RAPPORT CONSULTATIF POUR LES ÉQUIPES DE SÉCURITÉ

# Les meilleures recommandations pour éviter les ransomwares



**Les ransomwares sont passés du statut de nuisance de bas étage à celui d'activité criminelle sophistiquée pesant plusieurs millions de dollars, qui cible désormais les particuliers et les sociétés.** Ce modèle d'activité criminel fait appel à des logiciels malveillants qui retiennent vos données personnelles en otage, par cryptographie. Bien que la situation soit de plus en plus urgente, les logiciels malveillants peuvent être évités grâce à une formation appropriée, à des ajustements spécifiques selon l'environnement informatique actuel, et à une technologie de terminal avancée.

**Qu'est-ce qu'un ransomware ?**

Les agresseurs doivent suivre cinq étapes pour réussir une attaque par ransomware :

1. **Compromettre et contrôler le système.** La plupart des attaques commencent par un spear phishing, qui consiste à piéger un utilisateur en lui envoyant un e-mail frauduleux dont la pièce jointe infectée, une fois ouverte, compromet le système. L'infection peut toucher un seul ordinateur, un téléphone portable ou toute une entreprise.
2. **Empêcher l'accès au système.** Une fois l'infection survenue, l'attaquant identifie et chiffre certains types de fichiers susceptibles d'avoir de la valeur aux yeux de la victime, comme des documents professionnels (.doc, .xls et .pdf), ou refuse totalement l'accès à tout le système via des écrans de verrouillage ou des tactiques alarmistes.
3. **Alerter le propriétaire de l'appareil de l'attaque, du montant de la rançon et des étapes à suivre.** Cela peut paraître évident, mais les attaquants et victimes ne parlent souvent pas la même langue et possèdent des niveaux de compétences techniques différents. Les attaquants doivent donc expliquer aux victimes ce qui s'est passé, dans des termes qu'elles peuvent comprendre, ainsi que les étapes à suivre pour déverrouiller leur appareil.
4. **Recevoir le paiement de la rançon.** Un attaquant doit posséder un moyen de recevoir les paiements des rançons tout en échappant à la loi, ce qui explique l'utilisation de crypto-monnaies anonymes, comme le bitcoin, pour ces transactions.
5. **Promettre de rendre un accès complet dès réception du paiement.** La non-restauration des systèmes compromis détruirait l'efficacité du schéma, car personne ne paie une rançon sans avoir l'assurance que ses objets de valeur lui seront rendus.

## QUI EST EXPOSÉ ?

**Les sociétés en ligne de mire.** Les attaques par ransomware peuvent avoir un impact hautement public ; les opérations de l'organisation ciblée peuvent être fortement dégradées ou entièrement stoppées, comme l'ont illustré les attaques récentes sur des hôpitaux américains. Les criminels ont compris qu'il s'agissait d'une activité lucrative n'opposant que peu de barrières. Le ransomware remplace donc d'autres modèles d'activité du cybercrime. De plus, les attaquants vont recourir à des méthodes plus sophistiquées pour déterminer la valeur des informations compromises, étudier la capacité à payer de l'organisation, et exiger des rançons plus élevées.

**Davantage de plateformes.** Par le passé, les attaquants se concentraient exclusivement sur les systèmes Microsoft® Windowst® ; mais l'émergence des ransomwares pour AndroidTM et Mact® OS Xt®, comme l'a récemment découvert Palo Alto Networkst®, démontre qu'aucun système n'est immunisé face à ces attaques. Presque tous les ordinateurs ou appareils possédant une connexion à Internet sont des victimes potentielles de ransomwares. Ces derniers suscitent une inquiétude croissante face à la montée en puissance de l'Internet des objets (IdO) et à la prolifération d'autres appareils, comme des équipements domestiques et technologiques à porter, connectés à Internet.

## PRÉPARER ET PRÉVENIR

Les attaques par ransomware se déploient rapidement, généralement sous quelques minutes après l'infection. Il est donc essentiel d'agir et de mettre en œuvre des contrôles qui limitent ou évitent ces attaques. Les deux sections suivantes récapitulent les principales recommandations à ces fins.

## LES MEILLEURES RECOMMANDATIONS POUR MINIMISER L'IMPACT DES RANSOMWARES

**1. Développer et mettre en œuvre un programme de sensibilisation de l'utilisateur final**

- Obtenir l'autorisation d'envoyer des rappels de sécurité réguliers à toute l'entreprise peut s'avérer difficile, mais les utilisateurs finaux plus avertis rencontreront sans doute moins d'incidents liés aux ransomwares.

**2. Réviser/valider les processus de sauvegarde du serveur**

- Certaines organisations comprennent trop tard que leurs sauvegardes sont compromises ou n'ont pas été correctement configurées. Vous pourrez avoir à leur demander de restaurer le service.
- Commencez par les serveurs de fichiers qui hébergent des partages réseau pour les services stratégiques.

**3. Étudier les autorisations sur lecteur réseau pour minimiser l'impact possible d'un utilisateur**

*Étude des privilèges des utilisateurs finaux*

- Nommez un chef de projet qui organisera l'évaluation des autorisations dont bénéficient des utilisateurs sur des lecteurs réseau mappés. Mettez en œuvre le principe de privilège le moins élevé pour minimiser l'impact possible d'un utilisateur concernant les lecteurs partagés sur le réseau de l'organisation.
- Selon la taille de l'organisation, ce processus peut être complexe et étendu. Commencez donc par les emplacements de lecteur réseau utilisés par les services critiques.

*Étude des privilèges d'utilisateur des administrateurs*

- Auditez les rôles avec privilèges utilisés par les équipes de serveur, de sauvegarde et de réseau pour valider un accès approprié.
- Assurez-vous que les administrateurs bénéficient d'un compte normal et restreint, différent de leur compte à privilèges élevés.
- Demandez aux administrateurs d'utiliser leur compte à privilèges élevés uniquement lorsqu'ils en ont besoin.
- Si possible, retirez les mappages automatiques de lecteur réseau sur les comptes d'administrateur.
- Interdisez l'accès aux e-mails depuis des comptes d'administrateur.

**4. Documenter votre plan de réponse aux incidents face aux ransomwares**

- Vous possédez probablement déjà un plan de réponse aux incidents générique, mais vous devez être prêt à faire face aux ransomwares en particulier : ils requièrent la mise en place d'un processus de récupération très spécifique, bien différent des autres incidents liés à des logiciels malveillants.
- Les cas dans lesquels tous les fichiers du lecteur d'un service sont chiffrés peuvent se révéler assez complexes, car plusieurs équipes doivent être engagées : équipes de sauvegarde, de serveur de fichiers, de terminal, de répertoire, etc. Planifiez tout cela dès à présent pour réduire d'autant plus votre délai de réponse.

## LES MEILLEURES RECOMMANDATIONS POUR ÉVITER LES RANSOMWARES

**1. Désactiver les scripts de macro dans les fichiers MS Office grâce à une stratégie de groupe AD**

- Selon Microsoft, 98 pour cent des menaces visant Office font appel à des macros. La désactivation des scripts de macro dans les fichiers MS Office arrête les ransomwares tels que Locky.
- Seuls certains services de l'organisation peuvent avoir besoin des macros Office. Activez les macros uniquement en cas d'exception ou pour certains services.
- Office 2016 possède une nouvelle fonction qui permet aux administrateurs de bloquer l'exécution de macros dans les documents Word, Excel et PowerPoint provenant d'Internet. Ainsi, si vous le pouvez, procédez à une mise à niveau et activez cette fonction.

**2. Étudier vos processus de gestion des correctifs mensuels**

- De nombreuses organisations ont des difficultés à appliquer des correctifs à leurs systèmes dans les 30 jours suivant la publication mensuelle par Microsoft (« Patch Tuesday »).
- Passez en revue les processus liés aux correctifs et essayez de supprimer les barrages routiers.
- Étudiez le déploiement d'un produit de terminal avancé, qui évite les exploits liés à des correctifs manquants et à des logiciels malveillants.

**3. Étudier votre protection contre les spams/logiciels malveillants entrants**

- Vérifiez que votre système est configuré de manière à bloquer les e-mails entrants selon les recommandations du fournisseur de votre serveur de messagerie (bloquer les exécutables dans les pièces jointes, etc.).

**4. Déployer un pare-feu nouvelle génération pour protéger le réseau**

- Assurez-vous que votre pare-feu bloque automatiquement les menaces connues, d'après un flux de menaces constamment mis à jour.
- Vérifiez que votre pare-feu fournit des capacités de sandboxing pour vous permettre de stopper les menaces inconnues (URL et exécutables) avant qu'elles n'atteignent le terminal. Le sandboxing constitue le meilleur moyen de détecter de nouvelles variantes de ransomware, qui apparaissent constamment dans le paysage informatique.
- Configurez votre pare-feu/proxy de manière à exiger une interaction de la part des utilisateurs finaux accédant à des sites Web « non classés » (par ex. cliquer sur le bouton « Continuer »). Les campagnes de phishing ciblé utilisent de nombreux sites Web non classés pour diffuser des logiciels malveillants. Ce processus en deux étapes évite que certains types de ransomwares n'envoient un appel externe au serveur de commande et de contrôle. Sans cet appel, le ransomware ne pourra pas chiffrer vos fichiers.

**5. Déployer une protection de terminal avancée**

- Les antivirus traditionnels ne sont pas efficaces face aux logiciels malveillants avancés, tels que les ransomwares, qui se transforment sans cesse pour éviter toute détection. Assurez-vous que vos mesures de protection de terminal sont en mesure de détecter et de prévenir les logiciels malveillants connus et inconnus, ainsi que les exploits connus et inconnus, y compris les « zero-days ».
- Une liste blanche peut être utile pour des organisations simples et de taille réduite ; en revanche, pour les organisations en développement présentant de nombreuses applications et une certaine complexité, sa gestion peut rapidement nécessiter beaucoup de travail. La détection de logiciels malveillants basée sur la technique est très efficace dans la détection de ransomwares.
- Assurez-vous que vos systèmes de protection de terminal reçoivent des renseignements en temps réel sur les menaces, tirés de sources internes et externes qui dépassent les limites, lieux et secteurs de l'organisation.

**VOUS SOUHAITEZ OBTENIR PLUS D'INFORMATIONS ?**

*Ransomwares :* paloaltonetworks.com/solutions/initiatives/ransomware
*TRAPS :* paloaltonetworks.com/products/secure-the-endpoint/traps
*NGFW :* paloaltonetworks.com/products/secure-the-network/next-generation-firewall