Panorama des Attaques courantes

Logiciel Malveillant

Virus
Ver
Bombe logique
Cheval de Troie
Root Kit
Porte Dérobé
KeyLogger
SpyWare
...

Attaques Réseau/Système

Écoute Passive
Usurpation
Modification/Altération
Fabrication
Re-jeu
Déni de Service
Cassage Mot de Passe
….

Ingénierie Sociale

Hameçonage
Exploitation de la faiblesse humaine (peur, argent, etc.)

Panoramas d’Attaques

Logiciels Malveillants

Logiciel Malveillant

●Tout logiciel/programme, ayant un comportement malicieux, destiné à s'introduire dans un système informatique -à l'insu de l'utilisateur- dans le but de l'endommager ou en tirer profit de quelconque manière :

-Endommager: Suppression données, formatage disque, mettre hors services matériel

-Tirer profits: Vol données (Mdp, fichiers, etc.), avoir un accès/contrôle sur la cible, chantage, gain financier (rançon), lancer une attaque à partir de la cible, etc.

→ Porter **atteinte** aux besoins **DICP**

Virus

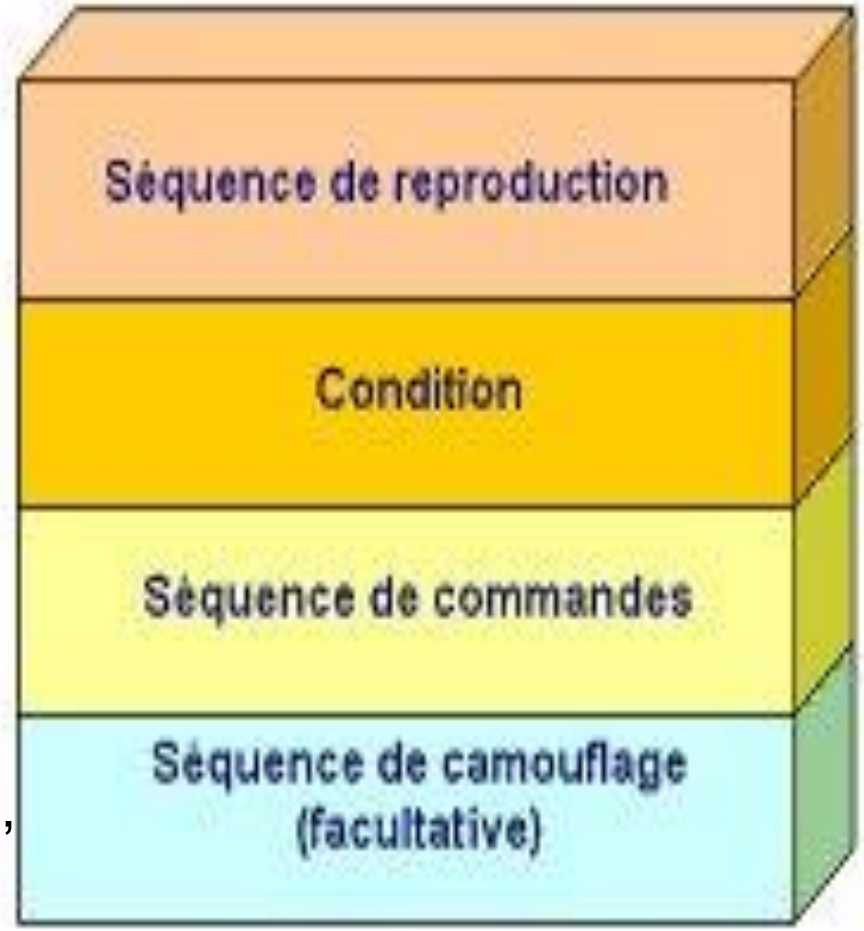
- C’est la forme la plus connue des logiciels malveillants
- Propriétés

-*Infection*: Infecte (se greffe à) tout fichier pouvant s'exécuter (.exe, .com, script, macros, etc.). Ne s'exécute pas tout seul, mais plutôt à travers l’hôte infecté.

-Infecte aussi les Secteurs d’amorçage et les Master Boot, parties sur support de stockage, contenant un code bootable par défaut

-*Propagation*: Se propage, grâce aux fichiers infectés, à travers tout moyen d’échange de données: réseaux, USB, disquette, CD/DVD, pièces jointe email, sites web infectés, etc.

Virus: Structure



Structure d'un virus

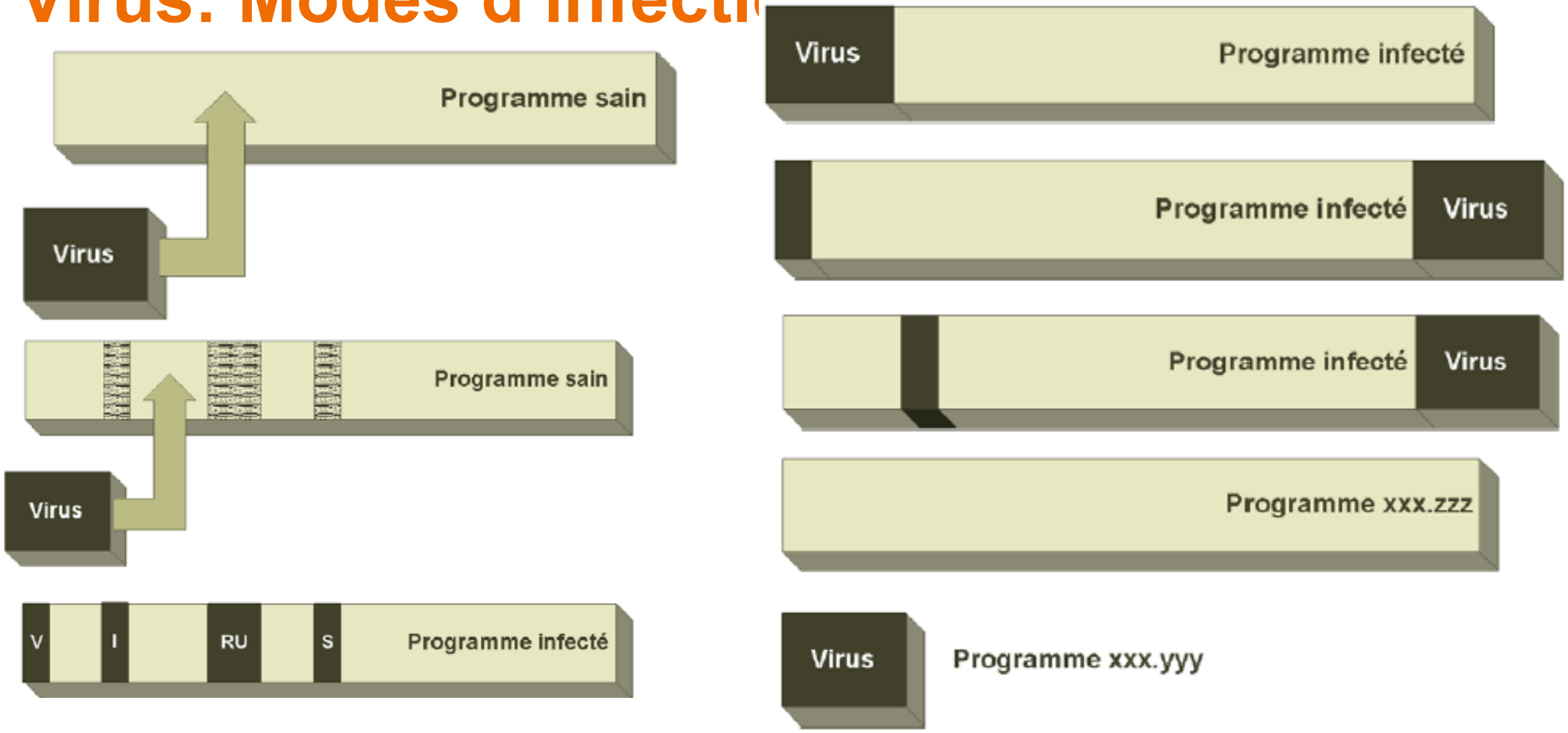
Infection des fichiers et supports

Condition pour s'exécuter

La charge du virus

Pour être transparent à l'OS, antivirus

Virus: Modes d’infection



Infection avec ou sans écrasement du programme sain

Virus: exemple de propagation via lien

Fake LinkedIn Email with a Virus

Virus: exemple de propagation via email

Commande - CD2533 — Boîte de réception

Gwenaelle DESPRES

aujourd'hui 00:24

GD

À :

Commande - CD2533

Madame, Monsieur,

Nous vous remercions pour votre nouvelle "Commande - CD2533".
Nous revenons vers vous au plus vite pour les de'lais

Meilleures salutations,
VEDISCOM SECURITE

Format A4.docm

Virus Tchernobyl (1998-2002)

- Principales caractéristiques:

-Vise le OS Windows 95/NT/XP
-Programmer pour se déclencher le 26/04
-Résidant en mémoire
-Essaye d'effacer le Bios
-Efface le 1er MO de chaque disque dure (MBR)
➔Écrasement de la table de partition du disque
➔Écrasement de la zone d'amorçage permettant de démarrer l'OS

Ver (Malware)

●Propriétés

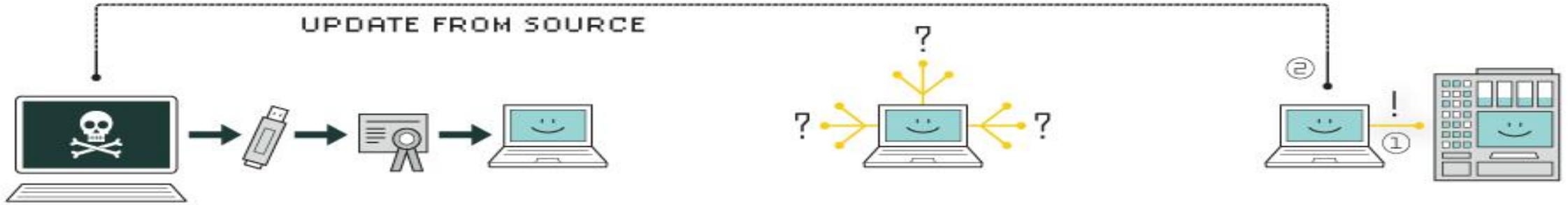
-Auto-contenu: contrairement à un virus, s'exécute de façon autonome sans besoin de se greffer sur d'autres programmes

-Se propage/multiplie par ses propre moyens, le plus souvent en s'envoyant à d'autres machines via émail ou en exploitant certaines vulnérabilités des machines cible, mais aussi via support amovible. Contrairement à un virus, il ne se propage pas localement sur une machine (n'infecte pas d'autres programmes saints), mais cherche plutôt à investir d'autres machines (du même réseau ou pas) pour les infecter.

Ver Stuxnet (2010)

- Principalement conçu pour s'attaquer à des équipement d'informatique Industriel (automates) fonctionnant sous Windows, fabriqués par Siemens , qui eux contrôlent un processus industriel critique (centrale nucléaire, hydro-électrique, distribution eau, électricité, etc.)
- Après Infection de ces automates, le fonctionnement du processus industriel peut être complètement compromis -tout en étant transparent-, pouvant résulter en une catastrophe
- L'une des principales cibles, l'industrie nucléaire iranienne, plus de 30000 systèmes infectés dans différents. A l'origine de l'attaque, une clé USB infecté
- Développé conjointement par la NSA et Israel, pour contrer le programme nucléaire iranien

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

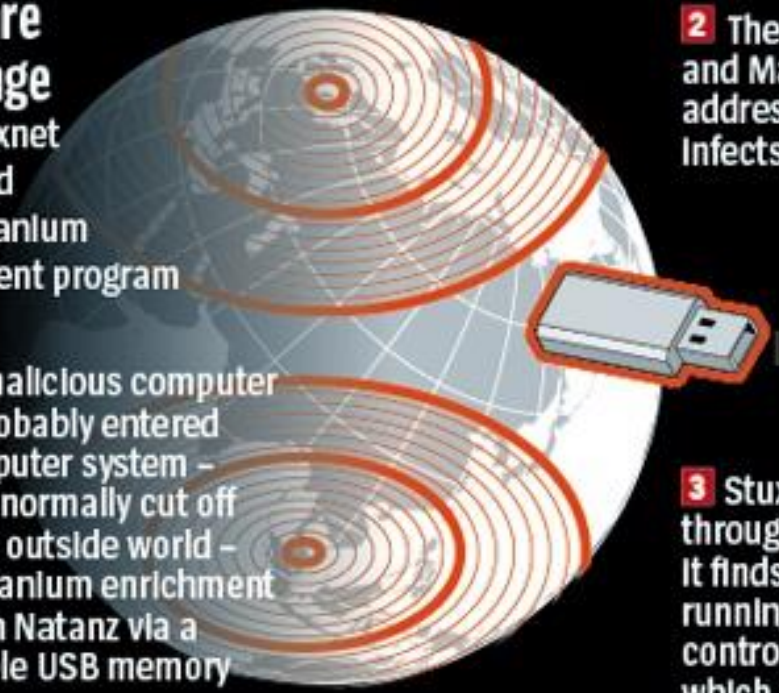
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

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.

Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program



1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

Iranian centrifuges for uranium enrichment

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Cheval de Troie (Trojan)

- Un programme/logiciel dont l'apparence est légitime, mais qui cache un autre malveillant/malicieux (virus, ver, etc.)

- Ainsi en exécutant le Chaval de Troie -supposé être légitime par l'utilisateur- le programme malveillant s'exécute aussi

- En général il s'agit d'un programme bien connu, mais qui a été modifié -ajout du code malveillant- puis redistribué (Windows, Pack Office, etc.). Toutefois, il peut aussi être un nouveau programme

- Se propage le plus souvent via téléchargement en pièce jointe ou via un lien

Trojan FlashBack

- Cibles les ordinateurs MAC OS X
- Prend l'apparence d'un installeur Java ou Flash
- Affecte/Altère le fonctionnement des navigateurs Webs

Porte Dérobée (Back door)

●Se présente souvent sous forme de méthode/paramètres/logiciel fournissant un passage secret/caché, permettant de prendre le contrôle de la cible (ordinateur) à distance sans la connaissance au préalable de l'utilisateur.

●Peut être introduite par le constructeur/développeur
-Mot de passe administrateur caché de certains équipements/logiciels, facilitant la maintenance à distance

●Mais le plus souvent est introduit par un attaquant grâce à un Trojan
-Permettent de lancer des commandes sur la machine distante (SSH, Telnet, etc.)
-De télécharger des fichiers infectés sur la machine distante

Porte Dérobée (Back door) : un compte caché sous routeur Cisco

```
ROM:0013DC50                LDR             R0, =aSCtUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
ROM:0013DC54                LDR             R1, =aAuth_admin_int ; "auth_admin_internal"
ROM:0013DC58                BL              sub_558F74
ROM:0013DC5C
ROM:0013DC5C loc_13DC5C                             ; CODE XREF: auth_admin_internal+2C↑j
ROM:0013DC5C                ADD             R0, R5, #0x44
ROM:0013DC60                LDR             R1, =aSUnSU ; "<<< %s(un='%s') = %u"
ROM:0013DC64                BL              strcmp
ROM:0013DC68                CMP             R0, #0
ROM:0013DC6C                BNE             loc_13DC78
ROM:0013DC70                MOV             R0, #0xFFFFFFFD
ROM:0013DC74                LDMDB           R11, {R4-R8,R11,SP,PC}
ROM:0013DC78 ; ---------------------------------------------------------------------------
```

Porte Dérobée (Backdoor) : connexion à distance et exécution de commandes sur machine cible

Backdoor:Win32.Hupigon

- Porte dérobée faisant partie d'un Cheval de Troie (Win32.Hupigon)
- Une fois installée sur machine, elle met en place un serveur sur un port, sur lequel d'autres machine (l'attaquant) peuvent se connecter, permettant ainsi le contrôle de la machine
- Permet aussi de se connecter aux périphériques multimédia de la cible (WebCam, Micro) et reporter les flux audio/vidéos à l'attaquant (atteinte à la vie privée)

Maliciel Furtif (RootKit)

●Un ensemble d'outils permettant de cacher la présence de logiciels malveillant sur une machine infecté → Le plus souvent difficilement détectable par les antivirus

●Considérer parmi les plus dangereux des logiciels malveillant, vu son caractère furtif.

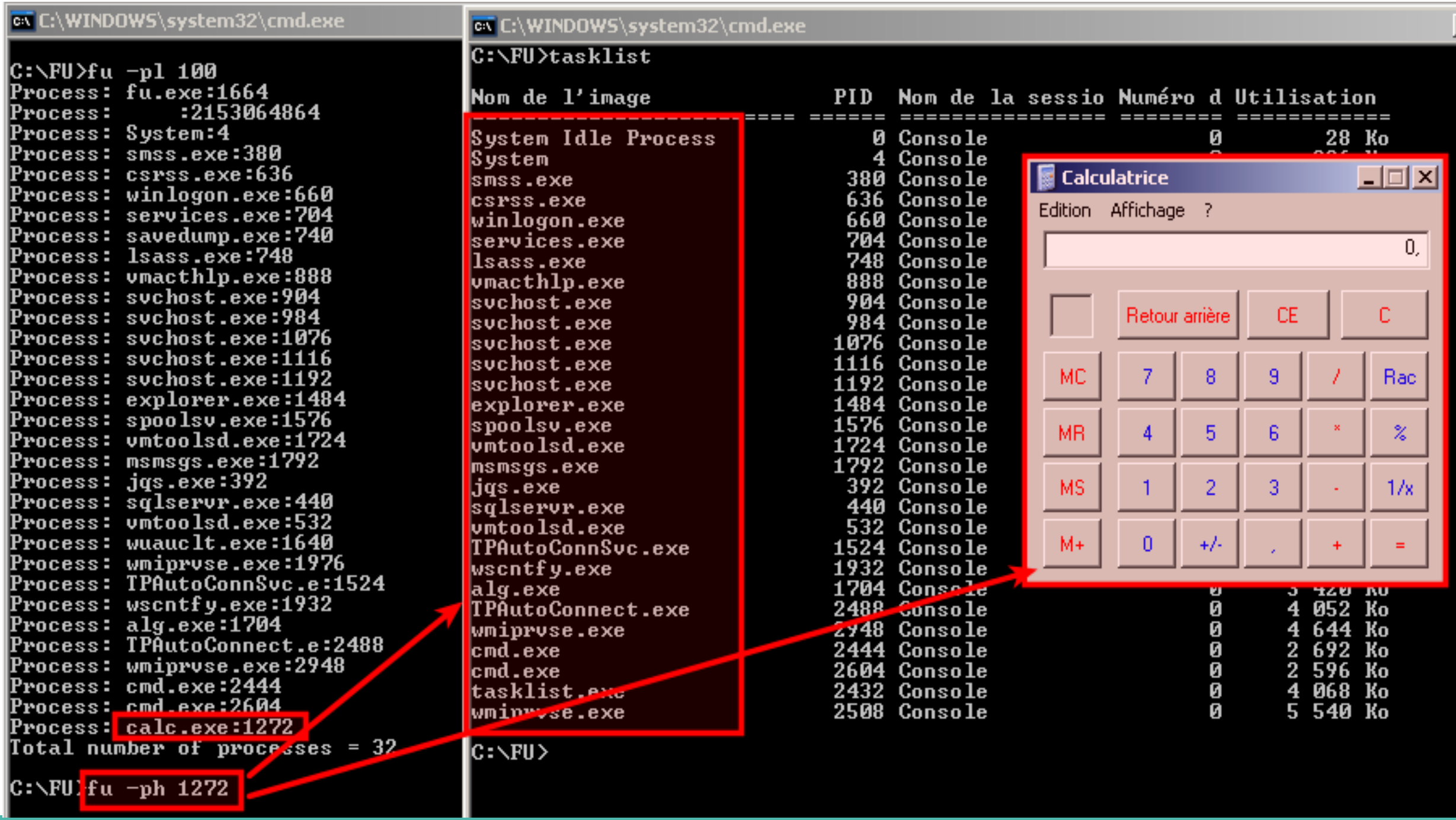
●Ils arrivent à infecter le noyau système de l'OS (gestion de processus, gestion mémoire, gestion fichier, gestion disque, gestion I/O, etc.), afin de procurer la furtive. Nécessite au préalable d'avoir les privilèges **admin** (**root**).

●

●De cette façon, les antivirus ne pourront pas détecter les processus en mémoire ni les fichiers sur disque associés au Rootkit → Pour sa détection, il est souvent nécessaire de démarrer l'antivirus depuis un disque extérieur contenant un OS saint c (non infecté) comme Kaspersky Rescue Disk par exemple.

Rootkit.Win32.Fu

- Infecte l’OS Windows


C:\WINDOWS\system32\cmd.exe
C:\FU>fu -pl 100
Process: fu.exe:1664
Process: :2153064864
Process: System:4
Process: smss.exe:380
Process: csrss.exe:636
Process: winlogon.exe:660
Process: services.exe:704
Process: savedump.exe:740
Process: lsass.exe:748
Process: vmacthlp.exe:888
Process: svchost.exe:904
Process: svchost.exe:984
Process: svchost.exe:1076
Process: svchost.exe:1116
Process: svchost.exe:1192
Process: explorer.exe:1484
Process: spoolsv.exe:1576
Process: vmtoolsd.exe:1724
Process: msmsgs.exe:1792
Process: jqs.exe:392
Process: sqlservr.exe:440
Process: vmtoolsd.exe:532
Process: wuauclt.exe:1640
Process: wmiprvse.exe:1976
Process: TPAutoConnSvc.e:1524
Process: wscntfy.exe:1932
Process: alg.exe:1704
Process: TPAutoConnect.e:2488
Process: wmiprvse.exe:2948
Process: cmd.exe:2444
Process: cmd.exe:2604
Process: calc.exe:1272
Total number of processes = 32
C:\FU>fu -ph 1272
C:\WINDOWS\system32\cmd.exe
C:\FU>tasklist
Nom de l'image PID Nom de la sessio Numéro d Utilisation
System Idle Process 0 Console 0 28 Ko
System 4 Console
smss.exe 380 Console
csrss.exe 636 Console
winlogon.exe 660 Console
services.exe 704 Console
lsass.exe 748 Console
vmacthlp.exe 888 Console
svchost.exe 904 Console
svchost.exe 984 Console
svchost.exe 1076 Console
svchost.exe 1116 Console
svchost.exe 1192 Console
explorer.exe 1484 Console
spoolsv.exe 1576 Console
vmtoolsd.exe 1724 Console
msmsgs.exe 1792 Console
jqs.exe 392 Console
sqlservr.exe 440 Console
vmtoolsd.exe 532 Console
TPAutoConnSvc.exe 1524 Console
wscntfy.exe 1932 Console
alg.exe 1704 Console
TPAutoConnect.exe 2488 Console 0 4 052 Ko
wmiprvse.exe 2948 Console 0 4 644 Ko
cmd.exe 2444 Console 0 2 692 Ko
cmd.exe 2604 Console 0 2 596 Ko
tasklist.exe 2432 Console 0 4 068 Ko
wmiprvse.exe 2508 Console 0 5 540 Ko
C:\FU>
Calculatrice
Edition Affichage ?
0,
Retour arrière CE C
MC 7 8 9 / Rac
MR 4 5 6 * %
MS 1 2 3 - 1/x
M+ 0 +/- , + =

Antivirus et Logiciels Malveillants

Comment un anti-virus arrive à détecter la présence d'un logiciel malveillant ?
Principalement grâce à base de signature virale, où chaque logiciel malveillant possède une signature qui le caractérise :
- Son code source
- une chaîne particulière (suite d'octets) qu'il laisse sur chaque fichier infecté dans le cas de virus
- un comportement anormale qui diverge du comportement normal/standard
- Le calcul d'une empreinte qui permet de déterminer si l'intégrité du fichier a été modifié ou pas

Ma machine est infecté, mon antivirus ne détecte rien !

Principalement, car la signature du logiciel malveillant ne figure pas encore dans le base de l'antivirus

* L'antivirus n'a pas été mis à jour
* L'antivirus est à jour, mais fait face à un nouveau logiciel malveillant qui n'a pas encore été détecté par les éditeurs d'anti-virus
→ soit c'est carrément un nouveau logiciel malveillant
→ soit c'est un logiciel malveillant existant qui a changé de forme (ex : virus polymorphes)
* Le logiciel malveillant en question est protégé par un rootkit
* L'antivirus a été désactivé

Panoramas d’Attaques

Ingénierie Sociale

Ingénierie Sociale

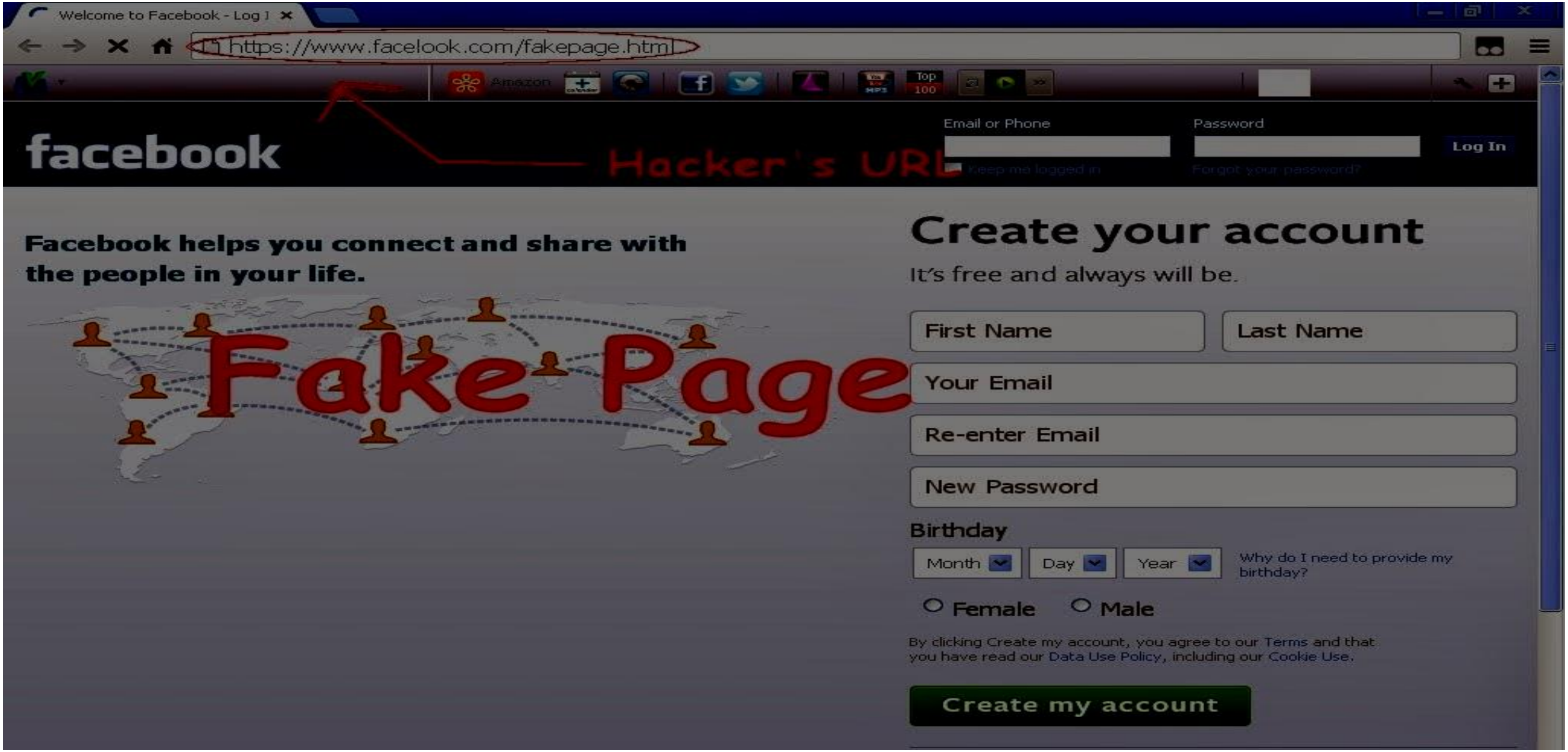
Exploiter la faiblesse humaine pour tirer un quelconque profit :
- Extraire/avoir accès à des informations sensibles (mot de passes, numéros de cartes bancaires, numéro téléphones, etc.) par un quelconque moyen (téléphone, conversation, mail, etc.)

- Induire l'utilisateur à faire une action (téléchargement et/ou ouverture d'une pièce jointe, cliquer sur un lien pour visiter un site, etc.)

Phishing(Hameçonage)

Un utilisateur reçoit le plus souvent un email provenant le plus souvent d'un service ou p

Phishing via un faux lien facebook



Phishing(Hameçonage) par pièce jointe

* Se présente souvent sous forme d'un mail bien structuré, introduisant un sujet d'intérêt (vous avez gagner un bon d'achat, des billets d'avion, voir même les slides de cours!), venant d'une personne connu ou d'une société, et vous incitan -de façon direct/indirect- à télécharger la pièce jointe, qui peut être :
- Un logiciel malveillant qui peut s’exécuter (sous forme ZIP ou autres)

-Un fichier (pdf, doc, jpeg) infectant c'est à dire embarquant une séquence qui peut être exécuté en exploitant une faille dans le logiciel (adobe, office word, paint) d'ouverture

* Le but est donc que l'utilisateur puisse exécuter sans ce rendre compte un bout de code, qui peut être le logiciel malveillant ou un petit programme téléchargeant le logiciel malveillant

Panoramas d’Attaques

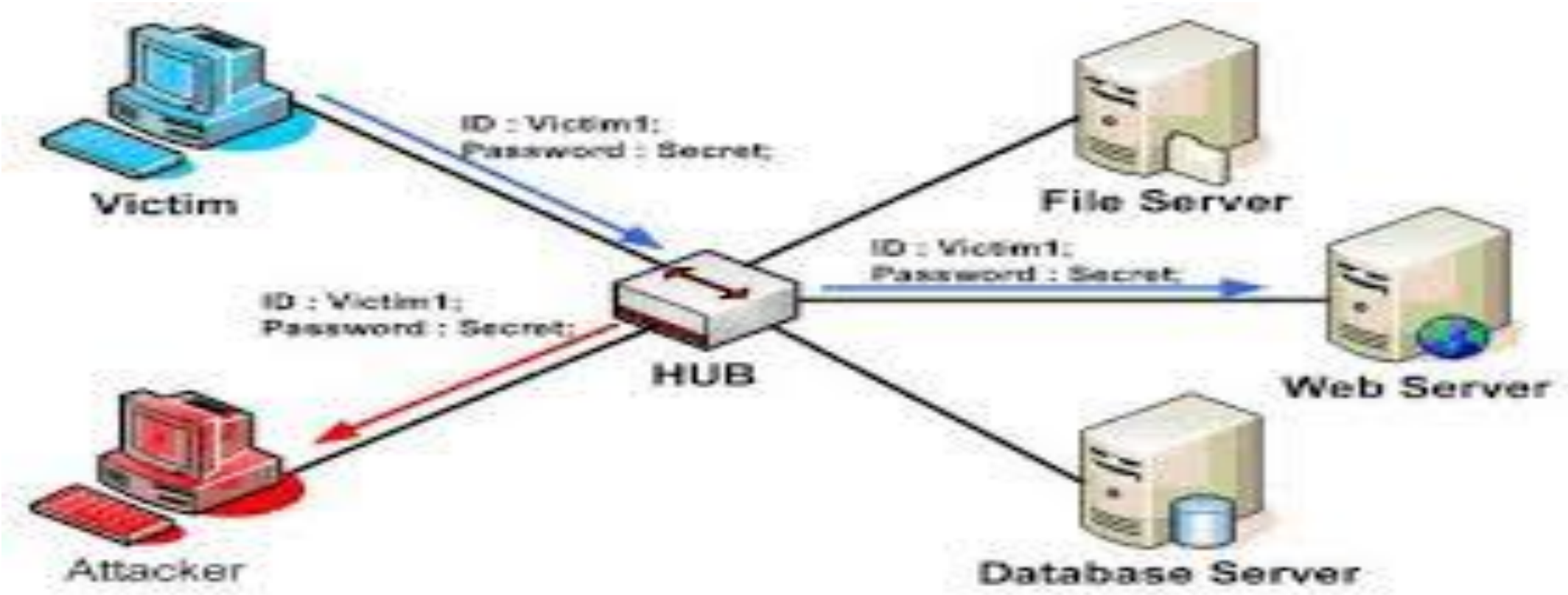
Attaques Réseaux

Écoute (Sniffing)

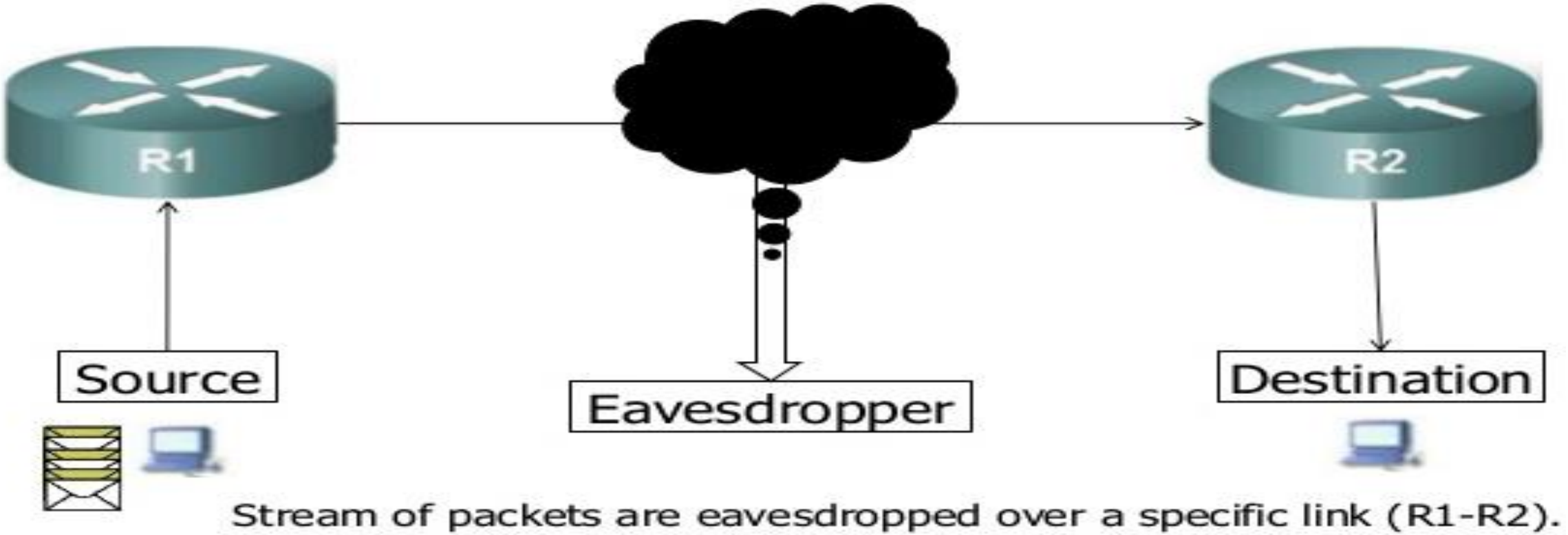
●Interception des paquets/messages transmis entre une source/destination sur un support filaire ou sans-fil

-L'accès au médium est souvent facile/faisable notamment sans-fil (Wifi, GSM, etc.)

-Risque de Divulgation de Données Importantes ou sensible

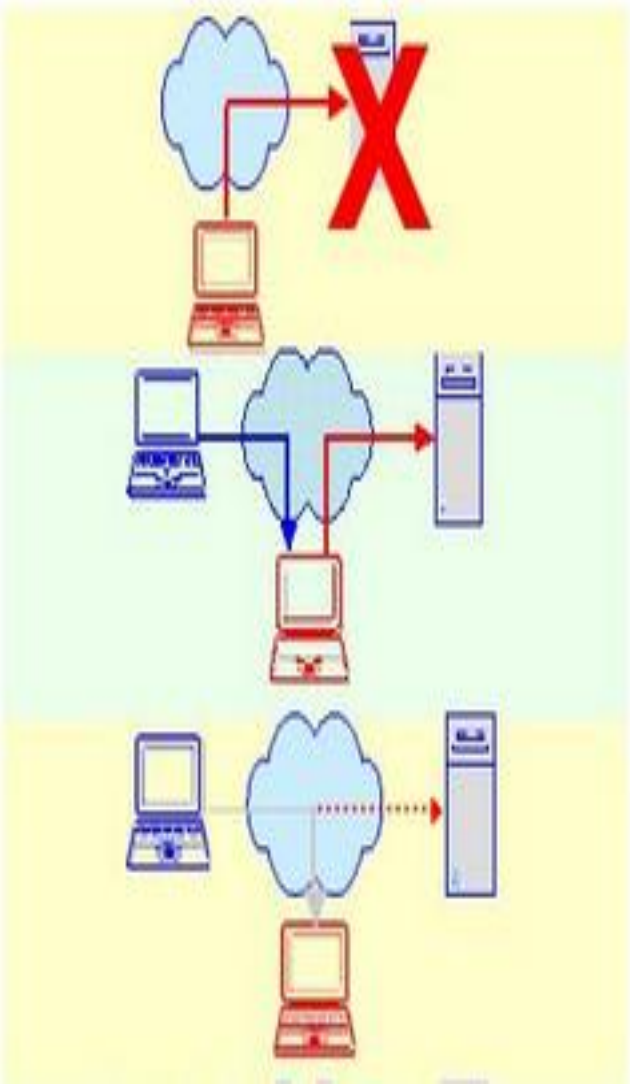


Écoute (Sniffing)



Stream of packets are eavesdropped over a specific link (R1-R2).

Injection/Modification/Destruction

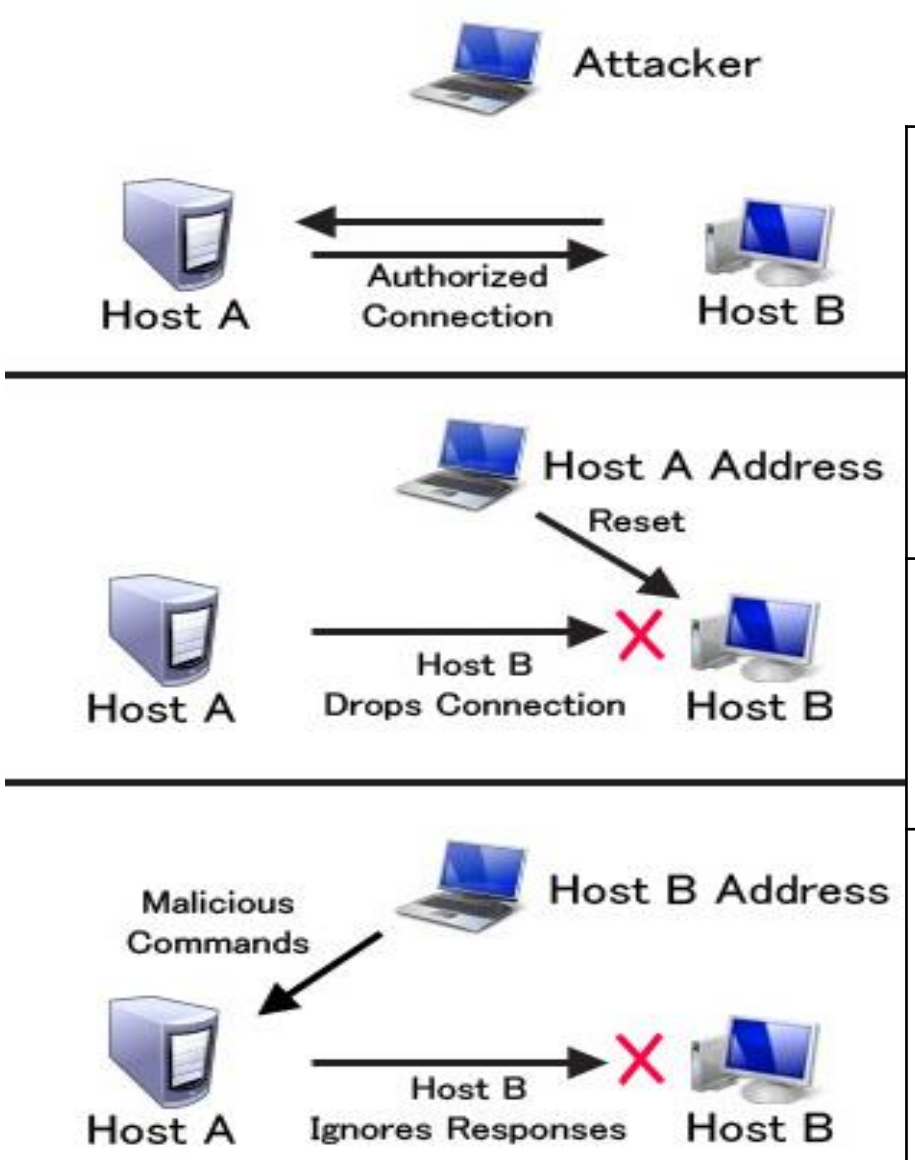


- Destruction sélective de paquets
- Modification sélective du contenu des paquets envoyés par une source
- Injection de faux paquets au nom de la source

Usurpation d’Identité (Spoofing)

●Se faire passer pour quelqu’un d’autre (machine, personne, site web, etc.) , ceci afin de faire une action illicite au nom de la victime où de tirer profit des privilèges de la victime
-Usurper l’@ MAC ou l’@ IP d’une machine, @ mail, etc.: envoi de spam, virus, ou lancer une attaque contre elle
-Usurper l’identité d’un site bancaire: attirer les clients de la banque (hameçonage)
●La base d’autres attaques:
-Homme au milieu
-Vol de session
-Déni de Service Distribué (DDoS)

Vol de Session (Session Hijacking)



-**But**: détourner un session (TCP, UDP) établit entre le client et le serveur.

-Le client doit présenter un **password** pour pouvoir établir la session, que l'attaquant ne possède pas. Après authentification, la communication n'est plus sécurisé entre client/serveur

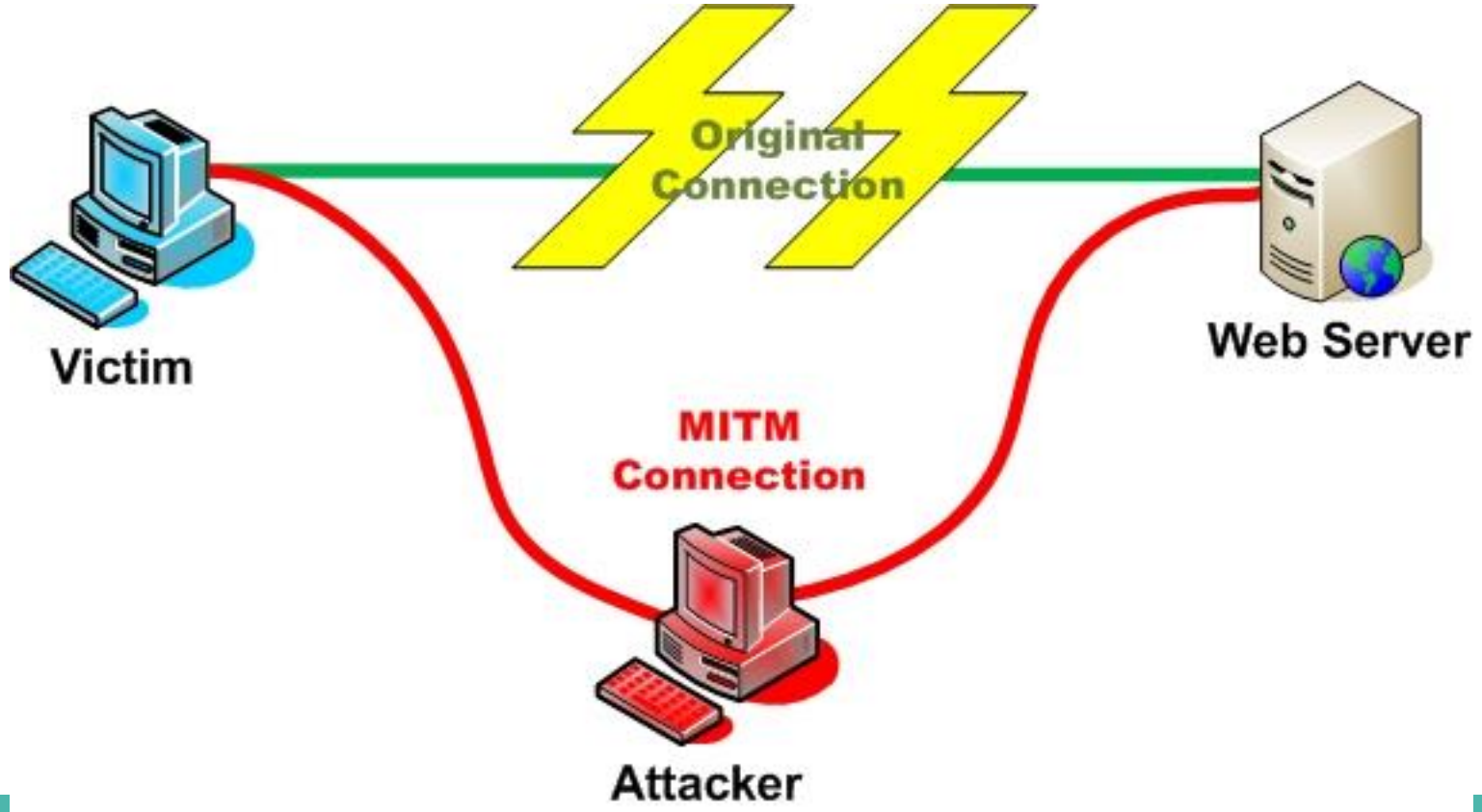
-Une fois l'authentification passée, l'attaquant récupère le *numéro de session* (**ID Session**) échangé, usurpe l'@IP du serveur, puis envoi un message de fermeture de session au client

-Ensuite, il usurpe l@IP du client et continue la session avec le serveur en utilisant **ID Session**

-**L'attaquant doit être sur le même réseau que la victime ou le serveur pour réussir**

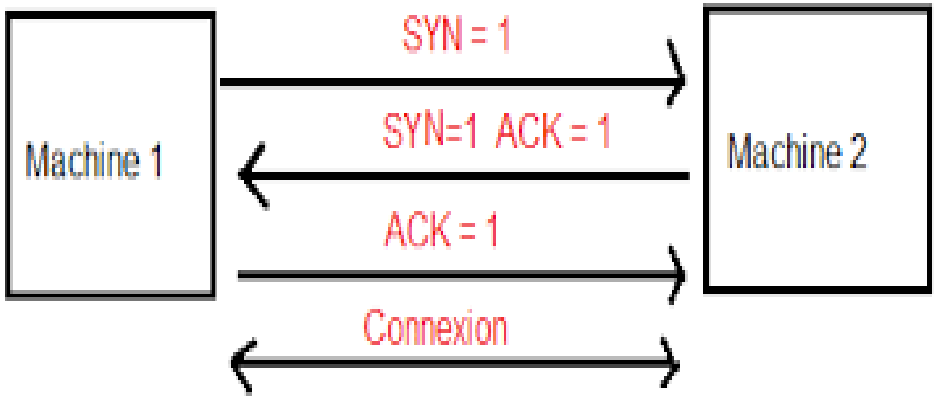
Homme au Milieu (Man-In-The-Middle)

- L'attaquant se situe au milieu de la communication. Il se fait passer pour le serveur quand il communique avec la victime, et se fait passer pour la victime quand il communique avec le serveur

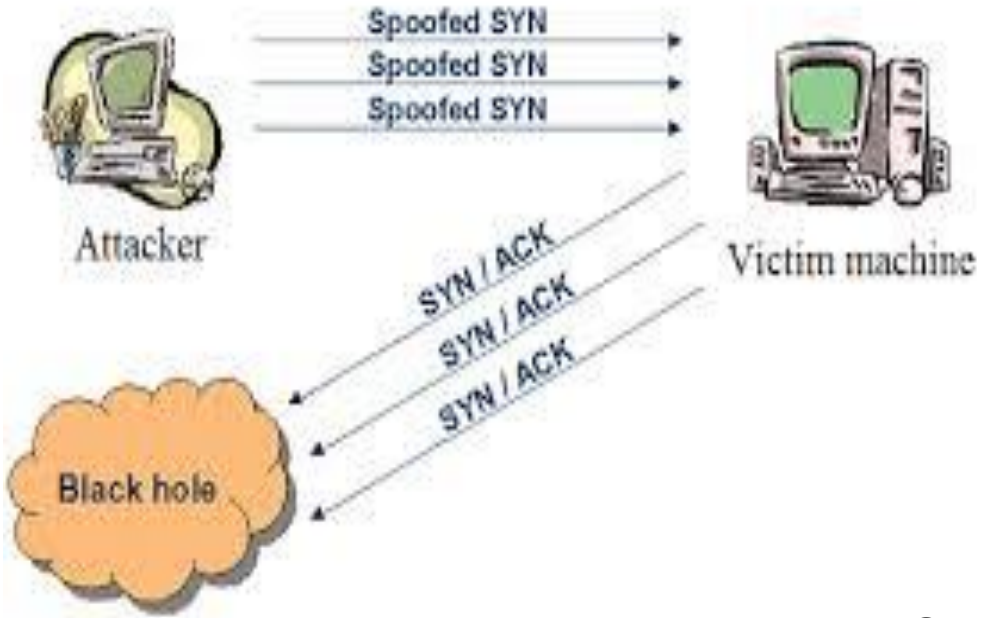


Déni de Service (DoS)

- **But:** Porter atteinte à la disponibilité d'une ressource (mémoire, BW, stockage, calcul, etc.)
- **TCP-SYN Flooding:** saturer les ressources mémoire d'une machine (serveur) en induisant des connexion semi ouvertes par envoi de SYN



Connexion légitime:
Serveur (Machine 2) alloue des ressources (espace mémoire) pour chaque SYN, jusqu'à la réception de ACK



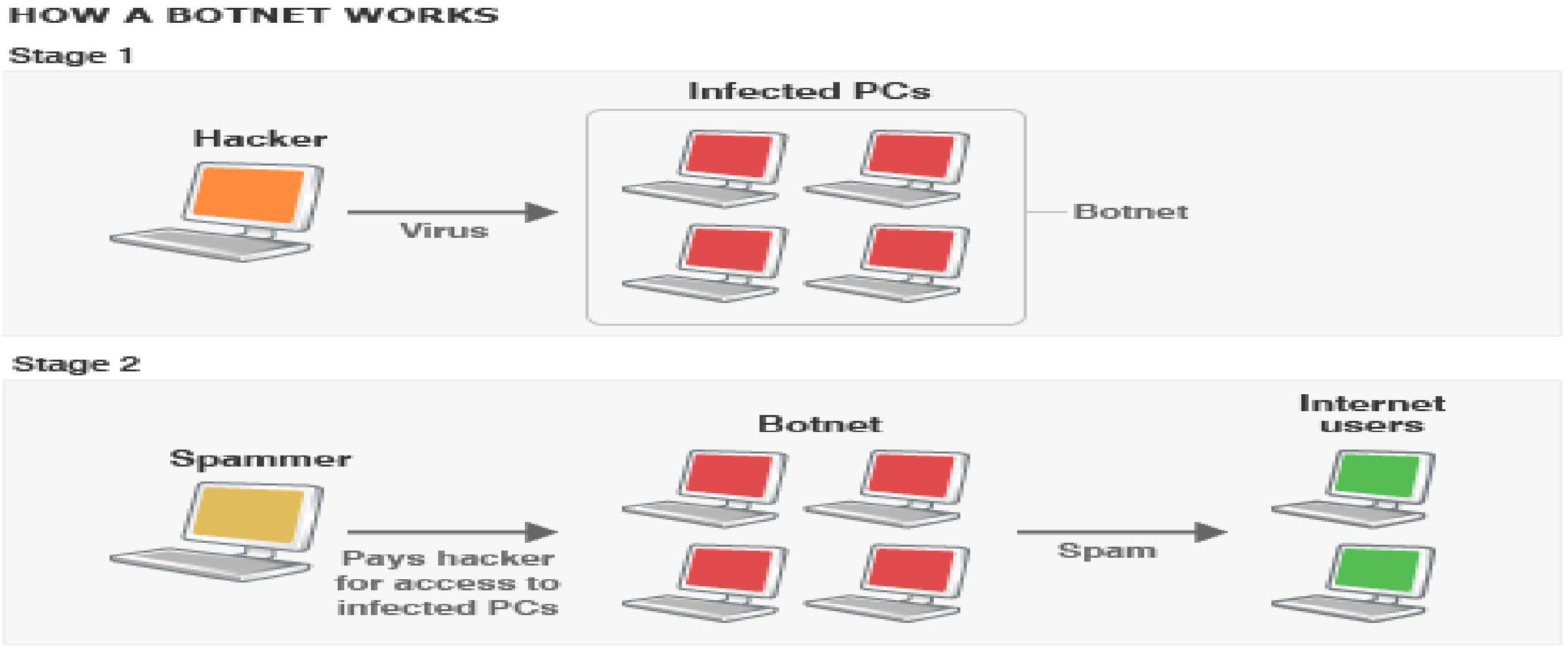
SYN-Flood: l'attaquant envoi plusieurs SYN frauduleux (@IP usurpées), qui ne seront jamais acquittés

Déni de Service (DoS) Distribué

●DoS dont la source est un ensemble de machines réel, le plus souvent des machines zombie

●**Botnet (Zombie)** : ensemble de machines infectées, contrôlées par un attaquant, et servant entre autres à effectuer un DDoS
-Détection difficile → difficile de différencier une requête légitime d'une requête zombie
-Saturation de la bande passante de la victime
-Saturation des ressources calcul/stockage de la victime
-Empêche des connexions en provenance de clients légitimes

Botnet source de DDoS



Stage 1: A hacker sends out a virus or worm over the internet to infect vulnerable home computers. This creates a network of slave machines known as a botnet.
Stage 2: The hacker sells or hires out the botnet to other criminals who use it for fraud, spamming, DDoS attacks and other cyber crimes.