LIVRE BLANC

La dernière ligne de défense contre le ransomware

Quantum®

SOMMAIRE

La dernière ligne de défense contre le ransomware n'est pas celle que vous croyez. 3
Comment les ransomwares pénètrent-ils dans votre environnement ? 4
Comment protéger ses données contre les attaques de ransomware ? 4
Protégez votre protection. 4
Protection Cloud contre les ransomwares : la solution idéale ?. 5
Les bandes : la dernière ligne de défense ?. 5
La règle du « 3-2-1 » de Quantum... 6

LA DERNIÈRE LIGNE DE DÉFENSE CONTRE LE RANSOMWARE N'EST PAS CELLE QUE VOUS CROYEZ

Les ransomwares ont régulièrement défrayé la chronique ces derniers temps. Des logiciels comme CryptoLocker et Locky ont été éclipsés par WannaCry, « une attaque de ransomware sans précédent » selon Trend Micro. L'attaque WannaCry a commencé le vendredi 12 mai 2017. En l'espace d'un jour, elle a frappé plus de 230 000 ordinateurs, se propageant à plus de 150 pays et infectant plusieurs grandes entreprises dans le monde entier. Elle a provoqué l'arrêt de cinq sites de production du constructeur automobile Renault-Nissan. Les ordinateurs de dizaines d'hôpitaux et d'établissements de santé au Royaume-Uni ont également été touchés. Le transporteur américain FedEx Corp. et le Japonais Hitachi Ltd figurent aussi parmi les victimes.

Pour ceux qui ne savent pas de quoi il retourne, un ransomware est un logiciel malveillant qui empêche ou limite l'accès d'un utilisateur à son système informatique, soit en verrouillant l'écran de ce dernier, soit en verrouillant/chiffrant les fichiers jusqu'au versement d'une rançon (souvent en bitcoins).

Le premier ransomware recensé a été créé en 1986. Depuis 2006 sont apparues des versions plus avancées, reposant sur un chiffrement RSA. Depuis 2015, les attaques de ce type augmentent à un rythme inquiétant dans le monde entier. Les cybercriminels ne se contentent plus de cibler les particuliers. Ils visent désormais également les entreprises à l'aide d'attaques ciblées plus évoluées. Ce genre de méfait à l'encontre des réseaux d'entreprise est en plein essor. De par leur nature trompeuse, les ransomwares peuvent infester la totalité d'un système avant d'être détectés.

Prenons l'exemple de Locky. Ce logiciel malveillant de 100 Ko développé en C++ et compilé via Microsoft Visual Studio se déploie sur un système et supprime les fichiers permettant normalement à Windows d'avertir l'utilisateur que des éléments suspects ont été téléchargés depuis Internet. Le ransomware interagit ensuite avec un serveur central pour signaler l'infection, puis reçoit une clé de chiffrement RSA-2048 ainsi qu'un identifiant lié au système corrompu. Il commence alors à chiffrer l'ordinateur ou le serveur. C'est là que les pirates peuvent exiger une rançon en échange d'un arrêt de l'attaque. Aujourd'hui, il existe un grand nombre de variantes ou de clones de Locky ou de CryptoLocker, et s'ils ne sont pas liés au cheval de Troie original, tous appliquent sensiblement la même méthode.

WannaCry est un autre exemple de ransomware bien plus dangereux que les formes courantes en raison de sa capacité à se propager très rapidement via le protocole standard de partage de fichiers utilisé par les PC : Microsoft Windows Server Message Block (SMB). Les écoles, universités, entreprises, hôpitaux et autres organisations orientées réseau sont particulièrement vulnérables. WannaCry semble également capable de se propager à d'autres ordinateurs en dehors des réseaux d'entreprise.

Les ransomwares ne se limitent pas à Windows. Ils s'attaquent également à des systèmes d'exploitation comme Mac OS avec des chevaux de Troie tels que KeRanger ou Mabouia, et Linux avec Linux.Encoder.1 et FairWare, ainsi qu'aux systèmes NAS avec SynoLocker. Des appareils mobiles et même des services de synchronisation de fichiers dans le Cloud ont aussi été touchés. Récemment, la variante ScareMeNot a infecté 30 000 appareils mobiles en trois semaines seulement. Clichés instantanés des volumes Windows (service VSS), fonctions de restauration du système : là encore, les ransomwares peuvent frapper. Désormais, les pirates visent les comptes administrateur, surtout ceux dédiés aux sauvegardes, pour chiffrer ces dernières avant les données primaires.

COMMENT LES RANSOMWARES PÉNÈTRENT-ILS DANS VOTRE ENVIRONNEMENT ?

Les e-mails contenant des pièces jointes et des liens malveillants représentent 59 % des infections provoquées par des ransomwares. Selon une enquête d'Osterman Research effectuée en juin 2016, les utilisateurs ont deux fois plus de chances d'être infectés en cliquant sur un lien dans un e-mail qu'en visitant directement un site infecté. Vous pensez que cela n'arrive qu'aux autres ? Dans la même enquête, près d'une personne interrogée sur deux indiquait que son entreprise avait subi au moins une attaque de ransomware au cours des 12 derniers mois. Avec l'apparition de nouveaux ransomwares, comme Locky, Symantec a déclaré avoir bloqué quelque 388 000 attaques par jour fin 2016, rien que pour les kits d'exploit.

Face à la popularité grandissante de ce type de logiciels auprès des cybercriminels, qui voient là une source facile de revenus, les créateurs de ransomwares se sont empressés de répondre à la demande. Ainsi, selon Trend Micro, 50 nouvelles familles de ransomwares ont été découvertes au cours des cinq premiers mois de l'année 2016. Le FBI estime que les ransomwares représenteront une source de revenus d'un milliard de dollars pour les cybercriminels cette année. Le montant total des rançons versées est peut-être plus important encore, de nombreuses victimes préférant ne pas signaler ce genre d'incident. L'un des cas ayant fait le plus de bruit est celui de la clinique américaine Hollywood Presbyterian Medical Center. D'après le New York Post, cet établissement a versé 17 000 $ à un pirate anonyme pour mettre fin à une cyberattaque.

Enfin, les spécialistes d'Invincea ont découvert une nouvelle variante de ransomware appelée Cerber. Outre le chiffrement des fichiers, ce cheval de Troie installe un botnet capable de lancer des attaques DDoS. Une attaque DDoS a pour but de rendre un service en ligne indisponible en le saturant de trafic provenant de plusieurs sources. Ici, le risque est double : si la rançon n'est pas payée, les fichiers continuent d'être chiffrés, mais en plus, le système ciblé est recruté comme botnet pour les attaques DDoS. Une véritable aubaine pour les criminels, car ce genre d'attaque constitue lui aussi une source de revenus.

COMMENT PROTÉGER SES DONNÉES CONTRE LES ATTAQUES DE RANSOMWARE ?

Protégez votre protection

Face à la multiplication des attaques de ransomware, il convient de mettre en place une stratégie de défense des fichiers contre ce genre d'événement. Dans cette optique, il faut commencer par une stratégie de protection des données adéquate. Sans plan de sauvegarde approprié, autant vous préparer tout de suite à verser la rançon en bitcoins. Bien évidemment, il est déconseillé de payer, les criminels ne respectant pas toujours leur engagement de déchiffrer les données, comme l'a appris à ses dépens le Kansas Heart Hospital en mai 2016 (d'après Healthcare IT News).

Le ransomware chiffrant discrètement les fichiers, votre programme sauvegardera probablement les versions récemment chiffrées. Il vous faut donc un programme prenant en charge la gestion des versions. Cela ne pose pas vraiment de problème, la majorité des professionnels de l'informatique conservant plusieurs sauvegardes afin de permettre la restauration d'applications ou de fichiers dans un état antérieur au chiffrement des données. Mais même ces versions plus anciennes ne seront d'aucune utilité si le ransomware parvient à chiffrer la totalité des fichiers de la cible de sauvegarde, voire d'un référentiel distant répliqué (pour rappel, les ransomwares peuvent se propager à d'autres machines via le réseau). Tant que l'utilisateur n'a pas accès en écriture à l'emplacement des fichiers de sauvegarde (partage NAS ou référentiel Veeam Backup & Replication), le cheval de Troie exécuté dans un contexte de sécurité d'utilisateur sera incapable de chiffrer des fichiers de sauvegarde spécifiques. Selon une étude de Barkly réalisée en 2016, seuls 42 % des professionnels de l'informatique ayant subi une attaque de ransomware ont déclaré être parvenus à restaurer toutes leurs données à partir de sauvegardes. L'une des principales raisons à cela est le fait que les sauvegardes étaient elles aussi chiffrées.

Une bonne pratique consiste à s'assurer que les administrateurs n'utilisent pas en permanence leur compte doté de privilèges avancés. Il faut savoir protéger le protecteur et faire preuve de prudence en matière de gestion des comptes administrateur dédiés aux sauvegardes. Les pirates les plus aguerris, et motivés, ciblent désormais les sauvegardes via l'ingénierie sociale ou d'autres méthodes permettant d'obtenir des privilèges d'administrateur. En témoigne la récente attaque perpétrée par des cybercriminels à l'encontre d'une grande université américaine. L'attaque a été minutieusement planifiée. L'étude de cas est accessible à l'adresse www.quantum.com/fighting-ransomware.

En matière de sauvegarde, la règle éprouvée du « 3-2-1 » constitue une excellente approche. Cette stratégie consiste à disposer d'au moins 3 copies intégrales des données : 2 stockées en local, mais sur des supports (appareils) différents, et au moins 1 hors site. Il est même possible d'aller plus loin avec la règle du « 3-2-1-0 » : il vous faut 3 copies, 2 médias, 1 copie hors site, et la dernière doit être hors ligne, avec 0 connectivité en temps réel. La bonne vieille sauvegarde redevient donc intéressante en tant que première ligne de défense pour la restauration.

Protection Cloud contre les ransomwares : la solution idéale ?

Les petites entreprises et les particuliers s'appuient de plus en plus sur les sauvegardes Cloud comme dernière ligne de défense. Des solutions de stockage dans le Cloud comme Dropbox, Google Drive et autres services de sauvegarde Cloud d'entreprise permettent indéniablement de protéger les données contre les attaques de ransomware.

La sauvegarde dans le Cloud est toujours active, mais le transfert des fichiers est lent. Si le manque de vitesse peut être gênant, cette méthode offre néanmoins un degré de protection supplémentaire. Il peut s'écouler des jours, voire des semaines entières, avant que tous les fichiers chiffrés ne soient transférés dans le Cloud. Mais compte tenu des dernières techniques de déduplication, de compression et d'optimisation de la bande passante, l'accès au Cloud s'accélère. Le problème est qu'à la moindre modification, la majorité des fichiers seront synchronisés. Et s'ils ont été chiffrés par une attaque de ransomware, ils seront transférés dans cet état. De plus, si votre entreprise utilise des outils de collaboration Cloud comme Office 365 OneDrive Entreprise ou Google Drive, l'impact d'une attaque de ransomware est multiplié par la puissance de calcul.

Certaines solutions de sauvegarde dans le Cloud permettent évidemment de gérer les versions des données… mais il y a un « mais ». Comme le stipulent les conditions générales d'un grand fournisseur de Cloud public, « vous ne pouvez restaurer les versions précédentes qu'un seul fichier à la fois ». Le délai de restauration — s'il n'est possible de restaurer qu'un seul fichier à la fois — est donc un paramètre clé de toute stratégie de sauvegarde.

Autre problème : les pirates peuvent désormais cibler spécifiquement les systèmes de stockage Cloud, notamment Dropbox. Dans ces conditions, il est impossible de savoir que l'on est en train de télécharger des fichiers chiffrés depuis l'un de ces emplacements. Les pirates n'ont même plus besoin de mot de passe pour accéder aux données Cloud. Il leur suffit de dérober des identifiants, puis de supprimer ou de chiffrer les sauvegardes Cloud à l'aide d'une attaque de type « homme du milieu » (désormais appelée « homme dans le Cloud » selon le spécialiste de la sécurité Imperva).

Les bandes : la dernière ligne de défense ?

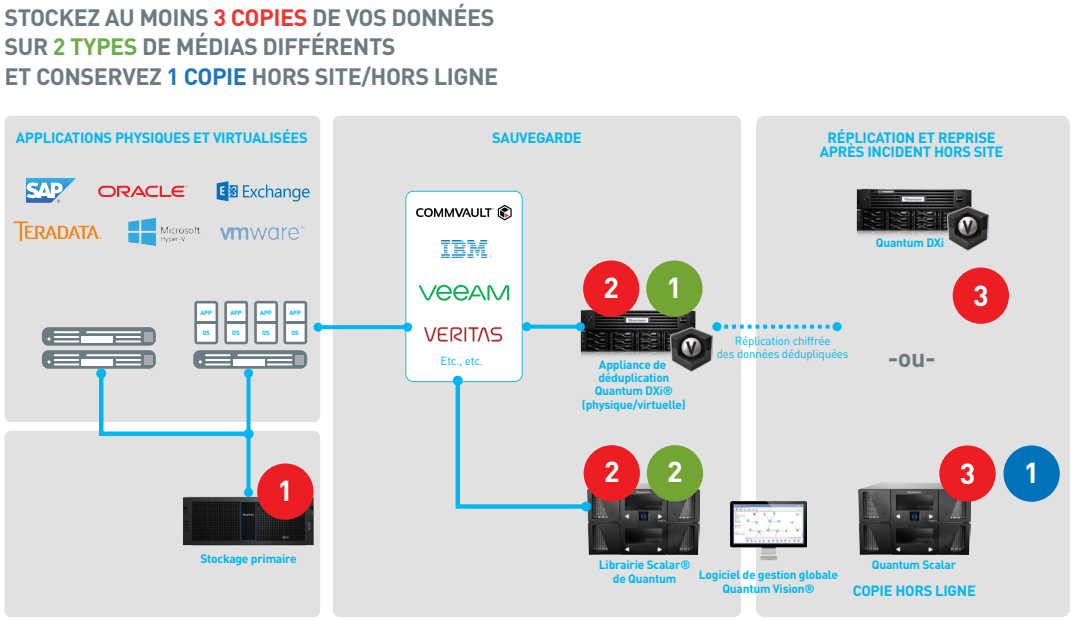
La conservation d'une copie hors ligne des données est un moyen pragmatique de renforcer sa stratégie de sauvegarde. Votre dernière ligne de défense doit être une sauvegarde hors ligne. Le stockage sur bande constitue l'une des meilleures solutions dans ce domaine. Il est économique, portable… et hors ligne, donc.

Les autres solutions incluent les technologies de réplication et les snapshots de stockage. Toutefois, elles ne sont pas totalement hors ligne. Elles sont simplement « hors bande » par rapport à la propagation en temps réel.

Les bandes constituent la dernière ligne de défense tout simplement parce que les pirates ne peuvent ni supprimer, ni chiffrer des données inaccessibles via le réseau.

Pour une protection complète de vos données contre les ransomwares, vous devez en premier lieu empêcher l'infection, puis effectuer des sauvegardes régulières selon la règle du « 3-2-1 », en répliquant les données sur des médias hors site et hors ligne comme les bandes.

Si vous êtes victime d'un ransomware, consultez le site www.nomoreransom.org afin de savoir s'il existe un outil de déchiffrement disponible pour le logiciel ayant servi à l'attaque.



Exemple de règle du « 3-2-1 » de Quantum

La règle du « 3-2-1 » de Quantum

Les solutions exclusives de stockage multiniveau de Quantum optimisent la disponibilité et les performances des systèmes de production tout en réduisant les coûts de stockage. Au cœur de notre solution se trouve l'appliance de déduplication DXi. Physique ou virtuel, le DXi utilise une technologie brevetée de déduplication à partir de blocs de taille variable pour optimiser la réduction des données et les gains de bande passante réseau, sans transiger sur les performances de sauvegarde et de restauration. Le logiciel DXi® permet des sauvegardes rapides et la prise en charge de fonctionnalités avancées comme Commvault Continuous Data Replicator (CDR), ou encore la duplication optimisée simultanée qui accélère la réplication pour les utilisateurs de Veritas Netbackup. Le logiciel DXi prend également en charge Veeam Data Mover Service (VDMS) pour gérer les tâches nécessaires à l'exécution de sauvegardes complètes, incrémentielles et complètes synthétiques. Il libère par conséquent des ressources pour les serveurs de sauvegarde Veeam, le réseau et le stockage primaire, tout en maximisant la réduction des données à l'aide d'une appliance de déduplication des données à partir de blocs de taille variable (référentiel prêt pour Veeam). Nos clients bénéficient ainsi de fonctions de sauvegarde, de réplication et de restauration rapides, tout en conservant les avantages de la déduplication des sauvegardes.

- Le DXi peut répliquer les données vers d'autres appliances DXi ou vers le Cloud, et aussi les transférer sur bande.
- La création de copies de sauvegarde hors ligne sur bande est le moyen le plus efficace de protéger vos données contre les attaques de ransomware.
- Le coût de la bande par pétaoctet (sur trois ans) est huit fois inférieur à celui du disque. De plus, avec une durée de vie de 30 ans, il s'agit du meilleur média pour la rétention longue durée.

Quantum offre des produits de stockage sur bande exclusifs pour de nombreux environnements d'applications de sauvegarde, notamment la fonctionnalité « Path to tape » pour les environnements Veritas NetBackup ou encore notre nouvelle solution convergée sur bande pour environnements Veeam qui élimine le recours à un serveur de bandes Veeam physique.

Dans tous les cas, les produits de stockage sur bande Scalar® de Quantum offrent la meilleure densité de stockage au coût le plus bas, évoluent en toute simplicité et intègrent les diagnostics proactifs Scalar iLayer™ pour faciliter la gestion des bandes.

Pour plus d'informations, rendez-vous sur le site www.quantum.com/fr
ou appelez le +33 (0)1 41 43 49 00.

Quantum®

À PROPOS DE QUANTUM

Quantum est un expert mondial en solutions de stockage multiniveau « scale-out », d'archivage et de protection des données, qui permettent de capturer, de partager et de protéger les contenus numériques tout au long du cycle de vie des données. Plus de 100 000 entreprises de toutes tailles font confiance à Quantum pour leurs besoins les plus pointus de gestion des workflows de contenu. L'infrastructure de stockage multiniveau « end-to-end » de Quantum aide les clients à optimiser la valeur de leurs données en les rendant accessibles à tout moment et en tout lieu, et en les conservant pendant une durée illimitée, tout en réduisant le coût total et la complexité du stockage. Découvrez comment en visitant **www.quantum.com/customerstories**.

www.quantum.com/fr • +33 (0)1 41 43 49 00

Quantum®

© 2018 Quantum Corporation. Tous droits réservés.

WP00221F-v03 Août 2018