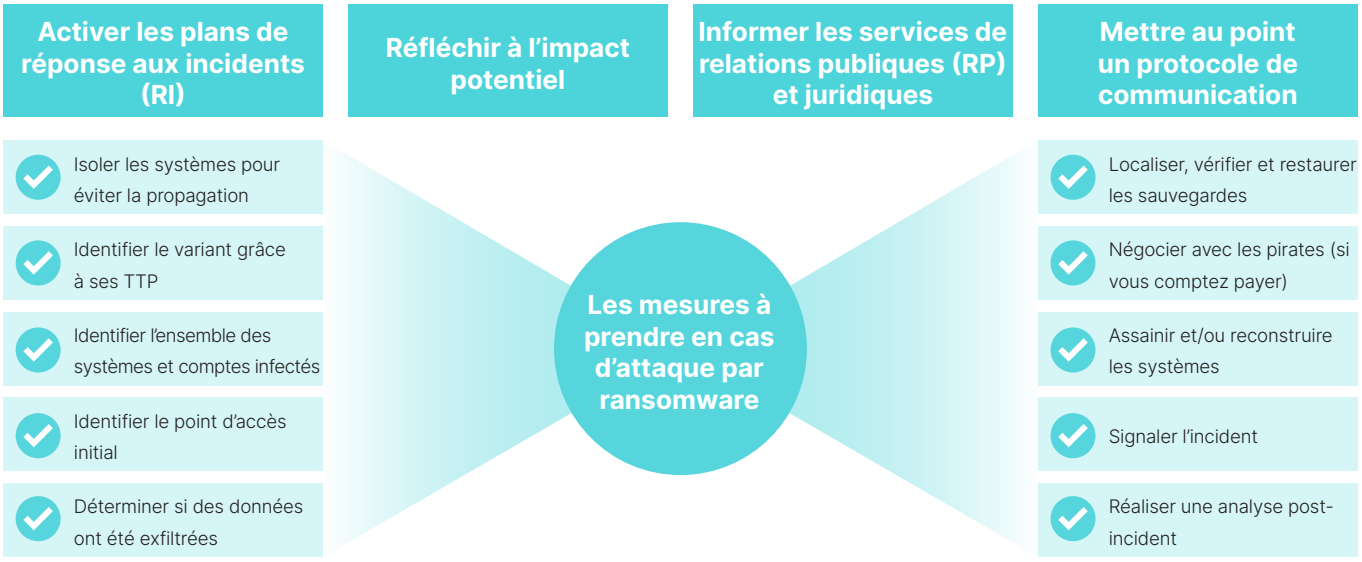
CHECKLIST

Que faire lorsque l'on est victime d'une attaque par ransomware



Plus de 187 millions d'attaques par ransomware ont eu lieu en 2019. Cela représente plus de 500 000 offensives menées chaque jour à l'encontre d'entreprises. Si vous n'en avez pas encore été victime, il y a malheureusement de bonnes chances que ce ne soit plus qu'une question de temps. Et si vous avez déjà subi un piratage, cela ne vous rend pas immunisé pour autant. Dans l'hypothèse d'une récidive, il vous faut absolument savoir comment minimiser l'impact d'un tel événement sur vous, votre équipe et votre entreprise.

Voici une brève vue d'ensemble des étapes à suivre pour faire face à une attaque active par ransomware :

Les mesures à prendre en cas d'attaque par ransomware

Premièrement : ne paniquez pas !

- Il vous faudra réagir rapidement, mais de façon méthodique. Restez calme et, le cas échéant, lancez les premières étapes de votre plan de réponse aux incidents (RI). En l'absence d'un tel plan, contactez votre fournisseur de technologies de sécurité. Notez également la date du signalement de l'incident à votre compagnie d'assurance : cette dernière est en effet susceptible de vous proposer une liste de prestataires expérimentés et formés pour vous aider.
- Réfléchissez à l'impact potentiel de l'incident. Tenez compte non seulement des ressources manifestement compromises, à l'image des données en cours de chiffrement et des applications en panne, mais aussi d'autres actifs.
- Informez vos services de relations publiques et juridiques afin qu'ils puissent se préparer. Faites-leur savoir que vous comptez mettre en place une structure de communication et de reddition d'informations plus formelle à mesure que vous collecterez des renseignements.
- Mettez au point un protocole de communication avec un individu désigné au sein de chacun de vos services. Par exemple, engagez-vous à tenir les équipes concernées au courant de l'évolution de la situation toutes les trois heures. Ce point est important pour éviter qu'elles ne viennent constamment s'enquérir de l'évolution de la situation, et ne se contentent de contenir l'attaque.

Isolez vos systèmes pour éviter la propagation

- Différentes options sont à votre disposition pour isoler la menace et l'empêcher de se propager. Si l'incident est d'ores et déjà répandu, envisagez de mettre en place des systèmes de blocage au niveau du réseau — qu'il s'agisse d'isoler le trafic au niveau du switch ou du pare-feu de périphérie, ou de couper temporairement la connexion à Internet. Si l'ampleur de l'incident est déjà confirmée comme étant plus limitée et que seuls quelques systèmes ont été infectés, il est possible de n'isoler que ceux-ci au niveau des dispositifs, par exemple en débranchant le câble Ethernet ou en déconnectant la connexion sans fil. Si vous possédez des technologies de détection et de réponse sur les vos terminaux (EDR), vous pouvez également adopter une approche plus chirurgicale et bloquer l'attaque au niveau du processus, ce qui serait l'option la plus rapide et perturbant le moins vos activités. N'oubliez pas de tenter de garder tous les systèmes sous tension afin d'éviter de la perte de preuves. Et souvenez-vous qu'en interférant avec l'activité de cybercriminels, vous les informez que vous êtes au courant de leur intrusion. Le risque est donc qu'ils se fassent passer pour morts, ce qui compliquerait l'identification de l'ampleur de l'attaque.
- Si la situation l'exige, prenez des images des disques durs et de la mémoire des systèmes infectés à des fins d'investigation numérique. Cependant, n'essayez pas ceci si vous ne l'avez jamais fait auparavant. Cela ne doit pas être la première fois que votre équipe tente de recueillir ces informations, aussi confiante soit-elle.

Si vous utilisez des outils en ligne ou cloud, n'oubliez pas que tout document que vous chargerez est susceptible d'être examiné par des entités publiques.

Identifiez le variant du ransomware

- Beaucoup des tactiques, techniques et procédures (TTP) d'une attaque sont documentées publiquement pour chacun de ses variants. Le fait de déterminer à quelle attaque vous avez affaire peut vous donner des indices quant aux endroits où chercher la menace et sur sa propagation, et vous fournir des détails sur sa persistance.
- En fonction du variant, des outils de déchiffrement sont peut-être disponibles pour vos fichiers. Le site web No More Ransom est une bonne référence pour trouver de tels outils. Souvent, la demande de rançon elle-même donne un bon indice du groupe et/ou du variant de ransomware utilisé. En outre, en chargeant le ransomware sur ID Ransomware, il est possible de l'identifier.
- Si vous utilisez des outils en ligne ou cloud, n'oubliez pas que tout document que vous chargerez est susceptible d'être examiné par des entités publiques.

Identifiez le point d'accès initial

- En identifiant le point d'accès initial, ou le patient zéro, vous pourrez combler les lacunes de votre système de sécurité. Les vecteurs classiques sont le phishing, les exploits sur vos services edge (à l'image des services Bureau à distance), ainsi que l'utilisation non autorisée d'identifiants. Parmi les autres vecteurs initiaux figurent les attaques en drive-by, les exploits ciblant des sites web et applications destinées au grand public, les supports amovibles, l'ajout de dispositifs de piratage, ainsi que les attaques sur les chaînes d'approvisionnement.
- Cette étape peut s'avérer difficile, et vous avez pourriez avoir besoin du soutien d'experts et de consultants en investigation numérique ou en réponse aux incidents afin de déterminer le point d'accès initial.

Identifiez l'ensemble des systèmes et comptes infectés (ampleur)

- Même une fois l'attaque terminée, il est plus que probable que les pirates aient encore un pied sur votre réseau. Il est donc essentiel d'identifier tout logiciel malveillant encore actif ou éléments nuisibles persistants toujours en communication avec le serveur de commande et de contrôle (C2). Les principales techniques de persistance sont :
  - la création de nouveaux processus exécutant des charges utiles malveillantes
  - l'utilisation de clés d'exécution dans le registre
  - la création de nouvelles tâches planifiées.

- En outre, vos assaillants peuvent avoir compromis plusieurs comptes disposant ou non de privilèges administratifs, à l'image des comptes Active Directory (AD). Il convient donc de les désactiver. Assurez-vous également qu'aucun compte indésirable ne soit en cours de création. D'autres composants Active Directory, à l'image des Objets de stratégie de groupe (GPO), devront être examinés à la recherche d'éléments récemment créés ou modifiés. Il s'agit en effet d'une tactique fréquemment utilisée par les pirates pour diffuser la charge utile de leur ransomware sur l'ensemble des systèmes.
- Documentez vos trouvailles avant de prendre des initiatives. Toute action de votre part est susceptible d'alerter les cybercriminels et de les pousser à lancer une attaque bien plus sérieuse. Vous risquez également de réduire votre capacité à récupérer vos données, ou à déterminer l'impact complet du piratage.

Souvent, les pirates tentent de corrompre vos sauvegardes en ligne. Il vous faudra donc contrôler que les données disponibles sont les bonnes et sont récupérables.

Déterminez si des données ont été exfiltrées

- Souvent, les attaques par ransomware exfiltrent vos données en plus de chiffrer vos fichiers. Les pirates augmentent ainsi leurs chances que vous payiez la rançon en menaçant de publier des informations propriétaires ou embarrassantes en ligne. Cherchez des signes d'exfiltration sur vos pare-feu de périphérie, à l'image de transferts massifs de données. Cherchez également des signes de communications suspectes depuis des serveurs jusqu'à des applications de stockage dans le cloud, à l'image de Dropbox ou d'AWS. Si vous avez mis en place une solution CASB (passerelle d'accès cloud sécurisé), celle-ci sera votre principale source d'informations avec les journaux des pare-feu.
- Cette étape peut s'avérer difficile, et peut nécessiter une fois de plus de faire appel à une équipe d'experts ou de consultants en investigation numérique ou en réponse aux incidents, afin de mener une enquête approfondie.

Localisez vos sauvegardes et vérifiez leur disponibilité

- Une attaque par ransomware tentera d'effacer vos sauvegardes en ligne et vos clichés instantanés pour réduire vos chances de récupérer vos données, et vous pousser à payer la rançon. Assurez-vous que vos technologies de sauvegarde ne sont pas affectées par l'incident et restent opérationnelles. Puis, vérifiez si vous disposez de sauvegardes en ligne ou hors ligne.
- Souvent, les pirates tentent de corrompre vos sauvegardes en ligne. Il vous faudra donc contrôler que les données disponibles soient les bonnes et soient récupérables.

Vérifiez l'intégrité de vos sauvegardes, et restaurez vos systèmes au dernier point stable

- Souvent, lors d'attaques par ransomware, les pirates ont infiltré le réseau depuis plusieurs jours, voire des semaines avant de décider de chiffre des fichiers. Il est donc possible que des sauvegardes contiennent elles aussi des charges utiles malveillantes qu'il conviendra alors de ne pas restaurer sur un système neuf. Grâce à votre travail d'investigation sur l'incident, vous devriez avoir une bonne idée de la date et de l'heure de l'accès initial. Essayez d'effectuer une sauvegarde datant de la veille. Quoi qu'il en soit, il vous faudra quand même analyser les fichiers afin d'en vérifier l'intégrité.

Assainissez ou créez de nouveaux systèmes

- Si vous êtes confiants dans votre capacité à identifier l'ensemble des logiciels malveillants et incidents persistants sur vos systèmes, vous gagnerez peut-être du temps en vous contentant de les nettoyer. Cependant, il sera probablement plus simple et sûr de créer de nouveaux systèmes immaculés. Vous avez même la possibilité de mettre en place un environnement distinct tout neuf vers lequel migrer. Cela ne devrait pas prendre trop de temps si vous utilisez un environnement virtuel. Veillez simplement à installer des contrôles de sécurité et à respecter les meilleures pratiques en vigueur lors de la reconstruction ou de l'assainissement de votre réseau ou segment de réseau, afin d'éviter la réinfection des appareils.

Signalez l'incident

- C'est le moment de retourner rendre visite aux membres de votre service juridique. Il est important de rendre compte de la situation à toutes les entités, y compris à votre compagnie d'assurance. Il vous faudra également déterminer la nécessité d'effectuer un signalement aux forces de l'ordre.
- Votre service juridique peut vous aider à satisfaire vos obligations légales relatives aux données réglementées (sur les cartes de paiement ou encore de santé, etc.). Que vous ayez ou non contracté une assurance cyber risques, il possible que votre assureur prenne en charge une partie des coûts de restauration. En outre, si vous devez faire appel à une société tierce de réponse aux incidents, votre compagnie est susceptible d'avoir une liste d'entreprises que vous pourriez embaucher pour vous aider dans votre investigation.

- Déterminez si vous comptez publiquement révéler l'attaque au grand public. Dans certains cas, il est possible que vous soyez légalement obligé de divulguer certains, voire tous les détails. Découvrez combien de temps vous avez pour révéler l'attaque, le cas échéant. Vos services juridiques devraient être en mesure de vous assister dans cette recherche une fois que vous aurez déterminé le type de données susceptibles d'avoir été compromises. Mais n'oubliez pas que le fait d'informer les forces de l'ordre peut entraîner la création d'un fichier public équivalent à la publication d'une annonce destinée au grand public.
- Si l'attaque est grave, et si votre entreprise est présente sur différentes régions dans le monde, il vous faudra peut-être contacter les forces de l'ordre national au lieu de services locaux ou régionaux. Aux États-Unis, cela reviendra à contacter votre bureau du FBI le plus proche.
- Si vous êtes membre du programme InfraGard du FBI, utilisez ces ressources dans le cas où votre organisation s'apprête à signaler un incident aux forces de l'ordre. Dans le cas contraire, ou si vous ignorez comment utiliser ces services, le Centre de plainte pour les crimes sur Internet du FBI (Internet Crime Complaint Center) est à votre disposition.

Il est essentiel de revoir votre plan de réponse aux incidents afin de comprendre ce qui a fonctionné et de noter vos axes d'amélioration.

- Selon les circonstances, le fait de contacter les autorités peut s'avérer bénéfique, en particulier si l'on tient compte des ressources supplémentaires qu'elles sont susceptibles de fournir pour aider à gérer votre incident. Dans certains cas, elles seront également en mesure de vous aider à localiser vos fichiers exfiltrés. En outre, le dépôt d'une déclaration à la police peut être nécessaire pour votre assurance cyber risques (il reviendra à votre service juridique de déterminer si cela est requis ou non).

Prêt à payer ? Négociez d'abord

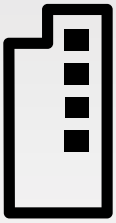
- Les autorités désapprouvent le paiement des rançons. Cependant, si tel est votre cas, faites appel aux services d'une société de sécurité compétente pour vous aider à négocier le montant de la rançon. Les pirates sont généralement prêts à faire des concessions. Votre service juridique ou votre avocat indépendant dispose généralement d'une liste de négociateurs recommandés. Sachez néanmoins que le paiement d'une rançon exigée par certains acteurs (à l'image d'États faisant l'objet de sanctions économiques) peut constituer une infraction aux règles du Bureau de contrôle des avoirs étrangers (OFAC) des États-Unis, et vous rendre passible d'une amende supplémentaire. Rendez-vous ici pour en savoir plus.
- Gardez également en tête que les négociations prendront du temps. Ne négociez que pour récupérer vos données. Et n'oubliez pas non plus que vous n'avez aucune garantie que le fait de traiter avec vos pirates les empêche de supprimer vos données ou de les rendre publiques.
- Lors de négociations, si les pirates affirment avoir dérobé vos données, demandez-leur de vous en fournir un échantillon vérifiable, à l'image de la structure d'un répertoire.
- Le paiement de la rançon ne fera pas disparaître les vulnérabilités exploitées par les cybercriminels, donc assurez-vous d'avoir identifié le point d'accès initial et d'avoir corrigé la faille.

Réalisez une analyse post-incident

- Selon le dicton militaire, « aucun plan de bataille ne survit au contact de l'ennemi ». Aucun plan n'est parfait, et d'autant plus s'il n'a jamais été testé dans le monde réel. Il est donc essentiel de revoir votre plan de réponse aux incidents afin de comprendre ce qui a fonctionné et de noter vos axes d'amélioration. Cette phase de « prise en compte des enseignements » vous aidera à améliorer constamment vos capacités de réponse et de reprise après incident. Il est bon de noter que ce passage en revue doit être effectué aussi vite que possible après la phase de reprise, même si c'est l'événement est encore tout frais dans l'esprit de tous.
- Envisagez de simuler les détails de l'attaque, techniques ou non, à l'aide de tests d'intrusion et d'exercices de mise en situation, afin d'examiner vos options.
- Envisagez de faire appel aux services d'un tiers pour évaluer votre surface d'attaque et identifier tout contrôle de sécurité manquant. Ces consultants externes doivent s'appuyer sur des cadres courants, à l'image de ceux du National Institute of Standards and Technology des États-Unis (Institut national des normes et technologies, ou NIST), afin de pouvoir mesurer leurs progrès.

Tout le monde peut se faire attaquer. Tout le monde a besoin d'un plan. Ne perdez plus la moindre seconde.

- Si vous lisez ce document après avoir été victime d'une attaque par ransomware, suivez attentivement ces conseils, en particulier le premier. La panique conduit à commettre des erreurs et peut faire empirer le problème. Souvenez-vous qu'il existe des professionnels pour vous aider.
- Dans le cas contraire, le moment est venu d'élaborer un plan de réponse aux incidents (RI), ainsi qu'un plan de continuité d'activité (PCA). Ces conseils ne sont qu'un point de départ. De nombreux éléments sont à préparer et à documenter : identifier votre équipe de gestion des incidents critiques ; définir les rôles de chacun ; établir des chaînes de commandement ; désigner un porte-parole ; faire des réserves et isoler les ressources critiques de restauration ; créer un lot de sauvegardes isolé du réseau ; effectuer des tests d'intrusion opposant équipes offensives et défensives, etc.
- De nombreuses organisations peuvent vous aider. Commencez par échanger avec le fournisseur de solutions de sécurité vous inspirant le plus confiance. Beaucoup possèdent des équipes d'experts prêts à vous aider à tester votre réseau, à élaborer un plan de réponse aux incidents, et capables de vous proposer des services d'investigation numérique et de restauration. Quel que soit votre choix, n'attendez plus ; c'est exactement ce que veulent les cybercriminels ciblant votre organisation.



De nombreuses organisations peuvent vous aider. Commencez par échanger avec le fournisseur de solutions de sécurité vous inspirant le plus confiance.

Avertissement : les sites externes cités dans ce document, et les informations qu'ils contiennent ont été considérés comme dignes de confiance par FortiGuard Labs. Cependant, ils n'ont pas été validés de façon indépendante par nos soins, et les extraits tirés ne font pas office de validation de ces renseignements, tous les réseaux et déploiements étant uniques.

FORTINET

www.fortinet.com/fr

juillet 15, 2021 1:45 PM

863720-A-1-FR