EMPÊCHER UN SINISTRE CAUSÉ PAR UN RANSOMWARE

Les ransomware ne constituent pas une simple cyberattaque parmi d'autres ; ces derniers peuvent proliférer rapidement parmi les dossiers partagés.

RÉSUMÉ

Les ransomware représentent une menace qui coûte déjà plusieurs millions de dollars chaque année aux entreprises et qui ne cesse, malheureusement, d'être de plus en plus sophistiquée. Heureusement, Mozy et Spanning d'EMC vous aident à protéger les postes et serveurs et les données des applications SaaS grâce à des solutions de sauvegarde faciles à déployer, efficaces et basées dans le Cloud.

Juin 2016

Pour en savoir plus sur la façon de prévenir un sinistre suite à l'attaque d'un ransomware grâce à la protection des données des postes, rendez-vous sur Mozy. Pour plus d'informations sur la protection de vos données SaaS, rendez-vous sur Spanning.

Référence H15174

SOMMAIRE

INTRODUCTION

Les ransomware représentent une menace qui coûte déjà plusieurs millions de dollars chaque année aux entreprises et qui ne cesse, malheureusement, d'être de plus en plus sophistiquée. Les cybercriminels introduisent des malwares dans votre réseau par l'utilisation de divers types d'attaques, y compris les e-mails ciblés et les sites Web infectés, afin de prendre vos données ou autres systèmes en otage jusqu'à ce que vous payiez une rançon. Il est très difficile de bloquer chacune des attaques de type ransomware. De nombreux experts, y compris le FBI, conseillent d'ailleurs aux organisations de disposer d'une défense multiniveau avec des sauvegardes protégées permettant une restauration rapide. Les organisations qui suivent ce conseil se concentrent souvent sur les systèmes internes clés et en oublient leurs postes utilisateurs (ordinateurs portables et de bureau), et les applications SaaS qui rassemblent des données essentielles aux employés. Heureusement, Mozy et Spanning d'EMC vous aident à mieux protéger vos données grâce à des solutions de sauvegarde faciles à déployer, efficaces et basées dans le Cloud.

L'ÉMERGENCE DES RANSOMWARE

Le tout premier ransomware a avoir été identifié est Trojan.Gpcoder. Découvert en 2005, il s'attaquait aux systèmes d'exploitation Windows. Plus de 10 ans plus tard, il ne fait plus aucun doute que les ransomware sont en plein essor. En réalité, d'après le tout récent Threat Report de McAfee Labs, ces derniers ont connu une croissance de 58 % au cours du second trimestre 2015.[1] Il n'existe aucune raison de douter de la poursuite de l'augmentation considérable de la menace liée à ce type de malwares. La raison est simple : « Les ransomware sont faciles à développer, simples à exécuter, et sont très efficaces dans leur mission consistant à convaincre les victimes de payer pour reprendre possession de leurs précieux fichiers ou systèmes. »[2]

Un récent résumé d'analyse mené par Recorded Future a d'ailleurs soulevé l'augmentation spectaculaire des infections par les ransomware en Europe et ce, en l'espace d'une année seulement.[3] Bien que les frontières géographiques ne puissent rien contre ces programmes de demande de rançon, les six pays principalement concernés par ce type de programmes malveillants sont les États-Unis, le Japon, le Royaume-Uni, l'Italie, l'Allemagne et la Russie.[4] Prenons pour exemple cette attaque via un ransomware ayant eu lieu plus tôt cette année.

Des cyberterroristes ont piraté l'important système informatique d'un centre médical situé aux États-Unis en rendant l'accès aux données de l'hôpital impossible grâce à leur chiffrement. Dans un premier temps, les pirates exigeaient 3,6 millions de dollars en échange de la libération de ces données. Leur demande a ensuite été ramenée à 40 bitcoins (environ 17 000 USD) pour la remise d'une clé de déchiffrement. Par leur action, ces pirates ont démontré au monde entier que les données des patients et les dossiers médicaux ne sont pas épargnés par ce type d'attaques. Après tout, si les informations de cet hôpital de Los Angeles ont pu être utilisées pour une demande de rançon, pourquoi est-ce que cette situation ne pourrait pas être reproduite ailleurs ? La réalité est que tous les types d'organisation, y compris les centres médicaux, les services administratifs, le secteur de l'éducation, celui de l'industrie et autres, peuvent devenir la cible d'un complot d'extorsion opéré via un programme de demande de rançon.

QU'EST-CE QU'UN RANSOMWARE ET COMMENT SE PROPAGE-T-IL ?

Les ransomware ne constituent pas simplement une autre cyberattaque parmi toutes les autres ; ces derniers peuvent proliférer rapidement parmi les dossiers partagés et ainsi affecter les systèmes internes et externes d'une organisation. Les ransomware verrouillent l'ordinateur (rançogiciels de verrouillage) ou chiffrent les fichiers de l'utilisateur (rançogiciels de chiffrement) avant d'exiger de ce dernier qu'il paye une certaine somme d'argent (généralement sous la forme d'un paiement numérique, par bitcoin par exemple, comme ce fut le cas pour le centre médical de Los Angeles) en échange d'une clé de déchiffrement permettant de déverrouiller l'ordinateur ou les fichiers.

Les ransomware accèdent aux systèmes informatiques par le maillon le plus faible d'un réseau, lequel correspond généralement aux comptes de messagerie des utilisateurs ou aux sites de réseaux sociaux. Dès que l'utilisateur clique sur un lien malveillant ou ouvre une pièce jointe infectée, le malware se propage dans tout le système. Une fois ouverts, les faux fichiers PDF infectés par un malware et prenant l'apparence de notifications FedEx et UPS alors qu'elles correspondent à des institutions financières frauduleuses, contournent rapidement la sécurité du réseau d'une organisation pour se propager hors du système local au moyen des partages réseau et autres postes utilisateurs utilisés pour la synchronisation des fichiers ou encore des outils de partage tels que Microsoft OneDrive, Google Drive ou Dropbox.

---

[1] McAfee Labs Threat Report, page 33, Intel Security Group, August 2015.
[2] Ransomware a Favorite of Cybercriminals, Matthew Rosenquist, McAfee Blog Central; September 1, 2015.
[3] Locking Up Europe With Ransomware: Origination, Targeting, and Payment, Recorded Future, Inc., 2016.
[4] The evolution of ransomware, Version 1, page 5; Kevin Savage, Peter Coogan, Hon Lau; Symantec; August 6, 2015.

Selon l'équipe du Centre gouvernemental de veille, d'alerte et de réponse aux attaques des États-Unis (US-CERT), si les cybercriminels qui utilisent les ransomware sont si efficaces, c'est qu'ils instillent peur et panique à leurs victimes, entre autres par l'utilisation de messages intimidants du type « Votre ordinateur a été utilisé pour consulter des sites Web présentant du contenu illégal. Vous devez vous acquitter d'une amende de 100 $ pour le déverrouiller. »[5] Les ransomware ont également vu leur popularité augmenter chez les cybercriminels pour d'autres raisons et notamment la facilité avec laquelle ils sont créés et déployés.

Le principe des ransomware est simple : en refusant de payer la rançon exigée, vous renoncez à l'accès à votre ordinateur et aux données qu'il contient. Par la même occasion, vous empêchez d'autres utilisateurs d'accéder aux documents en aggravant l'impact de manière exponentielle. Malheureusement, les victimes qui payent la rançon sont susceptibles de ne pas recouvrer l'accès à leurs fichiers. La dure vérité est qu'il existe un risque que le pirate impliqué ne remette pas la clé de déchiffrement en échange de la rançon. En fait, une récente enquête a démontré que seuls 71 % des victimes qui payent la rançon recouvrent véritablement l'accès à leurs fichiers.[6]

RÉALITÉ SUR LES RANSOMWARE

Les résultats de l'enquête Infosécurité Europe publiée en 2015 par ESET ont révélé que 84 % des personnes interrogées pensaient que leur entreprise en pâtirait sérieusement si elle venait à être infectée par un programme de demande de rançon. Près d'un tiers d'entre elles (31 %) ont admis qu'elles seraient contraintes de payer les auteurs de l'attaque afin de déchiffrer leurs données.[7]

Les entreprises savent qu'il est très difficile de se protéger de toutes les menaces et que les ransomware constituent un véritable défi. Par exemple, « CryptoWall, le ransomware actuellement leader est très sophistiqué et utilise une méthode de chiffrement inviolable. Si vous ne disposez d'aucune sauvegarde à jour, vous êtes véritablement dans le pétrin..., » selon Stu Sjouwerman, auteur et expert en programmes anti-espions.[8]

D'après le dernier rapport sur les menaces de sécurité Internet, la majorité des ransomware sont des rançogiciels de verrouillage au même titre que CryptoWall. « Avant ce jour, jamais dans l'histoire de l'humanité les personnes n'avaient été soumises à un tel niveau d'extorsion. »[9] En 2015, 362 000 types de rançogiciels de verrouillage différents ont été recensés (soit une hausse de 35 % par rapport à l'année précédente), pour une moyenne de 992 nouveaux rançogiciels créés chaque jour.[10]

Bien que vous et vos données puissiez échapper à la menace de CryptoWall, des millions de nouvelles variantes de programmes malveillants font littéralement leur apparition chaque année. 431 millions de variantes ont été ajoutées en 2015, soit 36 % de plus que l'année précédente.[11] La protection efficace contre les ransomware exige non seulement la prévention et la détection des menaces, mais également une stratégie de sauvegarde et de restauration. En omettant de le faire, on s'expose à des coûts importants. Il est à souligner que de récentes recherches ont estimé que 36 % des participants des organisations mondiales publiques et privées interrogées avaient eu à subir des arrêts de système et/ou des pertes de données à cause d'une atteinte à la sécurité interne ou externe. On estime que le coût moyen pour chacune des organisations qui subissent un arrêt de système s'élève à 555.000 US$ dans les 12 derniers mois. Encore plus important, le coût estimé pour les organisations qui ont été victimes d'une perte de données, dans les 12 derniers mois — 914.000 US$. De toute évidence, vos données doivent être protégées — et vous devez pouvoir faire confiance à la réactivité de votre protection.[12]

QUE POUVONS-NOUS DONC FAIRE ?

Les données essentielles aux opérations quotidiennes d'une organisation ou qui sont soumises au respect de la réglementation doivent toujours être protégées. Les pirates ne se soucient pas forcément de l'identité du propriétaire des informations. Leur objectif est d'exploiter au mieux les faiblesses de l'infrastructure IT pour voler, endommager ou détenir pour rançon les données d'une organisation. Comme la plupart des criminels, les cybercriminels sont opportunistes et recherchent les cibles faciles. Êtes-vous une cible facile ? Pour commencer, répondez à ces questions :

- Vos employés sont-ils conscients des risques liés aux e-mails indésirables ?
- Votre pare-feu et vos filtres de messagerie sont-ils toujours bien à jour ?

---

[5] Ransomware and Recent Variants, United States Computer Emergency Readiness Team; March 31, 2016.
[6] Crypto-Ransomware: Survey of IT Experts, page 16, Jeffrey Henning, Researchscape International; February 4, 2016.
[7] UK Companies Commonly Held Hostage by Hackers, Urban Schrott, ESET Ireland; June 29, 2015.
[8] Ransomware victims: Just pay up, grin, and bear it, says the FBI, The Register; October 27, 2015.
[9] Internet Security Threat Report, Volume 21, page 58, Symantec, April 2016.
[10] Ibid., page 8.
[11] Ibid.
[12] EMC Global Data Protection Index, independent research by Vanson Bourne, March–April 2016.

- Utilisez-vous un logiciel antivirus arrivé à expiration ?
- Synchronisez-vous des données entre des postes et des systèmes de partage de fichiers synchronisés basés dans le Cloud ?

Il est important de noter que les solutions de sauvegarde courantes comme les clés USB ou les périphériques de stockage rattachés au réseau (NAS) ne constituent pas des méthodes fiables pour sauvegarder et protéger vos données. Les ransomware se propagent généralement dans l'ensemble du système de fichiers d'une organisation, y compris sur les lecteurs connectés ou les partages réseau, et y chiffrent à la fois les données de production et de sauvegarde.

La méthode de protection la plus fiable dont les organisations peuvent tirer parti pour protéger leurs données reste la sauvegarde. Plus votre sauvegarde est rapide et restaure facilement les fichiers tels qu'ils étaient avant l'infection, moins vous êtes susceptible de subir une défaillance importante au niveau de la continuité de votre activité. Lorsque vous recherchez une solution de sauvegarde, que devez-vous évaluer afin de vous assurer que vos données seront bien protégées ? Tenez compte des points suivants :

- La sauvegarde est-elle située hors site (en dehors de votre site principal) ?
- Pouvez-vous vous assurer que les sauvegardes ont bien lieu ?
- Pouvez-vous vérifier que les données sont bien restaurées à leur état d'origine ?
- Pouvez-vous restaurer rapidement les données prises en otages ?

Disposer d'une stratégie de sauvegarde et de restauration viable ne constitue pas simplement une pratique répandue, celle-ci est souvent requise par les lois et réglementations, en fonction du type d'organisation et de son secteur d'activité :

- Les règles HIPAA exigent que les établissements de santé disposent d'une stratégie de reprise après sinistre et d'un système de sauvegarde pour leurs données de santé confidentielles électroniques. Lesquels doivent être testés régulièrement.[13]
- Deux organismes de mise en œuvre bancaire et financière, l'OCIE et le FFIEC, ont fait de la cybersécurité (dont la capacité à restaurer des données ayant subit des dommages) un élément essentiel parmi leurs priorités de mise en application et d'évaluation.[14]
- La SEC a rappelé aux entreprises publiques la nécessité d'un contrôle informatique approprié, lequel inclut les fonctions de sauvegarde et de restauration et la responsabilité de signaler les risques de cybersécurité. À l'heure actuelle, l'incapacité de restaurer des données face à une menace grandissante, telle que celle liée aux ransomware, doit incontestablement conduire à une plus grande divulgation.[15]

En cas de défaillance matérielle, vol, attaque virale (y compris l'extorsion via les ransomware !), suppression accidentelle, catastrophe naturelle ou erreur humaine, le fait de disposer des solutions de sauvegarde et de restauration appropriées vous assure de la disponibilité et de la récupération de vos données dans leur état d'origine tout en garantissant la conformité de votre organisation en matière de réglementations applicables.

SAUVEGARDE DE VOS DONNÉES AVEC EMC

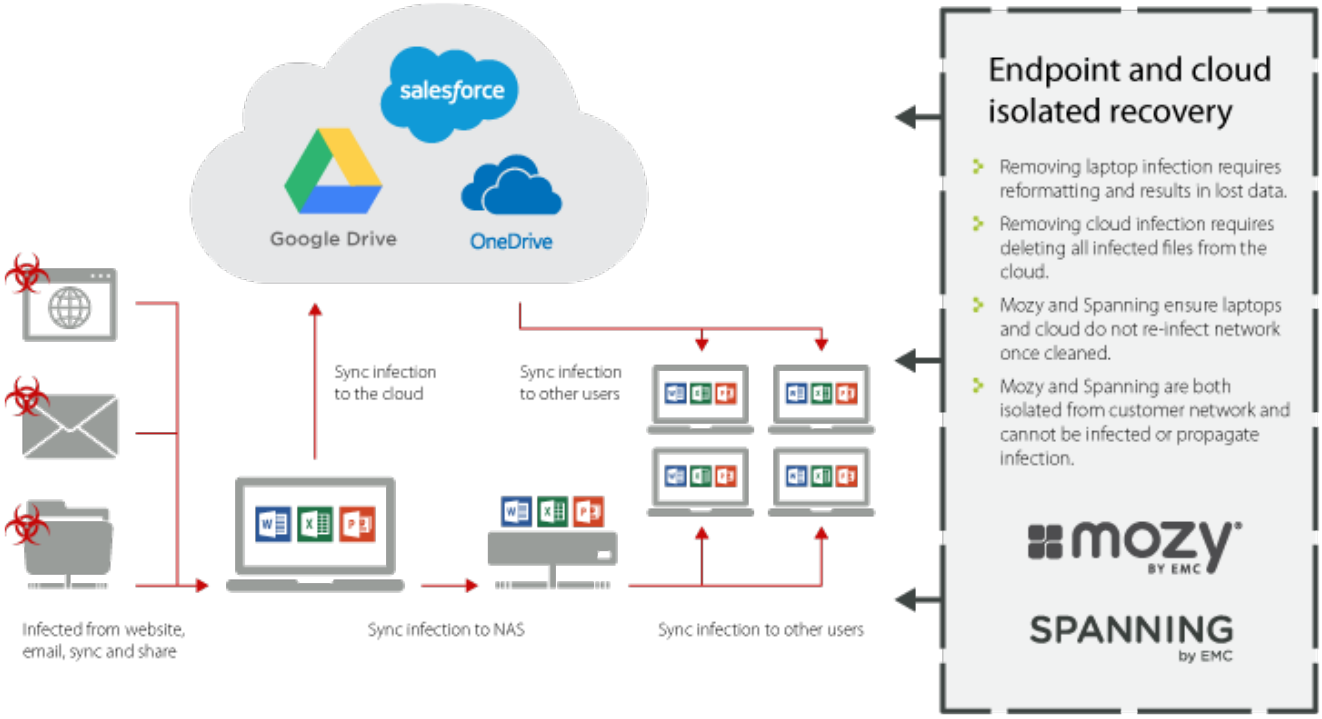
Prévenez la perte de données suite à une attaque par un ransomware en sauvegardant vos données importantes grâce aux solutions de protection fiables d'EMC.

Les postes utilisateurs, une cible privilégiée

La restauration des serveurs ne garantit pas la suppression de l'infection de votre réseau puisque celle-ci a probablement un poste utilisateur pour origine, tel qu'illustré dans l'image suivante. Les données sauvegardées par Mozy et Spanning (deux solutions d'EMC) sont isolées du réseau du client et ne peuvent pas être infectées ou servir de vecteur à une infection.

---

[13] HIPAA Security Rule, 45 CFR 164.308(7).
[14] National Exam Program Risk Alert, Volume IV, Issue 8; September 15, 2016.
[15] Emerging SEC guidance and enforcement regarding data privacy and breach disclosures, Joseph D. Masterson, Inside Counsel; June 25, 2015; and Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks, Paul Weiss; September 30, 2015.



Protection des données des postes via Mozy d'EMC

La sauvegarde Cloud de Mozy place les fichiers des postes importants et les données des serveurs hors d'atteinte des ransomware. Grâce à sa technologie back-end unique, Mozy empêche toute exécution de code au sein des fichiers ayant été sauvegardés. Toutefois, la simple sauvegarde des données ne suffit pas à garantir la protection de vos fichiers face aux ransomware.

Lorsqu'une infection par malware se produit, la restauration d'un serveur ou d'un poste à partir d'une sauvegarde est optimale dès lors que vous pouvez facilement sélectionner un moment à partir duquel effectuer la restauration. Mozy conserve les versions des fichiers pour les 90 derniers jours, ce qui signifie que si vous avez identifié le point d'infection (utilisateur et fichier) et le moment auquel le malware a été introduit dans l'ordinateur, Mozy est capable de restaurer tous les fichiers de l'utilisateur donné au point dans le temps se situant juste avant l'infection par le malware. Par exemple, si le malware a été introduit le 2 juin, les fichiers peuvent être restaurés à partir de la sauvegarde du 1er juin.

Protection des données SaaS via Spanning d'EMC

Les plates-formes de productivité bureautiques SaaS telles que Google Apps ou Microsoft Office 365 sont également vulnérables face aux attaques par programmes malveillants, et Google ou Microsoft ne sont pas toujours en mesure de revenir rapidement à une version avant infection de vos fichiers. Les périphériques de postes infectés peuvent se synchroniser avec ces plates-formes, et dans certains cas, le programme malveillant peut proliférer automatiquement par le biais des lecteurs partagés et des dossiers, chiffrant ainsi les fichiers partagés au sein de votre organisation et même en dehors.

Spanning Backup protège entièrement les données stockées et générées dans Google Apps et Office 365 et vous permet de restaurer rapidement les données à un point antérieur dans le temps, préalable au chiffrement des fichiers par le ransomware.

La sauvegarde et la protection des données critiques de votre organisation via les solutions de sauvegarde Mozy et Spanning vous offrent une plus grande tranquillité d'esprit, tout en sachant que vous pouvez, en cas de perte de données, les restaurer rapidement et facilement exactement comme elles étaient à n'importe quel point dans le temps donné. Vos données sont ainsi protégées, sécurisées et toujours disponibles. Ces solutions vous offrent la possibilité de répondre aux attaques et de restaurer rapidement vos données à leur état d'origine afin d'assurer la continuité de votre activité et de répondre aux objectifs de temps et de point de restauration (RTO et RPO).

CONCLUSION

D'après ESET Irlande, les ransomware deviennent de plus en plus agressifs et présentent à la fois des nouvelles fonctionnalités et une multitude de variantes.[16] Bien que la détection et la prévention soient décisives, une sauvegarde régulièrement mise à jour et qui permet une restauration précise et rapide constitue l'ultime ligne de défense. « … [L]a sauvegarde des fichiers est un moyen efficace pour minimiser l'impact des ransomware et… l'adoption des bonnes pratiques relatives à la sécurité informatique est le moyen le plus efficace d'éviter ce type d'infection. Les particuliers et les professionnels qui sauvegardent régulièrement leurs fichiers sur un périphérique ou un serveur externe peuvent nettoyer leur disque dur de manière à y supprimer tout ransomware et restaurer leurs fichiers à partir de la sauvegarde. Si tous les particuliers et les professionnels sauvegardaient leurs fichiers, l'utilisation des ransomware ne serait alors plus une activité rentable pour les cybercriminels. »[17]

Plus que jamais, les organisations comptent sur les données numériques. Dans ce sens, l'ensemble des organisations (depuis les petites PME aux plus grandes entreprises) doivent prendre les mesures nécessaires pour s'assurer que leurs données sont sauvegardées en toute sécurité et qu'elles peuvent être restaurées rapidement à leur état d'origine.

Pour plus d'informations sur la façon de prévenir un sinistre suite à l'attaque d'un ransomware grâce à la protection des données des postes, rendez-vous sur Mozy. Enfin, pour savoir comment protéger vos données SaaS, rendez-vous sur Spanning.

---

[16] Jigsaw and how ransomware is becoming more aggressive with new capabilities, Urban Schrott, ESET Ireland; May 4, 2016.
[17] U.S. Department of Justice, Federal Bureau of Investigation, Letter to Senator Ron Wyden, February 8, 2016.