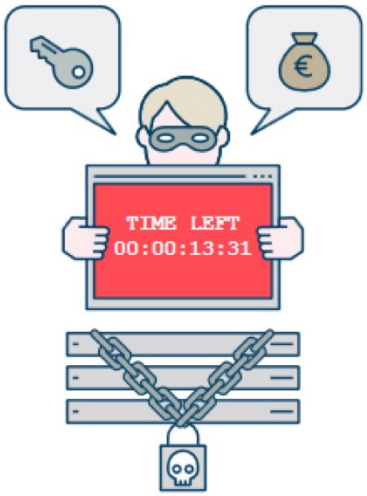
SÉCURITÉ DU NUMÉRIQUE
RANÇONGICIEL : VOS DONNÉES PRISES EN OTAGE

Cible : tous publics

- Un rançongiciel (*ransomware* en anglais) est un programme malveillant dont le but est de chiffrer partiellement ou entièrement les données d'un système, bloquant ainsi leur accès.
- La machine peut être infectée après l'ouverture d'une pièce-jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en navigant sur des sites compromis, ou encore suite à une intrusion dans le système.
- Le principal but recherché est d'extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Si l'intention de ce type d'attaque est cybercriminelle, le mode opératoire de ces attaques peut être lourd de conséquences pour les victimes qui peuvent par exemple voir leur activité paralysée.
- Particulièrement répandues, ces attaques sont de plus en plus sophistiquées et peuvent toucher l'ensemble des acteurs de la société, qu'il s'agisse de citoyens ou d'organisations publiques ou privées.



1 Comment réagir ?

1- N'éteignez pas la machine concernée

L'interruption du processus de chiffrement empêche toute tentative ultérieure de récupération des données.

Mettez la machine en veille prolongée si possible.

2- Déconnectez immédiatement du réseau les machines concernées

L'objectif est de limiter la propagation de l'attaque en bloquant la poursuite du chiffrement des documents sur le réseau. Ne connectez pas non plus d'appareil supplémentaire sur le réseau.

3- Contactez immédiatement votre service informatique ou un expert

Vous êtes un ministère, un opérateur d'importance vitale (OIV), un opérateur de service essentiel (OSE) ou un fournisseur de service numérique (FSN) ?

➔ Prévenez l'ANSSI :
www.ssi.gouv.fr/en-cas-dincident/

Vous êtes une collectivité territoriale, une entreprise privée (non OIV, non OSE), une association ?

➔ Contactez si besoin cybermalveillance :
www.cybermalveillance.gouv.fr

4- Ne payez pas la rançon réclamée

Le paiement ne garantit pas le déchiffrement des données et compromettra le moyen de paiement utilisé.

5- Portez plainte auprès des services compétents

Pensez à réunir toutes les traces et indices qui pourraient servir comme éléments de preuve (ex : copies physiques de disques durs des postes compromis).

6- Identifiez la source de l'infection

Prenez les mesures nécessaire pour que la source de l'infection ne puisse pas être utilisée à nouveau (par l'application d'un correctif de sécurité par exemple).

2 Comment se protéger ?

Effectuez des sauvegardes régulières de vos données critiques

Ces sauvegardes vous permettent de limiter le préjudice de l'incident et de reprendre vos activités rapidement. Les supports de ces sauvegardent doivent être déconnectées physiquement du réseau afin d'éviter toute compromission en cas d'incident. Faites également des tests de restauration de sauvegarde réguliers afin de vérifier votre capacité à restaurer vos données en cas d'incident.

Mettez à jour régulièrement vos logiciels

Les rançongiciels utilisent les vulnérabilités des programmes pour se propager, appliquez-donc de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur vos systèmes.

Privilégiez un compte utilisateur pour vos usages courants

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

Méfiez-vous des messages douteux

Ne faites pas confiance à l'expéditeur de courriers électroniques dont l'origine ou la forme vous semble douteuse et méfiez-vous des pièces-jointes et des liens suspects. Il convient en effet de ne pas cliquer sans vérification sur les liens ni d'ouvrir les pièces jointes présentes ; une attention toute particulière devant être apportée aux messages de provenance inconnue, d'apparence inhabituelle ou frauduleuse.

3 En savoir plus

Les bonnes pratiques de l'informatique :
www.ssi.gouv.fr/precautions-elementaires/

Guide d'hygiène informatique (à l'attention des DSI)
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

En cas d'incident : https://www.ssi.gouv.fr/en-cas-dincident/

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle graphique, fabrication, image – DSAF/DPGS – Avril 2019.