

Cybersécurité - théorie

L'utilisation massive des systèmes informatiques entraîne l'apparition de spécialistes qui vérifient que les systèmes fonctionnent correctement. Les dysfonctionnements peuvent être dus à des défauts matériels, logiciels, dans le traitement des données ou dans leur transmission via les réseaux comme l'internet, etc. Ils peuvent également être dus à des agissements malveillants. En effet, la cybercriminalité s'est rapidement développée pour profiter des failles de sécurité et en tirer un bénéfice.

Pour n'importe quel service (messagerie, opérations bancaires, jeux, etc.), la sécurité informatique a notamment pour but de préserver :

- la **disponibilité** (contenu disponible en tout temps)
- l'**intégrité** (certitude de l'authenticité du contenu)
- la **confidentialité** (contenu pas accessible par d'autres personnes)

Il s'agit dans tous les cas d'essayer d'assurer le fonctionnement des systèmes informatiques de manière conforme à ce qu'ils sont censés faire. Par exemple, si j'envoie un message via un réseau social à un(e) ami(e), j'aimerais :

- que mon message arrive à son destinataire (disponibilité du service)
- qu'il ne soit pas modifié, soit par une erreur de transmission, soit par un acte malveillant (intégrité)
- que personne d'autre ne puisse voir mon message (confidentialité)

De nombreuses vulnérabilités existent, comme les bogues (défauts de programmation involontaires), des OS obsolètes contenant des failles de sécurité, etc.

Les pirates ou cybercriminels peuvent exploiter ces failles pour produire des cyberattaques.

Techniques d'attaque :

- **backdoor**: porte secrète qui permet d'accéder à des ressources comme un ordinateur ou un smartphone de manière dérobée
- **man-in-the-middle**: une personne malveillante (Eve) intercepte les échanges d'information entre une personne (Alice) et une autre (Bob). Elle peut tout entendre et peut faire croire à chacun qu'il (elle) parle avec son interlocuteur.
Remarque : Le nom Eve vient de Eavesdropping = écoute clandestine en anglais...
- **DoS** : Deny of Service, autrement dit le système n'est plus disponible car il a trop de trafic, trop de requêtes dus à un (ou de nombreux) robot(s) attaquant le service.
- **SPAM** (email) : De nombreuses attaques se déroulent à travers la messagerie, notamment email. Par exemple :
 - attaques DoS qui rendent un serveur de messagerie inutilisable car il reçoit trop de messages simultanément de la part de machines infectées
 - fake News, canular, hoax
 - **phishing** (hameçonnage) : nous fait croire qu'on a à faire à un tiers de confiance pour soutirer données personnelles (typiquement à notre banque!)

Classification des hackers (=bidouilleur en anglais) :

- **Black Hats** → Ils sont mus par le désir de nuire ou par l'appât du gain, c'est donc la branche criminelle.
- **White Hats** → Ce sont les Robin Hood du Cyberspace : ils aident à sécuriser les systèmes pour découvrir les vulnérabilités.

Classification des Malwares (**Malicious Software** = logiciel malveillant → pourriiciel)

- **virus**
 - infection de fichiers, de logiciels sur un ordinateur, souvent transmis par email ou par clef USB
- **vers**
 - se propagent sans besoin d'intervention humaine en utilisant des vulnérabilités des réseaux.
- **Spyware**
 - espionne notre activité (clavier, connexions, etc.)
- **Ransomware**
 - infecte un ordinateur (souvent un serveur) puis chiffre toutes les données
 - demande une rançon pour déchiffrer
- **Bot** (ou Botnets pour les réseaux → robots)
 - exécution automatique de petits programmes (scripts) qui peuvent permettre au hacker ou à la personne à qui le hacker vendra son "exploit" de contrôler l'ordinateur de quelqu'un d'autre,
 - par exemple pour lancer des attaques DoS ou des SPAMS depuis de nombreux ordinateurs en même temps sans prendre de risques
- **Trojans** (chevaux de Troie)
 - se font passer pour des fichiers légitimes
 - Une fois téléchargés ou installés, déclenchent des activités malveillantes...

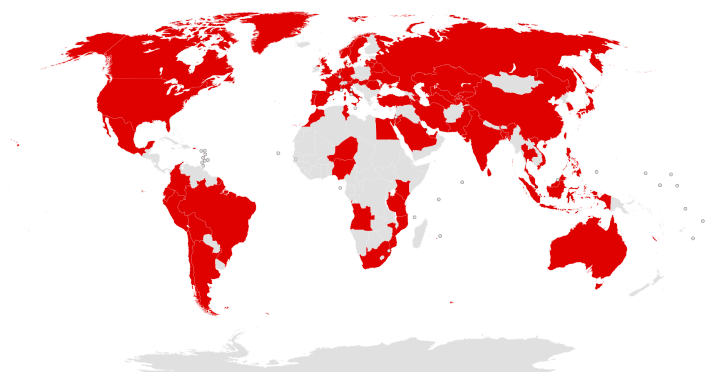
Défenses :

Pour se défendre contre les attaques (avant qu'elles ne se produisent), on peut appliquer une série de stratégies:

- **Sauvegardes** fréquentes des données
 - Permet de récupérer les données endommagées par une attaque.
- **Chiffrement** des données
 - Permet de rendre les données volées inutilisables sans une clef de déchiffrement.
- **Antivirus**, anti-malwares, etc.
 - Permet parfois de détecter les attaques quand elles se produisent et de les bloquer.
- **Mises à jour régulières**
 - Permet de limiter les vulnérabilités des logiciels, notamment de l'OS installé sur l'ordinateur.

Exemple d'attaque: WannaCry

[WannaCry](#) est un ransomware lancé en 2017. Il utilisait une vulnérabilité de certaines OS obsolètes de Windows (notamment XP). Cette vulnérabilité concernait un protocole réseau nommé SMB qui, dans sa version 1 était donc vulnérable. La [NSA](#) (agence de sécurité nationale aux USA) a développé des [outils](#) pour utiliser cette vulnérabilité à son avantage (espionnage). Une fuite due à des [hackers](#) a révélé ces outils qui sont donc devenus publics. Microsoft a rapidement développé des patches pour mettre à jour ses systèmes d'exploitation et ainsi empêcher cette vulnérabilité. Cependant, de nombreux utilisateurs (et notamment les entreprises) ne mettent pas à jour leurs serveur régulièrement, ce qui a permis aux black hackers de commettre cette attaque d'une ampleur énorme dans tout le monde (comme on peut le voir sur l'image ci-dessous).



Countries initially affected in WannaCry ransomware attack ([Wikipédia](#))

Ce [ver](#) est donc injecté grâce à l'[exploit](#) (outil développé par la NSA) dans un ordinateur et se réplique dans tous les ordinateurs accessibles via le réseau interne des entreprises (grâce au protocole SMBv1). Ensuite, il se déclenche et chiffre toutes les données présentes sur l'ordinateur hôte. Un écran affiche alors les instructions pour que la victime paie une rançon (à l'époque des faits, entre 300 et 600 €) afin de recevoir une clef permettant de déchiffrer les données (donc de les récupérer!).



Instructions destinées aux victimes de WannaCry ([Wikipédia](#))

Les auteurs de cette attaque ne sont pas déterminés de manière certaine mais on estime qu'il s'agit probablement d'un groupe de hackers nord-coréens nommé "Lazarus"

Cybersécurité - exercices

1. A quoi sert la Cybersécurité?
2. Les trois aspects de la cybersécurité...
 - a. Quels sont les trois points que la cybersécurité est censée assurer?
 - b. Donner un exemple pour chaque point où il n'est pas assuré.
3. Quelles sont les vulnérabilités (faiblesses) qui peuvent faciliter la tâche aux pirates informatiques?
4. Si un pirate a réussi à prendre le contrôle de mon ordinateur, quelle est la technique d'attaque dont il dispose?
5. Si quelqu'un se fait passer pour quelqu'un d'autre et transmet les messages que tu lui envoies vers la personne à qui tu penses parler mais en transformant certains détails à son avantage, quelle technique d'attaque utilise-t-il?
6. Lorsqu'un pirate malveillant contrôle des dizaines d'ordinateurs pour lancer des requêtes sur un serveur qu'il souhaite rendre inutilisable, car il sera débordé par les demandes, quelles est la technique (et éventuellement le type de malware employé) utilisés pour l'attaque ?
7. Si je reçois un message d'un pirate qui se fait passer pour Facebook et qui me prévient que quelqu'un a tenté de pirater mon compte et que je dois cliquer sur le lien figurant dans le message pour me connecter et changer de mot de passe, quelle technique d'attaque est employée?
8. Qu'est-ce qui différencie les hackers nommés "white hat" des autres nommés "black hat" ?
9. Quelle est la différence entre un virus et un ver informatique ?
10. Cite trois méthodes pour se défendre contre les menaces de cyberattaques avant qu'elles ne se produisent.
11. Explique pourquoi le fait de mettre à jour régulièrement son système d'exploitation est essentiel pour se prémunir contre des attaques.
12. Quelle est la technique qui permet d'assurer la confidentialité des échanges dans les logiciels de chat comme Signal ou Whatsapp ?
13. Pour éviter de perdre toutes tes données si un pirate les détruit, qu'est-ce que tu peux faire?