Bulletin Travelers sur le cyberrisque

Pleins feux sur les rançongiciels

LES INTERRUPTIONS DUES À DES **ATTAQUES PAR RANÇONGICIEL** ONT **TRIPLÉ** DE **2018** À **2019**.

Sources : Datto, "Global State of the Channel: Ransomware Report"

Votre entreprise est dans la ligne de mire. Les cybercriminels testent vos défenses, recherchent vos faiblesses. Leur but est de compromettre votre réseau, d'effacer vos sauvegardes et de chiffrer vos systèmes et vos données. Êtes-vous prêt?

L'année dernière, plus de 187 millions de rançongiciels ont été détectés, par seulement une société de sécurité.[1] La plupart des attaques par rançongiciel échoueront, mais celles qui réussissent sont de plus en plus malicieuses.

Les cybermalfaiteurs ne se contentent plus d'exiger des rançons modestes une fois qu'un réseau est compromis; ils demandent plutôt des rançons à six, sept, voire huit chiffres. Selon les données de réclamations de Travelers, le nombre de réclamations liées à des rançongiciels enregistrées, et la gravité de ces pertes, a été multiplié par quatre entre 2017 et 2019.

Pour obliger les entreprises à payer des sommes exorbitantes, les cybermalfaiteurs sont devenus de plus en plus agressifs. Ils creusent plus profondément dans les réseaux des victimes afin d'avoir accès aux systèmes et aux données critiques. Ils suppriment les sauvegardes et, dans certains cas, menacent de divulguer des données sensibles ou confidentielles. Par conséquent, il devient beaucoup plus difficile pour les entreprises de se remettre d'une attaque. Du troisième au quatrième trimestre 2019, le temps d'interruption moyen causé par les rançongiciels est passé de 12,1 jours à 16,2 jours.[2] De nos jours, une entreprise prise au dépourvu par un rançongiciel peut être paralysée, voire forcée de fermer ses portes.

À Travelers, notre objectif est d'aider les entreprises de toute taille et de tout secteur à gérer les cyberattaques existantes et émergentes, y compris les rançongiciels. Dans le présent bulletin de cyberrisque, nous répondons aux questions fréquemment posées au sujet des rançongiciels, y compris la question difficile de savoir si une entreprise attaquée par des cybermalfaiteurs devrait payer ou non la demande de rançon. Nous proposons également des mesures simples et rentables que peuvent prendre les entreprises pour réduire les risques de rançongiciels.

Nous sommes convaincus que toutes les entreprises peuvent bénéficier d'une sensibilisation et d'une vigilance accrues à l'égard de la menace en évolution rapide que représentent les rançongiciels.

Une fois à l'intérieur d'un réseau, les cybermalfaiteurs maximisent l'étendue des dégâts en chiffrant le plus de données possible. Leur objectif est de compromettre le réseau d'une victime à tel point qu'elle ne puisse pas se rétablir, la mettant face à un scénario de paiement.

— Kevin Haley, Symantec Security Response

Bulletin Travelers sur le cyberrisque

Rançon : Payer ou ne pas payer

Lorsqu'une entreprise est victime d'une attaque par rançongiciel, la décision de payer ou non la rançon peut se présenter. Cette décision peut être difficile à prendre : les entreprises et les attaques par rançongiciel sont toutes différentes. La décision devrait être prise selon les conseils de professionnels compétents qui possèdent une expertise en réponse aux attaques par rançongiciel, comme des conseillers juridiques ou des experts en criminalité numérique.

Dans de nombreuses circonstances, les coûts liés à l'engagement de ces professionnels seront couverts par une assurance cyberrisque de Travelers.

Pour décider s'il y a lieu de verser ou non une rançon, voici quelques-uns des points à considérer :

- L'entreprise peut-elle récupérer ses systèmes et ses données sans payer la rançon?
- Le paiement de la rançon réduirait-il le coût global du recouvrement?
- Si la rançon est payée, les criminels fourniront-ils les clés pour déchiffrer les données?

En ce qui concerne la dernière question, il est particulièrement important pour une entreprise de solliciter les conseils de professionnels compétents. Ce n'est pas tous les cybercriminels qui donneront les clés de déchiffrement après le paiement d'une rançon; certains demanderont des paiements supplémentaires, et d'autres refuseront tout simplement de le faire. Un expert en criminalité numérique qui s'occupe fréquemment des réponses aux rançongiciels peut aider à évaluer si cela vaut financièrement la peine de payer la rançon, ou si ce sera seulement une occasion pour le criminel d'extorquer de nouveau l'entreprise.

Certaines entreprises peuvent refuser de verser une rançon par principe.

En bout de compte, la décision de payer ou non appartient à l'entreprise concernée. C'est rarement une décision facile, mais elle peut être facilitée grâce au soutien offert par une police de cyberrisque Travelers.

Examen d'une réclamation

Que se passe-t-il après une attaque par rançongiciel? Bien que chaque réclamation soit différente, l'exemple concret suivant permet d'illustrer ce qui peut arriver, et comment une entreprise peut réussir à se rétablir après une attaque par rançongiciel. La victime décrite dans cette réclamation est une entreprise de services professionnels qui compte 105 employés dans trois bureaux.

Jour -60 : Les cybercriminels compromettent le réseau de la victime. Non détectés, ils obtiennent l'accès à un compte administrateur et peuvent se déplacer sur le réseau en utilisant le protocole Remote Desktop (connexion à distance) pendant deux mois.

Jour 0 : Peu après minuit, le rançongiciel « Ryuk » chiffre tous les serveurs de la victime. Les cybercriminels demandent 150 Bitcoins (BTC), équivalant à ce moment-là à 600 000 $. La victime communique avec Travelers, et un appel est passé le jour même avec un avocat spécialisé dans la confidentialité des données (« Services juridiques ») et une société de criminalité numérique (« Police scientifique »).

> ***Apprenez des erreurs des autres. Vous ne pouvez pas vivre assez longtemps pour les faire toutes vous-mêmes.***
> — Eleanor Roosevelt

Jour 1 : Bien que la victime ait fait des sauvegardes, certains dossiers critiques ne peuvent pas être restaurés. À l'aide des services de cybercriminalité, la victime négocie une baisse de la rançon à 80 BTC et obtient une « preuve de vie », à savoir la preuve que les cybercriminels seront en mesure d'annuler le chiffrement. Les services de cybercriminalité commencent alors à sécuriser le réseau de la victime.

Jour 2 : La police criminelle numérique prend en charge le paiement de la rançon négociée et obtient une clé de déchiffrement. Le processus de déchiffrement est lent, mais la plupart des données de la victime sont restaurées après une semaine. En tout et pour tout, les efforts de recouvrement s'échelonnent sur un mois.

Jour 21 : Les services d'usurpation d'identité et de surveillance du crédit sont mis à la disposition des personnes dont les données personnelles étaient sauvegardées sur l'un des serveurs de la victime.

Jour 86 : La victime rencontre Travelers pour examiner les améliorations qu'elle a apportées à ses contrôles de sécurité et, peu de temps après, renouvelle sa police d'assurance cyberrisque avec Travelers.

À ce jour, plus de 400 000 $ ont été payés pour cette réclamation. Les dépenses couvertes comprenaient le paiement de la rançon elle-même, ainsi que le remboursement des frais juridiques, des services de criminalité numérique, des services de restauration des données et des services de vol d'identité et de surveillance du crédit. L'assurance cyberrisque peut également couvrir les pertes de revenus dues à l'interruption des activités et aux « améliorations », un nouveau type de protection qui peut aider les entreprises à améliorer leurs contrôles après une cyberattaque.

Pour des mesures simples et économiques qui peuvent aider les entreprises à réduire les risques d'attaques par rançongiciel, consultez la page 4.

> ***Nous assistons à un bouleversement, le nombre de réclamations liées aux rançongiciels ayant explosé au cours des dernières années.***
> — John Mullen, Mullen Coughlin, LLC

Rançongiciel : Ce que vous devez savoir

Un rançongiciel, qu'est-ce que c'est?

Le rançongiciel est une forme de logiciel malveillant (« maliciel ») utilisé par les cybercriminels. Lorsque les cybercriminels gagnent accès au réseau de la victime, ils peuvent utiliser cet accès pour dérober des données ou commettre des infractions. Ils peuvent également lancer une attaque par rançongiciel, qui chiffrera les systèmes informatiques et les données de la victime. Les malfaiteurs demandent alors une rançon en échange d'une clé de déchiffrement

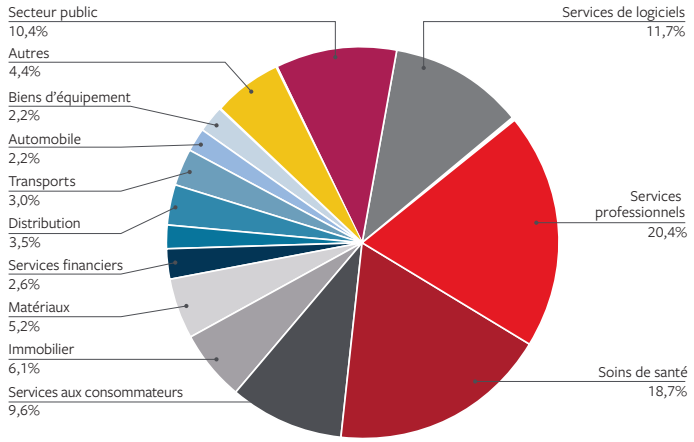
Quelles entreprises sont à risque?

Les entreprises de toute taille et de tout secteur courent le risque d'une attaque par rançongiciel. Les cybercriminels ne font généralement pas de discrimination dans le choix de leurs victimes.

Les forces de l'ordre peuvent-elles aider les victimes de rançongiciels?

La GRC a créé le Groupe national de coordination contre la cybercriminalité (GNC3). Lancé en avril 2020, le GNC3 se concentre sur sa collaboration avec la police pour coordonner les enquêtes de cybercriminalité et partager l'information. La GNC3 travaille également à l'élaboration d'un nouveau système public de signalement des cybercrimes qui ne sera cependant pas lancé avant le mois de mars 2022.[3]

Secteurs les plus couramment ciblés par les rançongiciels au 4e trimestre de 2019



Coveware, "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate."

Comment les rançons sont-elles payées?

Les demandes de rançon sont généralement faites en cryptomonnaie telle que le Bitcoin. Pour le paiement de la rançon, les victimes font habituellement appel à un fournisseur tiers pour l'aider aux négociations et pour s'occuper du paiement.

Existe-t-il une assurance pour les rançongiciels?

Oui. À Travelers, nous offrons une protection contre les rançongiciels, y compris le paiement de la rançon elle-même, les coûts de restauration des données, la perte des revenus en raison de l'interruption des activités, et les frais liés aux services juridiques, aux services de police numérique, et de relations publiques. La protection est également disponible pour l'amélioration qui aide les entreprises touchées à améliorer leurs contrôles après une attaque par rançongiciel. Pour de plus amples renseignements au sujet de l'assurance cyberrisque, communiquez avec votre courtier en assurance.

Un risque émergent : Les fournisseurs de services

De nombreuses entreprises sont fortement dépendantes des fournisseurs de services TI pour gérer leurs réseaux et leurs systèmes. Le recours à un fournisseur de services TI peut donner accès à des technologies et des solutions dont la mise en place à l'interne ne serait pas rentable pour l'entreprise, mais les entreprises doivent être conscientes des risques encourus.

En particulier, il y a un nombre croissant d'incidents liés à des rançongiciels dont la compromission initiale venait du fournisseur de services TI de la victime. Pour atténuer ce risque, les entreprises devraient envisager de mettre en œuvre un programme de gestion des risques par des tiers, notamment :

Exiger une certification de sécurité. Les fournisseurs de services TI peuvent obtenir diverses certifications qui prouvent que leurs propres réseaux et contrôles de sécurité sont à la hauteur. Citons par exemple les normes SOC 2 et ISO 27001.

Obtenir une évaluation de sécurité indépendante. Une entreprise peut vouloir obtenir une évaluation de sécurité indépendante pour s'assurer qu'elle dispose de contrôles adéquats sur la manière dont les fournisseurs de services informatiques accèdent à son réseau. Il se peut qu'une entreprise ne veuille pas se fier uniquement à un fournisseur de services TI pour décider comment ce fournisseur aura accès au réseau de l'entreprise.

S'assurer que les fournisseurs de services TI ont une assurance cyberrisque. Une police de cyberrisque peut aider à garantir que le fournisseur de services TI possède des ressources adéquates pour répondre de façon appropriée en cas de cyberincident, tel qu'une attaque par rançongiciel.

Des mesures simples pour réduire les risques de rançongiciels

Il n'existe pas de solution miracle face aux rançongiciels. Pour se défendre, une entreprise doit disposer d'une cybersécurité globale solide, comprenant des contrôles fondamentaux tels que les pare-feu, la protection des terminaux, le filtrage du courrier électronique et du contenu Web, et la gestion des correctifs.

Néanmoins, il existe des mesures simples et peu coûteuses qui peuvent rendre plus difficile la réussite d'une attaque par rançongiciel. En voici quelques exemples :

Formez vos employés

Les attaques par rançongiciel sont souvent lancées par courriel. Former les employés pour reconnaître et signaler les courriels suspects peut aider à prévenir les rançongiciels. De nombreux clients de l'assurance cyberrisque de Travelers peuvent permettre à leurs employés de recevoir un accès gratuit à des formations de sensibilisation à la cybersécurité de Symantec™, une société Broadcom (non disponible au Québec).

Désactivez les macros Microsoft Office

Si un employé clique sur la pièce jointe d'un courriel malveillant, cela peut provoquer l'exécution d'une « macro » de Microsoft Office qui tentera d'installer un rançongiciel. Bien que les macros soient souvent désactivées par défaut, les utilisateurs peuvent « accepter » et autoriser ainsi l'exécution d'une macro. Pour les entreprises ou les utilisateurs qui n'ont pas besoin de la fonctionnalité des macros Office, il est plus sûr (et gratuit) de désactiver l'ensemble des macros via la politique du groupe.

Bloquez le protocole de connexion à distance (RDP)

Les attaques par rançongiciel peuvent aussi être lancées au moyen du protocole de connexion à distance (RDP). Les entreprises qui n'ont pas besoin de RDP devraient le bloquer à l'externe et, si possible, à l'interne. Cela peut se faire facilement grâce à une configuration simple des pare-feu de l'entreprise.

Renforcer les contrôles des accès privilégiés

Après avoir initialement compromis un réseau, les attaquants tenteront souvent d'obtenir des privilèges administratifs afin d'accéder aux actifs les plus importants d'une entreprise. La plupart des entreprises peuvent renforcer les contrôles des accès privilégiés à moindres frais, en exigeant des utilisateurs privilégiés qu'ils utilisent des mots de passe plus robustes et des comptes administratifs séparés et en interdisant aux utilisateurs réguliers d'avoir des privilèges administratifs locaux. Exiger une authentification multifactorielle pour l'accès privilégié est un moyen encore plus efficace de limiter l'impact d'une attaque par rançongiciel.

Tirez parti des renseignements « open-source »

Les entreprises peuvent utiliser des sources gratuites ou peu coûteuses de renseignements sur les menaces pour se tenir au courant des outils et des techniques utilisés par les cybercriminels et pour mieux adapter leurs défenses.

Revoyez et testez les capacités de sauvegarde et de restauration

Posséder des sauvegardes de données ne suffit plus. Les entreprises doivent s'assurer qu'elles sauvegardent également les ressources réseau critiques, comme les serveurs « Active Directory », ainsi que les logiciels propriétaires et les bases de données qui ne peuvent pas être facilement remplacées. Les sauvegardes doivent être stockées dans un endroit sûr, de sorte que les cybercriminels ne puissent pas les chiffrer ou les supprimer. Enfin, il est essentiel que les entreprises testent leurs capacités de sauvegarde et de restauration au moins une fois par an, pour s'assurer que les sauvegardes seront disponibles au moment où elles en auront le plus besoin.

Au quatrième trimestre 2019, près de 60 % de toutes les attaques par rançongiciel concernaient le protocole de connexion à distance.[2]

Sources et documents supplémentaires

1. SonicWall, "2020 Cyber Threat Report."
2. Coveware, "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate."
3. Le Groupe national de coordination contre la cybercriminalité (GNC3) de la GRC
4. Accenture, "Managing Ransomware: Practical Steps to Avoid Future Attacks."

Pour en savoir plus sur nos cybercapacités, rendez-vous sur travelerscanada.ca

TRAVELERS

travelerscanada.ca