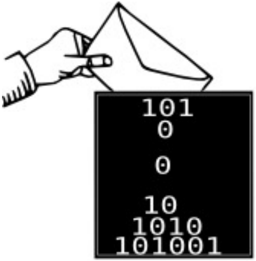
Cybersécurité une réalité

Pascal LAFOURCADE

Novembre 2018

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

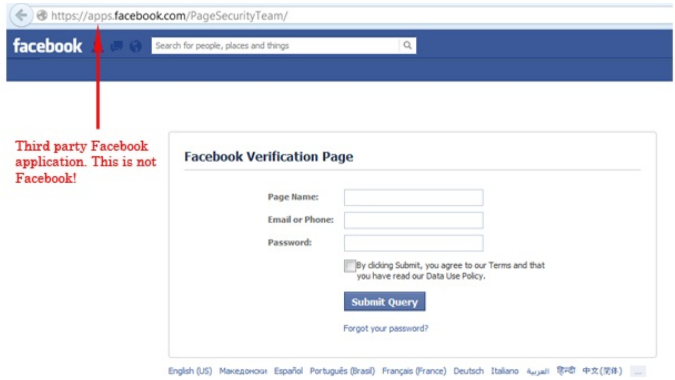
Computers are everywhere!



5 Famillies of Cyber Criminality

- Escroquerie
- Sabotage
- Ransomwares
- Espionnage
- Destabilisation

Escroquerie : Phishing



https://apps.facebook.com/PageSecurityTeam/

facebook

Search for people, places and things

Third party Facebook application. This is not Facebook!

Facebook Verification Page

Page Name:

Email or Phone:

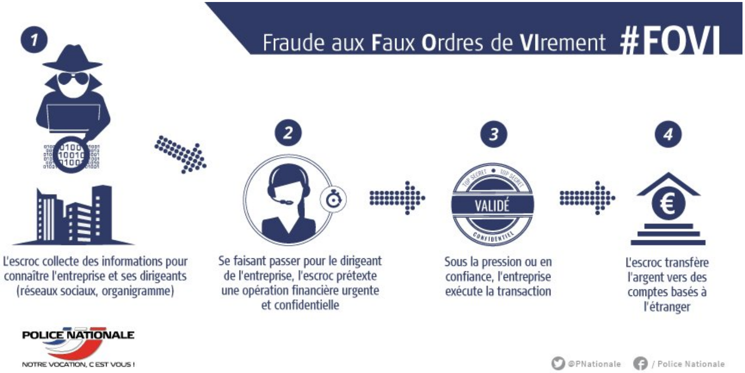
Password:

□ By clicking Submit, you agree to our Terms and that you have read our Data Use Policy.

Submit Query
Forgot your password?
English (US) Македонски Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体) ...

Voyant + Papillon

Escroquerie : Fraude au président



Fraude aux Faux Ordres de VIrement #FOVI

1 L'escroc collecte des informations pour connaître l'entreprise et ses dirigeants (réseaux sociaux, organigramme)

2 Se faisant passer pour le dirigeant de l'entreprise, l'escroc prétexte une opération financière urgente et confidentielle

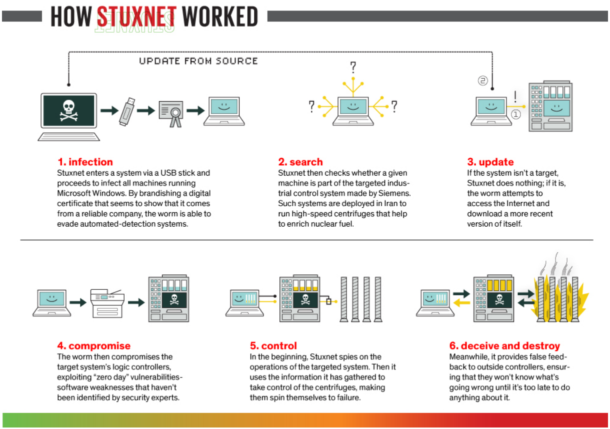
3 Sous la pression ou en confiance, l'entreprise exécute la transaction

4 L'escroc transfère l'argent vers des comptes basés à l'étranger

VIDEO

Sabotage

Stuxnet, 2010



HOW STUXNET WORKED

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.

2. search
Stuxnet then checks whether a given 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.

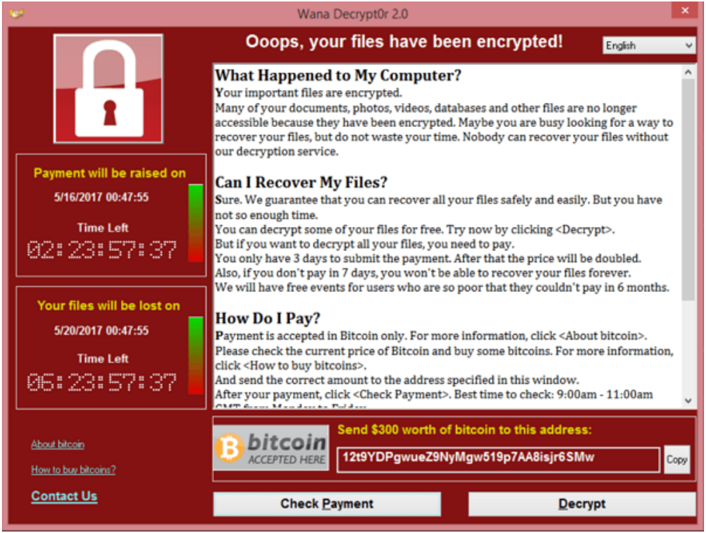
4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

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.

Saudi Aramco 35 000 PC deleted in 2012.

Ransomwares: Wannacry et al. 12 may 2017



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

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.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
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.

How Do I Pay?

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, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

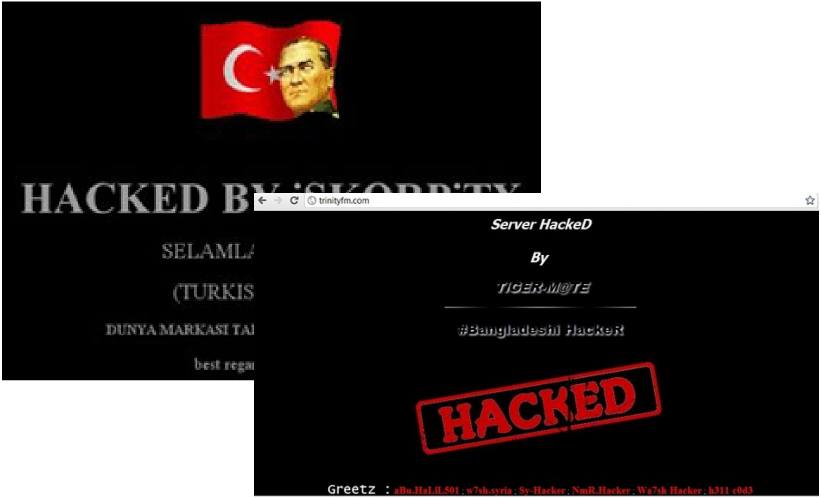
http://stopransomware.fr/

Espionnage

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

Edward Joseph Snowden, 6th june 2013

Destabilisation: Defacing



HACKED BY :SKORPiTY

SELAML

(TURKIS

DUNYA MARKASI TA

best rega

Server HackeD

By

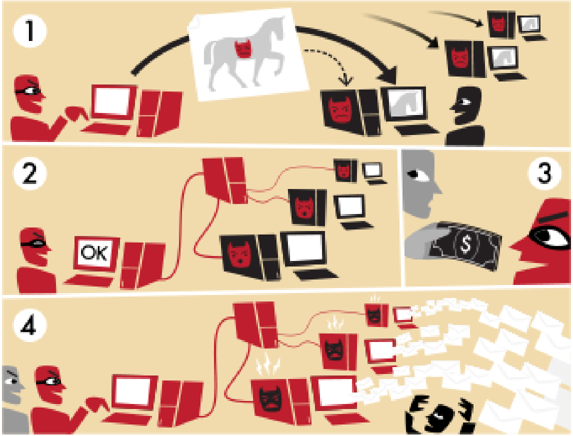
TIGER-M@TE

#Bangladeshi HackeR

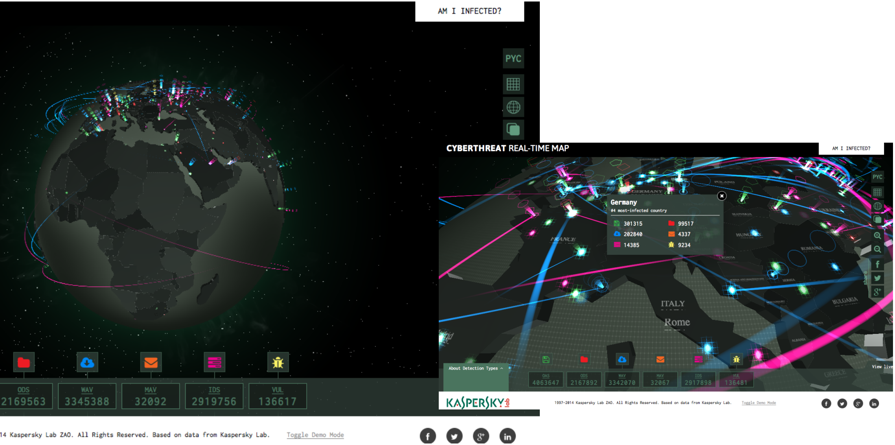
HACKED

Greetz : aBu.HaLiL501 ; w7sh.syria ; Sy-Hacker ; NmR.Hacker ; Wa7sh Hacker ; h311 c0d3

Destabilisation: Trojan, Botnets and Zombies



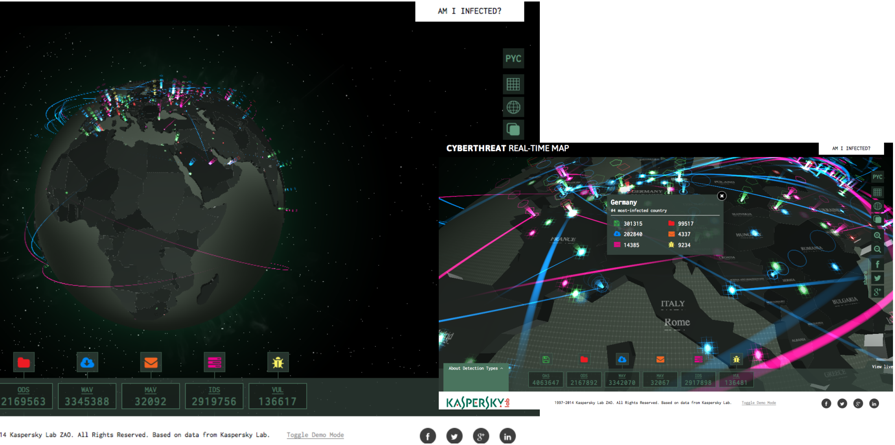
http://cybermap.kaspersky.com/



14 Kaspersky Lab ZAO. All Rights Reserved. Based on data from Kaspersky Lab.

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

http://cybermap.kaspersky.com/



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

14 Kaspersky Lab ZAO. All Rights Reserved. Based on data from Kaspersky Lab.

14 September 2017 USA stops to use Kaspersky

29 September 2017 France is doing the same

Quelques conseils

FESTIVAL
du FILM
SÉCURITÉ

2018

GRAND PRIX DU FESTIVAL
Les 10 commandements de la Cyber-Victime
par Micode
VIDEO

Why are there more and more attacks?

Why are there more and more attacks?

Why are there more and more attacks?

Why are there more and more attacks?

Fast, large scale, semi-automatic...

Why are there more and more attacks?

Fast, large scale, semi-automatic...

but you wrongly feel anonymous!

Why are there more and more attacks?

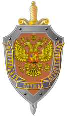
Fast, large scale, semi-automatic...

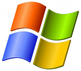
but you wrongly feel anonymous!

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

Computer Science Security Agencies

- 1919

- 1952,
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
- 1995, 

- 2002, 
- 7 July 2009,
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Cyberwar is a reality

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

Cyberwar is a reality

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

- Communications are crucial: Egypt, Tunisia revolutions

Cyberwar is a reality

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

- Communications are crucial: Egypt, Tunisia revolutions

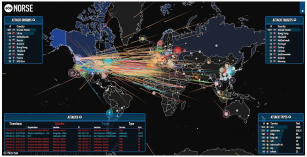
- Tracking authors is not always easy

Cyberwar is a reality

$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



ATTACK ORIGINS

#	Country
907	United States
574	China
77	Netherlands
70	Russia
67	Austria
51	Hong Kong
48	Thailand
47	Taiwan
44	France
38	Mil/Gov

ATTACK TARGETS

#	Country
1871	United States
73	Hong Kong
55	Thailand
39	Netherlands
34	Portugal
32	Turkey
31	Canada
30	Liechtenstein
25	Austria
25	Norway

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-26 18:57:53.[illegible]	Thefirst-RU clients [illegible]	Moscow, Russia	188.138.225.71	unknown, Austria	http	80
2014-06-26 18:57:54.85	Aliyun Computing Co., LTD	Hangzhou, China	182.92.75.35	San Francisco, United States	unknown	33435
2014-06-26 18:57:54.86	N/A	unknown, Chile	190.110.121.63	San Francisco, United States	unknown	33435
2014-06-26 18:57:57.32	Thefirst-RU clients [illegible]	Moscow, Russia	188.138.225.71	unknown, Austria	http	80
2014-06-26 18:57:57.33	Thefirst-RU clients [illegible]	Moscow, Russia	188.138.225.71	unknown, Austria	http	80
2014-06-26 18:57:57.33	Thefirst-RU clients [illegible]	Moscow, Russia	188.138.225.71	unknown, Austria	http	80
2014-06-26 18:57:57.54	Thefirst-RU clients [illegible]	Moscow, Russia	188.138.225.71	unknown, Austria	http	80

ATTACK TYPES

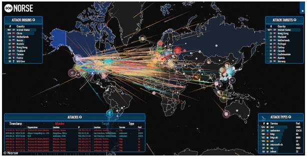
#	Service	Port
524	vnc	5900
241	unknown	33435
180	http	80
143	http-alt	8080
126	ssh	22
94	microsoft-ds	445
67	sip	5060
64	telnet	23

Cyberwar is a reality

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

- Communications are crucial: Egypt, Tunisia revolutions

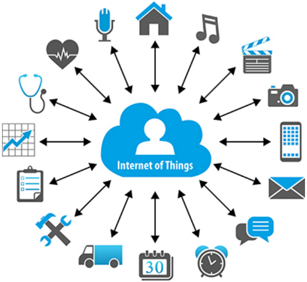
- Tracking authors is not always easy
- Defense and attack strategies are different



- Cyberattacks can have physical consequences

Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Ransomware Hospital Attacks
A New Weapon of Mass Destruction

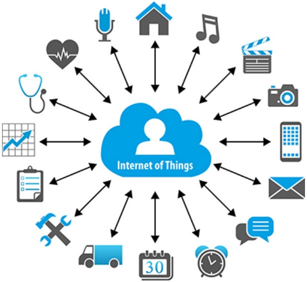
Reasons of the Succes of IOT



Technology

- Wireless : Wifi, 3G, 4G, 5G, Bluethooth, Sigfox ...
- Batteries
- CPU
- Sensors
- Price

Reasons of the Succes of IOT



Technology

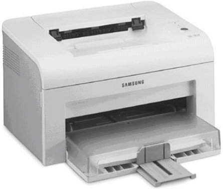
- Wireless : Wifi, 3G, 4G, 5G, Bluethooth, Sigfox ...
- Batteries
- CPU
- Sensors
- Price

Usage

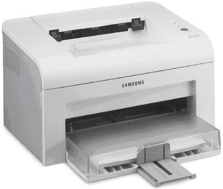
- Monitoring services
- Hyperconnectivity
- Avaibility

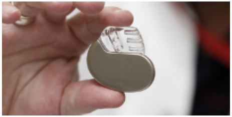
Real attacks on IoT from 2007 ...

Real attacks on IoT from 2007 ...



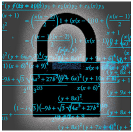
Real attacks on IoT from 2007 ...





Formal Verification Approaches

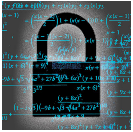
Designer



Attacker

Formal Verification Approaches

Designer

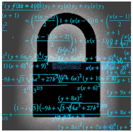


Attacker

Security Team

Formal Verification Approaches

Designer



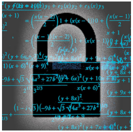
Attacker

Give a proof

Security Team

Formal Verification Approaches

Designer



Attacker

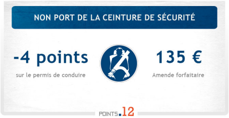
Give a proof

Find a flaw

Security Team

Applications

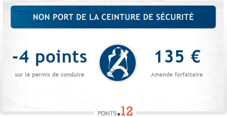
RIP


NON PORT DE LA CEINTURE DE SÉCURITÉ

-4 points
sur le permis de conduire

135 €
Amende forfaitaire

POINTS.12

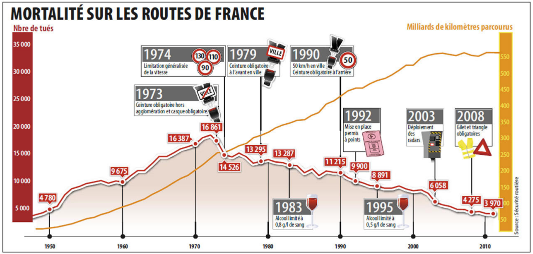


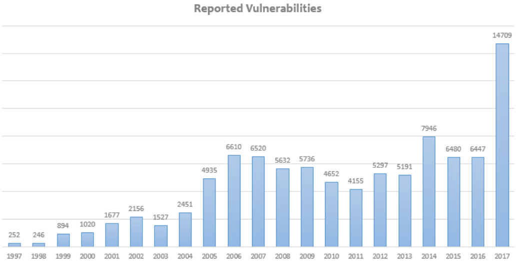
NON PORT DE LA CEINTURE DE SÉCURITÉ

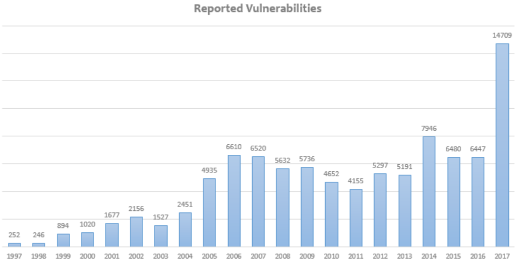
-4 points
sur le permis de conduire

135 €
Amende forfaitaire

POINTS.12




Reported Vulnerabilities
252
246
894
1020
1677
2156
1527
2451
4935
6610
6520
5632
5736
4652
4155
5297
5191
7946
6480
6447
14709
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

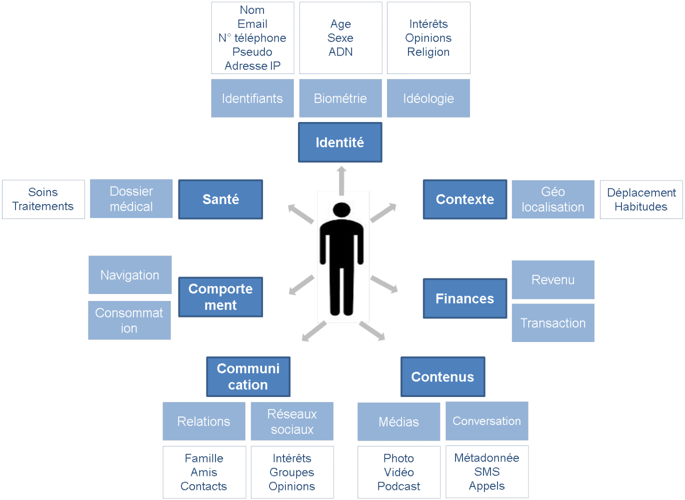


Règlement Général sur la Protection des Données
GDPR : General Data Protection Regulation

Qui est touché ?

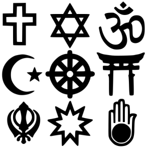
TOUT LE MONDE !

Qu’est-ce qu’une donnée personnelle ?



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

LCR
100% À GAUCHE
L'ÉCOLOGIE Les Verts
UMP
PCF
Parti communiste français
FN
UDF
lutte ouvrière
UNION COMMUNISTE (trotskyste)
MPF
Mouvement Pour la France



CGPME
Solidaires
la cgt
FO
la force syndicale
CFTC
La Vie à Défendre
UNSA
libres ensemble
cfdt
MEDEF

Collecte sans consentement préalable écrit, clair et explicite

⛔

Plus de droits pour vos données !

Sanction

Plus de transparence

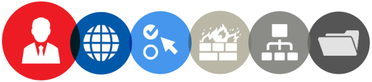
Droit à l'oubli

Guichet unique

Protection des mineurs

Portabilité

RPGD : en 6 étapes @CNIL



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

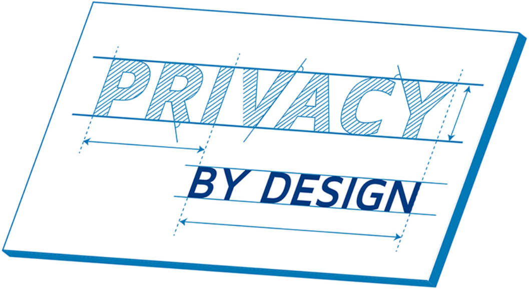
Sanctions

20 millions

€

ou 4 %

RGPD



Thanks for your attention.

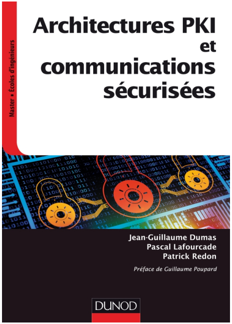
Questions?

Les BLOCKCHAINS EN 50 QUESTIONS

Comprendre le fonctionnement et les enjeux de cette technologie innovante

Jean-Guillaume DUMAS
Pascal LAFOURCADE
Ariane TICHIT
Sébastien VARRETTE

DUNOD



Architectures PKI et communications sécurisées

Master • Écoles d'ingénieurs

Jean-Guillaume Dumas
Pascal Lafourcade
Patrick Redon

Préface de Guillaume Poupard

DUNOD