efrei PARIS
Ecole d'ingénieurs du numérique

GROUPE 316

RANSOMTION PROTECWARE

LA SOLUTION POUR VOUS PROTÉGER DES RANSOMWARES

PRÉVENTION EMPLOYÉ

LES SOURCES DES RANSOMWARES

Le plus souvent ce sont des mails spams, très ressemblant à un mail du gouvernement, de votre banque ou d'un opérateur téléphonique qui vous demande de cliquer sur un lien.

Certains indices facilitent la détection

- **http au lieu de https**
- **Nom peu familier**
- **Domaine incorrect (.goov, .gouve au lieu de .gouv pour l'état français)**

L'HUMAIN, FACTEUR NUMÉRO 1

Tout le monde peut être un vecteur.

Un bon service de sécurité de l'information n'est pas garant d'une invulnérabilité à toute menace.

L'HUMAIN, FACTEUR NUMÉRO 1

L'ingénierie sociale est de plus en plus répandue et **facilitée par les nombreux réseaux sociaux**. Elle fonctionne parce que d'instinct, **l'humain fait confiance**.

Un courriel, un message vocal ou un texto bien ciblé est capable de convaincre les personnes visées à transférer de l'argent, divulguer des informations confidentielles ou télécharger un fichier qui **installera un logiciel malveillant sur le réseau de l'entreprise**, notamment un ransomware.

LES ERREURS À NE PAS FAIRE

- **UNE CLEF USB SUR LE PARKING ?**

Ne la connectez pas à un ordinateur sur le réseau de l'entreprise. Consultez le service informatique de l'entreprise.

- **BESOIN D'UN LOGICIEL ?**

Ne téléchargez pas un logiciel depuis un site tiers, ces derniers sont souvent corrompus et contiennent des fichiers indésirables. Utilisez uniquement les sites officiels

- **UN MAIL DE VOTRE BANQUE, VOTRE OPÉRATEUR TÉLÉPHONIQUE ?**

Attention au format de l'adresse mail et à ce que l'on vous demande. Par exemple vous rendre sur un lien http pour vous connecter à votre compte bancaire serait une drôle de façon de faire pour une banque. On vous demandera plutôt de vous rendre vous-même sur le site de la banque et de vous y connecter.

LES BONNES PRATIQUES

- **GARDER SES LOGICIELS À JOUR**
  Les éditeurs de logiciels mettent régulièrement leurs produits à jour pour contrer des failles de sécurité.

- **UTILISER DES PRODUITS ANTIVIRUS FIABLES**

Les solutions de protections grand public sont déjà une bonne façon de se protéger des logiciels malveillants les plus connus.

- **EVITER D'UTILISER SON ORDINATEUR PERSONNEL SUR LE RÉSEAU DE L'ENTREPRISE**

Du moins, limitez l'accès de votre ordinateur au réseau.

- **EVITER D'UTILISER DES APPLICATIONS PERSONNELLES SUR VOTRE ORDINATEUR PROFESSIONNEL**

Réseaux sociaux, messageries personnelles sont autant de vecteurs d'attaques entre internet et le réseau de l'entreprise.

- **ÊTRE CONSCIENT(E) DE QUOI FAIRE LORS D'UNE ATTAQUE**

Soyez prêt(e) à réagir en cas d'incident (voir prochaine partie).

COMMENT RÉAGIR FACE À UNE ATTAQUE RANSOMWARE

DÉMARCHES À SUIVRE

- Débrancher la machine infectée du réseau pour éviter la propagation
- Prévenir le service sécurité de votre entreprise
- Ne surtout pas éteindre la machine

LE SERVICE SÉCURITÉ VA AINSI POUVOIR

- Conserver toutes les preuves pour déposer plainte et avertir la CNIL
- Sur l'ordinateur touché, déceler sa vulnérabilité, récupérer si possible les données atteintes et éliminer le malware rançonneur.

La règle est de **ne jamais payer** : il faut essayer de résoudre le problème avec le service de sécurité de votre entreprise ou contacter des services compétents.