Ontrack®

Le guide définitif du ransomware

L’épidémie de ransomware

Les intrusions de ransomware ont atteint des proportions épidémiques. D’après une étude menée par la firme Datto, spécialisée dans la cybersécurité et la sauvegarde, parmi les petites et moyennes entreprises, une sur cinq a été victime d’une attaque ransomware en 2019. Les conséquences d’une attaque ransomware peuvent être désastreuses, qu’il s’agisse d’une organisation ne pouvant plus accéder à ses données d’entreprise pendant des semaines, de la suppression de bases de données entières, d’atteintes à la réputation considérables, ou de la perte de confiance des clients.

Cyber Security Ventures affirme qu’en 2019, une nouvelle organisation a été victime d’une attaque ransomware toutes les 14 secondes, et prévoit que d’ici 2021, la fréquence de ce phénomène passera à 11 secondes. En 2018, le FBI a reçu 1493 plaintes relatives à des attaques ransomware, avec des victimes subissant des pertes de 3 621 857 dollars en moyenne, mais ce chiffre prend en compte uniquement les versements de rançons, et non les répercussions financières sur les organisations. La ville d’Atlanta, par exemple, a dépensé environ 2,6 millions de dollars pour récupérer des données à la suite d’une attaque ransomware impliquant une demande de rançon de 52 000 dollars.

En 2019, une entreprise a été victime d’un ransomware toutes les 14 secondes.

PhishMe, leader mondial en solutions de défense contre le phishing, affirme que les attaques ransomware ont connu une hausse de plus de 97 % au cours des deux dernières années, une bonne raison pour les organisations de mettre davantage l’accent sur l’utilisation de sauvegardes complètes et à jour.

Néanmoins, les fichiers de sauvegarde des organisations sont souvent incomplets, négligés, ou dans certains cas, infectés par le même ransomware qui attaque les systèmes principaux. Si une récupération ne peut pas être effectuée au moyen des sauvegardes, d’autres mécanismes incluent certaines techniques de récupération des données telles que les outils de déchiffrement, la récupération des données logiques directement depuis le stockage de l’appareil et l’envoi du support à un laboratoire où des techniciens tentent d’extraire autant d’informations que possible.

Qu’est-ce qu’un ransomware ?

Un ransomware est un type de malware qui empêche les utilisateurs d’accéder à leurs fichiers en les chiffrant, ou par un autre moyen. Lorsque les utilisateurs tentent d’accéder à leurs données, ils reçoivent une notification exigeant le paiement d’une rançon pour obtenir l’accès à celles-ci.

Existant depuis les années 1980, la dernière décennie a vu de nombreux chevaux de Troie de type ransomware faire leur apparition, mais le phénomène s’est surtout accentué depuis l’introduction du Bitcoin. Cette cryptomonnaie permet aux assaillants de collecter les rançons versées par leurs victimes sans passer par les canaux traditionnels.

Combien les attaques ransomware coûtent-elles aux organisations ?

Les chiffres présentés par Datto montrent que les attaques ransomware coûtent aux entreprises 75 milliards de dollars par an en moyenne. Ceci inclut la rançon, les efforts en matière de récupération consécutifs aux attaques, les initiatives organisationnelles et informatiques pour protéger l'organisation contre d'autres attaques, ainsi que les temps d'arrêts, les enquêtes judiciaires, les coûts en formation, les restaurations de données, ainsi que les pertes de revenus et la baisse de productivité.

Des estimations plus prudentes faites par Cybersécurité Ventures situent les dégâts liés aux attaques ransomware à un niveau supérieur à 11,5 milliards de dollars en 2019, ce qui représente une hausse alarmante si l'on compare aux 325 million de dollars d'il y a quatre ans. Qu'il s'agisse de 75 milliards ou de 11,5 milliards de dollars, l'effet est véritablement dévastateur pour ceux qui subissent ces attaques. En mai 2019, par exemple, la ville de Baltimore a été exclue des systèmes du gouvernement pendant plus d'un mois. Les systèmes essentiels pour la production de vaccins, les DAB, les aéroports et les hôpitaux ont tous été touchés. Bien que la demande de rançon ait été de 76 000 dollars seulement, le prix de la récupération s'est élevé à près de 20 millions de dollars.

Qui se trouve derrière les attaques ransomware ?

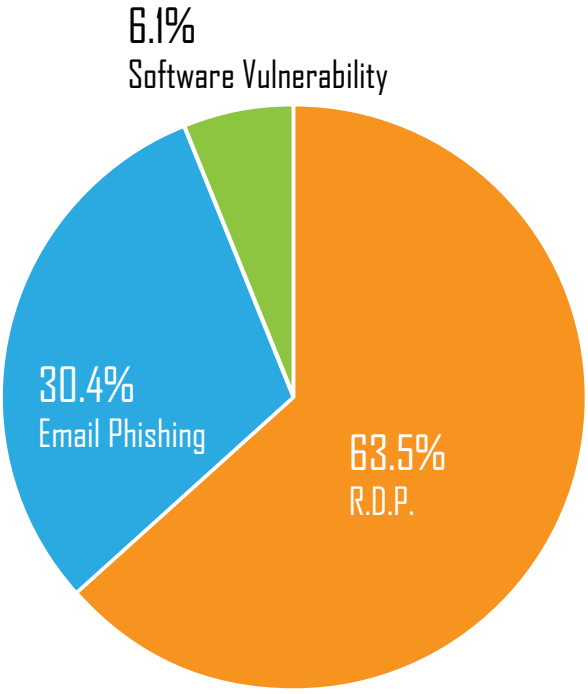
Les personnes derrière les attaques ransomware sont généralement des escrocs hautement qualifiés ayant une expertise en programmation informatique. De façon générale, un ransomware infecte un ordinateur par le biais d'une pièce jointe dans un email, par le réseau, ou par un navigateur infecté.

Comment un ransomware attaque-t-il ?

Spear-Phishing

Le système de diffusion de ransomware le plus courant est un email de phishing contenant une pièce jointe ou un lien. Lorsque l'utilisateur ouvre la pièce jointe ou clique sur le lien, le ransomware exécute un programme qui verrouille le système et affiche une demande de rançon. Lorsque cela se produit, le seul moyen de déchiffrer les données est en utilisant une clé mathématique que seul l'assaillant connaît.

D'autres cas ont été relevés où un malware affiche un message indiquant que le « Windows » de l'utilisateur est verrouillé. L'utilisateur est alors encouragé à appeler un numéro de téléphone « Microsoft » et à entrer un code à six chiffres pour réactiver le système. Le message affirme que l'appel est gratuit, mais ce n'est pas vrai. Tandis que l'utilisateur est au téléphone avec le faux service Microsoft, celui-ci paye le prix d'une communication longue distance.



Source: Coveware - https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

Points d'accès à distance

Les chercheurs McAfee ont observé ceci : tandis que les cybercriminels continuent d'utiliser les tactiques dites de spear-phishing, un nombre croissant d'attaques s'introduisent dans le réseau d'entreprises ayant des points d'accès à distance ouverts et vulnérables, tels que le RDP et le virtual network computing (VNC).

Les identifiants RDP peuvent être obtenus à l'aide d'une attaque par force brute, via des fuites de mots de passe, ou tout simplement achetés sur le marché noir.

Là où les auteurs d'attaques ransomware utilisaient autrefois un environnement de commande et de contrôle pour le ransomware et les clés de déchiffrement, la plupart des malfaiteurs approchent aujourd'hui leurs victimes avec des notifications de rançon contenant une adresse de service email anonyme leur permettant de rester discrets.

Les nouvelles familles de ransomware

D'après le dernier rapport sur les menaces McAfee, au cours du premier trimestre 2019, les attaques ransomware ont augmenté de 118 %. Non seulement une hausse importante du nombre d'attaques a été relevée, mais cette année a également vu l'apparition de nouvelles familles de ransomware et l'utilisation des techniques les plus innovantes par les malfaiteurs pour semer le chaos. Quelques-unes des principales variantes de ransomware ayant causé d'importantes perturbations au cours des années passées sont décrites ci-dessous.

Anatova

L'une des découvertes de 2019 a été le ransomware Anatova. Cette nouvelle famille de ransomware imite l'icône d'un jeu ou d'une application afin de tromper l'utilisateur pour qu'il le télécharge.

Il s'agit d'une sorte de malware extrêmement avancée qui s'adapte rapidement et utilise des techniques de contournement et de diffusion pour empêcher sa découverte. Du fait de sa conception modulaire, il peut intégrer des fonctions supplémentaires lui permettant de contrecarrer les méthodes anti-ransomware. Heureusement, l'équipe McAfee Advanced Threat Research a découvert cette nouvelle famille de ransomware début 2019, avant qu'elle ne devienne une menace importante.

Dharma

Le ransomware Dharma, une variante de CrySiS, est présent depuis 2018, mais les cybercriminels continuent de publier de nouvelles variantes impossibles à déchiffrer.

GandCrab

Un ransomware malicieux qui utilise le chiffrement AES et place un fichier appelé « GandCrab.exe » sur le système. GandCrab cible consommateurs et entreprises ayant des PC fonctionnant avec Microsoft Windows.

Le 31 mai 2019, les cybercriminels à l'origine de GandCrab ont envoyé un message indiquant qu'ils arrêtaient les attaques ransomware avec GandCrab, affirmant qu'ils avaient reçu plus de 2 milliards de dollars de rançons et qu'ils souhaitaient « profiter d'une retraite bien méritée ».

Emotet

Emotet, un cheval de Troie utilisé pour intercepter les identifiants bancaires, a été découvert en 2014. Plus récemment, les cybercriminels l'utilisent pour la diffusion d'autres chevaux de Troie. Il a introduit plusieurs fonctionnalités avancées au cours des années suivantes du fait de sa structure modulaire, telles qu'un module d'installation, un module bancaire et un module DDoS. Emotet est principalement diffusé par le biais d'emails de phishing à l'aide de différentes techniques d'ingénierie sociale.

Ryuk

Ryuk cible en particulier les organisations de grande taille dont le rendement financier est élevé. D'après CrowdStrike, entre août 2018 et janvier 2019, Ryuk a dégagé un revenu net supérieur à 705,80 bitcoins sur 52 transactions, ce qui représente un total de 3 701 893,98 dollars. Il a commencé à faire parler de lui avec son attaque sur les opérations de Tribune Publishing pendant la période de Noël 2018. La société a d'abord cru à une panne de serveur, mais il est très vite apparu qu'il s'agissait d'une attaque du ransomware Ryuk.

La « chasse au gros gibier » est un autre terme pour désigner ce type de ransomware qui cible les grandes entreprises au ROI élevé. Ces attaques à grande échelle impliquent une personnalisation détaillée des campagnes afin d'être le mieux adaptées aux cibles individuelles, augmentant ainsi l'efficacité des attaques. Par conséquent, la « chasse au gros gibier » demande beaucoup plus de travail de la part d'un hacker ; d'autre part, celle-ci est lancée par phases.

Par exemple, la phase un peut être une attaque par phishing ayant pour but d'infecter un réseau d'entreprise avec un malware afin de cartographier le système et d'identifier les actifs majeurs à cibler. Les phases deux et trois seront des attaques en séries avec extorsion et demande de rançon.

Comment prévenir les attaques ransomware

À cause du succès continu du phishing, la formation des utilisateurs est plus que jamais une première ligne de défense contre le ransomware. Des pratiques standards en matière de sécurité et des technologies telles qu'anti-virus, anti-malware, systèmes de détection/prévention des intrusions, pare-feu, surveillance du réseau et contrôles d'accès doivent également être en place.

La formation des utilisateurs est la première ligne de défense contre les ransomwares.

Les organisations doivent fermer tous les ports n'ayant pas besoin d'un accès à Internet, et ceux en ayant besoin doivent être surveillés de près et protégés. Dernièrement, des programmes de machine learning et d'heuristique pouvant analyser le comportement du ransomware, tel que le chiffrement par des programmes non autorisés, sont apparus sur le marché. Appuyé par les renseignements sur les menaces et autres protections, un département informatique vigilant peut limiter la possibilité d'une intrusion

Par ailleurs, d'autres couches de protection telles que les sauvegardes régulières doivent être en place. Ces sauvegardes doivent être complètes, facilement accessibles, et les organisations doivent les tester régulièrement pour vérifier leur fiabilité.

Malheureusement, le ransomware évolue continuellement et trouve de nouveaux moyens d'infecter les systèmes. Parfois, il s'attaque à des systèmes ou à des bases de données spécifiques. Le malware commence souvent par utiliser des droits d'administrateur volés pour désactiver les sauvegardes en ligne, en particulier sur les SAN. Ensuite, le malware supprime les systèmes NAS. D'autres fois, il parvient également à infiltrer et à chiffrer les fichiers de sauvegarde. Les applications de sauvegarde virtualisées telles que Veeam, par exemple, ont été la cible d'attaques ransomware par le passé. Il ne s'agit alors pas de savoir s'il va frapper, mais quand.

Les organisations doivent être préparées. Les bandes laissées dans un système de bibliothèque de bandes peuvent être potentiellement écrasées, chiffrées ou corrompues par un ransomware. Les sauvegardes dites « air gap » éliminent la possibilité d'une infection généralisée si la sauvegarde originale ne contient aucun malware.

Les meilleures pratiques spécifiques ont évolué, détaillant les actions à initier si un ransomware frappe. Un des principes essentiels est de ne jamais payer la rançon. Le FBI est un fervent défenseur du non-paiement, et la Conférence des maires des États-Unis a obtenu de ses membres leur engagement de ne jamais payer une rançon aux cybercriminels. Après tout, les personnes répondant à une demande de rançon n'ont aucune garantie que leurs fichiers soient déchiffrés. Il est même possible qu'il leur soit demandé de verser davantage, ou que leurs données et systèmes se retrouvent truffés d'autres types de malware.

Outre le fait de ne pas payer la rançon, les victimes doivent immédiatement contacter les autorités policières. Les organisations doivent immédiatement fermer et déconnecter du réseau tous les systèmes infectés et cloner tous les disques critiques avant de faire la moindre modification. Dès qu'une organisation détecte une attaque, il n'y a pas de temps à perdre. Sinon, l'infection pourrait s'étendre à davantage d'utilisateurs, de systèmes et d'applications.

Les dernières années ont vu le développement de nouveaux programmes en mesure de déchiffrer certaines souches de ransomware. Le département informatique d'une organisation doit contacter les fournisseurs ou les autorités policières afin de voir si l'infection peut être facilement déchiffrée. De nos jours, il existe plus de 100 outils de déchiffrement pouvant être utilisés contre plus de 400 variantes de ransomware.

Un bon exemple : le FBI a publié les clés de déchiffrement pour le ransomware GandCrab afin de permettre aux victimes de déchiffrer leurs données.

À noter, cependant, que les cybercriminels s'efforcent de garder une longueur d'avance. Lorsqu'une souche a été déchiffrée, ils commencent à développer une souche modifiée de sorte à ce qu'elle soit indéchiffrable. Une fois qu'une infection est contenue, les sauvegardes sont généralement le meilleur moyen de récupérer les données.

Les fichiers de sauvegarde nécessaires, provenant du cloud, des applications de sauvegarde ou des bandes, permettent à l'organisation de reprendre ses activités. Mais des précautions doivent être prises avec les fichiers de sauvegarde afin de s'assurer qu'ils ne sont pas sujets à une infection. Restaurer des fichiers contenant un ransomware entraînerait une réinfection des systèmes informatiques. D'autre part, les sauvegardes ont la réputation d'être incomplètes, obsolètes ou même corrompues.

Conseils de prévention

1. La sécurité des boîtes email est essentielle,
2. Sécurisez votre réseau et votre environnement informatique,
3. Formation des employés,
4. Sécurisez le protocole de bureau à distance (RDP) de votre organisation,
5. Faites en sorte d'avoir une sauvegarde à jour.

Les meilleurs conseils en matière de prévention contre les ransomware

1 La sécurité des boîtes email est essentielle

D'après McAfee, le phishing par email est encore l'un des principaux points d'entrée du ransomware, particulièrement dans le cas d'attaques ciblées. Ainsi, sécuriser cette principale source de vulnérabilité est essentiel pour quiconque administre un réseau ou se connecte à Internet.

La plupart des individus déclenchent une attaque ransomware en ouvrant ce qui semble être un email normal contenant le virus dans un document, une photo, une vidéo ou tout autre type de fichier. La plupart des hackers aujourd'hui n'ont pas besoin de compétences avancées pour insérer un malware dans un fichier. Il existe de nombreux articles et tutoriels YouTube avec les instructions détaillées sur la façon de procéder.

En gardant ceci à l'esprit, vous devez toujours éviter d'ouvrir un email provenant d'un expéditeur inconnu. Si vous recevez un email d'une source inconnue, informez le conseiller en sécurité des données ou l'équipe informatique de votre société immédiatement.

N'oubliez pas : mettre les systèmes informatiques et les données de votre société à l'abri est la bonne décision.

2 Sécurisez votre réseau et votre environnement informatique

Lorsqu'un ransomware infecte un ordinateur, il ne fait aucun doute qu'il s'agit d'un problème sérieux. Mais lorsqu'il se propage dans l'ensemble du réseau, cela peut virer au cauchemar pour le département informatique et mettre en danger l'entreprise dans son ensemble.

Les sociétés qui ne l'ont pas déjà fait doivent envisager l'implémentation d'un logiciel de sécurité des données qui contrôle tous les emails entrants avant que les destinataires ne les reçoivent. Une telle solution réduira drastiquement les risques qu'un virus se diffuse à l'intérieur d'un réseau d'entreprise. Les administrateurs informatiques ainsi que les responsables du département doivent également envisager l'implémentation d'un logiciel de sécurité réseau qui surveille automatiquement le réseau et ses fichiers à la recherche d'éventuelles menaces. La solution alertera les administrateurs si une attaque ransomware tente de chiffrer d'importantes quantités de fichiers sur le réseau.

Dernier point, mais non des moindres : toujours mettre à jour vos logiciels et systèmes d'exploitation à l'aide des derniers correctifs lorsqu'ils sont disponibles. Comme il est souvent souligné, les attaques de hackers réussissent uniquement lorsque les politiques en matière de sécurité des données de la victime présentent des failles.

3 Formation des employés

Même les utilisateurs expérimentés en informatique commencent à paniquer lorsqu'ils se rendent compte qu'ils font face à une attaque ransomware. Il est donc primordial que chaque employé dans une société sache exactement que faire si une attaque ransomware se produit, y compris la direction et les responsables du département informatique.

Les protocoles concernant la conduite à tenir en cas d'attaque ransomware doivent non seulement faire partie d'un plan de continuité des opérations pour les cadres supérieurs ou les experts informatiques,

mais des directives précises quant aux actions à mener doivent être visibles et assimilées dans chaque bureau. Celles-ci peuvent être simples mais efficaces ; par exemple :

- Déconnecter les ordinateurs d'Internet et du réseau interne,
- Essayer d'arrêter l'appareil infecté correctement et appeler immédiatement la sécurité et l'administration informatiques.

Les personnels de la sécurité et de l'administration informatiques doivent être informés en permanence des derniers développements en matière de cybersécurité et de hacking. Par conséquent, il est impératif qu'une formation continue soit suivie, que les dernières actualités sur ces sujets soient consultées, et que les nouveaux développements dans ce domaine et les failles des réseaux ou des solutions logicielles soient assimilés.

4 Sécurisez le protocole de bureau à distance (RDP) de votre organisation

Le protocole de bureau à distance est couramment utilisé avec les services à distance. Tandis qu'en 2018/2019 la vulnérabilité du BlueKeep CVE 2019 0708 devenait préoccupante, les correctifs Microsoft récents ont répondu à cette tendance. Dernièrement, l'utilisation d'identifiants RDP volés ou achetés et du bon vieux phishing est critique.

Si votre organisation n'a pas besoin d'utiliser le protocole RDP, le mieux est de le remplacer par une solution plus sécurisée. Si ce n'est pas possible, les mesures suivantes doivent être mises en place :

- Utiliser un VPN pour accéder au RDP de votre organisation, ceci permet de créer une connexion sécurisée entre les employés d'une organisation et Internet. L'ensemble du trafic de données passe par un tunnel virtuel chiffré, ainsi les cybercriminels ne sont pas en mesure d'accéder à un système par la force brute,
- S'assurer qu'une authentification à deux facteurs est configurée
- Les employés responsables de la maintenance d'importants services internes doivent disposer de l'accès maximum requis pour être en mesure de faire leur travail. Une authentification à deux facteurs doit être configurée pour tout employé ayant accès aux systèmes ou sauvegardes critiques,
- Disposer d'un plan de récupération en cas de sinistre à jour pour garantir que vous avez sous la main une sauvegarde de toutes les données critiques si votre RDP est compromis.

5 Faites en sorte d'avoir une sauvegarde à jour

Vous protéger signifie également disposer d'une sauvegarde de vos données. Une sauvegarde hautement sécurisée est un élément primordial dans la préparation de votre organisation en cas d'attaque ransomware. Vous devez tester votre sauvegarde de façon rigoureuse et fréquente, mais surtout, elle doit également permettre de restaurer les données en toute simplicité.

Cela signifie que si vous êtes frappé par un malware quel qu'il soit, vous serez en mesure de reconstruire votre système rapidement et sans problème. Si possible, assurez-vous que votre système de sauvegarde n'est pas connecté à votre réseau (ou alors seulement pendant la durée où vous en avez besoin), ceci vous permettra d'éviter que votre sauvegarde soit affectée par un malware également.

Que devez-vous faire en cas d'attaque de ransomware ?

Si pour une quelconque raison un ransomware parvient à franchir votre ligne de défense, vous devez faire ce qui suit :

- **Ne jamais payer la rançon !** Accéder à la requête des malfaiteurs ne garantit pas que vous récupérerez vos données. Très souvent, et très certainement s'il s'agit d'un ranscam ou d'un malware wiper, vous ne récupérerez pas vos données, et vous vous retrouverez sans données et avec un gouffre dans vos finances,
- **Ne pas essayer de déchiffrer les données vous-même.** Certains spécialistes en informatique peuvent avoir les compétences pour récupérer les données perdues, mais c'est risqué. Si les choses se déroulent mal, vous pourriez détruire vos données pour toujours,
- **Vérifier vos sauvegardes.** Même si votre sauvegarde est manquante après une attaque ransomware, n'excluez jamais la possibilité d'une récupération. Les solutions possibles dépendent du type de support ou du système de stockage, ainsi que du type de ransomware.

Récupération des données à partir de sauvegardes Veeam

Veeam est le leader du marché des sauvegardes de machines virtuelles. De nombreuses organisations font appel aux machines virtuelles dans leurs centres de données et réalisent leurs sauvegardes par le biais des logiciels Veeam.

En général, les moyennes et grandes entreprises placent leurs sauvegardes sur des volumes dédiés sur des systèmes de fichiers MS NTFS / ReFS. Les entreprises plus petites utilisent souvent des systèmes NAS externes avec Linux Ext3/Ext4/XFS/BTRFS/ZFS.

Veeam Software est une méthode de sauvegarde fiable et sécurisée. Cependant, le ransomware étant tellement répandu aujourd'hui et susceptible de cibler les données de sauvegarde, les organisations doivent prendre particulièrement soin de protéger les serveurs virtuels, physiques et basés sur le cloud, ainsi que les appareils NAS.

Comment prévenir les attaques ransomware sur les fichiers de sauvegarde Veeam

Voici les conseils d'Ontrack aux organisations :

- Mettre en œuvre un plan de sauvegarde et de récupération pour toutes les données critiques à l'aide de la stratégie 3-2-1 :

  3 - conserver un minimum de trois copies des données,

  2 - stocker les données sur deux types de supports différents,

  1 - sécuriser une copie de vos sauvegardes hors des locaux de l'organisation.

- Tester les sauvegardes régulièrement pour garantir une bonne configuration, ce qui limitera l'impact d'une fuite de données et accélérera le processus de récupération,
- Isoler les sauvegardes critiques du réseau (air gap) pour une protection maximum,

- Instaurer des systèmes de fichiers de type « copy-on-write » (NetApp WAFL – Linux ZFS) ou les fonctionnalités WORM des systèmes ou appareils NAS,
- Appliquer les correctifs critiques aux systèmes d'exploitation et aux logiciels antivirus et de sauvegarde dès que possible,
- Instaurer des formations en cybersécurité pour les utilisateurs et administrateurs afin d'identifier les emails de phishing.

Comment Ontrack peut aider

Si un ransomware s'introduit dans le périmètre du réseau et qu'une sauvegarde complète n'est pas disponible, il existe une chance que la récupération des données soit encore possible. Chaque scénario nécessite une approche différente pour récupérer les données. Toutefois, il convient de se fier uniquement aux fournisseurs mondiaux ayant fait leurs preuves avec les systèmes d'entreprise.

Chaque scénario nécessite une approche différente pour récupérer les données.

Ontrack possède une vaste expérience dans la récupération de données à partir des plateformes et supports de stockage les plus répandus. La ligne politique ferme d'Ontrack est de ne jamais payer une rançon. Au lieu de cela, nous mettons tout en œuvre pour récupérer toutes les données possibles à l'aide de techniques avancées. Ontrack possède une expertise interne exceptionnelle ainsi que les installations et outils nécessaires à une récupération complète des données d'entreprise.

Ontrack peut récupérer à partir de sauvegardes Veeam

Ontrack prend entièrement en charge la récupération de VMware, vSphere, et Microsoft Hyper-V intégrés dans l'environnement Veeam. Ontrack possède des années d'expertise spécialisée et a développé un logiciel propriétaire pour récupérer les données des fichiers de sauvegarde Veeam. Par conséquent, Ontrack peut récupérer les données à partir d'un grand nombre de jobs Veeam, même lorsque le malware a corrompu le fichier. Nos méthodes de récupération exclusives traitent les fichiers VBK, VIB et VBM endommagés, entre autres.

Etude de cas

Une rançon de 400 000 € et 100 serveurs

Une société d'exposition européenne de premier plan a fait l'objet d'une cyber-attaque avec 100 serveurs partiellement chiffrés. Une rançon de 400 000 € a été demandée et la police fédérale ainsi qu'une équipe internationale composée d'experts en cybersécurité et en informatique légale sont intervenues mais n'ont pas été en mesure d'identifier le type de ransomware. Il a été établi que le client avait été directement ciblé et qu'il s'agissait du premier cas de ce type.

Le client possédait un SAN IBM avec 50 lecteurs, et après analyse légale, nous nous sommes aperçus que les données se trouvant à l'intérieur des LUN avaient été soit supprimées, soit écrasées. Ceci concernait six LUN de 25 TB chacun avec des systèmes de fichiers différents : quatre ReFS et deux NTFS.

Les ingénieurs Ontrack sont parvenus à réparer les dommages logiques à tel point qu'une récupération à 100 % du système de fichiers ReFS a été réalisée. L'équipe de développement interne d'Ontrack a ensuite créé des outils sur mesure pour rassembler le système de fichiers NTFS et redupliquer la base de données, afin que les données d'une sauvegarde Veeam puissent être extraites et livrées régulièrement au client.

Etude de cas

Comment la technologie NetApp a permis à Ontrack de résoudre une infection de ransomware

Un ordinateur portable qui était connecté à un réseau d'entreprise a été la cible d'une attaque ransomware Cryptolocker. Le malware avait infecté un volume CIFS qui était configuré en partage de fichiers sur un FAS NetApp, chiffrant la plupart des fichiers. Du fait que l'équipe informatique n'avait pas été avertie avant l'expiration de la période de rétention des sauvegardes, tous les fichiers de sauvegarde étaient touchés.

L'impact global du ransomware a entraîné l'inaccessibilité des données sur :

- 46 lecteurs,
- Un agrégat,
- Un volume infecté sur un RAID-DP.

Pour que la récupération puisse être effectuée, les ingénieurs Ontrack ont dû déconnecter l'agrégat, et il a été demandé au client d'apporter les 46 lecteurs au laboratoire Ontrack pour une évaluation.

L'équipe d'ingénieurs Ontrack a ensuite :

- Reconstruit virtuellement les groupes RAID sur 10 racks différents,
- Reconstruit virtuellement l'agrégat,
- Reconstruit virtuellement le volume critique.

Cette récupération a présenté des difficultés supplémentaires, l'agrégat n'ayant pas cessé d'être utilisé pendant deux semaines après que l'attaque s'est produite, ce qui a entraîné l'écrasement de certaines données.

En utilisant OnTap (le système d'exploitation propriétaire de NetApp) et le système de fichiers WAFL, les ingénieurs Ontrack ont utilisé plusieurs points de consistance pour « remonter le temps » afin de trouver et fusionner les copies non chiffrées des données critiques qui ont ensuite été retournées au client.

Ce type de récupération est uniquement possible sur un stockage tel que le FAS NetApp à cause de la façon dont les données sont stockées dans le volume.

Ontrack®
2, impasse de la Noisette
91370 Verrières-le-Buisson, France
24/7 +33 (0)1 69 53 66 99
www.ontrack.com/fr