CI-CERT

Cote d'Ivoire Computer Emergency Response Team

RANSOMWARE

COMMENT SE PREMUNIR DE CETTE ATTAQUE ?

Document Public

Version 1.0

www.cicert.ci
info@cicert.ci
00225 – 20 34 43 73

Sommaire

I. Définition

Un rançongiciel est un programme malveillant qui provoque le chiffrement de tous les fichiers d'un ordinateur (et des fichiers accessibles en écriture sur les dossiers partagés si votre ordinateur est connecté à un réseau informatique). De plus en plus de personnes reçoivent des messages douteux contenant des pièces jointes ou des liens vous invitant à les ouvrir. Il faut prendre garde à ces messages car des logiciels malveillants appelés « rançongiciel » ou « ransomware » peuvent s'y cacher. Leur but est de chiffrer (coder) vos données pour vous les rendre moyennant une rançon. Bien entendu, la payer ne garantit pas la récupération de vos données. Mieux vaut donc vous prémunir contre ce type d'attaque.

Contre les Ransomwares, la meilleure défense est la prévention. Les mesures suivantes vous permettront de ne pas être attaqués ou au moins de minimiser l'impact d'une attaque.

II. Mesures comportementales

De façon générale, voici les conseils à appliquer pour se protéger des ransomwares (les éviter et récupérer vos fichiers en cas de soucis). N'ouvrez pas les messages dont la provenance ou la forme est douteuse, il pourrait s'agir d'un rançongiciel. Ne vous laissez pas tromper par un simple logo ! pire, le hacker peut avoir récupéré certaines de vos données préalablement (les noms de vos clients ou de vos collègues par exemple) et créer des adresses de messagerie ressemblant à un détail près à celle de vos interlocuteurs habituels. Restez donc très vigilants ! Certains messages paraissent tout à fait originaux

- N'ouvrez pas les messages dont la provenance ou la forme est douteuse, il pourrait s'agir d'un rançongiciel ;
- Éviter de cliquer sur des liens trop alléchants ;
- Afficher les extensions des fichiers sur l'ordinateur ;
- Apprenez à identifier les extensions des fichiers douteuses (si vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute finit par un autre type d'extension, ne les ouvrez surtout pas. Exemples : pif ; .com ; .bat ; .exe ; .vbs ;. lnk.
  Attention à l'ouverture de pièces jointes de type .scr ou .cab. Il s'agit des extensions de compression des campagnes CTB-Locker sévissant chez les particuliers, les PME, etc.

- Restez méfiants encore et toujours en ne cliquant que sur des programmes dont vous avez confiance ;
- La plupart des courriers électroniques contenant des fichiers joints sont annoncés par des discussions précédentes, respectivement s'inscrivent dans un contexte spécifique légitimant l'ajout de pièces jointes. Si cela n'est pas le cas, soyez très prudents lors de la réception de courrier avec fichier joint, car ceux-ci peuvent contenir des codes malicieux.

III. Mesures organisationnelles

- Rédiger et faire appliquer les politiques sectorielles de sécurité (protection contre les logiciels malveillant, courrier électronique, contrôle d'accès, la formation et l'information, etc.) ;
- Faire des sauvegardes régulières des données importes et sensibles ;
- Formation du personnel sur les questions de sécurité ;
- Formation du personnel aux risques liés à l'ingénierie sociale ('social engineering') ;
- Essayez d'éliminer tout processus impliquant des pièces jointes ;
- En cas d'obligation à ouvrir les fichiers joints :
    - ✓ Attendez quatre (04) jours avant d'ouvrir les fichiers joints. Ce laps de temps augmente les chances de détection par l'antivirus de codes malicieux. En effet, au moins 3 à 4 jours sont nécessaires pour détecter un nouveau virus après sa première apparition et l'introduire dans les bases de signatures les antivirus correspondants.
    - ✓ Équipez les ordinateurs servant à ouvrir les fichiers joints, d'un système d'exploitation moins répandu et de ce fait moins attaqué, comme par exemple 'Linux' ;
    - ✓ Appelez la personne qui vous a envoyé un courrier électronique suspect et demandez-lui si elle vous a vraiment envoyé ce courrier. Informez-la sur les raisons qui vous ont poussé à estimer le courrier électronique comme étant suspect ;
    - ✓ Evitez de consulter des courriers électroniques sur des actifs critiques ou ayant accès à des actifs critiques comme notamment des informations confidentielles ou encore des actifs indispensables.

IV. Mesures techniques

Pour se prémunir d'un ransomware, utilisez un compte « utilisateur » plutôt qu'un compte « administrateur ». Il ne faut pas naviguez depuis un compte administrateur car l'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur. Préférez l'utilisation d'un compte utilisateur et cela ralentira, voire dissuadera le pirate dans ses actions malveillantes.

- Ne travaillez pas sur une station de travail en étant connecté en mode administrateur. Les codes malicieux exécutés sur ces postes héritent de vos droits et peuvent donc s'installer et accéder à tous les comptes de la machine;
- Sauvegardez régulièrement vos fichiers de façon chiffrée sur un service de stockage en ligne ;
- Sauvegardez régulièrement les fichiers sur un support externe et non connecté en permanence au réseau ;
- Utiliser un logiciel antivirus et un système à jour ;
- Si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera en effet la propagation des rançongiciel via les vulnérabilités des applications ;
- Faites-en sorte que votre pare-feu soient à jour ;
- Vérifiez que tous les logiciels de votre ordinateur sont à jour, y compris votre système d'exploitation, votre navigateur et toute barre d'outils supplémentaire utilisée.

V. En cas d'incident – Mesures Réactives

Si le code malveillant est découvert sur vos systèmes :

- Déconnectez immédiatement du réseau les équipements identifiés comme compromis. L'objectif est de bloquer la poursuite du chiffrement et la destruction des documents partagés ;
- Alertez le responsable sécurité ou le CI-CERT au plus tôt ;
- Sauvegardez les fichiers importants sur des supports amovibles isolés. Ces fichiers peuvent être altérés ou encore être infectés. Il convient donc de les traiter comme tels. De plus, les sauvegardes antérieures doivent être préservées d'écrasement par des sauvegardes plus récentes.

- Ne payez pas la rançon. Le paiement ne garantit en rien le déchiffrement de vos données et peut compromettre le moyen de paiement utilisé (notamment carte bancaire).

Liens utiles

https://www.nomoreransom.org/fr/decryption-tools.html

https://www.avast.com/fr-fr/c-ransomware

https://noransom.kaspersky.com/fr/

https://www.emsisoft.com/decrypter/