Cybercriminality

not only a cyber, a cyber criminality…
sorry
not only a criminality, a cyber criminality

What is a cybercrime?

Cybercrime is any type of criminal activity that involves the use of a computer or other cyber device.

- Computers used as the tool
- Computers used as the target

What is a cybercrime?

It regroup many categories of crimes:

- Financial fraud crimes
- Cyberterrorism
- Cyberextortion
- Cyberwarfare

Cybercrime facts

- Cybercrime has recently surpassed illegal drug trafficking as a criminal money-maker
- A personal identity is stolen once every 3.1 seconds as a result of cybercrime
- Nearly half of all cybercrimes are committed against small businesses

Cybercrime facts : Cost

Global cost of cybercrime is estimated to hit

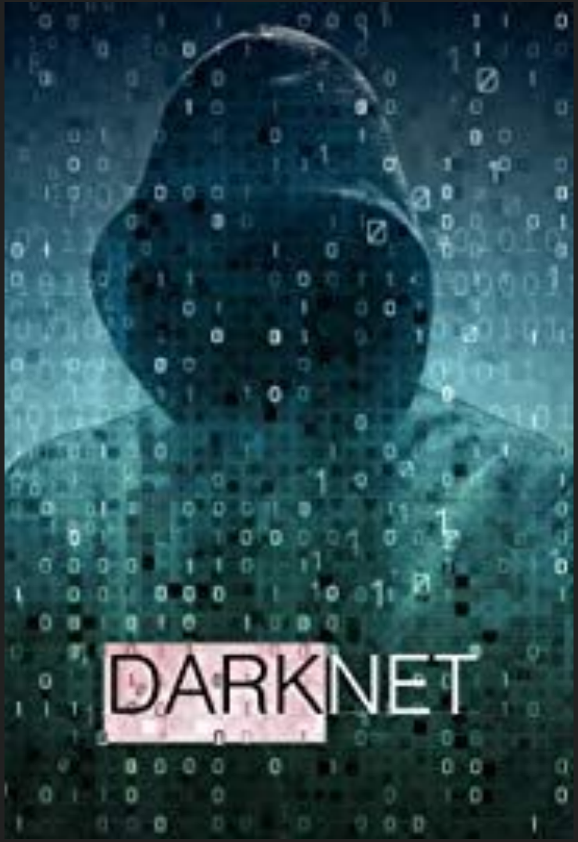
$2 trillion

by 2019

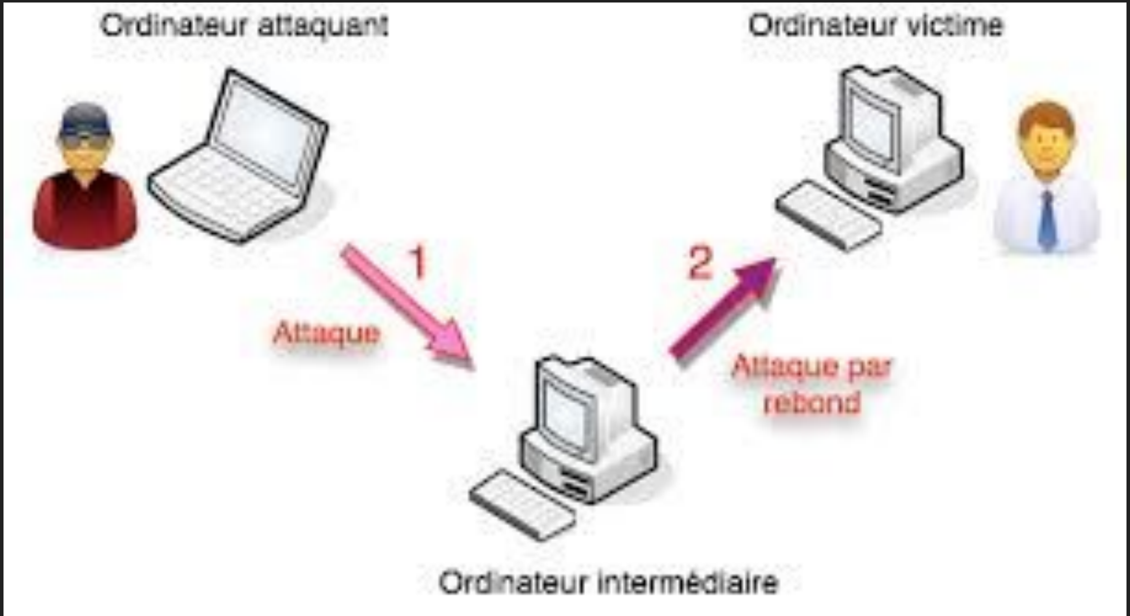
Cybercrime facts : DarkNet

- Cryptocurrency
- Drug trafficking
- Illegals activities

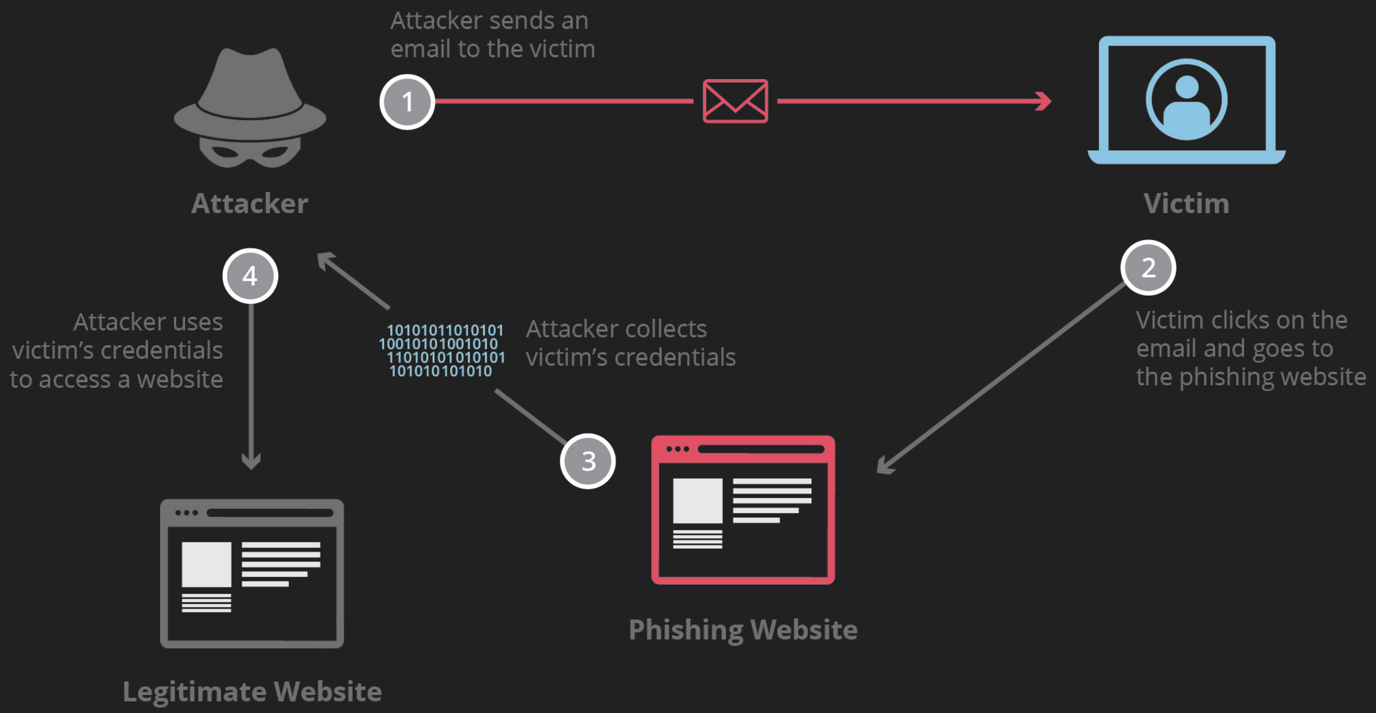
BITCOIN · DIGITAL · DECENTRALIZED · PEER TO PEER
TROYOZ 999 FINE COPPER MJB MONETARY METALS



Man-In-The-Middle Attack



Phishing Attack



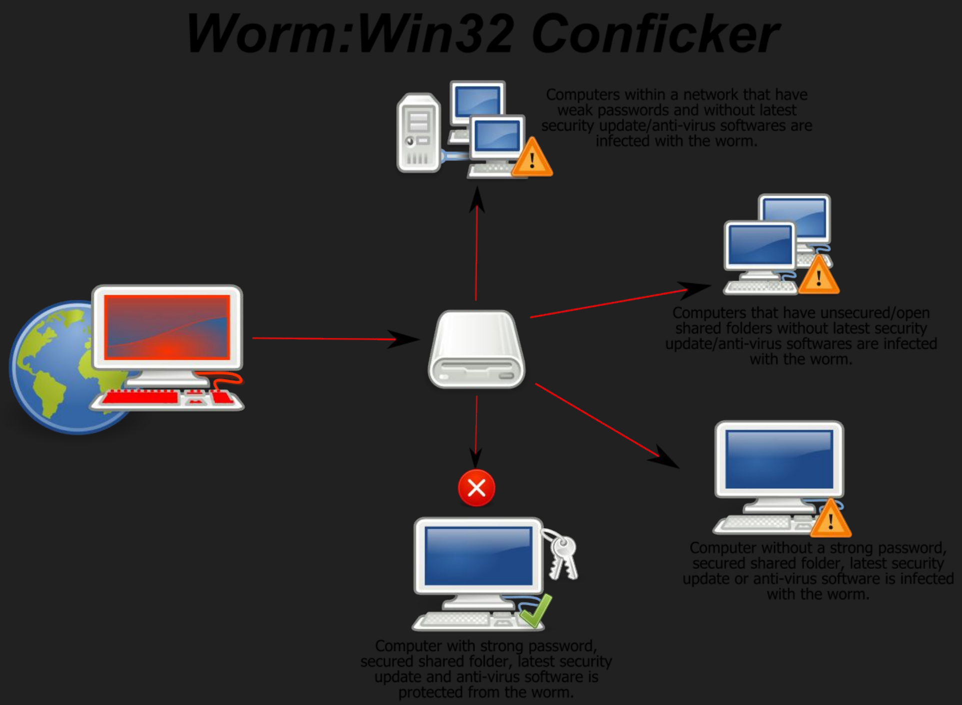
1. Attacker sends an email to the victim

2. Victim clicks on the email and goes to the phishing website

3. Attacker collects victim's credentials

4. Attacker uses victim's credentials to access a website

Worm Attack



Worm:Win32 Conficker

Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.

Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.

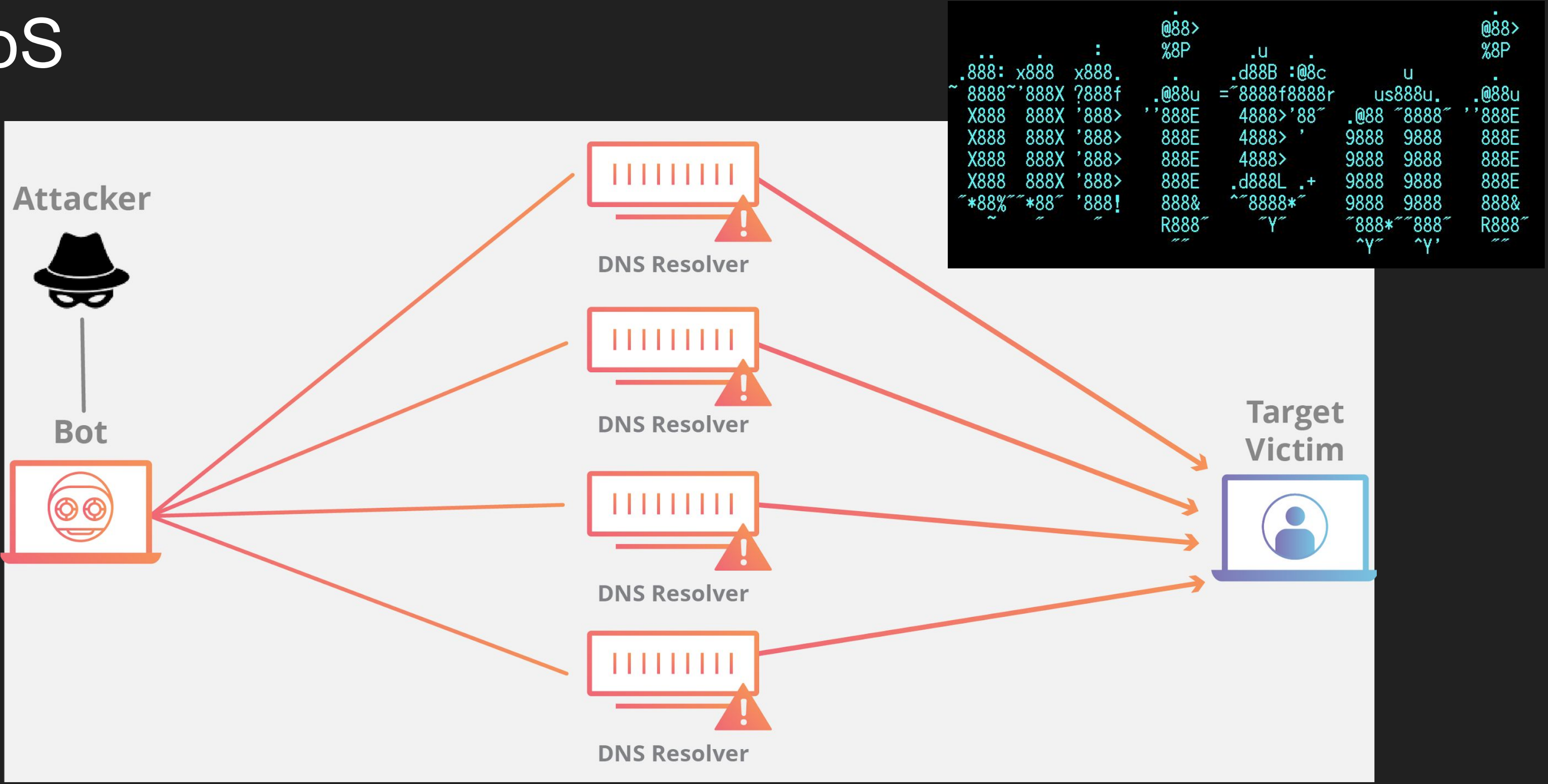
Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.

Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.

Trojan horses

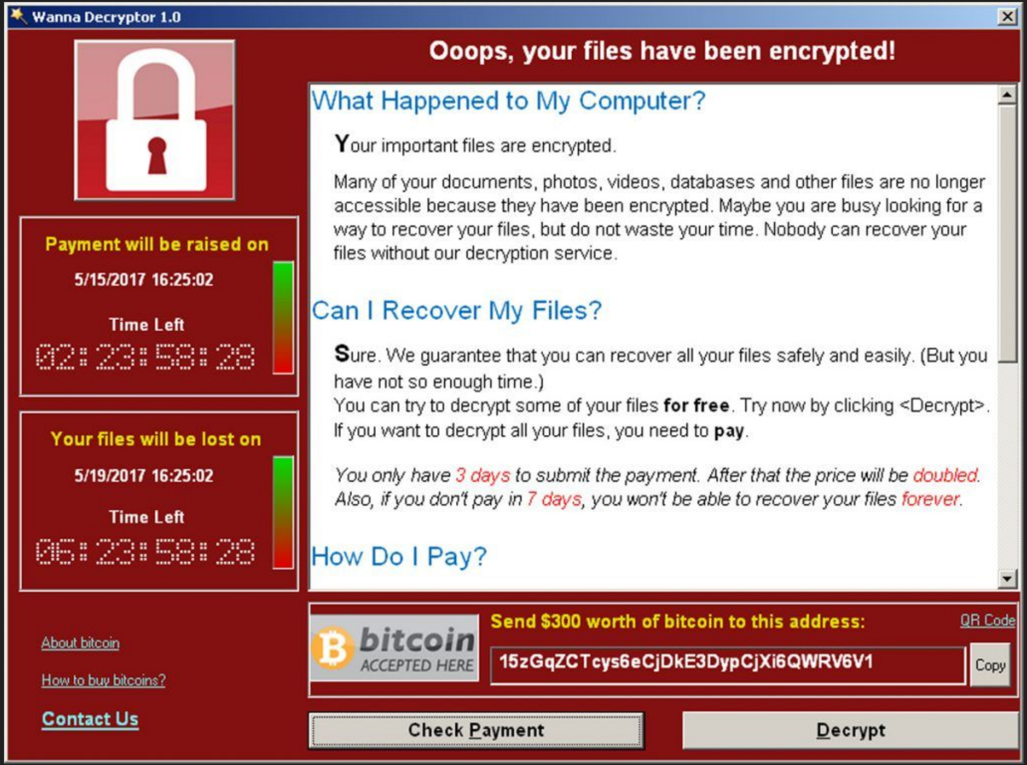
- Trusted software which contains some undesirable lines of code

DDoS



```
                       .                                .
                      @88>                             @88>
   ..    .     :      %8P      .u    .                 %8P
 .888: x888  x888.     .     .d88B :@8c        u        .
~ 8888~'888X ?888f   .@88u  ="8888f8888r    us888u.   .@88u
  X888  888X '888>  ''888E    4888>'88"  .@88 "8888" ''888E
  X888  888X '888>    888E    4888> '    9888  9888    888E
  X888  888X '888>    888E    4888>      9888  9888    888E
  X888  888X '888>    888E   .d888L .+   9888  9888    888E
 "*88%""*88" '888!    888&   ^"8888*"    9888  9888    888&
    ~    "     "      R888"     "Y"      "888*""888"   R888"
                       ""                 ^Y"   ^Y'     ""
```

Ransomware Attack



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 16:25:02

Time Left

02:23:58:28

Your files will be lost on

5/19/2017 16:25:02

Time Left

06:23:58:28

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 try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

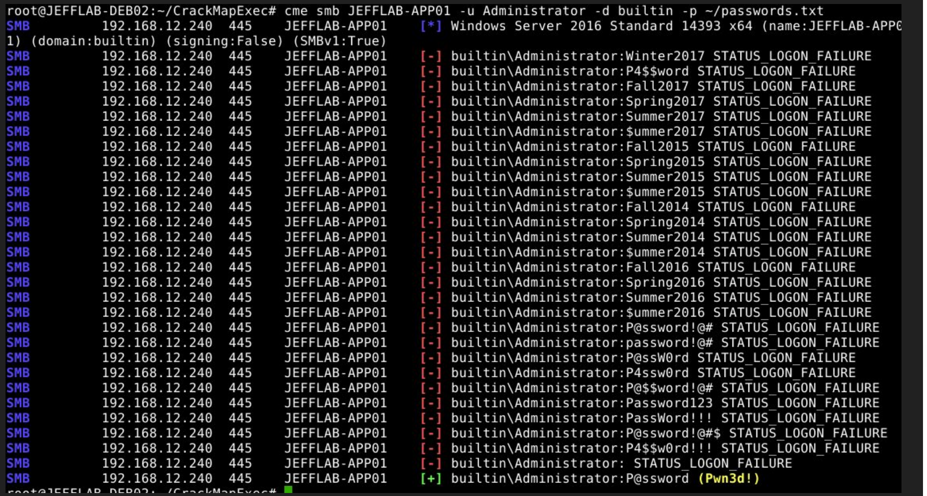
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Send $300 worth of bitcoin to this address:

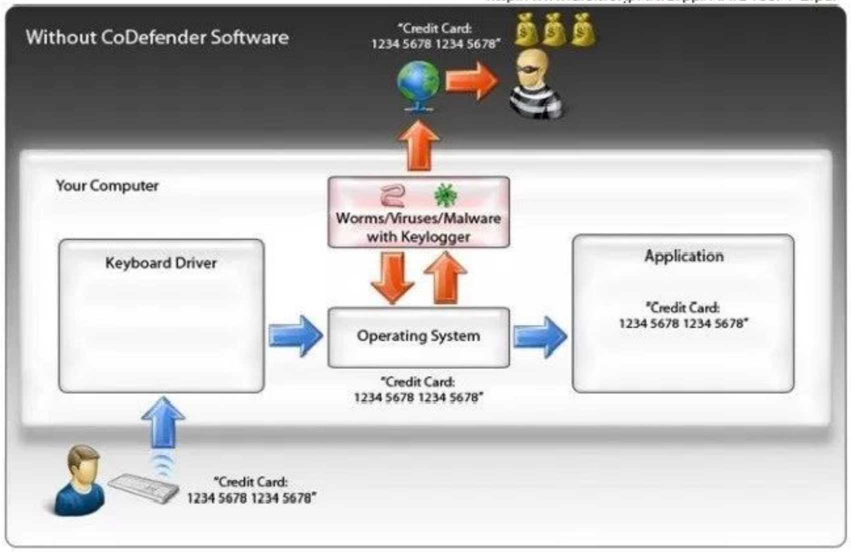
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Brute Force / Keylogger Attack



```
root@JEFFLAB-DEB02:~/CrackMapExec# cme smb JEFFLAB-APP01 -u Administrator -d builtin -p ~/passwords.txt
SMB         192.168.12.240  445    JEFFLAB-APP01    [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-APP0
1) (domain:builtin) (signing:False) (SMBv1:True)
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Winter2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:P4$$word STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Fall2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Spring2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Summer2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:$ummer2017 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Fall2015 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Spring2015 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Summer2015 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:$ummer2015 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Fall2014 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Spring2014 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Summer2014 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:$ummer2014 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Fall2016 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Spring2016 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Summer2016 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:$ummer2016 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:P@ssword!@# STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:password!@# STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:P@ssW0rd STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:P4ssw0rd STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:P@$$word!@# STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:Password123 STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:PassWord!!! STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:P@ssword!@#$ STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator:P4$$w0rd!!! STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [-] builtin\Administrator: STATUS_LOGON_FAILURE
SMB         192.168.12.240  445    JEFFLAB-APP01    [+] builtin\Administrator:P@ssword (Pwn3d!)
root@JEFFLAB-DEB02:~/CrackMapExec#
```

http://www.aicit.org/RNIS/ppl/RNIS168PPL.pdf



Keylogging process

Some historical cybercrimes

1981 - Ian Murphy, aka Captain Zap hacked AT&T computers internal clocks, it’s the first computer crime punished in history.

1983 - UCLA (LA University) students used a PC to break into the ARPA communication system.

1984 - Computer Fraud and Abuse Act

1994 - Russian hackers stole $10 millions to Citybank

Some historical cybercrimes

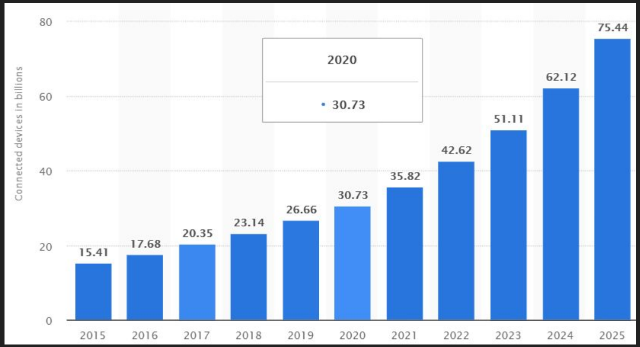
1995 - European hackers compromised TV companies to allow access to Star Trek re-runs in Germany.

1999 - Melissa, one of the first macro virus which can propagate automatically via emails thanks Outlook and Word..

2002 - British hacker accessed around hundred NASA, Army, department of defense and pentagon

2008 - In Mulouze (Ohio), a pedophile hacked a school database to enroll himself in a school

And today…

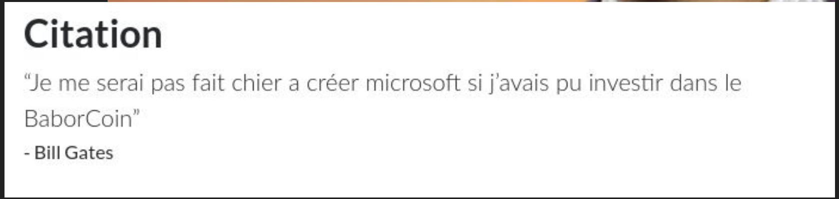


Internet of things allow hackers to easily make DDOS attacks and make new cybercrimes possibles.

Government intelligence agencies like NSA are monitoring almost all computer activities

Cryptocurrency

Some hackers are already trying to build and train Artificial intelligences to help them doing more sophisticated attacks...



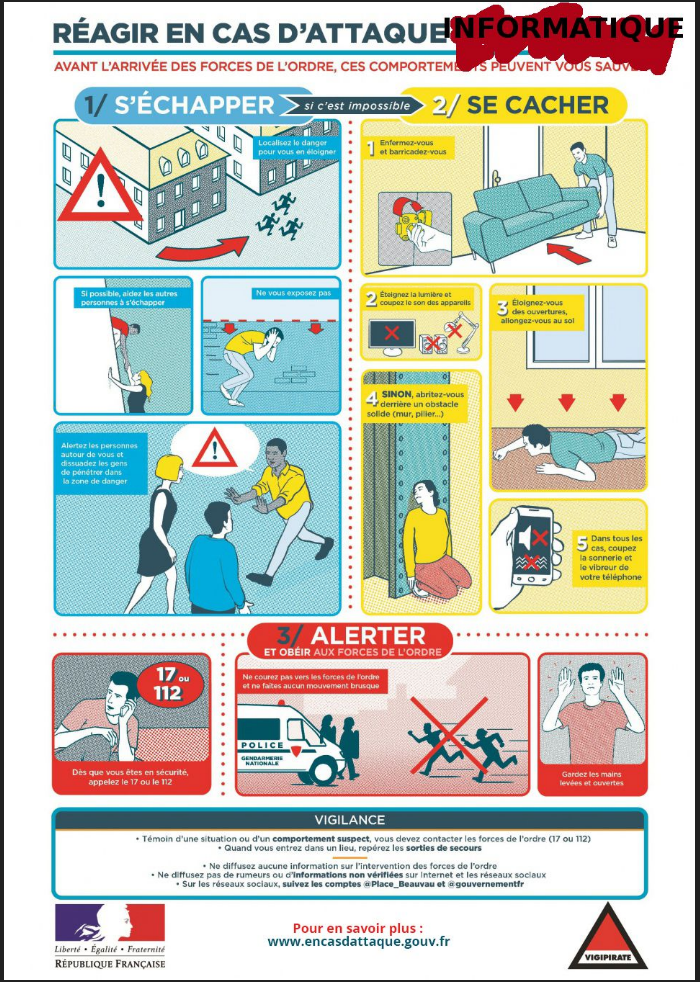
Citation

"Je me serai pas fait chier a créer microsoft si j'avais pu investir dans le BaborCoin"

- Bill Gates

What do in case of attack

- Cry
- Burn your PC
- Stay hide
- Call Interpol (because usually hacker is in another country)
- Hope and ask yourself what could you do to be protected next time.



RÉAGIR EN CAS D'ATTAQUE [redacted] INFORMATIQUE

AVANT L'ARRIVÉE DES FORCES DE L'ORDRE, CES COMPORTEME TS PEUVENT VOUS SAUV

1/ S'ÉCHAPPER

Localisez le danger pour vous en éloigner

Si possible, aidez les autres personnes à s'échapper

Ne vous exposez pas

Alertez les personnes autour de vous et dissuadez les gens de pénétrer dans la zone de danger

si c'est impossible

2/ SE CACHER

1 Enfermez-vous et barricadez-vous

2 Éteignez la lumière et coupez le son des appareils

3 Éloignez-vous des ouvertures, allongez-vous au sol

4 **SINON**, abritez-vous derrière un obstacle solide (mur, pilier...)

5 Dans tous les cas, coupez la sonnerie et le vibreur de votre téléphone

3/ ALERTER

ET OBÉIR AUX FORCES DE L'ORDRE

Dès que vous êtes en sécurité, appelez le 17 ou le 112

Ne courez pas vers les forces de l'ordre et ne faites aucun mouvement brusque

Gardez les mains levées et ouvertes

VIGILANCE

- Témoin d'une situation ou d'un **comportement suspect**, vous devez contacter les forces de l'ordre (17 ou 112)
- Quand vous entrez dans un lieu, repérez les **sorties de secours**

- Ne diffusez aucune information sur l'intervention des forces de l'ordre
- Ne diffusez pas de rumeurs ou d'**informations non vérifiées** sur Internet et les réseaux sociaux
- Sur les réseaux sociaux, **suivez les comptes @Place_Beauvau et @gouvernementfr**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

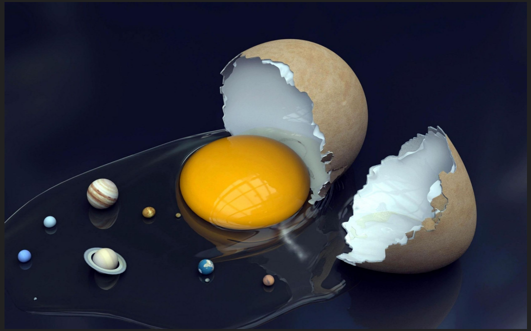
Pour en savoir plus :
www.encasdattaque.gouv.fr

VIGIPIRATE

How to protect yourself in the cyber espace!

Protect yourself from blue light

Use cyber Solar Cream



Protect your privacy

USE AVAST

How to choose a password?

1 123456

2 123456790

3 qwerty

4 12345678

5 111111

6 1234567890

7 1234567

8 password

9 123123

10 987654321

11 qwertyuiop

12 mynoob

13 123321

14 666666

15 18atcskd2w

16 7777777

17 1q2w3e4r

18 654321

19 555555

20 3rjs1la7qe

21 google

22 1q2w3e4r5t

23 123qwe

24 zxcvbnm

25 1q2w3e

How to choose a password?

~~1 123456~~
~~2 123456790~~
~~3 qwerty~~
~~4 12345678~~
~~5 111111~~
~~6 1234567890~~
~~7 1234567~~
~~8 password~~
~~9 123123~~
~~10 987654321~~
~~11 qwertyuiop~~
~~12 mynoob~~
~~13 123321~~
~~14 666666~~
~~15 18atcskd2w~~
~~16 7777777~~
~~17 1q2w3e4r~~
~~18 654321~~
~~19 555555~~
~~20 3rjs1la7qe~~
~~21 google~~
~~22 1q2w3e4r5t~~
~~23 123qwe~~
~~24 zxcvbnm~~
~~25 1q2w3e~~

- 8rbMC2j,5%K@
- gYD)w]q7+34B
- .Xd8/4i[LN3x
- 9>y)hB*KAi87
- 7Za43/bFRu#:
- v4ke766kw9f5
- 55upmhn834p6
- c659z2z7k6yi
- 87e46s9es7em
- j37i6g48vh5e

ZOHO

keeper

dashlane

Sticky Password

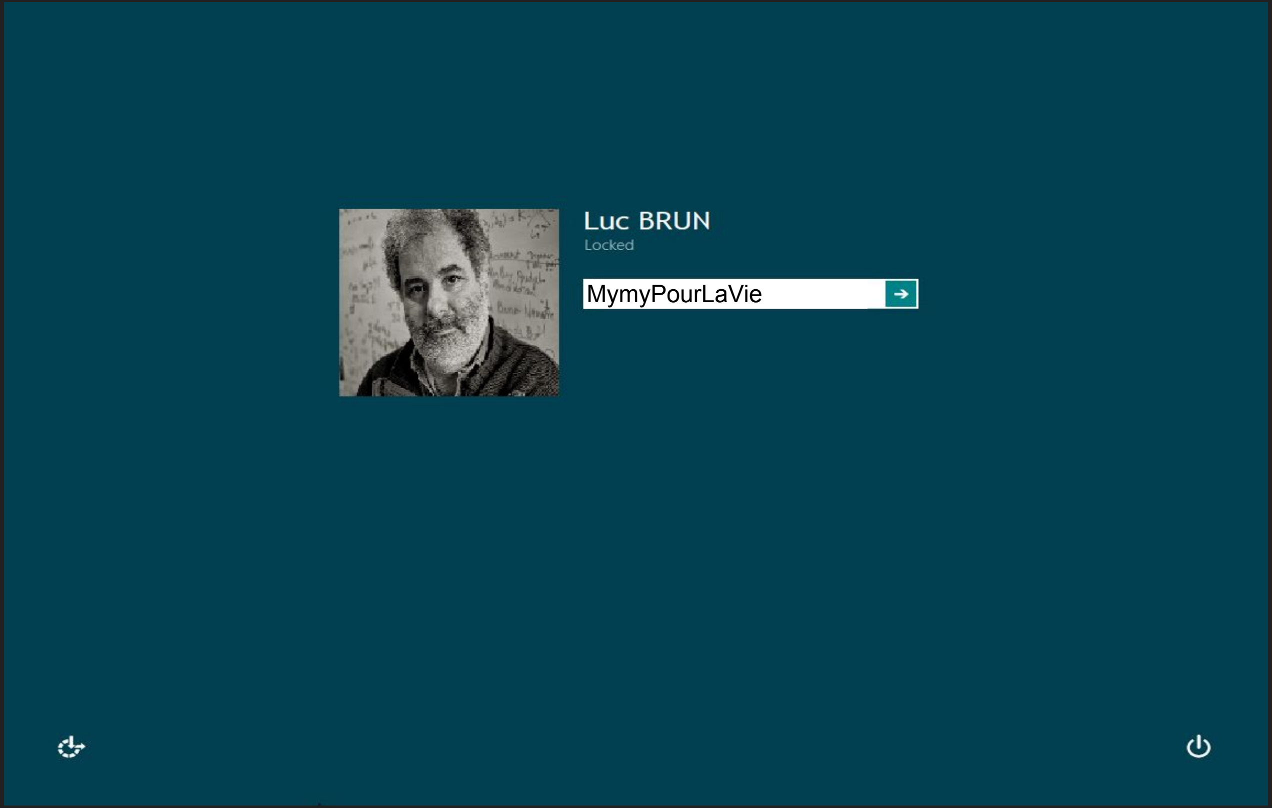
LastPass

LogmeOnce
Password Security with Convenience

The most powerful cybercriminal

faceb
YAHO
skyp
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Google

Do not forget to lock your session in the BAT E



Luc BRUN

Locked

MymyPourLaVie

DON’T USE ANY TECHNOLOGY

XPRIZE
BUSINESS
OF
CYBERCRIME