

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/útoků
- 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

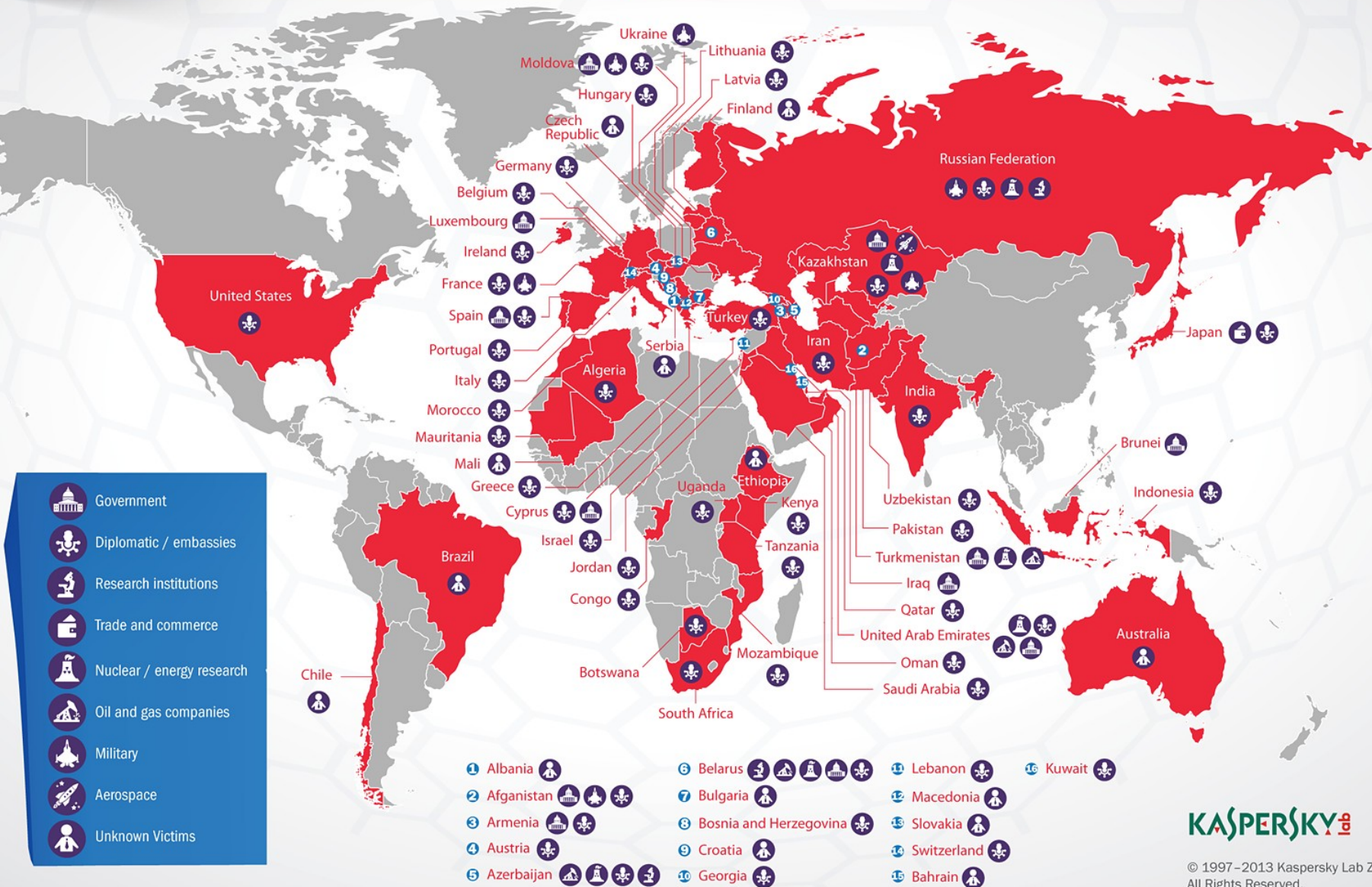
- Advanced Persistent Threat
 - typická charakteristika státních útoků
 - jdou za specifickým cílem, nikoliv za tím nejsnazším
 - sofistikované, dlouhodobé, plánované
 - <https://apt.securelist.com/#secondPage>

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



- 1.雷达罩
- 2.多功能扫描多功能雷达
- 3.红外传感器
- 4.电视红外光源
- 5.垂直升降进气口
- 6.垂直升降进气口
- 7.垂直升降进气口
- 8.垂直升降进气口
- 9.垂直升降进气口
- 10.垂直升降进气口
- 11.垂直升降进气口
- 12.垂直升降进气口
- 13.垂直升降进气口
- 14.垂直升降进气口
- 15.垂直升降进气口
- 16.垂直升降进气口
- 17.垂直升降进气口
- 18.垂直升降进气口
- 19.垂直升降进气口
- 20.垂直升降进气口
- 21.垂直升降进气口
- 22.垂直升降进气口
- 23.垂直升降进气口
- 24.垂直升降进气口
- 25.垂直升降进气口
- 26.垂直升降进气口
- 27.垂直升降进气口
- 28.垂直升降进气口
- 29.垂直升降进气口
- 30.垂直升降进气口
- 31.垂直升降进气口
- 32.垂直升降进气口
- 33.垂直升降进气口
- 34.垂直升降进气口
- 35.垂直升降进气口
- 36.垂直升降进气口
- 37.垂直升降进气口
- 38.垂直升降进气口
- 39.垂直升降进气口
- 40.垂直升降进气口
- 41.垂直升降进气口
- 42.垂直升降进气口
- 43.垂直升降进气口
- 44.垂直升降进气口
- 45.垂直升降进气口
- 46.垂直升降进气口
- 47.垂直升降进气口
- 48.垂直升降进气口
- 49.垂直升降进气口
- 50.垂直升降进气口
- 51.垂直升降进气口
- 52.垂直升降进气口
- 53.垂直升降进气口
- 54.垂直升降进气口

- 25.F119-611 发动机
- 26.主起落架
- 27.主起落架舱
- 28.天线
- 29.前缘襟翼
- 30.前缘襟翼旋转作动筒及传动轴
- 31.前缘襟翼操纵动力源
- 32.外挂架加强连接点
- 33.外挂架加强翼肋
- 34.机翼整体油箱
- 35.航行灯
- 36.襟副翼
- 37.襟副翼结构
- 38.襟副翼作动筒
- 39.横滚控制管道
- 40.横滚控制喷口(固定 87° 滚流角 4°)
- 41.加力燃烧室
- 42.三轴承支撑推力矢量喷管, 可向前下方偏转 95°; 垂直起降时, 可水平偏转 ±10°;

- 43.低可探测性轴对称喷口
- 44.可收放空中加油管
- 45.方向舵作动筒
- 46.低可探测性机体
- 47.多梁、肋式垂直尾翼
- 48.铝合金蜂窝结构垂直尾翼前缘、后缘
- 49.方向舵
- 50.全动水平尾翼
- 51.水平尾翼作动筒

- 52.鱼尾
- 53.水平尾翼结构
- 54.铝合金蜂窝结构水平尾翼前缘、后缘





Sabotáž

- útok na integritu
- destrukce něčeho, obvykle dat
- Stuxnet, Shamoon, BlackEnergy
- relativně méně časté
- trvající “kinetická bariéra”





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 regulární)
- 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?