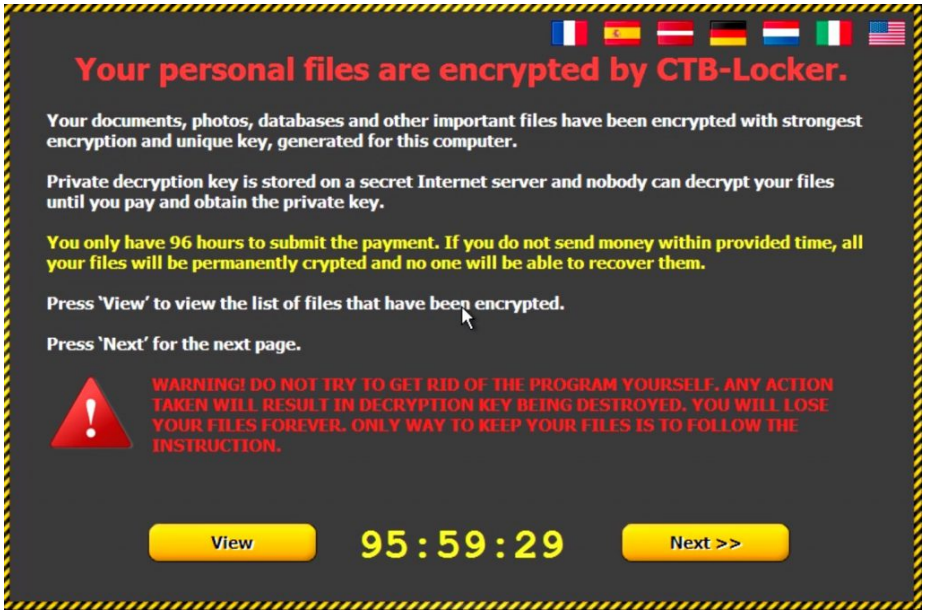
Comment vous protéger des Ransomwares ?



Comment vous protéger des Ransomwares ?

Cela n'est pas vraiment un scoop, les ransomwares sont en plein essor depuis quelques années. Comment concrètement protéger les utilisateurs d'un parc informatique contre ceux-ci ?

Il est d'abord crucial de rappeler que les utilisateurs sont le cœur du système d'information, ils en sont les principaux acteurs et représentent ainsi une ressource à protéger, en plus des données qu'ils manipulent et traitent, ils sont également le vecteur principal des attaques et des menaces.
Dans cet article nous allons passer en revu quelques points importants dans le but de protéger ses utilisateurs et son système d'information des infections de malware et notamment des ransomwares.
Pour rappel, un rançongiciel ou ransomware, est un malware (un programme, bout de code) qui va infecter un poste utilisateur, un serveur ou même un système informatique au complet, **pour chiffrer leur contenu de manière non définitive**. L'intérêt du pirate lors du déploiement d'un ransomware est de **prendre en otage les données de l'utilisateur**, qui n'y a plus accès puisqu'elles sont chiffrées. L'infection par un ransomware passe très souvent par l'affichage d'un message à l'utilisateur lui indiquant comment payer sa rançon afin, éventuellement, **d'obtenir une clé de déchiffrement lui permettant de récupérer ses données**.
Voici quelques exemple de ces messages :

Parmi les ransomwares les plus connus, et il y en a hélas beaucoup ces derniers temps, on retrouve :
• CryptoLocker : Ce cheval de Troie apparu en 2013 générait une pair de clé RSA 2048 bits et chiffrait certains documents en les repérant via leurs extensions. **Le malware demandait une rançon payable en Bitcoin et menaçait de supprimer les données au delà de 3 jours.** Ce délai n'était en réalité mis en place uniquement pour presser l'utilisateur et l'inciter à payer puisque les données étaient toujours récupérables, sous réserve d'en posséder la clé, après ce délai. Les gains de Evgeniy Bogachac, signalé comme responsable du déploiement du ransomware, ont été estimés à 3 millions de dollars.
• CryptoWall : Un cheval de Troie ciblant les OS Windows apparue en 2014, dérivé de CryptoLocker, **il se déployait notamment par l'intermédiaire de bannières publicitaires sur des sites web qui téléchargeaient et exécutaient le code malveillant.** La version 3.0 utilisait un payload écrit en Javascript, envoyé en pièce jointe des mails, qui était déguisé en image pour passer inaperçu auprès des utilisateurs. Environs 1 000 victimes de se ransomware on été constatée par le FBI en juin 2015, les rapports d'infection ont permis d'estimer une perte totale de 18 millions de dollars pour les victimes.
• Locky : Il s'agit d'un des ransomwares les plus actifs en 2016, il utilise le mail comme moyen d'infection avec un document word en pièce jointe. **Ce dernier contient des macros malicieuses et une partie de social engineering cherchant à convaincre les utilisateurs d'activer cette dernière.** La rançon demandée en échange de la clé de déchiffrement est généralement entre 0.5 et 1 bitcoins. Un fait marquant concernant ce ransomware est par exemple cas du Hollywood Presbyterian Medical Center qui a payé 17 000 dollars en bitcoin afin de récupérer ses données après une infection par le ransomware Locky
Il ne s'agit là que des plus connus, bien d'autres existent aujourd'hui.
Le scénario catastrophe est bien entendu celui présenté dans la série Mr Robot, **l'intégralité des postes utilisateurs et serveurs de l'entreprise E-corp se retrouvent infectés par un ransomware** et il est totalement impossible pour les administrateurs du parc informatique de retrouver une quelconque donnée, mis à part les backups restés offline.

Ainsi, toutes les données de l'entreprise sont prises en otage.. A ce propos, avez vous des backups offline et mis à jour régulièrement ? 😉
Voici quelques points importants concernant la protection contre les ransomwares :

Garder un système d'information à jour

Qu'il s'agisse de la base anti-virus centralisée, des règles IDS/IPS ou de l'ensemble des applications métier, **les mises à jour permettent dans la plupart des cas d'éviter une infection qui souhaiterait se déployer en exploitant des vulnérabilités connues.** Il est en effet fort dommage d'être infecté par le biais d'une vulnérabilité connue et dont le correctif est disponible et aurait pu être appliqué. Ainsi, il est important d'avoir un processus de mise à jour réactif et bien organisé pour ces différents éléments. **Les anti-virus centralisés sont par exemple une bonne option** car le déploiement de la mise à jour des bases-virales et des signatures est directement intégré pour un déploiement sur tous les postes.
Également, des solutions comme WSUS permettent bien souvent de gérer finement les mises à jour, notamment celles de sécurité, afin d'évaluer l'impact sur une application métier par exemple.

La sensibilisation des utilisateurs

Il s'agit certainement du point le plus important, **à la fois le plus ardu mais aussi le plus efficace.** La sensibilisation de tous les acteurs du SI, et notamment des utilisateurs non technique, permet de mettre en place un comportement et une approche de la sécurité qui peut faire la différence. **Cela passe par des éléments aussi simple que de savoir évaluer la pertinence et la provenance exacte d'un mail reçu**, ainsi que du comportement à adopter en cas de doute. Mais également par des éléments techniques comme la possibilité de voir, dans la configuration par défaut des postes utilisateurs, les extensions de fichier afin d'y repérer un « *.pdf.exe* » par exemple.
La sensibilisation des utilisateurs est souvent **gérée par un l'équipe de sécurité ou les administrateurs systèmes**, cela requiert une compétence réelle en terme de pédagogie et certaines entreprises peuvent faire le choix d'externaliser ce point pour une meilleur efficacité. Pour commencer, il peut être mis en place dans un premier temps la diffusion d'une newsletter « *Informatique et sécurité* » diffusée une fois par mois aux utilisateurs et qui contiendrait les bonnes pratiques à adopter, les risques du moment, etc. Le tout en des termes non technique et de façon succincte pour que la newsletter soit lue.

Les backups

Cela a déjà été évoqué plus haut dans l'article, mais les backups sont votre seul recours en cas d'infection. En effet, même si la rançon est payée, il n'est pas toujours certains que les données soient retrouvées saines et sauves. Ainsi, **il vaut mieux opter pour une rétablissement des sauvegardes.** Dans ce cas, il faut que ces sauvegardes soient le plus à jour possible. Ainsi, il est important de mettre en place un processus de backup efface et régulier. **Ce point ne pose généralement pas de problème aux grandes entreprises qui en sont déjà munies** (qui n'a jamais supprimer un dossier important après une mauvaise manipulation ?), mais les entreprises en pleines croissances peines souvent à le mettre en place avant qu'un incident arrive.
Dans ce cas, il est important d'être proactif. Également, et dans les cas les plus avancés, la mise en place de backup offline est également vital. La fameuse sauvegarde sur cassette est alors une option à mettre en place en cas d'infection globale du SI.

Les filtres anti-spams et l'analyse des mails

Nous l'avons vu en détaillant les principes de fonctionnement de quelques ransomwares, le vecteur de transmission reste généralement le mail. Ainsi, disposer de bons filtres et anti-virus permet d'écarter la menace avant qu'elle n'arrive sur le poste de l'utilisateur.
Des solutions managées en mode SaaS peuvent ainsi être utilisés sans un processus trop lourd de mise en place et d'installation…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Ransomwares, des actions pour protéger ses utilisateurs — Information Security