

Etude des Arnaques

Etude de cas : Le Ransomware et Le DDoS



Par :

CEVIK Meryem

Strasbourg, le 30 septembre 2022

Lycée René Cassin Strasbourg

BTS SIO

Les Arnaques

Les différents types d'arnaques

- **Arnaques à la vente en ligne**
- **Arnaques aux prix cassé** : les fraudeurs se font passer pour des vendeurs en ligne en proposant un article à petit prix
- **Arnaque à l'héritage ou la loterie**
- **Arnaque à l'emploi** : Fausse proposition d'emplois
- **La face Swapping/Morphing** : lorsqu'une personne se fait passer par quelqu'un d'autre en changeant son visage
- **La phishing/ Hameçonnage** : Technique utilisée par des fraudeurs pour obtenir des renseignements personnels (mot de passe, informations bancaires...) plus souvent pour but de le vendre
- **Le chantage affectif** : chantages émotionnels pour tirer de l'argent de la victime
- **Rançongiciel/Ransomware** : un type de malware qui empêche les utilisateurs d'accéder à leur système ou à leurs fichiers personnels et exige le paiement d'une rançon en échange du rétablissement de l'accès
- **Le spyware** : programmes qui enregistrent les frappes clavier, la webcam, le micro qui permet de récupérer des informations personnels (mot de passe, informations bancaires...)
- **Le DDoS** : arme de cybersécurité visant à perturber le fonctionnement des services et à extorquer de l'argent aux organisations ciblées



Etude des Ransomwares

Le **ransomware** est un logiciel malveillant qui empêche la victime d'accéder à ses données. Pour ce faire, il y a plusieurs manières de procéder, par exemple en chiffrant les données ou en bloquant l'accès de l'ordinateur.

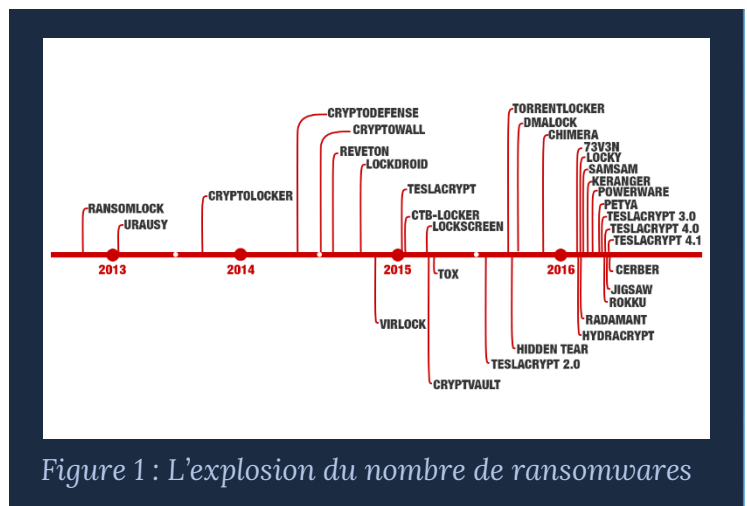
Ces manœuvres ont pour but d'obtenir le paiement d'une rançon. Une fois payée, la victime pourra accéder à ses données. Cependant payer la rançon ne garantit pas le retour des données. Ce type de logiciel est en constante évolution, il se professionnalise et infecte toujours plus de personnes

Nous allons commencer par nous **informer** sur cette menace. Nous poursuivons ensuite sur le **fonctionnement** du ransomwares. Nous continuons sur **les objectifs et la mise en œuvre** des ransomwares. Ensuite, nous allons expliquer **les faiblesses utilisées**. Pour conclure, nous proposerons des **outils et techniques pour se défendre et réagir au ransomware**.

L'évolution des ransomwares

Les ransomwares ont pris une autre dimension quand ils sont devenus professionnels, c'est-à-dire que les hackers proposent des marches à suivre pour guider les victimes lors du paiement.

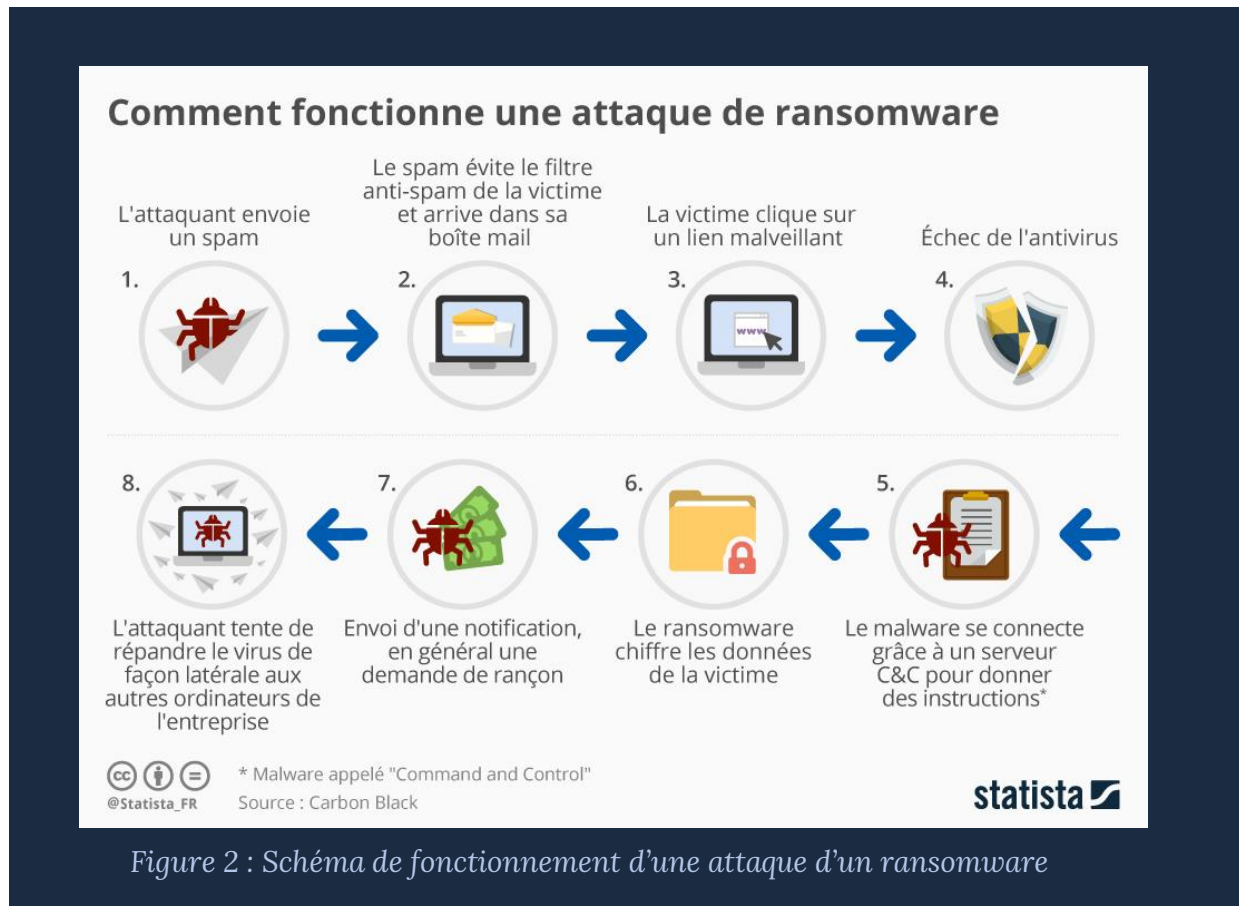
Ils mettent en place une clé de décryptage des données confidentielles de l'entreprise, ce qui pousse les entreprises à payer souvent la rançon. L'attractivité aux niveaux financiers a permis une explosion comme l'indique le graphique ([figure 1](#)).



Le fonctionnement des ransomwares

Le principe de base d'un ransomware est de verrouiller le système de la victime jusqu'à que celui-ci paie une rançon qui lui permettra de reprendre le contrôle de son ordinateur ou de ses données ([figure 2](#)).

Etude des Ransomwares



Les objectifs des différents types d'attaque

Le principe de base d'un ransomware est de verrouiller le système de la victime jusqu'à ce que celui-ci paie une rançon qui lui permettra de reprendre le contrôle de son ordinateur ou de ses données (figure 2).

- Attaques diffusées : Elles sont sans cible précise ou visent le grand public. Le marché noir du ransomware fonctionne comme une offre de service. Les données confidentielles qui ont été hackées par le rançongiciel, vont être partagées puis vendues sur des sites de commerces illégaux comme le dark web.
- Attaques opportunistes : D'un niveau technique plus avancé, elles vont viser les organismes les moins sécurisés dans un objectif de gain immédiat (vol de données personnelles, vols de données carte de crédit...).

Etude de cas n°1

Etude des Ransomwares

- Attaques ciblées : La spécificité des attaques ciblées est de viser des informations ou les systèmes sensibles dans une organisation donnée. Ses auteurs sont mandatés pour viser une cible en particulier avec un objectif clair.
Il s'agit en général de voler des données confidentielles sensibles. Ils sont organisés en équipes structurées avec des experts chargés d'accéder au Système informatique et d'en garder le contrôle, des explorateurs pour rechercher les informations visées et de la « main d'œuvre » pour exfiltrer des données.

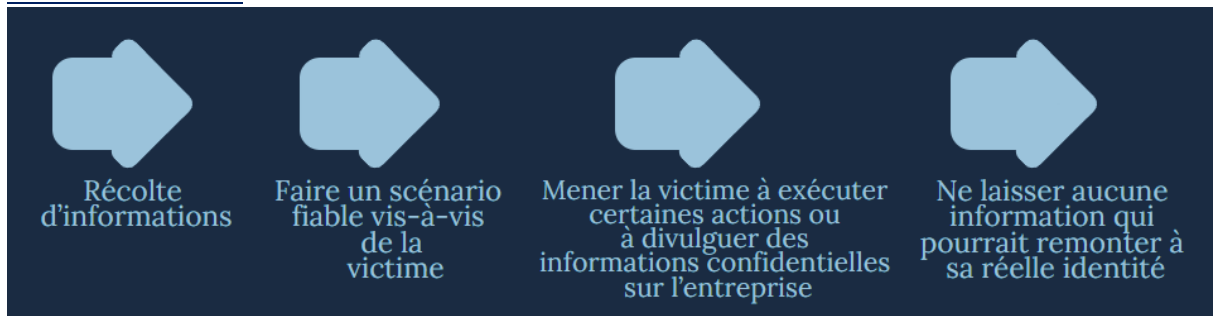
Les faiblesses utilisées et la mise en œuvre

On vient de voir l'impact que pouvaient avoir les ransomwares sur les entreprises, les particuliers ou les institutions. Mais comment les ransomwares arrivent sur vos ordinateurs. Il y a beaucoup de façons d'être infecté par un ransomware. Les principaux sont les suivants :

Faiblesses humaines :

- Convaincre une personne de nous révéler une information confidentielle ou à amener la victime à exécuter des actions (appuyer sur le lien de téléchargement du ransomware).

Mise en œuvre :



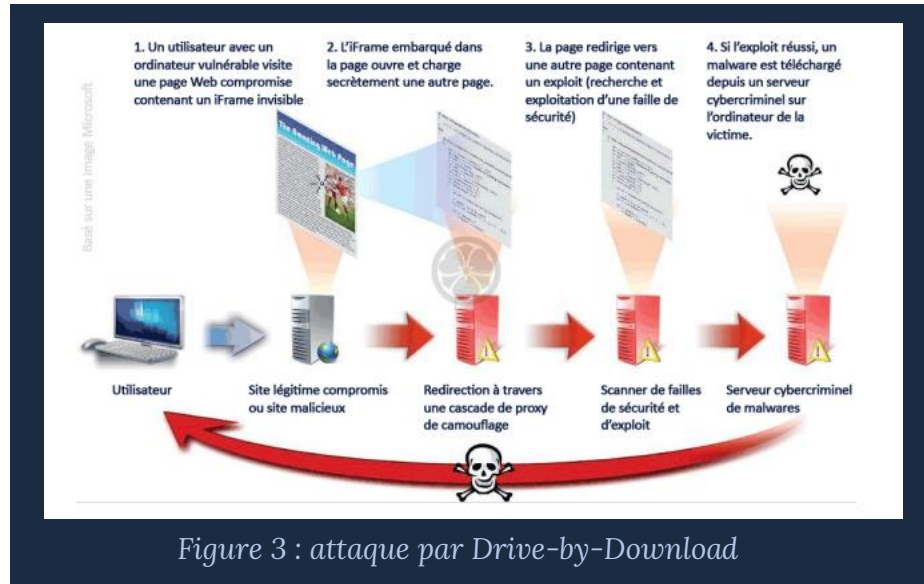
Faible de sécurité :

- C'est causé par les **vulnérabilités du navigateur ou mauvais paramétrages de sécurité**. Il s'agit d'un téléchargement et installation automatique sur un ordinateur. Le ransomware est téléchargé sur l'ordinateur sans demander l'avis de l'utilisateur. Il n'a même pas besoin de cliquer sur un lien.
En effet, les publicités ou pop-up de certains sites web peuvent détecter des failles présentes sur l'ordinateur et lancer automatiquement l'installation du ransomware.

Etude de cas n°1

Etude des Ransomwares

Mise en œuvre :



Les contre-mesures

Comment se protéger ?


- Sensibilisation
- Sauvegarde
- Solution anti-ransomware
- Mettre à jour



Etude des Ransomwares

En cas d'infection, que faire ?

VICTIME



COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

Conclusion

Les attaques de ransomwares ont commencé à évoluer dans tous les compartiments, le code des ransomware est devenu plus élaboré et les manières les diffuser sont devenu plus méthodique. Tout cela dans le but de gagner de l'argent.

On a analysé le fonctionnement et par la suite on a analysé les objectifs diverses et variés des ransomwares.

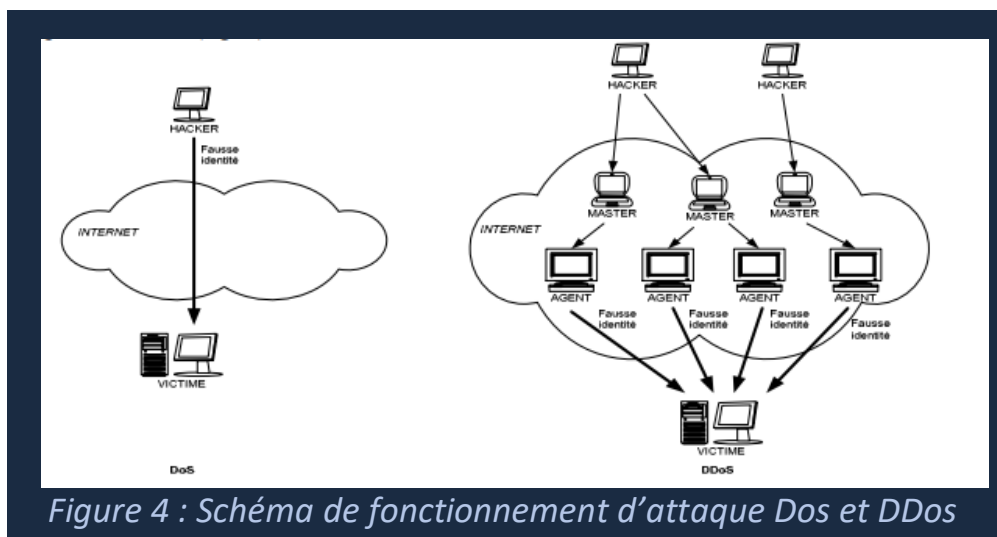
Puis on a pu constater que les méthodes les plus utilisées sont les faiblesses humaines et les faiblesses de sécurité. Les victimes ne sont pas assez formées pour décerner les emails malveillants ou bien sécuriser leur ordinateur. A la suite de ces types de faiblesses, on a expliqué la mise en place dans chaque cas.

S'il faut retenir une chose dans cette recherche c'est : les préventions et réactions. Toute individu doit savoir se prémunir d'une attaque et doit aussi savoir réagir en cas d'infection.

Etude des DDoS

Une attaque en déni de service ou en **déni de service distribué (DDoS)** vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. Ce type d'attaque peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou difficilement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité.

Le fonctionnement



Les objectifs et mise en œuvre des attaques

Les différents types d'attaques DDoS ciblent des composants variables d'une connexion réseau composé de couches (Modèle OSI).

Attaques sur la couche d'application

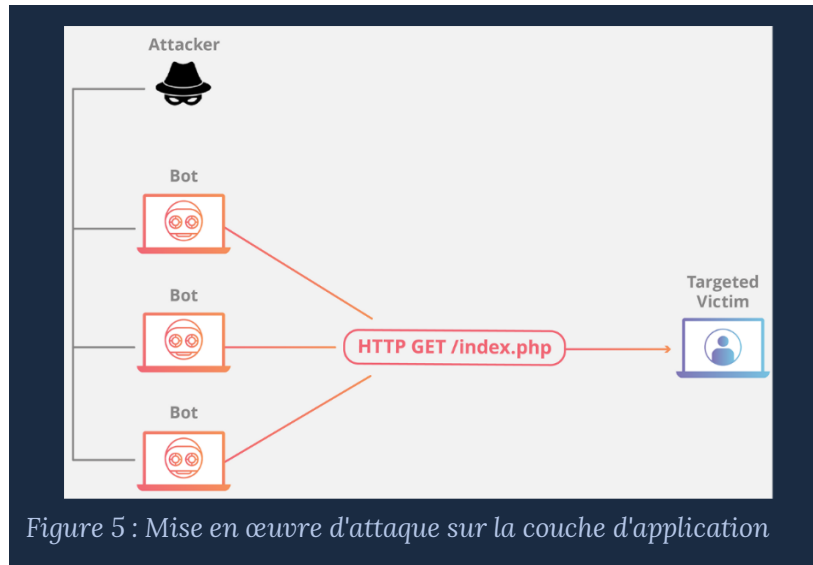
Objectif de l'attaque :

Parfois appelées attaques DDoS de la couche 7 (en référence à la septième couche du modèle OSI), ces attaques ont pour objectif d'épuiser les ressources de la cible afin de créer un déni de service.

Les attaques ciblent la couche où les pages Web sont générées sur le serveur et fournies en réponse aux requêtes HTTP. Une requête HTTP unique ne coûte pas cher à exécuter côté client, mais peut être coûteuse pour le serveur cible qui, pour y répondre, doit souvent charger plusieurs fichiers et exécuter des requêtes de base de données afin de créer une page web (figure 5).

Etude de cas n°2

Etude des DDoS

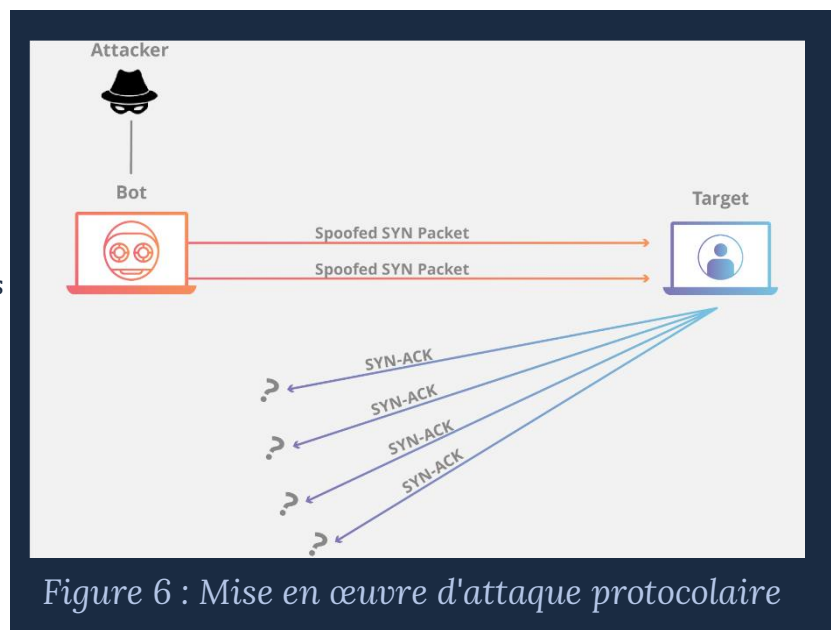


Attaques protocolaires

Objectif de l'attaque :

Les attaques protocolaires, également appelées attaques par épuisement des tables d'état, provoquent une interruption de service en consommant avec excès les ressources des serveurs ou les ressources des équipements réseau tels que les pare-feux et les équilibreurs de charge.

Les attaques protocolaires exploitent des faiblesses des couches 3 et 4 de la pile du protocole pour rendre la cible inaccessible.



Etude de cas n°2

Etude des DDoS

Attaques volumétriques

Objectif de l'attaque :

Cette catégorie d'attaques tente de créer une saturation en consommant toute la bande passante disponible entre la cible et Internet.

De grandes quantités de données sont envoyées vers la cible en utilisant une forme d'amplification ou un autre moyen de créer un trafic massif, comme des requêtes provenant d'un botnet.

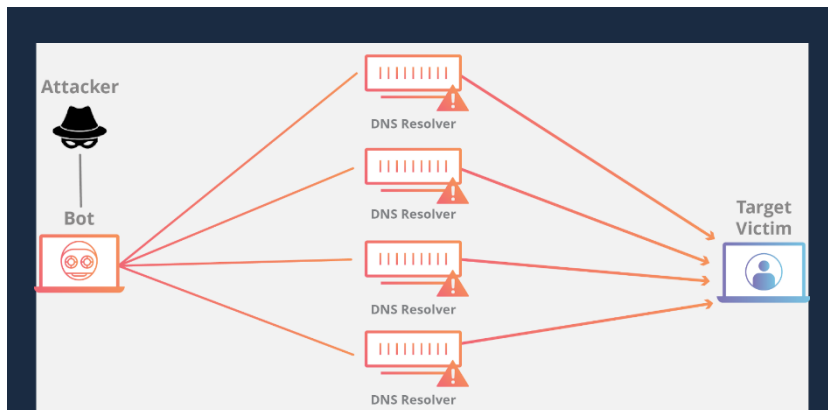


Figure 7 : Mise en place d'attaques volumétrique

Faiblesses utilisées

Tous les types d'attaques cités auparavant utilisaient des failles ou des limites des machines. On a encore une fois une exploitation des faiblesses humaines. Si la personne n'a pas mis en place des précautions de sécurité sur ces machines, elle aurait plus de chance d'être touchée par une attaque DDoS.

Les contre-mesures

1. Les pare-feux et les répartiteurs de charge peuvent contribuer à absorber certaines attaques DDoS, mais ils ne constituent pas une protection suffisante contre ce type d'attaque d'une manière générale.
2. Certains équipements dédiés offrent différentes contre-mesures spécifiques aux attaques DDoS. Leur mise en œuvre nécessite une prise en main préalable, et un paramétrage adapté au trafic de l'entité.
3. Les hébergeurs offrent parfois une protection contre les attaques DDoS. Les différentes options proposées peuvent constituer une solution pour les structures faisant appel à une société externe pour l'hébergement de leurs serveurs.
4. L'intervention de l'opérateur de transit est parfois nécessaire, en particulier lorsque le lien réseau mis à disposition du client est saturé. Les opérateurs permettent souvent d'effectuer du blackholing de trafic basé sur la destination. Il convient de noter que cette mesure, parfois nécessaire, rend le déni de service effectif.
5. Les CDN permettent la répartition de ressources sur un grand nombre de serveurs, ce qui peut contribuer à améliorer la résistance aux attaques DDoS.

Les Arnaques

Sources :

<https://www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos/>
<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos>
<https://www.elastic.co/fr/blog/your-package-has-been-successfully-encrypted-teslacrypt-41aand-malware-attack>
https://doc.rero.ch/record/323720/files/Misini_Leutrim_TDB.pdf
<https://go.sentinelone.com/rs/327-MNM-087/images/Data%20Summary%20-%20French.pdf>
<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiels-ransomwares>
<https://homepages.laas.fr/owe/METROSEC/gallon-aussibal.pdf>
<https://www.appvizer.fr/magazine/services-informatiques/securite-informatique/attaque-ransomware>
<https://www.wavestone.com/app/uploads/2016/09/Attaques-ciblees-refonte-gestion-crise.pdf>
<https://www.economie.gouv.fr/entreprises/rancongiels-ransomware-protection#>
<https://www.cloudflare.com/fr-fr/learning/ddos/what-is-a-ddos-attack/>
<https://www.lafinancepourtous.com/2022/07/28/baisse-de-la-fraude-des-paiements-sur-internet-en-france-en-2021/#:~:text=Le%20total%20des%20fraudes%20s,contre%200%2C088%20%25%20en%202020>
<https://www.ufcquechoisir-nimes.org/arnaques-sur-internet-vos-questions-nos-reponses-bien-reagir-en-cas-descroquerie>