Livre blanc

Protéger le talon d'Achille hautement exploitable des données de sauvegarde

Avec InfiniGuard® et InfiniSafe® d'Infinidat

par Marc Staimer

2022

Constat

Les ransomwares sont devenus la plus grande menace pour toute organisation informatique, quelle que soit sa taille. Cela représente plus de 60 % des reprises après sinistre selon une enquête de Dragon Slayer Consulting auprès de plus de 300 fournisseurs de services gérés (MSP) de type Backup as a Service (BaaS) et Disaster Recovery as a Service (DRaaS). Et ce chiffre est en augmentation par rapport aux 50 % enregistrés un an plus tôt. Or, lorsque les hébergeurs constatent une augmentation rapide des attaques ransomware dans leur base de clients, il est raisonnable de penser qu'il en va de même pour les entreprises non-clientes.

Ce constat est validé par les études de marché actuelles. Ces statistiques sont fournies à l'Annexe A.

Les attaques ransomware augmentent radicalement le niveau d'anxiété des DSI les plus optimistes. Les ransomwares ont évolué au point d'échapper aux défenses backend les plus courantes telles qu'une sauvegarde saine et robuste, un stockage immuable et des snapshots immuables. Le problème posé est considérable. Il est pratiquement impossible de se remettre d'une attaque par ransomware sans payer la rançon s'il n'y a pas de bonnes sauvegardes connues. Ce n'est pas bon.

Les professionnels de la cybersécurité recommandent systématiquement une approche à plusieurs niveaux de la cyberdéfense. Ces recommandations se concentrent généralement sur la porte d'entrée et comprennent des pare-feu, des scanners anti-malware sur les points de terminaison et les serveurs, une inspection approfondie des paquets, une heuristique comportementale des données internes, des VPN, une formation poussée du personnel et une sauvegarde robuste et récente des données.

Les cybercriminels ne sont pas stupides. Ils connaissent tout cela. Il leur est facile de contourner la porte d'entrée en exploitant les faiblesses humaines par un hameçonnage ciblé. Une campagne de

phishing simulée par la société de sécurité logicielle F-Secure[1] a révélé pourquoi ces attaques demeurent omniprésentes. Plus d'un cinquième des destinataires des e-mails de hameçonnage simulés, censés provenir de leurs ressources humaines, ont cliqué sur le lien. Étonnamment, les personnels techniques ont été plus enclins à le faire. C'est ainsi que la plupart des ransomwares passent la porte d'entrée.

Une fois la première machine infectée, ils utilisent des outils pour échapper aux analyses antivirus, puis exploitent les privilèges volés de la machine infectée pour propager l'infection. Ils répètent ensuite l'ensemble de l'opération pour chaque machine infectée. Notez que l'infection n'est pas la même chose que la détonation. Une détonation se produit lorsque le ransomware amorce le processus de chiffrement.

Une fois que l'infection s'est propagée aussi loin que possible, les dernières générations de ransomwares sont capables de lancer une mission de recherche et de destruction pour détruire ou corrompre les sauvegardes. C'est ainsi qu'est apparue une nouvelle couche de défense dans le stockage backend où sont stockées les données de sauvegarde, appelée communément « stockage immuable ». Le stockage immuable signifie que les données stockées sur un volume, un partage de fichiers ou un bucket d'objets ne peuvent pas être modifiées ni supprimées pendant une période déterminée appelée période de conservation. Cette pratique a été adoptée comme couche de défense contre les ransomwares.

Cependant, les cyber-escrocs ont trouvé une solution de contournement. À l'instar du phishing ciblé destiné à infecter l'organisation, ils utilisent des techniques sophistiquées similaires pour compromettre les informations d'identification et les privilèges des administrateurs de sauvegarde et de stockage. Cela leur permet de modifier la période de conservation des sauvegardes. Par exemple, une période de conservation de trois mois est réduite à trois heures, un délai suffisant pour que les administrateurs puissent valider l'exécution des sauvegardes, des instances dupliquées ou des snapshots, puis pouf… tout disparaît, et personne ne le remarque. Ensuite, le ransomware explose.

Ce n'est pas la seule évolution des ransomwares. Rappelez-vous les capacités des dernières versions : infecter, se cacher, se propager. Le ransomware est également sauvegardé, répliqué et capturé comme le reste des données. Autrement dit, il est intégré aux sauvegardes, aux instances dupliquées et aux snapshots. Donc, comme il est toujours présent, il infecte et explose à nouveau dès la récupération. Cela devient une attaque en boucle. Le ransomware explose. L'organisation informatique effectue une récupération à partir de ce qu'elle croit être une sauvegarde saine. Le ransomware explose à nouveau. Nouvelle récupération et on recommence.

L'organisation n'a aucune idée de la date de la dernière sauvegarde saine. Elle doit alors calculer la quantité de données qu'elle peut se permettre de perdre - des jours, des semaines, des mois ? Ou payer la rançon. La plupart finissent par payer. Mais la totalité des données n'est pas récupérée pour autant. Il est assez courant que le cyber-criminel ne déchiffre pas immédiatement toutes les données sensibles ou de valeur. Il demandera une autre rançon pour le reste des données. N'oublions pas que sont des cybercriminels.

Une autre innovation du ransomware est la double-extorsion. Le ransomware copie les données sensibles avant de les chiffrer. Les cybercriminels menacent de divulguer les données si la rançon n'est pas payée. Même en cas de paiement, ce sont des cybercriminels. Ils vendent fréquemment ces données sur le dark web à des organisations qui se les arrachent.

Qu'en est-il de la cyberassurance ? La cyberassurance indemnise rarement à hauteur de la totalité de la rançon. L'explosion des attaques ransomware et l'augmentation du montant des rançons ont fait monter en flèche les primes de cyberassurance. Les compagnies d'assurance se doivent de gagner de

[1] Dark Reading phishing analysis

l'argent, pas d'en perdre. Elles sont devenues beaucoup plus pointilleuses quant aux personnes qu'elles assurent, aux dommages couverts, aux protections que l'assuré doit mettre en place et au montant des indemnisations versées.

Tout cela nous ramène au constat de départ : les organisations informatiques doivent fournir des couches de défense contre les évolutions des ransomwares afin de limiter au maximum les dommages causés. C'est le talon d'Achille facilement exploitable des données de sauvegarde. La question est de savoir comment empêcher les ransomwares de les exploiter.

Table des matières

Comment protéger les données de sauvegardes, un talon d'Achille facilement exploitable

Cela commence par une ingénierie inverse des processus mis en œuvre dans la conception des dernières variantes de ransomware et par la mise en place de multiples barrières sur leur chemin. Ce que recommandent les experts de la cybersécurité pour la porte d'entrée doit être également appliqué aux données de sauvegarde, c'est-à-dire à la porte arrière. En d'autres termes, mettre en place une défense multicouche pour la porte arrière. Ces défenses doivent protéger contre différentes attaques. Pour certaines d'entre elles, ce seront des produits, des fonctionnalités ou des services. Pour d'autres, des processus et des produits.

Exigences en matière de défense multicouche contre les ransomwares

Le stockage des données de sauvegarde doit fournir une protection contre les trois attaques ransomware, à savoir la suppression, l'altération ou la corruption des sauvegardes, des instances dupliquées ou des snapshots, le vol des privilèges d'administration du stockage et la détection des ransomwares intégrés dans les sauvegardes, les instances dupliquées ou les snapshots.

1. *Défense contre la destruction des sauvegardes, des instances dupliquées ou des snapshots par les ransomwares*

Les ransomwares recherchent activement les sauvegardes et les détruisent. Ils repèrent les dépôts de sauvegarde connus, les instances dupliquées et les snapshots pour les supprimer, les modifier ou les corrompre. Des défenses efficaces nécessitent :

- Un stockage immuable ou des snapshots immuables. L'immuabilité signifie que les données ne peuvent pas être supprimées ni modifiées.
- L'immuabilité est liée à la politique de conservation. (Conserver toutes les sauvegardes indéfiniment est irresponsable, tant sur le plan opérationnel que financier. Les sauvegardes ne sont pas des archives mais des substituts coûteux qui n'en ont pas les avantages).

2. *Défense contre le vol de privilèges d'administrateur de stockage par les ransomwares*

Les ransomwares ciblent activement l'administrateur disposant de privilèges de conservation pour copier et voler ces privilèges. Ils s'en servent ensuite pour modifier la période de conservation en heures avant la suppression automatique, faisant ainsi disparaître les sauvegardes. Des défenses efficaces nécessitent :

- Une authentification multifacteur (MFA) pour toute action qui affecte les données ou la période de conservation, désignée également par MFA en profondeur (Deep MFA) ou MFA par étapes (Step-Up).
- La MFA doit être exécutée sur un appareil distinct, qui utilise de préférence la reconnaissance biométrique comme l'empreinte digitale ou la reconnaissance faciale.

3. *Défense contre les ransomwares intégrés aux sauvegardes, instances dupliquées et snapshots*

Les ransomwares restent en sommeil pendant des mois et sont sauvegardés chaque jour avec le reste des données. Lorsque le ransomware explose, toutes les récupérations réinstallent le même ransomware qui explose encore et encore. Des défenses efficaces nécessitent une combinaison de produits et de processus :

- Les sauvegardes, les instances dupliquées ou les snapshots doivent être récupérés au moins une fois par semaine, dans un environnement logique ou physique hermétique.
- Faites appel aux logiciels de protection des données les plus utilisés du marché.
- L'exécution de ces récupérations exige souvent un stockage très rapide, un très haut débit et une reprise quasi instantanée pour accélérer le processus. Sinon, l'opération devient trop chronophage. Un processus long sera probablement effectué beaucoup moins fréquemment et sera donc moins efficace, en particulier pour les grands comptes. Les logiciels de protection des données utilisent couramment plusieurs machines physiques ou virtuelles pour copier des données à partir de serveurs de production, de points de terminaison, de SaaS, de bases de données, etc. Le stockage cible doit être capable de gérer plusieurs flux simultanés à un débit très élevé, tout en restant abordable et rentable. Il existe de nombreux systèmes de stockage primaire offrant le débit

nécessaire. Mais les coûts excessifs le rendent généralement peu attrayant et non viable en tant que cible pour les logiciels de protection des données.

- La fréquence doit être déterminée par l'objectif de point de récupération (RPO) de cyber-résilience, qui correspond à la quantité de données que l'organisation peut se permettre de perdre.
- Les récupérations doivent ensuite être analysées par le logiciel anti-ransomware sans signature le plus récent.
- Chaque sauvegarde, instance dupliquée et snapshot dont l'état a été vérifié doit être retenu comme sauvegarde adéquate pour la récupération.
- Tout ransomware détecté doit être immédiatement identifié et mis en quarantaine.
- Exploitez ces informations pour supprimer immédiatement ces mêmes infections des systèmes de production compromis.

Solution Infinidat – InfiniGuard® avec InfiniSafe®

Infinidat a modifié en profondeur son système de stockage défini par logiciel primé InfiniBox en le dotant de trois moteurs de déduplication des données (DDE) - dont un destiné à la redondance en cas de panne - et d'une cyber-résilience multicouche. InfiniBox est désormais une appliance de sauvegarde dédiée (PBBA) spécifiquement conçue pour la protection des données dénommée InfiniGuard. La solution a été testée, validée et certifiée avec toutes les suites logicielles de protection des données les plus couramment utilisées telles que Veeam, Commvault, Veritas, Oracle RMAN, IBM Spectrum Protect et NetWorker entre autres.

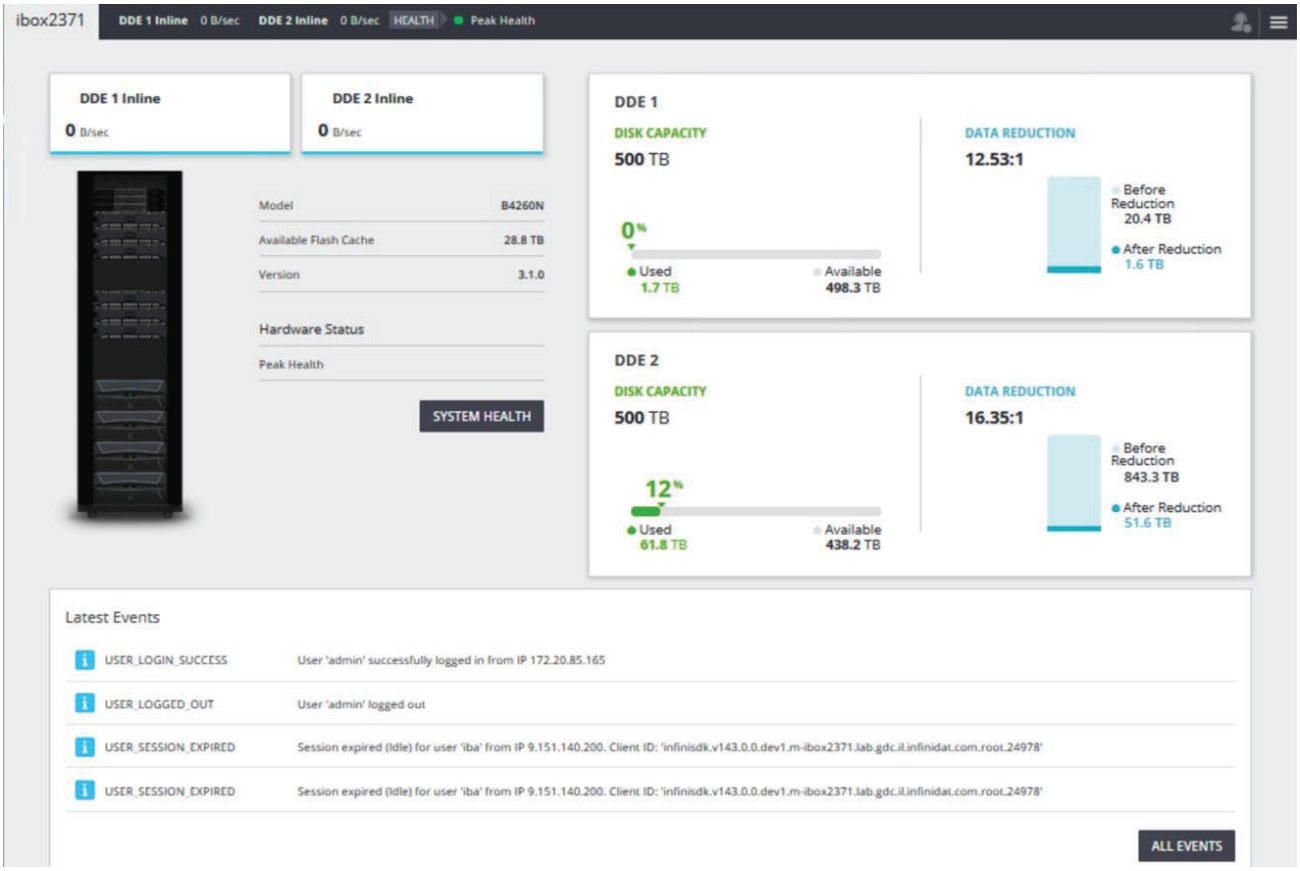
L'un des points forts d'InfiniGuard est la cyber-résilience intégrée d'InfiniSafe, qui est fourni en version standard avec tous les systèmes InfiniGuard sans frais supplémentaires. En remplissant toutes les conditions décrites précédemment, InfiniSafe répond aux exigences de cyber-résilience d'une infrastructure moderne de défense contre les ransomwares. InfiniSafe offre plusieurs couches de défense contre les ransomwares grâce aux composants suivants :

1. Snapshots immuables liés aux règles de conservation, qui capturent les informations complètes de sauvegarde du moteur DDE, y compris toutes les configurations, journaux et données. Assure la protection de tous les snapshots à un moment précis (PIT) contre toute modification, suppression, corruption, changement de règle ou autres actions. La protection s'applique également aux partages, dossiers, fichiers, utilisateurs, mots de passe, journaux, configurations réseau et accès aux partages - une fonctionnalité exclusive d'InfiniSafe. En outre, la déduplication haute performance et la technologie WORM faible consommation(write once, read many) minimisent la capacité consommée, contribuant ainsi à réduire les coûts.
2. Authentification multifacteur profonde (Deep MFA) pour toute modification que l'administrateur tente d'effectuer, déjouant ainsi le vol de privilèges par les ransomwares.
3. Récupération : protection logique de type "air-gapped/sécurisé et fermé pour s'assurer que les sauvegardes peuvent être analysées, testées et validées sans crainte que le ransomware ne s'échappe vers d'autres machines. Le tout dans un seul système hautement résilient. Pour fournir un isolement logique hermétique de l'environnement, la plupart des autres PBPA ou systèmes de stockage cible de sauvegarde nécessitent au moins deux systèmes, soit le double du coût.
4. Performances de débit de premier plan jusqu'à 180 To/h grâce à NetBoost[2] et trois moteurs de déduplication intégrés au système (un pour la redondance et la disponibilité améliorée). Ces performances représentent une capacité d'itération multipliée par deux par rapport à la précédente version d'InfiniGuard. La fenêtre de sauvegarde, essentielle pour les sauvegardes de volumes complets, est ainsi réduite de moitié.
5. Reprises quasi instantanées à grande échelle - pas seulement les fichiers et dossiers MTree - vers un point de récupération validé, quelle que soit la taille. Cela peut représenter jusqu'à 25 Po de données protégées par DDE ou jusqu'à 50 Po par InfiniGuard. Les reprises quasi instantanées sont extrêmement importantes lors de la récupération d'une attaque ransomware. Chaque seconde compte et le temps n'est pas un allié. Les temps d'arrêt sont extrêmement coûteux pour toute organisation. Il est essentiel de les minimiser. Encore faut-il savoir ce que l'on entend par reprises instantanées. Pour la plupart des fournisseurs de protection des données, ce délai peut atteindre 30 minutes. Infinidat vise beaucoup

[2] Logiciel de déduplication à la source d'Infinidat.

moins. Par exemple, la récupération par Infinidat d'une sauvegarde Veeam de 1,5 Po s'effectue en 12 minutes 15 secondes.

La cyber-résilience étendue d'InfiniSafe n'est qu'une partie des composants fournis avec InfiniGuard. InfiniGuard est construit sur les technologies éprouvées en production d'InfiniBox et InfiniBox SSA. La solution intègre les performances sans compromis, la configuration et les systèmes de gestion, des opérations et de contrôle intuitif d'Infinidat, ainsi que son interface utilisateur instinctivement simple, Le tout pour un coût total de possession très faible (TCo)[3]. Voici un exemple du tableau de bord de l'UI intuitive d'InfiniGuard.



Informations système affichées sur le tableau de bord d'InfiniGuard :

- Débit actuel.
- Taux d'opérations E/S actuel. État opérationnel
- État opérationnel InfiniGuard. En dehors du démarrage du système, celui-ci doit toujours être Actif.
- Modèle InfiniGuard.
- Quantité de cache flash du système.
- Version logicielle installée sur le système.
- Indicateurs visuels et textuels sur l'état des composants matériels du système.
- Quantité de capacité utilisée par rapport à la capacité utilisable disponible.
- Liste déroulante des derniers événements système.

Tous ces éléments auraient peu d'utilité si InfiniGuard était trop complexe à utiliser. C'est tout le contraire. Infinidat intègre une automatisation intuitive. De nombreuses tâches manuelles classiques des PBBA ont disparu. Les snapshots immuables sont automatisés avec la fonctionnalité avancée « Set & Forget It ». Il n'y a pas de groupes RAID à créer ou à gérer. Que ce soit le basculement du moteur DDE, les snapshots immuables ou l'isolement hermétique logique, tout se fait d'un clic ou par un « bouton ». En

[3] Infinidat ne facture pas de frais de licence supplémentaires pour InfiniSafe. Il fait partie intégrante d'InfiniGuard. La déduplication haute performance avec WORM réduit les besoins en capacité, ce qui diminue le coût total de possession.

d'autres termes, l'utilisation de l'ensemble des fonctionnalités d'InfiniGuard n'exige aucune formation, compétence ni expertise particulière.

lnfiniGuard est reconnu pour son niveau exceptionnel de disponibilité et de fiabilité. Il est conçu selon la norme Enterprise de redondance complète au niveau du système. Il offre une protection contre la corruption silencieuse des données de bout en bout. Il est possible de créer une instance dupliquée de site à site pour un deuxième module lnfiniGuard.

lnfiniGuard possède les meilleurs atouts en matière de cyber-résilience et de reprise après sinistre.

Résumé et conclusion

Les ransomwares sont le fléau technologique du début du 21e siècle. Ils représentent désormais une entreprise de plusieurs milliards de dollars dont les bénéfices sont réinvestis dans la recherche et le développement. Les ransomwares continuent d'évoluer et de nouvelles variantes émergent en permanence. Les cybercriminels sont implacables et sans remords. Les pros de l'informatique le sont aussi. Ne pas se défendre efficacement est une négligence fiduciaire.

Aujourd'hui, il n'existe pas de produits ou de services magiques capables de garantir une protection à 100 % contre les ransomwares, et il n'y en aura probablement jamais. Aucun bouclier n'est impénétrable. La clé de la protection des données de l'organisation est une défense en profondeur, c'est-à-dire une défense en couches. L'objectif est de faire en sorte qu'il soit plus difficile et beaucoup plus complexe pour les cybercriminels d'obtenir une rançon des organisations lT qui disposent d'une défense en couches que de celles qui n'en disposent pas. Ils empruntent le plus souvent le chemin de la moindre résistance.

Pour assurer cette défense en couches, il faut désormais rendre difficiles, voire impossibles, la suppression, la modification ou l'altération des sauvegardes, des instances dupliquées ou des snapshots. Cela signifie se défendre contre le vol de privilèges d'administrateur permettant de contourner les délais de conservation du stockage immuable. Cela signifie également se défendre contre les infections de ransomwares dormants intégrés dans les sauvegardes, les instances dupliquées ou les snapshots pour empêcher les récupérations.

lnfinidat a prouvé sa capacité de défense à maintes reprises avec le PBBA lnfiniGuard et le module lnfiniSafe intégré. La solution dispose de snapshots immuables combinés à une authentification multifacteur qui empêche les cybercriminels de supprimer, de modifier, d'altérer, de corrompre ces snapshots immuables ou de changer leurs périodes de conservation. Le réseau logique à isolement hermétique et analyse forensique, combiné aux reprises quasi instantanées, permet d'installer les snapshots et de les analyser pour la recherche de ransomwares, ce qui empêche le sabotage par infection intégrée.

Dans l'environnement actuel de ransomwares très agressifs, la solution lnfiniGuard avec lnfiniSafe intégré d'Infinidat constitue une défense multi-couche très efficace et un bouclier contre le talon d'Achille facilement exploitable des données de sauvegarde.

Pour en savoir plus sur InfiniGuard

Visitez : Infinidat InfiniGuard und InfiniSafe

Article sponsorisé par Infinidat. **À propos de DSC** : Marc Staimer, en tant que président et CDS de Dragon Slayer Consulting à Beaverton OR depuis 1998, est bien connu pour sa compréhension approfondie et pointue des problèmes des utilisateurs, notamment en matière de stockage, de mise en réseau, d'applications, de services cloud, de protection des données et de virtualisation. Marc a publié des milliers d'articles et de conseils technologiques du point de vue des utilisateurs pour des sites marchands en ligne de renommée internationale, dont de nombreux sites Web Searchxxx.com de TechTarget, Wikibon, Network Computing et GigaOM. Marc est également l'auteur de centaines de livres blancs, webinaires et séminaires pour le compte de nombreux géants de l'industrie tels que Brocade, Cisco, DELL, EMC, Emulex (Avago), HDS, HPE, LSI (Avago), Mellanox, NEC, NetApp, Oracle, QLogic, SanDisk, Toshiba et Western Digital. Il a également fourni des services similaires à des fournisseurs et startups moins connus, entre autres Asigra, BrainChip, Cloudtenna, Clustrix, Condusiv, DH2i, Diablo, FalconStor, Gridstore, ioFABRIC, Nexenta, Neuxpower, NetEx, NoviFlow, Pavilion Data, Permabit, Qumulo, SBDS, StorONE et Tegile. Ses conférences sont toujours très suivies, en raison des informations pragmatiques et immédiatement exploitables qu'il délivre. Marc peut être contacté à marcstaimer@me.com, (503)-312-2167, in Beaverton OR, 97007.

Annexe A: Statistiques inquiétantes compilées par Varonis sur les ransomwares

Statistiques générales

- Les logiciels malveillants restent la menace la plus importante. (Datto, 2019)
- Les emails malveillants ont augmenté de 600% à cause de COVID-19. (ABC News, 2021)
- 37 % des entreprises interrogées ont été affectées par des attaques ransomware au cours de l'année dernière. (Sophos, 2021)
- En 2021, le plus gros paiement de ransomware a été effectué par une compagnie d'assurance à hauteur de 40 millions de dollars, établissant ainsi un record mondial. (Business Insider, 2021)
- Le montant moyen des rançons demandées est passé de 5 000 dollars en 2018 à environ 200 000 dollars en 2020. (National Security Institute, 2021)
- Les experts estiment qu'une attaque ransomware se produira toutes les 11 secondes en 2021. (Cybercrime Magazine, 2019)
- Environ un e-mail sur 6 000 contient des URL suspectes, notamment des ransomwares. (Fortinet, 2020)
- Le temps d'arrêt moyen d'une entreprise après une attaque ransomware est de 21 jours. (Coveware, 2021)
- 71 % des organisations touchées par un ransomware ont été infectées. La moitié des attaques par ransomware qui réussissent infectent au moins 20 ordinateurs dans l'organisation. (Acronis, 2020)
- Les tactiques les plus courantes utilisées par les pirates informatiques pour mener des attaques ransomware sont les campagnes de phishing par e-mail, les vulnérabilités RDP et les failles logicielles. (Cybersecurity & Infrastructure Security Agency, 2021)
- 65 % des employeurs autorisent leurs employés à accéder aux applications de l'entreprise à partir d'appareils personnels non gérés. (Bitglass, 2020)
- D'après une enquête menée auprès de 1 263 entreprises, 80 % des victimes qui ont versé une rançon ont subi une autre attaque peu après, et 46 % ont pu accéder à leurs données, mais la plupart étaient corrompues. (Cybereason, 2021)
- En outre, 60 % des répondants à l'enquête ont subi une perte de revenus et 53 % ont déclaré que leurs marques en ont souffert. (Cybereason, 2021)
- 29 % des personnes interrogées ont déclaré que leur entreprise avait été contrainte de supprimer des emplois à la suite d'une attaque ransomware. (Cybereason, 2021)
- 42 % des entreprises ayant mis en place des politiques de cyberassurance ont indiqué que les garanties ne couvraient qu'une petite partie des dommages résultant d'une attaque ransomware. (Cybereason, 2021)

Santé

- Plus de 2 100 violations de données dans le secteur de la santé ont été signalées depuis 2009. (Tech Jury, 2021)
- Les organismes de santé ne consacrent qu'environ 6 % de leur budget aux mesures de cybersécurité. (Fierce Healthcare, 2020)
- Les attaques ransomware représentent près de 50 % de l'ensemble des violations de données de santé en 2020. (Health and Human Services, 2021)
- Les attaques dans le secteur de la santé coûtent plus cher que partout ailleurs, soit 408 dollars en moyenne par dossier. (HIPAA Journal, 2020)
- Les attaques ransomware contre les fournisseurs de soins de santé américains ont causé plus de 157 millions de dollars de pertes depuis 2016. (HIPAA Journal, 2020)
- En 2020, 560 établissements de soins ont été touchés par des attaques ransomware au cours de 80 incidents distincts. (Emsisoft, 2021)
- Près de 80 millions de personnes ont été touchées par la brèche Anthem en 2015, la plus grande

violation de données de santé de l'histoire. (Wall Street Journal, 2015)

- Le secteur de la santé a concentré 88 % de toutes les attaques ransomware aux États-Unis en 2016. (Becker's, 2016)
- Rien qu'en septembre 2020, des cybercriminels ont infiltré et volé 9,7 millions de dossiers médicaux. (HIPAA Journal, 2020)

Enseignement

- Les attaques ransomware contre les universités ont augmenté de 100 % entre 2019 et 2020. (BlueVoyant, 2021)
- Le coût moyen d'une attaque ransomware dans le secteur de l'enseignement supérieur est de 447 000 dollars. (BlueVoyant, 2021)
- Depuis 2020, 1 681 établissements d'enseignement supérieur ont été touchés par 84 attaques ransomware. (Emsisoft, 2021)
- 66 % des universités ne disposent pas des configurations de base pour la sécurité des emails. (BlueVoyant, 2021)
- 38 % des universités analysées dans le rapport sur la cybersécurité dans l'enseignement supérieur avaient des ports de base de données non sécurisés ou ouverts. (BlueVoyant, 2021)
- Les cyberattaques contre les établissements du primaire et du secondaire ont augmenté de 18 % en 2020. (K-12 Cybersecurity, 2020)
- Un district scolaire du Massachusetts a payé 10 000 dollars en bitcoins après une attaque ransomware en avril 2018. (Cyberscoop, 2018)

Finance et assurances

- 62 % de tous les dossiers ayant fait l'objet d'une fuite en 2019 provenaient d'institutions financières. (Bitglass, 2019)
- Plus de 204 000 personnes ont subi une tentative de connexion visant à accéder à leurs informations bancaires. (Hub Security, 2021)
- 90% of financial institutions have been targeted by ransomware attacks. (90 % des institutions financières ont été visées par des attaques ransomware. (PR Distribution, 2018)
- Une menace croissante pèse sur les petites institutions financières dont le chiffre d'affaires est inférieur à 35 millions de dollars. (National Credit Union Administration, 2019)
- En 2020, 70 % des 52 % d'attaques ayant visé des institutions financières provenaient du trojan Kryptik. (Hub Security, 2021)
- LokiBot a ciblé plus de 100 institutions financières, engrangeant plus de 2 millions de dollars de revenus. (Hub Security, 2021)
- Les banques ont connu une augmentation de 520 % des tentatives de phishing et de ransomware entre mars et juin 2020. (American Banker, 2020)

Administrations publiques

- En 2020, 33 % des attaques contre des organismes gouvernementaux étaient des ransomwares (Security Intelligence, 2020)
- En juin 2019, une ville de Floride a payé une rançon de 600 000 dollars pour récupérer des fichiers piratés. (CBS News, 2019)
- Seuls 38 % environ des employés des administrations locales et d'État sont formés à la prévention des attaques ransomware. (IBM, 2020)
- Une attaque ransomware contre une ville du Sud en 2020 a coûté plus de 7 millions de dollars. (SC Magazine, 2020)
- Une attaque ransomware a frappé une ville de la côte Est en 2019, causant une perte de plus de 18 millions de dollars. (Baltimore Sun, 2019)

- En 2019, 226 maires de villes américaines dans 40 États ont accepté de négocier avec les cybercriminels pour ne pas payer la rançon. (Hashed Out, 2020)
- En 2019, les attaques contre les municipalités ont augmenté de 60 % par rapport à l'année précédente. (Kaspersky Labs, 2019)
- La principale histoire de cybersécurité en 2019 a été les attaques par ransomware contre les gouvernements étatiques et locaux. (Government Technology, 2019)
- 48 des 50 États américains ont été touchés par au moins une attaque ransomware entre 2013 et 2018. (Bank Info Security, 2019)

Coût des ransomwares

- Le montant des demandes de rançon a augmenté, certaines demandes dépassant le million de dollars. (Cybersecurity & Infrastructure Security Agency, 2021)
- Le coût des attaques ransomware a dépassé les 7,5 milliards de dollars en 2019. (Emsisoft, 2019)
- En 2021, le montant moyen versé par une organisation de taille moyenne était de 170 404 dollars. (Sophos, 2021)
- En mai 2021, un dirigeant a versé aux pirates 4,4 millions de dollars en bitcoins après avoir reçu une demande de rançon. (The Wall Street Journal, 2021)
- Au premier trimestre 2017, FedEx a perdu environ 300 millions de dollars en raison du ransomware NotPetya. (Cyberscoop, 2021)
- Le coût moyen pour se remettre d'une attaque ransomware est de 1,85 million de dollars. (Sophos, 2021)
- Les dommages causés par les attaques ransomware ont dépassé les 5 milliards de dollars en 2017, soit 15 fois le coût de 2015. (Cyber Security Ventures, 2017)
- Les coûts des temps d'arrêt ont augmenté de 200 % par rapport à l'année précédente. (2018 vs 2019). (Datto, 2019)
- Les attaques ransomware entraînent en moyenne 15 jours ouvrables d'inactivité, soit une perte pour les entreprises d'environ 8 500 dollars par heure. (Health IT Security, 2020)
- Le ransomware qui a attaqué une société pétrolière et gazière non identifiée a coûté 30 millions de dollars. (Datto, 2017)
- Le groupe de pirates informatiques à l'origine de l'attaque d'une compagnie pétrolière aurait perçu au total 90 millions de dollars de rançons en seulement neuf mois auprès d'environ 47 victimes. (Fox Business, 2021)
- Quatre fois plus d'entreprises touchées par des attaques de ransomware comptant plus de 100 employés ont déclaré avoir payé des rançons. (Dark Reading survey, 2020)

Tendances et projections

- Le coût total des ransomwares devrait dépasser les 20 milliards de dollars en 2021. (Cybercrime Magazine, 2019)
- Selon Cybersecurity Ventures, le coût des ransomwares devrait atteindre les 6 trillons de dollars par an. (Cybersecurity Ventures, 2020)
- À l'avenir, les organisations seront de plus en plus nombreuses à adopter des modèles de sécurité à confiance zéro en raison de la vulnérabilité des menaces liées à l'identité. (RSA Security, 2020)
- Les travailleurs à distance seront la principale cible des cybercriminels tout au long de l'année 2021. (Security Magazine, 2020)
- Dans 84 % des entreprises, le télétravail restera la norme même après la levée des restrictions COVID-19, ce qui entraînera une augmentation du nombre d'utilisateurs d'Internet et un risque accru d'exposition des données. (Bitglass, 2020)
- À l'avenir, les pirates cibleront les travailleurs à domicile, car les appareils personnels sont plus faciles à pirater que le matériel de bureau. (Security Magazine, 2020)