

# Sécurité Informatique

## Chapitre 2 : Menaces et malveillances Informatiques

F.Z. Filali

Février 04, 2018



- 1 Rappel
- 2 Terminologies
  - Vulnérabilités
  - Menaces
  - Attaques
  - Exemples
- 3 Classification des Menaces
  - Menaces non informatiques
  - Menaces informatiques non intentionnelles
  - Menaces informatiques intentionnelles
  - Menaces Passives
  - Menaces Actives
  - Classe de Menaces selon l'action
- 4 Attaquants
  - Catégories
  - Types
- Attaquants
- 5 Recensements
- 6 Malveillance Informatique
  - Malveillance Informatique
  - Logiciels malveillants
  - Malveillance par Messagerie
  - Exploit et intrusion
  - Malveillance Web
- 7 Réalisation d'une attaque
- 8 Techniques d'attaque
  - Attaques de mots de passe
  - Attaques par Déni de service
  - Attaques par usurpation d'identité
  - Attaques man in the middle
  - Attaques par débordement de tampon
  - Attaques par faille matérielle
  - Attaques par ingénierie sociale



## Rappel : Critères de sécurité

### Confidentialité

- Assurer que l'information n'est pas divulguée sans autorisation.

### Disponibilité

- Assurer que l'information n'est pas interrompue sans autorisation.

### Intégrité

- Assurer que l'information n'est modifiée sans autorisation.

### Authentification

- Assurer que l'information n'est utilisée sans autorisation.



# Vulnérabilités

- Vulnérabilité :
  - faille, brèche, ou faiblesse inhérente à une entité (logicielle ou matérielle).
  - c'est une faiblesse dans la sécurité d'un système informatique qui permet à un utilisateur de faire une action malveillante.
  - elle peut être exploitée pour différentes raisons afin d'affecter plusieurs objets.
- Types possibles de vulnérabilités :
  - Logicielles ou matérielles.
  - Concernent la spécification, l'architecture, le codage, ...
  - Concernent l'utilisation (configuration, administration, déploiement, ... ).
  - Liées a l'utilisateur (mot de passe faible, non-respect des bonnes pratiques, ... )



# Vulnérabilités

- Exemples :
  - Faille dans un protocole ou algorithme cryptographique.
  - Mauvaise implémentation d'un algorithme cryptographique.
  - Mot de passe faible.
  - Comptes avec des privilèges système où le mot de passe par défaut n'a pas été modifié.
  - Programmes avec des privilèges inutiles
  - ...



# Menaces

- Une menace est un ensemble de circonstances qui pourraient causer des dommages.
- Une menace peut être un danger interne ou externe,
- C'est une violation d'une ou plusieurs propriétés de sécurité.
- Exemples :
  - Acte volontaire : écoute de trafic, usurpation d'identité, ...
  - Accident : panne électrique, bug, ...



# Attaques

- Une attaque est une tentative volontaire de violer une ou plusieurs propriétés de sécurité.
- Exemples :
  - attaque afin de voler,
  - attaque de Déni de service,
  - Attaque afin de détruire ou modifier des données,
  - ...



## Exemples

- Vulnérabilité : les ordinateurs d'une entreprise n'ont pas des logiciels anti-virus à jour.
- Menace : un attaquant peut installer un logiciel malveillant dans les ordinateurs de l'organisation afin qu'ils puissent voler des numéros de cartes de crédit.
- Attaque : Envoie d'un fichier contenant un programme malveillant à un ordinateur de l'entreprise.





UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel

Terminologies

Classification des Menaces

Attaquants

Recensements

Malveillance Informatique

Réalisation d'une attaque

Techniques d'attaque

Vulnérabilités

Menaces

Attaques

Exemples

# Exemples

- Vulnérabilité : la serrure d'une organisation est facile à crocheter.
- Menace : des voleurs pourraient entrer dans une organisation et voler des équipements.
- Attaque : récupérer une clé universelle pour ouvrir la serrure.



## Exemples

- Vulnérabilité : les employés de l'entreprise ne savent pas quelle information est sensible
- Menace : les employés divulguent des informations confidentielles.
- Attaque : Se faire passer pour un employé par téléphone pour récupérer son mot de passe.



UNIVERSITE

Abdelhamid Ibn Badis

Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
Malveillance Informatique  
Réalisation d'une attaque  
Techniques d'attaque

Menaces non informatiques  
Menaces informatiques non intentionnelles  
Menaces informatiques intentionnelles  
Menaces Passives  
Menaces Actives  
Classe de Menaces selon l'action

# Classification des Menaces

- Classification selon la technologie :
  - Informatique
  - Non informatique
- Classification selon l'intention :
  - Non intentionnelle.
  - Intentionnelle.
- Classification selon le comportement :
  - Active
  - Passive
- Classification selon l'action :
  - Interruption
  - Interception
  - Modification
  - Fabrication



UNIVERSITE

Abdelhamid Ibn Badis

Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
Malveillance Informatique  
Réalisation d'une attaque  
Techniques d'attaque

Menaces non informatiques

Menaces informatiques non intentionnelles

Menaces informatiques intentionnelles

Menaces Passives

Menaces Actives

Classe de Menaces selon l'action

- Accidents :
  - Incendie , explosion
  - Inondation, tempête
- Vol et sabotage de matériels :
  - Vol d'équipements matériels
  - Destruction d'équipements
  - Destruction de supports de sauvegarde
- Autres menaces :
  - Tout ce qui peut entraîner des pertes financières dans une société
  - Départ de personnels
  - Grèves



UNIVERSITE

Abdelhamid Ibn Badis

Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
Malveillance Informatique  
Réalisation d'une attaque  
Techniques d'attaque

Menaces non informatiques  
**Menaces informatiques non intentionnelles**  
Menaces informatiques intentionnelles  
Menaces Passives  
Menaces Actives  
Classe de Menaces selon l'action

# Menaces informatiques non intentionnelles

- Pannes/dysfonctionnements du matériel.
- Pannes/dysfonctionnements du logiciel.
- Erreurs :
  - Erreurs d'exploitation.
    - oubli de sauvegarde
    - écrasement de fichiers
  - Erreurs de manipulation des informations.
    - erreur de saisie
    - erreur de transmission
    - erreur d'utilisation
  - Erreurs de conception des applications.
  - Erreurs d'implantation.



UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
Malveillance Informatique  
Réalisation d'une attaque  
Techniques d'attaque

Menaces non informatiques  
Menaces informatiques non intentionnelles  
**Menaces informatiques intentionnelles**  
Menaces Passives  
Menaces Actives  
Classe de Menaces selon l'action

## Menaces informatiques intentionnelles

- L'ensemble des actions malveillantes faites de façon intentionnelle afin de nuire (Malveillance Informatique).
- Exemple: Virus, Vers, Cheval de Troie, logiciel espion, spam, ...



# Menaces Passives

- Menace qui ne modifie pas l'état des données ou du système.
- Faîte afin d'obtenir des données par écoute indiscretes ou surveillance des transmissions
- Deux types :
  - Analyse de trafic(écoute, indiscretion). Exemple : espionnage industriel ou commercial,
  - Capture et diffusion de données. Exemple: copie et diffusion illicite de logiciels.



UNIVERSITE

Abdelhamid Ibn Badis

Mostaganem

Rappel  
Terminologies  
**Classification des Menaces**  
Attaquants  
Recensements  
Malveillance Informatique  
Réalisation d'une attaque  
Techniques d'attaque

Menaces non informatiques  
Menaces informatiques non intentionnelles  
Menaces informatiques intentionnelles  
Menaces Passives  
**Menaces Actives**  
Classe de Menaces selon l'action

# Menaces Actives

- C'est une menace qui Implique la modification ou création des données.
- Exemples : Virus qui détruit des données, modification d'un email, ...



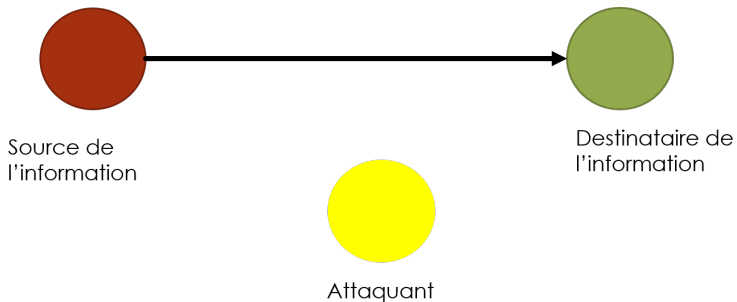


UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
**Classification des Menaces**  
Attaquants  
Recensements  
Malveillance Informatique  
Réalisation d'une attaque  
Techniques d'attaque

Menaces non informatiques  
Menaces informatiques non intentionnelles  
Menaces informatiques intentionnelles  
Menaces Passives  
Menaces Actives  
Classe de Menaces selon l'action

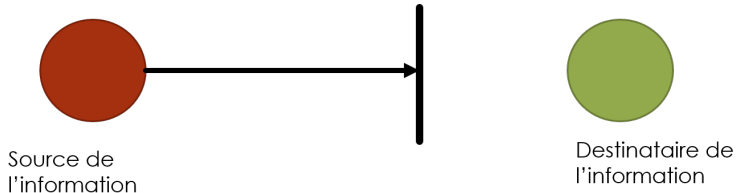
## Classe de Menaces selon l'action : Flux de données normal





## Classe de Menaces selon l'action : Interruption

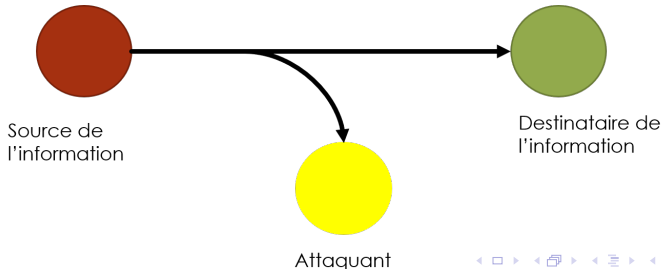
- Un composant du système est détruit ou devient indisponible ou inutilisable.
- Exemple :
  - La destruction d'un disque dur,
  - La coupure d'une ligne de communication,
  - La mise hors service d'un serveur web.





## Classe de Menaces selon l'action : Interception

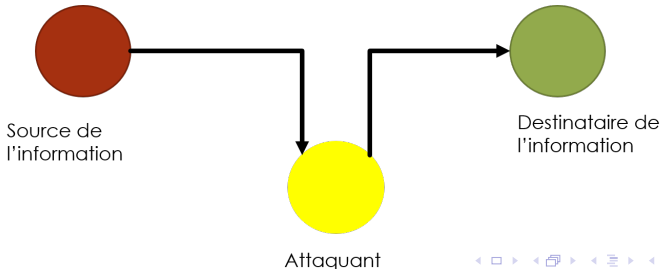
- Une tierce partie non autorisée obtient un accès à une ressource.
- Exemple :
  - Une écoute téléphonique,
  - Une copie non autorisée d'un fichier ou programme.





## Classe de Menaces selon l'action : Modification

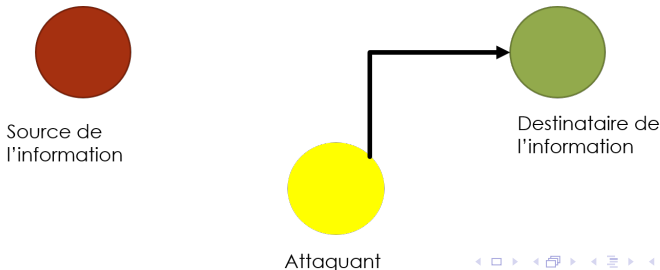
- Une tierce partie non autorisée obtient accès à une ressource et la modifie de façon (presque) indétectable.
- Exemple :
  - Modification d'un message envoyé sur le réseau,
  - Modification du comportement d'un programme par un virus.





## Classe de Menaces selon l'action : Fabrication

- Une tierce partie non autorisée insère des contrefaçons dans le système.
- Exemple :
  - Envoie d'un email en se faisant passer pour un autre.
  - L'ajout de données dans un fichier





UNIVERSITE

Abdelhamid Ibn Badis

Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
**Attaquants**  
Recensements  
Malveillance Informatique  
Réalisation d'une attaque  
Techniques d'attaque

Catégories  
Types  
Attaquants

## Catégories d'attaquants

- Hacker : s'introduire dans le système informatique (hacking=piratage)
- Cracker : destruction ou vol de données.

## Types d'attaquants par compétence

- Pirate amateur (script kiddies) : Utilise des outils d'exploitation automatique de failles.
- Web Pirate : failles connues (surtout web).
- Pirate professionnel : Connaissances pointues des systèmes et réseaux, travaille en équipe avec des moyens financiers, techniques, ...



UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
**Attaquants**  
Recensements  
Malveillance Informatique  
Réalisation d'une attaque  
Techniques d'attaque

Catégories  
Types  
Attaquants

# Types d'attaquants par objectif

- L'argent
- Hacktiviste : Terroriste , Anonymous
- Espions : Etatique, Industriel
- Petit rusé





# Attaquants

- La moyenne des pirates est plus bête qu'avant.
- Mais les meilleurs pirates sont bien meilleurs qu'avant :
  - plus psychologues (Social Engineering, virus)
  - plus pragmatiques (Efficacité, Argent)
  - plus techniques (Ingénieurs au chômage après éclatement de la bulle internet)

# Recensement de Vulnérabilités et Attaques

Recensement de failles : <https://www.cvedetails.com/>

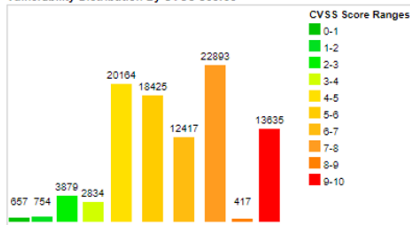
## Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	<a href="#">657</a>	0.70
1-2	<a href="#">754</a>	0.80
2-3	<a href="#">3879</a>	4.00
3-4	<a href="#">2834</a>	2.90
4-5	<a href="#">20164</a>	21.00
5-6	<a href="#">18425</a>	19.20
6-7	<a href="#">12417</a>	12.90
7-8	<a href="#">22893</a>	23.80
8-9	<a href="#">417</a>	0.40
9-10	<a href="#">13635</a>	14.20
<b>Total</b>	96075	

Weighted Average CVSS Score: **6.7**

Vulnerability Distribution By CVSS Scores



# Recensement de Vulnérabilités et Attaques

Utilisation des failles : <https://www.exploit-db.com>

## Remote Exploits

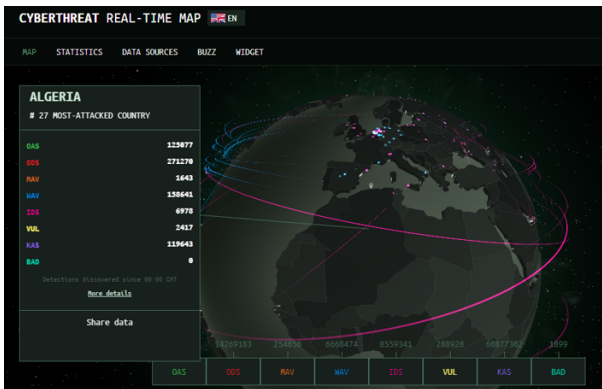


This exploit category includes exploits for remote services or applications, including client side exploits.

Date Added	D	A	V	Title	Platform	Author
2018-02-01		-		BMC Server Automation RSCD Agent - NSH Remote Command Execution (Metasploit)	Multiple	Metasploit
2018-02-01				Sync Breeze Enterprise 10.4.18 - Remote Buffer Overflow (SEH)	Windows	Daniel Teixeira
2018-01-30		-		HPE IMC 7.3 - RMI Java Deserialization	Windows	Chris Lyne
2018-01-29		-		Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution (Metasploit)	Multiple	Metasploit
2018-01-28		-		Trend Micro Threat Discovery Appliance 2.6.1062r1 - 'dlp_policy_upload.cgi' Remote Code...	Linux	mr_me
2018-01-26		-		BMC BladeLogic 8.3.00.64 - Remote Command Execution	Multiple	Paul Taylor
2018-01-26		-		Exodus Wallet (ElectronJS Framework) - Remote Code Execution	Windows	Wfiki






















# Recensement de Vulnérabilités et Attaques

Attaques en temps réels : <http://cybermap.kaspersky.com>



# Recensement de Vulnérabilités et Attaques

Attaques en temps différé : <http://zone-h.org>

Time	Notifier	H	M	R	L	★ Domain	OS	View
21:48	TEAM_CC	M				 sakarrubtech.com/hack.txt	Linux	<a href="#">mirror</a>
21:48	TEAM_CC	M	R			 maailindustries.com/hack.txt	Linux	<a href="#">mirror</a>
21:48	TEAM_CC	M				 amfluidtech.com/hack.txt	Linux	<a href="#">mirror</a>
21:48	TEAM_CC	M	R			 ngwater.in/hack.txt	Linux	<a href="#">mirror</a>
21:41	4ndr3v	M				 abbusroyalenfield.com/probros.php	Linux	<a href="#">mirror</a>
21:39	Beyaz_Hacker					 sadiqd.com/beyaz.html	Linux	<a href="#">mirror</a>
21:30	mhamdi_jeber					 ilovemydogmorethanmykids.com/j...	Linux	<a href="#">mirror</a>
21:30	4ndr3v					 truekirana.com/probros.php	Linux	<a href="#">mirror</a>
21:30	mhamdi_jeber					 www.doninspectacle.com/js.htm	Unknown	<a href="#">mirror</a>
21:30	mhamdi_jeber	M				 casmir.pl/js.php	Linux	<a href="#">mirror</a>
21:30	mhamdi_jeber	M				 avanua.com/js.php	Linux	<a href="#">mirror</a>
21:30	mhamdi_jeber	M				 avanua.pl/js.php	Linux	<a href="#">mirror</a>
21:30	mhamdi_jeber					 ander.pl/js.php	Linux	<a href="#">mirror</a>
21:28	LUN4T1C0					 www.zuikw.com/b0x.txt	Linux	<a href="#">mirror</a>
21:28	LUN4T1C0	M				 ufrs Jag-uao.com/b0x.txt	Linux	<a href="#">mirror</a>
21:28	LUN4T1C0					 miaplecic.com/b0x.txt	Linux	<a href="#">mirror</a>
21:28	LUN4T1C0					 galoshi.com.ua/b0x.txt	Linux	<a href="#">mirror</a>
21:28	LUN4T1C0					 www.ilikeonyabike.com/b0x.txt	Linux	<a href="#">mirror</a>
21:28	LUN4T1C0					 harmanlii.online/b0x.txt	Win 2012	<a href="#">mirror</a>
21:28	LUN4T1C0					 www.ladyzarina.com/b0x.txt	Linux	<a href="#">mirror</a>
21:28	LUN4T1C0					 wangnianming.com/b0x.txt	Unknown	<a href="#">mirror</a>



UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
**Malveillance Informatique**  
Réalisation d'une attaque  
Techniques d'attaque

**Malveillance Informatique**  
Logiciels malveillants  
Malveillance par Messagerie  
Exploit et intrusion  
Malveillance Web

# Malveillance Informatique

- La malveillance informatique représente les différentes menaces informatique intentionnelle.
- Classes de malveillances informatiques :
  - Logiciels malveillants,
  - Malveillance par Messagerie,
  - Exploit et intrusion,
  - Malveillance Web.



# Logiciels malveillants

- Malware en anglais, aussi dénommé logiciel nuisible ou programme malveillant.
- C'est une application développée dans le but de nuire à un système informatique, sans le consentement de l'utilisateur.
- Multitude de types : virus, ver, trojan, rootkit, botnet, spyware, ...



# Logiciels malveillants : Virus

- Est un programme illicite qui s'insère dans des programmes ou fichiers légitimes appelés hôtes.
- Capable de **se dupliquer automatiquement** sur d'autres ordinateurs (disquette, CD, Flash disque, web, ...)
- Il peut avoir comme effet plus ou moins grave de perturber le fonctionnement de l'ordinateur infecté.
- Plus de 100 000 virus connus : Yamanner, Cabir, Psyb0t, ...
- Surtout Windows.





# Logiciels malveillants : Virus

Types :

- **Virus programme (virus parasite).**
- **Virus d'amorçage (virus système).**
- **Virus interprété.**
- **Virus multiparties (virus RAM).**
- **Virus polymorphe.**
- **Rétrovirus.**



# Logiciels malveillants : Virus

Types :

- **Virus programme (virus parasite)** : conçu pour infecter un type particulier de fichiers exécutables (par exemple .EXE ou .COM ) en manipulant un logiciel particulier de manière à activer le virus lorsque le programme cible est exécuté, puis à le transmettre à d'autres fichiers. Les virus furtifs peuvent masquer leur présence de plusieurs façons et certains échappent à la détection pendant des années.
- **Virus d'amorçage (virus système).**
- **Virus interprété.**
- **Virus multiparties (virus RAM).**
- **Virus polymorphe.**
- **Rétrovirus.**

# Logiciels malveillants : Virus

Types :

- **Virus programme (virus parasite).**
- **Virus d'amorçage (virus système)** : les premiers secteurs du disque (secteur de la table de partition et secteur d'amorçage/ Boot et MBR) peuvent contenir du code exécutable. C'est là où va s'installer le virus et il sauvegarde le code excédent dans un autre secteur libre ou occupé et à chaque démarrage, le virus sera résident en mémoire et capable d'infecter une autre disque ou partition.
- **Virus interprété.**
- **Virus multiparties (virus RAM).**
- **Virus polymorphe.**
- **Rétrovirus**



# Logiciels malveillants : Virus

Types :

- **Virus programme (virus parasite).**
- **Virus d'amorçage (virus système).**
- **Virus interprété** : regroupe deux types :
  - Virus macro : Une macro est une série de commandes. Un fichier comportant une macro est un programme qui peut être infecté par un virus. Le simple fait d'ouvrir un document ou un tableur qui contient une macro peut activer le virus. Celui-ci infecte d'abord les fichiers de démarrage du programme, puis tous les fichiers auxquels on accède avec l'application.
  - Virus de script : Le langage script est un langage de programmation destiné à contrôler l'environnement d'un logiciel. Lorsqu'il est interprété, on peut l'exécuter sur tout ordinateur disposant de l'interpréteur approprié. Deux les plus utilisés sont les VBScript et les Javascript.
- **Virus multiparties (virus RAM).**
- **Virus polymorphe.**
- **Rétrovirus**



# Logiciels malveillants : Virus

Types :

- **Virus programme (virus parasite).**
- **Virus d'amorçage (virus système).**
- **Virus interprété.**
- **Virus multiparties (virus RAM) :** Ces sont des virus qui cumulent les cibles et renforcent ainsi leur capacité de contamination. Ils cherchent souvent à infecter les zones mémoire du disque dur ou des autres secteurs de masse et les fichiers exécutables. Leur but étant une plus grande propagation et tente de faire planter l'ordinateur. Certains virus de ce type infectent par exemple le secteur de partition du système puis, une fois résident en mémoire vive, infectes les fichiers exécutables sur d'autre unité logique.
- **Virus polymorphe.**
- **Rétrovirus**



# Logiciels malveillants : Virus

Types :

- **Virus programme (virus parasite).**
- **Virus d'amorçage (virus système).**
- **Virus interprété.**
- **Virus multiparties (virus RAM).**
- **Virus polymorphe** : Ce sont des virus qui peuvent prendre plusieurs formes. Les formes à prendre sont relatives en fonction de l'antivirus que l'utilisateur utilise. Cette relativité est réalisée en dotant les virus de fonction de chiffrement et de déchiffrement de leur signature (la succession de bits qui les identifie), de façon à ce que seuls ces virus soient capables de reconnaître leur propre signature. En effet, il est plus difficile pour les antivirus de détecter notamment les virus grâce à leur signature.
- **Rétrovirus.**



# Logiciels malveillants : Virus

Types :

- **Virus programme (virus parasite).**
- **Virus d'amorçage (virus système).**
- **Virus interprété.**
- **Virus multiparties (virus RAM).**
- **Virus polymorphe.**
- **Rétrovirus** : ou "virus flibustier" (bounty hunter) est un virus doté la faculté de déchiffrer et de modifier les signatures des antivirus afin de les rendre inopérants.



# Logiciels malveillants : Virus

## Techniques de Contamination :

- par **recouvrement**.
- par **ajout**.
- par **entrelacement**.





# Logiciels malveillants : Virus

## Techniques de Contamination :

- par **recouvrement** : le virus écrase les premières instructions du fichier ou programme par ses propres instructions. La taille du fichier ne change par contre le fichier ne pourra pas être utilisé.
- par **ajout**.
- par **entrelacement**.



# Logiciels malveillants : Virus

## Techniques de Contamination :

- par **recouvrement**.
- par **ajout** : le virus ajoute ces instructions avant le code du fichier ou programme contaminé. Ainsi le virus exécute son code puis repasse la main à ce dernier. La taille du fichier est modifiée.
- par **entrelacement**.



# Logiciels malveillants : Virus

## Techniques de Contamination :

- par **recouvrement**.
- par **ajout**.
- par **entrelacement** : le virus insère du code entre les blocs valides du programme. Elle est plus difficile à mettre en œuvre et difficile à détecter.



# Logiciels malveillants : Ver Informatique (Worm)

- Un ver informatique est un virus **réseau**.
- C'est un programme malveillant qui peut se reproduire et se déplacer à travers un réseau sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc.)
- Il exploite les ressources système de l'ordinateur infecté afin d'espionner, installer une porte dérobée, détruire des données, envoyer de multiple requêtes, ...
- Les vers actuels se propagent principalement grâce à la messagerie.
- Exemple : I love you, Kakworm, Bagle, ...



## Logiciels malveillants : Cheval de Troie (trojan)

- C'est un programme malveillant placé dans un programme sain. Il est programmé pour être installés de manière invisible par des utilisateurs naïfs, ou des programme illicite, ....
- Il peut servir à voler des mots de passe, copier des données sensibles, créer une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur (ouvrir un port).
- Exemple : Zeus, Back office, Vindo, ...





## Logiciels malveillants : Cheval de Troie (trojan)

Etapes de contamination d'un trojan :

- Intrusion de l'ordinateur cible,
- Modification du système d'exploitation (démarrage du trojan avec le système),
- Écoute et attente des commande du pirate,
- Accès à l'ordinateur infecté par le biais du trojan (contrôle à distance, récupération d'informations et fichiers, accès à la webcam, ...)



## Logiciels malveillants : Espioniciel (spyware)

- Un espioniciel (en anglais spyware) est un programme espion chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé.
- Ils s'installent généralement en même temps que d'autres logiciels (la plupart du temps des freewares ou sharewares, souvent légaux cités dans la licence).
- Il va enregistrer et transmettre à quelqu'un d'autre toute l'activité de l'ordinateur infecté. Il permet de tracer des URL des sites visités, traquer des mots-clés saisis dans les moteurs de recherche, analyser des achats réalisés via internet, voire les informations de paiement bancaire, ...





UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
**Malveillance Informatique**  
Réalisation d'une attaque  
Techniques d'attaque

Malveillance Informatique  
**Logiciels malveillants**  
Malveillance par Messagerie  
Exploit et intrusion  
Malveillance Web

## Logiciels malveillants : Sniffer

- Un sniffer est un type particulier d'espion logiciel qui permet de récupérer les données circulant sur le réseau (mots de passe, carte bancaires, ...)







# Logiciels malveillants : Keylogger

- Un keylogger (enregistreur de touches) est un programme espion chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur.
- Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur.



# Logiciels malveillants : Bombes logiques

- C'est un programme malveillant ne pouvant se reproduire, souvent associé avec un cheval de Troie.
- C'est un programme qui est toujours destructeur. Il contient une partie de code qui explosera à un moment donné (temps, date, action, signal ...) et non lors de l'installation de la bombe logique.
- Exemple : cheval de Troie associé à un écran de veille, la bombe logique explosera après quelques heures de veille.





## Logiciels malveillants : Zombies et Botnet

- Une machine zombie est un ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique (suite à une infection par ver ou cheval de Troie). La machine sera utilisée comme rebond, généralement pour faire des attaques.
- Un botnet est un ensemble de machines robots (bots) ou machines zombies sous le contrôle d'un ou plusieurs pirates. Il est Utilisé pour lancer des attaques à une grande échelle (déné de service, spams, ...) afin d'avoir des capacités considérables et un impact plus important.





# Logiciels malveillants : Rançongiciel (Ransomware)

- C'est un logiciel malveillant (virus ou cheval de Troie) qui prend en otage des données personnelles.
- Pour cela, il chiffre des données personnelles puis demande à la victime d'envoyer de l'argent en échange de la clé de déchiffrement.
- Il peut aussi bloquer l'accès à la machine jusqu'à ce que l'utilisateur paie une somme d'argent.





## Logiciels malveillants : Logiciel publicitaire (Adware)

- C'est un programme gratuit financé par des publicités qui s'affichent dans des fenêtres indépendantes ou dans une barre d'outils sur l'ordinateur ou dans le navigateur.
- La plupart des adwares sont désagréables, mais sûrs. Cependant, certains sont utilisés pour recueillir des informations personnelles, les sites web visités. . .





UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
**Malveillance Informatique**  
Réalisation d'une attaque  
Techniques d'attaque

Malveillance Informatique  
Logiciels malveillants  
**Malveillance par Messagerie**  
Exploit et intrusion  
Malveillance Web

## Malveillance par Messagerie : Pourriel (spam)

- Un spam (pourriel, junk mail, courrier indésirable) est l'envoi massif de courrier électronique à des destinataires ne l'ayant pas sollicité.
- Les spammeurs collectent les adresses électroniques sur internet (dans les forums, sur les sites internet, dans les groupes de discussion, ...)



## Malveillance par Messagerie : Hameçonnage (phishing)

- L'hameçonnage est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès des utilisateurs.
- Les utilisateurs reçoivent un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce (copie conforme du site original).



## 56 / 84





UNIVERSITE

Abdelhamid Ibn Badis

Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
**Malveillance Informatique**  
Réalisation d'une attaque  
Techniques d'attaque

Malveillance Informatique  
Logiciels malveillants  
Malveillance par Messagerie  
**Exploit et intrusion**  
Malveillance Web

## Exploit et intrusion : Porte dérobée (backdoor)

- Fonctionnalité secrète d'un logiciel permettant de surveiller ou de prendre le contrôle d'un ordinateur.
- Elle est due à une faute de conception accidentelle ou intentionnelle (cheval de Troie généralement).
- Exemple : une porte dérobé dans le SGBD Interbase de Borland qui permet de se connecter en tant qu'administrateur.



## Exploit et intrusion : Intrusion

- C'est une technique qui permet d'infiltrer un système informatique ou un réseau afin de réaliser une attaque.



UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
**Malveillance Informatique**  
Réalisation d'une attaque  
Techniques d'attaque

Malveillance Informatique  
Logiciels malveillants  
Malveillance par Messagerie  
**Exploit et intrusion**  
Malveillance Web

## Exploit et intrusion : Exploit

Un exploit est un programme permettant à un attaquant d'exploiter une faille de sécurité informatique :

- Exploit distant (remote exploit) : exécuté à distance.
- Exploit local : exécuté sur la machine locale.





UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
**Malveillance Informatique**  
Réalisation d'une attaque  
Techniques d'attaque

Malveillance Informatique  
Logiciels malveillants  
Malveillance par Messagerie  
**Exploit et intrusion**  
Malveillance Web

## Exploit et intrusion : Rootkit

- Un rootkit est un ensemble de programmes permettant d'installer sur un système des logiciels malveillants et de les rendre difficilement détectables.
- Un rootkit fournit un accès administrateur à un ordinateur à l'insu de l'utilisateur en exploitant une porte dérobée.





UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
**Malveillance Informatique**  
Réalisation d'une attaque  
Techniques d'attaque

Malveillance Informatique  
Logiciels malveillants  
Malveillance par Messagerie  
**Exploit et intrusion**  
Malveillance Web

# Exploit et intrusion : Zero Day

Zero day (zéro jour) fait référence à la date depuis laquelle les concepteurs et programmeurs ont connaissance du problème de sécurité dans le logiciel. Il existe deux types de zero days :

- Une vulnérabilité zero day est une faille de sécurité logicielle et peut être présente dans un navigateur ou une application.
- Un exploit zero day, est une menace informatique qui tire parti des vulnérabilités zero day pour installer un logiciel malveillant sur un appareil.





## Malveillance Web : Cookies

- Un cookie est un fichier texte disposé sur le disque dur local par un serveur Web. Il contient les informations d'identification, et ne peut pas être exécuté comme un programme, ni propager de virus.
- En lui-même, un cookie ne peut nuire à un ordinateur, car il ne contient pas et ne peut contenir de code.
- Toutefois, un cookie peut contribuer à ce que des actions malveillantes interviennent sur le système sur lequel il est hébergé. Etant un simple fichier texte, il est aussi vulnérable et peut être lu par d'autres applications.



UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
**Malveillance Informatique**  
Réalisation d'une attaque  
Techniques d'attaque

Malveillance Informatique  
Logiciels malveillants  
Malveillance par Messagerie  
Exploit et intrusion  
Malveillance Web

## Malveillance Web : Injection de Code

- Consiste à injecter du code afin de détourner l'utilisation normale d'un programme dans le but d'exécuter un code ou une commande arbitraire.





## Malveillance Web : Injection de Code

Elle peut prendre de multiples formes :

- Injection XSS (Cross Site Scripting) : exploitation d'une faille ou vulnérabilité des sites web permettant d'injecter du contenu dans une page web.
- Injection SQL : pour entrer des instructions dans le but d'effectuer des requêtes directement sur la base de données,
- Injection LDAP : pour modifier le contenu d'un annuaire,
- Injection XPath : afin d'extraire un document XML et ainsi pouvoir dans certaines configurations, accéder à une base de données et des fichiers sensibles.





UNIVERSITE  
Abdelhamid Ibn Badis  
Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
Malveillance Informatique  
**Réalisation d'une attaque**  
Techniques d'attaque

# Réalisation d'une attaque

- Reconnaissance.
- Scan et repérage des vulnérabilités.
- Utilisation des vulnérabilités et intrusion.
- Accès et maintien de l'accès.
- Camouflage et suppression des traces.



# Réalisation d'une attaque

- Reconnaissance : Collecte d'informations sur la machine cible par ingénierie sociale, interrogation TCP (scan des ports ouverts), interrogation des services (DNS, versions, ...).
- Scan et repérage des vulnérabilités.
- Utilisation des vulnérabilités et intrusion.
- Accès et maintien de l'accès.
- Camouflage et suppression des traces.

# Réalisation d'une attaque

- Reconnaissance.
- Scan et repérage des vulnérabilités : consiste à scanner le réseau ou la machine en utilisant des sniffer, outils ping, scanners de vulnérabilités ... afin d'extraire des informations telles que le type de la machine, les ports ouverts, les détails sur le système d'exploitation, les services installés, ...
- Utilisation des vulnérabilités et intrusion.
- Accès et maintien de l'accès.
- Camouflage et suppression des traces.



# Réalisation d'une attaque

- Reconnaissance.
- Scan et repérage des vulnérabilités.
- Utilisation des vulnérabilités et intrusion : exploitation des vulnérabilités afin d'accéder à la machine. Se fait à différents niveaux : Système d'exploitation, Application, Réseau.
- Accès et maintien de l'accès.
- Camouflage et suppression des traces.



# Réalisation d'une attaque

- Reconnaissance.
- Scan et repérage des vulnérabilités.
- Utilisation des vulnérabilités et intrusion.
- Accès et maintien de l'accès : consiste à conserver la propriété du système piraté. (backdoor, rootkit, trojan, ...)
- Camouflage et suppression des traces.



UNIVERSITE

Abdelhamid Ibn Badis

Mostaganem

Rappel  
Terminologies  
Classification des Menaces  
Attaquants  
Recensements  
Malveillance Informatique  
**Réalisation d'une attaque**  
Techniques d'attaque

# Réalisation d'une attaque

- Reconnaissance.
- Scan et repérage des vulnérabilités.
- Utilisation des vulnérabilités et intrusion.
- Accès et maintien de l'accès.
- Camouflage et suppression des traces : activités menées pour cacher les actes malveillants.



# Techniques d'attaque

Plusieurs techniques existantes :

- Mots de passe,
- Déni de service,
- Usurpation d'identité
- Man-in-the-Middle,
- Débordement de tampon,
- Failles matérielles,
- Ingénierie sociale.

# Attaques de mots de passe

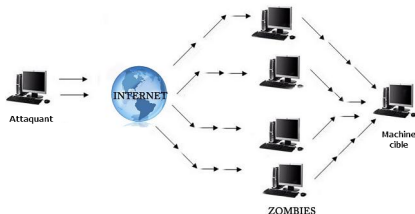
- Lors de la connexion à un système ou un compte → besoin d'un identifiant (login ou username) et un mot de passe (password) pour y accéder.
- Méthodes :
  - Attaque par force brute : tester tous les mots de passe possibles.
  - Attaque par dictionnaire : utiliser une liste (dictionnaire) de mots de passe connus.
  - Attaque hybride : combinaison d'attaque par force brute et d'attaque par dictionnaire. Elle vise particulièrement les mots de passe constitués d'un mot traditionnel et suivi d'une lettre ou d'un chiffre.
  - Attaque par tables Arc en ciel : une structure de données pour retrouver un mot de passe à partir de son empreinte.
  - Attaque par keylogger et spyware,
  - Attaque par Phishing.





## Attaques par Dénî de service

- Une attaque par déni de service (DoS, Denial of Service) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources informatiques. En général à l'encontre des serveurs, afin qu'ils ne puissent être utilisés et consultés.
- Un déni de service provoqué par plusieurs machines, est appelé déni de service distribué (DDoS, Distributed Denial of Service).





## Attaques par Déni de service : types

- déni de service par saturation : submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles.
- déni de service par exploitation de vulnérabilités : consiste à exploiter une faille du système distant afin de le rendre inutilisable.



## Attaques par Déni de service : techniques

- Attaque par réflexion (smurf) : est une attaque basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau.
- Attaque du ping de la mort (ping of death) : consiste à créer un datagramme IP dont la taille totale excède la taille maximum autorisée (65 536 octets).
- Attaque par fragmentation (fragment attack) : consiste à exploiter exploitant le principe de fragmentation du protocole IP. Par exemple, insérer dans des paquets fragmentés des informations de décalage erronées.
- Attaque LAND : consiste ainsi à envoyer un paquet possédant la même adresse IP et le même numéro de port dans les champs source et destination des paquets IP.

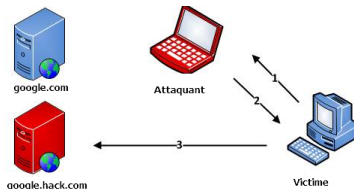


## Attaques par Déni de service : techniques

- Attaque SYN (TCP /SYN flooding) : exploite le mécanisme de poignée de mains en trois temps ( Three-ways handshake) du protocole TCP, en envoyant un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide.
- Attaque de la faille TLS/SSL : permet de faire des attaques de type DDOS contre des cibles utilisant le protocole HTTPS. Le principe est d'envoyer de nombreuses demandes de renégociation du protocole SSL. Le client demande au serveur de générer une nouvelle clé de chiffrement pour la connexion en cours. Ces demandes créent une grande consommation de ressources CPU sur le serveur Web .
- Attaque par requêtes élaborées : consiste à envoyer en masse, non pas des paquets sans objet ou exploiter des failles mais des requêtes légitimes (attaque sur la couche 7 du modèle OSI) afin de rendre inaccessible un site Web ou un service.

## Attaques par usurpation d'identité

- L'usurpation d'identité est une technique qui consiste à se faire passer pour une entité qu'on est pas (protocole, application, site Web, ...)
- L'usurpation d'identité peut prendre diverses formes difficiles à détecter. En général, l'attaquant n'essaie plus de tromper directement l'utilisateur mais plutôt les logiciels et les procédures automatisées du système d'exploitation .





## Attaques par usurpation d'identité : types

- L'usurpation d'adresse IP (mystification ou spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.
- Détournement DNS (DNS spoofing): substitution des paramètres TCP/IP de l'ordinateur afin qu'il pointe sur un serveur DNS de l'attaquant.
- ARP Spoofing. . .



# Attaques man in the middle

- Attaque de l'homme au milieu (ou attaques de l'intercepteur), parfois notée MITM, est une technique d'attaque dans laquelle un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.
- La plupart des attaques de type "man in the middle" consistent à écouter le réseau à l'aide d'un sniffer.



## Attaques man in the middle : techniques

- Attaque de rejeu (replay attack) : consiste à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel (sans aucun déchiffrement) au serveur destinataire. Ainsi, selon le contexte, le pirate peut bénéficier des droits de l'utilisateur.
- Détournement de session TCP (TCP session hijacking] : consiste à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où l'authentification s'effectue uniquement à l'ouverture de la session , un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.
- Attaque du protocole ARP : consiste à s'interposer entre deux machines du réseau et transmettre à chacune un paquet ARP falsifié indiquant que l'adresse ARP (adresse MAC) de l'autre machine a changé, l'adresse ARP fournie étant celle de l'attaquant.





## Attaques par débordement de tampon

- Appelée aussi débordement de tampon (buffer overflow) est une technique qui consiste à exécuter de code arbitraire par un programme en lui envoyant plus de données qu'il n'est censé en recevoir.
- Attaque fortement liée à l'architecture du processeur sur lequel l'application vulnérable est exécutée.
- Les données saisies dans une application sont stockées en mémoire vive dans une zone appelée tampon.
- Un attaquant ayant de bonnes connaissances techniques peut s'assurer que l'adresse mémoire écrasée correspond à une adresse réelle (située dans le tampon lui-même). Ainsi, en écrivant des instructions dans le tampon, il lui est simple de l'exécuter.



## Attaques par faille matérielle

- Les failles matérielles sont rares mais elles peuvent s'avérer très dangereuse.
- Exemples de quelques failles :
  - Routeur
  - Serveur DNS
  - Bluetooth
  - WiFi
  - Processeurs : failles des techniques de virtualisation, ...
  - Lecteur d'empreinte digitale et reconnaissance faciale.



# Attaques par ingénierie sociale

- L'ingénierie sociale permet parfois de pallier à l'absence de faille et d'extirper des informations de l'utilisateur d'un ordinateur sans que ce dernier n'ait conscience d'ouvrir son PC à une personne non désirée (la récupération de post-it sur l'écran, la lecture de listing dans les poubelles d'une entreprise, l'usurpation d'identité au téléphone, ...)
- Autres techniques :
  - Réseaux sociaux,
  - Watering hole,
  - Attaque par VoIP,
  - Réinitialisation de mot de passe par Phishing,

# Questions?