Cybersécurité :

Table des matières

[Présentation : 1](#_Toc42463411)

[Clop et TA505: 1](#_Toc42463412)

[Prévention et conclusion : 3](#_Toc42463413)

# Présentation :

Le 15 novembre 2019 un ransonware est détecté au CHU de Rouen.

En effet l’alerte est donné par un interne qui n’arrive plus à accéder à un logiciel. L’attaque ne s’arrête pas là, le pirate est en train de bloquer toutes les machines disponibles. Le service informatique se rend compte que de nombreux fichés sont chiffrés tant sur les serveurs que sur les postes de travail. Ces derniers sont cryptés sous le suffixe .clop, et génèrent spontanément un message. Une réponse est automatiquement générée lorsque l’on adresse un message aux contacts figurant sur le message. Il y est question d’une demande d’argent pour débloquer la situation. Celle-ci s’élève à 40 bitcoins, soit l’équivalent de 300 000 euros, selon le cours numérique actuel de la cryptomonnaie. L’hôpital à décidé de ne pas payer la rançon.

En moins de deux heures une vingtaine de membres compose la cellule de crise, appuyé par sept agents de l’ANSI.

Très vite il apparaît qu’il s’agit d’un ransomware fonctionnant avec un service Windows et un exécutable permettant de chiffrer les documents sur les serveurs et postes de travail. Le service de cybersécurité a réussi très rapidement à rendre l’attaque inopérante, mais cette phase d’identification a permis de constater qu’un attaquant s’était emparé d’un contrôleur de domaine et était en train de propager son ransomware de manière manuelle et effectuant une élévation de privilège via des comptes de l’Active Directory. En parallèle le service de cybersécurité décide de couper tous les flux internes et externes afin d’éviter la propagation du malware sur les serveurs sains. Enfin, toutes les sauvegardes sont arrêtées afin de préserver les sauvegardes le plus longtemps possible.

L’attaque informatique a forcé l’établissement à revoir ses méthodes de fonctionnement et à revenir aux papiers et crayons pour suivre les dossiers des patients.

Trois jours plus (lundi aprèm), d’après un responsable, « plus de cinquante applications sur les deux cents au total que compte l’hôpital » était à nouveau en service.

**L’Agence nationale de la sécurité informatique (ANSI)**

# Clop et TA505:

L'ANSI a pu apporter davantage de précisions sur cette cyberattaque. "Ces attaques semblent être le résultat d'une vaste campagne d'hameçonnage ayant eu lieu autour du 16 novembre 2019 et liée au groupe cybercriminel TA505", a révélé l'agence dans un rapport publié le 22 novembre 2019. Ce ransomware a paralysé le système en chiffrant l'intégralité des fichiers qui s'y trouvent. Il a touché les applications utilisées pour la gestion des blocs, les pharmacies et les prescriptions, les admissions des patients et le suivi des arrivées aux urgences.

Ce groupe agit sur la toile depuis 2014. Il cible principalement le secteur de la finance, de la distribution, les institutions gouvernementales et plus récemment, les secteurs de l'énergie, de la recherche, de l'aviation et de la santé. Son outil de prédilection : le rançongiciel "Clop". Il chiffre les documents stockés sur le système d'information et leur ajoute l’extension ".CIop". Il ne procède pas au chiffrement tout de suite mais quelques jours après l'intrusion. Pendant ce laps de temps, les attaquants se chargent manuellement de la propagation du malware au sein du réseau victime. Clop est le plus souvent déployé en début ou à la veille d'un week-end, à un moment où les équipes sont forcément moins réactives.

# Prévention et conclusion :

Pour limiter la casse, l’agence offre quelques recommandations : durcir les postes de travail en mettant en place par exemple des outils de contrôle de l’exécution des fichiers, prévoir un système de sauvegardes déconnectées du réseau et enfin renforcer la sécurité de l’active directory de l’entreprise. L’agence fait également remarquer que la diffusion du malware sur le réseau se fait de manière manuelle, via des comptes administrateur compromis : la surveillance de ces comptes peut donc permettre de détecter un comportement inhabituel.