SOPHOS
Security made simple.

COMMENT S'EN PROTÉGER

Toutes les entreprises, qu'elles soient petites ou grandes, sont sous la menace d'attaques de ransomware toujours plus agressives et brutales. Les performances d'une entreprise peuvent être perturbées de manière significative si des fichiers critiques ne sont plus accessibles.

Mais à quoi ressemble une attaque type ? Quelles solutions de sécurité devraient être en place pour une défense maximale ?

Ce livre blanc explore les techniques les plus couramment utilisées pour distribuer les ransomwares, analyse pourquoi ces attaques ont un tel succès et recommande neuf conseils de sécurité pour vous aider à rester protégé. Il met également en lumière les technologies de sécurité indispensables que toute stratégie de sécurité informatique devrait inclure.

Livre blanc Sophos Août 2016

Ransomwares - une brève introduction

Les ransomwares sont l'une des menaces les plus répandues et les plus nocives auxquelles les internautes sont confrontés. Depuis le premier et fameux Cryptolocker en 2013, on assiste à l'apparition de nouvelles variantes de ransomwares distribués via les messages de spam et les kits d'exploits, dont l'objectif est d'extorquer de l'argent aux particuliers et aux entreprises.

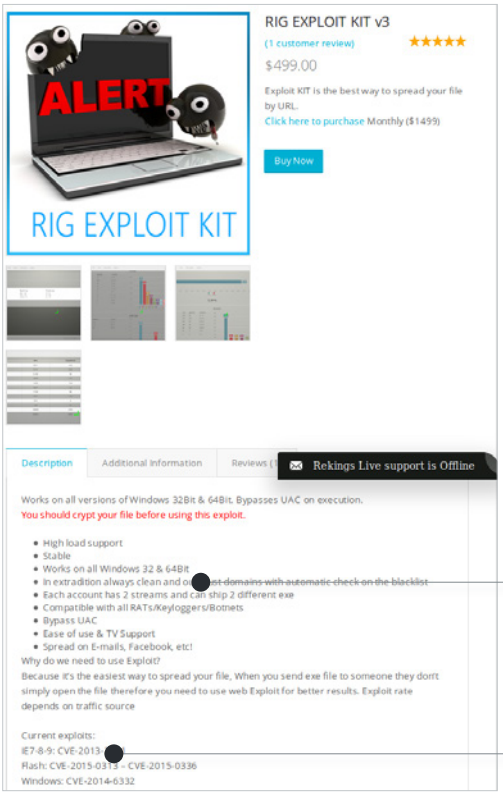
L'origine des différentes familles de ransomwares actuelles peut remonter aux premiers jours de Fake AV (faux antivirus), en passant par des variantes de « Locker » ou des variantes de chiffrement de fichiers qui prévalent aujourd'hui. Cela dit, chaque catégorie de malwares partage un objectif commun : extorquer de l'argent aux victimes grâce à l'ingénierie sociale et à l'intimidation pure et simple. Et les sommes exigées augmentent en force à chaque itération.

Les conséquences financières peuvent être dramatiques. Aux États-Unis, le Hollywood Presbyterian Medical Center a révélé avoir payé 40 bitcoins (17 000 dollars au moment du paiement) pour récupérer l'accès à ses fichiers, tandis que le Kansas Heart Hospital, moins chanceux, n'a jamais pu récupérer ses fichiers malgré le paiement d'une première rançon.

Pourquoi les attaques de ransomwares rencontrent-elles un tel succès ?

La plupart des entreprises ont mis en place un minimum en terme de sécurité informatique. Alors pourquoi les attaques de ransomwares passent-elles à travers les mailles du filet ?

1. **Techniques d'attaque sophistiquées et innovation continue**
   - Même les criminels les moins qualifiés peuvent accéder de plus en plus facilement à des programmes prêts à l'emploi 'Malware as a Service' (MaaS) simplifiant ainsi le lancement d'une attaque, sa réussite complète et ses retombées financières. L'image ci-dessous montre un exemple d'annonce pour un programme MaaS.



Comprend des techniques pour les réseaux et les systèmes d'extrémité : de l'infection d'un site Internet, jusqu'à l'administration d'une charge virale dans le système d'extrémité et la vente des résultats.

Multiplateformes et développement Agile.

Exploits inclus automatiquement.

- Ils utilisent intelligemment l'ingénierie sociale pour demander à l'utilisateur de lancer la procédure d'installation du ransomware. Par exemple, vous pouvez recevoir un email énonçant quelque chose comme :
  « Les demandes de mon entreprise sont dans le fichier en pièce jointe, merci de me faire parvenir un devis. »
- Les créateurs de ransomwares opèrent de manière très professionnelle. Ils fournissent un véritable outil de déchiffrement après le paiement de la rançon (mais il n'y a aucune garantie).

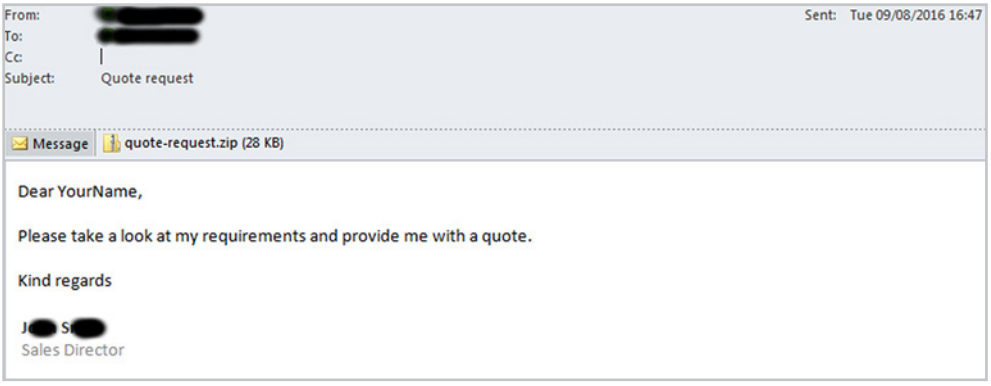
2. **Failles de sécurité dans les entreprises affectées**
   - Stratégie de sauvegarde insuffisante (pas de sauvegarde en temps réel, pas de sauvegarde hors ligne/hors site).
   - Les mises à jour et correctifs pour le système d'exploitation et les applications ne sont pas mis en œuvre assez rapidement.
   - Autorisations des droits/utilisateurs dangereuses (les utilisateurs travaillent comme administrateurs et/ou ont davantage de droits d'accès aux fichiers sur les lecteurs réseau que nécessaire pour accomplir leur travail).
   - Manque de formation à la sécurité auprès des utilisateurs (« Quels documents puis-je ouvrir et provenant de qui ? », « Quelle est la procédure à suivre si un document semble malveillant ? », « Comment puis-je reconnaître un email de phishing ? »).
   - Les systèmes de sécurité (antivirus, pare-feu, IPS, passerelles email/Web) ne sont pas actifs ou ne sont pas configurés correctement. La segmentation inadéquate du réseau peut également être incluse ici (serveurs et postes de travail sur le même réseau).
   - Manque de connaissances dans le domaine de la sécurité informatique (les fichiers .exe peuvent être bloqués dans les emails sans empêcher les macros Office ou tout autre contenu actif).
   - Conflits de priorités (« Nous savons que cette méthode n'est pas sûre, mais nos employés doivent travailler… »).
3. **Manque de technologies de prévention avancées**
   - De nombreuses entreprises disposent uniquement d'une protection de base.
   - Les ransomwares sont constamment mis à jour pour exploiter et éviter cette protection.
     Par exemple, ils s'auto-suppriment très rapidement après avoir chiffré les fichiers, pour qu'ils ne puissent pas être analysés.
   - Les solutions doivent être conçues spécifiquement pour lutter contre les techniques de ransomwares.

Comment se déroule une attaque de ransomware ?

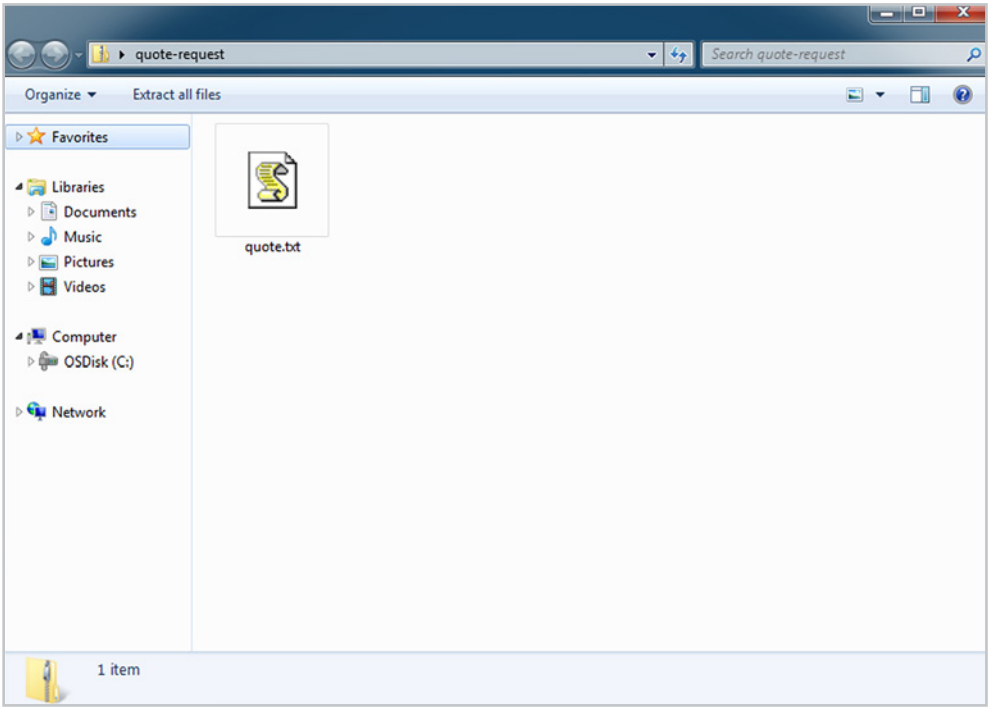
Les attaques de ransomware se produisent de deux manières principales : via un email contenant une pièce jointe malveillante ou via un site Web compromis (souvent légitime, grand public).

Email malveillant

Les criminels d'aujourd'hui créent des emails qui ressemblent en tous points à des emails légitimes. Il sont souvent bien écrits, sans fautes d'orthographe ni de grammaire, avec un style d'écriture que vous pourriez utiliser dans votre entreprise.



Une fois ouvert, le fichier .zip semble contenir un fichier .txt ordinaire.



Pourtant, une fois le fichier exécuté, le ransomware va être téléchargé et installé sur votre ordinateur. Dans cet exemple, le cheval de Troie est en fait un fichier JavaScript déguisé en fichier .txt, mais il existe de nombreuses autres variantes comme un document Word avec des macros ou les fichiers raccourcis .lnk.

Sites Web malveillants

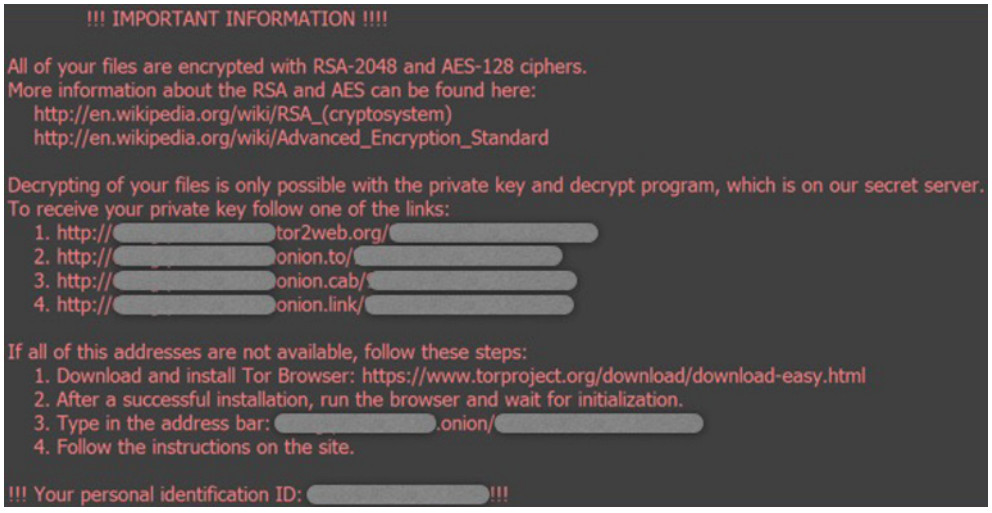
Un autre moyen de se retrouver infecté par un malware est de visiter un site Web légitime qui a lui-même été infecté par un kit d'exploit. Même les sites Web les plus importants peuvent être temporairement compromis. Les kits d'exploit sont des outils issus du marché noir que les pirates utilisent pour exploiter les vulnérabilités connues ou inconnues (tels que les exploits zero-day).

Vous naviguez alors sur le site Web piraté et cliquez sur un lien d'apparence légitime, passez votre souris au-dessus d'une publicité ou bien regardez simplement la page. Et cela suffit pour télécharger le ransomware sur votre ordinateur et le lancer, et bien souvent vous ne vous en rendez compte qu'une fois qu'il est trop tard.

Que se passe-t-il ensuite ?

Après l'exposition initiale via un email ou un site Web, le ransomware se met en action :

- Il contacte le serveur de Commande et de Contrôle de l'attaquant pour envoyer des informations sur l'ordinateur infecté et télécharger une clé publique de chiffrement individuelle pour cet ordinateur.
- Les types de fichiers spécifiques (qui varient selon les types de ransomwares) comme les documents Microsoft Office, les fichiers de base de données, les fichiers PDF, les documents CAD, HTML, XML, etc. sont alors chiffrés sur l'ordinateur local, les périphériques et sur tous les lecteurs réseau accessibles.
- Les sauvegardes automatiques du système d'exploitation Windows (copies masquées) sont souvent supprimées pour éviter la récupération de données.
- Un message apparaît ensuite sur le bureau expliquant la démarche à suivre pour payer la rançon (généralement en Bitcoins) dans le temps imparti.



- Pour finir, le ransomware s'auto-supprime, laissant les fichiers chiffrés et les notes de rançon derrière lui.

Neuf bonnes pratiques de sécurité à appliquer maintenant

Se protéger contre les ransomwares ne consiste pas uniquement à installer les dernières solutions de sécurité. De bonnes pratiques de sécurité informatique sont indispensables dans toute stratégie de sécurité. Suivez ces neuf bonnes pratiques :

1. **Sauvegardez régulièrement et conservez une copie de sauvegarde récente hors ligne et hors site**

Il existe de multiples raisons - autres que les ransomwares - pouvant être à l'origine de la disparition d'un fichier : un incendie, une inondation, un vol, un ordinateur portable qui tombe en panne ou encore une suppression accidentelle. En chiffrant votre sauvegarde, vous n'aurez plus à vous inquiéter du fait que le système de sauvegarde tombe entre de mauvaises mains.

2. **Affichez l'extension des fichiers**

Windows cache par défaut l'extension des fichiers, ce qui signifie que vous devez vous fier à l'icône du fichier pour être en mesure de l'identifier. Afficher les extensions permet de détecter plus facilement les types de fichiers que vous et vos utilisateurs n'avez pas l'habitude de recevoir, tels que le JavaScript.

3. **Ouvrez les fichiers JavaScript (.JS) dans Notepad**

Ouvrir un fichier JavaScript dans Notepad l'empêche d'exécuter un script malveillant et vous permet d'examiner son contenu.

4. **N'activez pas les macros des pièces jointes reçues par email**

Microsoft a délibérément désactivé l'auto-exécution de macros par défaut il y a plusieurs années comme mesure de sécurité. Un grand nombre d'infections consistent à vous persuader d'activer les macros, alors ne le faites pas !

5. **Soyez prudent avec les pièces jointes non sollicitées**

Les pirates comptent sur le dilemme qui consiste à ne pas ouvrir un document avant d'être sûr qu'il soit légitime, mais comment le savoir si on ne l'ouvre pas.... En cas de doute, abstenez-vous.

6. **Ne vous autorisez pas plus de privilèges que nécessaire.**

Ne restez pas connecté en tant qu'administrateur plus longtemps que ce dont vous avez strictement besoin, et évitez la navigation, l'ouverture de documents ou autres activités de « travail régulier » alors que vous avez des droits d'administrateur.

7. **Envisagez d'installer les visionneuses Microsoft Office**

Ces applications de visualisation vous permettent de voir à quoi ressemblent les documents sans avoir à les ouvrir dans Word ou Excel. En particulier, les visionneuses ne prennent pas en charge les macros, donc vous ne pouvez pas les activer par erreur !

8. **Mettez à jour les correctifs régulièrement et souvent**

Les malwares qui ne sont pas distribués via les documents recherchent souvent des failles dans les applications courantes telles que Microsoft Office, votre navigateur Web ou encore Flash. Plus tôt vous installerez les correctifs, moins il y aura de vulnérabilités à exploiter.

9. **Restez informé des dernières fonctionnalités de sécurité mises en œuvre dans vos applications professionnelles**

Par exemple, Office 2016 contient la commande « Bloquer l'exécution des macros dans les fichiers Office provenant d'Internet » qui vous protège contre les contenus malveillants externes tout en vous permettant d'utiliser des macros internes.

Technologies de protection qui vous aident à rester protégé contre les ransomwares

Pour rester protégé, vous avez besoin d'une protection efficace pour contrer *chaque* étape d'une attaque de ransomware. La technologie unique CryptoGuard, disponible dans Sophos Intercept X, vous permet de bloquer les ransomwares dès leur première apparition sur le système d'extrémité. CryptoGuard intervient sur vos systèmes et vos serveurs, en détectant et bloquant les ransomwares cherchant à chiffrer vos fichiers. Il complète votre solution de sécurité traditionnelle en place, en bloquant les processus qui essaient de modifier vos données sans autorisation.

Stopper les menaces diffusées par email

La meilleure défense contre les emails piégés est votre passerelle de messagerie. Les technologies anti-spam bloquent les emails contenant des ransomwares, tandis que les antivirus analysent et bloquent les menaces transmises dans le corps de l'email. Bloquer les emails avec des pièces jointes contenant des macros peut vous aider à éviter cette technique habituelle de diffusion des ransomwares. La technologie Time-of-Click empêche les utilisateurs de cliquer sur des liens de sites Web infectés, même s'ils étaient sans danger au moment d'entrer dans votre boîte de réception.

Stopper les menaces Web

Les menaces issues du Web sont neutralisées au niveau du pare-feu et de la passerelle Web. Le filtrage des URL bloque les sites Web hébergeant des ransomwares et leurs serveurs de Commande et de Contrôle. En imposant également des contrôles stricts vous pouvez empêcher le téléchargement de fichiers liés aux ransomwares.

La technologie de sandboxing, fonctionnant au niveau de la passerelle de messagerie et de la passerelle Web, bloque les menaces avancées zero-day, dont les ransomwares. C'est comme avoir votre propre laboratoire de recherche sur les malwares, où le comportement des fichiers suspects est étudié.

Protéger vos serveurs

La mise sur liste blanche et le verrouillage des serveurs permet de sécuriser vos serveurs en autorisant uniquement les applications présentes sur la liste blanche et en identifiant ce qu'elles peuvent modifier et mettre à jour. Toutes les autres tentatives de modifications sont automatiquement bloquées, arrêtant net les ransomwares. La détection du trafic malveillant empêche les ransomwares de contacter leurs serveurs de Commande et de Contrôle et de télécharger leur charge virale.

Security Heartbeat

Chacun de vos produits de sécurité est excellent, mais ils fonctionnent encore mieux lorsqu'ils sont combinés ensemble.
En permettant à votre système d'extrémité et votre pare-feu de partager des information de sécurité et de répondre de manière proactive aux menaces, vous obtenez une protection inégalée contre les menaces avancées.

Avez-vous mis en place les meilleures pratiques de paramétrage pour vos solutions Sophos ?

www.sophos.com/kb/120797

Essayez-le gratuitement sur sophos.fr/free-trials

Plus de 100 millions d'utilisateurs dans 150 pays font confiance à Sophos pour leur fournir la meilleure protection du marché contre les menaces complexes et les fuites de données. Régulièrement primées, ses solutions intégrées de sécurisation et de protection des informations sont simples à déployer, à administrer et à utiliser, et offrent le coût global de possession le plus avantageux du marché. Sophos offre des solutions de chiffrement des données, de protection des systèmes d'extrémité, de sécurité du Web, de la messagerie, des mobiles, des serveurs et des réseaux, avec le support permanent des SophosLabs, notre réseau mondial de centres d'analyse des menaces. Pour en savoir plus, consultez notre page : www.sophos.fr/products.

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

08/09/2016 WP-FR (RP)