

Les différentes techniques de cyberattaques :



Définition des termes :

Cyberattaques : accès non autorisé ; systèmes informatiques

techniques d'attaques : méthodes; spécifiques; cyberattaques

Problématiques :

Quelles sont les différentes techniques d'attaques ?

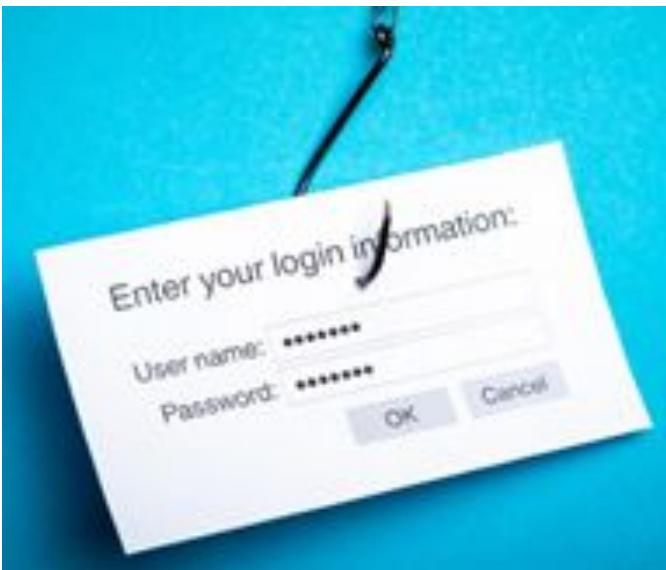
Le plan :

- 1) Les techniques les plus courantes.
- 2) les techniques les plus sophistiquées.

1) Les techniques les plus courantes :

- a) Le phishing
- b) ransomware
- c) DDOS

a) Le phishing :

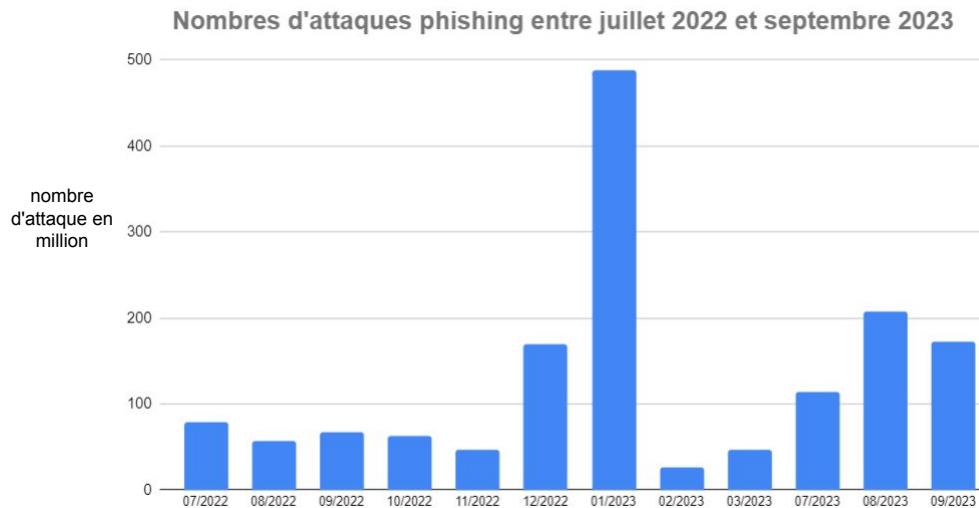


Le phishing : vols d'informations; usurpation d'identité; vente de donné; piratage.

<https://www.titanhq.fr/>

Le phishing :

- Des chiffres importants
- 650 millions d'attaques en 2 mois



<https://www.vadesecure.com>

Le phishing :



Votre espace Client

Chère Cliente, Cher Client,

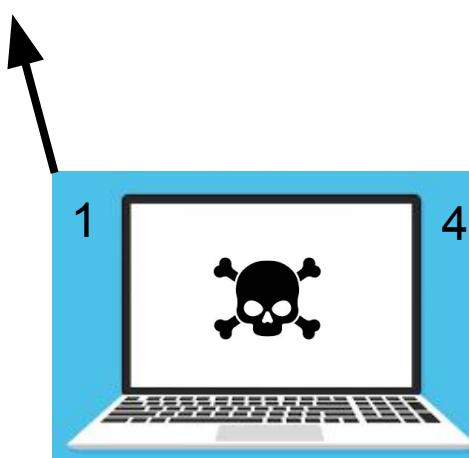
Suite au refus de votre banque lors d'un prélèvement bancaire, votre paiement a été malheureusement refusé.

Pour résoudre ce problème, veuillez vous connecter à votre compte afin de pouvoir effectuer ce paiement, vous disposez de 48h pour ce faire sinon votre contrat sera automatiquement résilié.

[Accéder à mon compte](#)

Cordialement,

2



- 1) envoi du mail
- 2) exemple d'un mail phishing
- 3) transmission des informations
- 4) récupération des informations.

Le phishing :



1. Ne communiquez jamais d'informations sensibles par messagerie ou téléphone :



2. Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien



3. Vérifiez l'adresse du site qui s'affiche dans votre navigateur.



4. En cas de doute, contactez si possible directement l'organisme concerné



5. Utilisez des mots de passe défendus et complexes pour chaque site et application



6. Si le site le permet, vérifiez les date et heure de dernière connexion à votre compte



7. Si le site vous le permet, activez la double authentification pour sécuriser vos accès.

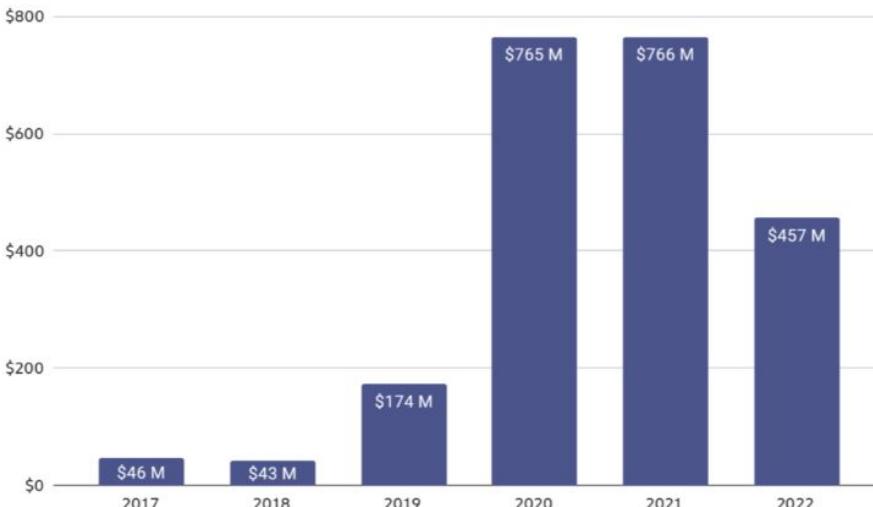
<https://www.cybermalveillance.gouv.fr>

b) Les ransomware



Ransomware : logiciel malveillant; cryptage de données; demande de rançon.

Total value received by ransomware attackers, 2017 - 2022



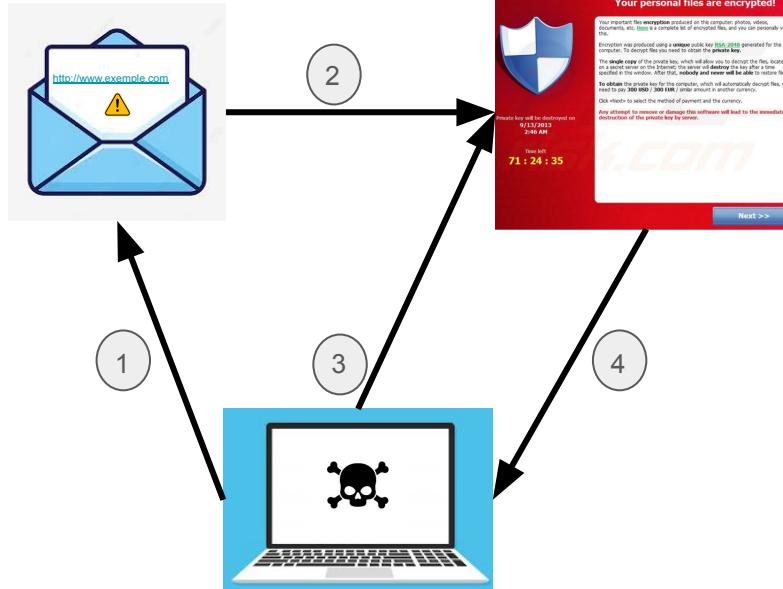
- Augmentation des attaques ces dernières années

- Augmentation des vols

© Chainalysis

<https://www.channelnews.fr/>

Les ransomware :



- 1) Envoi d'un mail frauduleux
- 2) Installation d'un logiciel malveillant
- 3) Envoi d'une demande de rançon
- 4) Transaction

Les ransomwares :

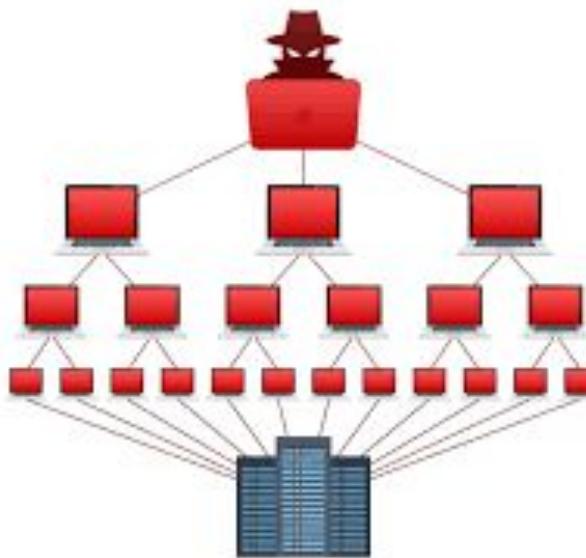
Se défendre:

1) attentif aux mails inconnus

2) extraire ces données

3) mise à jour logiciel.

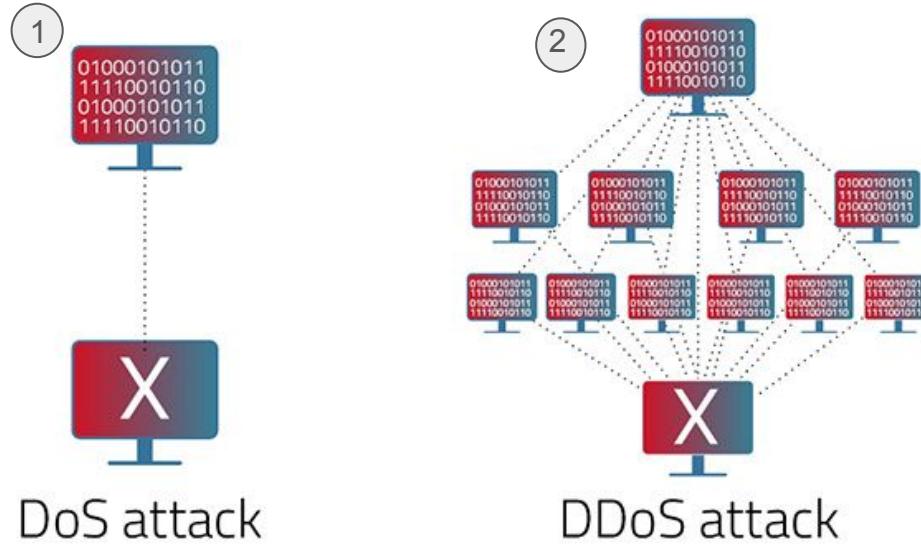
c) DOS :



- DOS : déni de service, stop un serveur

<https://www.istockphoto.com/>

c) DDOS:

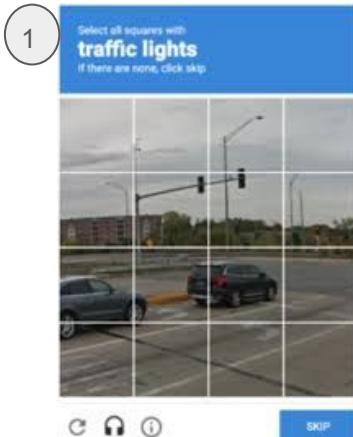


Dos: Déni de service; 1 points d'attaque

DDos: Déni de service distribué; plusieurs points d'attaque

<https://fr.radware.com>

c) DDOS :



1) Recaptch: Protection de sites



2) VPN : (Réseau privé virtuel) Protection personnel

- 1) <https://www.evina.com>
- 2) <https://www.istockphoto.com>

2) Les techniques d'attaques les plus sophistiquées :

a) Le pretexting

b) Man in the middle

a) Le pretexting

1- Attaquant

2- Cible

3- Masque



www.sapphire.net

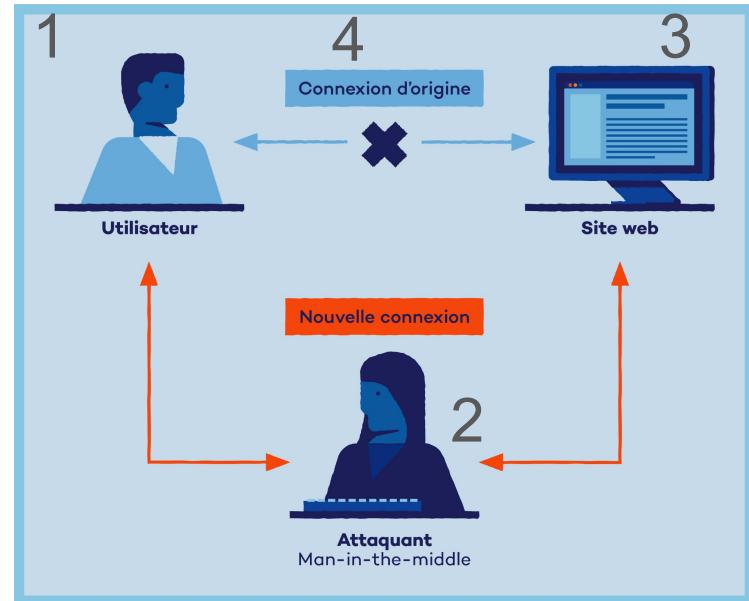
b) Man in the middle :

1- Utilisateur

2- Attaquant

3- Serveur web

4- Connexion d'origine



<https://fr.images.search.yahoo.com>

Conclusion :

- Attaques courantes: trop nombreuse; simple à parer
- Attaques sophistiqués: difficile à détecter; très efficaces; difficiles à stopper.