Les Rançongiciels

Définition

Les rançongiciels ou ransomwares sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

Le but est simple extorquer de l'argent à la victime.

Méthode d’infection

- Par mail
- Navigation sur des sites compromis
- Intrusion dans le système
- Liens malveillants
- Pièces jointes

2 types d’attaques

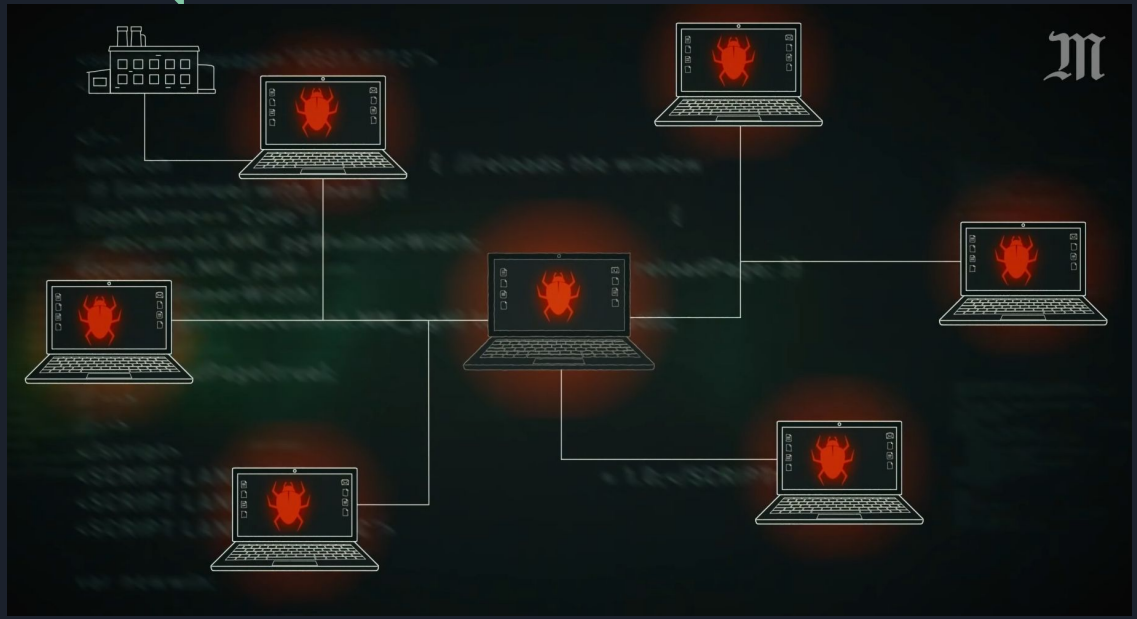
Attaque Opportuniste :

- Facile
- Attaque de masse
- 10-15 % de réussite

Attaque ciblée :

- Ciblage d’une entreprise
- Montant plus gros

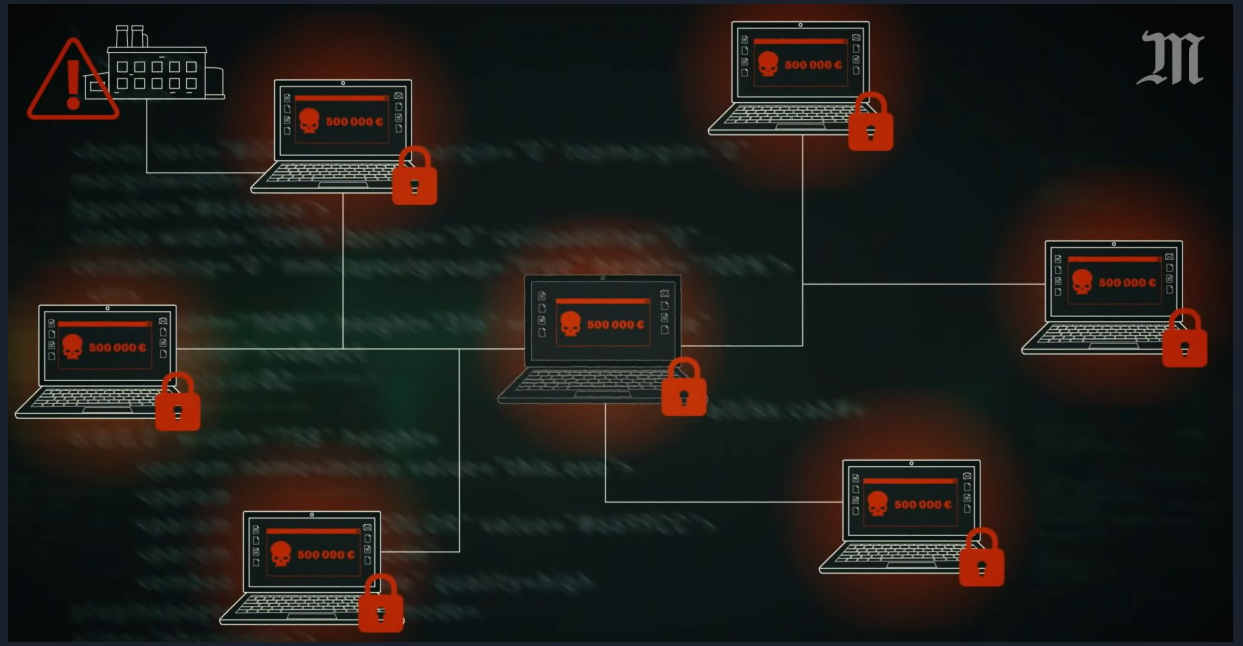
Déroulement d’une attaque



Une fois infecté, le virus ne se déclenche pas de suite, il se propage d’abord sur le réseau en quête d’autres machines à contaminer.

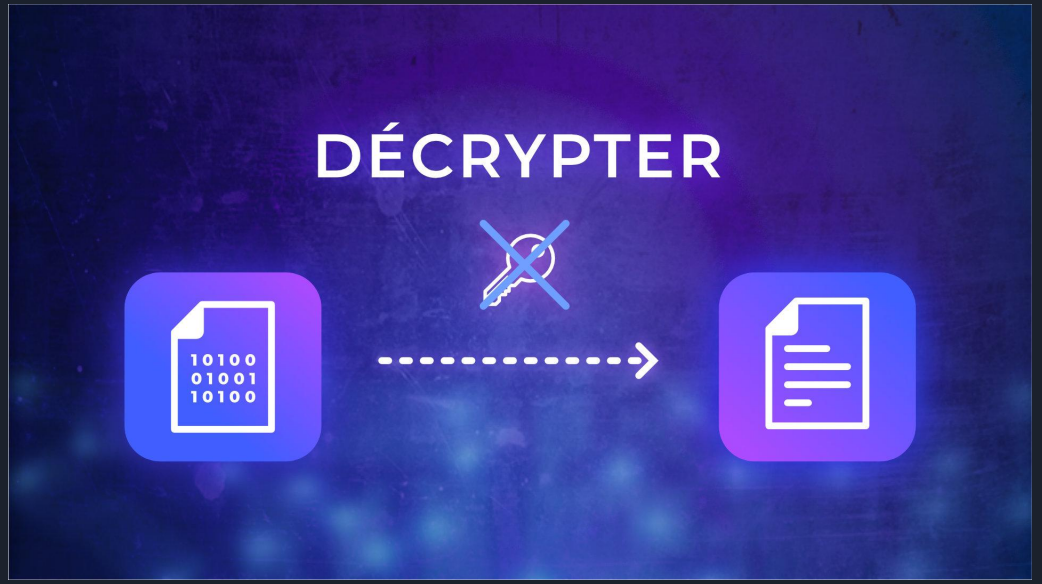
Après diffusion

Le logiciel est réveillé par les personnes malveillantes. Cela rend tous les dossiers et fichiers de l'ensemble des machines contaminées inna.



Comment deviennent-ils inaccessibles ?

Les fichiers/dossiers sont chiffrés ce qui les rend impossible à lire sans la clé de décryptage.



Quelques noms de rançongiciels

Ryuk : Ryuk est un logiciel malveillant de type rançongiciel. Découvert en 2018, il est l'un des rançongiciels les plus actifs à la fin des années 2010 et début des années 2020

Wannacry : WannaCry, aussi connu sous le nom WannaCrypt, WanaCrypt0r 2.0 ou similaires, est un logiciel malveillant de type rançongiciel auto-répliquant.

Auto-répliquant : logiciel qui utilise les systèmes obsolètes n'ayant pas effectué les dernières mises à jour de sécurité.

Cas n°1 : Hôpital de Rouen

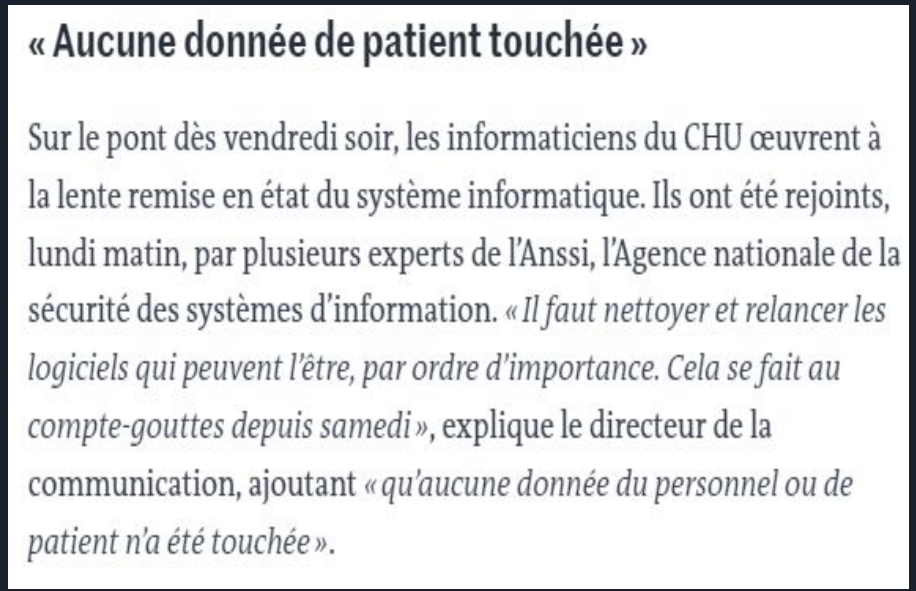
Frappé par une cyberattaque massive, le CHU de Rouen forcé de tourner sans ordinateurs

Le centre hospitalier, qui compte près de 2 500 lits d'accueil, se remet progressivement de la paralysie informatique provoquée par un virus de type rançongiciel.

On a ici le cas d'une attaque ciblée.

La variante de ransomware utilisée par les attaquants serait une variante de la souche CryptoMix, connue sous le nom de Cryptomix Clop.

Une rançon de 300 000 euros était demandée mais a été refusée. L'hopitale à préférer laisser les équipes informatiques réparer le système.



« Aucune donnée de patient touchée »

Sur le pont dès vendredi soir, les informaticiens du CHU œuvrent à la lente remise en état du système informatique. Ils ont été rejoints, lundi matin, par plusieurs experts de l'Anssi, l'Agence nationale de la sécurité des systèmes d'information. *« Il faut nettoyer et relancer les logiciels qui peuvent l'être, par ordre d'importance. Cela se fait au compte-gouttes depuis samedi »*, explique le directeur de la communication, ajoutant *« qu'aucune donnée du personnel ou de patient n'a été touchée »*.

Cas n°2 : Kaseya

De nouveau une attaque ciblée.

Kaseya : ce que l'on sait de la cyberattaque géante qui a paralysé des centaines d'entreprises

Chaîne de magasins en Suède, écoles en Nouvelle-Zélande, PME américaines... En ciblant la société informatique Kaseya le week-end dernier, une cyberattaque d'origine russe a fait plus de 1.000 victimes dans le monde. L'administration Biden a élevé la menace des ransomwares au rang de « priorité » pour la sécurité nationale.

Les hackers ont demandé une rançon de 70 millions de dollars sous forme de cryptomonnaies pour restaurer les données des entreprises affectées, tout en laissant transparaître à Kaseya la possibilité de négocier. Fred Voccola, qui s'est entretenu avec des représentants de la Maison-Blanche, avec le FBI et avec le département américain de la Sécurité intérieure, a refusé de commenter cette offre du groupe de pirates.

Dans un communiqué, la Maison-Blanche a déclaré avoir élevé la menace des ransomwares au rang de « priorité » pour la sécurité nationale. La lutte contre ce type de cyberattaques devient urgente pour l'administration Biden, qui a organisé une rencontre à huis clos avec divers dirigeants d'agences mercredi pour décider de la stratégie à adopter à la suite de cette nouvelle crise.

Pourquoi l'attaque est-elle de si grande ampleur ?

La faille exploitée par les hackers était une porte d'entrée idéale qui leur a permis d'affecter des milliers de machines en cascades. Tout d'abord, Kaseya, basé à Miami, est une société qui fournit des services informatiques à des entreprises qui, elles-mêmes, gèrent le back-office de nombreuses entreprises trop modestes pour disposer de leur propre service technique.

A l'étranger, les perturbations ont été importantes en Suède, où une chaîne a dû fermer la majorité de ses 800 magasins en raison de la panne des caisses enregistreuses. Une chaîne de pharmacie et une société de chemin de fer ont également été touchées dans le pays. En Nouvelle-Zélande, plusieurs écoles ont dû garder porte close, tandis qu'en Allemagne et au Pays-Bas, ce sont des sociétés de services informatiques qui ont été touchées. Le bilan global est compliqué à établir, la plupart des victimes de rançongiciels ne se signalant pas, d'autant plus si elles ont choisi de payer la rançon.

Prévention :

1. **Appliquez de manière régulière et systématique les mises à jour de sécurité**
du système et des logiciels installés sur votre machine.

2. **Tenez à jour l'antivirus et configurez votre pare-feu.**
Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.

3. **N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens**
provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.

4. **N'installez pas d'application ou de programme « piratés »**
ou dont l'origine ou la réputation sont douteuses.

5. **Évitez les sites non sûrs ou illicites**
tels ceux hébergeant des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

6. **Faites des sauvegardes régulières**
de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

7. **N'utilisez pas un compte avec des droits « administrateur »**
pour consulter vos messages ou naviguer sur Internet.

8. **Utilisez des mots de passe suffisamment complexes et changez-les régulièrement,**
mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés.

9. **Éteignez votre machine lorsque vous ne vous en servez pas.**

Que faire si on est victime de rançongiciel :

1.Débranchez la machine d'Internet ou du réseau informatique

2.En entreprise, alertez immédiatement votre service ou prestataire informatique

3.Ne payez pas la rançon

4.Conservez ou faites conserver les preuves par un professionnel

5.Déposez plainte

6.Pour une entreprise : notifiez cette infection à la CNIL s'il y a eu une violation de données à caractère personnel

7.Identifiez la source de l'infection et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire

8.Faites-vous assister au besoin par des professionnels qualifiés