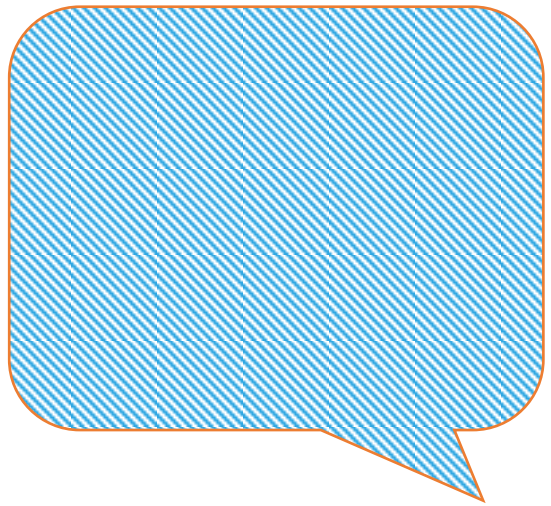
X JORNADAS STIC CCN-CERT

2006 2016

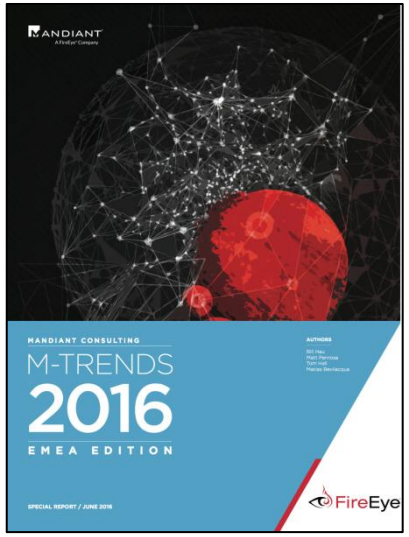
DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL

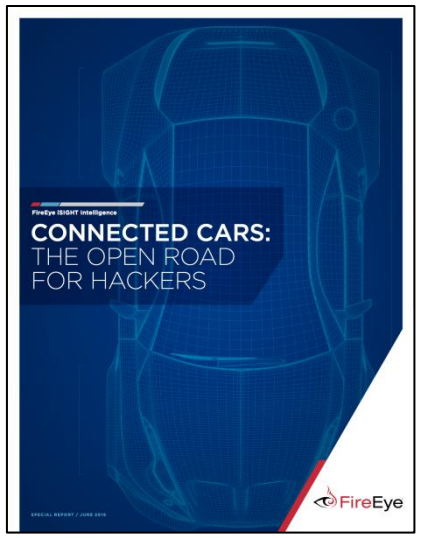
EVOLUCIÓN DE LAS APT EN 2016. TENDENCIAS

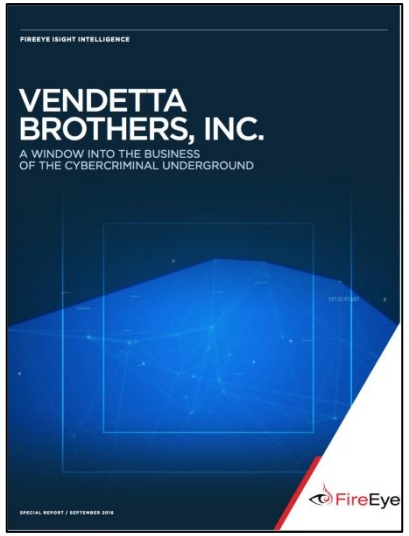


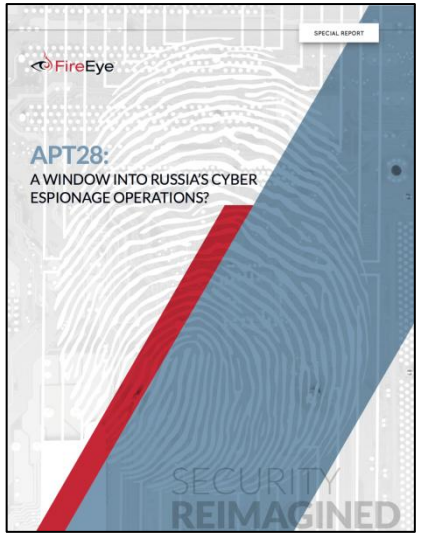
- Alvaro Garcia
- FireEye
- alvaro.garcia@fireeye.com

Índice







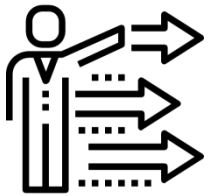


And.. Of course
Thanks to Jens Monrad
and iSight team.

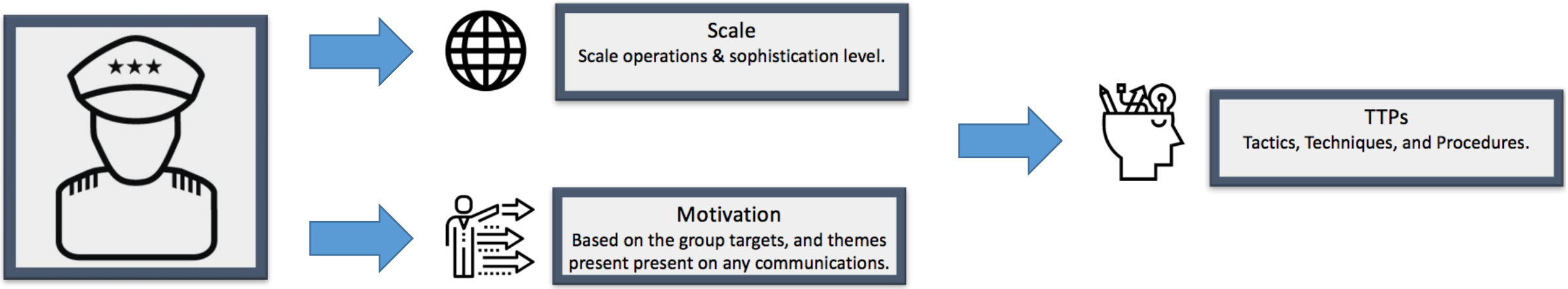
FireEye
SECURITY REIMAGINED

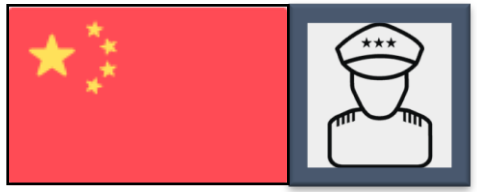
Scale
Scale operations & sophistication level.

TTPs
Tactics, Techniques, and Procedures.

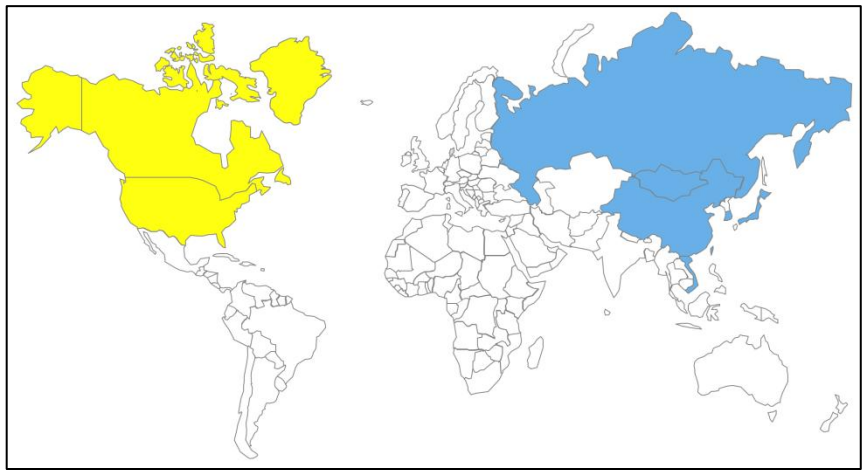


Motivation
Based on the group targets, and themes present present on any communications.


Scale
Scale operations & sophistication level.
Motivation
Based on the group targets, and themes present present on any communications.
TTPs
Tactics, Techniques, and Procedures.



APT19, APT10,APT26, APT30.



Reduce activity in 90% since Jun-2014.

China sea conflict.
Taiwan independency.

US and Europe financial services, space. education

72 active groups, no “monolith” behavior.

Conventional TTPs:
Phishing, known APT backdoors, DDOS.

Evolving to sophisticated TTPs:
ScanBox recon y new CnC methodology (aka Nflog, IsSpace, or Smac).

Complete new set of tools:
CnC Infrastructure, malware, etc.

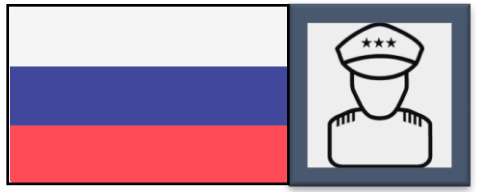
Therefore…

Diplomacy matters.

Army takes control of cybersecurity op.

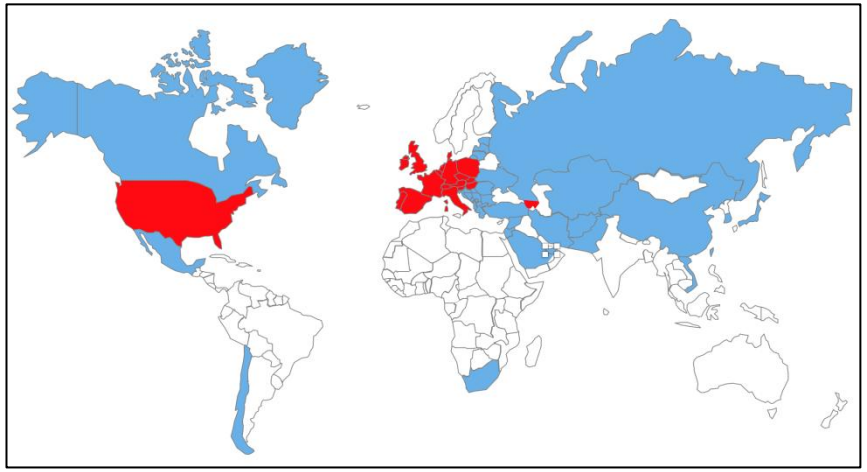
High OPSEC commercial targets.

Low OPSEC political targets.



APT28, APT29

a.k.a (TSAR TEAM, Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium / CozyDuke, CozyBear, SeaDuke, MiniDionis).



Due to Syria conflict & USA elections.

Ukraine and Syria conflict.

Not focus on financial interests.

Play offensive to from foreign espionage.

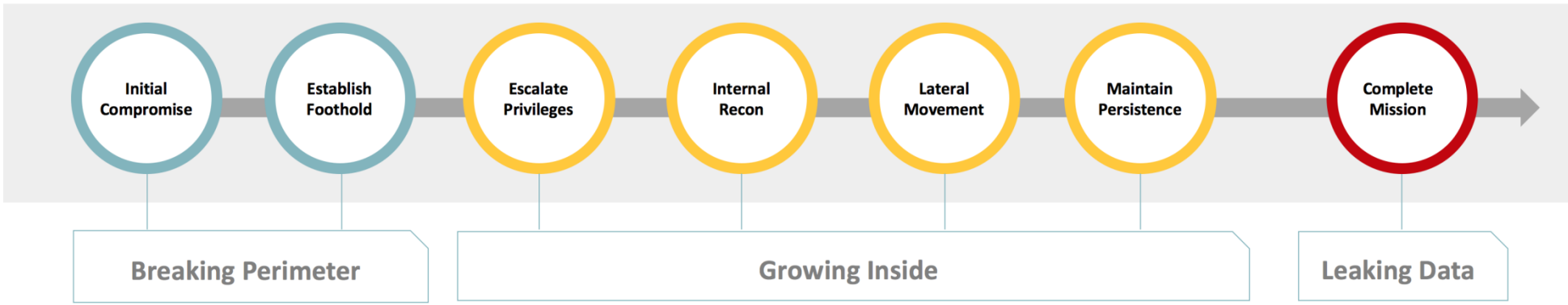
Exclusive set of tools:
Malware and scripting-based techniques.

Tailored, practiced and disciplined.

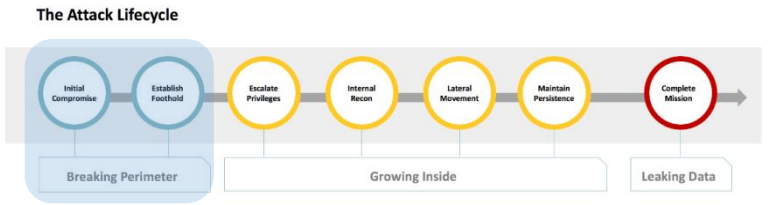
Novel TTPs:
From steganography, social networks exfiltration to compromised satellites.

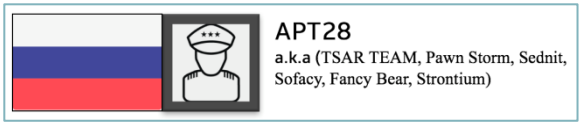
APT28
a.k.a (TSAR TEAM, Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium)

The Attack Lifecycle



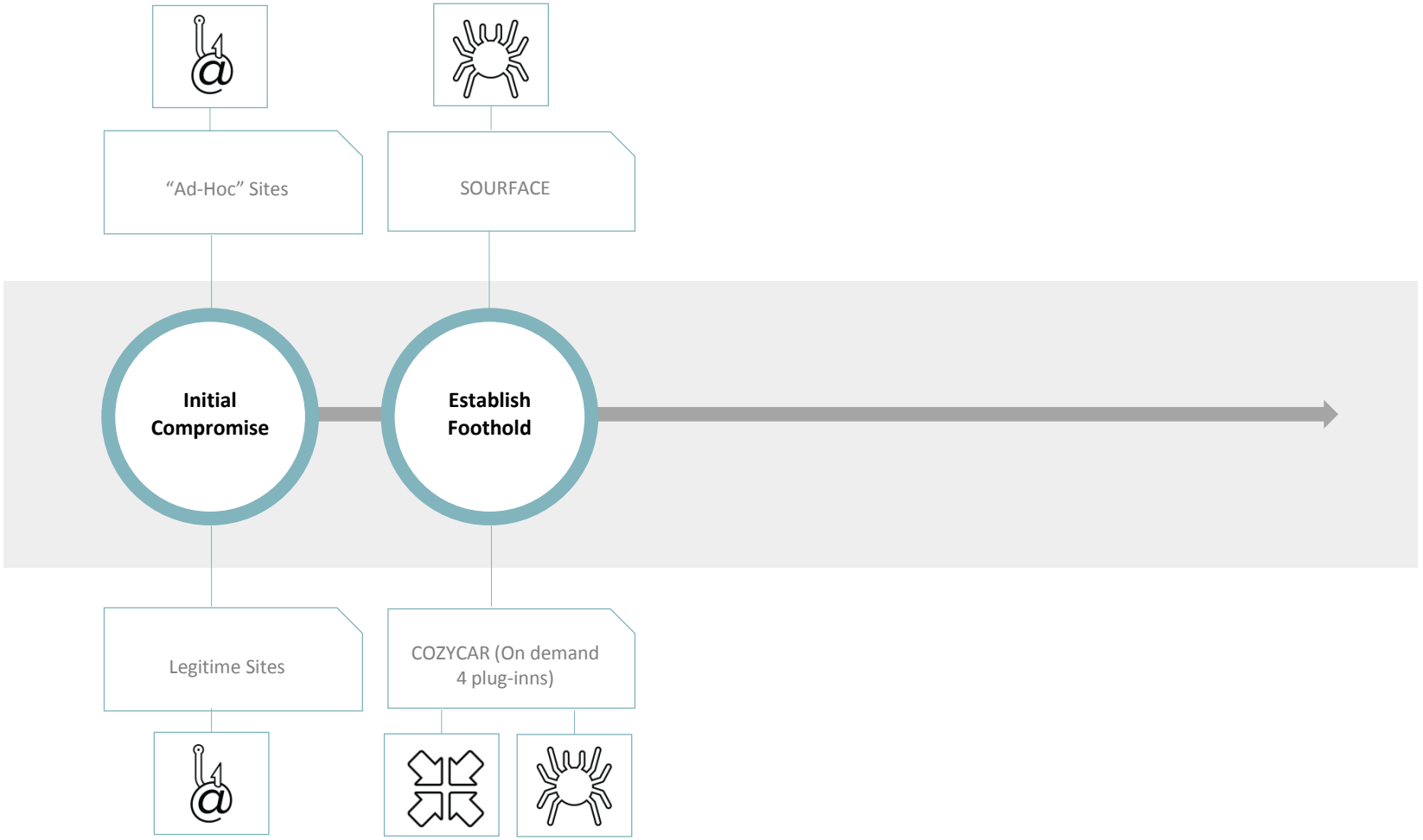
APT29.
a.k.a (CozyDuke, CozyBear, SeaDuke, MiniDionis)

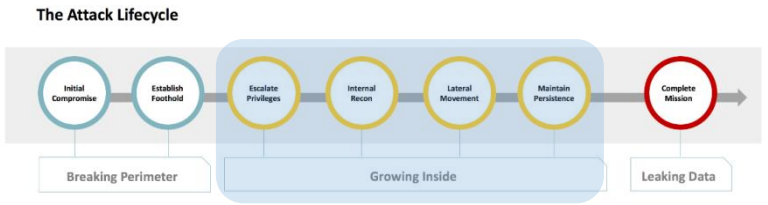


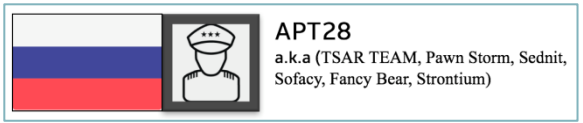


APT28
a.k.a (TSAR TEAM, Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium)

APT29.
a.k.a (CozyDuke, CozyBear, SeaDuke, MiniDionis)

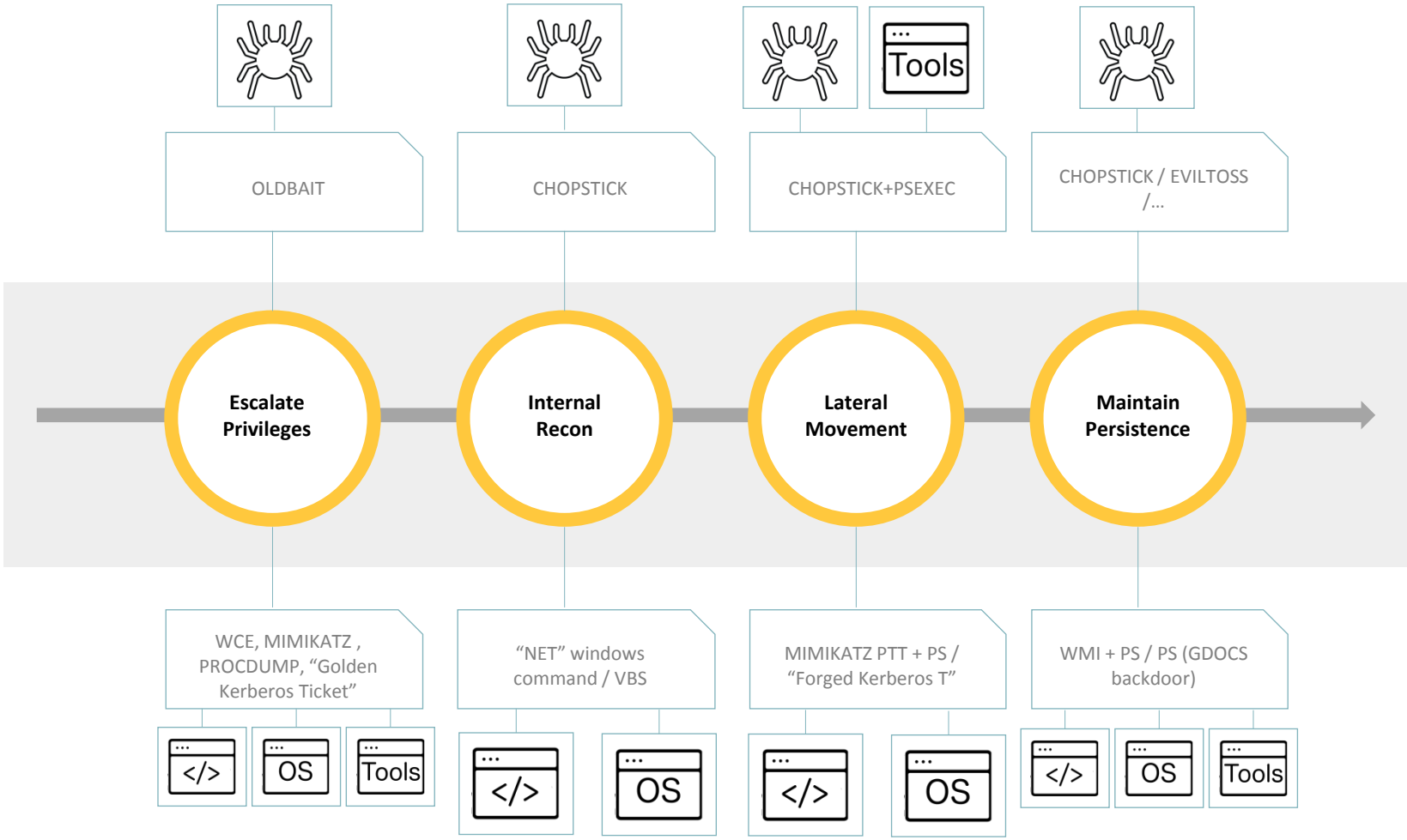


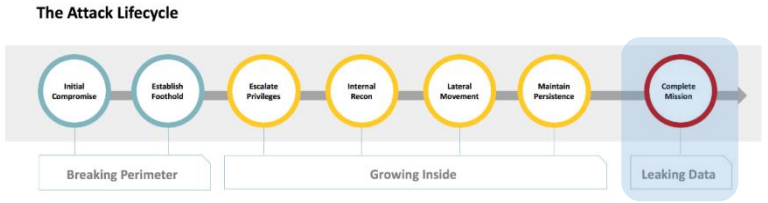


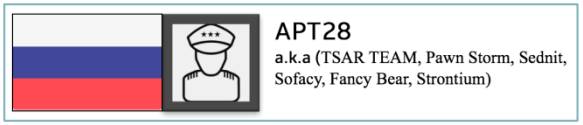


APT28
a.k.a (TSAR TEAM, Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium)

APT29.
a.k.a (CozyDuke, CozyBear, SeaDuke, MiniDionis)

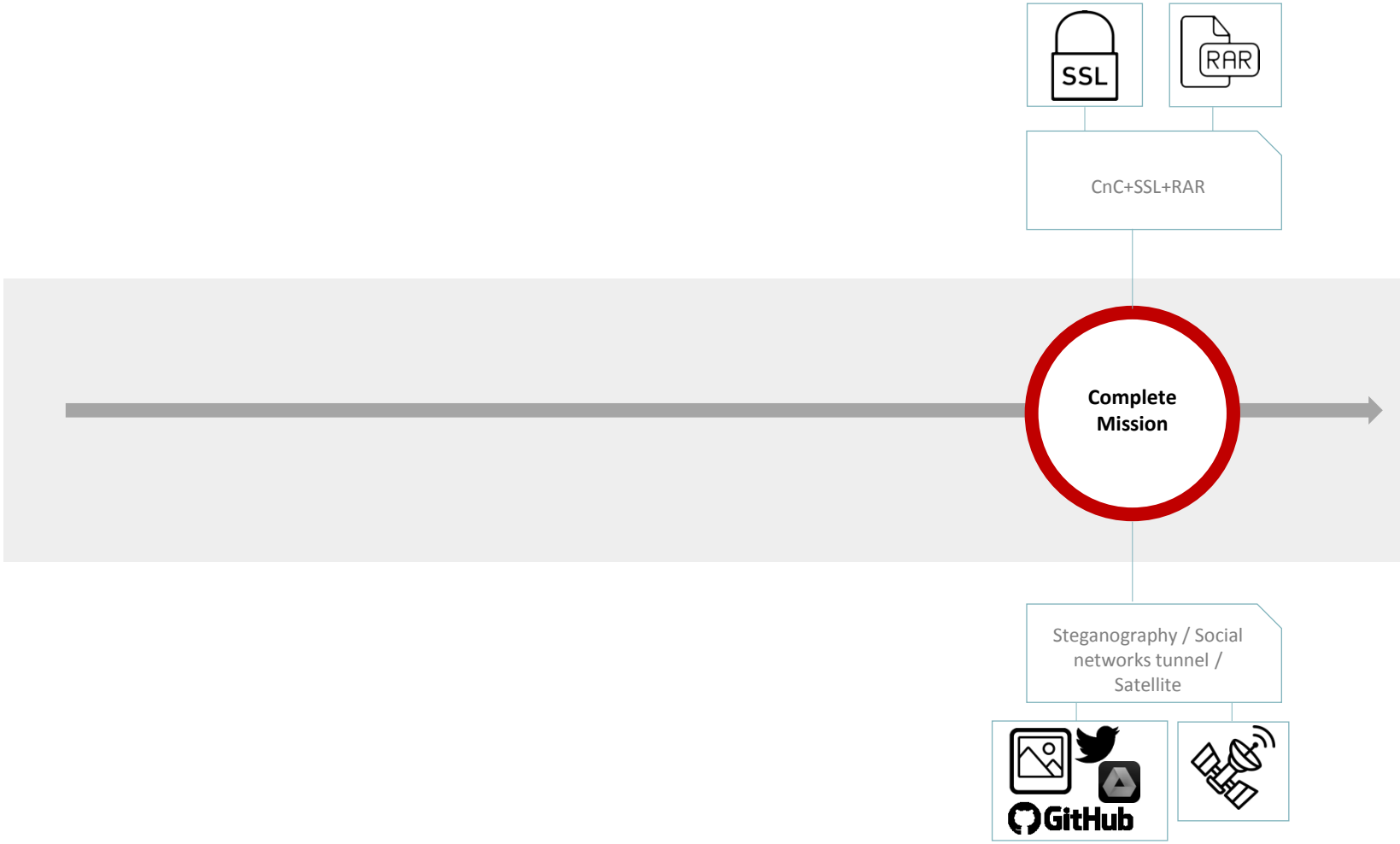


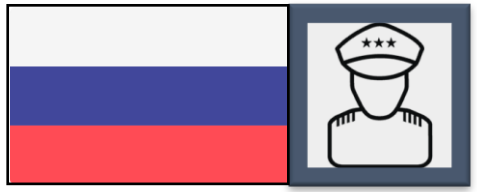




APT28
a.k.a (TSAR TEAM, Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium)

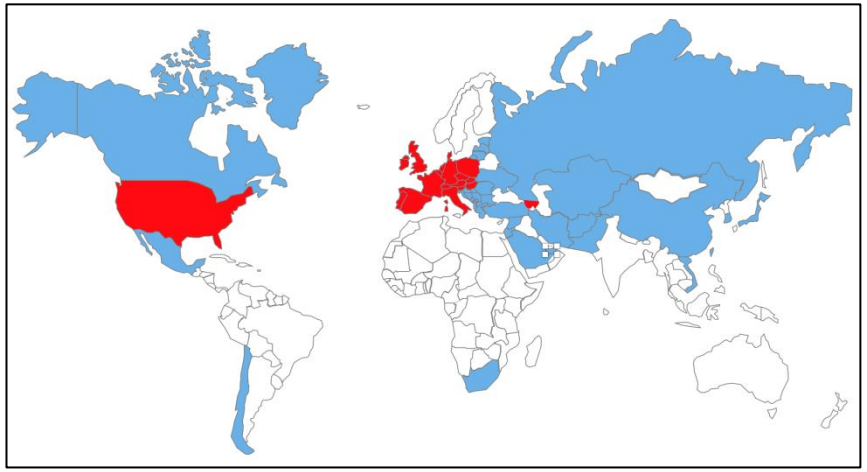
APT29.
a.k.a (CozyDuke, CozyBear, SeaDuke, MiniDionis)





APT28, APT29

a.k.a (TSAR TEAM, Pawn Storm, Sednit, Sofacy, Fancy Bear, Strontium / CozyDuke, CozyBear, SeaDuke, MiniDionis).



Due to Syria conflict & USA elections.

Ukraine and Syria conflict.

Not focus on financial interests.

Play offensive to from foreign espionage.

Exclusive set of tools:
Malware and scripting-based techniques.

Tailored, practiced and disciplined.

Novel TTPs:
From steganography, social networks exfiltration to compromised satellites.

Therefore…

Military dictates their activities in cyberspace.

Extending fast its activity's scope.

Not enough OPSEC (more visible).


COSTS
BENEFITS

Group Profile: The 'Vendetta Crew'

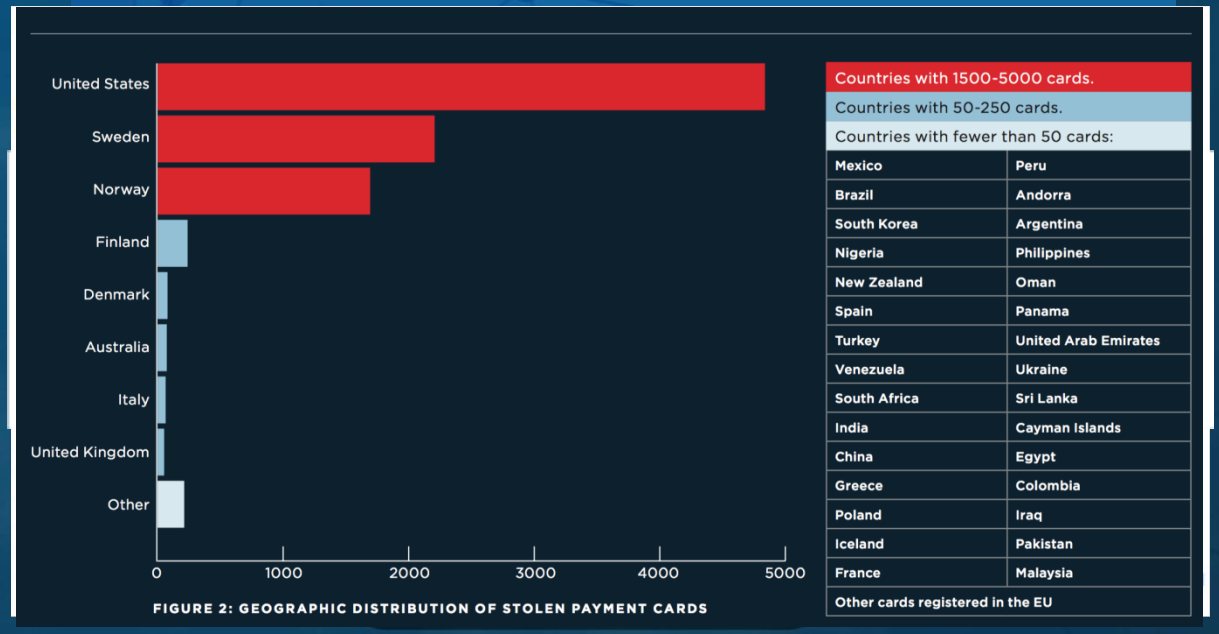


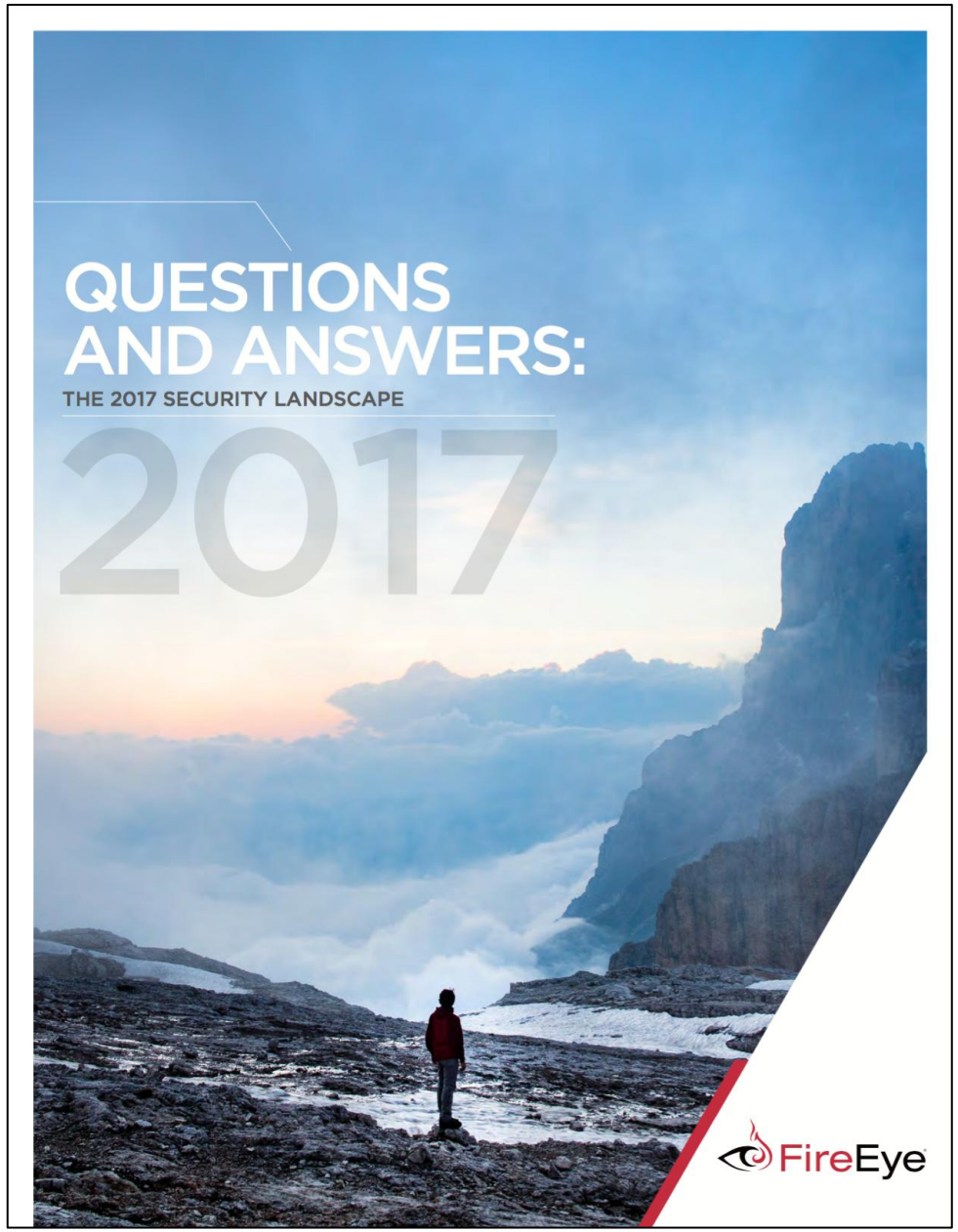
FIGURE 2: GEOGRAPHIC DISTRIBUTION OF STOLEN PAYMENT CARDS

Countries with 1500-5000 cards.	
Countries with 50-250 cards.	
Countries with fewer than 50 cards:	
Mexico	Peru
Brazil	Andorra
South Korea	Argentina
Nigeria	Philippines
New Zealand	Oman
Spain	Panama
Turkey	United Arab Emirates
Venezuela	Ukraine
South Africa	Sri Lanka
India	Cayman Islands
China	Egypt
Greece	Colombia
Poland	Iraq
Iceland	Pakistan
France	Malaysia
Other cards registered in the EU	

Key Findings:

- Team of 2 hackers.
- Outsourcing compromised POS / R.Sharing.
- Reselling of skimmers / Tools / Know-how.
- Customer satisfaction / 24h ICQ Support.

639 banks, 40 countries. U.S, and Nordics.



- Use of PPTM and DOTM formats on phishing attacks.
- Use of scripting recon tools + encrypted malware payload.
- ICS will be on the spot. 30% of the vulnerabilities doesn't have patch.
- IoT will lead new cybercrime abuses. I.E Ransomware over vehicles, public transport (I.E San Francisco Metro Nov-2016).

FireEye SECURITY REIMAGINED

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en