

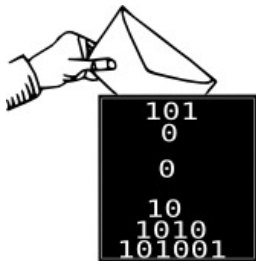
# Cyberguerre informatique une réalité

Pascal Lafourcade



Octobre 2017

# Computers are everywhere!



## 5 Families of Cyber Criminality

- ▶ Phishing
- ▶ Espionnage
- ▶ Ransomwares
- ▶ Sabotage
- ▶ Destabilisation



# Phishing



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.

[Forgot your password?](#)

English (US) Македонски Español Português (Brasil) Français (France) Deutsch Italiano العربية 繁體中文 (繁體) 中文(简体)



# Espionnage



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

Edward Joseph Snowden, 6th june 2013



# Ransomwares: Wannacry et al. 12 may 2017

Wana Decrypt0r 2.0

Oops, your files have been encrypted!

English

### 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

Send \$300 worth of bitcoin to this address:

 **bitcoin**  
ACCEPTED HERE

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

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

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

<http://stopransomware.fr/>

# 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.

# Destabilisation: Defacing



# Destabilisation: Trojan, Botnets and Zombies



<http://cybermap.kaspersky.com/>

MAP

AM I INFECTED?

PYC

Grid icon

Map icon

Search icon

Search icon

CYBERTHREAT REAL-TIME MAP

AM I INFECTED?

Germany  
an infected country

387315	99517
281646	4337
14385	9234

150	ODS 2169563	MAY 3345388	MAY 32092	IDS 2919756	VIA 136617
-----	----------------	----------------	--------------	----------------	---------------

KASPERSKY

1997-2014 Kaspersky Lab. All Rights Reserved. Based on data from Kaspersky Lab. 78620.7863.7863

Navigation icons

1997-2014 Kaspersky Lab ZAO. All Rights Reserved. Based on data from Kaspersky Lab. [Toggle Demo Mode](#)

Facebook, Twitter, Google+, LinkedIn icons

<http://cybermap.kaspersky.com/>



14 September 2017 USA stops to use Kaspersky  
29 September 2017 France is doing the same

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!

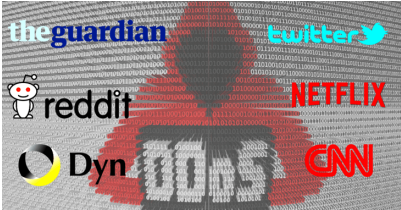
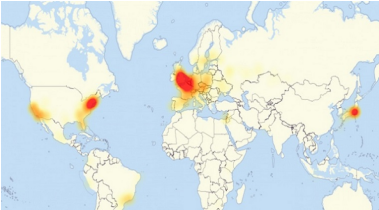


Internet was not designed to be secure but just to work!

# 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

▶ 1919



▶ 1952,



▶ 1995,



▶ 2002,



▶ 7 July 2009,



# Livre blanc sur la défense et la sécurité nationale 2013

## LIVRE BLANC

DÉFENSE  
ET SÉCURITÉ  
NATIONALE

2013

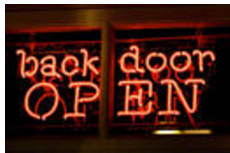


5 milieux (p84):

- ▶ terre
- ▶ air
- ▶ mer
- ▶ espace extra-atmosphérique
- ▶ cyberspace

“le dispositif de cyberdéfense, qui est appelé à s’amplifier dans les années qui viennent.” ANSSI et OIV

# 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.



## Conclusion: Cyberwar is a reality

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

## Conclusion: 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



## Conclusion: 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



## Conclusion: 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



# Conclusion: 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





**Thanks for your attention.**



War games, 1983  
Could be a reality?

**Questions?**