CARTOGRAPHIE DU PAYSAGE DES RANSOMWARES

Comprendre la portée et la sophistication de la menace

SYNTHÈSE

Lorsque les cybermenaces sont multipliées par 35 en un an, chaque entreprise doit en tenir compte. C'est précisément le cas avec les ransomwares. Les hacktivistes ont ciblé des entreprises de pratiquement toutes les tailles et représentant une multitude de secteurs industriels dans le monde entier. Les approches de sécurité traditionnelles ne suffisent plus à contrecarrer les attaques par ransomware. Les modèles avancés utilisant des Next-Generation Firewalls, une sécurité par couche et les renseignements proactifs sur les menaces constituent un prérequis.

Les modèles RaaS (Ransomware-as-a-service) et affiliés ont simplifié la tâche des cybercriminels tandis que les technologies monétaires, comme le bitcoin, rendent pratiquement impossible aux autorités policières de suivre le paiement des rançons. Du fait de la hausse exponentielle de rançons payées aux hacktivistes exploitant des ransomwares, il est fort probable que cela continue (à un rythme encore plus soutenu) dans les années à venir. Reconnaissant la menace grandissante, les banques font des réserves de bitcoins afin que leurs clients (et elles-mêmes) puissent rapidement payer les cybercriminels pour débloquer les données piratées.

L'incidence financière pour les entreprises va bien au-delà du simple paiement d'une rançon aux cybercriminels. L'interruption de son activité se traduit par une perte de productivité et de centaines de milliers de dollars de revenu. Des entreprises de plusieurs secteurs industriels peuvent attester de ces conséquences.

PORTÉE DE LA MENACE

Les données sont au cœur de la plupart des sociétés d'aujourd'hui, des TPE aux grandes entreprises. La numérisation de plus en plus d'actifs d'entreprise, ainsi que l'importance croissante du cloud, placent les données dans la ligne de mire des cybercriminels. Ce problème s'amplifie aujourd'hui du fait du développement des données, ces dernières faisant plus que doubler tous les deux ans.[1]

Conscients de la valeur des données, les cybercriminels utilisent de plus en plus les ransomwares comme un moyen de monétisation. Ils infiltrent les systèmes informatiques et accèdent aux données au moyen de divers piratages, afin de chiffrer, verrouiller et exfiltrer les fichiers. Se retrouvant dans l'impossibilité d'accéder à leurs informations sensibles, les entreprises n'ont d'autres choix que de payer pour récupérer leurs données. La sophistication de la majeure partie de ce processus a évolué au point que les cybercriminels fournissent à leurs victimes la marche à suivre pour payer et restaurer leurs données et leur système informatique.

HAUSSE VERTIGINEUSE DES ATTAQUES PAR RANSOMWARE

Quelle est l'ampleur de la menace des ransomwares ? L'année dernière, les attaques par ransomware ont plus que doublé.[2] Plus de 4 000 attaques par ransomware sont réalisées quotidiennement. Elles touchent en moyenne entre 30 000 et 50 000 appareils chaque mois[3] et le potentiel de hausse est immense. Malgré l'importance de cette augmentation, les ransomwares ne représentent que 2 % de toutes les attaques actuelles par un logiciel malveillant.[4]

Les répercussions financières des ransomwares ont également connue une hausse vertigineuse. En effet, en 2015, 24 millions de dollars de rançon ont été payés alors qu'en 2016 ce montant a grimpé à plus de 850 millions de dollars.[5] La somme demandée par les cybercriminels a suivi la même voie : le montant moyen exigé par attaque est passé de 294 dollars en 2015 à 679 dollars en 2016.[6]

Mais l'impact majeur des ransomwares n'est pas le paiement de la rançon. 63 % des entreprises ayant été victimes d'une attaque par ransomware l'année dernière indiquent avoir subi une interruption menaçant leur activité. 48 % des entreprises signalent la perte de données ou de matériels. Enfin, concernant les entreprises qui ont payé la rançon en échange de la récupération de leurs données (42 % ont reconnu avoir payé), une sur quatre n'a jamais rien récupéré.[7] C'est pourquoi le FBI recommande que les victimes ne paient pas les rançons.

SEULEMENT LA PARTIE VISIBLE DE L'ICEBERG

Il est toutefois probable que ces valeurs ne reflètent pas la réelle étendue du problème. Les attaques par ransomware sont largement sous-évaluées, moins d'un incident sur quatre étant signalé. Plus de la moitié des entreprises admettent avoir subi une attaque par ransomware au cours de l'année passée.[8] Parmi ces dernières, 34 % ont perdu de l'argent et 20 % ont dû cesser leur activité ! Lorsque ces facteurs sont pris en compte, l'incidence financière est alarmante. Mais il y a pourtant pire : 3,5 % indiquent que l'attaque par ransomware a mis des vies en danger.[9]

Même les entreprises qui pensent être trop petites pour être la cible d'attaques par ransomware, doivent réfléchir ! Du fait, bien souvent, de l'absence d'un expert informatique dédié dans les locaux et de contrôles nécessaires au niveau de la gestion des systèmes informatiques, les petites entreprises sont exposées aux attaques par ransomware. De plus, sans protection appropriée des données pour se prémunir contre les ransomwares, se préparer à les contrer et assurer la reprise de l'activité, ces entreprises deviennent rapidement une cible privilégiée pour les cybercriminels. Un rapport récent indique que les temps d'arrêt induits par un ransomware coûtent environ 8 500 dollars de l'heure aux petites entreprises. Il en résulte des pertes pouvant atteindre 75 milliards de dollars par an.[10]

Les ransomwares ont infecté entre **30 000** et **50 000** appareils par mois

Le montant des rançons inhérent aux **attaques par ransomware** s'est élevé à **850 millions de dollars** en 2016

Les ransomwares sont sous-évalués. Plus **d'une attaque sur 4** n'est pas signalée

63 % des entreprises ont subi une interruption **menaçant leur** activité

34 % des entreprises ont perdu de l'argent

INCIDENCE COMMERCIALE DES RANSOMWARES

Le coût inhérent à l'indisponibilité des systèmes et à l'impossibilité d'accéder aux informations suite à des attaques par ransomware s'élève à des milliards de dollars aujourd'hui et pourrait passer à des dizaines de milliards du fait de l'intérêt que les hacktivistes utilisant des ransomwares portent aux appareils IoT.

DOXXING

Les cybercriminels innovent. Plutôt que de menacer de supprimer les données verrouillées, certains n'hésitent pas à menacer de les divulguer (il s'agit du « doxxing »). Pour les entreprises qui gèrent des données clientes privées et sensibles, comme des services financiers, des hôpitaux, des cabinets juridiques et autres, cela peut avoir des conséquences néfastes. Outre l'impact sur la renommée de la marque, la réglementation comme la loi américaine sur l'assurance maladie (Health Information Portability and Accountability Act) requiert de notifier les clients et d'autres activités consciencieuses qui peuvent rapidement se chiffrer en centaines de milliers (voire de millions) de dollars.

CONSERVER DES BITCOINS POUR PAYER UNE RANÇON

L'impact des ransomwares ne s'arrête pas aux entreprises piratées. Prenons l'exemple du secteur bancaire. Comme l'incidence potentielle résultant de la perte des données ou de l'impossibilité d'y accéder se mesure en minutes, voire même en secondes, les entreprises ne peuvent pas attendre plusieurs jours que les cybercriminels débloquent l'accès aux informations piratées. Par conséquent, les banques conservent des bitcoins (il faut compter généralement 3 à 5 jours pour réunir la somme) afin que leurs clients puissent payer les cybercriminels immédiatement.[11]

PROPAGATION DES RANSOMWARES

DIFFUSION DES RANSOMWARES

Comment les ransomwares se propagent-ils ? Commençons déjà par découvrir comment ils sont diffusés. N'importe quel support numérique peut être utilisé : les e-mails, les pièces jointes d'un site Web, les applications commerciales, les réseaux sociaux et les lecteurs USB font notamment partie des mécanismes de diffusion numériques. Les e-mails constituent le principal vecteur de diffusion, les cybercriminels ayant une préférence pour l'utilisation de liens, puis de pièces jointes.

- Liens transmis par e-mail, 31 %
- Pièces jointes d'un e-mail, 28 %
- Pièces jointes d'un site Web, 24 %
- Sources inconnues, 9 %
- Réseaux sociaux, 4 %
- Applications commerciales, 1 %

Dans le cas des e-mails, le phishing est transmis sous forme de notifications de réception ou de fausses demandes de mises à jour logicielles. Dès qu'un utilisateur clique sur le lien ou sur la pièce jointe, se lance souvent le téléchargement transparent de composants malveillants supplémentaires (quoique moins souvent dernièrement), suivi du chiffrement des fichiers avec une clé privée 2 048 bits RSA, rendant ainsi le déchiffrement des fichiers presque impossible pour l'utilisateur. Il arrive également que le ransomware soit intégré à un site Web sous la forme d'un fichier qui, une fois téléchargé et installé, active l'attaque.

DIFFÉRENTS TYPES DE RANSOMWARES

Les attaques par ransomware revêtent diverses formes. Elles ont considérablement évolué au cours de l'année passée.
Les ransomwares traditionnels s'en prennent à vos données, verrouillant les fichiers jusqu'au paiement de la rançon. Cependant, avec la croissance rapide des appareils IoT, un nouveau type de ransomware a émergé. Il ne s'attaque plus aux données d'une entreprise mais cible les systèmes de commande (véhicules, lignes d'assemblage, systèmes d'alimentation, etc.) qu'il arrête jusqu'au paiement de la rançon.

Faisons brièvement le tour des principaux types de ransomwares existants :

- **Ransomwares génériques.** Certains ransomwares sont disponibles sous forme de logiciels génériques que les cybercriminels peuvent acheter sur le darknet et installer sur leurs propres serveurs malveillants. Le piratage et le chiffrement des données et des systèmes sont directement gérés par le logiciel fonctionnant sur les serveurs du cybercriminel. Ce type de ransomwares comprend Stampado et Cerber.
- **RaaS (Ransomware as a Service).** CryptoLocker est peut-être le plus connu des modèles RaaS. Depuis le démantèlement de ses serveurs, CTB-Locker a émergé comme la méthode d'attaque RaaS la plus courante. Autre RaaS qui s'impose rapidement, Tox est un kit que les cybercriminels peuvent télécharger. Il consiste en un fichier exécutable dédié que le cybercriminel peut installer ou distribuer sachant qu'avec ce ransomware 20 % des rançons brutes sont payées en bitcoins.
- **Programmes d'affiliation à un ransomware.** Les cybercriminels qui « s'affilient » peuvent accéder à un modèle RaaS et peuvent le distribuer aux cibles qu'ils ont choisies, engrangeant ainsi jusqu'à 70 % de profit.[12]

- **Attaques des appareils IoT.** Les ransomwares infiltrent les appareils IoT qui contrôlent les systèmes stratégiques d'une entreprise. Ils arrêtent ces systèmes et ne les déverrouillent qu'après le paiement d'une rançon. Comme certains de ces appareils IoT commandent des systèmes stratégiques et vitaux, le non-déverrouillage en temps opportun peut entraîner des dommages substantiels, voire catastrophiques.[13]

Les familles et variantes de ransomwares ont explosé en 2016 en étant multipliées par 10. FortiGuard Labs a détecté de nombreuses nouvelles variantes tous les jours tout au long de 2016. Curieusement, outre un code polymorphe, les ransomwares utilisent fréquemment un code métamorphe pour modifier leur identité numérique sans changer de mode de fonctionnement. Cette croissance rapide et cette constante évolution compliquent encore les choses pour les entreprises qui s'appuient sur des solutions antivirus traditionnelles basées sur les signatures pour se protéger. Le temps qu'une version soit identifiée et ajoutée à la liste noire, les cybercriminels utilisent déjà sur une nouvelle variante. C'est pourquoi, il n'est pas surprenant que près des trois quarts des entreprises ayant été victimes d'une attaque par ransomware en 2016 aient subi une ou plusieurs infections.[14]

Pratiquement tous les systèmes d'exploitation sont désormais ciblés par les ransomwares. Les attaques touchent également le cloud et les appareils mobiles. Par exemple, les attaques par ransomware des appareils Android ont plus que quadruplé en un an, depuis avril 2015.[15]

LE SÉQUENCEMENT TYPE D'UN RANSOMWARE

La majeure partie des attaques par ransomware se répandent par phishing, technique dans laquelle un e-mail provenant prétendument d'une personne ou entreprise connue cible un individu. Historiquement, la diffusion des ransomwares reposait sur la propagation par phishing. Le cas échéant, l'e-mail contient un lien ou une pièce jointe infecté. Ces liens ou pièces jointes sont facilement modifiables offrant ainsi aux cybercriminels la possibilité de préparer des sites récents en masse ou des pièces jointes se limitant à un simple code de téléchargement de composants supplémentaires ultérieurement afin de contourner les filtres de messagerie et atteindre la boîte de réception de l'utilisateur final.

Dans d'autres situations, un utilisateur visite un site ou accède à une application commerciale infectée à partir d'où le ransomware est exécuté. Généralement, le ransomware est configuré pour démarrer et télécharger une charge malveillante plus importante sans que l'utilisateur ne clique sur quoi que ce soit. Enfin, de plus en plus souvent, un appareil IoT infecté permet de contrôler (d'arrêter généralement) des systèmes stratégiques ou vitaux.

En supposant que le ransomware s'exécute correctement, voici le séquencement type :

1. Dès que l'utilisateur clique sur le lien ou la pièce jointe infecté, le ransomware s'exécute via un PowerShell ou une autre extension.
2. L'appareil infecté communique avec le serveur du cybercriminel (généralement par le biais de moyens indirects comme Google Apps) pour obtenir des instructions. Cela comprend fréquemment le téléchargement de nouvelles charges qui vont ensuite chiffrer les fichiers sur l'appareil individuel.
3. Une fois cette étape terminée (qui parfois prend moins d'une minute), une demande de rançon à payer en bitcoins est envoyée en échange d'une clé de déchiffrement.
4. Dans le même temps, le ransomware cherche à se déplacer latéralement au sein du réseau de l'entreprise pour infiltrer d'autres systèmes.

Une stratégie récente des hacktivistes utilisant des ransomwares consiste à cibler et compromettre des serveurs commerciaux vulnérables à l'aide d'un ransomware.[18] Ils peuvent ainsi identifier et cibler des hôtes, multipliant le nombre potentiel de serveurs et d'appareils infectés sur un réseau. La durée de l'attaque est ainsi réduite, ce qui la rend plus virale que les attaques visant un utilisateur final. Cette évolution pourrait se traduire par une hausse du coût des clés de déchiffrement et un allongement du délai de récupération des données chiffrées par les victimes.

INFECTIONS REPOSANT SUR DES SAAS

Dans un sondage réalisé récemment, les professionnels informatiques ont été invités à indiquer à quelles applications SaaS infectées par un ransomware ils ont été confrontés :

- Dropbox, 70 %
- Microsoft Office 365, 29 %
- Google Apps, 12 %
- Box, 6 %
- Salesforce, 3 %

ÉVOLUTION DES RANSOMWARES[16]

Principales familles de ransomwares en 2016

1. Locky
2. CryptoWall
3. CryptXXX
4. Bitman
5. Onion (CTB-Locker)

Principales familles de ransomwares en 2015

1. CryptoWall
2. Blocker
3. Onion (CTB-Locker)
4. Snocry
5. Bitman

97 %

des e-mails de phishing contiennent désormais un ransomware.[17]

AUCUNE IMMUNITÉ

Les entreprises qui pensent être à l'abri des attaques par ransomware car elles disposent de toutes les mesures de sécurité élémentaires doivent y réfléchir à deux fois. Un sondage réalisé auprès des fournisseurs de solutions hébergées a mis en avant que la plupart avaient mis en place une couche de base de protection.[19]

- Logiciels antivirus et anti-logiciel malveillant, 93 %
- Filtres des e-mails et des courriers indésirables, 77 %
- Applications corrigées/mises à jour, 58 %
- Bloqueurs de publicités et de fenêtres contextuelles, 21 %

INFECTION VIRALE

Les ransomwares sont viraux, se répandant à travers les réseaux dans 63 % des cas tandis qu'ils restent isolés sur un système dans les autres cas.[20]

DES ATTAQUES IMPACTANT LA VIE RÉELLE

Les ransomwares affectent presque tous les secteurs industriels et les entreprises de toutes tailles. En termes de pourcentage, l'industrie arrive en haut de la liste avec 16 %, suivie de près par les services publics et le secteur de l'énergie (15,4 %), puis viennent les technologies, les services professionnels, la vente au détail, la santé, les services financiers et le secteur juridique qui représentent une part substantielle. Plusieurs rapports considèrent les services professionnels comme le secteur ayant connu la hausse la plus rapide des attaques de ransomwares.

Voici une étude de l'implication des ransomwares sur certains segments industriels clés à travers des exemples spécifiques d'entreprises piratées qui ont non seulement payé la rançon mais également subi un impact financier et opérationnel conséquent.

LE SECTEUR DE LA SANTÉ

Le secteur de la santé soulève le plus de préoccupations en matière de ransomware. Cela n'a rien de surprenant vu que de nombreux systèmes informatiques et de nombreuses données médicales sont liés aux soins des patients. L'indisponibilité d'un système ou l'impossibilité d'accès aux informations met des vies en danger. Même si l'attaque par ransomware n'affecte ni le système ni les données inhérentes aux soins des patients, la perte de dossiers médicaux peut exposer à des sanctions tangibles sans compter le temps requis pour réparer les dommages.

Dans le cadre du doxxing, les cybercriminels menacent de divulguer les données privées plutôt que de les supprimer. Les répercussions sont toujours plus graves. Ajoutez des attaques par ransomware sur les appareils IoT utilisés pour délivrer les soins aux patients et les implications deviennent mortelles.

Les attaques par ransomware ne vont pas ralentir l'année prochaine, elles devraient même doubler contre les organismes de santé. Par rapport aux autres segments industriels, les données médicales personnelles sont 50 fois plus chères sur le darknet que les informations financières. Les dossiers médicaux volés peuvent valoir 60 dollars chacun.[21] Les exemples d'organismes de santé infectés par un ransomware sont légion. Voyez ces trois exemples :

Les hacktivistes sont parvenus à accéder à la base de données de MongoDB qui contient les données médicales protégées des 200 000 patients de l'*Emery Brain Health Center.* La base de données a été effacée et remplacée par une demande de rançon de 180 000 dollars en bitcoin pour sa récupération.

Le *Hollywood Presbyterian Medical Center à Hollywood (Californie)* a décrété un état d'urgence interne après l'infection de ses systèmes par le ransomware Locky. L'accès des médecins et autres soignants aux dossiers médicaux électroniques a été verrouillé, contraignant le personnel à consigner les informations sur les patients de manière manuscrite et à utiliser la télécopie (à la place du courrier électronique) pour communiquer entre eux. L'hacktiviste a demandé 40 bitcoins (soit environ 17 000 dollars) en échange d'une clé de déchiffrement des fichiers verrouillés, somme payée par l'hôpital.

Pourtant les cybercriminels ne permettent pas toujours à leurs victimes de réaccéder à leurs données. Dans le cas du *Kansas Heart Hospital à Wichita (Kansas)*, l'hôpital a payé la rançon initiale mais les hacktivistes n'ont pas déverrouillé l'intégralité des fichiers. Pour ce faire, ils ont exigé une rançon supplémentaire. Ce n'est qu'à ce moment que l'hôpital a décidé de ne pas payer.

SERVICES PUBLICS ET SECTEUR ÉNERGÉTIQUE

Les services publics et le secteur de l'énergie sont tout autant la cible des cyberattaques que les autres industries. Les systèmes de contrôle industriels (ICS) utilisés pour gérer et exécuter les infrastructures stratégiques des services publics et des compagnies énergétiques offrent de nouvelles opportunités aux cybercriminels, y compris aux hacktivistes utilisant des ransomwares.

Heureusement pour *Lansing Board of Water & Light* qui dessert la ville de Lansing (Michigan), l'attaque par ransomware qui a affecté son ICS, contraignant ainsi l'installation à arrêter son serveur et à couper ses lignes téléphoniques pendant une semaine, ne s'est pas propagée par phishing. L'infection résultait probablement de l'ouverture, par un employé, d'un e-mail contenant un fichier infecté. Le ransomware a rapidement verrouillé l'installation à partir de la messagerie électronique de ce dernier, le système de comptabilité, les imprimantes et les autres technologies. Il a fallu une semaine à l'entreprise pour résoudre le problème et remettre ses systèmes en ligne.

L'INDUSTRIE

L'industrie est en passe de devenir la cible à forte valeur ajoutée des hacktivistes utilisant des ransomwares. Les fabricants courent plus de risques que les autres segments de l'industrie, car ils ne sont pas soumis aux mêmes contraintes réglementaires et de conformités que d'autres secteurs comme les services financiers.

Outre les systèmes informatiques qui contiennent des informations propriétaires et de propriété intellectuelle, les industriels accordent une grande importance à l'efficacité des processus et des opérations. Une interruption peut entraîner une indisponibilité induisant une baisse de la rentabilité financière. Comme « le temps c'est de l'argent », les industriels peuvent trouver un plus grand intérêt à payer la rançon pour récupérer et restaurer leurs systèmes le plus vite possible.

L'année dernière, sur les 8,63 millions d'attaques par ransomware enregistrées chez les industriels, plus des trois quarts ont touché des sociétés de 1 000 employés ou plus. Le botnet Necurs était le principal véhicule de diffusion du ransomware dans le secteur de la fabrication, comptabilisant 41 % de toutes les attaques. Conficker le suit de très loin avec 17,7 %.[23]

Un fabricant de béton s'est retrouvé à l'arrêt pendant plus d'une semaine après que l'un de ses employés ait cliqué sur une pièce jointe infectée par le ransomware CryptoWall dans un e-mail. Le ransomware s'est propagé à travers le réseau de l'entreprise et a chiffré les données comptables et les fichiers stratégiques de plusieurs systèmes de production. Il a été découvert un matin lorsqu'un employé n'a pas pu accéder aux fichiers de production pour lancer la fabrication. Malgré le paiement de la rançon, certains fichiers comptables de l'entreprise étaient toujours verrouillés deux jours plus tard. Sans sauvegarde de ces données, l'entreprise a dû lancer un long projet de récupération de la comptabilité.

L'ÉDUCATION

Les gros titres sur les attaques par ransomware se concentrent généralement sur les brèches dans le secteur de la santé, des services financiers et de l'industrie. Mais l'éducation figure également dans le haut de la liste des entreprises ciblées par les ransomwares. Pourquoi ? Les établissements scolaires possèdent diverses informations (numéros de sécurité sociale, dossiers médicaux, données financières et propriété intellectuelle) qui leur sont propres ou qui concernent le personnel et les élèves de sorte qu'ils constituent des cibles lucratives. Ajoutez à cela que les établissement primaires, secondaires et supérieurs disposent d'une cybersécurité parmi les moins élaborées de l'industrie et, dès lors, il n'y a rien de surprenant à ce que les cybercriminels les prennent pour cible.

L'*université de Calgary* a été victime d'une attaque par ransomware qui a verrouillé son serveur de messagerie électronique. L'établissement a payé une rançon de 16 000 dollars en échange de la clé de déverrouillage des fichiers cryptés. Heureusement, le personnel informatique a isolé l'infiltration avant qu'elle n'ait pu affecter d'autres systèmes.

L'université *Los Angeles Valley College* a payé près de 28 000 dollars en bitcoins après qu'une attaque par ransomware ait verrouillé des centaines de milliers de fichiers sur son réseau informatique, son serveur de messagerie électronique et son système de messagerie vocale. L'infection a été identifiée le 30 décembre 2016 et le collège a choisi de payer la rançon le 4 janvier 2017, un jour après la reprise des cours du semestre d'hiver.

Les ransomwares dans le secteur de l'éducation sont un problème à l'échelle mondiale. L'*université Queen's à Belfast (Irlande)* le sait bien. Trois ransomwares ont infiltré son réseau avec succès l'an dernier. Dans l'un des cas, l'université Queen's a payé une rançon d'environ 600 dollars après que les hacktivistes aient infecté un serveur Windows XP contenant des documents et des images.

LES SERVICES FINANCIERS ET LES BANQUES

L'ampleur des informations que les services financiers et les banques conservent sur leurs clients en font des cibles de choix pour les attaques par ransomware. Les sociétés de services financiers et les banques confirment : elles sont 55 % à considérer les ransomwares comme le principal vecteur de menace de cyberattaque. Près d'un tiers d'entre elles déclarent également avoir perdu entre 100 000 et 500 000 dollars à cause d'attaques par ransomware.[24]

Les coopératives de crédit et les petites banques observent une hausse significative du hacktivisme par ransomware. Elles ont concentré 81 % des incidents totaux touchant les services financiers et les banques en 2016 contre 54 % en 2015.[25] Ceci s'explique principalement par un budget en cybersécurité généralement plus faible que leurs homologues de plus grande taille.

LE SECTEUR PUBLIC

Près de 10 % des organisations impactées par une attaque par ransomware appartiennent au secteur public. Parce que leurs systèmes contiennent des informations stratégiques, les agences gouvernementales constituent une cible attrayante pour les cybercriminels.

L'état de l'Ohio a transmis un avertissement aux municipalités locales l'année dernière en précisant que les attaques par ransomware sont en forte hausse et qu'elles doivent donc tenir compte de cette menace en mettant en place les technologies et processus appropriés.

Plusieurs municipalités locales d'Ohio ont été infectées par un ransomware au cours de l'an dernier. Plus de 170 000 listes des votes du *comté d'Henry* ont été compromises, les hacktivistes menaçant de les divulguer en l'absence du paiement d'une rançon. Aucune rançon n'a été remise et les listes n'ont toujours pas été divulguées.

Les systèmes informatiques du *tribunal du comté de Morrow (Ohio)* ont été infectés par un ransomware. Le comté a choisi de ne pas payer la rançon en bitcoins et les fichiers ont été détruits par les cybercriminels. Malheureusement, les systèmes de sauvegarde du tribunal n'étaient pas à jour et le comté de Morrow ne possédait que des copies papier de ses dossiers. La restauration des fichiers à partir de ces dernières a coûté plus de 30 000 dollars au comté.

Les cybercriminels ciblent même les organismes d'application de la loi. Les systèmes informatiques utilisés par le *bureau du shérif du comté de Lincoln (Maine)* ont été infectés par un ransomware. Après plusieurs tentatives de récupération des données, le bureau a choisi de payer environ 300 dollars en bitcoins à l'hacktiviste.

CONCLUSION

Les cybercriminels ont vu leurs revenus multipliés par 35 avec les attaques par ransomware en 2016. Quant à la fréquence et à la sophistication des attaques, elle va sans nul doute gagner en vélocité et en portée. Les entreprises, de pratiquement toute taille et forme, ne devront pas perdre de vue les conclusions suivantes car les ransomwares évoluent et mutent en une menace toujours plus forte à leur encontre :

1. **Bloquer les menaces connues.** Recherche d'une solution de cybersécurité qui bloque les menaces inhérentes aux ransomwares au niveau de tous les vecteurs d'attaque. Pour ce faire, un modèle de sécurité par couche s'impose. Il doit couvrir le réseau, les terminaux, les applications et les commandes du datacenter grâce à des renseignements généraux et proactifs sur les menaces.
2. **Détecter les nouvelles menaces.** Comme les ransomwares existants ne cessent de se transformer et que de nouveaux ransomwares apparaissent, il est important de développer la technologie Sandbox appropriée et d'autres techniques de détection avancées pour identifier les variantes sur ces mêmes vecteurs.
3. **Neutraliser «l'invisible».** Les informations exploitables en temps réel doivent être partagées entre les différentes couches de sécurité (et les produits des fournisseurs généralement), voire même de manière étendue avec la communauté de cybersécurité élargie extérieure à votre entreprise comme les Computer Emergency Response Teams (CERT), les Information Sharing and Analysis Centers (ISAC) et les coalitions industrielles telles que la Cyber Threat Alliance. Ce partage rapide constitue le meilleur moyen de répondre rapidement aux attaques et de briser la chaîne avant une mutation ou une propagation à d'autres systèmes ou entreprises.
4. **Se préparer à l'inattendu.** La segmentation de la sécurité du réseau facilite la protection contre le comportement de type « ver » des ransomwares comme SamSam et ZCryptor. La sauvegarde et la récupération des données sont tout aussi importantes. Les entreprises qui disposent de sauvegardes récentes des données peuvent refuser les demandes de rançon et récupérer rapidement et facilement leur système.
5. **Sauvegarder les systèmes et les données stratégiques.** Bien que le processus de restauration d'un système puisse prendre du temps, tout en imposant une interruption de l'activité et une baisse drastique de la productivité, restaurer une sauvegarde constitue une bien meilleure option que d'être pris en otage sans garantie que le paiement de la rançon permettra le déverrouillage et la restauration des données et systèmes. Dans ce cas, vous avez besoin de la technologie, des processus et même du partenaire commercial appropriés pour avoir l'assurance que la sauvegarde de vos données satisfera les exigences commerciales et que leur récupération pourra être exécutée efficacement.

[1] « The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things », IDC, avril 2014.

[2] « Non-Malware Attacks and Ransomware Take Center Stage in 2016 », Carbon Black Threat Report, 2016.

[3] Minal Khatri, « Ransomware Statistics – Growth of Ransomware in 2016 », Systweak, 25 août 2016.

[4] « Non-Malware Attacks ».

[5] Ibid.

[6] Khatri, « Ransomware Statistics ».

[7] « State of the Channel Ransomware Report 2016 », Datto, 2016.

[8] Angela Moscaritolo, « Ransomware Hit 40 Percent of Businesses in the Last Year », PC Magazine, 3 août 2016.

[9] Ibid.

[10] « Non-Malware Attacks ».

[11] Adam Chandler, « How Ransomware Became a Billion-Dollar Nightmare for Businesses », The Atlantic, 3 septembre 2016.

[12] Vincent Weafer, « Franchising Ransomware », DARKReading.com, 1er juillet 2015.

[13] Ben Dickson, « What Makes IoT Ransomware a Different and More Dangerous Threat? », TechCrunch, 2 octobre 2016.

[14] « The Complete Guide to Ransomware », Barkly, 30 janvier 2017.

[15] Khatri, « Ransomware Statistics ».

[16] « Non-Malware Attacks ».

[17] « 2016 Q3 Malware Review », PhishMe, octobre 2016.

[18] « Ransomware Getting More Targeted, Expensive », KrebonSecurity.com, 20 septembre 2016.

[19] « State of the Channel Ransomware Report ».

[20] Ibid.

[21] Jennifer Schlesinger, « Dark Web Is Fertile Ground for Stolen Medical Records », CNBC, 11 mars 2016.

[22] Erin Dietsche, « 12 Healthcare Ransomware Attacks of 2016 », Health IT & CIO Review, 29 décembre 2016.

[23] Bill McGee, « Move Over Healthcare, Ransomware Has Manufacturing in Its Sights », Fortinet Blog, 6 juin 2016.

[24] G. Mark Hardy, « From the Trenches: 2016 Survey on Security and Risk in the Financial Sector », SANS Institute, octobre 2016.

[25] « Cyber Attacks on Financial Firms Up; Ransomware Attacks Way Up », Insurance Journal, 22 juillet 2016.

SIÈGE SOCIAL INTERNATIONAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1.408.235.7700
www.fortinet.com/sales

SUCCURSALE EMEA
905 rue Albert Einstein
06560 Valbonne
France
Tél. : +33.4.8987.0500

SUCCURSALE APAC
300 Beach Road 20-01
The Concourse
Singapour 199555
Tél. : +65.6513.3730

AMÉRIQUE LATINE — SIÈGE SOCIAL
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tél. : +1.954.368.9990

TOUR ATLANTIQUE
11ème étage,
1 place de la Pyramide
92911 Paris La
Défense Cedex
France
Ventes: +33-1-8003-1655

9 février 2017