CYBERSECURITE

I) POSITION DU PROBLEME

LES CYBERMENACES

Cybercriminalité : comprend des acteurs isolés ou des groupes qui ciblent des systèmes pour des gains financiers ou pour causer des perturbations

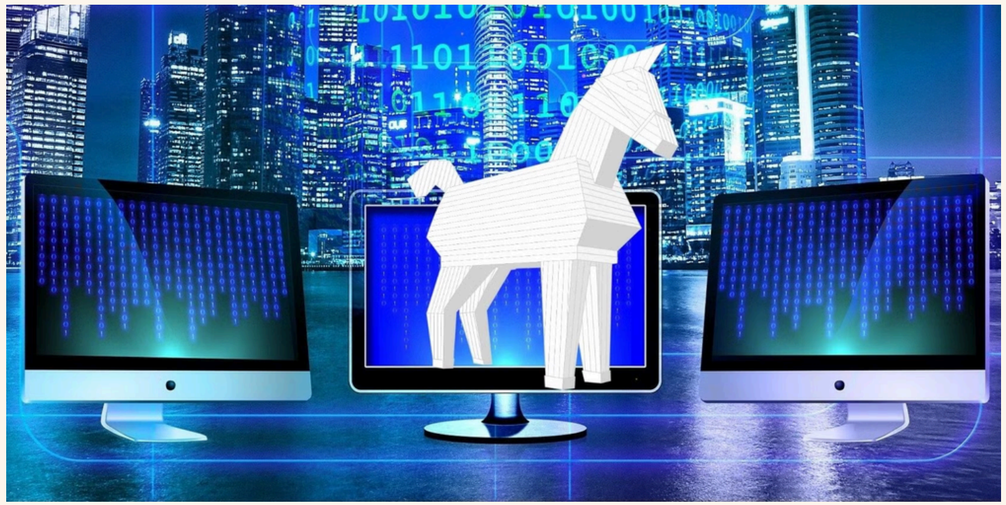
Cyberattaques : impliquent souvent la collecte d'informations pour des raisons politiques

Cyberterrorisme : vise à saper les systèmes électroniques pour entraîner la panique ou la peur

TYPOLOGIE DES MÊTHODES D'ATTAQUE

- **Malware :** logiciels malveillants.
- **Injection SQL :** le pirate insère un code malveillant dans une base de données via une déclaration SQL ; il gagne ainsi l'accès à des données sensibles.
- **Phishing :** l'envoi d'e-mails qui semblent provenir d'une entreprise légitime, servant à tromper les utilisateurs pour récupérer leurs coordonnées bancaires ou leurs informations personnelles.
- **Homme du milieu :** consiste à intercepter la communication entre deux individus pour leur voler des données.
- **Déni de service :** empêche un système informatique de répondre à des requêtes légitimes en surchargeant les réseaux et les serveurs avec du trafic. Le système devient ainsi inutilisable, empêchant une entreprise de fonctionner correctement.
- **L'inside job :** la fuite de données provient d'un des collaborateurs de l'entreprise.

NOUVELLES CYBERMENACES



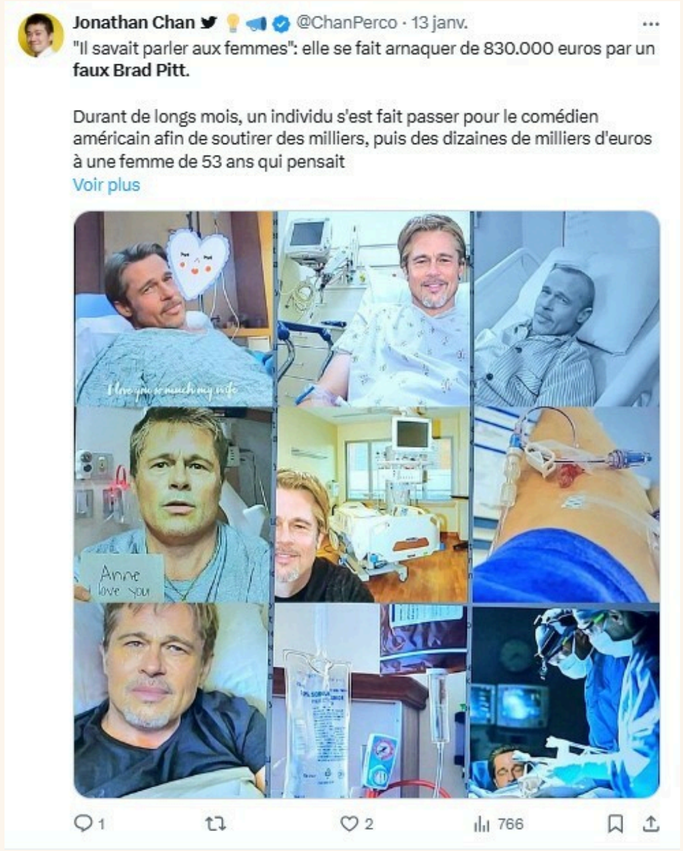
1 MALWARE DRIDEX

- **Quand** : décembre 2019
- **Par qui** : ministère de la Justice américain
- **Contre qui** : chef d’un groupe cybercriminel organisé
- **Quoi** : attaque mondiale utilisant le cheval de Troie bancaire par un logiciel appelé Dridex
- **Origine** : apparu en 2014
- **Mode d’infection** : e-mails de phishing ou malwares existants
- **Objectif** : vol de mots de passe, coordonnées bancaires et données personnelles
- **Conséquences** : pertes financières massives (centaines de millions de dollars)
- **Réponse / Prévention (NCSC) :**

-Mettre à jour / patcher les appareils
-Antivirus activé et à jour
-Sauvegarder régulièrement les fichiers

NOUVELLES CYBERMENACES

2 ARNAQUES SENTIMENTALES



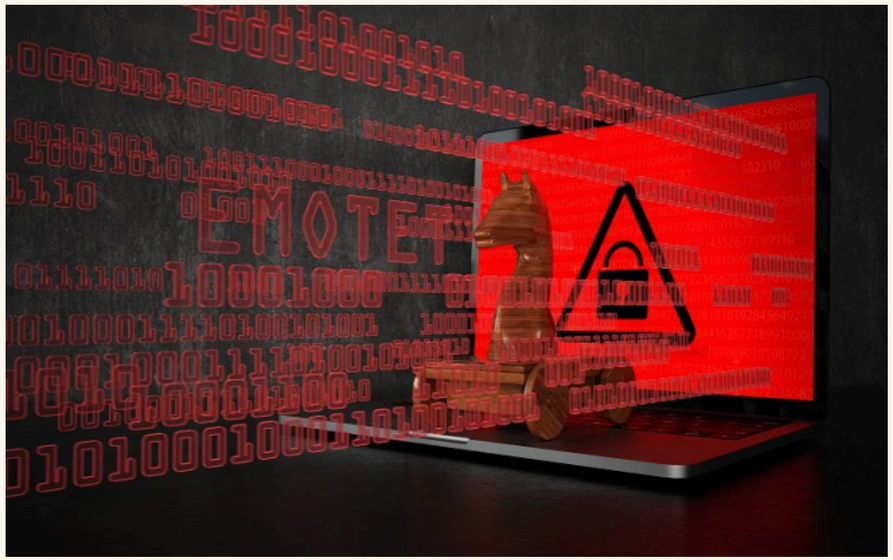
ex : histoire de Brad pitt & Anne

- En **février 2020**, le FBI alerte sur la **hausse des arnaques sentimentales en ligne**.
- Les cybercriminels piègent leurs victimes sur les sites de rencontre et applications.
- En **2019**, au **Nouveau-Mexique**, **114 victimes ont perdu 1,6 million $.**

NOUVELLES CYBERMENACES

3

MALWARE EMOTET



- **Fin 2019**, l'Australian Cyber Security Center alerte sur une **cybermenace mondiale** : le **malware Emotet**.
- Emotet est un **cheval de Troie** sophistiqué capable de **voler des données** et **installer d'autres malwares.**
- Il se **propage** grâce à des **mots de passe faibles.**
- Rappel : il est essentiel de créer des mots de passe sécurisés pour éviter les cyberattaques.

PROGRAMMES MALVEILLANTS

Malwares :

- Des logiciels malveillants créés par des cybercriminels ou hackers.
- Une des cybermenaces les plus courantes
- Leur but : perturber, endommager ou pirater un ordinateur.
- Ils se propagent via des pièces jointes d’emails ou des téléchargements piégés.
- Utilisés pour voler de l’argent ou mener des cyberattaques politiques.

PROGRAMMES MALVEILLANTS

Il existe pluseurs type de malwares :

- **Virus** : un programme pouvant se **dupliquer** qui s'attache à un **fichier sain** et se propage dans tout le système en **infectant les fichiers** à l'aide d'un **code malveillant.**
- **Cheval de Troie** : type de programmes malveillants se faisant passer pour des **logiciels authentiques**. Les cybercriminels piègent les utilisateurs en téléchargeant des chevaux de Troie dans leur ordinateur pour **endommager** ou **collecter des données.**
- **Spyware** : un programme **espion** qui enregistre secrètement les **actions d'un utilisateur** au profit des cybercriminels.
- **Ransomware** : un malware qui **verrouille les fichiers** et les **données** de l'utilisateur sous menace de les effacer si une **rançon** n'est pas payée.
- **Adware** : un logiciel **publicitaire** qui peut être utilisé pour propager un malware
- **Botnets** : des réseaux **d'ordinateurs infectés par des malwares** que les cybercriminels peuvent utiliser pour **effectuer des tâches en ligne sans l'autorisation** de l'utilisateur.

FUITE DE DONNEES

= exposition non désirée, qu'elle soit publique ou privée, touchant une entreprise ou un particulier

Les causes : Cyberattaques (48%) / Erreur humaine (27%) /erreur système (25%)

- Au **1er semestre 2019**, la France a enregistré **5,7 violations de données par jour**, contre **4,5 au 2e semestre 2018.**

54 % des fuites sont malveillantes, dont :

- 69,8 % dues à du piratage en ligne
- 15 % à du vol physique
- 26 % des fuites sont accidentelles, le reste ayant des causes inconnues ou diverses.

FUITE DE DONNEES

Secteurs les plus touchés :

- 🧪 Sciences et techniques : 297 notifications
- 🛒 Commerce : 279 notifications
- 💰 Finance : 275 notifications
- 🏛️ Administration publique : 229 notifications
- 🍽️ Hébergement & restauration : 202 notifications

Risques pour un attaquant :

1. Financiariser une arnaque : vente des données collectées
2. Compléter une attaque : acquérir des informations sur une cible pour préparer une attaque plus importante

En moyenne, une entreprise met **197 jours à détecter une fuite de données**, puis **69 jours pour la résoudre.**

FUITE DE DONNEES

🛡️ Facteurs qui réduisent l’impact :

- Comité de direction impliqué
- Sensibilisation des employés
- Classification des données sensibles
- Logiciel DLP (Data Loss Protection)
- Équipe de réponse aux incidents (interne/externe)

Conduite en cas d’incident :

- **Prévenir** : préparer équipes techniques et non techniques
- **Détecter** : équipe de cyber intelligence pour identifier rapidement
- **Assurer** : couverture adaptée (frais, notifications, pertes)
- **Réagir** : notifier la CNIL sous 72h

EXERCICE

1) Virus
2) Cheval de Troie
3) Spyware
4) Ransomware
5) Adware
6) Botnets

a) Logiciel qui affiche de la publicité, parfois utilisé pour diffuser d’autres malwares.

b) Logiciel espion qui surveille les actions d’un utilisateur à son insu.

c) Programme qui s’attache à un fichier sain et se propage en infectant d’autres fichiers.

d) Logiciel malveillant qui bloque l’accès aux fichiers et exige une rançon.

e) Programme se faisant passer pour un logiciel légitime afin de tromper l’utilisateur.

f) Réseaux d’ordinateurs infectés utilisés à distance par des cybercriminels.

CORRECTION

1) Virus
2) Cheval de Troie
3) Spyware
4) Ransomware
5) Adware
6) Botnets

a) Logiciel qui affiche de la publicité, parfois utilisé pour diffuser d'autres malwares.

b) Logiciel espion qui surveille les actions d'un utilisateur à son insu.

c) Programme qui s'attache à un fichier sain et se propage en infectant d'autres fichiers.

d) Logiciel malveillant qui bloque l'accès aux fichiers et exige une rançon.

e) Programme se faisant passer pour un logiciel légitime afin de tromper l'utilisateur.

f) Réseaux d'ordinateurs infectés utilisés à distance par des cybercriminels.

II) SECURITE INFORMATIQUE

DEF DE LA CYBERSECURITE

La **cybersécurite** assure une **gestion de la donnée dans des conditions optimales et sécurisées.** Elle consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes.

On l’appelle également **sécurité informatique** ou **sécurité des systèmes d’information**.

OBJECTIF DE LA CYBERSECURITE

AUTHENTIFICATION

Assure que seules les personnes autorisées aient accès aux ressources

DISPONIBILITE

Maintient le bon fonctionnement du système d’information

INTEGRITE

Garantit qu’une transaction ne peut être niée

NON-REPUDIATION

Garantit que les données sont bien celles que l’on croit être

CONFIDENTIALITE

Veiller à ce que seules les personnes autorisées puissent accéder aux ressources ou informations échangées

SECURITE PHYSIQUE

- **Controle l’accès** (aux locaux, ordinateurs et equipements)
- utilier des **barrières, alarmes, serrures** et d’autres mécanismes de controle d’accès.
- Ces mesures sont essentielles pour **protéger les matériels** et leur contenu contre : **le vol, l’espionnage, la destruction accidentelle ou intentionnelle**

SECURITE LOGIQUE

- Repose sur un **système de contrôle d'accès logique**

→ basé sur les services **d'identification**, **d'authentification** et **d'autorisation**.

- Comprend des mesures garantissant la **confidentialité** :

→ utilisation de la **cryptographie**,
→ gestion efficace des **mots de passe**,
→ **procédures d'authentification** solides,
→ solutions **antivirus** fiables,
→ systèmes de **sauvegarde** des informations sensibles.

TYPOLOGIE DES SECURITÉS

- **Sécurité des réseaux :**

Protège le réseau contre les intrusions et malwares.

- **Sécurité des applications :**

Protège les logiciels et appareils dès la conception.

- **Sécurité des informations :**

Assure confidentialité et intégrité des données (stockées ou en transit).

- **Sécurité opérationnelle :**

Gère les droits d’accès, le stockage et la localisation des données.

- **Reprise après sinistre & continuité :**

Permet de rétablir les opérations et maintenir l’activité après un incident.

- **Formation des utilisateurs :**

Sensibilise aux bonnes pratiques pour éviter les erreurs humaines (pièces jointes, clés USB, etc.).

CLASSES DES CYBERSECURITÉS

- **Classe 1 → Risque faible**

Application autonome des mesures de sécurité

Basée sur les règles d’hygiène informatique de l’ANSSI

- **Classe 2 → Risque significatif**

Pas de contrôle étatique direct

L’entité doit prouver la mise en place de mesures adéquates

- **Classe 3 → Risque critique**

Obligations renforcées

Conformité vérifiée par une autorité ou un organisme accrédité

THANK YOU