MINI GUIDE KASPERSKY LAB
Sensibilisation des collaborateurs à la sécurité informatique

N°1
SE PROTÉGER DES RANSOMWARES

Comment reconnaître et éviter
les attaques de ransomwares

KASPERSKY lab

Sommaire

1. Qu'est-ce qu'un ransomware ?

Un logiciel malveillant qui vous prend en otage

Un ransomware (ou rançongiciel, ou cryptovirus) est un logiciel malveillant qui verrouille votre écran ou chiffre l'ordinateur et/ou les fichiers d'un utilisateur et demande une rançon pour libérer l'accès aux données. Il est souvent transmis par des emails contenant des pièces jointes dangereuses ou des liens frauduleux, des plugins de navigateur obsolètes, des sites Internet, etc.

Certains pirates informatiques dérobent également des données sensibles (par ex., des données financières d'une société d'investissement) et menacent de les divulguer publiquement à moins de recevoir une rançon.

Et qui s'attaque à votre argent ou vos données

Il peut s'attaquer à tout le réseau d'ordinateurs, de disques durs externes, d'appareils USB et de serveurs Internet.

Contrairement à d'autres virus qui cherchent à altérer vos fichiers ou systèmes, un ransomware kidnappe généralement vos fichiers (des informations relatives à vos clients pour une entreprise, vos photos de famille pour un particulier...) contre une demande de rançon anonyme.

Sa réussite repose sur sa conception

Les cybercriminels ne sont pas obligés de respecter leur part du marché et de vous donner la clé si vous payez la rançon. En cas de défaut dans le code du ransomware, vos données peuvent être irrécupérables et ce, de manière permanente, même si vous avez la clé de déchiffrement. Les fichiers peuvent également ne pas fonctionner de la bonne façon après le déchiffrement. Et le pire : vous pourriez également être visé à nouveau à l'avenir.

À quoi ressemble un ransomware ?

Une fois que des fichiers sont chiffrés, des instructions apparaissent sur votre écran, demandant le paiement d'une somme en général en bitcoins en échange de la clé de déchiffrement. Les instructions peuvent apparaitre comme un document texte ou un graphique sur votre bureau d'ordinateur ou une page Internet sur votre navigateur.

Le chiffrement est si fort que, selon les estimations, un ordinateur de bureau standard aurait besoin de 4,6 quadrillions d'années pour le déchiffrer

2. Qui et quoi peut-être visé par un ransomware ?

Un ransomware peut toucher n'importe qui : de grandes entreprises, de petites sociétés, des hôpitaux, des écoles/universités ou des particuliers.

Il peut infecter tous les ordinateurs, les serveurs de fichiers, les tablettes et les smartphones. Un ransomware peut impacter votre appareil de stockage USB ou votre disque dur externe.

Un ransomware peut s'emparer de tout ce qui se connecte à Internet.

Exemple 1. Un service de police bloqué par un ransomware

Prenons l'exemple réel d'un service de police qui a été infecté. Dans un premier temps, les difficultés pour retrouver des fichiers d'incidents et d'arrestations ont été considérées comme des problèmes techniques normaux. Rien de bien inquiétant.

Les problèmes ont persisté et le service de police a fait appel à un technicien. Leurs dernières sauvegardes sur un disque dur externe étaient altérées et la dernière sauvegarde exploitable datait de 18 mois.

Il a fallu plusieurs jours pour réaliser qu'ils avaient été infectés par un ransomware qui bloquait tout accès à moins de payer une forte somme avant une certaine date.

Étant donné que les ordinateurs du service de police ont des lecteurs mappés et sont connectés sur un réseau, le ransomware a chiffré un important serveur contenant la gestion des dossiers, les registres des arrestations, les demandes de services, les dossiers relatifs aux véhicules motorisés, etc.
Le problème a finalement été résolu avec l'aide des autorités fédérales américaines et de sociétés de sécurité du secteur privé. 'Je peux vous dire que cette expérience nous a ouvert les yeux. On avait l'impression de ne plus rien contrôler du tout', dit le chef de la police.

Exemple 2. Un géant de la santé touché par un ransomware

Cela a commencé lorsque quelques employés ont vu d'étranges messages demandant de l'argent s'afficher sur leurs écrans. Lorsque le nombre de signalements a augmenté, le FBI a commencé à enquêter.
Le ransomware a obligé 10 hôpitaux du géant de la santé et plus de 250 cliniques ambulatoires à éteindre tous leurs ordinateurs. Certains patients n'ont pas pu être soignés ou ont été soignés sans qu'on puisse accéder à leur dossier numérique tandis que la société travaillait jour et nuit pour restaurer le système.

Les problèmes étaient très sérieux. La peur partagée par les 30 000 employés de la société était le risque d'erreur médicale.

Rien ne prouvait que les dossiers avaient été dérobés, mais les retards que le logiciel malveillant avaient entrainés ont coûté beaucoup d'argent à la société.

3. Comment se protéger des ransomwares ?

Méthodes courantes d'infection par ransomware

La principale méthode est l'infection par email

Un ransomware peut se propager de la même manière que les virus d'ordinateurs traditionnels : par des spams et des pièces jointes dans des emails.
Un cybercriminel peut envoyer un email de masse avec une pièce jointe malveillante déguisée en facture, pdf ou fichier ZIP, mais il peut s'agir d'un fichier exécutable.
Certains emails sont plus sophistiqués : ils utilisent le nom de la personne visée ainsi que d'autres détails personnels pour leur donner l'air d'être des emails sûrs. Si vous les ouvrez, le système est menacé par le ransomware.

Logiciel piraté ou gratuit

Un ransomware peut être transmis par des versions piratées de logiciels connus, de jeux gratuits, d'écrans de veille gratuits.

Navigation sur Internet

Un logiciel malveillant peut venir de publicités, de vidéos, de fenêtres pop-ups ou de plugins de navigateur qui tentent d'exploiter des navigateurs obsolètes ou des logiciels vulnérables sur l'ordinateur d'un utilisateur.
Il peut se télécharger à partir de liens sur des réseaux sociaux ou de sites Internet pour adultes.
Les cybercriminels peuvent élaborer des fenêtres pop-ups sur Internet pour qu'ils aient l'air de messages de menaces provenant d'autorités légales, demandant à l'utilisateur d'agir immédiatement. Cela s'appelle un rogue.

Sites Internet compromis ou malveillants

Les ransomwares ne se propagent pas uniquement par email. Des sites Internet légitimes peuvent être piratés par des cybercriminels, il suffit dans ce cas, de visiter la page pour se faire infecter.

La prévention est le meilleur des remparts

La protection et la formation des utilisateurs sont les clés pour éviter les ransomwares.

Utilisation d'emails

Faites attention lorsque vous ouvrez un email. Vérifiez l'authenticité de l'expéditeur ainsi que le contenu de l'email, comme les pièces jointes et les liens.

Contactez votre service informatique pour savoir comment ouvrir en toute sécurité les pièces jointes inconnues et inattendues.

Navigation sur Internet

Désactivez les fenêtres pop-ups dans les paramètres de votre navigateur Internet. Désactivez les plugins de navigateur ou paramétrez votre navigateur de manière à ce qu'il vous demande avant d'exécuter un plugin. Cela s'appelle en général click-to-run (cliquer pour exécuter). Mettez à jour les plugins comme Java, Flash et Adobe Reader.

Faites des sauvegardes et soyez prêt

Faites régulièrement des sauvegardes des fichiers stockés sur votre ordinateur, votre tablette et votre smartphone.
Rapprochez-vous de votre service informatique pour savoir comment sauvegarder et protéger vos fichiers les plus importants.
Si votre machine est infectée par un logiciel malveillant, ces sauvegardes pourront être utilisées pour restaurer votre système. Si vous faites vos propres sauvegardes, déconnectez votre disque dur externe après chaque sauvegarde manuelle.

Mises à jour de logiciels

Mettez à jour tous vos logiciels, comme votre antivirus.
N'oubliez pas que tous les antivirus ne peuvent pas détecter tous les types de virus ou de ransomware.
Les opérateurs de ransomwares profitent des logiciels obsolètes en modifiant constamment le code du ransomware pour qu'il ne soit jamais détecté.

Le vrai coût est celui du temps d'arrêt

En cas d'infection par un ransomware, ce qui compte c'est la rapidité avec laquelle les employés peuvent recommencer à travailler. Une infection peut bloquer plusieurs services d'un seul coup. Cela peut prendre des semaines de travail pour récupérer les fichiers perdus, et encore plus de temps si les ordinateurs doivent être nettoyés et rechargés. Un ransomware peut également impacter le niveau de satisfaction des clients.

4. Comment savoir si mon ordinateur est infecté ?

Voici certaines des caractéristiques :

- Vous ne pouvez tout d'un coup plus ouvrir les fichiers alors que vous le pouviez auparavant
- Des messages d'erreur apparaissent, indiquant que votre fichier est altéré, ne peut pas être trouvé ou n'a pas la bonne extension
- Vous pouvez voir une fenêtre affichant un décompte de paiement, un programme ou des instructions de demande de rançon
- Des fichiers que vous n'avez pas créés ou ajoutés apparaissent sur votre bureau et ressemblent à des demandes de rançon

Si vous pensez que vous êtes infecté…
ne perdez pas espoir, mais agissez rapidement

Le chiffrement prend beaucoup de temps. Si vous pensez que vos fichiers sont en train d'être chiffrés par un ransomware :

1. Déconnectez-vous immédiatement de tout réseau.
2. Appuyez sur le bouton d'extinction de votre ordinateur de bureau. Si vous utilisez un ordinateur portable, appuyez sur le bouton d'extinction jusqu'à ce qu'il s'éteigne. Si vous utilisez un smartphone, éteignez-le.
3. Appelez le service informatique ou le service d'assistance de votre société pour obtenir de l'aide. Ne vous en occupez pas tout seul.

Pour en savoir plus :

https://kas.pr/Minisite_Ransomware

ou *www.kaspersky.fr*

REJOIGNEZ-NOUS

Regardez-nous sur YouTube

Aimez notre page sur Facebook

Consultez notre blog

Suivez-nous sur Twitter

Rejoignez-nous sur LinkedIn

Pour en savoir plus :
http://www.kaspersky.fr/enterprise-security/

KASPERSKY lab