APTs a “kyberválka”

Jakub Drmola, BSS152, 17.10. 2019

Hlavní problémy

- atribuce (aneb kdo to udělal)
  - dopad na odstrašování
  - „false flag“ ops
- neteritorialita
  - dopad na vymáhání práva
- asymetrie
  - aktéry
  - obrany/útoku
- prolínání s nestátní/komerční sférou

Znaky státních útoků?

- motivace?
  - peníze či politika?
- plánované jako „overt/covert“?
- co cíl ztrácí a co útočník získává?
  - nemusí být totéž

APT

- Advanced Persistent Threat
  - typická charakteristika státních útoků
  - jdou za specifickým cílem, nikoliv za tím nejsnazším
  - sofistikované, dlouhodobé, plánované

  - https://apt.securelist.com/#secondPage

Špionáž

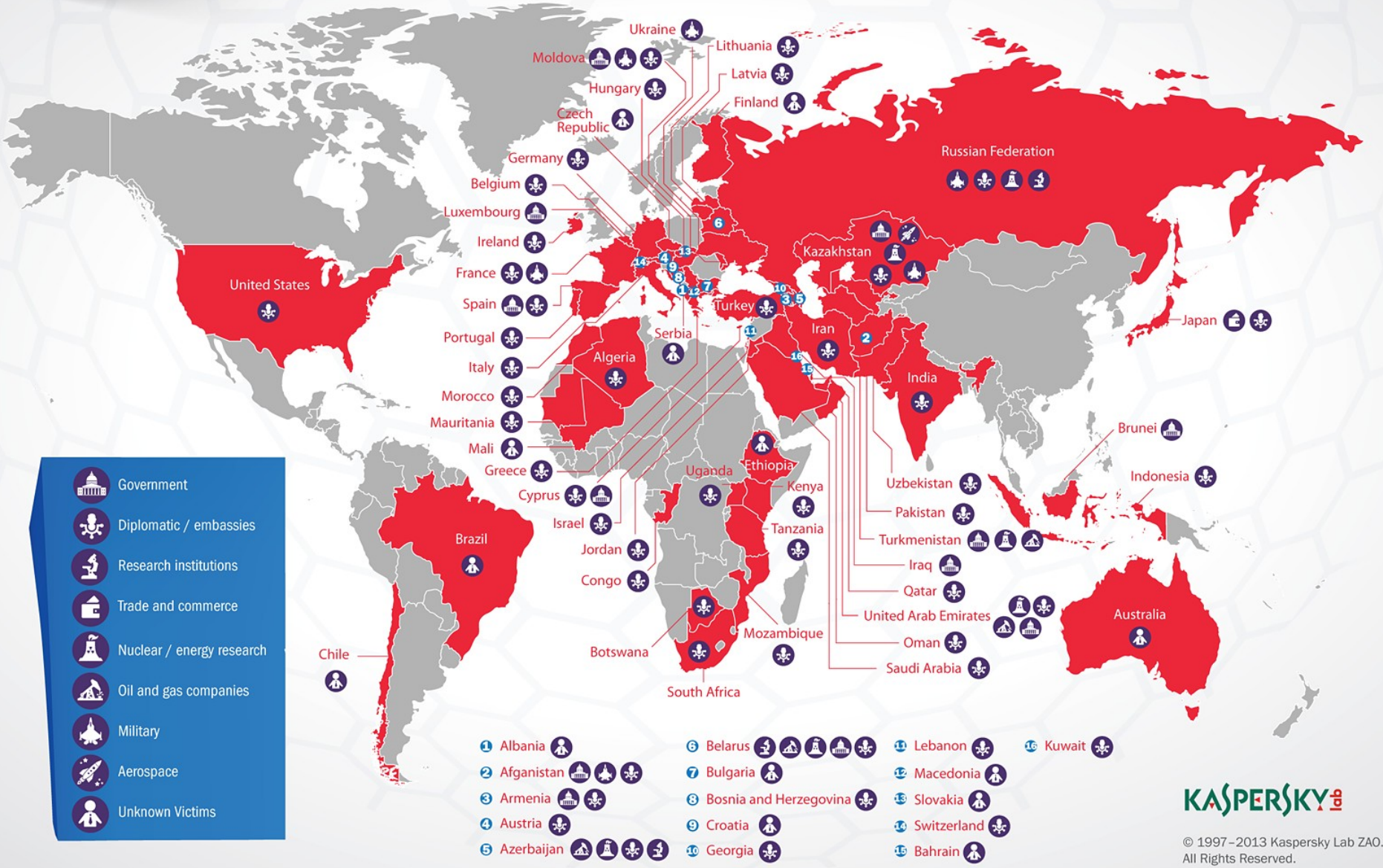
- útok na důvěrnost (C)
- např. Flame, Red October, Sandworm, Turla

- sběr dat všeho druhu, ze všech zařízení

- účel:
  - politická špionáž
  - ekonomická špionáž
  - strategická špionáž
  - taktická špionáž

Operation “Red October”

Victims of advanced cyber-espionage network



KASPERSKY lab

Sabotáž

- útok na integritu

- destrukce něčeho, obvykle dat
- Stuxnet, Shamoon, BlackEnergy

- relativně méně časté
- trvající “kinetická bariéra”


OK
OK
www.President.ir

Kyberválka?

- Kontroverzní koncept
- Rozmělněný koncept?
- Otázka reálných dopadů a závažnosti

"Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků." (Jirásek, Novák a Požár 2013)

Co je válka?

např:

- Minimálně 2 ozbrojené síly (alespoň jedna regulérní)
- Organizace v bitvách, organizace obrany, strategicky plánované útoky
- Jistá úroveň kontinuity ozbrojených operací
- Válka od 1 000 obětí/kalendářní rok

- kyberválka by tohoto měla být podmnožinou

Násilí

- Pojetí války dle Clausewitze?
- Je přítomno instrumentální násilí s politickým cílem?

- "Válka, v níž by nikdo neriskoval svůj život, by byla turnajem, hrou..." (Huyghe 2011)

- Kybernetické útoky jako projev sekundárního násilí (Rid 2013)

Problém atribuce

- Kybernetické útoky v současnosti problematické přisuzovat aktérům
- Přisouzení u státních aktérů
- Rid: "Historie nezná nepřisouzené války."
- Gartzke: Politicky motivovaný konflikt bude přisouzen

Kontinuita

- Válka není izolovaným jevem!
- Požadavek dlouhodobé organizované strategie
- Záležitost poplatná především nestátním aktérům
- Je dlouhodobé vedení kybernetické války možné

Kybernetické zbraně?

- Nikoliv kulky a šrapnely, ale jedničky a nuly
- Weapons of Mass Disruption
- (Ne)schopnost způsobit trvalé škody, podrobit, dobýt?
- Omezené schopnosti podle typu cíle
- Gartzkeho "perishable nature of CW"

Kyberválka?

- Co všechno je tedy kybernetická válka?
- Jde skrze převážně kybernetické prostředky vyhrát válka?
- Jsou špionáž a sabotáž válečnými akty?