Sécurité : définitions

2 Définitions

1. Sécurité informatique

- **Comprendre** la protection
- **Explorer** les **solutions de protection** des données d'entreprise

2. Cybersécurité

- Se concentrer sur les **menaces** rencontrées **via Internet**

6 types de sécurités

1. Sécurité du réseau

- Protège une **infrastructure** numérique : réseau interne ou externe

2. Sécurité Internet

- Protège les **navigateurs** et les **informations** contenues dans les applications utilisant Internet

3. Sécurité des terminaux

- Se concentre sur la protection des **points de connexion** de nos smartphones, ordinateurs portables, objets connectés…

6 types de sécurités

4. Sécurité Cloud

- Protège les utilisateurs connectés via des applications basées sur le cloud

5. Sécurité des applications

- Aide les développeurs à sécuriser leurs applications : « bonnes pratiques »
- Aide à analyser les codes pour trouver les violations

6. Sécurité opérationnelle

- Analyse les pratiques et comportements humains qui pourraient être exploités par des hackers

3 types de menaces

1. Cybercriminalité

- Acte criminel à l'aide d'ordinateurs en échange d'une **récompense financière**
- Exemple : usurpation d'identité, extorsion

2. Cyberattaque

- Attaque à plus grande échelle s'attaquant à **tout un système d'information**
- Exemple : cyberattaque sur Facebook (2018), les données de millions d'utilisateurs ont été compromises

3. Cyberterrorisme

- Identique à la cybercriminalité et aux cyberattaques mais **la cible est un pays et ses infrastructures**
- Exemple : prise de contrôle sur de sites gouvernementaux, de réseaux de télévision …

Malware

- Un malware est un logiciel **malveillant** qui endommage un **service** ou un **réseau**

Quelques types de malwares :

- Virus
- Ransomware
- Spyware
- Keylogger
- Trojan (cheval de Troie)
- Adware
- File Less malware

Virus

- Le logiciel **modifie le fonctionnement** d'un ordinateur ou d'un réseau
- Il peut se **propager** d'un ordinateur à un autre
- Il **nécessite un utilisateur humain pour l'activer** : ouverture d'un email infecté, clic sur un lien, ouverture d'un document …
- Exemple : « MyDoom » (2004) a pris le contrôle d'ordinateurs pour envoyer du spam et lancer des attaques contre des entreprises comme Google ou Microsoft
- 7,4 millions d'e-mails contenaient le virus « MyDoom »
- 700 000 PC ont été infectés

Virus

- Microsoft a dépensé 5 millions de dollars pour aider le FBI à retrouver le hacker
- 250 000 $ de récompense ont été offerts à toute personne donnant des informations
- En juillet 2004, Google a fermé ses accès pendant une journée entière à la suite d'une attaque menée par une variante de « MyDoom »
- « MyDoom » aura coûté environ 38 milliards de dollars à l'État américain et à toutes les entreprises attaquées entre 2004 et 2007
- L'auteur du virus n'a jamais été retrouvé

Ransomware

- Le logiciel **prend en otage** des informations vitales pour obtenir une rançon
- Il **verrouille** des ordinateurs ou un réseau puis le pirate demande de l'argent ou quelque chose de valeur en échange
- En 2021, la ville de Baltimore (Maryland - USA) a été touchée par le ransomware « Robin Hood » qui a interrompu toutes les activités de la ville, y compris la collecte des impôts et les transferts de propriété pendant des semaines
- Cette attaque a coûté plus de 18 millions de dollars
- Le même type de malware a été utilisé contre la ville d'Atlanta en 2018, entraînant une perte de 17 millions de dollars

Ransomware

- 4,5 millions de dollars ont été versés par « Carlson Wagon Lit Travel », spécialiste du voyage d'affaires
- L'entreprise a été victime du ransomware « Ragnar Locker »
- 2 téraoctets de données ont été volés
- Toute l'infrastructure informatique était verrouillée
- Le groupe a payé la rançon pour redémarrer plus de 30 000 PC paralysés

Spyware

- Ce logiciel pénètre un système informatique pour **recueillir des informations personnelles**, cartes de crédit, identifiants de connexion à des comptes …
- Une fois trouvée sur votre ordinateur, **l'information est transmise au pirate**
- Exemple : « Darkhotel » a ciblé des chefs d'entreprise en utilisant le réseau Wi-Fi des hôtels dans lesquels ils séjournaient lors de déplacements professionnels
- Le pirate veut accéder à des ordinateurs et smartphones appartenant à des personnes influentes et ciblées
- Une fois l'accès obtenu, les attaquants installent des enregistreurs de frappe pour capturer les mots de passe de leurs cibles et d'autres informations sensibles

Keylogger

(enregistreur de frappes)

- Ce logiciel **surveille l'activité** des utilisateurs
- Les entreprises peuvent surveiller l'activité des employés
- Les familles peuvent surveiller les comportements des enfants sur leurs ordinateurs
- Un keylogger peut être utilisé pour voler les données de mot de passe, des informations de compte …
- Exemple : « Olympic Vision » a été utilisé pour cibler des hommes d'affaires et notamment leur courrier électronique professionnel
- Il est très accessible car disponible sur le marché noir pour quelques dollars

Trojan

(cheval de Troie)

- Le logiciel « **se déguise** » en code ou logiciel « **désirable** »
- Une fois téléchargé par des utilisateurs peu méfiants, le cheval de Troie prend le contrôle de votre ordinateur
- Il se cache dans les jeux, dans les applications ou même les correctifs logiciels
- Il se cache dans les pièces jointes incluses dans les e-mails
- Exemple : « Emotet » est un cheval de Troie bancaire sophistiqué créé en 2014
- Il intégrait des modules de diffusion qui l'aidaient à se propager au sein du réseau des banques
- Il était si répandu qu'il a fait l'objet d'une alerte du département américain de la sécurité intérieure

Adware

- Ce logiciel affiche par exemple continuellement des pop-ups
- Il **ralentit l'ordinateur** pour **masquer** une autre cybermenace en cours d'exécution
- Exemple : « Fireball » a infecté 250 millions d'ordinateurs et d'appareils en 2017
- Il reconfigurait les navigateurs Web pour modifier les moteurs de recherche par défaut
- D'autres changent votre page d'accueil
- Ces logiciels permettent également de suivre l'activité de l'utilisateur

DoS

Denial Of Service

- Un attaquant rend un réseau inaccessible aux utilisateurs en générant un **trafic massif et inhabituel**
- Cela **empêche les utilisateurs autorisés d'accéder** correctement au réseau
- Il n'y a **pas d'intrusion**
- L'attaquant utilise des **botnets**
- Exemple : après la fermeture du site Megaupload par le FBI en 2012, de nombreux sites Web importants (Paypal, Ebay, FBI, ...) ont fait l'objet d'une attaque DoS en représailles

Botnet

- C’est un réseau d'**ordinateurs infectés** par un logiciel malveillant
- Ils sont utilisés comme **une seule entité** pour lancer des attaques plus puissantes
- Les botnets sont souvent utilisés dans les attaques **DoS** (Denial of Service)
- Exemple : « Echobot » attaque un large éventail d'appareils « IoT » et exploite plus de 50 vulnérabilités différentes sur ces objets connectés

File less Malware

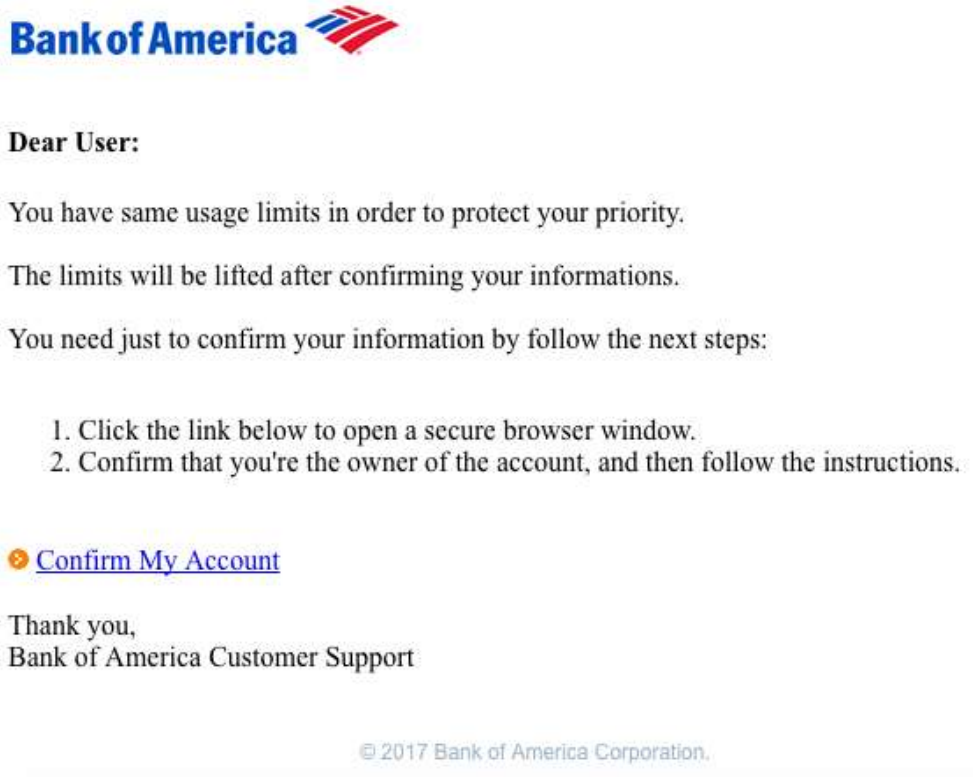
- Le logiciel apporte des modifications aux **fichiers natifs** du système d'exploitation
- Exemples : PowerShell ou WMI sous Windows
- Le système d'exploitation reconnaît les fichiers modifiés comme **légitimes**
- Cette attaque n'est **pas détectée par un logiciel antivirus**
- **Elle ne laisse aucune trace**

File less Malware

- Exemple : "Astaroth" spamme les utilisateurs avec des liens vers un fichier de raccourci de type .LNK.
- Lorsque les utilisateurs téléchargent le fichier, un service Windows est lancé **légitimement**
- Ce service, contrôlé par le pirate, dépose du code supplémentaire exécuté uniquement en mémoire, **ne laissant aucune preuve sur disque**
- Ensuite, l'attaquant dépose et exécute un cheval de Troie (Trojan) qui **vole** les informations d'identification et les **télécharge** sur un serveur distant

Phishing

- Un pirate se fait passer pour quelqu'un d'autre et essaie d'amener les gens à livrer des informations sensibles
- Cela représente un tiers de toutes les attaques
- Exemple: mails



Bank of America

Dear User:

You have same usage limits in order to protect your priority.

The limits will be lifted after confirming your informations.

You need just to confirm your information by follow the next steps:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

Confirm My Account

Thank you,
Bank of America Customer Support