

COMMENT SE PROTÉGER DES RANSOMWARES

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.

Ransomwares - une brève introduction

Les ransomwares sont l'une des menaces les plus répandues et les plus nocives auxquelles les internautes sont confrontés. Depuis l'apparition du tristement célèbre Cryptolocker en 2013, on assiste à l'émergence 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 des Fake AV (faux antivirus), en passant par des variantes de « Locker » jusqu'aux 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. Et les sommes exigées augmentent en force à chaque itération.

Une enquête réalisée par Sophos auprès de 2 700 entreprises a démontré que 54 % des entreprises ont été touchées par un ransomware, en moyenne deux fois. Parmi celles touchées, 77 % possédaient un antivirus à jour au moment de l'attaque. Et les coûts sont foudroyants, avec un impact médian par entreprise estimé à 133k \$ (~100k €).

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

La plupart des entreprises disposent d'un minimum en terme de sécurité informatique. Alors pourquoi les attaques de ransomware 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, 'Exploit as a Service' (EaaS), 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 EaaS.

RIG EXPLOIT KIT v3
(1 customer review) ★★★★★
\$499.00
Exploit KIT is the best way to spread your file by URL.
[Click here to purchase Monthly \(\\$1499\)](#)
[Buy Now](#)

Description Additional information Reviews **Live support is Offline**

Works on all versions of Windows 32Bit & 64Bit. Bypasses UAC on execution.
You should crypt your file before using this exploit.

- High load support
- Stable
- Works on all Windows 32 & 64Bit
- In extradition always clean and our trust domains with automatic check on the blacklist
- Each account has 2 streams and can ship 2 different exe
- Compatible with all RATs/Keyloggers/Botnets
- Bypass UAC
- Ease of use & TV Support
- Spread on E-mails, Facebook, etc!

Why do we need to use Exploit?
Because it's the easiest way to spread your file. When you send exe file to someone they don't simply open the file therefore you need to use web Exploit for better results. Exploit rate depends on traffic source

Current exploits:
IE7-8-9: CVE-2013-2551
Rosh: CVE-2015-0313 - CVE-2015-0336
Windows: CVE-2014-6332

Comment se protéger contre les ransomwares ?

- 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 en général un outil de déchiffrement fonctionnel après le paiement de la rançon, mais sans aucune garantie.

2. Failles de sécurité dans les entreprises affectées

- Stratégie de sauvegarde insuffisante (pas de sauvegarde en temps réel, ni hors ligne/hors site).
- Les mises à jour et correctifs des systèmes d'exploitation et des applications ne sont pas appliqués 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 des utilisateurs (« Quels documents puis-je ouvrir et provenant de qui ? », « Quelle est la procédure à suivre si un document semble malveillant ? », « Comment 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 ne pas être analysés.
- Les solutions doivent être conçues spécifiquement pour lutter contre les techniques des ransomwares.

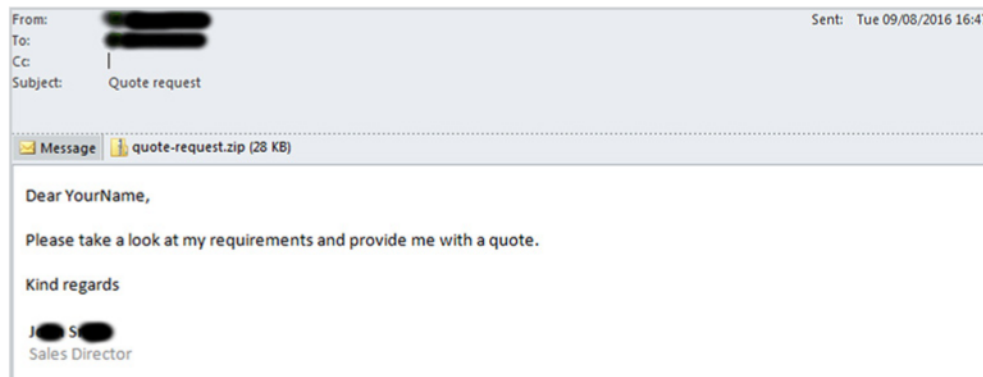
Comment se protéger contre les ransomwares ?

Comment se déroule une attaque de ransomware ?

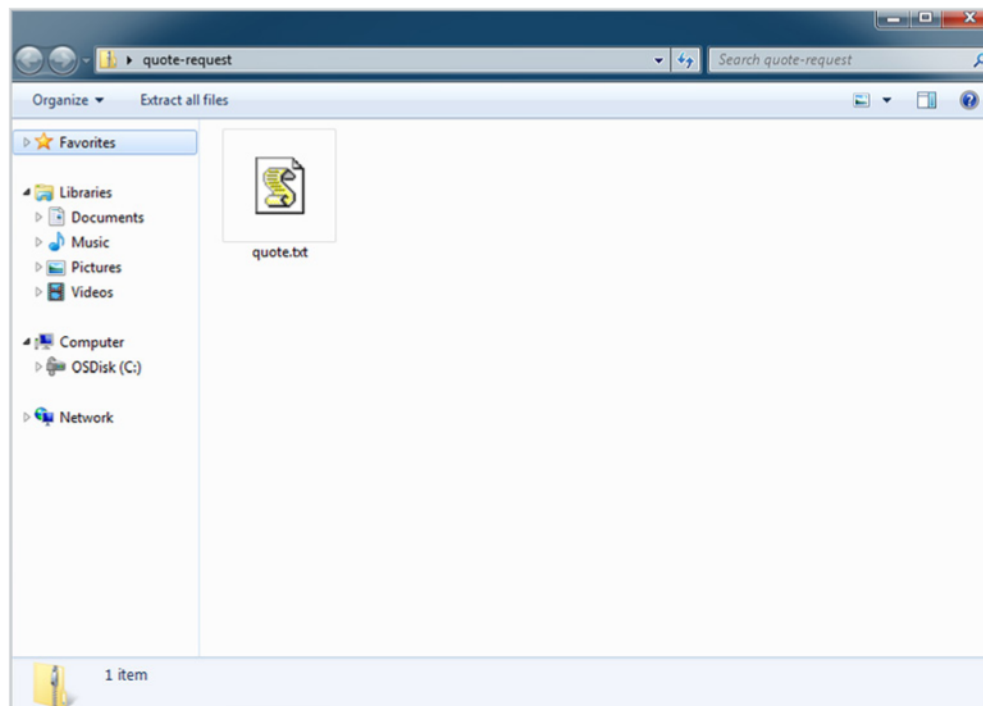
Les attaques de ransomware se produisent de deux manières principales : via un email contenant une pièce jointe malveillante ou via un site Web compromis (souvent légitime, grand public).

Email malveillant

Les criminels d'aujourd'hui créent des emails qui ressemblent en tous points à des emails légitimes. Ils 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.

Comment se protéger contre les ransomwares ?

Sites Web malveillants

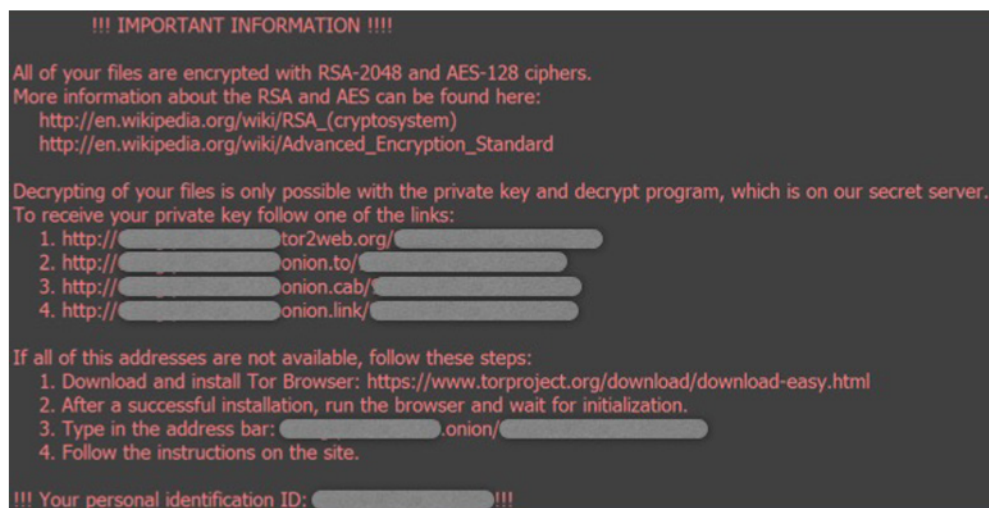
Un autre moyen de se retrouver infecté par un malware est de visiter un site Web légitime qui a lui-même été infecté par un kit d'exploit. Même des sites Web populaires peuvent être temporairement compromis. Les kits d'exploit sont des outils issus du marché noir que les criminels utilisent pour exploiter 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.

L'attaque du ransomware « Wanna DecryptOr 2.0 »

Wanna (appelé encore WannaCry, WCry, WanaCrypt, WanaCrypt0r ou Wana DeCrypt0r) est une attaque de ransomware à propagation ultra rapide, lancée le 12 mai 2017 à l'échelle mondiale.

L'analyse a confirmé que l'attaque a été lancée à l'aide d'un code NSA suspect publié par le groupe de pirates «Shadow Brokers». Elle utilise l'exploit ShadowBrokers APT EternalBlue (CC-1353), basé sur un chiffrement puissant des fichiers (documents, images et vidéos).

Fait exceptionnel, Wanna a pu exploiter une vulnérabilité RCE (Remote Code Execution), ce qui lui a permis d'infecter des systèmes sans correctifs sans que les utilisateurs ne fassent quoi que soit. De ce fait, Wanna a pu se propager très rapidement, à la manière des épidémies virales telles que Slammer ou Conficker d'il y a quelques années.

La vulnérabilité RCE exploitée était une faille dans le service SMB (Server Message Block) de Windows, utilisé par les machines Windows pour partager des fichiers et des imprimantes sur les réseaux locaux. Microsoft a répondu par le bulletin MS17-010 de mars 2017, mais les systèmes qui n'ont pas eu la mise à jour installée ou qui avaient des versions de Windows non prises en charge sont restés vulnérables.

En réponse à l'attaque, Microsoft a pris la décision inhabituelle de publier la mise à jour de sécurité pour les plateformes dans le support personnalisé (tel que Windows XP) pour tout le monde. Il est vivement recommandé d'installer cette mise à jour dès que possible.

Pour plus d'informations, veuillez consulter l'article de la base de connaissances suivant (en anglais) : www.sophos.com/kb/126733

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. 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.

2. 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.

3. 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.

4. 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.

5. 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 !

6. 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.

7. 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.

8. 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.

9. Mettez à jour les correctifs régulièrement et souvent.

Il est bon de le répéter : appliquer rapidement les correctifs est extrêmement important. Ne laissez pas les ransomwares utiliser des vulnérabilités pour lesquelles des correctifs existent !

Comment se protéger contre les ransomwares ?

Comment Sophos vous aide à rester protégé

Pour bloquer efficacement les ransomwares, vous avez besoin d'une protection avancée agissant à chacune des étapes de l'attaque.

Sécuriser les systèmes d'extrémité

Intercept X utilise plusieurs niveaux de défense pour stopper les ransomwares dans leur élan. La technologie anti-exploit stoppe la diffusion du ransomware, le Deep Learning bloque le ransomware avant qu'il ne s'exécute et CryptoGuard empêche le chiffrement malveillant des fichiers, et restaure les fichiers affectés. Intercept X fonctionne en parallèle de votre antivirus actuel, qu'il s'agisse d'une solution Sophos ou non.

Protéger vos serveurs

Server Advanced inclut la fonction CryptoGuard pour empêcher le chiffrement malveillant de vos fichiers et restaurer les fichiers affectés. La mise sur liste blanche et le verrouillage ne permettent que les applications autorisées et identifient ce que celles-ci peuvent modifier - toutes les autres tentatives de modification sont bloquées. La détection du trafic malveillant empêche les ransomwares de contacter leurs serveurs de Commande et de Contrôle et de télécharger la charge virale.

Stopper les emails de phishing

Sophos Phish Threat envoie des simulations d'attaques de phishing à vos employés, pour tester leur niveau de préparation aux attaques réelles. Les emails peuvent être adaptés à votre entreprise et à votre secteur industriel, et sont disponibles en plusieurs langues. Des rapports détaillés vous donnent une vue d'ensemble de vos utilisateurs tombés dans le piège, le niveau de risque global aux attaques et bien plus.

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

www.sophos.com/kb/120797

**Essayez Sophos Intercept X
gratuitement à la page :**

Sophos.fr/intercept-x

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

Copyright 2018. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

2018-02 WP-FR (NP)

SOPHOS