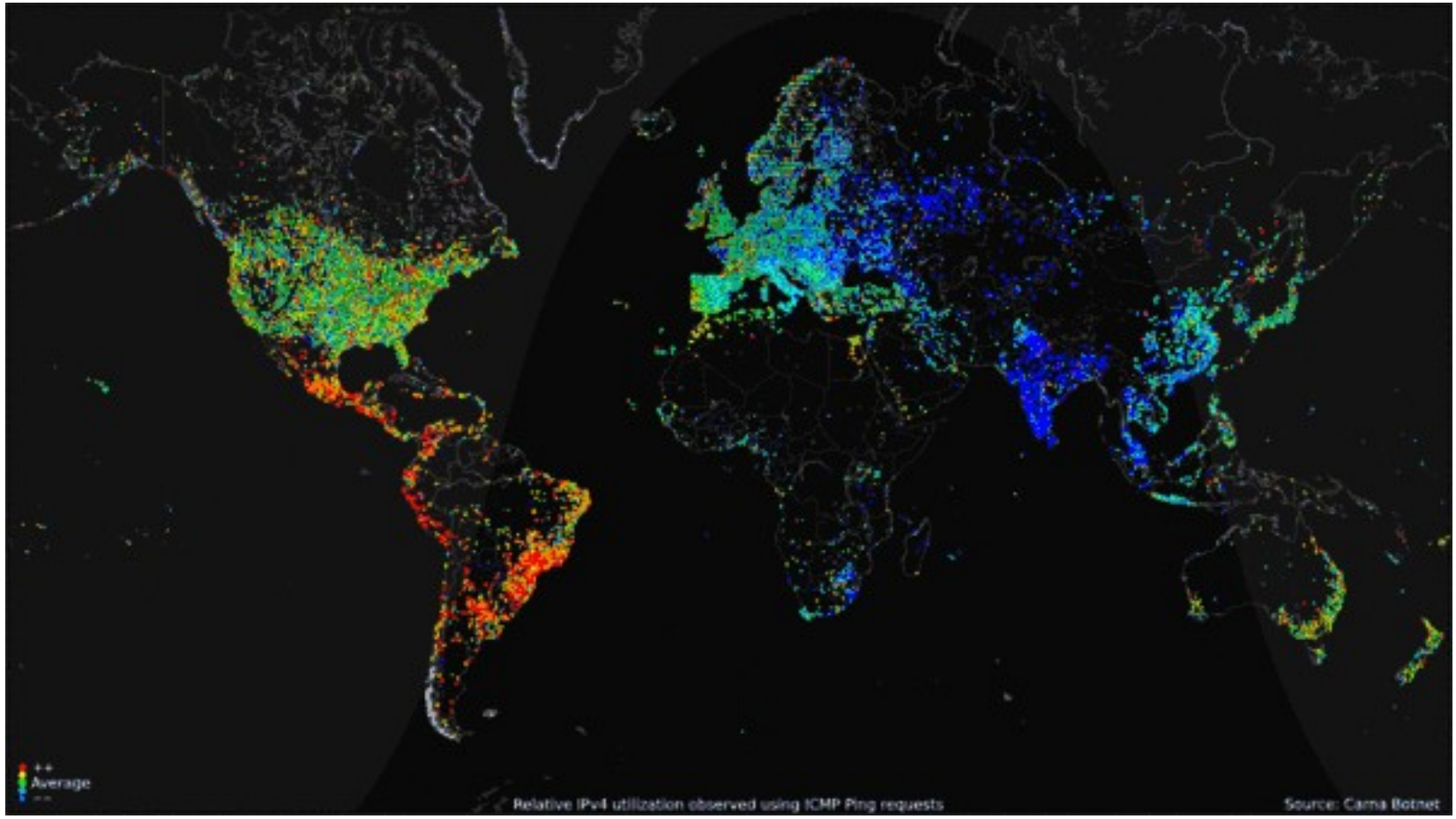
DDoS on DYN

- październik 2016
- ataki dochodzące do 1.2Tbps
- serwisy które miały problemy z dostępnością:
  - twitter, amazon, shopify, paypal, netflix, ….

Internet Census 2012

- używane niezabezpieczone urządzenia z linuksem (bez hasła, lub hasłem typu root)
- setki tysięcy maszyn (420tys. ?)
- zdolność przeskanowania całego internetu IPv4 w ciągu godziny
- http://internetcensus2012.github.io/InternetCensus2012/paper.html

Internet Census 2012



Stuxnet, Duqu, Flame

- Gdzie: Iran/Korea Północna
- Cel: Uszkodzić urządzenia wzbogacające uran.

IoT – problems

- Interfejs zarządający:
  - znane konta i hasła
  - brak blokowania kont
  - błędy w kodzie interfejsu (XSS, CSRF)
  - brak 2FA
  - mechanizmy odzyskiwania hasła z błędami

IoT – problems

- Usługi sieciowe:
  - otwarte porty do dodatkowych usług (np.. telnet)
  - udostępnianie poprzez UpnP usług wew. w internecie
  - usługi ze znanymi błędami
  - brak szyfrowania ruchu lub używanie „własnych” mechanizmów

IoT – problems

- Prywatność:
  - zbieranie dużej ilości danych o użytkownikach
  - niezabezpieczanie tych informacji

IoT – problems

- Prywatność:
  - zbieranie dużej ilości danych o użytkownikach
  - niezabezpieczanie tych informacji

    Przykład:
  - https://andreascarpino.it/posts/how-my-car-insurance-exposed-my-position.html

IoT – problems

- Uaktualnienia:
  - brak uaktualnień
  - brak szyfrowanego kanału uaktualnień
  - brak podpisów uaktualnień

IoT – problems

- Słabe bezpieczeństwo:
  - dostępne niepotrzebne porty np.. USB
  - całość działa jako „root”

Open Source IoT bots?

- Mirai – used on OVH, Krebs,
  - https://github.com/jgamblin/Mirai-Source-Code
- Linux.Wifatch – zabezpiecza IoT
  - https://gitlab.com/rav7teif/linux.wifatch/
  - licencja GPL v3

The real problem with IoT?

- „Nobody cares”.
- Nobody – most of the owners of IoT devices do not care about IoT security for many different reasons.

Pytania?

Dariusz.Puchalak@osec.pl