Êtes-vous prêts à faire face à un ransomware ?

Depuis le début de l'année 2016, la tendance massive est au ***ransomware***.

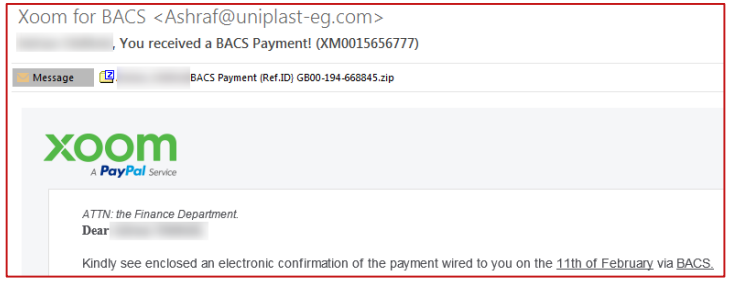
Ces programmes malveillants chiffrent les données et rendent inaccessibles le contenu des disques locaux et volumes partagés.
Cette forme de cybercriminalité vise à **extorquer de l'argent en prenant en otage les données**. Il s'agit d'attaques de masse renouvelées fréquemment.

Le ransomware est **distribué par mail** à l'occasion de campagnes de *phishing,* ou **par l'intermédiaire de sites Web** compromis. Le nombre de systèmes affectés (personnels ou professionnels) est très important.

Des mesures préventives basiques sont à prendre en compte :

- **Communiquer** sur cette menace **auprès des collaborateurs**, rappelez leur la vigilance minimale nécessaire dans l'ouverture des mails et la navigation Web ;
- Rappeler les bonnes pratiques de stockage des informations critiques : limiter l'usage du stockage local au poste de travail et les droits en écriture ;
- Effectuer les **renforcements de base** (désactivation des macros, blocage des pièces jointes aux extensions improbables)
- S'assurer de la bonne **sauvegarde des informations** : tester les procédures de restauration, conserver des sauvegardes hors ligne, … ;
- Faciliter les opérations de détection et de réponse aux incidents avec logiciels adaptés : protection antivirale, analyse des flux web et messagerie, centralisation des journaux (notamment des serveurs de messagerie, des proxy, des serveurs de fichiers), … ;
- Préparer et **tester vos capacités de détection et de réponse**, avant de faire face à un incident réel, au travers d'un exercice.

SOLLICITEZ LE CERT-Intrinsec EN CAS DE BESOIN D'ASSISTANCE PREVENTIVE OU CURATIVE
01 47 28 38 39 - cert@intrinsec.com



Les mails de phishing sont relativement soignés : langue adaptée au destinataire, bons prétextes pour faire ouvrir la pièce jointe…

Même si une demande de rançon apparaît, il n'est pas trop tard. La situation peut être rattrapée ou enrayée rapidement.