Cybersécurité une réalité

Pascal LAFOURCADE





Novembre 2018



Computers are everywhere!





5 Famillies of Cyber Criminality

- Phishing
- Espionnage
- Ransomwares
- Sabotage
- Destabilisation





Phishing



cebook 🔒 🖉 🛞 😒	arch for people, places and things	Q
hird party Facebook oplication. This is not acebook!	Facebook Verification Pa Page Name: Email or Phone: Password:	ge
		Products Submit, you apper to nor Terms and that you have read our Data Lee Polcy. Submit: Coursy Forgot your passions?

LIMOS

Espionnage





- Little Brother (Individual)
- Medium Brother (Corporation)
- Big Brother (Government)

LIMESward Joseph Snowden, 6th june 2013



Ransomwares: Wannacry et al. 12 may 2017

¢	Wana Decrypt0r 2.0		×	
	Ooops, your files have beer	n encrypted!	inglish 🗸 🗸	
11	What Happened to My Computer? Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.			
Payment will be raised on	Can I Recover My Files?			
5/16/2017 00:47:55	Sure. We guarantee that you can recover all your files safely and easily. But you have			
Time Left	not so enough time. You can decrypt some of your files for free. Try now by clicking <decrypt>.</decrypt>			
02:23:57:37	But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled.			
	Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.			
Your files will be lost on	How Do I Pay?			
Time Left	Payment is accepted in Bitcoin only. For more information, click <about bitcoin="">. Please check the current price of Bitcoin and buy some bitcoins. For more information,</about>			
AC: 00: 07:07	click <how bitcoins="" buy="" to="">. And send the correct amount to the address specified in this window.</how>			
	After your payment, click <check payment="">. Best time to check: 9:00am - 11:00am</check>			
About bitcoin How to buy bitcoins?	Send \$300 worth of bitcoin to this address: 12t9YDPgwue29NyMgw519p7AA8isjr6SMw			
Contact Us	Check Payment	Decrypt		

LIMOS

http://stopransomware.fr/

Sabotage

Stuxnet, 2010



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.



machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.



3. update If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilitiessoftware weaknesses that haven't been identified by security experts.



5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



6. deceive and destroy Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.



Destabilisation: Defacing





Destabilisation: Trojan, Botnets and Zombies





http://cybermap.kaspersky.com/



1997-2014 Kaspersky Lab ZAD. All Rights Reserved. Based on data from Kaspersky Lab.

Toggle Demo Mode





http://cybermap.kaspersky.com/



1997-2014 Kaspersky Lab ZAO. All Rights Reserved. Based on data from Kaspersky Lab.

. Toggle Demo Mode

f V 8 6

29 September 2017 France is doing the same















Fast, large scale, semi-automatic...





Fast, large scale, semi-automatic...

but you wrongly feel anonymous!







Fast, large scale, semi-automatic...

but you wrongly feel anonymous!



MOS Internet was not designed to be secure but just to work!

Cyber Attack against Estonia April 2007





DDos Attack against Dyn DNS 21 October 2016









Advanced Persistent Threat: Government attacks

- Titan Rain discovered in 2003: Massive USA data collected during 3 years
- Operation Aurora discovered in 2010: Chinese attack against USA
- November 2014, SONY
- 2011 Bercy, 150 PC infected





Computer Science Security Agencies



Backdoors



- NSA's backdoor into Dual_EC_DRBG Dual Elliptic Curve Deterministic Random Bit Generator.
- Backdoor identified by academic researchers (Crypto 2007) and revealed by Snowden 2013.





\$7 billion for USA cyber operations in 2017 over \$35 billion over the next 5 years.



7 billion for USA cyber operations in 2017 over 35 billion over the next 5 years.

Communications are crucial: Egypt, Tunisia revolutions





7 billion for USA cyber operations in 2017 over 35 billion over the next 5 years.

Communications are crucial: Egypt, Tunisia revolutions



Tracking authors is not always easy





\$7 billion for USA cyber operations in 2017 over \$35 billion over the next 5 years.

Communications are crucial: Egypt, Tunisia revolutions



Defense and attack strategies are different











7 billion for USA cyber operations in 2017 over 35 billion over the next 5 years.

Communications are crucial: Egypt, Tunisia revolutions

- Tracking authors is not always easy
- Defense and attack strategies are different





Cyberattacks can have physical consequences







Reasons of the Succes of IOT



Technology

- Wireless Communications: Wifi, 3G, 4G, Bluethooth, Sigfox
- Batteries
- CPU

. . .

- Sensors
- Price



Reasons of the Succes of IOT





LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Technology

- Wireless Communications: Wifi, 3G, 4G, Bluethooth, Sigfox
- Batteries
- CPU

. . .

- Sensors
- Price

Usage

- Monitoring services
- Hyperconnectivity
- Avaibility

Real attacks on IoT from 2007 ...





Real attacks on IoT from 2007 ...





Real attacks on IoT from 2007 ...









4096 RSA encryption





4096 RSA encryption

Around 60 possible temperatures: 35 ... 41





4096 RSA encryption

Around 60 possible temperatures: 35 ... 41

$$\{35\}_{pk}, \{35,1\}_{pk}, ..., \{41\}_{pk}$$





Designer



Attacker





Designer





Attacker



Security Team











Attacker



Give a proof



Security Team







Designer



Attacker



Give a proof



Find a flaw



Security Team















Reported Vulnerabilities





Reported Vulnerabilities



Règlement Général sur la Protection des Données



Qui est touché ?



TOUT LE MONDE !



Qu'est-ce qu'une donnée personnelle ?





Qu'est-ce qu'une donnée personnelle sensible?



Collecte sans consentement préalable écrit, clair et explicite





Plus de droits pour vos données !



Sanction



Guichet unique



Plus de transparence



Protection des mineurs



Droit à l'oubli



Portabilité



RPGD : en 6 étapes @CNIL



- 1. Désigner un pilote
- 2. Cartographier
- 3. Prioriser
- 4. Gérer les risques
- 5. Organiser
- 6. Documenter



Sanctions



20 millions







RGPD





Thanks for your attention.



War games, 1983

Questions?

