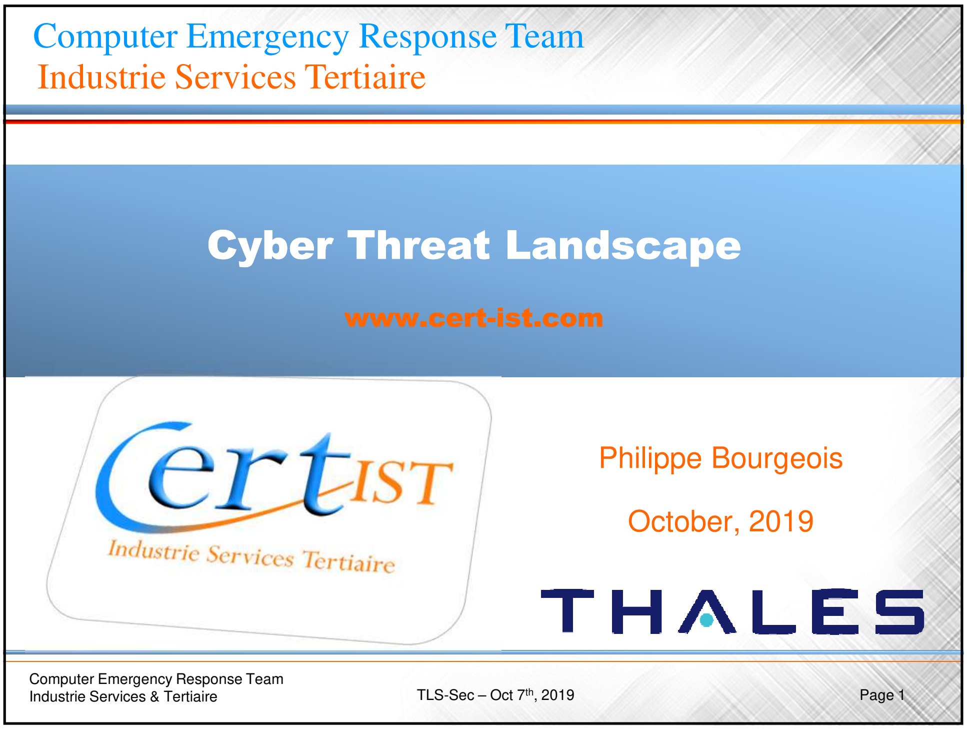


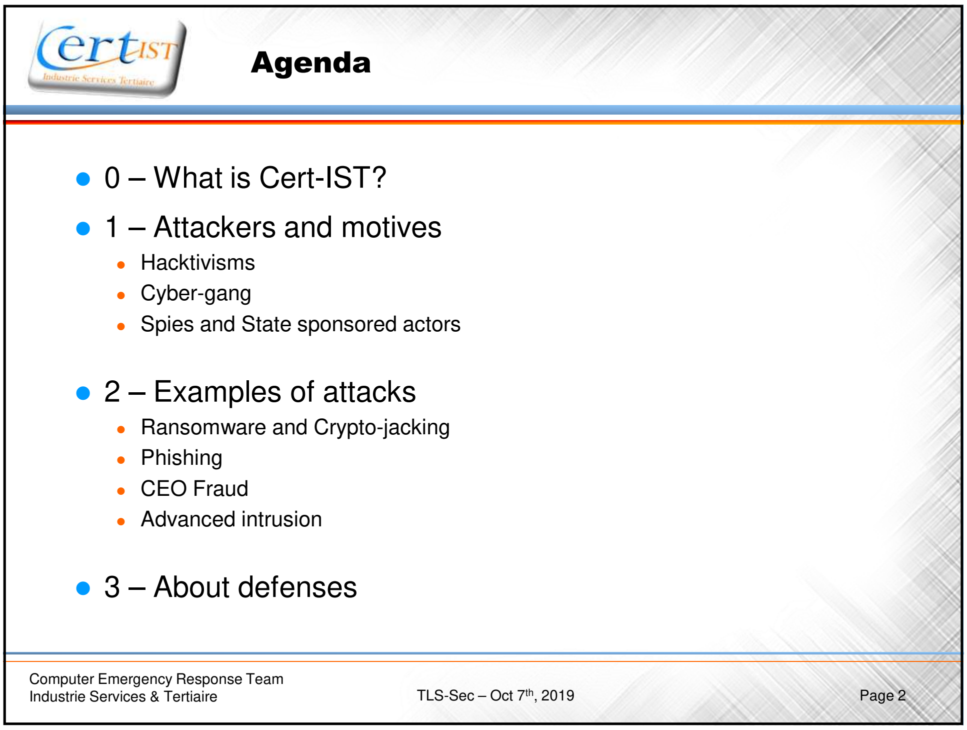
Computer Emergency Response Team
Industrie Services Tertiaire

Cyber Threat Landscape

www.cert-ist.com

Philippe Bourgeois

October, 2019



Agenda

- 0 – What is Cert-IST?
- 1 – Attackers and motives
  - Hacktivisms
  - Cyber-gang
  - Spies and State sponsored actors
- 2 – Examples of attacks
  - Ransomware and Crypto-jacking
  - Phishing
  - CEO Fraud
  - Advanced intrusion
- 3 – About defenses

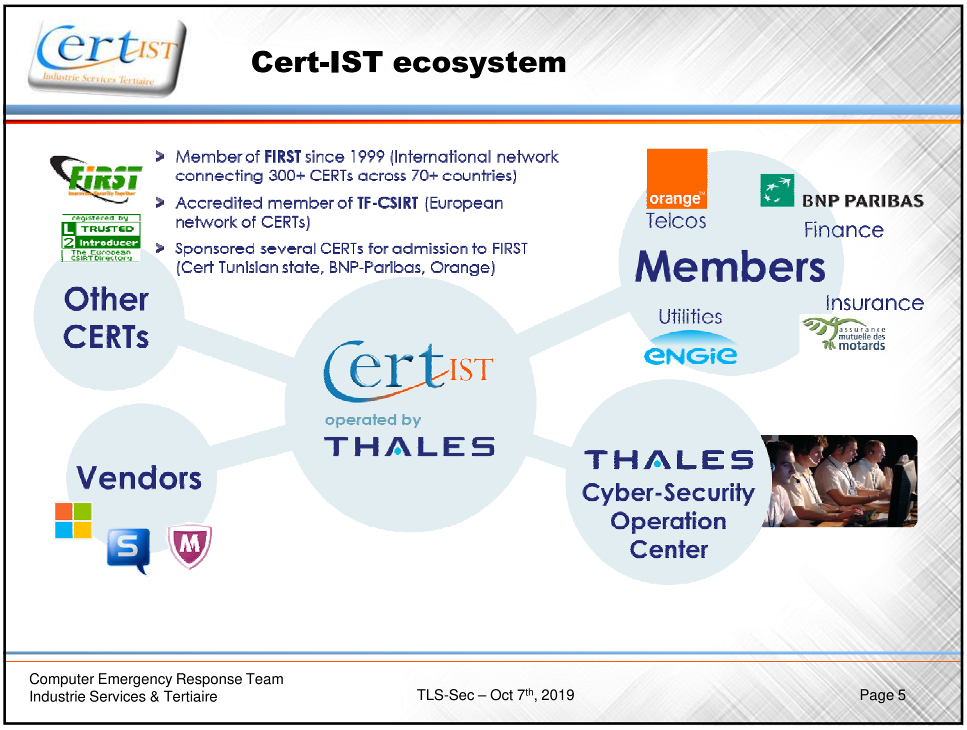
Computer Emergency Response Team
Industrie Services Tertiaire

What is Cert-IST?

Cert IST
Industrie Services Tertiaire

What is Cert-IST?

- Center dedicated to vulnerabilities and attacks mitigations
  - Cert-IST is a CERT team (Computer Emergency Response Team) for IST (Industries, Services and Tertiary sectors)
  - Located in France
- Cert-IST provides services to its members
  - Cyber Threats Watch & Alert , through:
    - Security advisories on vulnerabilities
    - Alerts about expected or on-going attacks
    - Datasheets on disclosed Attacks (with IOC : Indicators Of Compromise)
    - Daily press reviews and monthly & yearly reports on threat landscape
  - Support to deal with incidents
    - Share information on incidents
    - Technical expertise



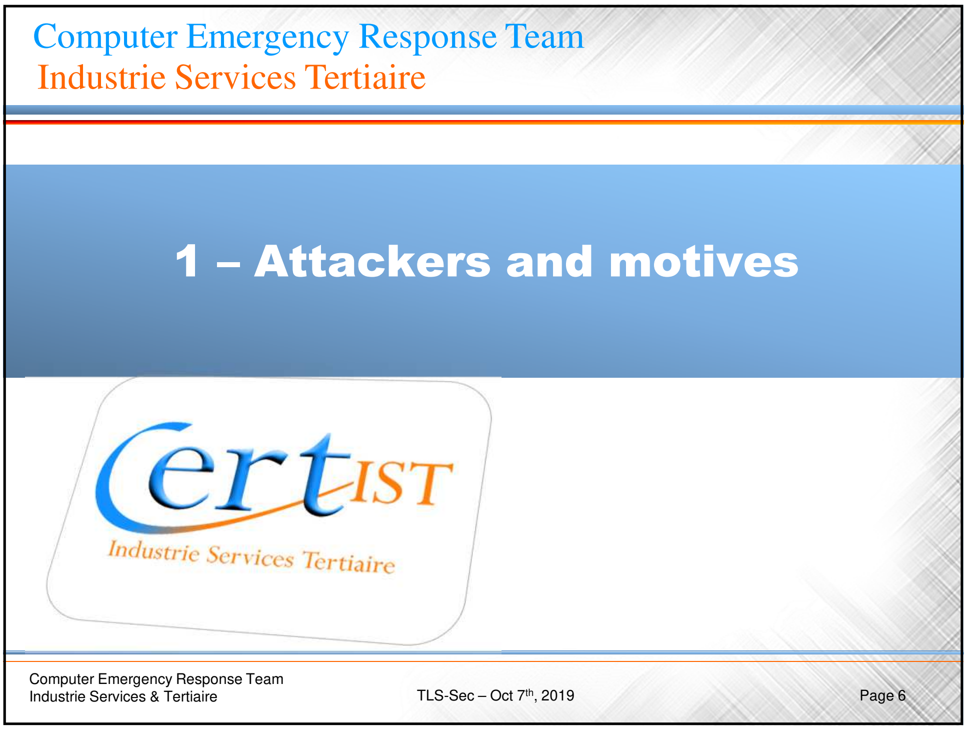
Cert-IST ecosystem

- Member of **FIRST** since 1999 (International network connecting 300+ CERTs across 70+ countries)
- Accredited member of **TF-CSIRT** (European network of CERTs)
- Sponsored several CERTs for admission to FIRST (Cert Tunisian state, BNP-Paribas, Orange)

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 5



Computer Emergency Response Team
Industrie Services Tertiaire

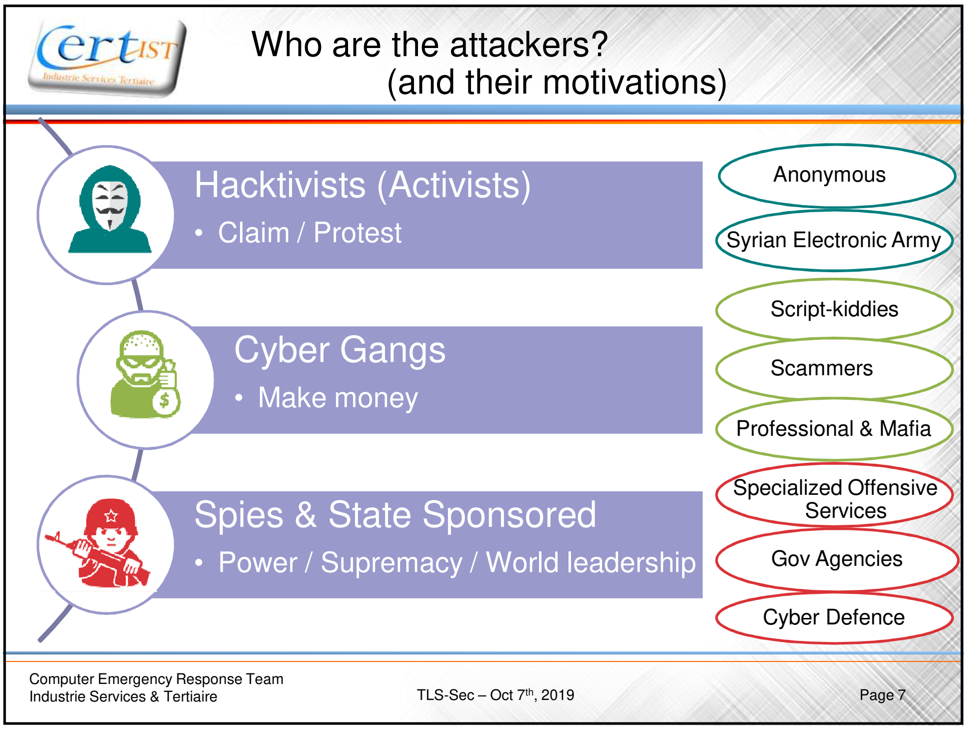
1 – Attackers and motives

Cert IST
Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 6



Who are the attackers?
(and their motivations)

Hacktivists (Activists)

- Claim / Protest

Anonymous

Syrian Electronic Army

Cyber Gangs

- Make money

Script-kiddies

Scammers

Professional & Mafia

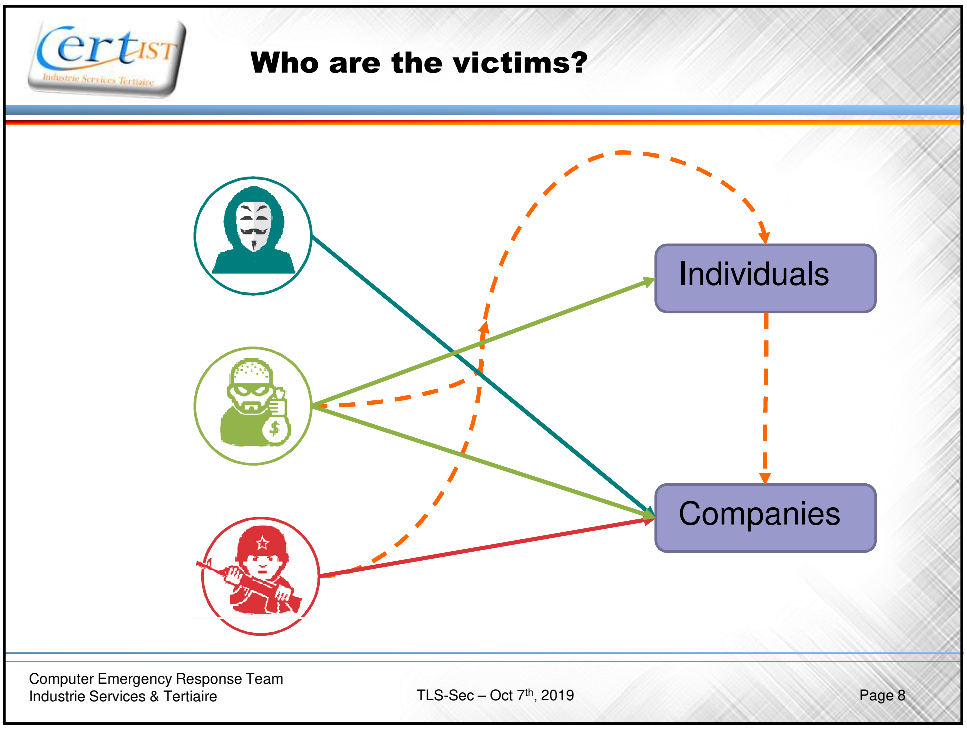
Spies & State Sponsored

- Power / Supremacy / World leadership

Specialized Offensive Services

Gov Agencies

Cyber Defence



Who are the victims?

Individuals

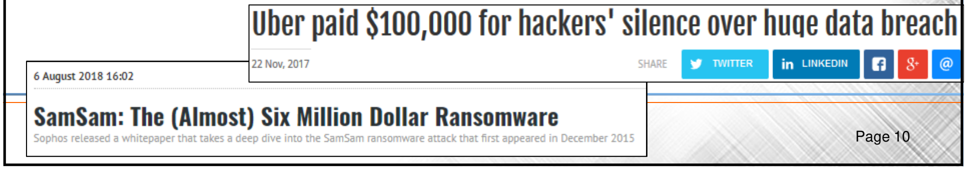
Companies

Hacktivists

- Motivations
  - Political claims / Use IT attacks to protest or act
  - Highly motivated, but limited resources
- Actions
  - Opportunist attacks on « low hanging fruits » to catch media attention
  - DDOS, web site Defacements, Doxxing (publish companies internal data)
- Examples
  - DDOS of MasterCard and Visa (Anonymous – 2010)
  - Takeover of Twitter accounts (SEA – 2013)
    - E.g. New York Times and Huffington Post (UK)
- Real threat for companies but on decline after 2013
  - Very severe sentences against identified attackers

Cyber Gangs

- Motivations
  - Make money
  - Range from no-skill scammers to professional cyber-crime ecosystem (including: The Boss, Developers, Infrastructure Operators, Sellers, etc.)
- Actions
  - Scam : from Nigerian Prince (4-1-9 frauds) to CEO Fraud (BEC)
  - Ransomware, Crypto-jacking against individuals or single computer
  - Blackmail (DOS or IT Destruction) against companies
  - Advanced intrusions and extortion schemes (Bank heist)
  - Etc.
- Target both individuals and companies
  - Annoyances that could cost a lot of money



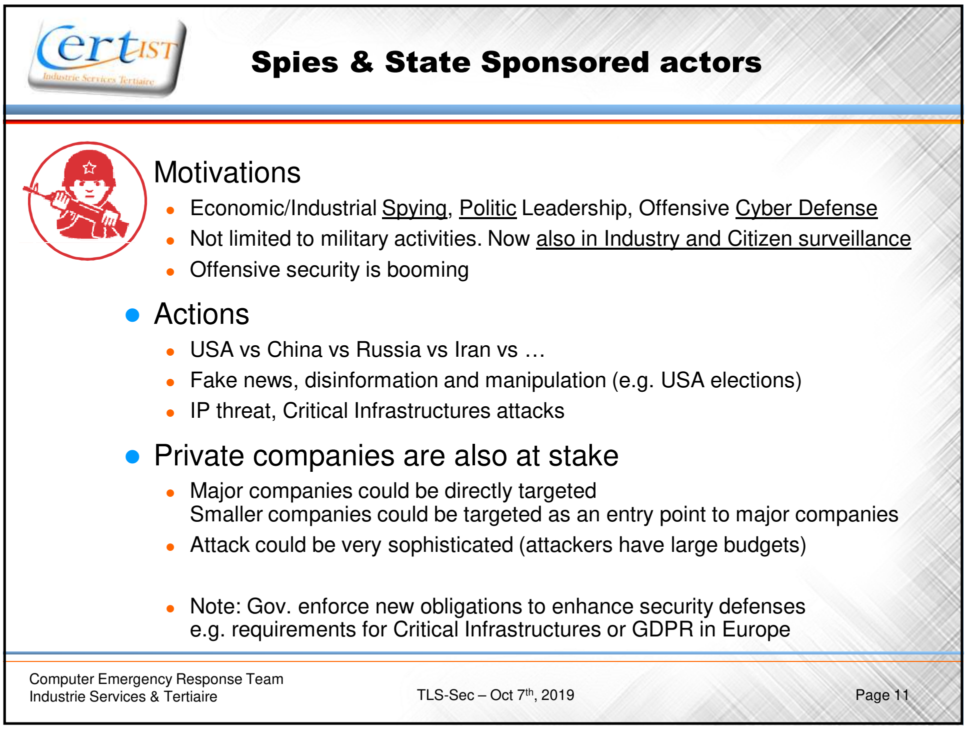
Uber paid $100,000 for hackers' silence over huge data breach

22 Nov, 2017

6 August 2018 16:02

SamSam: The (Almost) Six Million Dollar Ransomware

Sophos released a whitepaper that takes a deep dive into the SamSam ransomware attack that first appeared in December 2015



Spies & State Sponsored actors

Motivations

- Economic/Industrial Spying, Politic Leadership, Offensive Cyber Defense
- Not limited to military activities. Now also in Industry and Citizen surveillance
- Offensive security is booming

Actions

- USA vs China vs Russia vs Iran vs …
- Fake news, disinformation and manipulation (e.g. USA elections)
- IP threat, Critical Infrastructures attacks

Private companies are also at stake

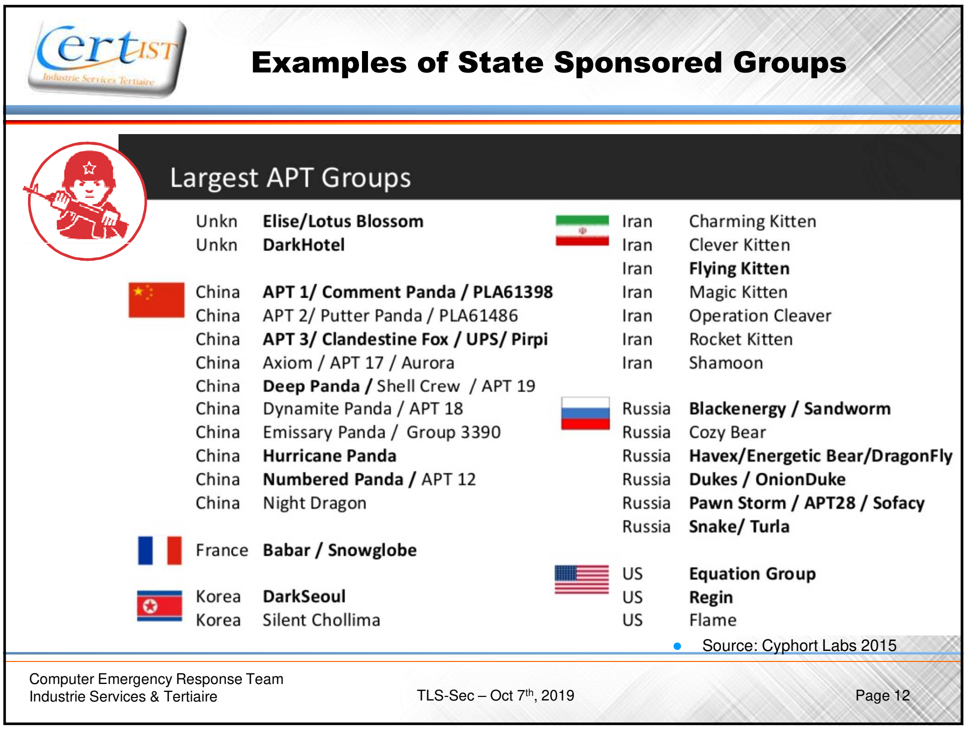
- Major companies could be directly targeted
  Smaller companies could be targeted as an entry point to major companies
- Attack could be very sophisticated (attackers have large budgets)

- Note: Gov. enforce new obligations to enhance security defenses
  e.g. requirements for Critical Infrastructures or GDPR in Europe

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 11



Examples of State Sponsored Groups

Largest APT Groups

Unkn	**Elise/Lotus Blossom**
Unkn	**DarkHotel**
China	**APT 1/ Comment Panda / PLA61398**
China	APT 2/ Putter Panda / PLA61486
China	**APT 3/ Clandestine Fox / UPS/ Pirpi**
China	Axiom / APT 17 / Aurora
China	**Deep Panda /** Shell Crew / APT 19
China	Dynamite Panda / APT 18
China	Emissary Panda / Group 3390
China	**Hurricane Panda**
China	**Numbered Panda /** APT 12
China	Night Dragon
France	**Babar / Snowglobe**
Korea	**DarkSeoul**
Korea	Silent Chollima

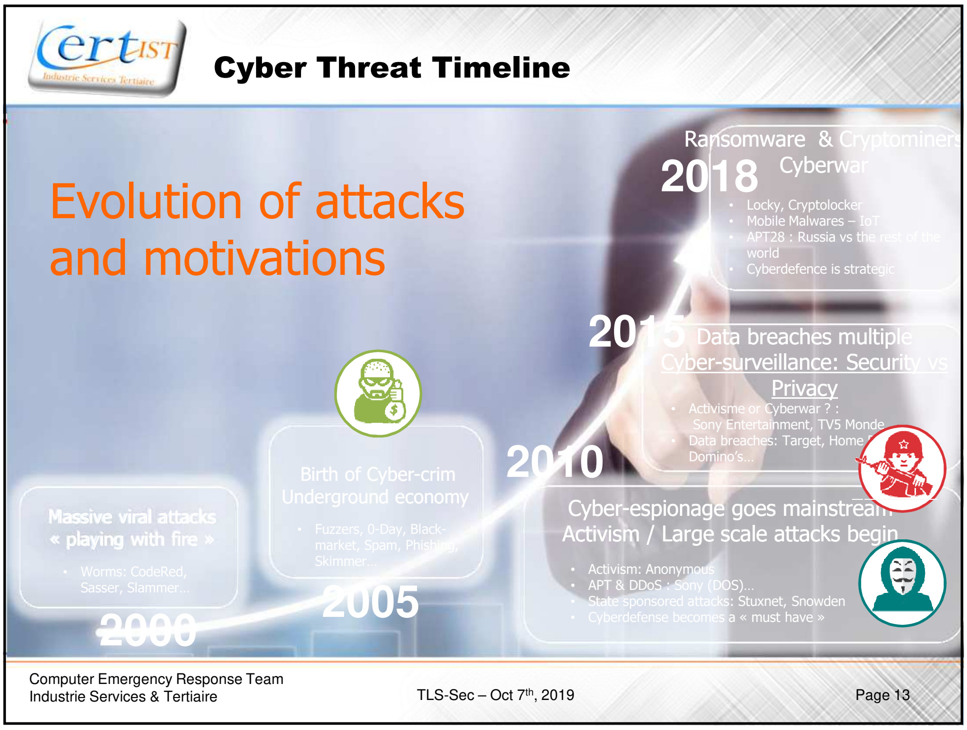
Iran	Charming Kitten
Iran	Clever Kitten
Iran	**Flying Kitten**
Iran	Magic Kitten
Iran	Operation Cleaver
Iran	Rocket Kitten
Iran	Shamoon
Russia	**Blackenergy / Sandworm**
Russia	Cozy Bear
Russia	**Havex/Energetic Bear/DragonFly**
Russia	**Dukes / OnionDuke**
Russia	**Pawn Storm / APT28 / Sofacy**
Russia	**Snake/ Turla**
US	**Equation Group**
US	**Regin**
US	Flame

- Source: Cyphort Labs 2015

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 12



Cyber Threat Timeline

Evolution of attacks and motivations

2000

Massive viral attacks « playing with fire »

- Worms: CodeRed, Sasser, Slammer…

2005

Birth of Cyber-crim Underground economy

- Fuzzers, 0-Day, Black-market, Spam, Phishing, Skimmer…

2010

Cyber-espionage goes mainstream
Activism / Large scale attacks begin

- Activism: Anonymous
- APT & DDoS : Sony (DOS)…
- State sponsored attacks: Stuxnet, Snowden
- Cyberdefense becomes a « must have »

2015 Data breaches multiple
Cyber-surveillance: Security vs Privacy

- Activisme or Cyberwar ? : Sony Entertainment, TV5 Monde
- Data breaches: Target, Home D… Domino's…

2018

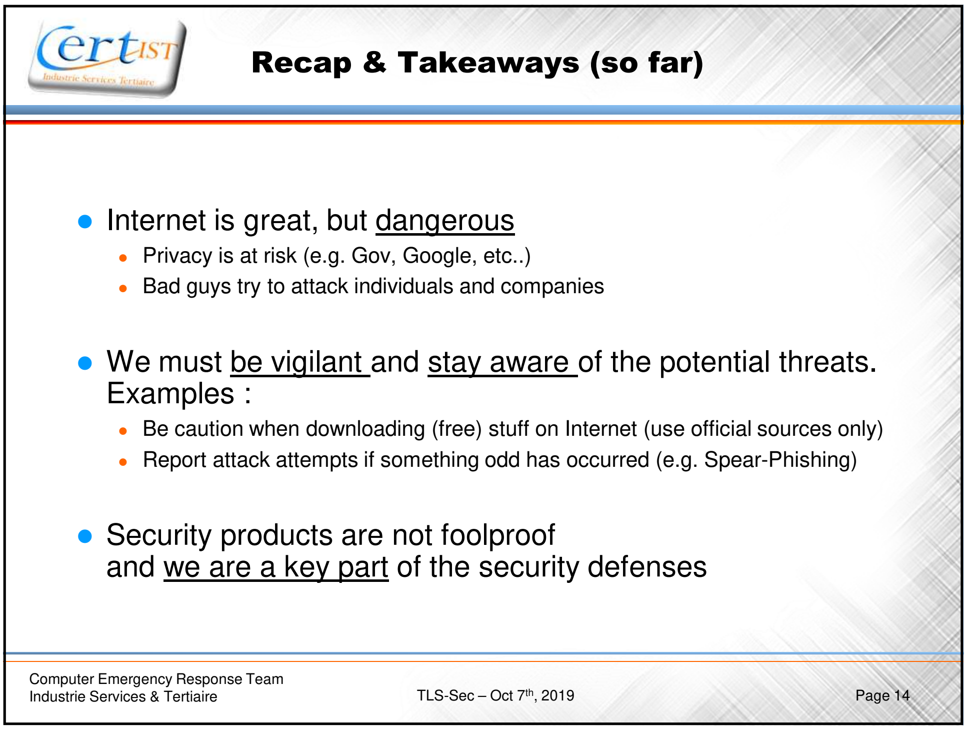
Ransomware & Cryptominers
Cyberwar

- Locky, Cryptolocker
- Mobile Malwares – IoT
- APT28 : Russia vs the rest of the world
- Cyberdefence is strategic

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 13



Recap & Takeaways (so far)

- Internet is great, but dangerous
  - Privacy is at risk (e.g. Gov, Google, etc..)
  - Bad guys try to attack individuals and companies
- We must be vigilant and stay aware of the potential threats. Examples :
  - Be caution when downloading (free) stuff on Internet (use official sources only)
  - Report attack attempts if something odd has occurred (e.g. Spear-Phishing)
- Security products are not foolproof
  and we are a key part of the security defenses

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

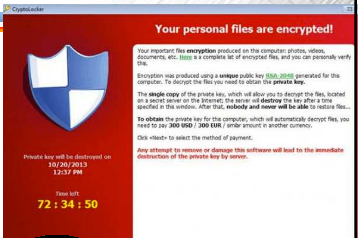
Page 14

Computer Emergency Response Team
Industrie Services Tertiaire

2 – Examples of Attacks

Ransomware & Crypto-jacking

- They are the most common attacks today
- Ransomware :
  - Pay a ransom to get your files back
  - Now tries to infect large organisations (Hospitals, City administration, etc.) with RansomWorm
- Cryptojacking (Crypto-money Hijacking)
  - Illegally use CPUs to mine crypto-money (Mostly « Monero » instead of « Bitcoins »)
  - Large farms of infected CPUs required to make enough money (including Amazon AWS, Docker, etc..)
- Microsoft Technicians Scams



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

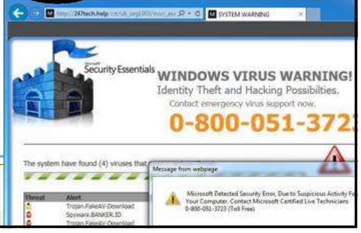
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50



WINDOWS VIRUS WARNING!
Identity Theft and Hacking Possibilties.
Contact emergency virus support now.
0-800-051-372

The system have found (4) viruses that

Threat	Alert
	Trojan.FakeAV-Download
	Spyware.BANKER.ID
	Trojan.FakeAV-Download

Microsoft Detected Security Error, Due to Suspicious Activity Fo
Your Computer. Contact Microsoft Certified Live Technicians
0-800-051-3723 (Toll Free)

Phishing

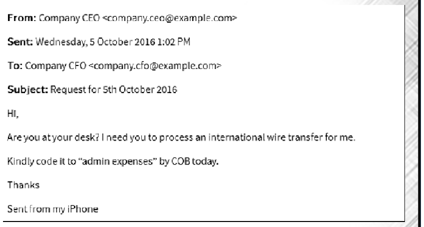
- Please, give me your password

- Or any attempt to trap a email recipient
  - Check your Bank account
  - Open this attachment
  - Go on that web site
- Phishing vs Spear-phishing

Cyber Criminals are 'fishers of men'
what's the difference?
PHISHING
IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.
SPEAR-PHISHING
IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY
ATLANTA
#SNH18

Phishing examples

- CEO Fraud (aka BEC: Business Email Compromise)



From: Company CEO <company.ceo@example.com>

Sent: Wednesday, 5 October 2016 1:02 PM

To: Company CFO <company.cfo@example.com>

Subject: Request for 5th October 2016

HI,

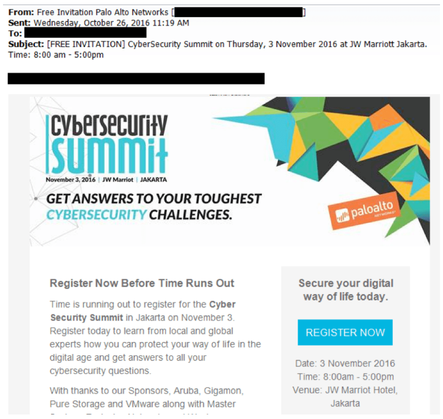
Are you at your desk? I need you to process an international wire transfer for me.

Kindly code it to "admin expenses" by COB today.

Thanks

Sent from my iPhone

- Cyber-espionage attempt
  (here: Chinese APT « Lotus Blossom »)



From: Free Invitation Palo Alto Networks [[redacted]]
Sent: Wednesday, October 26, 2016 11:19 AM
To: [redacted]
Subject: [FREE INVITATION] CyberSecurity Summit on Thursday, 3 November 2016 at JW Marriott Jakarta.
Time: 8:00 am - 5:00pm

[redacted]

CYBERSECURITY
SUMMIT
November 3, 2016 | JW Marriot | JAKARTA
GET ANSWERS TO YOUR TOUGHEST CYBERSECURITY CHALLENGES.
paloalto

Register Now Before Time Runs Out

Time is running out to register for the **Cyber Security Summit** in Jakarta on November 3. Register today to learn from local and global experts how you can protect your way of life in the digital age and get answers to all your cybersecurity questions.

With thanks to our Sponsors, Aruba, Gigamon, Pure Storage and VMware along with Master

Secure your digital way of life today.

Date: 3 November 2016
Time: 8:00am - 5:00pm
Venue: JW Marriot Hotel, Jakarta

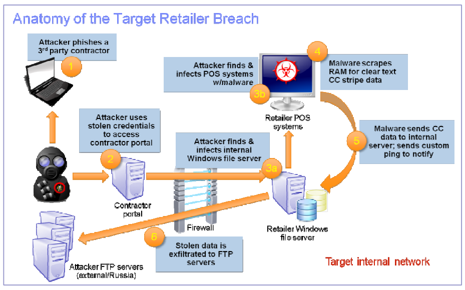
Advanced intrusions

- Use elaborated intrusion scenario
  - From the begining in the espionage world (aka J. Bond 007)
  - Goes mainstream in 2010
  - Often called « APT » : Advanced Persistent Threat

- Intrusion can last 200 days (Staying under the radar)
  - Prepare
  - Infect one computer (« patient zero »)
  - Lateral movement within the company
  - Exfiltrate, sabotage, etc.

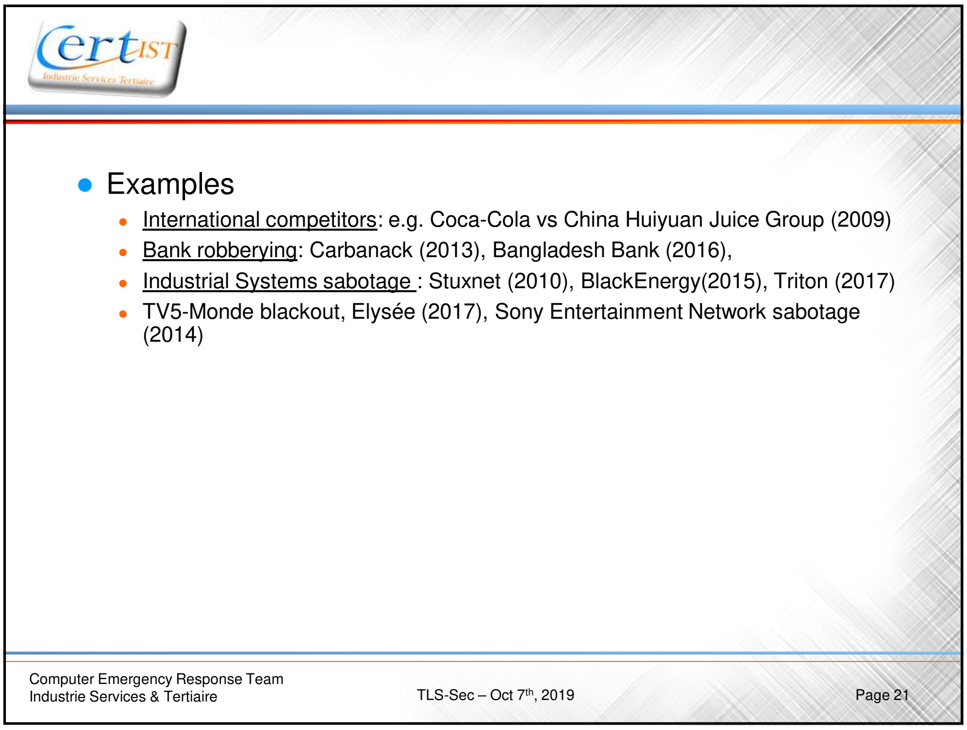
Examples of an Advanced intrusions

- December 2013 : Target retailer incident


Anatomy of the Target Retailer Breach
1
Attacker phishes a 3rd party contractor
2
Attacker uses stolen credentials to access contractor portal
Contractor portal
Firewall
3a
Attacker finds & infects internal Windows file server
3b
Attacker finds & infects POS systems w/malware
Retailer POS systems
4
Malware scrapes RAM for clear text CC stripe data
5
Malware sends CC data to internal server; sends custom ping to notify
Retailer Windows file server
6
Stolen data is exfiltrated to FTP servers
Attacker FTP servers (external/Russia)
Target internal network

[source: SecurityIntelligence.com]

- Rely on
  - Spear-phishing
  - Stealing Windows credentials
  - Supply-chain attack

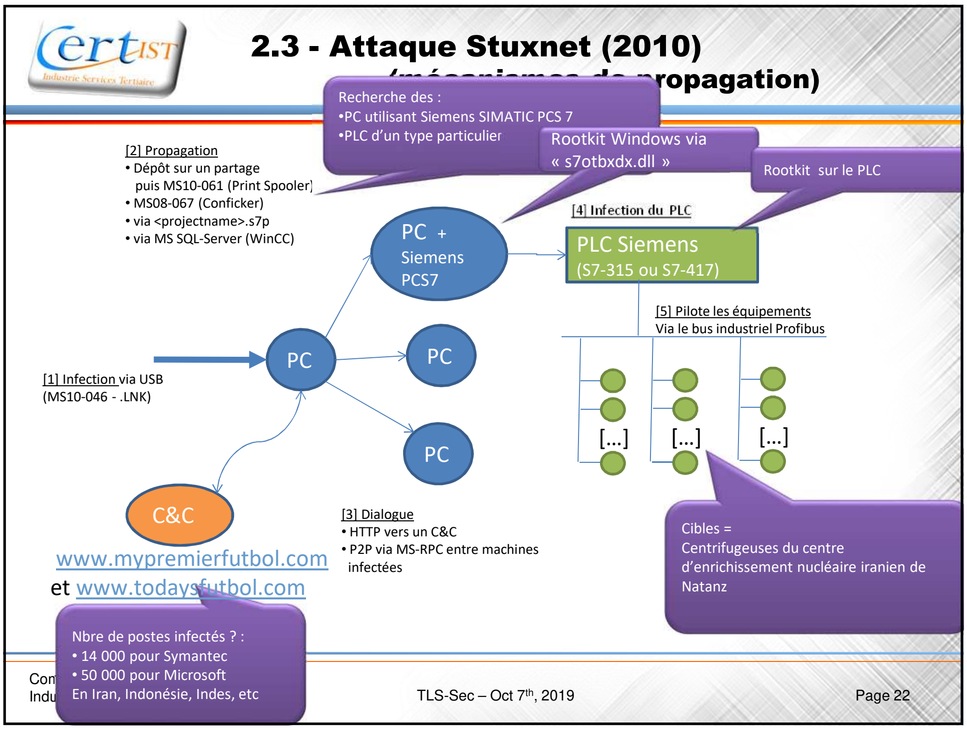


- Examples
  - International competitors: e.g. Coca-Cola vs China Huiyuan Juice Group (2009)
  - Bank robberying: Carbanack (2013), Bangladesh Bank (2016),
  - Industrial Systems sabotage : Stuxnet (2010), BlackEnergy(2015), Triton (2017)
  - TV5-Monde blackout, Elysée (2017), Sony Entertainment Network sabotage (2014)

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 21



2.3 - Attaque Stuxnet (2010) (mécanismes de propagation)

Recherche des :
•PC utilisant Siemens SIMATIC PCS 7
•PLC d'un type particulier

Rootkit Windows via « s7otbxdx.dll »

Rootkit sur le PLC

[2] Propagation
- Dépôt sur un partage puis MS10-061 (Print Spooler)
- MS08-067 (Conficker)
- via <projectname>.s7p
- via MS SQL-Server (WinCC)

[4] Infection du PLC

[5] Pilote les équipements
Via le bus industriel Profibus

[1] Infection via USB
(MS10-046 - .LNK)

[3] Dialogue
- HTTP vers un C&C
- P2P via MS-RPC entre machines infectées

www.mypremierfutbol.com
et www.todaysfutbol.com

Cibles =
Centrifugeuses du centre d'enrichissement nucléaire iranien de Natanz

Nbre de postes infectés ? :
- 14 000 pour Symantec
- 50 000 pour Microsoft

En Iran, Indonésie, Indes, etc

Com
Indu

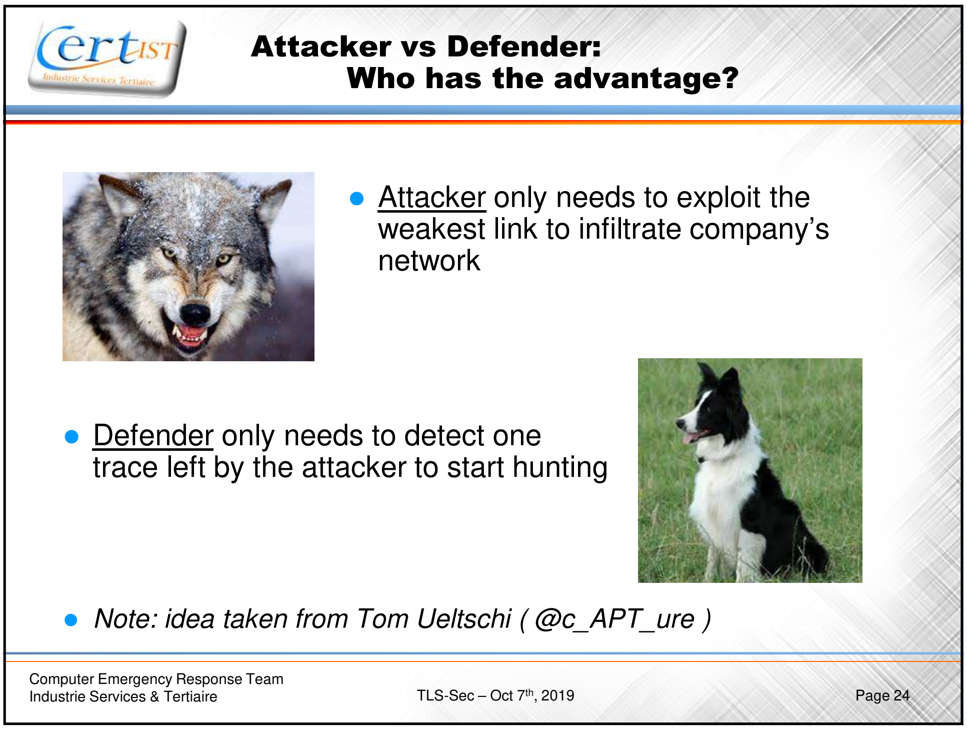
TLS-Sec – Oct 7th, 2019

Page 22

Computer Emergency Response Team
Industrie Services Tertiaire

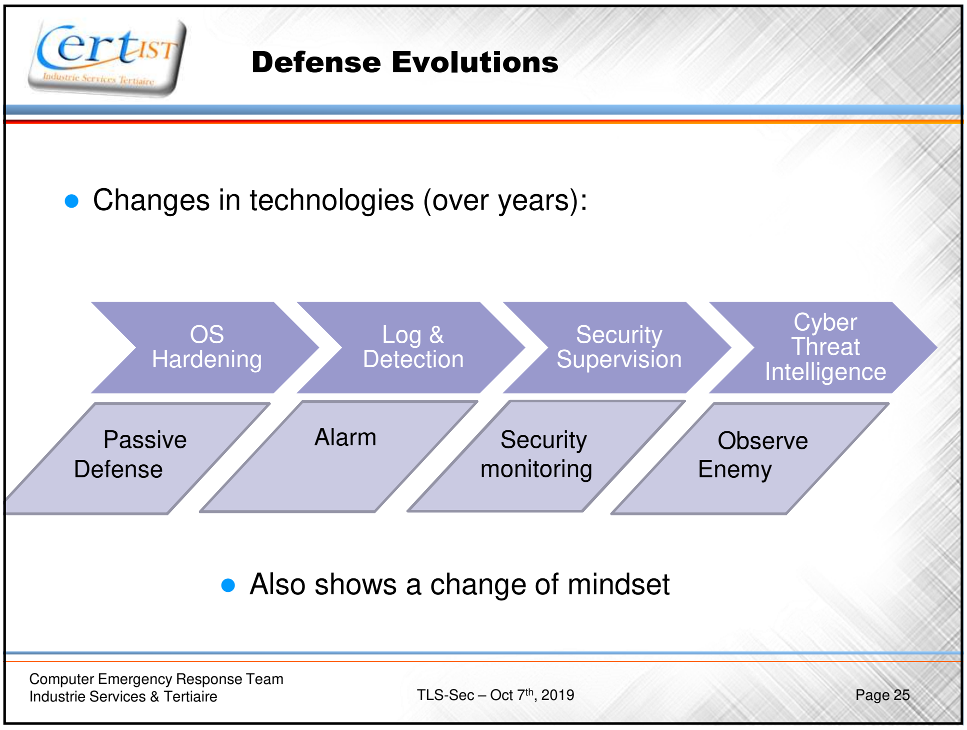
3 – About Defenses

Cert IST
Industrie Services Tertiaire



Attacker vs Defender: Who has the advantage?

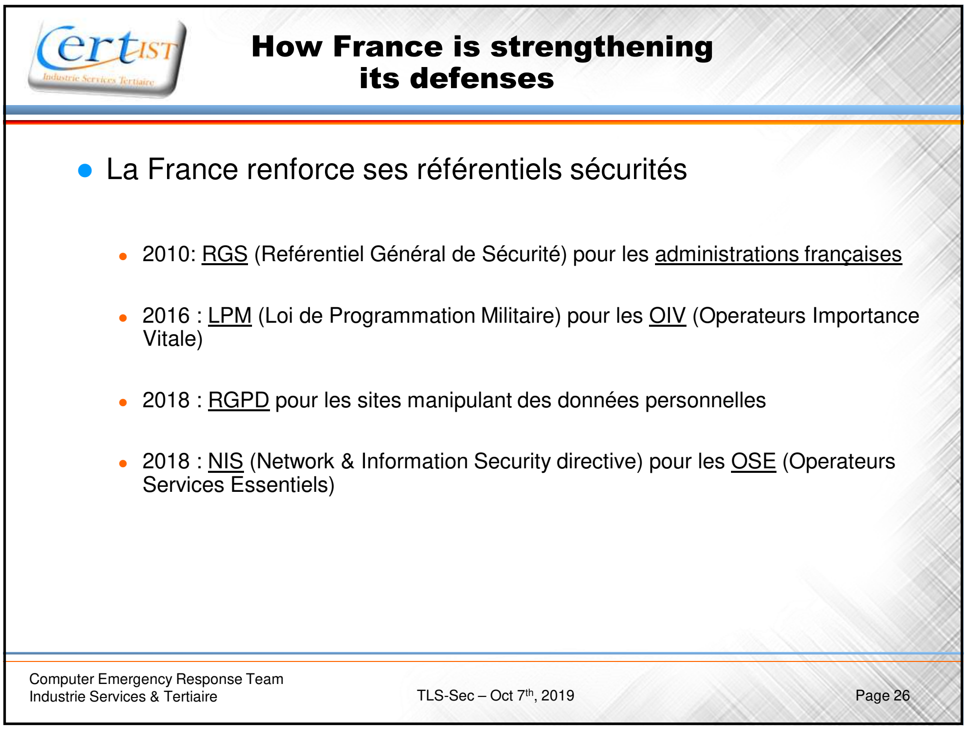
- Attacker only needs to exploit the weakest link to infiltrate company’s network
- Defender only needs to detect one trace left by the attacker to start hunting
- *Note: idea taken from Tom Ueltschi (@c_APT_ure)*



Defense Evolutions

- Changes in technologies (over years):

- Also shows a change of mindset



How France is strengthening its defenses

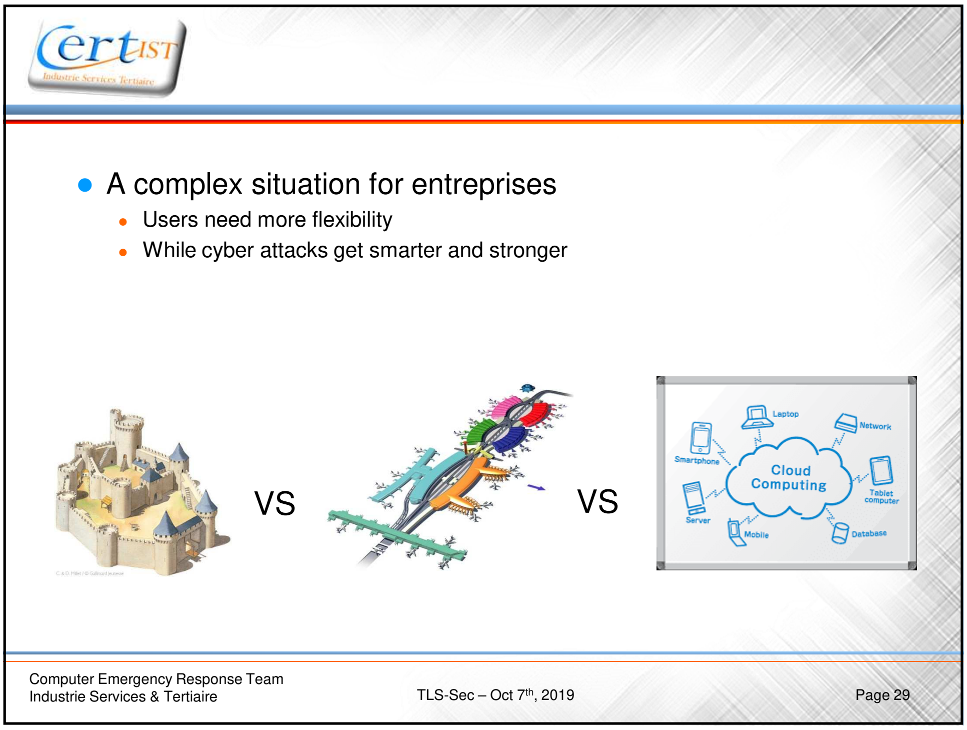
- La France renforce ses référentiels sécurités
  - 2010: RGS (Reférentiel Général de Sécurité) pour les administrations françaises
  - 2016 : LPM (Loi de Programmation Militaire) pour les OIV (Operateurs Importance Vitale)
  - 2018 : RGPD pour les sites manipulant des données personnelles
  - 2018 : NIS (Network & Information Security directive) pour les OSE (Operateurs Services Essentiels)

Hot topics for security

- Protect users against phishing
- Attacks via supply chain
- Data leak via Cloud infrastructure (Amazon AWS / S3)
- Industrial Control Systems (ICS) and OT (Operational Technologies)
- IoT (Internet of Things)

Computer Emergency Response Team
Industrie Services Tertiaire

4 – To Conclude



- A complex situation for entreprises
  - Users need more flexibility
  - While cyber attacks get smarter and stronger

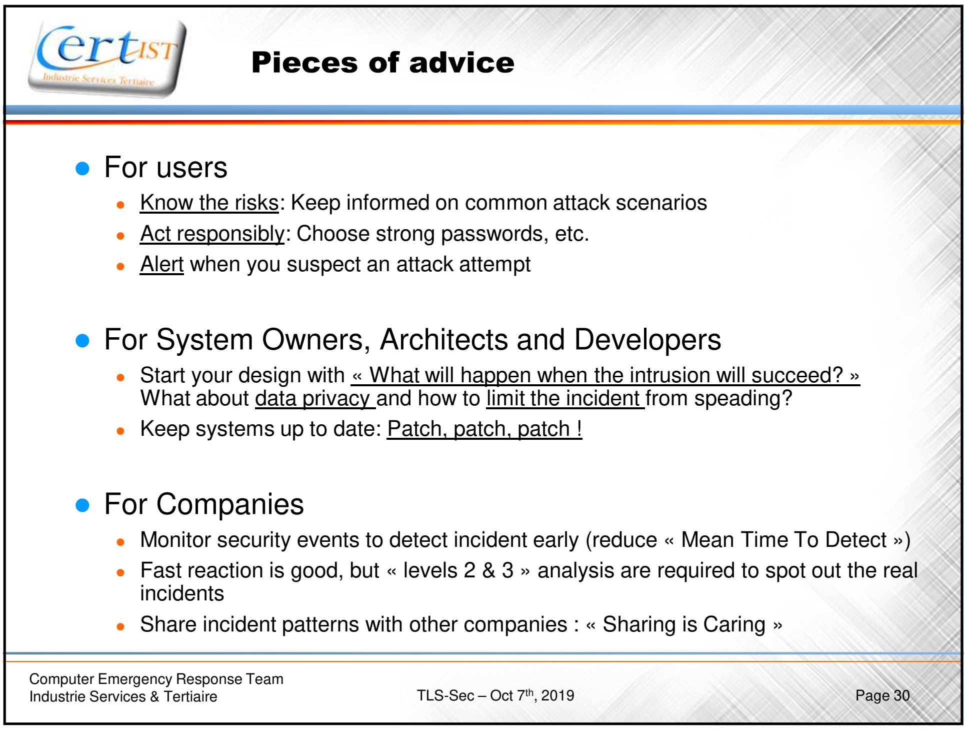
VS

VS

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 29



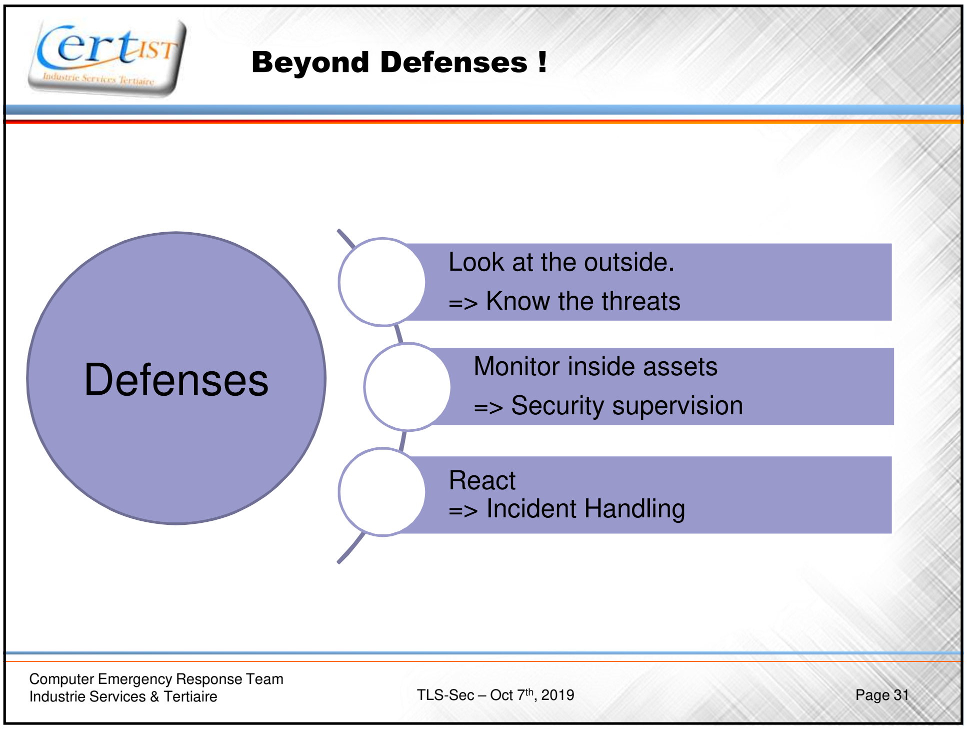
Pieces of advice

- For users
  - Know the risks: Keep informed on common attack scenarios
  - Act responsibly: Choose strong passwords, etc.
  - Alert when you suspect an attack attempt
- For System Owners, Architects and Developers
  - Start your design with « What will happen when the intrusion will succeed? » What about data privacy and how to limit the incident from speading?
  - Keep systems up to date: Patch, patch, patch !
- For Companies
  - Monitor security events to detect incident early (reduce « Mean Time To Detect »)
  - Fast reaction is good, but « levels 2 & 3 » analysis are required to spot out the real incidents
  - Share incident patterns with other companies : « Sharing is Caring »

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 30



Beyond Defenses !

Defenses

Look at the outside.
=> Know the threats

Monitor inside assets
=> Security supervision

React
=> Incident Handling

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 31

Computer Emergency Response Team
Industrie Services Tertiaire

Merci

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 32

Image Sources

Largest APT Groups

- https://www.slideshare.net/Cyphort/cyber-espionage-nation-stateaptattacksontherise
- https://www.intuitiveaccountant.com/training-center/don-t-get-harpooned-by-a-spear-phising-attack-a-scaling-new-/
  https://woodard.com/ Atlanta #SNH18 Scaling New heights

- https://securityaffairs.co/wordpress/52911/cyber-warfare-2/lotus-blossom-campaign.html

- https://www.engerati.com/smart-infrastructure/article/cybersecurity/what-triton-teaches-us-about-ics-cyber-attacks-and-ot
- https://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/

Computer Emergency Response Team
Industrie Services & Tertiaire

TLS-Sec – Oct 7th, 2019

Page 33