proofpoint™

LE RANSOMWARE

GUIDE DE SURVIE

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

RÉSUMÉ ANALYTIQUE

La vieille menace du ransomware fait un retour en force. Ce type de logiciel malveillant, dont le nom découle de la demande de rançon exigée une fois les fichiers de la victime verrouillés, est vite devenu l'un des principaux types de cyber-attaque. Près d'un quart des attaques de la messagerie avec des documents malveillants utilise à présent la souche de ransomware Locky.[1]

Selon le FBI, les auteurs d'attaques par ransomware ont déjà obtenu de leurs victimes plus de 209 millions de dollars au cours du seul premier trimestre 2016, pour un nombre d'attaques 10 fois supérieur à celui de 2015.[2] Outre la rançon elle-même (en supposant que les victimes payent), le coût de ce type d'attaques peut être exorbitant : interruption des activités, frais de restauration et atteinte à l'image de marque.

Bien que les appareils portables et les sites Web infectés soient aussi des vecteurs de distribution, la plupart des ransomware sont propagés par des messages électroniques de phishing.

Pour quelle raison les ransomware sont-ils en pleine croissance ?
Quatre facteurs clés sont à l'origine de l'explosion du nombre de ransomware ces dernières années :

- Pour multiplier leurs chances de succès, les auteurs d'attaque exploitent de nombreux circuits de distribution.
- Créer un ransomware est plus rentable que jamais.
- Les cibles sont plus lucratives, car davantage susceptibles de payer la rançon puisque très motivées.
- Grâce au Bitcoin et autres devises numériques, la collecte d'argent est plus facile.

Survivre aux ransomware
Comme le montre le rapport 2016 du Ponemon Institute sur l'état des terminaux, la plupart des entreprises sont mal préparées pour affronter les ransomware. Selon cette étude, 56 % des entreprises interrogées déclarent ne pas être prêtes à repousser les attaques de ransomware. Seules 38 % d'entre elles déclarent disposer d'une stratégie susceptible de gérer les logiciels destructifs.[3]

Comme base de départ, tenez compte des éléments suivants.

Avant l'attaque
La meilleure stratégie de sécurité consiste à éviter totalement les ransomware. Cela implique une certaine planification et quelques efforts, avant que la crise ne survienne.

Sauvegarder et restaurer
L'élément le plus important de toute stratégie de sécurité contre les ransomware consiste à sauvegarder régulièrement les données. Étonnement, très peu d'entreprises réalisent des exercices de sauvegarde et restauration. Ces deux opérations sont importantes : les exercices de restauration sont le seul moyen de vérifier à l'avance le bon fonctionnement du plan de sauvegarde.

Appliquer les mises à jour et les correctifs
Veillez à ce que les systèmes d'exploitation, les logiciels de sécurité et les correctifs soient systématiquement à jour, sur tous les appareils.

Former et sensibiliser aux macros
Former et sensibiliser les employés est essentiel. Votre personnel doit savoir ce qu'il doit faire et ne pas faire, comment éviter les ransomware et comment les signaler. En cas de réception d'une demande de rançon, vos employés doivent aussitôt le signaler à l'équipe en charge de la sécurité et ne jamais même tenter de payer eux-mêmes la rançon.

Investir dans de solides solutions de sécurité pour la messagerie, les appareils mobiles et les réseaux sociaux
Même les utilisateurs les mieux formés ne pourront pas intercepter tous les ransomware.

1 Proofpoint. « Résumé trimestriel des menaces - Janvier-Mars 2016 » Avril 2016.
2 Chris Francescani (NBC News). « Des pirates informatiques utilisent un ransomware pour faire chanter les services de la police américaine. » Avril 2016. David Fitzpatrick et Drew Griffin (CNN Money). « Selon le FBI, les pertes dues à l'extorsion électronique grimpent en flèche. » Avril 2016.
3 Ponemon Institute LLC. « Rapport 2016 sur l'état des terminaux » Avril 2016.

Les solutions avancées de sécurité de la messagerie assurent une protection contre les pièces jointes, les URL et les documents malveillants présents dans des e-mails et menant aux ransomware. Investissez également dans des produits de protection des portables afin d'empêcher les applications mobiles malveillantes de compromettre votre environnement.

Pendant l'attaque : Reprendre vos activités habituelles
Bien que la meilleure stratégie contre les ransomware soit avant tout de les éviter, ce conseil ne sert à rien si vous venez d'être infecté.

Certains problèmes nécessitent une résolution immédiate, par exemple remettre les ordinateurs, les téléphones et les réseaux en ligne, et gérer la demande de rançon.

Contacter la police
Avertir les autorités compétentes est la première étape. Pour localiser le bureau le plus proche ou les contacter, consultez le site www.fbi.gov/contact-us/legal-attache-offices/europe/paris-france.

Se déconnecter du réseau
Au moment même où il voit la demande de rançon ou remarque quelque chose d'anormal, l'employé doit se déconnecter du réseau et confier la machine infectée au département informatique.

Seule l'équipe de sécurité doit tenter de la redémarrer, une opération qui ne fonctionne d'ailleurs qu'avec les faux scareware (logiciel conçu pour déstabiliser ou effrayer l'utilisateur) ou les logiciels malveillants rudimentaires.

Évaluer l'ampleur du problème grâce aux renseignements sur les menaces
Votre réaction, y compris la décision de payer ou non la rançon, dépend de plusieurs facteurs :

- Du type d'attaque
- De la personne compromise sur le réseau
- Des autorisations réseau associées aux comptes compromis

Orchestrer la réaction
Votre réponse consiste avant tout à décider de payer ou non la rançon. Prendre la bonne décision n'est pas simple, et les conseils des autorités compétentes et de votre avocat seront précieux. Payer la rançon peut être inévitable.

Ne comptez pas sur les outils gratuits de décryptage des ransomware.
La plupart de ces outils gratuits ne fonctionnent qu'avec une seule souche de ransomware, voire une seule campagne d'attaques. À mesure que les auteurs actualisent leur ransomware, les outils gratuits deviennent obsolètes ; ils ne fonctionneront donc probablement pas avec votre ransomware.

Restaurer à partir d'une sauvegarde
Le seul moyen de résister complètement à une infection par ransomware est de restaurer entièrement le système à partir d'une sauvegarde. Même avec des sauvegardes récentes, payer la rançon peut toutefois se révéler préférable sur le plan opérationnel et financier.

Après l'attaque : Inpecter et consolider
Nous vous conseillons d'effectuer une évaluation complète de votre environnement afin de déceler les menaces éventuellement encore présentes. Examinez attentivement vos outils et procédures de sécurité, et surtout leurs lacunes.

Nettoyer
Certains ransomware contiennent d'autres menaces ou chevaux de Troie dérobés, susceptibles de fomenter d'autres attaques dans le futur.

Examinez attentivement les menaces masquées qui ont pu vous échapper en pleine pagaille.

Faire une analyse rétrospective
Évaluez votre état de préparation et vos réactions aux menaces. Si vous ignorez comment est arrivé le ransomware, vous n'avez aucun moyen d'intercepter la prochaine attaque.

Évaluer le niveau de sensibilisation des utilisateurs
L'employé bien avisé est votre dernière ligne de défense. Veillez à ce que vos employés, votre personnel ou vos enseignants soient à la hauteur.

Sensibiliser et former
Élaborez un programme d'éducation pour combler les lacunes de vos employés en matière de cyber-attaques. Élaborez un Plan de communication de crise capable de répondre aux prochaines attaques, et mettez-le en pratique à travers des exercices et des tests d'intrusion.

Renforcer vos défenses
L'évolution rapide des menaces implique de disposer de solutions de sécurité capables d'analyser, d'identifier et de bloquer, en temps réel, les URL et les pièces jointes malveillantes qui constituent le principal vecteur d'attaque des ransomware.

Optez pour des solutions de sécurité capables de s'adapter aux menaces nouvelles et émergentes, et de vous permettre de réagir plus rapidement.

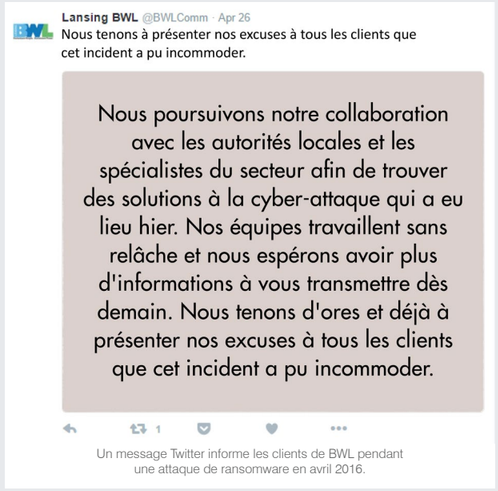
INTRODUCTION

INTRODUCTION

Toute la lumière n'a pas encore été faite sur ce qui s'est passé le 25 avril 2016, lorsqu'un employé du Lansing Board of Water & Light (BWL), dans le Michigan, a ouvert une pièce jointe à un e-mail, apparemment inoffensive. Déclenchée par ce simple clic, l'infection s'est rapidement propagée à travers tout le réseau de l'entreprise BWL. Le ransomware verrouillait des fichiers sensibles et demandait le versement d'une rançon pour les restaurer.

Le troisième plus grand fournisseur d'électricité de l'État a été victime de ce ransomware. Les dirigeants ont rapidement fermé le réseau de l'entreprise pour limiter sa propagation.

« En 40 ans de siège au Conseil, je n'avais jamais vu un événement d'une telle ampleur », déclare Dick Peffley, Directeur général chez BWL. « Nos plannings, nos téléphones, nos ordinateurs, nos imprimantes, tout ce qui chez BTW nous permet de mener à bien nos tâches administratives est désormais inaccessible. »[4]



Un message Twitter informe les clients de BWL pendant une attaque de ransomware en avril 2016.

Une semaine s'est écoulée avant que les choses ne se calment et que les services informatiques ne soient restaurés dans l'entreprise.[5]

Malheureusement, ce cas n'est pas isolé. Au cours de ces derniers mois, le ransomware est vite devenu l'un des principaux types de cyber-attaque. Près d'un quart des attaques de la messagerie avec des documents malveillants utilise à présent la souche de ransomware Locky.[6]

Comme le montre le rapport 2016 du Ponemon Institute sur l'état des terminaux, la plupart des entreprises sont mal préparées pour affronter les ransomware. Selon cette étude, 56 % des entreprises interrogées déclarent ne pas être prêtes à repousser les attaques de ransomware. Seules 38 % d'entre elles déclarent disposer d'une stratégie susceptible de gérer les logiciels destructifs.[7]

Comme base de départ, tenez compte des éléments suivants. Nous y révélons les facteurs à l'origine de l'essor stratosphérique du ransomware, ce que vous devez faire si vous y êtes confronté et, plus important encore, comment éviter d'en devenir victime en premier lieu.

« DEPUIS 40 ANS QUE JE SIÈGE AU CONSEIL, JE N'AVAIS JAMAIS VU UN ÉVÉNEMENT D'UNE TELLE AMPLEUR. »

Dick Peffley, Directeur général chez BWL

4 Alexandra Ilitch (WLNS). « Le réseau de BWL contaminé par un virus de phishing de type 'ransomware'. » Avril 2016.
5 Max Metzger (SC Magazine UK). « Une compagnie d'électricité du Michigan visée par une attaque de ransomware. » Mai 2016.
6 Proofpoint. « Résumé trimestriel des menaces - Janvier-Mars 2016 » Avril 2016.
7 Ponemon Institute LLC. « Rapport 2016 sur l'état des terminaux » Avril 2016.

RÉSURGENCE D'UNE VIEILLE MENACE

Ces derniers temps, la vieille menace du ransomware fait un retour en force sous de nouvelles variantes. Ce ransomware bloque l'accès au système ou aux données, généralement en cryptant les fichiers dotés de certaines extensions (JPG, DOC, PPT, etc.). Les fichiers restent inaccessibles tant que la victime ne paye pas l'auteur de l'attaque pour obtenir le code de décryptage qui permettra de les déverrouiller. Dans la plupart des cas, la demande de rançon est assujettie à une date d'échéance. Si cette dernière n'est pas respectée, la rançon peut doubler ou les données sont définitivement perdues, voire détruites.

Le coût réel
Selon le FBI, les auteurs d'attaques par ransomware ont déjà obtenus de leurs victimes plus de 209 millions de dollars au cours du seul premier trimestre 2016, pour un nombre d'attaques 10 fois supérieur à celui de 2015.[8]

Outre la rançon elle-même (en supposant que les victimes payent), le coût de ce type d'attaques peut être exorbitant : interruption des activités, frais de restauration et atteinte à l'image de marque.

Prenons l'exemple de l'attaque de BWL. S'il ne semble pas avoir véritablement visé les systèmes de contrôle industriels, le ransomware s'est montré extrêmement perturbant. Le fait de ne pas pouvoir accéder aux informations sensibles et aux systèmes professionnels peut ralentir les interventions d'urgence et mettre en péril la sécurité publique.

Le secteur de la santé a été particulièrement touché. Une telle attaque empêche d'accéder aux dossiers des patients, ralentit les procédures et peut même avoir une incidence sur les systèmes de surveillance des malades. Résoudre le problème du ransomware devient alors une question de survie.

Exploiter le facteur humain
Comme pour l'attaque de BWL, la plupart des ransomware se propagent par le biais de messages électroniques de phishing. Ces e-mails incitent l'utilisateur à ouvrir une pièce jointe malveillante ou à cliquer sur une URL malveillante.

En février 2016, le ransomware Locky a infecté l'Hôpital méthodiste du Kentucky à travers une campagne d'e-mails ciblée.

Dès qu'un employé a ouvert ce qu'il a pris pour une facture impayée, Locky s'est exécuté et s'est propagé dans tout le réseau interne. Il a alors verrouillé les stations de travail et interdit tout accès au serveur central. L'hôpital a alors eu le choix entre restaurer chacun des postes de travail à partir d'une sauvegarde ou verser la somme relativement modeste de quatre bitcoins (1 600 dollars environ) pour déverrouiller ses fichiers.

Nos chercheurs avaient identifié la souche Locky près d'un mois auparavant. La propagation du ransomware Locky passe essentiellement par des pièces jointes Microsoft Word, souvent déguisées en factures impayées. Lorsqu'ils ouvrent ce document, les utilisateurs sont invités à activer les macros. S'ils le font, un fichier exécutable nommé Troj/Ransom-CGXis est téléchargé depuis un serveur distant. Ce fichier crypte alors les fichiers sensibles et finit par lancer Locky.[9]

Une fois les fichiers cryptés, un message s'affiche et exige le paiement d'une rançon, en donnant généralement les instructions à suivre concernant le réseau Tor et les bitcoins. Les victimes ne peuvent ni fermer ni contourner ce message. Aucune combinaison de touches du type CTRL+ALT+SUPPR ni redémarrage ne permet de résoudre le problème.

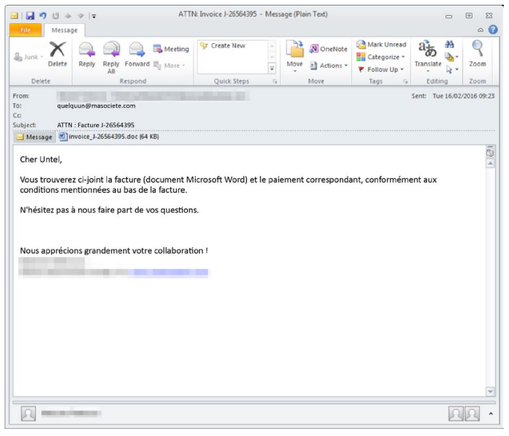
LA PROVENANCE

La propagation des ransomware passe par trois principaux vecteurs d'attaque :

- Messages électroniques
- Appareils mobiles
- Sites Web/liens infectés via les réseaux sociaux et les publicités contenant des logiciels malveillants (publicités malveillantes)

Les e-mails incluant des pièces jointes et des liens sont de loin le plus gros vecteur de menaces, et représentent environ 85 % de tous les ransomware détectés.

Ces e-mails semblent légitimes et peuvent leurrer les employés peu méfiants. Ils se font souvent passer pour des mises à jour logicielles officielles, pour des factures impayées, voire pour une note du patron adressée à un subordonné.



La plupart des ransomware se propagent par le biais d'un e-mail de phishing tel que celui-ci.

8 Chris Francescani (NBC News). « Des pirates informatiques utilisent un ransomware pour faire chanter les services de la police américaine. » Avril 2016. David Fitzpatrick et Drew Griffin (CNN Money). « Selon le FBI, les pertes dues à l'extorsion électronique grimpent en flèche. » Avril 2016.
9 « Les pirates à l'origine de la propagation de Dridex se lancent dans le ransomware avec 'Locky'. » Février 2016.

POURQUOI CETTE INTENSIFICATION ?

Les ransomware existent depuis des décennies. Quatre facteurs clés ont toutefois permis leur montée en flèche ces dernières années :

Multiplication des canaux de distribution
Les cybercriminels peuvent cibler des milliers d'entités simultanément à travers un large éventail de vecteurs d'attaque. Cela signifie que les ransomware atteignent plus souvent leur but.

Les passerelles de messagerie conventionnelle sont dépassées alors que les menaces arrivent de tous côtés :

- Campagnes massives d'e-mails, menées par botnet
- Logiciels malveillants polymorphiques trop rapides par rapport à la capacité des fournisseurs de solution de sécurité à collecter les nouvelles signatures
- URL et publicités malveillantes sans pièces jointes

Réunis, ces différents facteurs assurent de meilleures chances de succès aux ransomware.

Moins coûteux à élaborer
Comme dans toute entreprise, le succès engendre le succès. Les auteurs de ransomware ont peaufiné leurs armes. Les outils perfectionnés, que seuls les meilleurs cybercriminels auraient pu mettre au point il n'y a encore que quelques années, sont à présent communément disponibles. Le taux de succès augmente donc et, les économies d'échelle également.

Si 4 000 attaques ont lieu en une seule journée, même si 1 % seulement des destinataires verse une rançon de 400 dollars, le revenu atteint déjà 16 000 dollars par jour. En une année, les bénéfices peuvent se compter en millions.

Des cibles plus rentables
Au lieu de cibler les particuliers, les cybercriminels se tournent de plus en plus vers les organisations détentrices de données sensibles, dotées de département informatique aux ressources déjà insuffisantes et débordées, car elles seront plus fortement incitées à négocier au plus vite. Pour ajouter de l'huile sur le feu, dans les hôpitaux, les services de police, les écoles et autres administrations nationales ou locales, les réseaux sont généralement configurés de manière médiocre.

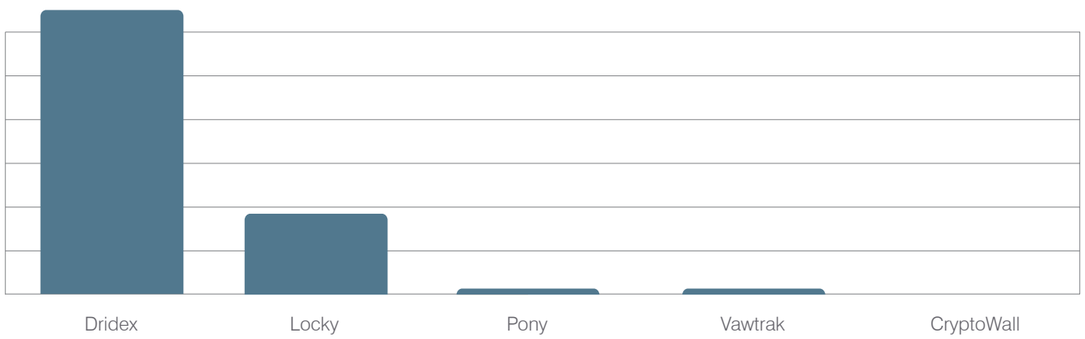
Pour de telles organisations, un réseau à l'arrêt n'est guère envisageable. Rien d'étonnant donc dans le fait qu'après un rapide calcul, verser la rançon est la meilleure décision à prendre pour nombre d'entre elles.

Bitcoin et autres devises numériques
Depuis ses débuts en 2009, le Bitcoin est une aubaine pour les défenseurs des libertés fondamentales comme pour les cybercriminels. Comme il est impossible de suivre le paiement pour remonter à l'expéditeur ou au destinataire, la transaction reste privée et anonyme.

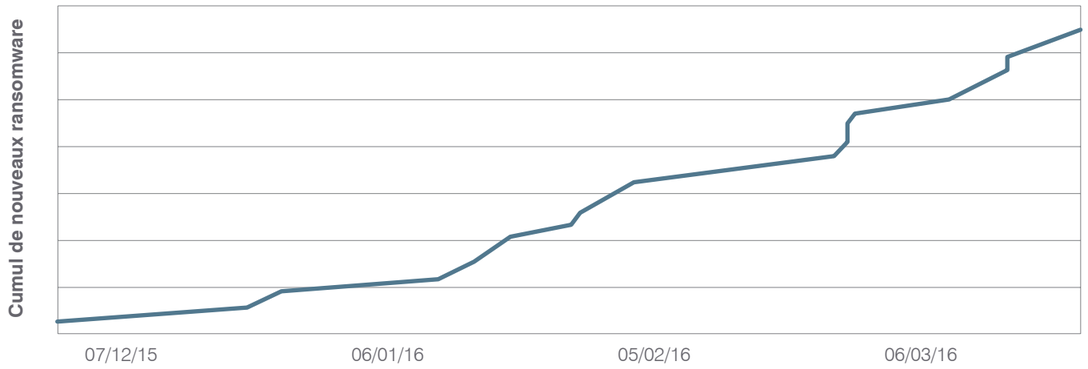
En demandant à être payé en Bitcoins, les cybercriminels bénéficient d'un anonymat qui leur permet de collecter les rançons plus facilement que jamais. Les anciennes formes de ransomware peuvent avoir besoin d'une pré-autorisation de carte bancaire. Bien que cette approche puisse contourner les mesures antifraude mises en place par les banques, elle reste bien plus laborieuse des deux côtés de la transaction.

Toutes les variantes majeures de ransomware exigent désormais un paiement en bitcoins. (Voir encadré page 9)

Principales charges utiles malveillantes par nombre de messages
Campagnes par pièces jointes, Janvier-Mars 2016
Source : Proofpoint, Inc.



Essor des variantes de ransomware depuis décembre 2015
Source : Proofpoint, Inc.



LA PISTE DU BITCOIN

Lors des enlèvements traditionnels de personne contre rançon, la plus grosse difficulté pour les criminels a toujours été de récupérer la rançon avant de disparaître. Malheureusement, cette opération est bien plus facile pour les cybercriminels et leurs ransomware.

La forme de paiement la plus commune passe par des monnaies cryptographiques intraçables, dont la plus connue est le Bitcoin. Le bitcoin autorise les opérations de paiement entre deux personnes via Internet, et n'implique aucune banque ou administration. Il y a 21 millions de bitcoins à travers le monde. Depuis ses débuts en 2008, la valeur de cette devise a connu de fortes fluctuations. À la date de cette publication, un bitcoin vaut environ 600 dollars USD.

Pour bien comprendre ce que sont les monnaies cryptographiques (ou chiffrées), il suffit de les considérer comme l'équivalent électronique d'un jeton de casino. Ces jetons n'ont aucune valeur propre dans le monde réel, mais les utilisateurs peuvent en acheter dans leur monnaie locale, les dépenser au sein de l'établissement (dans ce cas, Internet), puis les échanger contre des devises avant de partir.

De la même façon, il est possible d'utiliser une carte de débit ou un compte bancaire pour acheter des devises cryptographiques en ligne auprès de sources légitimes. Dans le cas des ransomware, les victimes convertissent leur monnaie locale en « trois bitcoins », par exemple, puis les transfèrent d'un portefeuille de bitcoins vers l'adresse Bitcoin anonyme fournie par l'auteur de l'attaque.

L'argent ne va pas toujours directement dans les mains de celui-ci. En général, les jetons passent par une « timbale », c'est-à-dire un service électronique qui mélange les bitcoins avec d'autres, puis les verse à l'auteur de l'attaque (numérotés différemment, mais de même valeur moins la commission).

Comme pour le blanchiment d'argent dans le monde réel, les auteurs d'attaque peuvent ainsi rendre ces paiements intraçables. Ce paiement est ensuite reconverti en devise physique locale en échangeant les bitcoins (jetons) contre des espèces.

Notez que, contrairement aux devises garanties par les gouvernements, les monnaies cryptographiques ne sont pas largement reconnues, mais davantage considérées comme l'équivalent des jetons de poker ou de casino. De ce fait, le système de transmission et les timbales ne sont ni régulés ni considérés comme du blanchiment d'argent, alors que l'effet est sans doute le même.

L'attrait que suscite le bitcoin est évident. Il fournit aux pirates une cyber-devise disponible dans le monde entier et difficile à tracer qu'ils peuvent directement convertir en devise locale, donc en d'autres termes, en « billets non marqués ».

Les avantages d'une telle approche sont évidents par rapport au vol de cartes bancaires, dont la rentabilité s'effondre de jour en jour à mesure que les institutions financières gagnent en maîtrise et ferment rapidement les comptes des victimes.

RANSOMWARE POUR PORTABLES

Imaginez que vous saisissiez votre téléphone et qu'en lieu et place de votre écran d'accueil s'affiche un avertissement semblant provenir de la police, vous accusant de visionner des images illicites. Votre téléphone a été chiffré et quelqu'un vous menace d'avertir les autorités à moins que vous ne versiez 300 dollars pour tout faire disparaître.

Pour une multitude d'utilisateurs de portable, cette situation n'est que trop réelle, et ce n'est là qu'un exemple parmi les centaines de versions de ransomware qui ciblent les appareils mobiles. Près de 98 % d'entre elles ciblent le système d'exploitation Android.

Dans le cas des ransomware ciblant les mobiles, nous avons pu détecter trois principaux vecteurs d'attaque.

Android
Le ransomware destiné au système Android découle de la même grande famille que la variante Cryptolocker. Il peut prendre la forme d'une mise à jour d'Adobe Flash Player demandant des autorisations. Il peut également « s'ajouter » à un jeu très répandu ou à une appli « gratuite » téléchargée depuis un AppStore suspect. (Dans leur grande majorité, les ransomware Android proviennent de magasins d'applis tiers, pas du site Google Play officiel.)

Une fois lancé, le ransomware crypte l'appareil portable et exige une rançon,généralement en bitcoins.

Applications distribuées par SMS
Généralement pornographiques, ces applis prennent le contrôle del'écran de l'appareil (en y affichant des images délictueuses) et exigent le paiement d'une rançon pour disparaître. Elles se propagent habituellement par SMS, mais sont aussi présentes sur les réseaux sociaux et très souvent dans les messages Twitter ou Instagram directs.

Contrairement à la plupart des ransomware, les données ne sont généralement pas cryptées. Pour les utilisateurs toutefois, le résultat est le même : leur appareil est verrouillé. Passer outre ce type de menace est possible, mais aussi très compliqué. Nombre d'utilisateurs préfèrent simplement payer la rançon.

Navigateurs iOS
Les attaques qui ciblent les appareils iOS prennent généralement la forme de ransomware de type navigateur. En général, ils signalent à la victime qu'ils ont téléchargé des images illégales ou prétendent que leur appareil est infecté. Pour déverrouiller ou « réparer » l'appareil, la victime est dirigée vers un certain site, où elle peut payer en bitcoins ou par carte de débit prépayée.

Ces ransomware frauduleux se propagent principalement via les publicités malveillantes des sites Web réservés aux adultes. Le taux de conversion de ces sites en victimes rentables reste faible. Pour autant, lorsque des centaines de milliers de victimes, voire des millions, sont infectées chaque semaine, l'opération est payante.

À la date de cette publication, nous n'avons pas encore décelé de cryptage général sur des appareils iOS. La majorité de ces dispositifs se contente d'empêcher les victimes d'accéder à leurs navigateurs Web.

INCIDENTS OU MISES EN DANGER LES PLUS GRAVES

Source : Ponemon

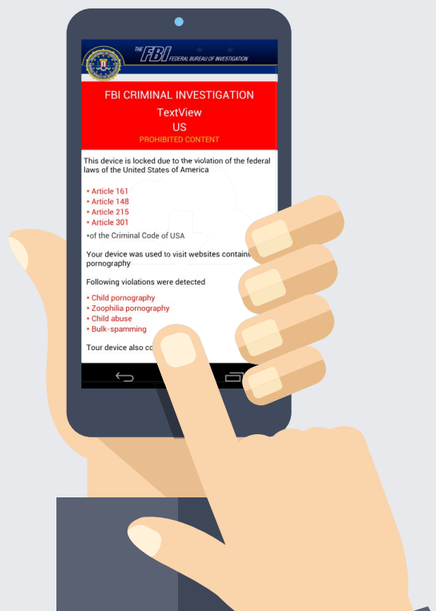
71 %
Attaques Zero Day

68 %
Attaques DDoS

53 %
Exploitation de vulnérabilités logicielles existantes
(de plus de trois mois)

51 %
Ransomware

47 %
Attaques malveillantes via Internet



PRÉVENIR LES RANSOMWARE

La meilleure stratégie de sécurité consiste en tout premier lieu à éviter ce type d'extorsion. C'est tout à fait dans les cordes de la plupart des entreprises, mais cela implique une certaine planification et quelques efforts, avant que la crise ne survienne.

Sauvegarder et restaurer
L'élément le plus important de toute stratégie de sécurité contre les ransomware consiste à sauvegarder régulièrement les données. La plupart des entreprises le font, mais étonnement, très peu d'entre elles réalisent des exercices de sauvegarde et restauration. Ces deux opérations sont importantes : les exercices de restauration sont le seul moyen de vérifier à l'avance le bon fonctionnement du plan de sauvegarde.

Il vous faudra peut-être résoudre quelques problèmes avant que la crise ne survienne. Dans la mesure où la sauvegarde et la restauration sont testées régulièrement, l'incidence des ransomware ne sera pas catastrophique. Vous disposez d'un point de restauration, récent et sûr.

Répétons-le : la plupart des entreprises et des particuliers effectuent des sauvegardes. Mais tester régulièrement la restauration complète est tout aussi essentiel.

Mises à jour et correctifs
Veillez à ce que les systèmes d'exploitation, les logiciels de sécurité et les correctifs soient systématiquement à jour, sur tous les appareils. Cela peut sembler évident, mais selon une étude récente, près de la moitié des professionnels de l'informatique admettent avoir du mal à gérer la multitude de correctifs publiés chaque mois. Les personnes interrogées déclarent qu'en termes de complexité et de calendrier de diffusion, les mises à jour varient grandement.

Les équipes ont également du mal à mettre à jour certaines applications, par exemple Adobe Flash, alors que d'autres services internes en ont besoin pour fonctionner. Les pirates informatiques savent très bien que cela peut induire une certaine « lassitude vis-à-vis des correctifs », et développent leurs exploits en conséquence.[9]

Former et sensibiliser aux macros
La plupart des attaques de ransomware commencent lorsqu'un seul employé bien intentionné ouvre ce qui lui semble être un e-mail lié à ses activités professionnelles.

C'est pour cela qu'il est crucial de former et de sensibiliser les employés. Votre personnel doit savoir ce qu'il doit faire et ne pas faire, comment éviter les ransomware et comment les signaler. En cas de réception d'une demande de rançon, vos employés doivent aussitôt le signaler à l'équipe en charge de la sécurité et ne jamais même tenter de payer eux-mêmes la rançon. (Un tel paiement peu avoir de graves conséquences sur la réputation de la marque et la sécurité.)

Nos études montrent que les cybercriminels profitent activement de nos erreurs et de notre curiosité.
Le déferlement récent d'e-mails de ransomware illustre une tendance généralisée de la cybercriminalité : tromper les utilisateurs en les rendant à leur insu complices du verrouillage des informations et de la demande de rançon.[10]

Ces attaques jouent sur la naïveté de l'utilisateur, et l'invite généralement à ouvrir un document Word ou des pièces jointes JavaScript malveillantes, puis à activer des macros. Lorsque l'utilisateur clique sur le bouton « Activer le contenu », la macro malveillante télécharge le ransomware et lance la procédure d'attaque. La première solution consiste à désactiver les scripts de macro dans les fichiers Office transmis par e-mail. Certaines macros sont toutefois utiles, et les désactiver toutes peut altérer la productivité.

Investir dans de solides solutions de sécurité pour la messagerie, les appareils mobiles et les réseaux sociaux
Même la meilleure des formations des utilisateurs ne suffira pas pour éviter tous les ransomware. Les messages de phishing actuels sont à la fois sophistiqués et très ciblés. Les auteurs d'attaques étudient soigneusement leurs cibles, élaborent des messages d'apparence légitime, puis comptent sur la nature humaine pour que l'utilisateur clique sur le déclencheur.

Comme la plupart des ransomware se propagent via les messages électroniques, les appareils mobiles et les réseaux sociaux, il vous faut des solutions avancées, capables d'intercepter de telles menaces en temps réel. Selon nos recherches, le volume global d'e-mails malveillants a fortement augmenté au premier trimestre 2016 : plus de 66 % par rapport au 4e trimestre 2015 et plus de 800 % sur la même période en 2015.[11]

Les passerelles de messagerie héritées, les filtres Web et les logiciels antivirus classiques doivent être mis à jour et s'exécuter sur tous les réseaux. À eux seuls toutefois, ces dispositifs ne suffiront pas à enrayer la menace des ransomware. Pour être efficace, la solution de protection de la messagerie doit aller plus loin. Cela signifie analyser les URL et les pièces jointes afin de s'assurer qu'aucun contenu malveillant ne pénètre dans le système. Les cybercriminels ont toujours une longueur d'avance et les configurations de sécurité de la messagerie reposent beaucoup trop sur des signatures obsolètes.

Les solutions de sécurité avancées assurent une protection contre les pièces jointes, les URL et les documents malveillants, inclus dans les e-mails, qui conduisent à des ransomware. Investissez en parallèle dans des produits de protection contre les attaques des mobiles afin d'empêcher les applications mobiles malveillantes de compromettre votre environnement.

9 Tripwire, Inc. « Étude sur la gestion des correctifs - Tripwire 2016 » Mars 2016.
10 Proofpoint. « Le facteur humain en 2016 » Février 2016.
11 Proofpoint. « Le facteur humain en 2016 » Février 2016.

INCIDENCE RÉELLE DES RANSOMWARE : CENTRE MÉDICAL PRESBYTÉRIEN D'HOLLYWOOD

L'incident de ransomware le plus connu et le plus médiatisé est probablement celui qu'a connu le Centre médical presbytérien d'Hollywood. Le 5 février 2016, les employés de l'hôpital découvraient qu'ils ne pouvaient ni accéder à leurs ordinateurs ni au réseau.

Des pirates informatiques en avaient pris le contrôle via le ransomware Locky par le biais d'un e-mail infecté. Comme la grande majorité des infections dues au ransomware Locky, l'e-mail se faisait passer pour une facture impayée. Le destinataire a malheureusement cliqué sur « Activer les macros » lorsqu'il y a été invité, ce qui a entraîné le téléchargement et l'exécution du logiciel malveillant. Tous ceux qui tentaient d'accéder au réseau se voyaient informés de la demande de rançon et étaient dirigés vers un site de paiement.

Les pirates exigeaient 40 bitcoins, soit près de 17 000 dollars à l'époque. Les ordinateurs sont restés hors ligne pendant plus d'une semaine pendant que les dirigeants de l'hôpital s'efforçaient de trouver une solution. Les services d'urgence ont été contactés pour certains patients ; d'autres ont été dispatchés vers les hôpitaux de la région. La direction a fini par conclure que la seule solution était de payer la rançon, et l'a donc fait. L'hôpital a alors reçu l'outil de décryptage de Locky et remis le réseau en service.

Centre médical presbytérien d'Hollywood, Los Angeles, Californie.

PENDANT L'ATTAQUE

RETOUR À L'ESSENTIEL

Vous êtes victime d'une attaque de ransomware. Que faire à présent ?

Bien que la meilleure stratégie contre les ransomware consiste avant tout à les éviter, ce conseil ne sert à rien si vous venez d'être infecté. Certains problèmes nécessitent une résolution immédiate, par exemple remettre les ordinateurs, les téléphones et les réseaux en ligne, et gérer la demande de rançon.

Toutefois, paniquer ne sert à rien et peut même faire empirer la situation.

Contacter les autorités compétentes
Le ransomware est un crime, qui implique vol et extorsion. Personne n'est en droit de s'emparer d'appareils, de réseaux ou de données, encore moins d'exiger une rançon en échange. Avertir les autorités compétentes est donc la première étape indispensable.

Rendez-vous dans le commissariat de police le plus proche. N'hésitez pas à les contacter par téléphone. Ils sont là pour vous aider.

Se déconnecter du réseau
Au moment même où il voit la demande de rançon ou remarque quelque chose d'anormal, par exemple lorsqu'il n'a soudainement plus accès à ses propres fichiers, l'employé doit se déconnecter du réseau et confier sa machine infectée au département informatique.

Pour les employés, redémarrer leur système est déconseillé. Seule l'équipe en charge de la sécurité doit tenter de redémarrer la machine, une opération qui ne fonctionne d'ailleurs qu'avec les faux scareware (logiciel conçu pour déstabiliser ou effrayer l'utilisateur) ou les logiciels malveillants rudimentaires.

Dans un tel cas, le ransomware en question est davantage un « scareware », c'est-à-dire destiné à faire peur. Il peut éventuellement afficher une demande de rançon et des instructions de paiement à l'écran, mais les données ne sont pas véritablement cryptées. Dans un tel scénario, il suffit d'appuyer sur les touches CTRL+ALT+SUPPR, pour ouvrir le Gestionnaire des tâches de Windows, et de fermer le navigateur pour résoudre le problème.

Évaluer l'ampleur du problème grâce aux renseignements sur les menaces
Bien que tous les ransomware soient malveillants, certaines attaques sont pires que d'autres. Votre réaction, y compris le fait de payer ou non la rançon, dépend de plusieurs facteurs.

Posez-vous les questions suivantes :

- De quel type d'attaque s'agit-il ? Les ransomware laissent des cartes de visite, et les mesures à prendre peuvent dépendre de la personne à l'origine de l'attaque et des outils employés.
- Qui est compromis sur le réseau ?
- Quelles sont les autorisations réseau associées aux comptes compromis ?

Vos réponses doivent permettre aux administrateurs réseau d'évaluer l'ampleur du problème, d'établir un plan d'action et éventuellement d'arrêter la propagation.

Orchestrer la réaction
Selon la configuration du réseau, il peut être possible de limiter la propagation à une seule station de travail.

Le scénario idéal est le remplacement de la machine infectée par un nouvel ordinateur, sur lequel est restaurée une sauvegarde complète. Le pire scénario est une propagation à tous les ordinateurs du réseau. Dans ce cas, un rapide calcul du rapport coût/bénéfice est nécessaire afin d'évaluer les heures de travail nécessaires pour résoudre le problème par rapport au montant de la rançon.

Votre réponse consiste avant tout à décider de payer ou non la rançon. Prendre la bonne décision n'est pas simple, et les conseils des autorités compétentes et de votre avocat seront précieux. Pour bon nombre de victimes, payer la rançon peut être inévitable (voir page 16).

Ne comptez pas sur les outils gratuits de décryptage des ransomware.
Certains fournisseurs de sécurité offrent des logiciels gratuits pour le décryptage des ransomware. Ils vous permettront parfois de récupérer vos données sans payer la rançon.

Toutefois, la plupart ne fonctionnent qu'avec une seule souche de ransomware, voire une seule campagne d'attaques. À mesure que les auteurs d'attaque actualisent leur ransomware, les outils gratuits deviennent obsolètes ; ils ne fonctionneront donc probablement pas avec votre ransomware.

Vous pouvez avoir de la chance et vous en sortir avec un outil de décryptage gratuit, mais n'en faites pas un élément de votre stratégie de défense.

Restaurer à partir d'une sauvegarde
Le seul moyen de résister complètement à une infection par ransomware est de restaurer entièrement le système à partir d'une sauvegarde, opération qui devrait avoir lieu chaque jour. L'opération peut sembler intervenir en dernier recours en cas d'infection, mais est prioritaire en termes de prévention.

Même avec des sauvegardes récentes, payer la rançon peut toutefois se révéler préférable sur le plan opérationnel et financier. Restaurer des sauvegardes se révèle fastidieux, et certaines entreprises n'ont pas forcément les moyens d'interrompre leurs activités.

PAYER OU NE PAS PAYER : LES RANSOMWARE POSENT UN DILEMME MORAL

Les ransomware sont déjà suffisamment perturbants en eux-mêmes. L'un de leurs aspects particulièrement détestables est qu'ils obligent la victime à faire un choix cornélien, qui pose un dilemme moral. Une fois sous la menace du ransomware, vous n'avez pas toujours le loisir de pouvoir évaluer avec soin les subtilités morales associées au paiement de la rançon. L'attaque est en cours, maintenant.

Jusqu'à présent, les exploits malveillants entraînaient des mesures simples et évidentes : détection de la fraude, déclaration et résolution. Les ransomware introduisent maintenant des questions morales dans l'équation.

Payer n'est pas simplement odieux mais un mal nécessaire. Cet argent finance l'auteur de l'attaque qui vient de pénétrer dans votre réseau et de voler vos données. Le fait de payer met en avant la vulnérabilité de votre réseau et votre intérêt à payer. Cela permet au cybercriminel de financer ces futures attaques.

Pour autant, l'exemple récent de l'attaque subie par le Centre médical presbytérien d'Hollywood (page 13) met en évidence un élément troublant : payer ou ne pas payer n'est pas toujours une question facile à trancher.

Aucune organisation ne souhaite se voir extorquée, encore moins financer des réseaux criminels. Mais une fois encore, l'hôpital avait-il réellement le choix ? D'une certaine manière, il s'agit-là du prix à payer pour des départements informatiques au budget insuffisant qui exécutent des logiciels sans correctifs ou obsolètes. Certains hôpitaux américains utilisent encore Windows XP. Et 17 000 dollars est un prix relativement peu élevé lorsque des vies sont en jeu.

Selon Joseph Bonavolonta, agent spécial en charge du programme de contre-espionnage et de la cybercriminalité au bureau du FBI à Boston, le FBI lui-même a conseillé à certaines victimes « de simplement payer la rançon ».[12] Officiellement, l'agence déconseille néanmoins tout paiement, et souligne que le fait de payer ne permet pas toujours de récupérer les données.[13]

Lorsqu'il s'agit de choisir la meilleure ligne d'action possible, les organisations doivent mettre en balance les intérêts contradictoires en jeu. Ces derniers peuvent inclure :

- Les heures de travail nécessaires pour restaurer le réseau
- L'obligation pour les actionnaires de maintenir l'activité
- La sécurité des clients et des employés
- L'activité criminelle éventuellement financée par le paiement de la rançon

Comme pour la plupart des questions complexes, la réponse sera différente pour chaque organisation.

PAYER N'EST PAS SIMPLEMENT ODIEUX, C'EST UN MAL NÉCESSAIRE. CET ARGENT FINANCE L'AUTEUR DE L'ATTAQUE QUI VIENT DE PÉNÉTRER DANS VOTRE RÉSEAU ET DE VOLER VOS DONNÉES.

12 Tess Danielson (Business Insider). « Le FBI déclare que l'on peut être amené à payer la rançon lorsque des pirates infectent votre ordinateur avec un ransomware. » Octobre 2015.
13 FBI. « Ransomware » Avril 2016.

APRÈS L'ATTAQUE

VÉRIFIER ET RENFORCER

Quels que soient les dommages causés par le ransomware, l'attaque révèle une faille de sécurité qui compromet un appareil ou un réseau. Maintenant que tout est rétabli normalement, vous avez l'opportunité de tirer des enseignements de cette violation de la sécurité pour éviter de futures attaques.

Nous vous conseillons d'évaluer entièrement votre environnement afin d'y déceler les menaces éventuellement encore latentes. Il est également temps d'inspecter de près vos outils et procédures de sécurité, ainsi que leurs lacunes.

Nettoyer
Certains ransomware contiennent d'autres menaces ou chevaux de Troie dérobés, susceptibles de fomenter d'autres attaques dans le futur. C'est pour cela qu'il est crucial de nettoyer entièrement chaque appareil et d'effectuer une restauration à partir d'une sauvegarde saine. Examinez attentivement les menaces masquées qui ont pu vous échapper en pleine pagaille.

Analyse rétrospective
Évaluez votre état de préparation et vos réactions aux menaces. Comment s'est déroulé le plan de crise ? Est-il possible d'améliorer les configurations du réseau pour éviter de futures attaques ? Est-il possible d'implémenter une solution de protection de la messagerie plus robuste ?

Évaluez les mesures de sécurité en vigueur et demandez-vous si elles sont suffisantes face aux menaces modernes. Tirez des enseignements de cette expérience, car elle pourrait bien se renouveler. Si vous ignorez comment est arrivé le ransomware, vous n'avez aucun moyen d'intercepter la prochaine attaque.

Évaluer le niveau de sensibilisation des utilisateurs
Pour déployer les charges utiles, la plupart des souches de ransomware comptent sur une interaction humaine. En cas de défaillance des mesures de sécurité en vigueur, lorsqu'une « facture impayée » infectée parvient jusqu'au serveur de messagerie, l'employé bien avisé devient la dernière ligne de défense entre l'entreprise, l'hôpital ou l'école qui veut rester en ligne, ou vient gonfler les statistiques des ransomware. Veillez à ce que vos employés, votre personnel ou vos enseignants soient à la hauteur.

Il peut également être intéressant de faire appel à des sociétés de test des intrusions, dont la mission est de sensibiliser les employés et de renforcer la sécurité de l'entreprise. En reproduisant des attaques réalistes via phishing, ingénierie sociale et exploits sur les réseaux sociaux, les « tests d'intrusion » permettent d'analyser et d'identifier les lacunes de sécurité avant que de vraies attaques ne se produisent.

Sensibiliser et former
Après avoir évalué le niveau de sensibilisation des utilisateurs, élaborez un programme chargé de combler leurs lacunes en matière de cyber-attaque, en tenant compte des enseignements tirés de vos précédents « incidents ». Élaborez un plan de communication de crise capable de répondre aux prochaines attaques, et comme nous l'avons vu précédemment, mettez-le en pratique à travers des exercices et des tests d'intrusion.

Investir dans des mécanismes de protection modernes
Les pirates informatiques et autres cybercriminels ont toujours eu une longueur d'avance sur les mesures de sécurité et les forces de l'ordre.

Bien que la plupart des réseaux parviennent à bloquer les menaces connues, l'évolution rapide des attaques implique de disposer de solutions de sécurité capables d'analyser, d'identifier et de bloquer en temps réel les URL et les pièces jointes malveillantes, qui constituent le principal vecteur d'attaque des ransomware.

Optez pour des solutions de sécurité capables de s'adapter aux menaces nouvelles et émergentes et de vous permettre de réagir plus rapidement.

CONCLUSION

Les ransomware reviennent en force et se révèlent lucratifs. Ces quelques directives vous aideront à mieux gérer les ransomware avant, pendant et après une véritable attaque.

À l'évidence, le moyen le plus simple de combattre les ransomware est de les arrêter aux portes du réseau. Cela implique de disposer d'une solution avancée capable de détecter les ransomware que propagent les e-mails, les appareils portables et les réseaux sociaux.

Une solide sécurité informatique identifie et supprime les ransomware avant même qu'ils n'aient mis un pied dans votre environnement. Cela inclut la possibilité d'analyser en temps réel les pièces jointes au courrier électronique et les liens, de démanteler les menaces dans un environnement virtuel et d'actualiser les stratégies à la volée. Le facteur humain, maillon le plus faible de la plupart des infrastructures de sécurité, est ainsi plus limité.

Pour plus d'informations sur l'interception des attaques de ransomware, consultez la page www.proofpoint.com/targeted-attack-protection.

TROUSSE DE SURVIE FACE AUX RANSOMWARE

Voici une brève liste d'éléments à évaluer pour savoir si vous êtes prêt à éviter et gérer les menaces que constituent les ransomware.

Avant : prévenir les ransomware

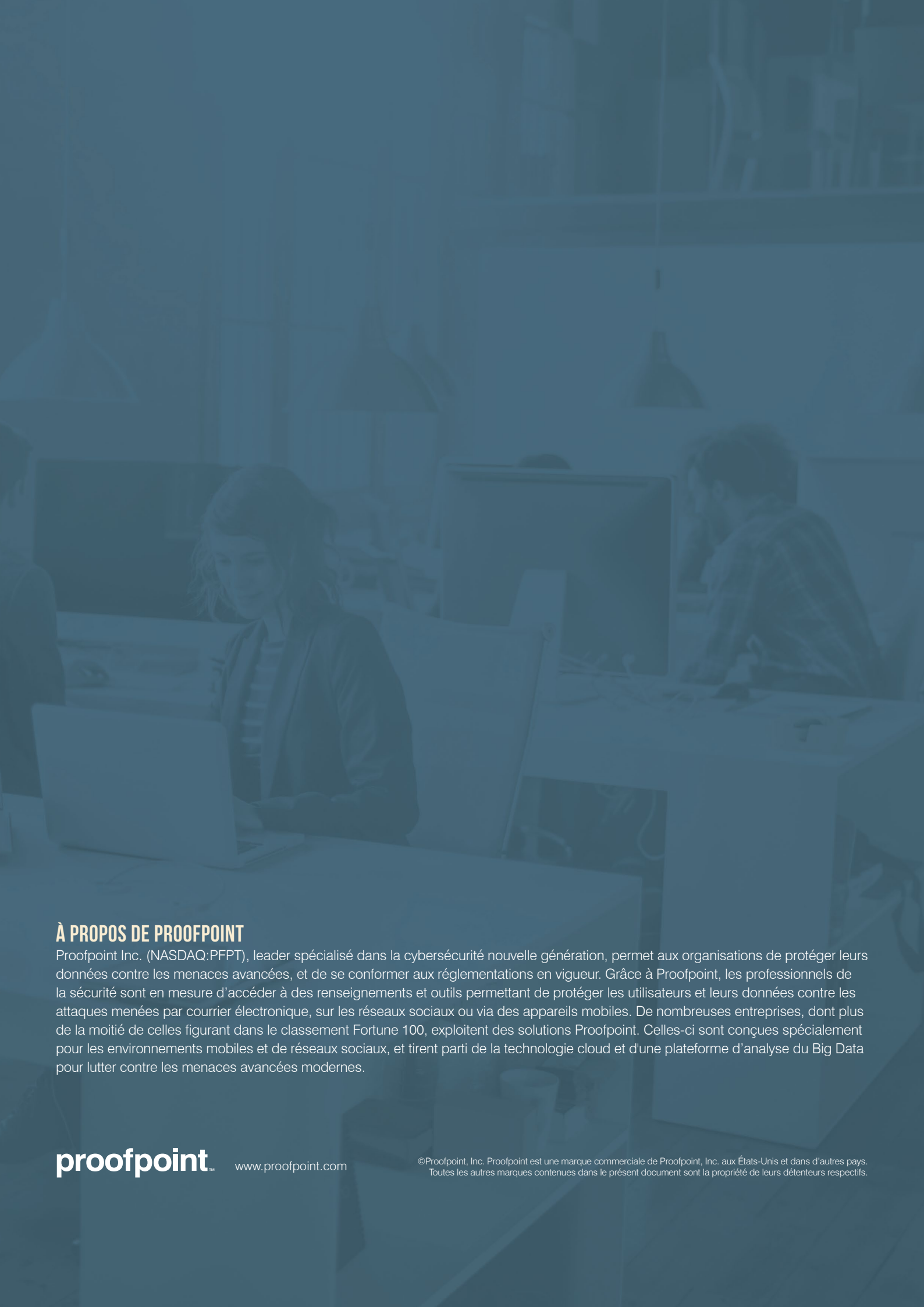
- [ ] Sauvegarder et restaurer
- [ ] Appliquer les mises à jour et les correctifs
- [ ] Former et sensibiliser les utilisateurs
- [ ] Investir dans de solides solutions de sécurité pour la messagerie, les appareils mobiles et les réseaux sociaux

Pendant : reprise des activités

- [ ] Contacter les autorités compétentes
- [ ] Se déconnecter du réseau
- [ ] Évaluer l'ampleur du problème grâce aux renseignements sur les menaces
- [ ] Planifier la réaction
- [ ] Ne pas compter sur les outils gratuits de décryptage de ransomware
- [ ] Restaurer à partir d'une sauvegarde

Après : vérifier et renforcer

- [ ] Nettoyer
- [ ] Effectuer une analyse rétrospective
- [ ] Évaluer le niveau de sensibilisation des utilisateurs
- [ ] Sensibiliser et former
- [ ] Investir dans des mécanismes de protection modernes



À PROPOS DE PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT), leader spécialisé dans la cybersécurité nouvelle génération, permet aux organisations de protéger leurs données contre les menaces avancées, et de se conformer aux réglementations en vigueur. Grâce à Proofpoint, les professionnels de la sécurité sont en mesure d'accéder à des renseignements et outils permettant de protéger les utilisateurs et leurs données contre les attaques menées par courrier électronique, sur les réseaux sociaux ou via des appareils mobiles. De nombreuses entreprises, dont plus de la moitié de celles figurant dans le classement Fortune 100, exploitent des solutions Proofpoint. Celles-ci sont conçues spécialement pour les environnements mobiles et de réseaux sociaux, et tirent parti de la technologie cloud et d'une plateforme d'analyse du Big Data pour lutter contre les menaces avancées modernes.

proofpoint™ www.proofpoint.com