VERITAS

Résilience contre les ransomwares : les risques liés à une attaque et les avantages de la planification de la reprise

Un aperçu de l'histoire des ransomwares, leur impact potentiel et les bonnes pratiques pour protéger les systèmes informatiques.

Livre blanc Veritas™ | Mars 2020

Sommaire

Synthèse 3

Introduction 3

L'aspect économique du ransomware 3

Les cinq phases du chiffrement de ransomware 4

Définition des bonnes pratiques de sauvegarde et de restauration pour votre organisation 5

Augmentation de la résilience contre les ransomwares avec Veritas NetBackup 5

Conclusion 7

SYNTHÈSE

Les attaques de ransomwares sont en pleine augmentation. Selon Cybersecurity Ventures, les ransomwares coûteront plus de 20 milliards de dollars aux organisations dans le monde entier en 2021, et on estime que la cybercriminalité en général aura un impact de 6 mille milliards de dollars. Ces estimations comprennent les coûts associés à la restauration des données et des infrastructures ainsi que les dépenses souvent masquées pour atténuer les dommages sociaux d'une attaque.

Le ransomware constitue la menace de logiciel malveillant grandissant le plus vite dans le monde et l'une de celles qui impactent souvent les organisations de manière catastrophique, à l'origine de la majorité des événements basés sur l'extorsion et causant des milliards de dollars de pertes pour les organisations dans le monde aujourd'hui. Il est capable toutes les organisations utilisant des infrastructures informatiques, qu'elles soient sur site, gérées par un tiers, virtuelles ou dans le cloud.

Les vecteurs d'attaque classiques sont notamment les attaques de phishing, le malvertising et les vulnérabilités inaltérées. Une fois qu'un ransomware réussit à accéder à une organisation, il peut se répandre et corrompre les données sur les systèmes en réseau. Les données vulnérables peuvent comprendre les informations sur les transactions quotidiennes et les données sur les systèmes d'exploitation, les configurations système, les sauvegardes et les données cloud. Lorsque les systèmes sont infectés et que le stockage se retrouve chiffré après une attaque les entreprises ont le choix de payer la rançon, en espérant que leurs données seront préservées, ou de restaurer et reconstruire. Chaque situation comporte des risques car l'accès aux données n'est jamais garanti et il existe la possibilité d'être à nouveau ciblée par des cybercriminels. Selon une enquête de CyberEdge Group, parmi les 38,7 % de participants qui acceptent de payer une rançon, moins de la moitié sont capables de récupérer les fichiers à l'aide des outils fournis.

Heureusement, des systèmes de sauvegarde correctement protégés et sécurisés peuvent être utilisés pour restaurer les données et l'infrastructure dans l'état où elles se trouvaient avant l'attaque de ransomware. Chez Veritas, nous avons soutenu cette approche de récupération avec de nombreux clients NetBackup™, y compris pour une attaque par DoppelPaymer, un ransomware crypto-locker. L'administrateur de l'organisation indiquait que toutes les bandes de la bibliothèque avaient été effacées, mais avec la collaboration de Veritas Support, l'équipe informatique sur site a pu récupérer les données et les infrastructures à partir des sauvegardes protégées. Bien que la solution se soit montrée fructueuse, elle aurait été moins mouvementée si l'entreprise avait eu un plan de reprise testé et fiable pour les attaques de ransomwares, en lien avec des évaluations des risques de sécurité des informations.

INTRODUCTION

Le concept de ransomware a été introduit pour la première fois lors d'une conférence médicale internationale sur le SIDA en 1989, et était connu sous le nom de « cheval de Troie SIDA ». Il a été distribué aux participants via 20 000 disquettes de 5,25 pouces. Les ordinateurs des participants ont été infectés, bien que le virus restait inactif lors des 89 premiers redémarrages de l'ordinateur ; au 90ème redémarrage, un avertissement indiquait que les fichiers avaient été chiffrés et qu'un paiement était requis pour déverrouiller les systèmes. Aujourd'hui, les ransomwares sont beaucoup plus malveillants, et entraînent des coûts économiques et sociaux importants.

Et les effets des ransomwares vont au-delà de la perte de données. L'Owen Graduate School of Management de Vanderbilt University montre que ces violations de données peuvent causer des blessures, voire même la mort. Une étude récente de l'école démontre l'impact important sur les hôpitaux en particulier, avec 36 décès pour 10 000 crises cardiaques qui auraient pu être empêchés si les systèmes n'avaient pas été infectés. Dans une unité de soins intensifs, 2,7 minutes supplémentaires peuvent être nécessaires pour qu'une victime soupçonnée de faire une crise cardiaque puisse recevoir un ECG. Ces 2,7 minutes supplémentaires, additionnées à la redirection nécessaire des patients montrent que les ransomwares peuvent présenter des conséquences mortelles. En Angleterre, l'attaque WannaCry contre le National Health Service (NHS) a forcé l'annulation de milliers de rendez-vous et d'opérations dans cinq hôpitaux régionaux. Quasiment une année a été nécessaire pour évaluer complètement les dégâts causés par l'attaque sur les systèmes et les coûts de santé individuels.

L'ASPECT ÉCONOMIQUE DU RANSOMWARE

L'un des objectifs principaux des cybercriminels consiste à profiter des systèmes infectés. Leur profit dépend fortement de la volonté des victimes des attaques de payer la rançon, une décision souvent guidée par plusieurs facteurs :

1. La gravité de la violation, notamment le nombre et la valeur des applications ou fichiers impactés.
2. La durée d'activité du logiciel malveillant dans l'environnement.
3. L'efficacité des équipes de sauvegarde et de sécurité pour revenir au moment de l'attaque.
4. La capacité à obtenir les codes de déchiffrement pour obtenir à nouveau l'accès aux données.

De plus, il est important de comprendre l'aspect économique du ransomware et la motivation de l'attaquant pour cibler une entreprise en particulier, ce qui peut être représenté par le fait que le montant maximum qu'une victime particulière est prête à payer pour récupérer des fichiers est défini par (vi) la volonté de la personne (i) à payer. Par exemple, une organisation qui évalue les fichiers à 10 000 dollars et fait confiance aux criminels aurait une vi = 10 000, tandis qu'une organisation qui évalue les fichiers à 20 000 dollars et qui a une faible confiance dans le retour de la clé de chiffrement ou qui fait confiance à une restauration par sauvegarde ou assainissement des fichiers pourrait avoir une vi = 0. Le profit peut donc être exprimé par N=Σ Ni=1 (pi-c)1i-F, où N correspond au nombre de personnes attaquées, pi correspond à la rançon demandée à l'organisation I, c correspond au coût de traitement de l'argent de la rançon, 1i est une variable indicatrice qui prend la valeur 1 si pi ⩽ vi et 0 sinon, et F correspond au coût fixe d'exploitation du logiciel malveillant.

Les criminels derrière les ransomwares recherchent des cibles présentant une faible résistance et le retour sur investissement le plus important. Cette formule permet de clarifier : si vi = 0, il n'y a qu'une faible valeur économique à réaliser une attaque étant donné le retour sur investissement limité d'une organisation dotée d'une forte cybersécurité et d'un environnement de sauvegarde renforcé.

L'émergence de la crypto-monnaie est un défi pour les forces de l'ordre en ce qui concerne les ransomwares. La crypto-monnaie Bitcoin a joué un rôle fondamental dans la prolifération des ransomwares, en permettant des transferts d'argent faciles avec une traçabilité limitée. Ces caractéristiques fournissent aux cybercriminels un outil puissant pour profiter de leur criminalité, en utilisant le Bitcoin pour passer outre les mesures de contrôle connues pour tracer, suivre et empêcher le paiement. Le Bitcoin constitue actuellement la crypto-monnaie la plus populaire, mais il existe un flot continu de nouvelles options, et certaines d'entre elles proposent un anonymat complet et une intraçabilité totale, ce qui rend les efforts des forces de l'ordre pour suivre les flux d'argents presque impossibles.

LES CINQ PHASES DU CHIFFREMENT DE RANSOMWARE

On considère généralement qu'il existe cinq phases de chiffrement de ransomware, de l'attaque ou l'infection (Phase 1) d'un environnement d'entreprise à la notification de l'utilisateur/règlement et remédiation (Phase 5). Il existe un ensemble de phases légèrement différent pour les hôpitaux étant donné qu'ils sont excessivement exposés aux ransomwares.

Phase 1 – Infection : la pénétration initiale dans le système par le biais de courriers électroniques de spam, d'attaques de phishing ou d'un kit d'exploitation prêt à l'emploi du Dark Web. Au cours de cette phase, les vulnérabilités des systèmes et des utilisateurs sont exploitées. Les moments d'inattention de l'utilisateur et lors de la formation ainsi que le non respect des politiques de sécurité de l'entreprise permettent l'entrée du ransomware dans l'infrastructure informatique.

Phase 2 – Livraison : les mécanismes de persistance sont établis. Ces mécanismes modifient les clés de registre pour protéger le ransomware, le cacher et permettre un redémarrage automatique, même après un arrêt du système. Cette phase permet au ransomware de chiffrer les fichiers à une date ultérieure sans nécessiter d'action supplémentaire de la part de l'utilisateur ou un centre de commande et de contrôle du ransomware.

Phase 3 – Attaque de sauvegarde : il s'agit d'un mécanisme d'auto-défense pour assurer l'efficacité du ransomware et pour faciliter le paiement. CryptoLocker et Locky, deux variantes de ransomwares, exécutent des commandes pour supprimer tous les clichés instantanés des systèmes infectés. D'autres variantes recherchent les dossiers contenant des fichiers de sauvegarde et les suppriment.

Phase 4 – Chiffrement : lors de cette étape, les clés de chiffrement sont établies sur le système local. Les premières formes de ransomwares comprenaient la clé de chiffrement dans l'application, ce qui facilitait l'identification de la clé et le déchiffrement des informations pour les équipes de sécurité. Aujourd'hui, les clés de chiffrement ne sont pas fournies avec l'application, et le temps de restauration des fichiers varie en fonction des caractéristiques de l'infrastructure informatique telles que la taille des fichiers, les caractéristiques du réseau et le nombre d'appareils connectés.

Phase 5 – Notification de l'utilisateur/règlement et remédiation : le ransomware informe l'utilisateur de l'infection, demande le paiement et présente les instructions pour le paiement. Généralement, l'utilisateur obtient une fenêtre de paiement, avec des pénalités ou une rançon de plus en plus importantes s'il ne paie pas. Après le paiement de la rançon, le ransomware essaie souvent de supprimer toute trace de sa présence qui pourrait être identifiée par des enquêteurs.

Avec le cheval de Troie SIDA, l'algorithme de chiffrement était primitif et les professionnels de la sécurité ont pu remédier au problème rapidement. Avec le temps, les ransomwares sont devenus de plus en plus sophistiqués, avec des techniques de codage améliorées comprenant une combinaison de chiffrement traditionnel au secret partagé utilisant des algorithmes rapides, tels que le Triple Data Encryption Algorithm et les Advanced Encryption Standards, ainsi qu'un système à clé publique qui chiffre la clé de chiffrement afin qu'elle ne puisse pas être trouvée. Cette méthodologie présente deux possibilités :

1. Utiliser un système de commande et de contrôle pour fournir la clé publique à utiliser pour chiffrer la clé de chiffrement au secret partagé.
2. Intégrer la clé publique dans l'application elle-même.

Dans le premier cas, le chiffrement ne peut pas être complètement sécurisé (par exemple, en chiffrant la clé de chiffrement au secret partagé) jusqu'à ce que le système puisse se connecter au centre de commande et de contrôle, alors que dans le deuxième cas, tous les systèmes attaqués partagent la même clé publique. Une fois que la clé privée est fournie aux utilisateurs qui ont payé la rançon, la clé privée peut alors être partagée pour les autres qui ont été attaqués de la même manière. En fait, les enquêteurs ont découvert que le système est marqué avec un identifiant unique donné à l'utilisateur pour le paiement de la rançon.

DÉFINITION DES BONNES PRATIQUES DE SAUVEGARDE ET DE RESTAURATION POUR VOTRE ORGANISATION

Avoir une solution fiable de sauvegarde et de restauration est l'étape la plus vitale pour construire un plan de prévention fiable contre les ransomwares. Aujourd'hui, les entreprises se reposent souvent sur plusieurs paradigmes de sauvegarde, y compris la sauvegarde traditionnelle ainsi que la réplication et la protection des données continue (CDP). Chacune de ces méthodes est importante pour créer des copies de données et, dans le cas de la réplication, pour déplacer les copies vers un stockage local ou distant, un avantage notable dans l'effort pour créer une distance, ou un vide, entre les données de sauvegarde et le réseau de l'organisation.

Cependant, chaque paradigme de sauvegarde a ses avantages et ses inconvénients que les organisations doivent prendre en compte lors du développement d'un plan de reprise face aux ransomwares. Avec la réplication, les données sont souvent répliquées en temps réel, ce qui réplique le virus ransomware dans le processus. En définissant la fréquence, l'heure et les paramètres de stockage pour la réplication tout en étant guidé par l'objectif de protéger les données en cas d'attaque, les organisations peuvent assurer l'existence d'une version fiable et déconnectée du réseau des données de sauvegarde.

La CDP permet la restauration de fichiers à un instant T et basée sur la version en prenant des snapshots périodiques ou à des moments programmés, ce qui permet aux organisations de revenir à un moment antérieur à l'attaque par le ransomware. La CDP présente l'inconvénient d'utiliser un espace de stockage sur disque important en raison du nombre de snapshots gérés, bien que cela ne soit qu'un faible prix à payer pour être prêt en cas de reprise après une attaque de ransomware.

Les organisations gagnent également à fixer un RPO (perte de données maximale admissible) et un RTO (durée maximale d'interruption admissible). Le RPO définit la tolérance de perte de l'entreprise, ou la quantité de données qui peut être perdue avant que les dégâts causés à l'entreprise ne soient trop importants. L'objectif est exprimé sous la forme d'une mesure de temps entre l'événement de perte et la dernière sauvegarde réalisée. Le RTO désigne le temps d'arrêt maximal d'une application sans dégâts trop importants pour l'entreprise. Certaines applications peuvent subir une interruption pendant plusieurs jours sans qu'il n'y ait de conséquences trop importantes, mais beaucoup ne le peuvent pas. Ces deux unités jouent un rôle important dans le développement d'une base à partir de laquelle une organisation peut construire un plan de reprise après une attaque de ransomware qui répond aux besoins de l'entreprise tout en restant attentif aux réalités informatiques.

AUGMENTATION DE LA RÉSILIENCE CONTRE LES RANSOMWARES AVEC VERITAS NETBACKUP

NetBackup empêche la dévastation potentielle causée par une attaque de ransomware et soutient la restauration des données prête et fiable. Même lorsque les cybercriminels ont ciblé les logiciels et appliances de sauvegarde, NetBackup permet aux utilisateurs de restaurer une copie valide des données à un certain point dans le temps, à des mois voire des années dans le passé, selon la configuration et le taux de rétention.

Avec NetBackup, l'organisation peut utiliser des sauvegardes incrémentielles pour identifier une augmentation soudaine, inattendue du taux de changement, ce qui peut indiquer une attaque de ransomware non détectée. Lorsque le ransomware commence à chiffrer des données sur un système hôte et sur le réseau, il modifie ces fichiers. NetBackup suit les métadonnées de sauvegarde au fil du temps, et ces données peuvent être analysées et comparées aux motifs de l'historique pour soutenir la détection précoce d'une attaque de ransomware, voire pour informer les administrateurs de sauvegarde et de sécurité du changement.

Voici comment votre organisation peut utiliser NetBackup pour construire un plan robuste de reprise après une attaque de ransomware :

1. **Sécurisez l'accès physique au serveur de production NetBackup et/ou à l'appliance :** la sécurité physique du serveur de sauvegarde est la première ligne de défense pour protéger les sauvegardes. Limitez l'accès physique à l'environnement du serveur de sauvegarde, et si possible, séparez votre environnement de sauvegarde de votre environnement de production.

2. **Renforcez et protégez les serveurs maîtres NetBackup :** limitez fortement l'accès aux serveurs maîtres NetBackup. Mettez en place un chiffrement de sécurité et centré sur l'organisation pour fournir une protection pour les opérations NetBackup sur les serveurs maîtres NetBackup, les serveurs média et les clients attachés.

3. **Sécurisez les voies de communication et les ports :** Veritas recommande d'utiliser les réglages par défaut du numéro de port pour les services NetBackup et les ports de service Internet. Il peut également être nécessaire de mettre en place des règles IPsec, telles que le blocage des connexions du client de sauvegarde à un serveur non autorisé et des connexions entrantes d'un client non autorisé au serveur de sauvegarde, pour réduire la probabilité d'un accès aux données par le ransomware via un serveur client.

4. **Protégez et sécurisez les nœuds clients :** sécurisez les nœuds clients et soumettez les à des audits et des analyses de sécurité de manière régulière. Sur les systèmes critiques, les audits devraient inclure l'analyse des journaux, la taille des fichiers et le taux de changement incrémentiel.

5. **Gérez les correctifs de sécurité et les alertes :** Veritas a développé le logiciel NetBackup et les appliances NetBackup avec la sécurité comme objectif de conception principal. Nous testons chaque élément de l'appliance, y compris son système d'exploitation Linux et l'application centrale NetBackup, à la recherche de vulnérabilités en utilisant les normes industrielles et des produits de sécurité avancés. Ces mesures minimisent l'exposition aux accès non autorisés et les pertes ou vols de données conséquents.

   Nous analysons chaque nouvelle version de logiciel et de matériel NetBackup ou d'appliance NetBackup à la recherche de vulnérabilités avant son lancement. Selon la gravité des problèmes trouvés, Veritas sort un correctif ou fournit une correction dans une version planifiée. Pour réduire le risque de menaces inconnues, Veritas met régulièrement à jour les packages tiers et les modules du produit dans le cadre de cycles réguliers de versions de maintenance.

6. **Testez votre plan de reprise après incident :** le test de la reprise après incident est nécessaire pour sécuriser un environnement de sauvegarde. Pour confirmer la préparation pour un ransomware, il est important de tester régulièrement le basculement en cas de catastrophe et/ou de faille de sécurité, ainsi que les restaurations.

7. **Récupérez après les fuites de données :** la fuite de données désigne le transfert d'informations confidentielles ou sensibles vers des systèmes, des individus, des applications ou des médias non certifiés ou non autorisés, comme le transfert d'enregistrements financiers chiffrés vers un client de messagerie électronique non autorisé. Les fuites de données deviennent de plus en plus courantes car la tendance croissante au partage d'informations a affaibli les contrôles d'accès. Lorsque les fuites de données sont associées au faible niveau de conscience de l'utilisateur final en matière de sécurité, aux réseaux non gérables et à des politiques de données mises en œuvre de manière incorrecte, les organisations pavent la route pour les ransomwares. Il est important de gérer l'accès basé sur le rôle à NetBackup pour renforcer le serveur maître NetBackup et protéger les données auxquelles il accède.

8. **Réalisez des audits, des vérifications et des formations de sécurité fréquents :** il est difficile de surestimer la valeur des audits fréquents et des formations de sécurité. Les ransomwares infectent généralement les environnements d'entreprise via l'activité humaine, souvent répandus par les courriers électroniques de phishing ou les téléchargements furtifs qui peuvent survenir lorsqu'un utilisateur visite un site web infecté. La formation constante des employés et les audits fréquents des systèmes aident à réduire le risque d'attaques de ransomware.

9. **Assurez la protection des systèmes critiques pour le serveur de sauvegarde :** toutes les appliances Veritas comportent une protection des systèmes critiques, ce qui fournit une sécurité contre l'installation de fichiers exécutables non autorisés.

CONCLUSION

Les ransomwares représentent une menace sérieuse aux organisations d'aujourd'hui basées sur les données, avec des conséquences économiques et sociales potentiellement graves. Bien que certains puissent considérer la sauvegarde et la restauration comme les dernières lignes de défense contre les ransomwares, il est plus juste de les considérer comme une partie importante de la planification stratégique proactive. Une stratégie de sauvegarde et de restauration fiable et testée minimise les risques de votre entreprise et de ses systèmes et vous apporte la confiance dont vous avez besoin pour réussir face à une attaque de ransomware, en assurant la disponibilité des données et la continuité des affaires.

À PROPOS DE VERITAS

Veritas Technologies est un leader mondial de la protection et de la disponibilité des données. Plus de 50 000 entreprises, dont 99 des entreprises du classement Fortune 100, nous font confiance pour faire abstraction de la complexité informatique et simplifier la gestion des données. La plate-forme Enterprise Data Services automatise la protection et orchestre la récupération des données partout où elles se trouvent, garantit la disponibilité des applications critiques, 24 h/24 et 7 j/7, et fournit aux entreprises les informations dont elles ont besoin pour se conformer à une réglementation en constante évolution. Réputée pour sa fiabilité à grande échelle et son modèle de déploiement adapté à tous les besoins, Veritas prend en charge plus de 500 sources de données et plus de 150 cibles de stockage, dont 60 clouds. Pour en savoir plus : www.veritas.com/fr Suivez-nous sur Twitter : @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com/fr

Vous trouverez sur notre site web les adresses et numéros de téléphone de nos agences locales.
www.veritas.com/fr/fr/company/contact

V1004 03/20