APTs a “kyberválka”

Jakub Drmola, BSSb1152

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

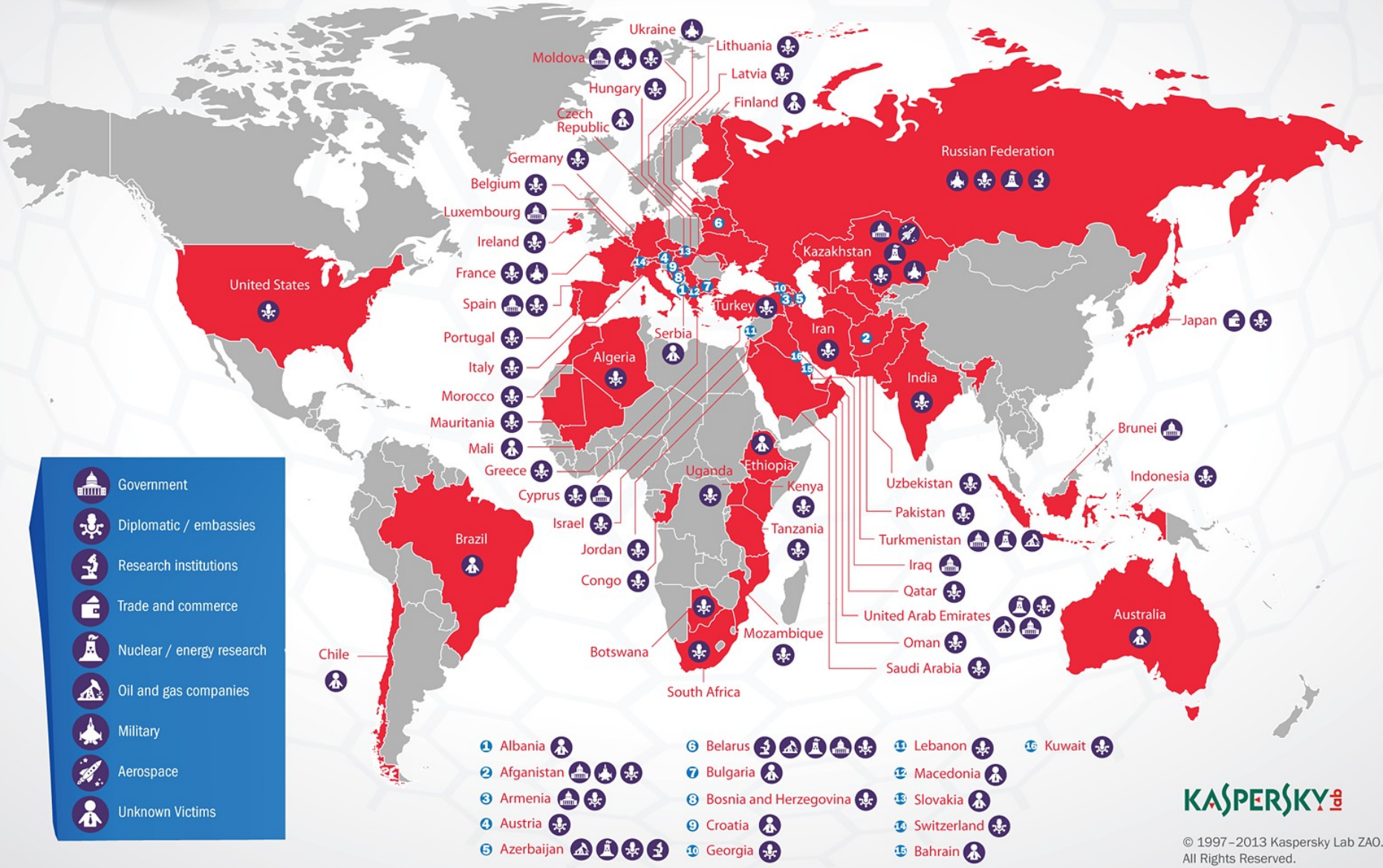
- útok na důvěrnost (C)
- např. Flame, Red October, Sandworm, Turla

- 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, NotPetya?

- relativně méně časté
- trvající “kinetická bariéra”

APT – příklady

Equation Group

- součást NSA – TAO/S32

APT – příklady

Comment Crew (61398部队)

APT – příklady

Fancy Bear (*Главное разведывательное управление*)

2016 DEMOCRATIC NATIONAL CONVENTION

PHILADELPHIA, PENNSYLVANIA | JULY 25-28

Ministry of Foreign Affairs of the Czech Republic

WANTED BY THE FBI

CONSPIRACY TO COMMIT COMPUTER FRAUD; CONSPIRACY TO COMMIT WIRE FRAUD; WIRE FRAUD; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

GRU HACKING TO UNDERMINE ANTI-DOPING EFFORTS

DETAILS

On October 3, 2018, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against 7 Russian individuals for their alleged roles in hacking and related influence and disinformation operations targeting, among others, international anti-doping agencies, sporting federations, and anti-doping officials. The indictment charges Dmitriy Sergeyevich Badin, Artem Andreyevich Malyshev, Alexey Valerevich Minin, Aleksei Sergeyevich Morenets, Evgenii Mikhaylovich Serebriakov, Oleg Mikhaylovich Sotnikov, and Ivan Sergeyevich Yermakov, with computer hacking activity spanning from 2014 through May of 2018, including the computer intrusions of the United States Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), and other victim entities during the 2016 Summer Olympics and Paralympics and afterwards. The indictment charges these defendants with conspiracy to commit computer fraud, conspiracy to commit wire fraud, wire fraud, aggravated identity theft, and conspiracy to commit money laundering. The United States District Court for the Western District of Pennsylvania in Pittsburgh, Pennsylvania, issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

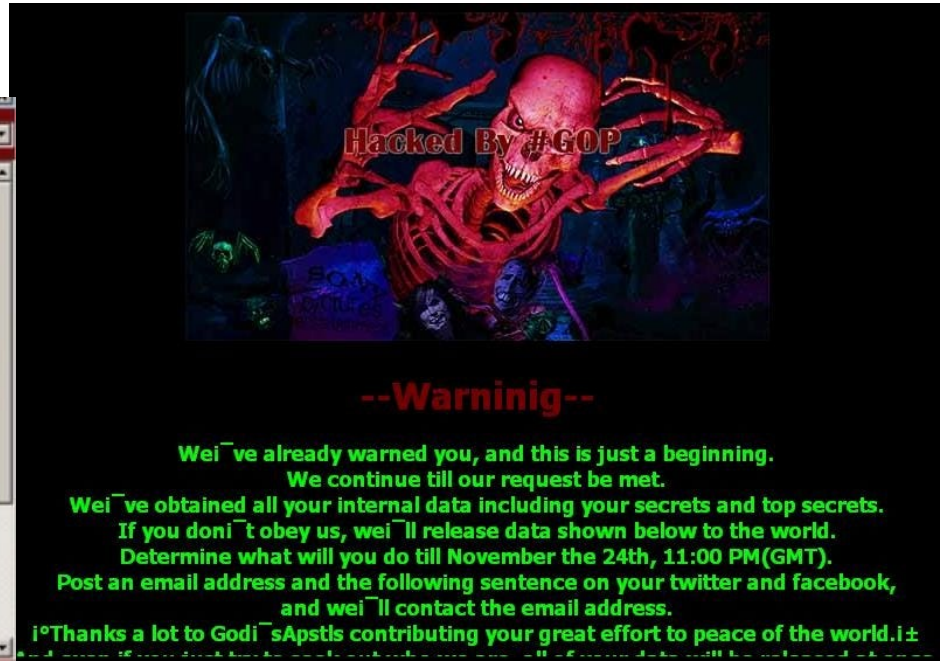
THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

APT – příklady

Lazarus Group (정찰총국)



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"

Operační podpora

- různé formy podpory vojenských operací

- Orchard 2007 (integrity)
  - útok na protileteckou obranu
- Gruzie 2008 (availability)
  - DDoS na média a komunikační kanály
- ISIS 2016 (confidentiality)
  - sběr dat pro cílení

Kyberválka?

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