KASPERSKY lab

VOTRE ENTREPRISE POURRAIT-ELLE SURMONTER UNE ATTAQUE DE CRYPTOVIRUS ?

Apprendre à se prémunir contre les programmes malveillants de type ransomware

www.kaspersky.com/fr/business
#SecureBiz

Un guide pratique pour les attaques de cryptovirus

Les dégâts qu'ils causent aux entreprises et comment éviter une infection

- Qu'est-ce qu'un ransomware ?
- Quels dégâts cause-t-il ?
- Des frais encore plus élevés pour les entreprises
- Il y a plus d'attaques de cryptovirus que jamais
- Comment attaque un cryptovirus
- Ce qu'il attaque
- Les cryptovirus d'aujourd'hui sont plus dangereux
- Cacher leurs traces
- Comment protéger votre entreprise
- Obtenez une sécurité primée

Qu'est-ce qu'un ransomware ?

Le temps des programmes malveillants simples (développés par des amateurs qui cherchaient juste à se mettre en avant) est révolu depuis longtemps. Le crime organisé se trouve derrière la plupart des programmes malveillants d'aujourd'hui... et l'objectif est de gagner de l'argent.

Comme son nom en anglais l'indique, un ransomware est un type spécifique de programme malveillant qui tente d'extraire une rançon, en échange du déblocage de l'accès à une ressource qui appartient à la victime.

Dans le cas des cryptolockers, les ressources « kidnappées » sont les fichiers et les données qui sont stockées sur l'appareil infecté. Le cryptovirus chiffre les données de la victime sous une forme illisible et les données peuvent uniquement être déchiffrées en utilisant la clé de déchiffrement nécessaire... mais cette clé est uniquement donnée par le criminel après que la victime a payé la demande de rançon.

Un cryptovirus affichera souvent une boîte de dialogue qui stipule que le chiffrement a été effectué à la suite d'un acte illégal de la part de la victime.

Souvent, le message prétendra provenir de la police ou du FBI.

Quels dégâts cause-t-il ?

Les attaques de cryptovirus affectent à la fois les consommateurs et les entreprises.

Alors que les consommateurs sont souvent confrontés à des demandes de rançon de 300 à 500 $, les cyber-criminels comprennent tout à fait la valeur des données pour une entreprise... les demandes de rançon peuvent donc être beaucoup plus élevées.

Si l'un de vos appareils est infecté, l'attaquant vous donnera normalement de 48 à 72 heures pour payer la rançon. Si vous ne payez pas dans ce délai, le prix du déchiffrement est susceptible d'augmenter. Après qu'une deuxième échéance a été fixée, et si le paiement n'est pas encore effectué, il est probable que la clé de déchiffrement soit supprimée. À ce stade, il peut être impossible de récupérer vos fichiers dans un format lisible.

D'ailleurs, même si vous payez la rançon, il n'y a aucune garantie que vos données soient déchiffrées. Certains cryptovirus contiennent des bugs logiciels qui peuvent provoquer leur dysfonctionnement, de sorte que le processus de déchiffrement échoue. Dans d'autres cas, le criminel peut tout simplement ne jamais avoir eu l'intention de permettre le déchiffrement. Au lieu de cela, il prend simplement l'argent des victimes.

Selon un sondage mené par le Centre de Recherche Interdisciplinaire sur la cyber-sécurité de l'Université de Kent, en février 2014, **plus de 40 %** des victimes de cryptolocker ont accepté de payer la rançon.

« Un cryptovirus moderne effectuera souvent un certain nombre d'actions supplémentaires qui empêcheront la récupération des données chiffrées, y compris la suppression ou le chiffrement des copies masquées utilisées pour stocker les points de restauration système et les sauvegardes Windows régulières. »

Andrey Pozhogin, Cybersecurity Expert, Kaspersky Lab

Des frais encore plus élevés pour les entreprises

Bien que les criminels exigent souvent des paiements plus importants des entreprises victimes, la rançon ne pourrait représenter qu'une petite partie des coûts totaux de l'entreprise. La nuisance de cette attaque peut entraîner des pertes financières beaucoup plus importantes.

À l'heure de « l'ère de l'information », toute perte temporaire de données peut totalement perturber les processus essentiels de l'entreprise, entraînant :

- **Un impact sur les ventes**
- **Une diminution de la productivité**
- **Des coûts importants pour la récupération du système**

Par ailleurs, la perte permanente de données peut avoir des conséquences encore plus graves :

- Nuire de façon permanente à la position concurrentielle de l'entreprise
- Réduire les recettes de ventes à long terme
- Empêcher l'accès permanent à la propriété intellectuelle et aux données de conception

... et même mettre en péril l'ensemble de l'entreprise.

Imaginez perdre accès à tous vos registres de ventes, aux dossiers des clients, aux données comptables, aux informations produits et aux données de conception. Comment votre entreprise pourrait-elle faire face à cela et, si elle y fait face, quel montant de chiffre d'affaires perdriez-vous pendant que votre équipe tente de tout remettre sur la bonne voie ?

Il est clair que chaque entreprise doit faire tout son possible pour éviter de devenir une autre victime d'une attaque de cryptovirus.

Si votre entreprise est attaquée, méfiez-vous des « faux remèdes » qui peuvent être promus sur Internet, car ils pourraient seulement s'ajouter à vos problèmes :

1

Souvent, ils ne fonctionnent pas, mais prennent juste plus d'argent à la victime

2

Certains peuvent même télécharger d'autres programmes malveillants sur le réseau de la victime

Il y a plus d'attaques de cryptovirus que jamais

Parce que c'est relativement peu coûteux d'élaborer et de lancer un cryptovirus, et qu'un seul élément de crypto-malware peut générer un chiffre d'affaires important, le nombre d'attaques augmente.

Voici quelques exemples de récents cryptovirus :

CoinVault : utilise l'algorithme AES à 256 bits pour chiffrer les fichiers des victimes

CryptoLocker : a infecté des dizaines de milliers de machines et généré des millions de dollars pour les criminels

CryptoWall : double souvent la demande de rançon si le paiement n'est pas effectué dans le délai initial

TorLocker : chiffre les données et utilise le réseau Tor pour contacter les criminels qui ont lancé l'attaque

Durant les six premiers mois de l'année 2015, le nombre de crypto-attaques égalait le volume connu pour l'ensemble de l'année 2014.

Source : Kaspersky Security Network

En dépit de l'augmentation des attaques de ransomwares, une récente étude a révélé que seulement **40 %** des entreprises considéraient le ransomware comme un danger sérieux.

De toute évidence, cette attitude peut mener à des faiblesses en matière de sécurité, qui pourront être exploitées par les cyber-criminels.

Source : Global IT Risks Survey 2015 de Kaspersky Lab

Comment attaque un cryptovirus

Comme la plupart des autres types de programmes malveillants, il existe de nombreuses façons permettant à un cryptovirus d'accéder à des ordinateurs et autres appareils.

Toutefois, deux des moyens les plus courants sont :

- **Les courriers indésirables de phishing** : quand la victime reçoit un e-mail contenant une pièce jointe infectée ou un lien vers un site Web de phishing.
- **L'attaque de type «watering hole» (point d'eau)** : lorsque l'on visite un site Web légitime qui est populaire, avec un type spécifique d'utilisateur ou de poste (comme un forum de comptabilité ou un site de conseils pour entreprise), cela peut entraîner l'infection de l'appareil de l'employé. Dans ces cas d'infection « par simple passage », le site Web aura déjà été infecté par un programme malveillant qui est prêt à exploiter les vulnérabilités se trouvant sur les appareils des visiteurs.

Ce qu'il attaque

Il est utile de rappeler qu'un cryptovirus peut attaquer une large gamme d'appareils, y compris :

- PC
- Mac
- Tablettes et smartphones Android
- Environnement de machines virtuelles (VDI)

En outre, si l'appareil attaqué est également relié à un lecteur réseau (qui permet le partage de fichiers d'entreprise), les fichiers partagés sont également susceptibles d'être chiffrés par le cryptovirus... quel que soit le système d'exploitation sous lequel le serveur de fichiers fonctionne.

Malheureusement, quel que soit l'appareil attaqué, les droits d'administration ne sont pas requis pour la plupart des actions malveillantes que les cryptovirus effectuent.

Les cryptovirus d'aujourd'hui sont plus dangereux

Lorsque les premiers cryptovirus ont été déployés, il était souvent possible de contrer leurs effets.

Parfois la clé de déchiffrement était en fait cachée dans l'appareil infecté. Ainsi, la correction consistait simplement à trouver la clé, puis à l'utiliser pour déverrouiller les données. Pour certaines autres attaques, des spécialistes en sécurité informatique pouvaient pratiquer l'ingénierie inverse sur le programme malveillant et trouver des moyens pour déchiffrer les données.

Toutefois, aujourd'hui, les cyber-criminels ne font plus d'erreurs basiques. Ils utilisent également des techniques beaucoup plus complexes, sur lesquelles il peut être extrêmement difficile de pratiquer l'ingénierie inverse. De plus, même dans les cas où l'ingénierie inverse est possible, il est peu probable que la clé de déchiffrement soit présente sur l'appareil attaqué.

La majorité des cryptovirus génère désormais aussi une clé de déchiffrement unique pour chaque appareil attaqué. Ainsi, même si vous parvenez à accéder à une clé de déchiffrement, cela ne vous aidera pas à déchiffrer des fichiers sur d'autres appareils.

Ces techniques, ainsi que des schémas de chiffrement de plus en plus sophistiqués, comprennent :

- **La méthode RSA / AES combinés**, qui permet une grande vitesse de chiffrement de données, à l'aide de l'algorithme AES, et qui chiffre ensuite la clé AES avec le puissant algorithme RSA
- **Les algorithmes à courbes elliptiques**, qui permettent des niveaux de chiffrement encore plus élevés, tout en conservant la vitesse

Le déchiffrement des données est souvent impossible.

Cacher leurs traces

Les cyber-criminels qui lancent les cryptovirus consacrent aussi davantage de ressources pour frustrer les efforts des organismes d'application de la loi. Ainsi, il est de plus en plus difficile de localiser et de fermer des opérations cryptographiques modernes :

- Le paiement est généralement demandé en Bitcoin ou autres devises numériques, de sorte que sa trace n'est pas facile à suivre
- L'utilisation de l'anonymisation des mécanismes, comme le réseau Tor, fait qu'il est presque impossible de localiser les criminels

Comment protéger votre entreprise

Lorsqu'il s'agit de traiter le risque d'une attaque de cryptovirus, vous avez deux choix :

1. Espérer ne pas être attaqué, mais avec le nombre croissant de cryptovirus, ce n'est pas vraiment une option viable !

OU

2. Suivre certaines règles faciles à appliquer, afin de protéger vos données et vos opérations.

Formez vos utilisateurs
Les gens sont souvent l'élément le plus vulnérable dans toute entreprise. Apprenez à vos employés les bases de la sécurité informatique, notamment :

- La sensibilisation aux risques du phishing et du harponnage
- Les répercussions sur la sécurité de l'ouverture de toute pièce jointe d'e-mail paraissant suspect, même si, à première vue, il semble provenir d'une source fiable

Sauvegardez régulièrement les données et vérifiez la possibilité de restauration de vos sauvegardes
Presque toutes les entreprises auront déjà des politiques de sauvegarde des données. Toutefois, il est essentiel que vous sauvegardiez vos données sur un sous-système de sauvegarde hors ligne, au lieu de simplement copier les fichiers vers un autre système « actif » sur votre réseau d'entreprise... autrement un cryptovirus sera en mesure de chiffrer vos fichiers de sauvegarde.

Établissez une politique de « sauvegarde et déconnexion », de sorte que vous ne copiez pas simplement les données sur un serveur de fichiers connecté en permanence.

Protégez tous les appareils et systèmes
Parce que les cryptovirus ne se contentent pas d'attaquer les PC, vous devrez également vous assurer que votre logiciel de sécurité peut protéger vos ordinateurs Mac, les machines virtuelles et les appareils mobiles Android.

Il est également important de vous assurer d'avoir une bonne protection installée sur votre système de messagerie.

Déployez et mettez à jour votre logiciel de sécurité
Comme pour toutes les préventions contre les programmes malveillants, votre mot d'ordre devrait être « mettre à jour de façon rapidement et souvent»... ainsi vous :

- **mettez à jour toutes les applications et tous les systèmes d'exploitation** - pour éliminer les vulnérabilités nouvellement découvertes
- **mettez à jour l'application de sécurité et sa base de données de protection contre les programmes malveillants** - pour vous assurer de bénéficier de la protection la plus récente

Essayez de sélectionner une solution de sécurité qui comprend des outils qui vous permettent de :

- **Gérer l'utilisation d'Internet** - par exemple, en fonction du poste occupé
- **Contrôler l'accès aux données d'entreprise** - encore une fois, selon le poste ou le service
- **Gérer le lancement de programmes** - à l'aide de technologies de contrôle d'application qui vous aident à bloquer ou à autoriser des programmes

« Les cyber-criminels sont de plus en plus doués pour élaborer des ransomwares pouvant fonctionner sans être remarqués. De plus, ils ont de nombreux outils et techniques à leur disposition pour s'assurer que le ransomware n'est pas découvert par la victime. »

Andrey Pozhogin, Cybersecurity Expert, Kaspersky Lab

Choisissez une sécurité primée

Kaspersky Endpoint Security for Business offre une sécurité multi-niveaux pour vous aider à protéger votre entreprise contre les menaces connues, inconnues et avancées... y compris les cryptovirus.

Nous fournissons des mises à jour pour notre agent de sécurité et notre base de données de protection contre les programmes malveillants beaucoup plus souvent que la plupart des autres fournisseurs de solutions de sécurité. En outre, Kaspersky Endpoint Security for Business comprend des techniques proactives, heuristiques et comportementales, ainsi que des technologies assistées par le cloud, pour apporter une réponse extrêmement rapide à de nouvelles menaces.

Beaucoup de nos produits offrent également une foule d'outils et de technologies de sécurité supplémentaires.[1]

System Watcher[2] comprenant la technologie Crypto-Malware Countermeasures
System Watcher surveille le comportement de tous les programmes en cours d'exécution sur vos systèmes et compare le comportement de chaque programme aux modèles de comportement typique de programmes malveillants.

Si un comportement suspect est détecté, System Watcher met automatiquement le programme en quarantaine. Étant donné que System Watcher conserve un journal dynamique du système d'exploitation, de la base de registre et d'autres éléments, il permet d'annuler les actions malveillantes qui ont été mises en place avant que le programme malveillant n'ait été identifié.

En outre, System Watcher surveille en permanence l'accès à certains types de fichiers, y compris aux documents Microsoft Office, et conserve temporairement des copies si ces fichiers sont consultés. Si System Watcher détecte que c'est un processus suspect, comme un cryptovirus, qui a accédé aux dossiers, les « sauvegardes » temporaires peuvent être utilisées pour restaurer les fichiers dans leur forme non chiffrée. Bien que les sauvegardes temporaires générées par System Watcher ne soient pas destinées à remplacer l'exécution d'une stratégie de sauvegarde complète des données, elles peuvent être utiles pour vous aider à vous protéger contre les effets d'une attaque de cryptovirus.

Fonctionnant conjointement avec System Watcher, Application Privilege Control permet également aux administrateurs de limiter les ressources système essentielles auxquelles les applications sont autorisées à accéder, y compris l'accès de bas niveau au disque.

Évaluation des vulnérabilités et gestion des correctifs[3]
Les vulnérabilités, ou bugs, dans toutes les applications et les systèmes d'exploitation fonctionnant sur vos appareils, peuvent fournir des points d'entrée aux attaques de programmes malveillants... y compris aux cryptovirus.

Notre outil automatisé d'évaluation des vulnérabilités et de gestion des correctifs peut analyser vos systèmes, identifier des vulnérabilités connues et vous aider à distribuer les correctifs et les mises à jour nécessaires. Ainsi, les vulnérabilités connues peuvent être éliminées.

Prévention automatique de l'exploitation des failles (AEP)[4]
Notre technologie AEP contribue également à empêcher les programmes malveillants d'exploiter les failles dans des applications et des systèmes d'exploitation. Elle surveille plus particulièrement les applications ciblées le plus fréquemment, comme par exemple Adobe Reader, Internet Explorer, Microsoft Office et Java, pour offrir une couche de sécurité puissante et supplémentaire.

Les experts en sécurité sont parfois en mesure de déceler une vulnérabilité dans un cryptovirus, puis d'exploiter cette faille afin d'aider les victimes à récupérer leurs fichiers.

Kaspersky Lab a récemment établi un partenariat avec le National High Tech Crime Unit (NHTCU) de la police néerlandaise afin de créer un répertoire de clés de déchiffrement et une application de déchiffrement pour les victimes de CoinVault.

1 : Les fonctionnalités de sécurité varient selon les différents types de système / plate-forme. Pour obtenir plus de d'informations, veuillez consulter www.kaspersky.fr/business
2 : System Watcher est disponible dans Kaspersky Endpoint Security for Business (tous niveaux) et KSV|Light Agent. Systèmes d'exploitation Windows Workstation uniquement, les plates-formes de serveur ne sont pas supportées. Non disponible pour les appareils Mac et Android.
3 : L'évaluation des vulnérabilités et la gestion des correctifs sont incluses dans Kaspersky Total Security for Business, Kaspersky Endpoint Security for Business Advanced et Kaspersky Systems Management.
4 : AEP est disponible dans Kaspersky Endpoint Security for Business (tous niveaux) et KSV|Light Agent. Systèmes d'exploitation Windows Workstation uniquement, les plates-formes de serveur ne sont pas supportées. Non disponible pour les appareils Mac et Android.

Contrôle des applications et liste blanche
Les outils de contrôle des applications flexibles et la liste blanche dynamique vous permettent d'autoriser ou d'empêcher facilement le lancement de programmes. En plus de bloquer les programmes inscrits sur la liste noire, vous pouvez choisir d'appliquer une politique de blocage par défaut pour certains de vos postes de travail et serveurs, de sorte que seules les applications qui sont sur votre liste blanche sont autorisées à fonctionner... et cela signifie que les cryptovirus seront automatiquement bloqués.

Contrôle Web
Des outils faciles à utiliser vous permettent de définir des politiques d'accès à Internet et de surveiller l'utilisation d'Internet. Vous pouvez interdire, autoriser ou vérifier les activités des utilisateurs sur des sites Web particuliers ou des catégories de sites, tels que des réseaux sociaux, des sites de jeu. Il y a ainsi moins de probabilité pour que des utilisateurs visitent un site Web ayant été infecté par un cryptovirus.

Protection contre le phishing
Notre moteur anti-phishing assisté par cloud permet d'empêcher vos employés de devenir des victimes de campagnes de phishing et de harponnage qui peuvent mener à des infections par cryptovirus.

Sécurité du système de messagerie
Kaspersky Security for Mail Server analyse les courriers entrants, sortants et conservés, sur les serveurs de messagerie Microsoft Exchange, Linux Mail et Lotus Domino.

Notre moteur avancé de protection contre les courriers indésirables, assisté par le cloud, et notre moteur anti-phishing vous aident à éliminer les distractions et à vous protéger contre les cryptovirus et autres menaces.

Nous vous aidons à protéger tous vos terminaux[1]... et plus encore
Nous avons des solutions pour protéger une large gamme de terminaux :

- PC
- Mac
- Serveurs de fichiers
- Téléphones portables et tablettes
- Serveurs virtuels
- Environnement de machines virtuelles (VDI)

ainsi que les passerelles Internet et les systèmes de collaboration.

1 : Les fonctionnalités de sécurité varient selon les différents types de système / plate-forme. Pour obtenir plus de d'informations, veuillez consulter www.kaspersky.fr/business

PRENEZ DES MESURES SANS PLUS ATTENDRE : ESSAI GRATUIT DE 30 JOURS

Découvrez comment nos solutions de sécurité peuvent protéger votre entreprise des programmes malveillants et de la cyber-criminalité en les essayant gratuitement pendant un mois.

Rendez-vous dès aujourd'hui sur **http://www.kaspersky.fr/downloads/trials/business-trials** pour télécharger des versions complètes de nos produits et évaluer leur capacité à protéger parfaitement votre infrastructure informatique, vos terminaux et les données confidentielles de votre entreprise.

EFFECTUEZ UN ESSAI GRATUIT DÈS MAINTENANT

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

#SecureBiz

Visionnez nos vidéos sur YouTube

Rejoignez nos fans sur Facebook

Suivez-nous sur Twitter

Retrouvez-nous sur LinkedIn

Découvrez nos présentations sur Slideshare

Découvrez notre blog

Rejoignez-nous sur Threatpost

Retrouvez-nous sur Securelist

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est une des entreprises de cyber-sécurité du monde connaissant la croissance la plus rapide. C'est aussi la plus grande société privée du secteur. Elle fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité informatique (IDC, 2014). Depuis 1997, Kaspersky Lab a été pionnière en matière de cyber-sécurité. Elle offre des solutions de sécurité numériques efficaces et une surveillance des menaces pour les grandes entreprises, les PME et les consommateurs. Kaspersky Lab est une société internationale et est actuellement présente dans près de 200 pays et territoires à travers le monde, où elle apporte une protection à plus de 400 millions d'utilisateurs.

kaspersky.fr/business
kaspersky.fr/entreprise-securite-it
#SecureBiz