Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE CHARGÉ DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

REAGIR A LA MENACE CRYPTOVIRUS – REFLEXES

QU'EST-CE QU'UN CRYPTOVIRUS ?

Un cryptovirus en anglais, est un programme informatique malveillant, qui prend en otage les données en les chiffrant.

OBJECTIFS DE L'ATTAQUE

- Prendre en otage les données de l'ordinateur et forcer l'utilisateur à payer pour les débloquer et les récupérer.
- Bloquer les données ou rendre le poste inaccessible

RISQUES

- ➔ **PROPAGATION SUR LE RESEAU**
- ➔ **CHIFFREMENT DES REPERTOIRES EN PARTAGE**
- ➔ **PERTE DEFINITIVE DE DONNEES**

SYMPTOMES

AFFICHAGE D'UNE DEMANDE DE RANÇON
BLOCAGE DU POSTE

ORIGINES

- Mail piégé (selon une étude PhishMe, 93% des mails malveillants contiennent un cryptovirus)
- Contamination par des systèmes voisins compromis
- Contamination par l'installation d'un logiciel infecté
- Périphérique amovible
- Navigation web

QUOI FAIRE

- **DECONNECTER L'ORDINATEUR DU RESEAU (CABLE RESEAU, CARTE WIFI)**
- **AVERTIR LE RESPONSABLE SECURITE**
- **AVERTIR LES TECHNICIENS**
- **NE PAS PAYER LA RANÇON**
- **PORTER PLAINTE AUPRES DE LA POLICE OU LA GENDARMERIE**

REAGIR A LA MENACE CRYPTOVIRUS – REFLEXES

PAYER OU NE PAS PAYER ?

Le paiement de la rançon ne garantit pas la récupération de la clé de déchiffrement permettant la récupération des données.

LES BONNES PRATIQUES

- Installer régulièrement et au plus tôt en fonction des contraintes opérationnelles les correctifs de sécurité du système et des logiciels
- Réaliser des sauvegardes régulières, hors ligne et les tester
- Durcir les systèmes
- Restreindre autant que possible les droits d'accès en écriture sur les partages réseau
- Eviter de donner aux utilisateurs les droits administrateurs
- Sensibiliser les utilisateurs (réaction face à des courriels suspects, utilisation des périphériques amovibles, etc.)
- Limiter l'exposition depuis Internet
- Utiliser des passerelles de messagerie équipées de solution de sécurité afin de réduire le risque

RESSOURCES

- Nomoreransom
- Analyser un poste avant le démarrage de l'ordinateur
- Protection contre les rançongiciels

REPARER ET ENQUETER

LES PRINCIPALES ETAPES DE L'ENQUETE •

- **Identifier le cryptovirus**

L'identification du cryptovirus peut permettre d'identifier s'il existe une solution de déchiffrement. Plusieurs solutions existent :

- envoyer un échantillon infecté sur le site https://www.nomoreransom.org/
- regarder l'extension des fichiers infectés
- analyser le système avec un autre anti-virus (boot-cd)

- **Réinstaller le système**

La réinstallation totale (et donc le reformatage) du système s'avère souvent nécessaire pour s'assurer que le poste n'est plus infecté.

- **Restaurer les données**

Il est indispensable de posséder des sauvegardes, afin de permettre une reprise de l'activité dans un délai acceptable.

- **Déterminer l'origine de l'infection**

Quel que soit l'origine de l'incident, sensibiliser les utilisateurs et déployer des patches de sécurité.

- **Sensibiliser les utilisateurs**

Selon l'origine de l'infection, il est indispensable de sensibiliser les utilisateurs afin d'éviter une reproduction de l'incident.

PLAN D'ACTION RAPIDE

• ISOLER LA OU LES MACHINES COMPROMISE(S) POUR ARRETER LA PROPAGATION • NE PAS PAYER LA RANÇON • AVERTIR LES UTILISATEURS PAR MAIL • DESINFECTER L'ORDINATEUR • ORGANISER UNE REUNION POST-INCIDENT

• EN FONCTION DES ELEMENTS QUI CARACTERISE LE MESSAGE A L'ORIGINE DE L'INFECTION (URL UTILISEES, NOM DE FICHIER, SUJET DU COURRIER ELECTRONIQUE, ETC.), DES ACTIONS PEUVENT NOTAMMENT ETRE ENTREPRISES SUR LES PASSERELLES DE MESSAGERIE, DE NAVIGATION SUR INTERNET OU LES SERVEURS DE BOITE AUX LETTRES POUR EVITER DE NOUVELLES INFECTIONS. IDENTIFIER D'AUTRES PERSONNES QUI AURAIENT ETE DESTINATAIRES DU MEME MESSAGE POUR QU'IL SOIT SUPPRIME.