Actorii statali

Emil SIMION

Agenda

- **Anatomia unui APT;**
- **motivatie strategica**: Rusia (APT28 (GRU), APT29 (FSB, SVR), BlackEnergy;
- **motivatie financiara**: Corea de Nord (APT38 (Gruparea Lazarus, Coreea de Nord, transfer ilicit de fonduri catre Coreea de Nord), WannaCry).

Anatomia unui APT

- **Dacă știți cum funcționează, puteți învăța cum să le opriți!**

De la infractorii cibernetici care caută informații financiare personale și proprietate intelectuală până la atacuri cibernetice sponsorizate de stat concepute pentru a fura date și a compromite infrastructura, amenințările persistente avansate (APT) de astăzi pot evita eforturile de securitate cibernetică și pot provoca daune grave organizației dvs.

Un criminal cibernetic abil și hotărât poate folosi mai mulți vectori și puncte de intrare pentru a naviga perimetrului defensiv, a intra in rețea în câteva minute și a se sustrage detectarii timp de luni de zile. APT-urile reprezintă o provocare pentru eforturile organizaționale de implementare a securitatii cibernetice.

Sase pasi ale unui atac APT

- Criminalul cibernetic, sau atacatorul, intră printr-un e-mail, rețea, fișier sau vulnerabilitate a unei aplicații și introduce malware în rețeaua unei organizații. Rețeaua este considerată compromisă, dar nu s-au scurs inca date;
- Componentele malware avansate analizează accesul la rețea și vulnerabilitățile suplimentare si comunică cu serverele de comandă și control (CnC) pentru a primi instrucțiuni suplimentare și / sau cod rău intenționat;
- Programul malware stabilește de obicei puncte de compromitere suplimentare pentru a se asigura că atacul cibernetic poate continua dacă un punct este închis;
- Odată ce un atacatorul stabilește că a stabilit un acces fiabil la rețea, colectează date țintă, cum ar fi numele conturilor și parolele. Chiar dacă parolele sunt adesea criptate, criptarea poate fi spartă. Odată ce acest lucru se întâmplă, atacatorul poate identifica și accesa datele;
- Programul malware colectează date pe un server intermediar, apoi le exfiltrează în rețea și sub controlul complet al atacatorului. În acest moment, rețeaua este considerată încălcată.
- Dovezile atacului APT sunt eliminate, dar rețeaua rămâne compromisă. Criminalul cibernetic poate reveni oricând pentru a continua colectarea datelor.

Exemplu: APT28 (Mandiant report)

- Grup de spionaj rusesc (GRU), multiple denumiri: Fancy Bear (cf. Dmitri Alperovitch), Sofacy Group (cf. Kaspersky), Sednit, Tsar Team (cf. FireEye) and STRONTIUM (cf. Microsoft);
- Tehnici utilizate: zero-day exploits; spear phishing; malware;
- Tehnici avansate de criptografie.

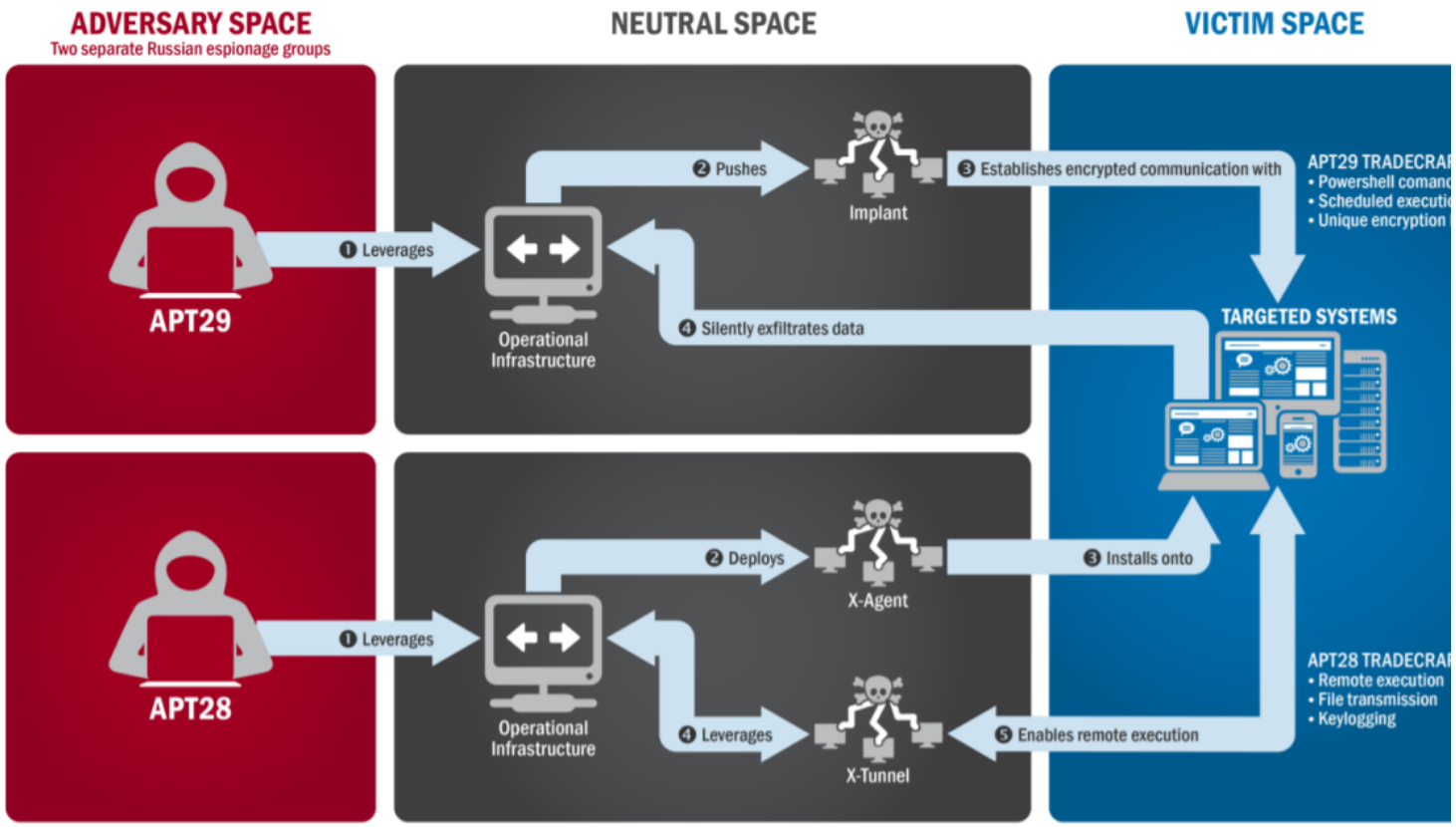
APT28: Atacuri

- atacuri asupra unor jurnaliști proeminenți din Rusia, Statele Unite, Ucraina, Moldova, Țările Baltice ….;
- parlamentul din Germania 2014 *(off-line 6 luni de zile)*;
- amenintari cu moartea asupra familiilor personalului militar americani *(CyberCaliphate, februarie 2015)*;
- televiziunea franceza *(TV5Monde, CyberCaliphate, mai 2015)*;
- atacuri asupra institutiilor financiare: United Bank for Africa, Bank of America, TD Bank, and UAE Bank *(Sofacy, raportul firmei root9B mai 2015);*
- EFF spoofing, atacuri asupra Casei Albe si NATO *(august 2015)*;
- agentia anti-doping (august 2016);
- consiliul olandez de siguranță a zborurilor și grupul de investigatii Bellingcat (exemplu: Malaysia Airlines Flight 17);
- comitetul national al Partidului Democrat (2016);
- artileria din Ucraina;
- organizatii guvernamentale olandeze (2016);
- alegerile din Germania si Franta (2016-2017);
- comitetul international olimpic (2018);
- confederatia sporturilor din Suedia;
- Patriarhia ecumenica

APT28: Caracteristici

- Fancy Bear folosește metode avansate specifice atacatorilor statali;
- foloseste e-mailuri de tip phishing, site-uri web malware deghizate în surse de știri și vulnerabilități tip zero-day;
- un grup de cercetare în domeniul securității cibernetice a remarcat utilizarea lor de nu mai puțin de șase exploatări diferite de tip zero-day (in anul 2015), o activitate tehnică considerabilă care ar necesita un număr mare de programatori care caută vulnerabilități necunoscute. Acesta este un semn că Fancy Bear este un program administrat de stat și nu o bandă sau un hacker singuratic!!!

Tehnici & tactici



- Conform raportului comun DHS si FBI (https://us-cert.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf), ambele grupari au vizat sistematic organizații guvernamentale, thnk tak-uri, universități și corporații din întreaga lume;
- **APT29 (cozy bear, FSB/SVR)**: spear phishing email, link catre un website malitios;
- **APT28 (fancy bear, GRU):** valorificarea domeniilor care imită îndeaproape cele ale organizațiilor vizate și potențialul de inselare a victimelor să introducă credentialele de autentificare.

APT28: schema de propagare & valorificare

- Conform raportului DHS si FBI:….

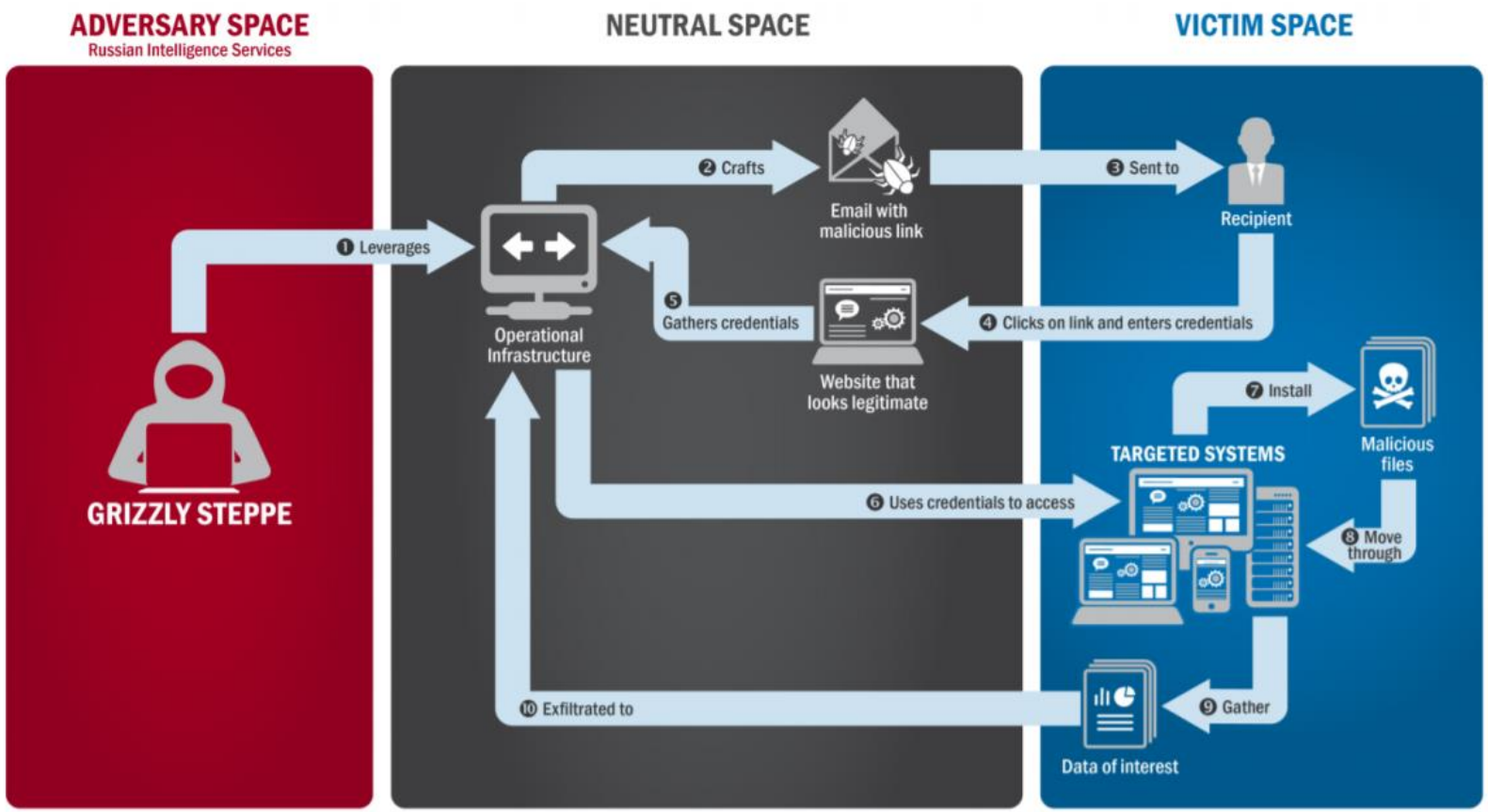


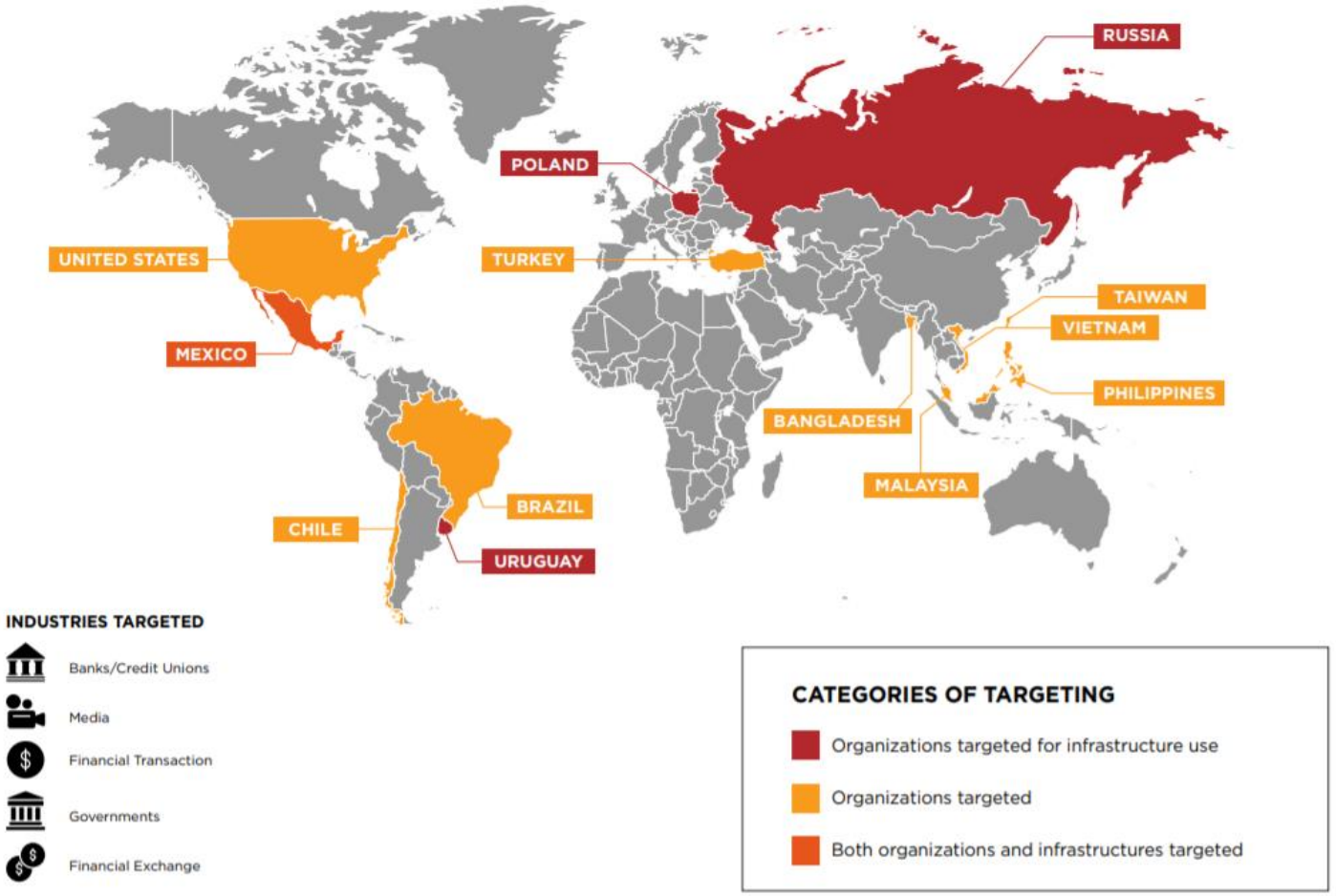
Figure 2: APT28's Use of Spearphishing and Stolen Credentials

APT38

- Gruparea Lazarus (Corea de Nord) a compormis 16 institutii financiare din 11 state;
- motivatie financiar-ideologica (transfer ilicit de fonduri in Corea de Nord);
- actiunile gruparii nu sunt corelate cu un efort diplomatic;
- rezida in reteaua victimei, in medie, 155 de zile;
- implementeaza malware distructiv la iesirea din retea;
- au incercat sa fure mai mult de 1,1 miliarde USD;
- https://content.fireeye.com/apt/rpt-apt38

APT38

- https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html



Tehnici si metode de reducere a riscului datorat APT

- back-up, analiza de risc, pregatirea personalului, scanarea de vulnerabilitati si aplicarea de patch-uri, aplicatiile autorizate, raspunsul la incidente, continuitatea misiunii;
- 7 strategii de reducere a riscurilor cu 85%:
  - aplicarea de patch-uri asupra aplicatiilor si sistemelor;
  - autorizarea aplicatiilor;
  - restrictionarea privilegiilor administrative;
  - segmentarea retelei si segregarea in zone de securitate;
  - validarea intrarilor;
  - configurarea antivirusului;
  - configurarea firewall-urilor;

Sase pasi de urmat in urma infectarii cu un ransomware

- Deconectati echipamentele infectate de la retea si efectuati toate procedurile de back-up offline, deoarece si back-up-ul poate fi infectat daca echipamentele sunt conectate permanent la retea.
- Activati planul de raspuns la incidente si nu tratati investigatia ca pe un simplu exercitiu IT. Asigurati-va o echipa mixta responsabila cu investigarea incidentului formata din reprezentanti ai departamentului juridic, ai celui de conformitate, securitate informatica, business, relatii publice, resurse umane si asa mai departe
- Identificati si raspundeti vunerabilitatilor din cadrul ecosistemului dumneavoastra conectat; instalati suficiente actualizari de securitate, de detectare malware si anti-virus pentru a complica eforturile atacatorilor de a reintra in retea; intariti capabilitatile de detectare si de raspuns la atacurile viitoare si pregatiti-va pentru masuri de eradicare.
- Asigurati-va ca sistemele sunt protejate cu mijloacele necesare de protectie inainte de a reconecta calculatoarele la retea. Mentineti sistemele actualizate cu un program bine pus la punct de management al vulnerabilitatilor la nivelul companiei. Acest program ar trebui sa includa un ciclu de viata formal, repetabil, pentru gestionarea vulnerabilitatilor si a evolutiei riscurilor, si un model care sa protejeze toate activele care pot fi afectate de aceste riscuri, inclusiv orice fel de conectivitate cu alte active.
- Activati planurile de continuitate a afacerii. Pregatiti toate informatiile necesare diverselor raportari legate de cerintele de reglementare, asigurari si litigii, informatii privind amenintarile infomatice si de notificare a clientilor.
- Colectati si pastrati dovezile intr-un format care sa raspunda cerintelor legale, astfel incat sa fie relevante pentru investigatii, corecte si utilizabile in situatia unor litigii civile sau investigatii ale autoritatilor competente.