Alerte destinée aux clients : L'épidémie de rançongiciels

Solutions pour la cybersécurité d'Aon et Intervention en cas d'incident de Stroz Friedberg

Selon plusieurs mesures, les rançongiciels sont la principale menace cybernétique qui pèse sur les entreprises à l'heure actuelle[1]. Contrairement à l'atteinte à la protection des données, les attaques par rançongiciel ne se produisent pas de façon discrète. Toute entreprise qui doit pouvoir accéder à des données critiques ou qui est susceptible de connaître des pertes ou des difficultés en cas d'interruption de ses activités pourrait être victime d'un rançongiciel.

L'évolution des attaques

Lors d'une attaque par rançongiciel, les auteurs de la menace parviennent à obtenir un accès non autorisé aux réseaux et aux fichiers d'une entreprise au moyen d'un logiciel malveillant (ou maliciel). Après avoir réussi à y accéder, ces cybercriminels chiffrent les fichiers, les rendant ainsi inaccessibles, et exigent le paiement d'une rançon en cryptomonnaie en échange du ou des codes numériques servant à déchiffrer les fichiers. Les attaques par rançongiciel sont de plus en plus sophistiquées, comprenant, entre autres, des mesures préventives visant à forcer le paiement d'une rançon telles que le repérage et la destruction des copies de sauvegarde des données pour empêcher leur restauration, ou encore le vol des données avant leur chiffrement et la menace d'une diffusion publique. De nombreuses victimes se retrouvent devant un choix difficile : subir une perte permanente de données et une perturbation prolongée de leurs activités ou payer une rançon pour recouvrer leur accès et rétablir leurs activités.

Pour plusieurs victimes de rançongiciels, payer la rançon peut sembler être la seule option viable. Les conséquences possibles de la perturbation des activités et de la perte ou de la divulgation publique de données sensibles sont graves et peuvent comprendre la perte de revenus, la violation de contrats, le non-respect d'échéances, l'incapacité à satisfaire aux attentes des clients, les dommages à la réputation ou même, dans les cas extrêmes, notamment pour les fournisseurs de soins de santé, la perte de vies.

Les statistiques les plus récentes concernant les rançongiciels sont ahurissantes. Le nombre total d'attaques par rançongiciel signalées à l'échelle mondiale a augmenté de 715,8 % de 2019 à 2020[2]. Les paiements de rançon ont également augmenté. En effet, la valeur des paiements a bondi de 60 % depuis l'an dernier[3]. Certains des groupes d'attaques par rançongiciel et certaines des variantes de logiciels malveillants comptant parmi les plus sophistiqués génèrent maintenant plus de 780 000 $ par paiement, en moyenne[4]. Compte tenu de ces taux et de ces montants, il n'est pas surprenant qu'on estime que les dommages attribuables aux rançongiciels s'élèveront à 20 milliards de dollars en 2021[5].

Le casse-tête des paiements

Dans le contexte de cette crise cybernétique, les forces de l'ordre sont restées neutres à l'égard des paiements de rançon. En général, les organismes d'application de la loi incitent les personnes touchées à faire preuve de prudence en ce qui a trait aux risques associés au paiement d'une rançon, et les préviennent que les fichiers de déchiffrement fournis pourraient ne pas fonctionner ou que le paiement d'une rançon pourrait donner lieu à une exploitation accrue. Néanmoins, tous les organismes d'application de la loi s'entendent pour dire que les entités qui subissent des attaques par rançongiciel sont des victimes. Il n'est pas surprenant de constater que, jusqu'à présent, il y a eu peu de poursuites, et encore moins de condamnations, de victimes de rançongiciels qui ont choisi de payer une rançon pour récupérer des dossiers critiques ou rétablir le fonctionnement de systèmes essentiels.

Jusqu'à tout récemment, les décisions difficiles auxquelles étaient confrontées les entités visées par une attaque par rançongiciel (ou les entreprises participant aux activités d'intervention en cas d'incident) ne consistaient pas à déterminer si le paiement d'une rançon constituait un risque juridique. Il s'agissait plutôt de savoir s'il était judicieux sur le plan des affaires de payer la rançon et, dans l'affirmative, de déterminer comment communiquer avec l'auteur de la menace aux fins de négociation et comment s'y retrouver dans l'univers souvent mal connu de la cryptomonnaie afin d'effectuer le paiement. Une fois le paiement versé, le processus de déchiffrement, souvent long et laborieux sur le plan technique, constituait le problème le plus difficile auquel l'entité touchée était confrontée.

Découvrez comment nos solutions de cybersécurité peuvent vous aider.

Visitez le site
aon.com/cyber-solutions
ou contactez
cyber.deal.desk@aon.ca

Empower Results®

Si une entité victime d'un rançongiciel faisait appel aux forces de l'ordre ou les informait de la situation, c'était dans l'espoir de recevoir des conseils ou d'obtenir justice (si les forces de l'ordre étaient en mesure d'identifier les auteurs de la menace). Malgré la volonté des forces de l'ordre de collaborer avec les entreprises visées, la hausse des attaques par rançongiciel a rendu nécessaire la sélection des dossiers à traiter selon un ordre de priorité. Les dossiers que les organismes d'application de la loi pouvaient prendre en charge étaient axés sur le mandat de ces derniers consistant à mener des enquêtes et à traduire les contrevenants en justice. Ce mandat, combiné à la quantité diluvienne d'enjeux liés aux rançongiciels, fait en sorte que les entités visées qui informent les forces de l'ordre et collaborent avec elles continuent de s'occuper elles-mêmes de la plupart des aspects de l'enquête liée à l'intervention en cas d'incident, y compris l'analyse des causes fondamentales de l'incident, l'étendue de l'intrusion et le rétablissement des affaires.

L'effet « Evil Corp »

Le contexte des paiements de rançons dans le cadre d'attaques par rançongiciel a commencé à changer lorsqu'un groupe sophistiqué d'auteurs de menaces basé en Russie et appelé Evil Corp (par l'intermédiaire de certains de ses membres connus) a fait son apparition pour la première fois sur la liste des ressortissants expressément désignés (Specially Designated Nationals [SDN]) de l'Office of Foreign Assets Control (OFAC) du département du Trésor,
tout comme plusieurs autres cybercriminels. Comme d'autres auteurs de menaces sophistiqués, Evil Corp est passé à la monétisation facile des rançongiciels. Cependant, ce qui distinguait le réseau Evil Corp de nombreuses autres entreprises criminelles, c'était les logiciels malveillants complexes qu'il avait développés. De manière générale, la communauté du renseignement sur les menaces estimait que les logiciels malveillants de Evil Corp étaient utilisés de façon singulière par Evil Corp et qu'ils n'étaient pas partagés avec d'autres entreprises criminelles. Plus précisément, selon de nombreux membres de la communauté du renseignement sur les menaces, le dangereux logiciel malveillant « WastedLocker » utilisé dans de nombreuses attaques par rançongiciel dévastatrices appartiendrait exclusivement à Evil Corp.

Le contrôle diligent relatif à la liste des SDN de l'OFAC visait auparavant à déterminer si les portefeuilles de cryptomonnaie facilement modifiables utilisés pour recevoir des paiements de rançon pouvaient être liés à des groupes d'auteurs de menaces en particulier susceptibles de figurer sur la liste des SDN de l'OFAC. En général, ce n'était pas le cas, de sorte que très peu de paiements de rançon dans le cadre d'attaques par rançongiciel ont été touchés par le contrôle diligent relatif à l'OFAC. Cependant, dans les cas où le logiciel malveillant WastedLocker était en cause dans l'attaque par rançongiciel, il se peut que le contrôle diligent relatif à la liste des SDN de l'OFAC mène à la conclusion que le destinataire de la rançon était une personne ou une entité bloquée sans qu'il soit déterminé indépendamment que le portefeuille de cryptomonnaie utilisé par le pirate informatique pour recevoir le paiement était associé à Evil Corp ou à un autre SDN connu.

Avis des départements du Trésor et de la Justice

Récemment, le gouvernement fédéral des États-Unis a publié deux documents importants sur les cryptomonnaies et le paiement de rançons dans le cadre d'attaques par rançongiciel. Ces documents ont probablement été publiés en réponse aux pressions croissantes exercées sur les forces de l'ordre et le milieu des affaires en raison de l'ampleur de l'épidémie de rançongiciels, de l'augmentation des questions au sujet de paiements potentiels à des personnes ou à des entités bloquées, et de la nécessité de disposer de directives sur les précautions à prendre avant de verser un paiement et sur la façon de collaborer avec les forces de l'ordre et les organismes de réglementation.

Le 1er octobre 2020, le département du Trésor a publié un avis d'information sur le paiement de rançons dans le cadre d'attaques par rançongiciel. Celui-ci rappelait au public plusieurs dispositions préexistantes importantes relatives à l'intervention en cas d'incident dans le contexte d'une attaque par rançongiciel.

Le 9 octobre 2020, le département de la Justice a publié son cadre d'application de la réglementation en matière de cryptomonnaie (Cryptocurrency Enforcement Framework), qui décrit notamment :

- l'utilisation actuelle de la technologie des cryptomonnaies et la façon dont des individus malveillants ont abusé de cette technologie;
- les lois et règlements en vigueur qui régissent les transactions en cryptomonnaie au niveau fédéral;
- les difficultés liées aux cryptomonnaies sur le plan de la sécurité publique.

Les principaux éléments à retenir de ces documents sont :

- Les forces de l'ordre continueront de traiter les entités touchées par des rançongiciels comme des victimes. Rien dans ces documents n'indique une intention contraire.
- Les cryptomonnaies ont des usages légitimes et illégitimes. Les transferts de fonds inadmissibles à des entités figurant sur la liste des SDN de l'OFAC – tout comme le blanchiment d'argent et l'évasion fiscale – sont expressément identifiés comme constituant un usage illégitime de la cryptomonnaie.
- Les transactions en cryptomonnaie, qu'elles soient effectuées dans le cadre du paiement d'une rançon ou autrement, peuvent être réglementées, notamment en vertu des règlements du Financial Crimes Enforcement Network (FinCEN). Les règlements peuvent varier toutefois en fonction de plusieurs facteurs, dont le montant de la transaction, la source du paiement et le destinataire.

- Bien que ce soit considéré comme une pratique exemplaire, aucun des deux documents mentionnés ne renferme une nouvelle exigence selon laquelle une entité doit informer les forces de l'ordre si elle est victime d'une attaque par rançongiciel ou si un paiement est versé dans le cadre d'une telle attaque. Cela semble demeurer à la discrétion de l'organisation touchée, à moins que d'autres règlements déjà en vigueur ne soient en cause. Au moment de prendre leur décision, les entreprises devraient toutefois tenir compte des avantages de collaborer avec les forces de l'ordre (et de les aviser du paiement), notamment celui de tirer parti de l'expérience acquise par les forces de l'ordre auprès d'auteurs de menaces lors de divers incidents survenus dans divers secteurs.
- Le contrôle diligent relatif à la liste des SDN de l'OFAC et aux territoires bloqués doit faire partie intégrante du processus précédant le paiement d'une rançon liée à une attaque par rançongiciel de toute organisation.
- S'il est établi qu'une rançon sera probablement versée à une entité figurant sur la liste des SDN de l'OFAC, les directives du département du Trésor sont claires : agissez en étant avisé. À ce stade, il serait imprudent d'envisager de verser une rançon sans d'abord faire appel à un conseiller juridique, aux forces de l'ordre et aux organismes gouvernementaux pertinents.
- Les avis du département du Trésor semblent reconnaître implicitement qu'il est possible de verser une rançon à une entité figurant sur la liste des SDN de l'OFAC sans le savoir. S'il est établi ultérieurement qu'un tel paiement a eu lieu, les facteurs d'atténuation comprendraient probablement le signalement aux forces de l'ordre et le recours à celles-ci, ainsi que l'existence et la qualité du contrôle diligent relatif à la liste des SDN de l'OFAC effectué avant le paiement de la rançon.
- Aucune réponse n'est fournie en ce qui a trait à la situation la plus délicate, soit celle où la victime d'un rançongiciel effectue un contrôle diligent et détermine que l'auteur de la menace figure, ou est susceptible de figurer, sur la liste des SDN de l'OFAC. L'entité victime est alors confrontée à un choix impossible : effectuer un paiement qui pourrait être considéré comme étant illégal ou se retrouver avec des systèmes irrécupérables pouvant entraîner des dommages importants, voire fatals, à l'entreprise. Dans une telle situation, la meilleure façon de procéder pour une entité victime serait la suivante : i) retenir les services d'un conseiller juridique et collaborer avec lui; ii) informer les forces de l'ordre et les organismes de réglementation pertinents et collaborer avec eux. En procédant ainsi, il est possible que l'entité victime puisse atténuer ou même éviter de lourdes poursuites si elle en vient à payer une rançon à un SDN figurant sur la liste de l'OFAC sous l'effet de la contrainte.

Stratégies d'atténuation des risques

Bien souvent, les pirates informatiques à l'origine d'attaques par rançongiciel mènent leurs activités avec la même discipline et la même approche que les entreprises traditionnelles, à la différence près qu'ils mènent des activités criminelles délibérées. Les auteurs de menaces choisissent généralement la voie de la moindre résistance pour atteindre leurs objectifs d'affaires. Ils s'en prennent à des entreprises vulnérables en tirant parti d'exploits courants ou de lacunes sur le plan de la cyberdéfense et de la préparation. Pour réduire les risques d'être victime d'un rançongiciel et mieux vous préparer à l'éventualité d'un incident lié à un rançongiciel, suivez les huit conseils qui suivent :

1 **Soyez proactif** — Être victime d'un rançongiciel est une expérience bouleversante qui met à l'épreuve la réponse émotionnelle en cas de crise, les procédures de transmission à un échelon supérieur, la performance technique, les plans de continuité des activités et les compétences en communication d'une organisation, en particulier parce que cette dernière est parfois appelée à interagir directement avec les auteurs de la menace. Assurez-vous que le plan et les manuels d'intervention en cas d'incident et le plan de continuité des opérations ou de reprise après sinistre ont récemment été évalués, révisés et mis à jour. Plus important encore, mettez ces plans et ces manuels à l'essai en réalisant des simulations réalistes dans le but d'accroître la résilience de l'organisation.

2 **Sensibilisez les employés à la cybersécurité et à l'hameçonnage** – L'hameçonnage demeure l'une des principales causes d'accès non autorisé à un réseau d'entreprise, notamment lorsqu'il sert de point d'entrée en vue d'une attaque par rançongiciel. Former les utilisateurs pour qu'ils puissent non seulement repérer les courriels d'hameçonnage, mais aussi les signaler à leur équipe de cybersécurité interne est une étape essentielle à réaliser pour pouvoir détecter les premiers stades d'une attaque par rançongiciel. Les entreprises doivent créer une culture au sein de laquelle tous les employés se sentent responsables de la sécurité de l'entreprise et sont encouragés à participer à la détection proactive des menaces, des risques et des attaques, ainsi qu'aux efforts de protection contre ceux-ci. La sensibilisation à l'hameçonnage est un élément crucial de la création d'une telle culture de cybersécurité.

3 **Ayez recours à l'authentification à facteurs multiples ou en deux étapes** – L'authentification à facteurs multiples (p. ex., un mot de passe – quelque chose que l'employé connaît – et une clé d'authentification – quelque chose que l'employé possède) pour toutes les formes de connexion et d'accès aux courriels, aux ordinateurs distants, aux systèmes infonuagiques ou destinés à l'externe et aux réseaux (p. ex., paie, suivi des heures, mobilisation des clients) devrait être une exigence pour tous les utilisateurs. Dans de nombreuses situations, mais pas dans tous les cas, le recours à l'authentification à facteurs multiples peut même empêcher l'exploitation d'identifiants de connexion volés, car le pirate informatique ne possède pas le deuxième élément nécessaire à l'ouverture de session, soit la clé d'authentification. Il est important de veiller à ce que la configuration multifactorielle soit appropriée. Les contrôles d'accès à facteurs multiples peuvent s'avérer encore plus efficaces s'ils sont combinés à l'utilisation d'un réseau privé virtuel (RPV).

4 **Assurez-vous que vos systèmes sont à jour et que tous les correctifs nécessaires y sont apportés** – L'activité de cyberhygiène de base qui consiste à installer les mises à jour et les correctifs requis est souvent négligée. Cela est particulièrement vrai alors que les équipes responsables des opérations et de la sécurité sont débordées, que les systèmes et les terminaux vieillissent et sont remplacés et que de nouveaux systèmes, du nouveau matériel et de nouvelles applications sont introduits au fil de la croissance, de la maturité, de la fusion et de la cession des entreprises. Il existe – et il existera toujours – d'importantes vulnérabilités non corrigées qui permettent aux pirates informatiques de compromettre les réseaux d'entreprise. Les pirates peuvent souvent repérer un système vulnérable en procédant à un simple balayage Internet au moyen d'outils gratuits. Ils se livrent à cet exercice de façon globale et aléatoire, à la recherche de systèmes exploitables où ils pourront déployer leurs rançongiciels et autres cyberattaques.

5 **Installez et configurez adéquatement des outils de détection et de réponse des terminaux** – Les outils axés sur la détection et la réponse des terminaux peuvent contribuer à réduire les risques d'attaque par rançongiciel, en plus d'être utiles dans le processus d'enquête et d'intervention relatif aux incidents. Toutefois, bien des entités qui investissent dans ces outils ne les configurent pas de façon à ce qu'ils soient efficaces en cas de cyberincident et d'enquête. Disposer d'outils de sécurité bien configurés renforce grandement la capacité à détecter, à signaler et à bloquer les actions d'auteurs de menaces.

6 **Concevez vos réseaux, vos systèmes et vos copies de sauvegarde de façon à réduire l'incidence des rançongiciels** – Assurez-vous que vos comptes privilégiés font l'objet d'un contrôle rigoureux. Segmentez votre réseau pour réduire la propagation des éléments criminels ou des logiciels malveillants. Mettez en place de solides systèmes de consignation et d'alerte pour améliorer la détection et le rassemblement de preuves en cas d'incident. Il est important de disposer d'une stratégie de sécurité technique basée sur les conseils d'architectes qui connaissent les dernières tendances en matière d'attaques et d'éléments criminels, et de tirer parti d'une surveillance continue des renseignements sur les menaces dans les sources ouvertes et sur le Web invisible.

7 **Envisagez d'avoir recours à des options de transfert des risques** – Comme une attaque par rançongiciel peut mettre en péril la réputation d'une entité et la confiance du public à son égard, il est impossible de contrôler ou de transférer entièrement le risque de rançongiciel. Toutefois, dans le cadre de leur préparation en cas de rançongiciels, les organisations devraient songer à souscrire une cyberassurance appropriée. Ce faisant, les organisations devraient s'attarder à ce que la protection d'assurance prévoit en matière d'indemnisation pour les pertes financières, l'interruption des activités, les frais associés à la rançon et l'intervention en cas d'incident, ainsi qu'en matière de fournisseurs de services, par exemple la possibilité de faire appel aux fournisseurs de services d'intervention en cas d'incident de leur choix.

8 **Constituez à l'avance votre équipe externe d'intervention en cas d'incident** – Une intervention efficace en cas d'attaque par rançongiciel comprend souvent le recours, en totalité ou en partie, à l'expertise de tiers des domaines de l'intervention judiciaire en cas d'incident, des conseils juridiques, des communications en cas de crise, ainsi que de la négociation et du paiement de rançon. Le fait de rechercher, d'évaluer et de mobiliser ces professionnels pendant un incident lié à un rançongiciel constitue un fardeau supplémentaire pour l'entreprise déjà mise à rude épreuve et ne produit pas les résultats escomptés lorsque chaque seconde compte et que chaque décision est critique. Comme ces situations nécessitent une réponse rapide, il est essentiel de sélectionner et d'engager au préalable une équipe de professionnels qui exercera une surveillance et sera prête à intervenir en cas d'attaque par rançongiciel.

AON
Empower Results®

Personnes-ressources :

Chad Pinson
Président, Expertise judiciaire numérique et intervention en cas d'incident,
Gestion de la mobilisation et Enquêtes
Stroz Friedberg
+1 214 377-4553
chad.pinson@strozfriedberg.com

Jonathan Rajewski
Vice-président, Expertise judiciaire numérique et intervention en cas d'incident
Stroz Friedberg
+1 802 238-8530
jonathan.rajewski@strozfriedberg.com

Stephanie Snyder
Vice-présidente principale et chef, Stratégie commerciale
Solutions de risques cybernétiques d'Aon
+1 312 381-5078
stephanie.snyder@aon.com

Sources

1. **Ransomware Is the No. 1 Cyber Threat This Year. Here's What You Can Do. (en anglais seulement)**
2. **Rapport de mi-année 2020 de Bitdefender sur les menaces (en anglais seulement)**, page 14
3. **Rapport de Coveware sur les rançongiciels (en anglais seulement)**, le 3 août 2020
4. **Coveware (en anglais seulement)**, le 23 janvier 2020
5. Cybersecurity Ventures, **https://www.thesslstore.com/blog/ransomware-statistics/ (en anglais seulement)**
6. **Document du FBI sur la prévention des rançongiciels et l'intervention en cas d'attaque pour les RSI (en anglais seulement)**
7. **Directive présidentielle 30 de Barack Obama (en anglais seulement)**

À propos de Solutions de cybersécurité: Solutions de cybersécurité d'Aon offre une approche globale de la gestion des cyberrisques, des compétences inégalées en investigation, ainsi que des technologies exclusives qui aident les clients à repérer et à quantifier les cyberrisques, à protéger les actifs essentiels et à se rétablir après des cyberincidents.

À propos d'Aon : Aon plc (NYSE : AON) est le principal fournisseur mondial d'une vaste gamme de solutions pour la gestion du risque, des régimes de retraite et des programmes de santé. Nos 50 000 employés de 120 pays génèrent des résultats pour les clients grâce à des données et à des analyses exclusives produisant des points de vue permettant de réduire la volatilité et d'améliorer le rendement.

Empower Results®