proofpoint.

EBOOK

Le ransomware – Guide de survie 2022

Ce que toute entreprise doit savoir avant, pendant et après une attaque

proofpoint.com/fr

Sommaire

Résumé

Le ransomware est une menace ancienne mais néanmoins toujours d'actualité. Ce type de malware, qui doit son nom aux rançons exigées par ses auteurs pour débloquer les fichiers de la victime, est un véritable fléau pour les entreprises modernes. C'est l'une des formes de cyberattaque les plus déstabilisantes. Les incidents majeurs qui ont affecté en 2021 l'approvisionnement en carburant[1], l'alimentaire[2] et les soins de santé[3] aux États-Unis ont clairement montré qu'aucune cible n'est hors d'atteinte. Il est donc plus important que jamais de se doter d'un plan permettant non seulement de limiter les risques, mais aussi d'intervenir efficacement si vos systèmes devaient être infectés par un ransomware.

Pourquoi le ransomware perdure

Le ransomware perdure et prospère en raison de quatre facteurs principaux :

- Les paiements de rançons sont plus faciles à percevoir que dans d'autres types de fraudes, grâce au bitcoin et à d'autres monnaies numériques.
- Les cybercriminels disposent de nombreux canaux de distribution, notamment les infections préalables, ce qui augmente leurs chances de réussite.
- De nombreuses entreprises ne disposent que de cyberdéfenses peu performantes ou obsolètes, et de plans de sauvegarde et restauration mal conçus, de sorte qu'elles constituent un large réservoir de cibles potentielles.
- Les cybercriminels ne cessent d'affiner leurs stratégies de ciblage et leurs tactiques.

Comme la plupart des cyberattaques, les ransomwares exigent souvent une action de la part de la victime, par exemple ouvrir une pièce jointe ou cliquer sur une URL.

Survivre aux ransomwares

Les ransomwares compromettent les systèmes et les données, mais les attaques qui leur permettent de prendre pied ciblent les personnes. Comme la plupart des cyberattaques, les ransomwares exigent souvent une action de la part de la victime, par exemple ouvrir une pièce jointe ou cliquer sur une URL. La lutte contre les ransomwares exige donc une approche centrée sur les personnes.

Ce guide est votre point de départ.

1 David Sanger, Clifford Krauss, Nicole Perlroth *(New York Times)*, « Cyberattack Forces a Shutdown of a Top U.S. Pipeline » (Une cyberattaque force la fermeture d'un important pipeline américain), mai 2021.
2 Julie Creswell, Nicole Perlroth, Noam Schreiber *(New York Times)* « Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business » (Un ransomware paralyse des usines de viande lors de la dernière attaque en date contre des entreprises américaines critiques), juin 2021.
3 Nicole Perlroth, Adam Satariano *(New York Times)*, « Irish Hospitals Are Latest to Be Hit by Ransomware Attacks » (Des hôpitaux irlandais parmi les dernières victimes d'attaques de ransomware), mai 2021.

Avant l'attaque

Face aux ransomwares, la meilleure stratégie consiste naturellement à les éviter. Cela exige des efforts et une planification rigoureuse, avant tout incident.

Élaborez un plan de sauvegarde et de restauration

Une composante essentielle de toute stratégie de lutte contre les ransomwares est l'exécution de sauvegardes régulières. Étant donné qu'un grand nombre de souches de ransomwares ciblent les sauvegardes connectées au réseau, conservez ces sauvegardes sur un réseau séparé ou dans le cloud. Veillez en outre à désactiver l'accès à ces sauvegardes[4].

Étonnamment, peu d'entreprises réalisent des tests de sauvegarde et restauration. Or, ces deux aspects sont importants, puisque les tests de restauration sont la seule façon de déterminer à l'avance si votre plan de sauvegarde fonctionne.

Mettez vos systèmes à jour et appliquez les correctifs nécessaires

Maintenez à jour les systèmes d'exploitation, les logiciels de sécurité, les applications et le matériel réseau et appliquez tous les correctifs requis.

Investissez dans des solutions de sécurité robustes centrées sur les personnes

Les solutions avancées de sécurité de la messagerie électronique offrent une protection contre les pièces jointes, les documents et les liens malveillants vecteurs de ransomwares contenus dans les emails. Ces solutions vous protègent également contre d'autres malwares, souvent diffusés via email, susceptibles d'installer des ransomwares lors d'attaques de suivi ciblées.

La formation et la sensibilisation de vos collaborateurs sont essentielles. Ceux-ci doivent savoir comment réagir, ce qu'ils doivent faire et ne pas faire, comment éviter le piège des ransomwares et comment signaler ces menaces. Si un collaborateur reçoit une demande de rançon associée à un ransomware, il doit savoir qu'il doit en informer immédiatement l'équipe de sécurité, sans jamais prendre l'initiative de payer lui-même.

Planifiez votre réponse

Se voir bloquer l'accès à des systèmes critiques est source de stress, et ce stress affecte notre capacité de prise de décision[5]. Déterminez à l'avance comment vous allez réagir, de façon à pouvoir vous concentrer sur le confinement de la menace et la reprise des activités en cas d'attaque.

Il n'existe pas de plan d'intervention universel valable pour toutes les attaques de ransomwares. Le coût d'une interruption d'activité sera mesuré très différemment selon que celle-ci touche un hôpital/ une infrastructure critique ou une entreprise commerciale. L'exécution d'une simulation complète est une méthode utile pour planifier chaque étape de votre réponse sur incident.

4 W. Curtis Preston *(Network World)*, « How to protect backups from ransomware » (Comment protéger les sauvegardes des ransomwares), février 2021.
5 Kathleen M. Kowalski, Charles Vaught *(International Journal of Emergency Management)*, « Judgement and Decision-Making Under Stress: An Overview for Emergency Managers » (Jugement et prise de décision en situation d'urgence : synthèse à l'intention des chefs d'équipes d'intervention d'urgence), juin 2003.

Pendant l'attaque

Si la meilleure stratégie reste l'évitement, les attaques de plus en plus sophistiquées contre la chaîne logistique logicielle ont montré que même les entreprises les mieux préparées peuvent tomber dans le piège du ransomware[6]. Les ransomwares ne sont d'ailleurs pas toujours la première charge virale à infecter vos systèmes. De nombreux gangs de ransomware préfèrent acheter des accès à des cibles déjà infectées par un chargeur ou un cheval de Troie.

Pendant l'attaque, vous avez des problèmes urgents à résoudre, comme remettre en service les ordinateurs, les téléphones et les réseaux, ou encore donner suite à la demande de rançon.

Contactez les autorités

Le ransomware, comme toute autre forme de vol et d'extorsion, est un délit. Notifier les autorités compétentes constitue une première étape indispensable.

Vous devez également contacter votre compagnie d'assurance si vous disposez d'une couverture contre les cyberrisques.

Déconnectez-vous du réseau

Dès qu'un collaborateur reçoit une demande de rançon ou remarque une anomalie, il doit se déconnecter du réseau et remettre l'équipement infecté à l'équipe informatique. Seule l'équipe de sécurité IT doit entreprendre une opération telle qu'un redémarrage, et même une mesure de ce genre ne sera efficace que s'il s'agit d'un scareware ou d'un malware classique.

Si le ransomware a déjà atteint un serveur, l'équipe de sécurité doit l'isoler aussi rapidement que possible et mettre en place une procédure de réponse.

Attention, cependant : à l'instar des infestations affectant vos animaux domestiques, un système infecté est généralement indicateur d'un problème plus vaste. Veillez donc à analyser votre environnement à la recherche d'autres systèmes infectés éventuels.

Appliquez la réponse planifiée

Votre plan de réponse doit être suffisamment flexible pour tenir compte d'une série de facteurs :

- Le type d'attaque, à savoir la souche de ransomware utilisée et le cybercriminel qui en est responsable
- La présence de charges virales antérieures de malwares qui auraient pu être utilisées pour effectuer une reconnaissance ou charger le ransomware
- Les personnes compromises au sein du réseau
- Les autorisations réseau dont disposent les comptes compromis

Les infections par des ransomwares sont souvent des infections secondaires qui touchent des réseaux déjà compromis. Chacun de ces facteurs est donc essentiel pour évaluer l'ampleur du problème et empêcher de futures infections et fuites de données.

Ne comptez pas sur les outils gratuits de déchiffrement des ransomwares

La plupart des outils gratuits ne fonctionnent que contre une souche de ransomware particulière, voire une seule campagne d'attaque. À mesure que les pirates mettent à jour leurs ransomwares, les outils gratuits deviennent obsolètes et ne fonctionnent plus contre les nouvelles variantes.

Restaurez vos données à partir des sauvegardes

La seule façon de se remettre totalement d'une infection par ransomware est de tout restaurer à partir d'une sauvegarde. Mais même avec des sauvegardes récentes, le paiement de la rançon est parfois la solution la plus simple du point de vue financier et opérationnel.

6 Kellen Browning *(New York Times)*, « Hundreds of Businesses, from Sweden to U.S., Affected by Cyberattack » (Des centaines d'entreprises, de la Suède aux États-Unis, affectées par une cyberattaque), juillet 2021.

Après l'attaque

Une fois la crise passée, le travail est loin d'être terminé.

Évaluez et renforcez votre sécurité

Nous vous recommandons de réaliser une évaluation de sécurité de bout en bout, afin d'identifier les menaces qui pourraient subsister dans votre environnement. Passez soigneusement en revue vos procédures et vos outils de sécurité et identifiez leurs lacunes.

Nettoyez

Certains ransomwares sont distribués par le biais d'autres menaces ou chevaux de Troie de type porte dérobée (backdoor) pouvant donner lieu à des attaques ultérieures. Souvent, l'environnement de la victime était déjà compromis, ouvrant grand la porte au ransomware.

Recherchez activement toute menace dissimulée que vous pourriez avoir négligée dans la confusion de l'attaque, surtout s'il existe un risque que les sauvegardes aient elles aussi été compromises.

Procédez à une analyse post-mortem

Passez en revue votre stratégie de préparation aux menaces, la chaîne d'événements qui a donné lieu à l'infection ainsi que votre réponse à l'incident. Si vous n'identifiez pas le moyen par lequel le ransomware s'est infiltré, vous serez incapable de bloquer la prochaine attaque.

Évaluez la sensibilisation des utilisateurs

Un utilisateur bien informé constitue votre dernière ligne de défense. Assurez-vous que tous les collaborateurs, des équipes de terrain aux dirigeants, sont à la hauteur de la tâche. Des évaluations régulières et des simulations d'attaques de phishing peuvent vous aider à identifier les utilisateurs les plus vulnérables, ainsi que les leurres et autres tactiques auxquels ils sont les plus sensibles.

Formez les utilisateurs

Mettez au point un programme de formation pour réduire la vulnérabilité des collaborateurs aux cyberattaques. Ce programme doit reposer sur des campagnes et tactiques d'attaque observées en environnement réel. Élaborez un plan de communication de crise en cas d'attaque future et faites-le suivre d'exercices et de tests d'intrusion.

Renforcez vos défenses technologiques

Le paysage des menaces actuel, en mutation rapide, nécessite des solutions de sécurité capables d'analyser, d'identifier et de bloquer en temps réel les URL et pièces jointes malveillantes qui servent de points d'entrée principaux aux ransomwares.

Dotez-vous de solutions de sécurité qui peuvent s'adapter aux menaces nouvelles et émergentes et vous aider à réagir plus rapidement.

Introduction

Le ransomware existe depuis plus de 30 ans, et a connu plusieurs évolutions au fil du temps. Lorsque nous avons rédigé la version précédente de ce rapport, les statistiques des ransomwares étaient en baisse, étant donné que les entreprises et les fournisseurs de solutions de sécurité étaient parvenus à bloquer Locky, le ransomware responsable de la réémergence de la menace en 2016.

AUGMENTATION DE 300 %
des attaques de ransomware au premier semestre 2021 selon les statistiques du gouvernement américain.

La situation est en train de changer. D'après les chiffres du gouvernement américain, les ransomwares ont connu une recrudescence dès le début de 2021, avec une augmentation de 300 % de ces types d'attaques[7].

Cette hausse est notamment due à l'évolution de l'écosystème cybercriminel. Les attaquants n'emploient plus un modèle de distribution de grande ampleur, associé à des rançons peu élevées. Désormais, les gangs de ransomware collaborent souvent avec d'autres distributeurs de malwares, qui leur procurent un accès à des systèmes déjà infectés par un chargeur ou un cheval de Troie à des fins de prospection, de reconnaissance et d'attaque. Cette approche permet aux cybercriminels d'identifier les cibles de valeur qui ont plus à perdre en cas de perturbation des activités, et plus de moyens financiers.

Cette nouvelle tendance, qui va de pair avec la montée du cours du bitcoin et d'autres cryptomonnaies, a créé les conditions nécessaires pour une épidémie de ransomwares.

À la une

Au premier semestre 2021, les ransomwares ont dépassé le stade de problème de cybersécurité pour atteindre celui de crise débattue aux plus hauts niveaux de l'État. Les attaques dirigées contre des zones scolaires, les services de police et les transports publics montrent une volonté croissante de la part des gangs de ransomware de cibler les infrastructures publiques.

Les attaques dirigées contre des zones scolaires, les services de police et les transports publics montrent une volonté croissante de la part des gangs de ransomware de cibler les infrastructures publiques.

Par ailleurs, en mai 2021, des pirates affiliés au gang de ransomware DarkSide ont attaqué Colonial Pipeline, dont les oléoducs alimentent une grande partie de la côte Est des États-Unis. L'attaque a provoqué des pénuries dans plusieurs États lorsque des citoyens, pris de panique, ont effectué des achats en masse de biens de consommation courants. Finalement, Colonial Pipeline a choisi de payer une rançon de plus de 4 millions de dollars en bitcoins pour récupérer l'accès à ses systèmes[8].

Au cours du même mois, des cybercriminels associés au gang de ransomware REvil ont infecté JBS Foods, un producteur de viande actif dans plusieurs pays, dont les États-Unis, le Brésil et l'Australie. L'approvisionnement en bœuf et autres produits de viande a été interrompu jusqu'à ce que JBS accepte de payer une rançon de 11 millions de dollars[9].

7 James Rundle et David Uberti *(The Wall Street Journal)*, « How Can Companies Cope with Ransomware? » (Comment les entreprises font-elles face aux ransomwares ?), mai 2021.
8 Collin Eaton et Dustin Volz *(The Wall Street Journal)*, « Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom » (Le PDG de Colonial Pipeline explique pourquoi il a versé une rançon de 4,4 millions de dollars aux cybercriminels), mai 2021.
9 Jacob Bunge *(The Wall Street Journal)*, « JBS Paid $11 Million to Resolve Ransomware Attack » (JBS a déboursé 11 millions de dollars pour résoudre une attaque de ransomware), juin 2021.
10 Jonathan Vanian *(Fortune)*, « Everything to know about REvil, the group behind a big ransomware spree » (Tout ce qu'il faut savoir sur REvil, le groupe derrière une vague d'attaques de ransomwares), juillet 2021.

Début juillet, il a été révélé que REvil était également le groupe responsable d'une compromission de la chaîne logistique de l'éditeur de logiciels Kaseya[10]. Depuis, DarkSide et REvil ont disparu des radars. Mais de nouveaux opérateurs de ransomwares font leur apparition en permanence, et il n'est pas rare que les gangs changent de nom pour échapper aux projecteurs.

Face aux montants des rançons qui augmentent et aux cybercriminels de plus en plus susceptibles de causer de graves dommages aux infrastructures nationales (intentionnellement ou non), les États à travers le monde commencent à prendre conscience de la gravité de la situation. Dans le sillage de l'incident ayant affecté Colonial Pipeline, le président américain Joe Biden a promulgué un décret destiné à renforcer les cyberdéfenses du pays. Il a par ailleurs interpellé le président russe Vladimir Poutine sur l'incapacité de son gouvernement à traîner en justice les gangs de ransomware qui opèrent sur son territoire.

Fonctionnement des ransomwares

Un ransomware bloque l'accès à un système informatique ou à des données, généralement en chiffrant des fichiers portant des extensions spécifiques (JPG, DOC, PPT, etc.). Les fichiers restent inaccessibles jusqu'à ce que la victime paie une rançon en échange d'une clé de déchiffrement permettant de débloquer les données. Dans de nombreux cas, la demande de rançon est assortie d'une échéance. En cas de refus de payer, il arrive que la rançon double ou que les données soient perdues à tout jamais, divulguées publiquement ou même détruites.

De plus en plus souvent, les victimes subissent de multiples extorsions : tout d'abord pour obtenir une clé de chiffrement destinée à débloquer les données, ensuite pour que les pirates ne vendent pas ou ne publient pas des copies de ces données sur le Dark Web.

Le coût réel

80 %
des entreprises américaines ont subi une attaque de ransomware en 2020.

68 %
ont choisi de payer la rançon.

Près de 80 % des entreprises américaines ont subi une attaque de ransomware en 2020, et 68 % d'entre elles ont choisi de payer la rançon[11]. Les conséquences financières d'une attaque peuvent être dramatiques, et les montants des rançons augmentent chaque année.

Au premier semestre 2021, diverses entreprises ont confirmé avoir versé des rançons à hauteur de 4,4 millions de dollars dans le cas de Colonial Pipeline[12] et de 11 millions pour JBS Foods[13], ainsi qu'un montant record de 40 millions pour CNA Financial[14]. Et ce ne sont là que les cas qui ont été portés à la connaissance du grand public. Le véritable coût financier des ransomwares est vraisemblablement beaucoup plus élevé que ne le laissent supposer ces chiffres, puisque certaines entreprises vont inévitablement gérer ce type d'intrusion dans la plus grande discrétion.

Mais le coût pour l'entreprise ne se limite pas aux aspects financiers.

11 Proofpoint, « State of the Phish 2021 », février 2021.
12 Collin Eaton et Dustin Volz (The Wall Street Journal), « Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom » (Le PDG de Colonial Pipeline explique pourquoi il a versé une rançon de 4,4 millions de dollars aux cybercriminels), mai 2021.
13 Jacob Bunge (The Wall Street Journal), « JBS Paid $11 Million to Resolve Ransomware Attack » (JBS a déboursé 11 millions de dollars pour résoudre une attaque de ransomware), juin 2021.
14 Kartikay Mehrotra et William Turton (Bloomberg), « CNA Financial Paid $40 Million in Ransom After March Cyberattack » (CNA Financial a payé une rançon de 40 millions de dollars après une cyberattaque subie en mars), mai 2021.

Selon Coveware, un bureau de conseil spécialisé dans la réponse aux incidents liés à des ransomwares, plus de trois quarts des attaques de ransomwares au premier semestre 2021 impliquaient une menace de diffusion publique des données exfiltrées[15]. En 2020, le même bureau a indiqué que 65 % des victimes sous le coup d'une menace de divulgation ont choisi de payer la rançon, soulignant le risque important pour la réputation d'une exfiltration criminelle de données.

Le coût sans doute le plus difficile à anticiper est celui de la perturbation des activités : paralysie de la chaîne logistique, impossibilité pour les commerciaux de communiquer avec les clients et les prospects, voire inaccessibilité totale des outils de communication de base. Les conséquences peuvent être encore plus graves dans des secteurs critiques tels que les soins de santé. Un constat amer qu'a pu faire le Health Service Executive irlandais lorsqu'une attaque du gang de ransomware Conti a forcé des reports de traitements et des annulations de procédures ambulatoires telles que des radiographies[16].

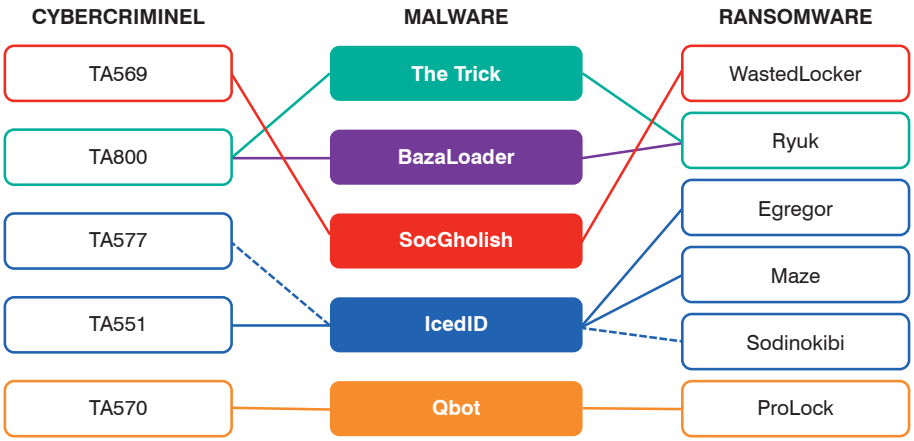
Ransomwares et messagerie électronique

Un grand nombre d'attaques de ransomwares débutent, directement ou indirectement, par un email de phishing. Ces emails incitent les utilisateurs à ouvrir une pièce jointe dangereuse ou à cliquer sur une URL malveillante.

Un grand nombre d'attaques de ransomwares débutent, directement ou indirectement, par un email de phishing.

Mais la situation a changé au cours des cinq dernières années, depuis que Locky a fait son apparition en envahissant des millions de boîtes de réception. Plus récemment, les ransomwares ont été distribués en tant qu'infection secondaire, après la compromission initiale d'un système par un chargeur ou un cheval de Troie. Les groupes qui distribuent ces types de malwares vendent ensuite des droits d'accès à des gangs de ransomware, qui explorent alors les possibilités qu'offrent les réseaux déjà infectés à la recherche de cibles particulièrement intéressantes. Les courtiers ou facilitateurs empochent soit une commission fixe, soit un pourcentage de la rançon en échange de ce point d'accès au réseau compromis.

Il n'existe pas nécessairement de lien univoque entre le malware servant à l'accès initial et la souche de ransomware qui infecte ensuite les victimes. Cependant, les chercheurs de Proofpoint et du secteur de la cybersécurité en général ont mis en évidence certaines associations.



15 Coveware, « Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority » (Les montants des paiements de rançon diminuent au 2e semestre tandis que les ransomwares deviennent une priorité de sécurité nationale)

16 Danny Palmer (ZDNet), « The human cost of ransomware: Disruption to Irish health service will continue for months » (Le coût humain des ransomwares : les perturbations subies par les services de santé irlandais vont durer plusieurs mois), juin 2021.

Si le réseau de relations entre les groupes cybercriminels est complexe, la séquence d'événements dans le cadre d'une attaque de ransomware classique lancée par email ne l'est en revanche pas : l'infection par un chargeur ou un cheval de Troie laisse le réseau vulnérable aux gangs de ransomware en quête de cibles de grande valeur. Pour la plupart des entreprises, la première ligne de défense contre les ransomwares consiste donc à se protéger contre d'autres types de malwares.

En d'autres termes, il leur faut bloquer le chargeur pour bloquer le ransomware.

La menace interne

En 2020, un employé de Tesla s'est vu offrir 500 000 dollars pour installer un ransomware dans le réseau de l'entreprise.

Au-delà des leurres envoyés par email et des exploits techniques, les cyberattaquants ont ouvert un autre front dans la guerre des ransomwares : les collaborateurs complices. Dans un nombre de cas limité mais alarmant, les cybercriminels tentent de recruter des collaborateurs des entreprises ciblées pour qu'ils installent des ransomwares sur leur lieu de travail contre paiement.

En 2020, un employé de Tesla s'est vu offrir 500 000 dollars pour installer un ransomware dans le réseau de l'entreprise. L'employé a révélé la tentative de corruption et le responsable a été arrêté et a plaidé coupable, mais non sans s'être vanté d'être parvenu à ses fins ailleurs.

En août 2021, nous avons découvert une campagne email qui proposait à des employés 1 million de dollars pour installer le ransomware DemonWare sur leur lieu de travail. À peu près à la même époque, LockBit a mis à jour son message de rançon pour offrir plusieurs millions de dollars aux utilisateurs internes en échange d'identifiants de connexion valides.

L'attaquant DemonWare n'a pas tenté de diffuser des malwares dans ces emails de recrutement. Certaines solutions avancées de protection de la messagerie sont capables de détecter de telles tentatives de corruption sur la base de certains signaux. Dans tous les cas, il est utile de former les collaborateurs à reconnaître ces menaces et à les signaler sans tarder.

Origines

Les ransomwares sont distribués au moyen d'une série de vecteurs d'attaque principaux :

- Email contenant des pièces jointes renfermant des ransomwares et des liens pointant vers des fichiers malveillants
- Piratage de connexions distantes de type RDP (Remote Desktop Protocol) et VPN (Virtual Private Network)
- Vulnérabilités de l'équipement réseau d'entreprise
- Sites Web infectés, liens malveillants sur les réseaux sociaux et publicités infectées par des malwares (malvertising)
- Autres malwares (tels des chargeurs et des voleurs d'identifiants) qui peuvent injecter des ransomwares dans des systèmes déjà compromis

Même lorsque le ransomware découle d'autres malwares, le vecteur initial est souvent un email.

Ces emails d'apparence légitime n'éveillent pas les soupçons des collaborateurs qui les reçoivent. Souvent, ils prétendent communiquer des mises à jour logicielles officielles, des factures impayées, voire des messages de leur supérieur hiérarchique immédiat.

Pourquoi le ransomware a la vie dure

Le ransomware est un type d'exploit qui existe depuis des dizaines d'années, mais il est devenu une menace de plus en plus critique en raison de quatre facteurs principaux.

Multiplication des canaux de distribution

Les cybercriminels peuvent attaquer des milliers d'entités simultanément à l'aide d'une série de vecteurs et ainsi ouvrir la porte à des attaques de ransomware secondaires.

Les cyberdéfenses traditionnelles sont dépassées par les menaces qui frappent tous azimuts :

- Campagnes email massives via des botnets
- Vulnérabilités exploitables dans les logiciels et le matériel réseau
- Malwares polymorphes pour lesquels les éditeurs de solutions de sécurité sont incapables d'élaborer suffisamment rapidement de nouvelles signatures de malware
- Publicités malveillantes et sites Web compromis en dehors du périmètre de l'entreprise

Ensemble, ces facteurs augmentent la probabilité de compromissions, offrant ainsi aux ransomwares plus d'opportunités de s'implanter.

Des cibles plus lucratives

Plutôt que de se lancer dans des attaques de grande envergure, les cybercriminels ciblent de plus en plus des entreprises qui traitent des données sensibles, dont les départements IT sont débordés et qui ont tout intérêt à trouver une solution rapide.

Les défis de sécurité communs aux hôpitaux, aux services de police, aux établissements d'enseignement et autres organismes publics locaux et nationaux sont autant de facteurs qui aggravent la situation.

Pour ce type d'organisations, une panne réseau n'est pas envisageable. Il n'est dès lors pas étonnant qu'un grand nombre d'entre elles estiment que le paiement de la rançon est l'option la plus logique du point de vue de la gestion de l'activité.

Un ciblage plus précis et des tactiques plus sophistiquées

Par le passé, les ransomwares adoptaient une approche quantitative : ils attaquaient des centaines de milliers de destinataires lors de campagnes email de masse réclamant des rançons modérées dans l'espoir qu'un certain nombre de victimes se laissent prendre au piège.

Aujourd'hui, les cybercriminels se montrent plus sélectifs dans le choix de leurs cibles. Ils recherchent des données et des systèmes critiques et stratégiques, à la fois vulnérables et indispensables à leurs victimes, dans l'espoir d'obtenir un plus gros butin.

Parallèlement, les attaques de ransomwares deviennent de plus en plus sophistiquées. Plutôt que d'utiliser le ransomware lors de la première phase de l'attaque, les cybercriminels compromettent les systèmes à l'aide de malwares plus polyvalents et résistants.

Une fois implantés, ils déploient un ransomware sur les terminaux qui les intéressent.

Bitcoin et autres monnaies numériques

Depuis ses débuts en 2009, le bitcoin est une aubaine tant pour les défenseurs des libertés civiles que pour les cybercriminels. Il est impossible de remonter aux expéditeurs ou aux bénéficiaires de la transaction, ce qui permet d'effectuer des paiements anonymes et sans friction pour le commerce d'ordre privé.

En demandant un paiement en bitcoins, les cybercriminels bénéficient d'un anonymat qui leur permet de percevoir des rançons bien plus facilement. Certaines formes plus anciennes de ransomware peuvent nécessiter l'utilisation d'une carte de débit prépayée. Si cette méthode permet de contourner les mesures antifraudes des banques, elle est par contre moins pratique pour les deux parties impliquées dans la transaction.

Toutes les variantes principales de ransomwares exigent des paiements en bitcoins. (Voir **« La piste des bitcoins » à la page 13**.)

Une menace durable

Pour comprendre à quel point les attaques de ransomwares sont insidieuses, et comment elles peuvent affecter les consommateurs, étudions l'attaque dirigée contre Garmin Ltd., un service réseau qui diffuse des données aux montres et bracelets connectés dotés de la technologie Garmin, entre autres.

Garmin Ltd. utilise la technologie GPS pour partager des données avec des capteurs d'activité connectés, comme ceux de FitBit et d'Apple. Ces services ont été interrompus le 23 juillet 2020, lorsque Garmin a été victime d'une cyberattaque qui a chiffré ses systèmes en ligne, notamment « son support client, ses applications côté client et les communications d'entreprise », selon le communiqué de presse publié par la société.

Garmin a vu une partie de ses activités paralysées, car ses services et ceux fournis par ses centres d'appels étaient bloqués par chiffrement et inaccessibles par les utilisateurs ou l'entreprise. Les services n'ont pu être débloqués qu'après le paiement d'une rançon de 10 millions de dollars, selon certaines sources.

Le site d'actualité axé technologies BleepingComputer a affirmé le 1er août : « Une source proche de l'équipe d'intervention Garmin et un employé de Garmin ont confirmé (...) que le ransomware WastedLocker a attaqué Garmin ».

> « L'équipe informatique de Garmin a essayé d'arrêter à distance tous les ordinateurs du réseau après avoir constaté que des terminaux étaient chiffrés, notamment des ordinateurs à domicile connectés via VPN », a expliqué BleepingComputer. « L'opération n'ayant pas fonctionné, elle a demandé aux employés d'arrêter tout ordinateur sur le réseau auquel ils avaient accès. »

Garmin a déclaré avoir commencé à redémarrer ses services en ligne après quatre jours.

D'après BleepingComputer, l'origine du ransomware WastedLocker a été attribuée à un groupe cybercriminel établi en Russie appelé Evil Corp. Et si ce nom évoque un méchant de bande dessinée, Evil Corp a été épinglé par le ministère américain de la Justice en décembre 2019 pour son rôle dans l'incident du malware Dridex et pour l'utilisation de ransomwares dans le cadre d'autres attaques, dont le ransomware Locky et sa propre souche baptisée BitPaymer.

La piste des bitcoins

Lors d'un kidnapping traditionnel avec rançon, la phase la plus critique a toujours été de récupérer la rançon et de réussir à s'enfuir. Malheureusement, les cybercriminels qui recourent à des ransomwares ont la tâche bien plus facile.

La forme de paiement la plus courante consiste en des cryptomonnaies intraçables, la plus courante étant le bitcoin. Celui-ci permet d'effectuer un paiement de personne à personne via Internet sans impliquer une banque ou un État.

Pour faire simple, les cryptomonnaies sont un peu l'équivalent électronique des jetons de casino. Les jetons n'ont aucune valeur intrinsèque dans le monde réel, mais les utilisateurs peuvent en acheter dans leur monnaie locale et les utiliser dans l'établissement (dans ce cas-ci, sur Internet), puis les échanger contre des devises lorsqu'ils le quittent.

De même, les cryptomonnaies peuvent être achetées en ligne auprès de sources légitimes avec une carte de crédit ou un compte bancaire. Dans le cas d'un ransomware, une victime pourrait par exemple acheter des bitcoins dans sa propre devise, puis les envoyer là un portefeuille de cryptomonnaie anonyme fourni par le cyberattaquant.

Les bitcoins ne sont pas toujours directement envoyés au cybercriminel. Souvent, ils sont transférés vers un « mixeur » de cryptomonnaie (tumbler), un service électronique qui mélange les bitcoins de différentes transactions pour les verser ensuite au bénéficiaire. (Ils sont numérotés différemment, mais possèdent la même valeur moins la commission.)

Comme pour le blanchiment d'argent dans le monde physique, les cybercriminels se retrouvent avec un paiement impossible à tracer. Ce paiement est ensuite reconverti en devise physique au moment de l'échange des bitcoins contre de l'argent liquide.

Contrairement aux devises officielles, les cryptomonnaies ne sont pas universellement reconnues comme des instruments financiers. Elles sont un peu considérées comme l'équivalent des jetons de jeu ou de poker. Dès lors, le système de transmission et les mixeurs de cryptomonnaie ne sont pas réglementés ni considérés comme du blanchiment d'argent – même si le résultat est fondamentalement le même.

L'intérêt des bitcoins est évident. Ils constituent une cybermonnaie internationale difficile à tracer pouvant être convertie directement en devise locale – l'équivalent des « billets non marqués » des rançons traditionnelles.

Cette approche présente des avantages évidents par rapport à l'usage de cartes de crédit volées, dont la valeur plonge de jour en jour dans la mesure où les institutions financières parviennent désormais à bloquer très rapidement les comptes des victimes.

De plus, la valeur du bitcoin a augmenté ces dernières années, atteignant un niveau record de près de 65 000 dollars par bitcoin, ce qui constitue un incitant financier supplémentaire pour les cybercriminels.

Dans le sillage de l'attaque contre Colonial Pipeline, le FBI a révélé qu'il avait récupéré environ la moitié de la rançon payée en bitcoins. Le service fédéral n'a pas révélé comment il s'y était pris, et l'on ignore si cette performance peut être rééditée[17].

17 Katie Brenner, Nicole Perlroth *(New York Times)* « U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack » (Les États-Unis saisissent une part de la rançon payée à des hackers lors de l'attaque de Colonial Pipeline), juin 2021.

Avant l'attaque

La meilleure stratégie en termes de sécurité consiste à résister à ces tentatives d'extorsion. C'est à la portée de beaucoup d'entreprises, mais cela exige des efforts et une planification rigoureuse, avant tout incident.

Élaborez un plan de sauvegarde et de restauration

La composante indispensable d'une stratégie de lutte contre les ransomwares est l'exécution de sauvegardes régulières. La plupart des entreprises disposent de sauvegardes, mais étonnamment peu d'entre elles réalisent des tests de sauvegarde et restauration. Or, ces deux aspects sont importants, puisque les tests de restauration sont la seule façon de déterminer à l'avance si votre plan de sauvegarde fonctionne.

Il peut être nécessaire de rectifier l'une ou l'autre procédure avant un incident. Si des tests de sauvegarde et de restauration sont réalisés régulièrement, une infection par ransomware n'aura pas d'effet dévastateur, puisque vous disposerez d'un point de restauration récent et sûr.

Mettez vos systèmes à jour et appliquez les correctifs nécessaires

Veillez à ce que les systèmes d'exploitation, les logiciels de sécurité, les applications et le matériel réseau soient parfaitement à jour et dotés de tous les correctifs requis. Cela peut sembler évident, mais selon une enquête récente, plus de la moitié des entreprises affirment ne pas disposer d'un moyen simple pour déterminer si les vulnérabilités sont corrigées rapidement. D'après les responsables interrogés, les mises à jour varient fortement en termes de complexité et de calendrier de publication[18].

Mais il existe des référents pour obtenir de l'aide en ce qui concerne la gestion des correctifs, notamment le CIS (Center for Internet Security), une association à but non lucratif qui partage et promeut de bonnes pratiques pour la gestion de la sécurité informatique, notamment les menaces de ransomware.

En matière de correctifs, il est indispensable d'éviter toute baisse de vigilance, car la rigueur dans ce domaine est essentielle pour préserver la sécurité de l'environnement. Corriger les failles de sécurité des protocoles d'accès distant et des connexions VPN peut être la solution pour bloquer des points d'accès à certaines attaques de ransomwares.

Planifiez votre réponse

Déterminez à l'avance comment vous allez réagir, de façon à pouvoir vous concentrer sur le confinement de la menace et la reprise des activités en cas d'attaque. Subir une attaque de ransomware est éprouvant, et chaque seconde compte pour empêcher les cybercriminels de se propager dans le réseau et d'aggraver les dommages.

18 Ponemon Institute, « Today's State of Vulnerability Response: Patch Work Demands Attention » (Rapport sur la correction des vulnérabilités : l'application des correctifs nécessite l'attention des entreprises), avril 2018.

En plein incident, il est plus difficile de répondre à des questions critiques et urgentes : qui faut-il informer, comment préserver les communications et quelle somme êtes-vous prêt à payer (pour autant que vous acceptiez de payer une rançon) ? La pression que cette situation engendre crée des goulets d'étranglement potentiels dans la prise de décision et peut entraîner des retards coûteux. Si vous décidez de payer la rançon, vous devez définir une procédure appropriée qui inclut les principaux cadres dirigeants, le personnel opérationnel et un conseiller juridique.

Il n'existe pas de plan d'intervention universel valable pour toutes les attaques de ransomwares. Le coût d'une interruption d'activité sera mesuré très différemment selon que celle-ci touche un hôpital/une infrastructure critique ou une entreprise commerciale. L'exécution d'une simulation complète est une méthode utile pour planifier chaque étape de votre réponse sur incident.

Investissez dans des solutions de sécurité robustes, centrées sur les personnes, pour protéger vos environnements de messagerie électronique, Web et cloud

Les emails de phishing sont aujourd'hui très sophistiqués et extrêmement ciblés. Les pirates étudient leurs cibles afin de les manipuler à l'aide de messages qui sembleront légitimes.

L'email, le vecteur le plus critique

Les passerelles email, les filtres Web et les antivirus d'ancienne génération doivent être mis à jour et actifs sur tous les réseaux. Cependant, ils ne pourront pas contrer les ransomwares à eux seuls. Une solution de protection de la messagerie électronique efficace doit aller plus loin.

La messagerie étant le point d'infection initial de la plupart des attaques de ransomwares, vous devez implémenter des solutions avancées qui protègent ce vecteur critique.

Cela implique, par exemple, d'analyser les pièces jointes et les URL incorporées pour s'assurer qu'aucun contenu malveillant ne s'insinue dans le système. Les cybercriminels ont toujours une longueur d'avance, et les configurations des dispositifs classiques de sécurité email s'appuient dans une trop grande mesure sur des signatures obsolètes.

Les solutions avancées de sécurité de la messagerie électronique offrent une protection contre les pièces jointes, les documents et les liens malveillants vecteurs de ransomwares contenus dans les emails. De plus, l'authentification des emails basée sur la norme DMARC contribue à bloquer les attaques qui s'appuient sur l'usurpation de domaines pour inspirer confiance aux utilisateurs. Votre solution de protection de la messagerie électronique doit aussi vous protéger d'autres types de fraudes à l'identité, comme l'usurpation du nom d'affichage ou les domaines similaires malveillants.

Protégez vos comptes cloud

Les comptes de messagerie cloud constituent un autre vecteur privilégié pour la distribution de malwares. Les cybercriminels peuvent prendre le contrôle de certains comptes cloud pour cibler d'autres utilisateurs au sein de la même entreprise. Les comptes email peuvent être compromis de différentes façons, notamment :

- Attaques par force brute automatisées (tentatives de connexion avec d'innombrables combinaisons nom d'utilisateur/mot de passe jusqu'à ce que l'une d'elles fonctionne)
- Vol d'identifiants de connexion d'autres comptes du même utilisateur (exploitant le fait que les utilisateurs réutilisent souvent les mêmes mots de passe pour différents comptes)
- Malwares conçus pour dérober des identifiants de connexion
- Contrôles cloud défaillants

Sécuriser les comptes cloud des utilisateurs est une composante essentielle de toute stratégie de protection contre les ransomwares.

Enfin, il est important d'exiger des utilisateurs distants qu'ils se connectent à Internet via un VPN d'entreprise, de façon à être protégés par vos cyberdéfenses où qu'ils se trouvent.

Faites des collaborateurs votre dernière ligne de défense

La plupart des attaques de ransomwares commencent par l'ouverture d'un email d'apparence professionnelle par un collaborateur bien intentionné.

Voilà pourquoi la formation et la sensibilisation de vos collaborateurs sont essentielles. Ceux-ci doivent savoir comment réagir, ce qu'ils doivent faire et ne pas faire, comment éviter le piège des ransomwares et comment signaler ces menaces. Un programme de formation qui se fonde sur des attaques réelles et met à disposition un système de signalement des messages suspects aidera les utilisateurs à repérer les messages malveillants et permettra de renforcer les comportements positifs.

Si un utilisateur reçoit une demande de rançon associée à un ransomware, il doit savoir qu'il doit en informer immédiatement l'équipe de sécurité, sans jamais prendre l'initiative de payer lui-même. Un tel paiement peut avoir des ramifications importantes en matière d'image de marque et de sécurité, et peut même contrevenir à la législation en vigueur. Cette décision doit être mûrement réfléchie par les cadres dirigeants, avec l'avis d'un conseiller juridique.

Nos recherches montrent que les cybercriminels exploitent activement les erreurs et la curiosité humaines. Cette approche s'inscrit dans une stratégie cybercriminelle plus large : manipuler les utilisateurs pour qu'ils soient les complices involontaires d'attaques visant à verrouiller des données et à exiger une rançon pour leur libération.

Ces attaques profitent de la méconnaissance des utilisateurs. Elles nécessitent souvent que les utilisateurs effectuent diverses actions, comme ouvrir des pièces jointes malveillantes, ou encore télécharger et ouvrir ou exécuter des documents ou des scripts. L'activation des macros d'un document malveillant, par exemple, peut entraîner le téléchargement d'un ransomware et lancer le processus d'attaque.

Une formation efficace sensibilise les utilisateurs aux campagnes et techniques d'attaque observées en environnement réel. Elle inclut également la threat intelligence la plus récente, afin que les utilisateurs se familiarisent avec les menaces auxquelles ils sont les plus susceptibles d'être confrontés. Les simulations de phishing peuvent permettre d'identifier les utilisateurs particulièrement enclins à tomber dans le piège des ransomwares et autres attaques.

Recommandations techniques des forces de l'ordre américaines

En plus de la stratégie générale exposée dans ce guide, le FBI recommande diverses mesures techniques pour contrer les attaques de ransomwares.

Auditez et gérez les privilèges des utilisateurs

Adoptez l'approche du moindre privilège pour les autorisations liées aux fichiers, répertoires et partages réseau.

Les utilisateurs qui n'ont pas besoin de modifier un fichier, par exemple, doivent disposer d'un accès en lecture seule uniquement. Dans de nombreux cas, les utilisateurs ne doivent pas disposer d'accès du tout. Ainsi, le personnel de caisse n'a pas besoin d'un accès aux dossiers financiers de l'entreprise. De même, le directeur d'un hôpital n'a pas besoin de consulter les dossiers patients.

Octroyez aux utilisateurs uniquement le niveau d'accès dont ils ont besoin pour exercer leurs fonctions.

Bloquez l'exécution de code à certains emplacements

Définissez des contrôles logiciels pour bloquer l'exécution de code à certains emplacements couramment utilisés par les ransomwares. C'est notamment le cas des dossiers temporaires créés par les navigateurs et des répertoires de fichiers compressés dans le dossier AppData/LocalAppData de Windows.

Bloquez les logiciels inconnus

Il est conseillé d'adopter une politique de liste d'autorisation permettant aux systèmes de n'exécuter que les programmes connus et validés. Elle devrait empêcher l'exécution de la plupart des ransomwares, même si elle n'est pas applicable dans tous les environnements de travail.

Utilisez des machines virtuelles

Les machines virtuelles permettent d'exécuter des applications, voire des systèmes d'exploitation complets, dans un environnement isolé.

Il s'agit en quelque sorte d'une « chambre de détonation » pour logiciels. L'exécution de code sensible ou non validé au sein d'un environnement de machine virtuelle ou d'un conteneur de machine virtuelle permet de s'assurer que les éventuels problèmes de sécurité qui en découlent restent confinés à cet environnement virtuel, épargnant ainsi les autres parties du système.

Segmentez les systèmes et les données

Gardez les données et systèmes critiques séparés, de façon à ce qu'un problème de sécurité sur un système n'affecte pas les autres. Par exemple, les données de recherche sensibles ou les informations commerciales ne doivent pas résider sur le même serveur et segment réseau que l'environnement email de l'entreprise.

Les recommandations complètes du gouvernement américain sont disponibles ici : **fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf.**

Pendant l'attaque

Vous êtes victime d'un ransomware. Que faire ?

Si la meilleure stratégie reste l'évitement, les attaques de plus en plus sophistiquées contre la chaîne logistique logicielle ont montré que même les entreprises les mieux préparées peuvent tomber dans le piège du ransomware. Les ransomwares ne sont d'ailleurs pas toujours la première charge virale à infecter vos systèmes : de nombreux gangs de ransomware préfèrent acheter des accès à des cibles déjà infectées par un chargeur ou un cheval de Troie.

Pendant l'attaque, vous avez des problèmes à résoudre à court terme, comme remettre en service les ordinateurs, les téléphones et les réseaux, ou encore donner suite à la demande de rançon.

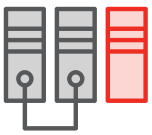
Mais réagir dans la panique n'est certainement pas une solution, et risque plutôt d'aggraver la situation.

Contactez les autorités

Le ransomware, comme toute autre forme de vol et d'extorsion, est un délit. Personne n'a le droit de bloquer l'accès aux appareils, réseaux ou données d'autrui, et encore moins de demander une rançon pour restaurer cet accès. Notifier les autorités compétentes constitue une première étape indispensable.

Contactez les forces de l'ordre immédiatement. N'hésitez pas à les appeler, elles sont là pour ça.

Vous devez également contacter votre compagnie d'assurance si vous disposez d'une couverture contre les cyberrisques. Elle pourra vous aider à coordonner votre réponse et votre investigation.



Isolez les systèmes infectés

Dès qu'un collaborateur reçoit une demande de rançon ou remarque une anomalie (il n'a plus accès à ses propres fichiers, par exemple), il doit se déconnecter du réseau et remettre l'équipement infecté à l'équipe informatique.

Nous déconseillons toujours de laisser les collaborateurs redémarrer leur système. Seule l'équipe de sécurité informatique doit entreprendre un redémarrage, et même une telle mesure ne sera efficace que s'il s'agit d'un scareware (ou faux ransomware).

Dans ce cas, ce qui ressemble à un ransomware est en réalité un logiciel destiné à effrayer l'utilisateur, mais inoffensif. Il se peut qu'il bloque l'écran en affichant une demande de rançon et des instructions de paiement, mais les données ne sont pas effectivement chiffrées. Dans de tels scénarios, les outils antimalware standard peuvent être utiles.

Mais faire la différence entre les deux n'est pas chose facile. Déterminez l'ampleur du problème en utilisant la threat intelligence. Si tous les ransomwares sont dangereux, certaines attaques sont plus agressives que d'autres. Votre réaction, notamment votre décision de payer ou non la rançon, dépendra de plusieurs facteurs.

Les questions à se poser sont les suivantes :

- **De quel type d'attaque s'agit-il ?** S'agit-il d'une infection secondaire ? Provient-elle d'un téléchargeur, d'un cheval de Troie d'accès à distance (RAT) ou d'un autre malware installé sur la machine infectée ou d'autres machines sur le réseau ?
- **Qui est compromis au sein du réseau ?** Quelle est l'étendue de l'infection ? Un acteur malveillant est-il en train d'effectuer une reconnaissance sur votre réseau, d'exfiltrer des données ou de préparer la distribution d'un ransomware sur d'autres terminaux ?
- **De quelles autorisations réseau disposent les comptes ou terminaux compromis ?** Il se peut que le ransomware ait été installé uniquement après que les cybercriminels se sont déjà déplacés latéralement sur le réseau ou ont volé des identifiants de connexion et autres données.

Vos réponses doivent aider les administrateurs réseau à déterminer l'étendue du problème, à élaborer un plan d'action et, si possible, à endiguer la propagation.

N'oubliez pas que le ransomware s'étend rapidement et a souvent pour origine d'autres menaces. Si vous constatez une infection, il est probable que d'autres soient présentes à votre insu. Recherchez activement d'autres problèmes potentiels au sein de votre environnement.

Appliquez votre plan de réponse

Selon la configuration réseau, il est parfois possible de limiter l'infection à un seul poste de travail.

Scénario idéal : la machine infectée est remplacée par un nouvel ordinateur et les données sont restaurées à partir d'une sauvegarde. Scénario catastrophe : toutes les machines du réseau sont infectées. Cela nécessitera un calcul coût-bénéfice qui mette en balance le temps et les ressources nécessaires pour restaurer les données, d'une part, et le paiement de la rançon, d'autre part.

Si le ransomware a déjà atteint vos serveurs, isolez les systèmes affectés ; c'est là que votre stratégie de segmentation du réseau montrera toute son utilité.

Un aspect important de votre réponse consiste à décider si vous payez ou non la rançon. La réponse est compliquée et exigera sans doute de consulter à la fois les forces de l'ordre et votre conseiller juridique. Pour certaines victimes, payer la rançon est parfois inévitable. (Voir la section **« Payer ou ne pas payer : le dilemme moral et juridique des ransomwares », page 21**.)

Ne comptez pas sur les outils gratuits de déchiffrement des ransomwares. Certains éditeurs proposent des programmes gratuits de déchiffrement des ransomwares. Dans certains cas, ces programmes peuvent vous aider à récupérer vos données sans qu'il soit nécessaire de payer la rançon.

Cela étant, la plupart ne fonctionnent que contre une souche de ransomware particulière, voire une seule campagne d'attaque. À mesure que les pirates mettent à jour leurs ransomwares, les outils gratuits deviennent obsolètes et ne fonctionnent plus contre les nouvelles variantes.

En bref, il est possible que vous ayez la chance de votre côté et qu'un outil de déchiffrement gratuit vous aide, mais ne considérez pas qu'il fait partie de votre plan de réponse aux incidents.

Restaurez vos données à partir des sauvegardes

La seule façon de se remettre totalement d'une infection par ransomware est de tout restaurer à partir d'une sauvegarde – des sauvegardes qui doivent être exécutées quotidiennement. S'il s'agit de la dernière mesure à prendre en cas d'infection, cela doit être la première étape en matière de prévention.

Cela dit, même avec des sauvegardes récentes, le paiement de la rançon est parfois la solution la plus simple du point de vue financier et opérationnel. La restauration de sauvegardes exige du temps et de l'énergie. Certaines entreprises ne peuvent pas se permettre des interruptions d'activité.

Payer ou ne pas payer : le dilemme moral et juridique des ransomwares

Un ransomware constitue déjà un problème grave en soi. L'un de ses aspects les plus déplaisants, cependant, est qu'il oblige ses victimes à opérer un choix délicat sur le plan moral. Lorsqu'un ransomware vous met le couteau sous la gorge, vous n'avez pas toujours le luxe de peser les implications morales du paiement de la rançon. Vous devez agir sans tarder.

Le paiement de la rançon peut s'avérer un mal aussi détestable que nécessaire. Il enrichit l'auteur de l'attaque qui vient d'infiltrer votre réseau et de voler vos données. Il fait de vous une victime, dont le réseau est vulnérable et qui n'a d'autre choix que de céder au chantage. Et il permet aux cybercriminels de financer de futures attaques.

Mais les récentes attaques nous amènent à un constat troublant : la décision de payer ou non la rançon n'est pas une évidence.

Aucune entreprise n'a envie de se faire extorquer, et encore moins de financer des groupes criminels. Il n'en reste pas moins que de nombreuses victimes estiment ne pas avoir d'autre choix. Dans une certaine mesure, c'est le prix à payer pour des départements informatiques sous-financés et des logiciels obsolètes ou dépourvus des correctifs nécessaires. Il existe toujours en Europe et aux États-Unis des hôpitaux équipés de terminaux d'ancienne génération tournant sous Microsoft Windows XP. Et la demande de rançon est souvent un prix à payer relativement faible lorsque des vies sont en jeu.

Il est même arrivé que le FBI lui-même conseille aux victimes de payer la rançon demandée. Il décourage officiellement la pratique, mais a récemment émis un avis défavorable à l'interdiction des paiements lors d'attaques de ransomware proposée par le Congrès américain[19]. Même si vous payez, souligne le FBI, vous ne récupérez pas forcément vos données.

Mais en 2020, le ministère américain des Finances a émis un avis consultatif rappelant aux entreprises et citoyens américains que payer une rançon peut entraîner des sanctions financières ou autres. Les ramifications de cet avis sont toujours à l'étude par les assureurs et les négociateurs chargés de répondre aux incidents, mais les éventuels risques juridiques viennent compliquer une prise de décision déjà délicate.

Europol, l'agence de l'Union européenne pour la coopération des services répressifs, fait elle aussi campagne pour que les victimes de ransomwares refusent de payer les rançons. Son initiative « No More Ransom », lancée il y a cinq ans, repose sur un partenariat public-privé destiné à aider les victimes de cyberattaques à reconstituer leurs données et à les déchiffrer sans payer.

Elle a aidé six millions de victimes de ransomwares à récupérer leurs fichiers, leur évitant des paiements pour un total de près d'un milliard d'euros. (Les outils de No More Ransom sont accessibles partout dans le monde, et pas uniquement aux citoyens européens.)

Les entreprises doivent peser le pour et le contre au moment de prendre une décision. Parmi les facteurs conflictuels à prendre en considération :

- Temps et ressources nécessaires pour rétablir l'activité
- Responsabilité à l'égard des actionnaires en termes de maintien des activités
- Sécurité des clients et des collaborateurs
- Type d'activité criminelle que le paiement de la rançon servira potentiellement à financer
- Toute responsabilité juridique qui pourrait découler du versement de fonds à un individu ou État reconnu coupable d'un délit

La question est complexe et entraînera des prises de position différentes selon les entreprises.

Les récentes attaques nous amènent à un constat troublant : la décision de payer ou non la rançon n'est pas une évidence.

19 Maggie Miller *(The Hill)*, « Top FBI Official Advises Congress Against Banning Ransomware Payments » (Un dirigeant du FBI déconseille au Congrès américain d'interdire les paiements de rançon en cas d'attaque de ransomware), juillet 2021.

Après l'attaque

Indépendamment des dommages causés par un ransomware, une attaque aboutie révèle une faille de sécurité qui a entraîné la compromission d'un terminal ou d'un réseau. Après un retour à la normale, vous avez l'occasion de tirer des leçons de cette violation de sécurité et d'éviter de futures attaques.

Nous recommandons de réaliser une évaluation de sécurité de bout en bout, éventuellement en confiant cette tâche à un prestataire externe, afin d'identifier les menaces qui pourraient subsister dans votre environnement. C'est également le moment de passer soigneusement en revue vos procédures et vos outils de sécurité et d'identifier leurs lacunes.

Nettoyez

Certains ransomwares contiennent d'autres menaces ou chevaux de Troie de type porte dérobée (backdoor) pouvant donner lieu à de futures attaques. Dans d'autres cas, c'est une compromission existante qui a ouvert la porte à une infection par ransomware. C'est pourquoi l'effacement des données contenues sur tous les terminaux et leur restauration à partir d'une sauvegarde saine constituent la procédure idéale. Recherchez activement toute menace que vous pourriez avoir négligée dans la confusion de l'attaque.

Procédez à une analyse post-mortem

Évaluez votre niveau de préparation et votre réponse aux incidents. Comment le plan de crise a-t-il été exécuté ? Est-il possible d'améliorer la configuration réseau afin de limiter la propagation de futures attaques ? Est-il possible d'implémenter une solution de protection de la messagerie électronique plus robuste ? Faut-il adopter une approche totalement nouvelle de la cybersécurité en général ?

Examinez les mesures de sécurité en place et demandez-vous si elles sont suffisantes pour lutter contre les menaces actuelles. Tirez toutes les leçons possibles de l'incident, car il pourrait se reproduire.

Si vous n'identifiez pas le moyen par lequel le ransomware s'est infiltré, vous serez incapable de bloquer la prochaine attaque.

Évaluez la sensibilisation des utilisateurs

De nombreuses souches de ransomware nécessitent une interaction humaine pour déployer leur charge virale, que ce soit par une infection directe ou par une distribution ultérieure par un autre type de malware. Si les mesures de sécurité sont inefficaces et qu'un message frauduleux signalant une « facture impayée » parvient jusqu'au serveur de messagerie, un utilisateur bien informé devient la dernière ligne de défense qui évitera à une entreprise, à un hôpital ou à un établissement d'enseignement de rejoindre la longue liste des victimes de ransomwares. Assurez-vous que tous les collaborateurs, des équipes de terrain aux dirigeants, sont à la hauteur de la tâche.

Il peut être utile également d'investir dans des outils de simulation de phishing pour améliorer la sensibilisation des collaborateurs, identifier les utilisateurs particulièrement vulnérables et renforcer la sécurité globale. En imitant des attaques réelles et les techniques d'ingénierie sociale et autres tactiques les plus récentes, les simulations de phishing peuvent contribuer à l'analyse et à l'identification de vulnérabilités axées sur les personnes, avant qu'une attaque se produise.

Formez les utilisateurs

Après analyse du degré de sensibilisation des utilisateurs, mettez au point un programme de formation pour réduire la vulnérabilité des collaborateurs aux cyberattaques, en y incluant notamment les leçons tirées des incidents déjà subis par l'entreprise. Ce programme doit comprendre une formation continue pour les utilisateurs les plus vulnérables, les plus susceptibles d'être ciblés ou dotés de privilèges élevés sur des données, systèmes et autres ressources sensibles.

Il doit également s'intégrer à vos autres cyberdéfenses, pour aider les utilisateurs non seulement à identifier les attaques, mais aussi à les signaler rapidement.

Investissez dans des défenses de pointe

Les cyberattaques d'aujourd'hui ciblent les individus, pas l'infrastructure. Optez pour des solutions adoptant une approche centrée sur les personnes afin de protéger celles-ci.

Les cybercriminels ne voient pas le monde en termes de topologie réseau. Déployez une solution qui vous permettra d'identifier les personnes ciblées et les méthodes utilisées à cette fin et de déterminer si elles sont tombées dans le piège. Tenez compte du risque individuel que chaque utilisateur représente : de quelle manière est-il ciblé, à quelles données a-t-il accès et a-t-il tendance à être la cible d'attaques ?

Parallèlement, empêchez le contenu Web à risque d'entrer en contact avec votre environnement. La technologie d'isolation du Web peut effectuer un rendu de pages Web référencées par des URL suspectes ou non vérifiées dans un conteneur protégé, au sein du navigateur Web habituel de l'utilisateur. L'isolation du Web peut constituer une protection critique pour les comptes de messagerie partagés, qui sont difficiles à sécuriser au moyen de l'authentification à plusieurs facteurs. Cette même technologie peut isoler la navigation Web personnelle et les services de messagerie Web des utilisateurs, ce qui leur garantit liberté et confidentialité sans mettre en danger l'entreprise.

Pour faire face aux attaques extrêmement ciblées, vous avez besoin d'informations de threat intelligence avancées sur les menaces. Dotez-vous d'une solution combinant des techniques statiques et dynamiques de détection des nouvelles caractéristiques des attaques (c'est-à-dire leurs outils, tactiques et cibles), et qui soit en mesure d'en tirer les enseignements nécessaires.

Étapes suivantes

Tant que le ransomware restera lucratif, il existera sous l'une ou l'autre forme. Les recommandations de ce guide ont pour but de vous aider à gérer cette menace avant, pendant et après une attaque.

Bien évidemment, la meilleure façon de lutter contre le ransomware consiste à l'empêcher d'infiltrer votre environnement, ce qui nécessite des cyberdéfenses adaptées aux menaces actuelles.

Une cybersécurité efficace est centrée sur les personnes. Elle rend les utilisateurs plus résilients grâce à des formations de sensibilisation basées sur des techniques d'attaque réelles. Elle identifie les ransomwares et les empêche de cibler vos collaborateurs. Enfin, elle neutralise les menaces et vous aide à intervenir rapidement et efficacement en cas d'incident.

Pour en savoir plus sur la lutte contre les ransomwares, consultez le site **www.proofpoint.com/fr**.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0501-006-01-01 11/21