Octobre 2021

Ne payez pas la rançon

Un guide en trois étapes pour la protection contre les ransomwares

Barracuda®
Your journey, secured.

Table des matières

Les ransomwares et leur évolution

Pour dire les choses simplement, un ransomware est un logiciel malveillant qui chiffre vos données ou vous empêche d'accéder à vos propres systèmes d'une manière ou d'une autre. Les criminels exigent ensuite une rançon en échange de la clé de déchiffrage bien qu'il n'y ait, bien entendu, aucune garantie que la clé fonctionne et que vous récupériez vos données. De nombreuses victimes ont payé sans jamais récupérer leurs données.

Contrairement aux attaques « compromettre et chiffrer », façon WannaCry, observées il y a quelques années, une approche multivecteur, plus sophistiquée, est désormais privilégiée par les cybercriminels. Souvent, les attaques démarrent encore par un e-mail de harponnage mais les attaques par ransomware modernes ne se déclenchent plus immédiatement lorsque la cible clique sur le lien malveillant.

Au lieu de cela, les cybercriminels profitent de cette étape pour voler les identifiants de la victime. Ces derniers sont ensuite utilisés pour accéder au réseau de l'entreprise et espionner ses ressources, ses serveurs, ses bases de données ainsi que sa plateforme de messagerie. Cette surveillance peut durer des semaines, voire des mois, avant que l'attaque ne soit lancée. C'est exactement ce qui s'est passé lors de l'attaque par ransomware contre le service public de santé irlandais, le HSE. Les pirates disent avoir passé plusieurs semaines à l'intérieur du réseau du HSE avant de lancer cette attaque qui a permis de chiffrer et de voler 700 Go de données médicales.

L'une des raisons pour lesquelles vous entendez davantage parler de ransomware aujourd'hui est que les barrières à l'entrée ont sauté. La technologie du crime est de plus en plus simple à utiliser. N'importe qui peut aujourd'hui acheter un kit de ransomware et choisir une cible. Des gangs proposent une assistance technique contre un pourcentage de la rançon. Et si ça reste encore trop compliqué, le criminel en herbe peut embaucher des cybercriminels pour mener l'attaque à sa place, créant ainsi un accord de « cybercrime en tant que service ». Avec l'augmentation de la valeur des cryptomonnaies et la popularité des cyberassurances, les attaques par ransomware deviennent également plus rentables pour les criminels, ce qui attire des gangs très organisés. Par ailleurs, les attaques par ransomware commanditées par des États ont repoussé les limites de la cyberguerre.

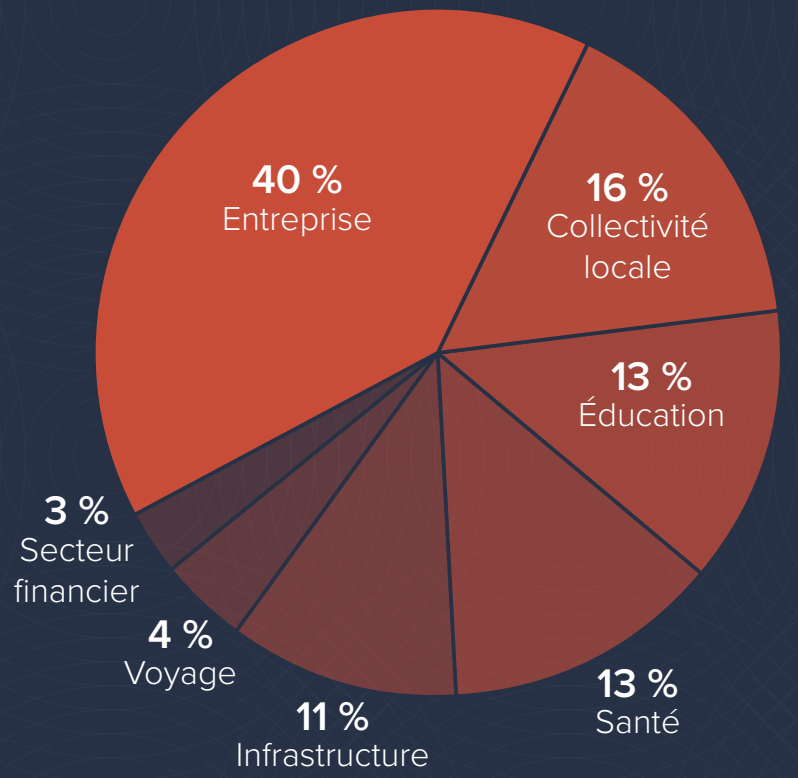
Les cybercriminels surenchérissent

Les attaques par ransomware ont atteint un niveau tel que les gouvernements les traitent désormais comme des actes terroristes. Cette réaction n'a rien d'excessif. Ces attaques ont fortement perturbé des administrations locales, des services de police, des établissements d'enseignement, des systèmes de santé, des infrastructures stratégiques, etc. Aucun secteur, aucune entreprise, aucune institution gouvernementale n'est à l'abri de ces attaques.

Selon une étude récente menée par Barracuda, les attaques contre les sociétés, notamment chez les opérateurs d'infrastructures, les agences de voyages, les services financiers et d'autres entreprises, représentent jusqu'à 57 % des attaques par ransomware observées entre août 2020 et juillet 2021, contre seulement 18 % lors de notre étude de 2020. Les opérateurs d'infrastructures ont subi 11 % des attaques que nous avons étudiées.

Par ailleurs, le montant des rançons augmente radicalement, la rançon moyenne par incident dépassant désormais les 10 millions de dollars. Seuls 18 % des incidents analysés par Barracuda entre août 2020 et juillet 2021 étaient accompagnés d'une demande de rançon inférieure à 10 millions de dollars et dans 30 % des cas, les montants exigés étaient supérieurs à 30 millions de dollars.

Attaques par ransomware, par secteur

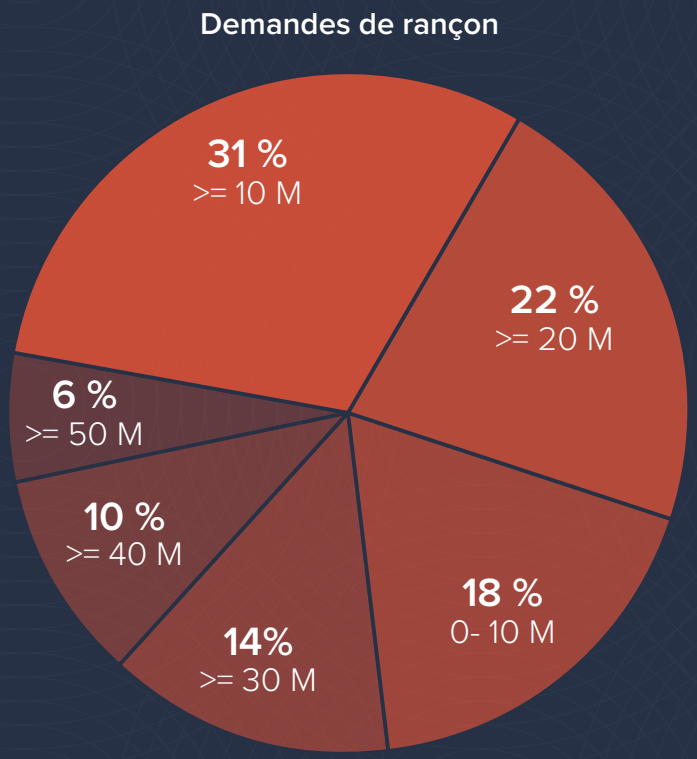


Les ransomwares ne sont pas une menace nouvelle mais leur capacité de nuisance a considérablement augmenté récemment. Les pirates ont élargi leurs compétences et affiné leurs tactiques en vue de créer un double système d'extorsion. Ils basent leurs demandes de rançons sur les recherches effectuées avant l'attaque. Ils dérobent des données sensibles à leurs victimes puis exigent un paiement en échange de la promesse de ne pas publier ni vendre ces données à d'autres criminels. Étant donné que ces gens sont peu fiables, les victimes qui paient se voient souvent demander un nouveau paiement quelques mois plus tard afin de préserver le secret des données volées. Certains pirates acceptent les paiements mais revendent quand même les données.

Payer une rançon ne garantit nullement de récupérer toutes les données chiffrées. Les victimes doivent désormais prendre conscience que toute donnée volée lors d'une attaque par ransomware est compromise à jamais. Par ailleurs, rien ne saurait justifier de payer les criminels pour leurs crimes.

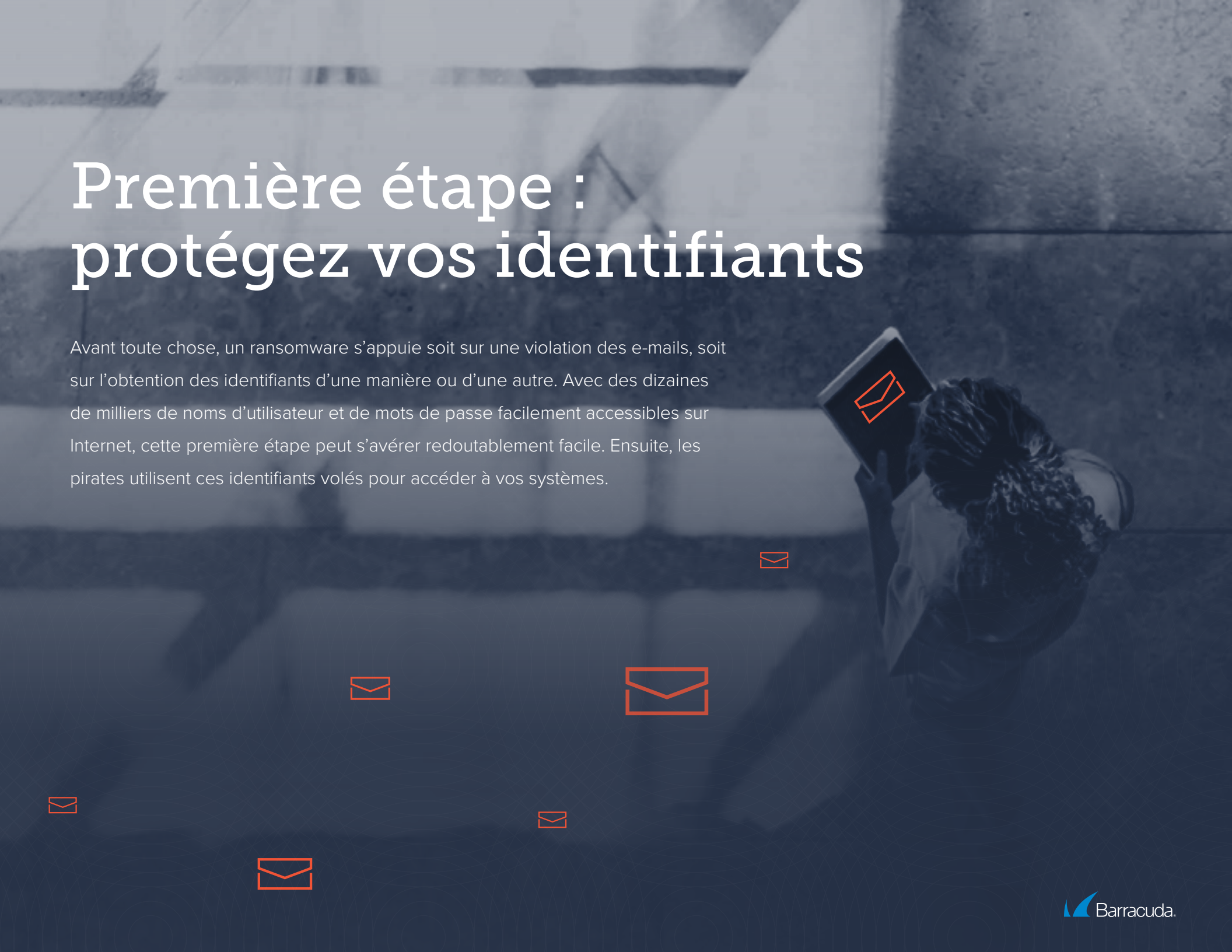
Vous devez donc partir du principe que votre entreprise sera tôt ou tard la cible d'attaques par ransomware. Si l'une d'elles venait à faire mouche, vous devez disposer d'un plan pour ne pas avoir à payer la rançon.

Protéger votre entreprise contre les attaques par ransomware revient à protéger vos données. Cette protection peut se décomposer en trois domaines principaux : la protection de vos identifiants, la sécurisation de vos applications Web, et la sauvegarde de vos données. Examinons plus en détail chacune de ces trois étapes.



Première étape : protégez vos identifiants

Avant toute chose, un ransomware s'appuie soit sur une violation des e-mails, soit sur l'obtention des identifiants d'une manière ou d'une autre. Avec des dizaines de milliers de noms d'utilisateur et de mots de passe facilement accessibles sur Internet, cette première étape peut s'avérer redoutablement facile. Ensuite, les pirates utilisent ces identifiants volés pour accéder à vos systèmes.



Barracuda

Le phishing représentant le principal vecteur d'attaque par ransomware, il est primordial de bien sensibiliser vos collaborateurs à la sécurité des identifiants. Mettez en place un programme de formation des employés à la sécurité des e-mails et déployez une technologie anti-hameçonnage capable d'identifier et de signaler toute activité inhabituelle. En empêchant les pirates informatiques d'accéder aux identifiants, leurs attaques de phishing auront beaucoup plus de mal à aboutir à la propagation de ransomwares.

Les attaques par phishing fonctionnent parce que les gens ne peuvent pas s'empêcher de cliquer sur des liens. Les hackers adaptent minutieusement leurs attaques à leurs victimes en recueillant des informations personnelles publiquement disponibles et en jouant sur l'urgence d'une situation pour déclencher une réponse. Pour les pirates, il suffit qu'une seule personne de votre entreprise clique sur un lien ou ouvre une pièce jointe. Une étude récente de Barracuda a montré qu'en moyenne, 3 % des gens qui reçoivent un e-mail de phishing cliquent sur le lien. En général, l'attaque a pour but de recueillir des identifiants de compte pour permettre au hacker de se déplacer latéralement dans l'entreprise et d'exiger une rançon.

La protection des identifiants et des accès suppose une approche en deux phases : tout d'abord, investir dans des outils de détection et de réponse, puis, dans un deuxième temps, assurer la formation des utilisateurs.

2,94 %
CLIQUENT SUR UN LIEN VERS UN E-MAIL MALVEILLANT

0,78 %
TRANSMETTENT DES E-MAILS MALVEILLANTS

0,17 %
RÉPONDENT AUX E-MAILS MALVEILLANTS

Source: Threat Spotlight : menaces par e-mail après réception

Barracuda

Outils de détection et d'intervention

Votre technologie de protection des e-mails doit non seulement assurer la détection des charges utiles malveillantes (qui sont transportées par des liens ou des pièces jointes), mais également reconnaître quand ces attaques utilisent des tactiques d'ingénierie sociale conçues pour contourner la technologie de filtrage et inciter les utilisateurs à agir. Votre solution de protection doit pouvoir identifier les mauvaises intentions au sein d'un e-mail, même si celui-ci ne contient pas de charge utile malveillante. Les outils de sécurité des e-mails basés sur des algorithmes d'apprentissage machine peuvent détecter les attaques d'ingénierie sociale avec plus de précision. Pour cela, ils recherchent la moindre petite variante d'une forme de communication habituelle.

Vous ne pouvez pas protéger les identifiants de vos utilisateurs sans une bonne solution de protection contre le piratage de comptes. L'authentification multifacteur (MFA) reste une bonne pratique. Toutes les entreprises d'aujourd'hui se doivent de l'adopter. Toutefois, elle n'est pas infaillible et ne suffit pas toujours. Les pirates peuvent trouver des moyens de contourner la MFA en trompant les utilisateurs soit pour qu'ils installent un malware sur les appareils servant à la vérification de leur compte, soit pour qu'ils donnent à de fausses applications un accès à leur compte.

Les entreprises doivent avoir mis en place une protection contre le piratage de compte qui puisse rapidement identifier et signaler les activités malveillantes (comme des connexions suspectes ou des attaques lancées à partir de comptes compromis).

La protection des identifiants et des accès suppose une approche en deux phases : tout d'abord investir dans des outils de détection et d'intervention, puis, dans un deuxième temps, assurer la formation des utilisateurs.

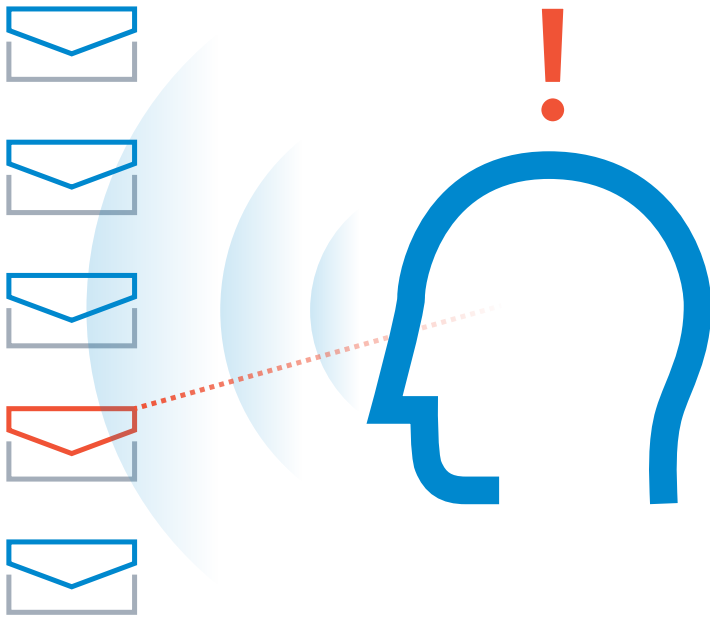
Barracuda

Formez vos utilisateurs

Enfin, dernière ligne de défense, il est primordial de former vos employés à reconnaître et à signaler les attaques. La formation de sensibilisation à la sécurité et les simulations de phishing doivent faire partie de votre stratégie pour la sécurité des e-mails. Historiquement, les attaques par phishing étaient uniquement associées aux e-mails, mais aujourd'hui, les cybercriminels peuvent aussi se servir d'autres canaux comme les SMS et les messages vocaux. Utilisez des simulations de phishing par e-mail, par message vocal et par SMS afin de former les utilisateurs à identifier les cyberattaques, de tester l'efficacité de la formation et d'évaluer quels sont les utilisateurs les plus vulnérables.

Assurez-vous que les formations de cybersécurité ne se limitent pas aux journées d'accueil des nouvelles recrues. Ces formations doivent avoir lieu en continu pour que le personnel reste informé des nouvelles menaces. Par exemple, les criminels utilisent aujourd'hui des méthodes d'ingénierie sociale sophistiquées et difficiles à détecter. Les attaques par spear phishing ciblent un employé précis, ou une partie d'un service, par exemple le service financier, avec des messages sur mesure.

Il est essentiel que vos formations bénéficient de la confiance de vos équipes et les incitent à effectuer des signalements même dans le cas où il s'agit d'une erreur qu'elles ont commises par accident. Une formation de rattrapage peut s'avérer nécessaire mais ne sanctionnez pas un membre du personnel qui effectue un signalement. De nombreuses attaques ne sont pas signalées parce que des employés craignent d'être accusés d'avoir cliqué sur un lien ou ouvert une pièce jointe. Or, les alertes précoces ont une valeur inestimable et doivent être encouragées.



Barracuda

Deuxième étape : sécurisez vos applications et accès Web

Le passage au télétravail a permis à encore plus d'applications de sortir des datacenters pour être proposées sur Internet. Il est parfois arrivé que la sécurité passe au second plan face à l'urgence du maintien des services en état de fonctionnement ; les cybercriminels se tiennent toujours prêts à exploiter de telles vulnérabilités.

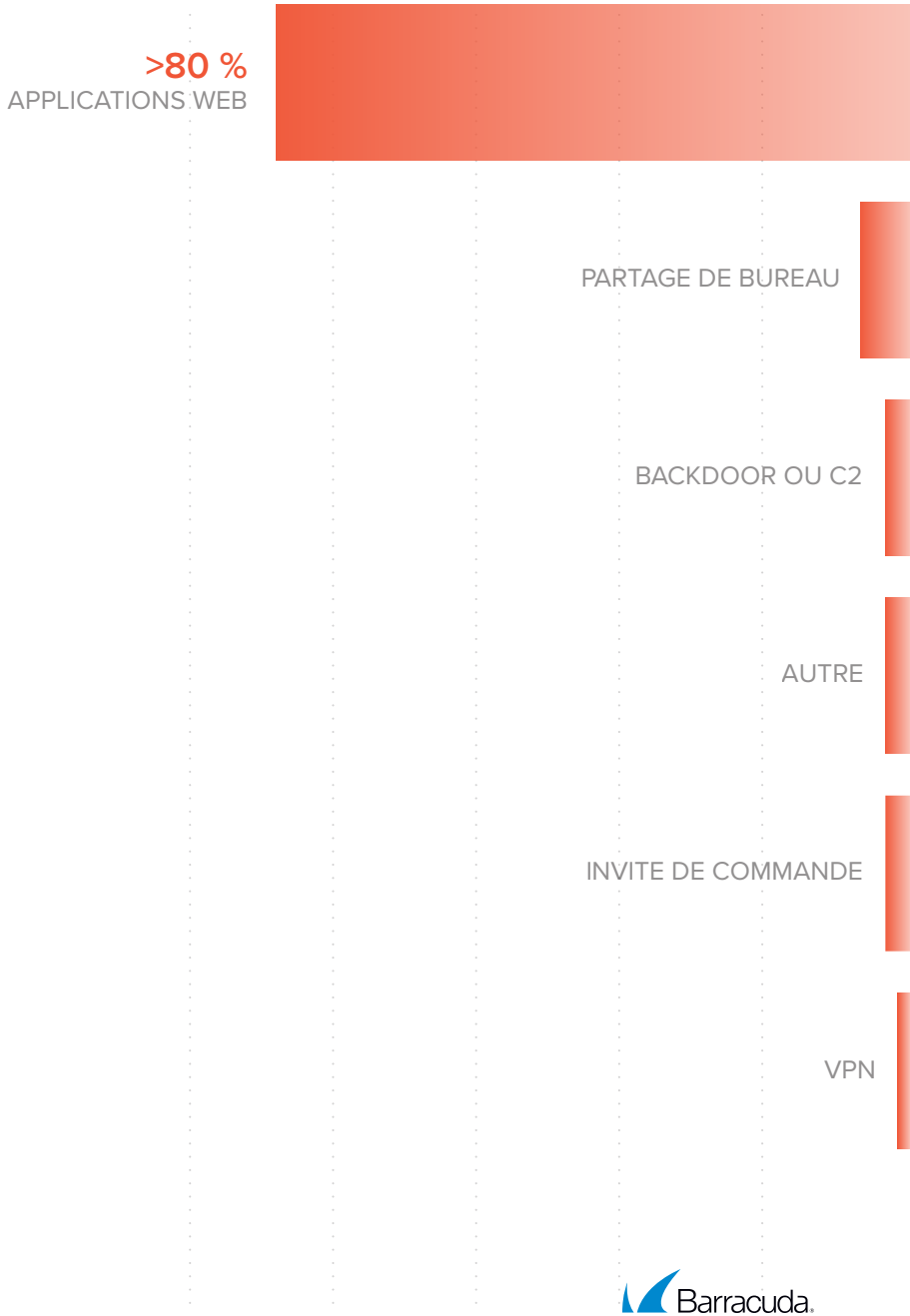
Barracuda

Le rapport 2021 sur les violations de données (Data Breach Investigations Report) de Verizon indique qu'en matière de piratage, les applications Web représentent le premier vecteur d'attaque utilisé. Elles représentent plus de 80 % des violations de données observées.

Les applications en ligne telles que les services de partage de fichiers, les formulaires Web et les sites d'e-commerce peuvent être compromis par des pirates. Les applications Web sont attaquées par le biais de leur interface utilisateur ou par une interface d'API. Ces attaques reposent souvent sur le credential stuffing, la force brute ou l'exploitation des vulnérabilités répertoriées par l'OWASP. Une fois l'application compromise, le pirate peut introduire un ransomware ou autre malware dans le système. Celui-ci peut ensuite se déployer latéralement pour infecter votre réseau ainsi que les utilisateurs de votre application.

Il est important de bien comprendre que la protection des applications est aussi essentielle que la sécurité des e-mails lorsqu'il s'agit de se défendre contre les ransomwares et les autres malwares. L'OWASP (Open Web Application Security Project) vise à sensibiliser le public aux vulnérabilités les plus courantes qui peuvent être exploitées dans le cadre d'une attaque par ransomware.

Source : Verizon – Rapport 2021 sur les violations de données (Data Breach Investigations Report)



Un exemple classique est le piratage d'une chaîne logistique par le ransomware REvil révélé en juillet 2021. Les vulnérabilités d'une application MSP destinée au public ont été exploitées pour diffuser un ransomware auprès de ses clients. En raison des autorisations avancées dont disposait cette application, le ransomware a pu se propager massivement et causer d'importants dégâts avant qu'il ne puisse être arrêté. Toute application Web peut faire l'objet de ce type d'attaque. En effet, les pirates s'introduisent dans l'application et se déplacent ensuite latéralement pour faire des ravages. Un scénario similaire est possible si vous laissez vos ports RDP ouverts sur Internet même si vous modifiez le port par défaut. Lorsqu'elles sont mal protégées, les connexions RDP constituent un vecteur d'attaque idéal pour les cybercriminels, qui exploitent les identifiants dérobés pour tenter d'infecter l'ensemble du réseau par un ransomware.

Jusqu'à

1500

entreprises touchées par l'attaque sur la chaîne logistique par REvil

Barracuda.

Quatre vecteurs d'attaque pour les applications Web

Les applications représentent aujourd'hui l'une des principales cibles des ransomwares. Il y a donc quatre vecteurs d'attaque à protéger : l'accès aux applications, les vulnérabilités des applications Web, l'accès à l'infrastructure et les déplacements latéraux.

1. Accès aux applications

Pour savoir si l'accès aux applications est un problème pouvant compromettre votre organisation, voici quelques questions importantes à vous poser.

- **Vos prestataires et vos salariés en télétravail utilisent-ils des appareils non gérés ou selon le principe du Bring Your Own Device (BYOD) ?** L'exemple le plus classique est sans doute celui des appareils mobiles. Un appareil non géré ou en BYOD peut se faire compromettre puis être utilisé pour récupérer des identifiants ou attaquer votre application.
- **Avez-vous une bonne visibilité sur tous les utilisateurs et appareils connectés à votre réseau ?** Par exemple, vous devez savoir qui se connecte à votre réseau invité et si celui-ci est correctement isolé.
- **Disposez-vous d'une piste d'audit permettant d'identifier qui accède à quoi et à quel moment ?** Vous devez pouvoir accéder à un historique et savoir qui accède à vos applications, comment ces personnes y accèdent et si elles disposent des autorisations nécessaires.

Si un appareil qui n'est pas censé pouvoir accéder au réseau y est connecté et que quelqu'un y a placé des outils de piratage, vous allez au-devant de graves problèmes. Et si vous n'avez pas la visibilité nécessaire pour détecter cela, alors identifier qui accède à quoi et de quelle vulnérabilité il s'agit devient un véritable défi, si bien que vous vous trouverez incapable de combler la faille ou de bloquer l'accès du pirate.

2. Vulnérabilités d'une application Web

Les vulnérabilités des applications Web constituent le deuxième vecteur d'attaque à évaluer pour connaître le niveau réel de sécurisation de vos applications.

Posez-vous les questions suivantes :

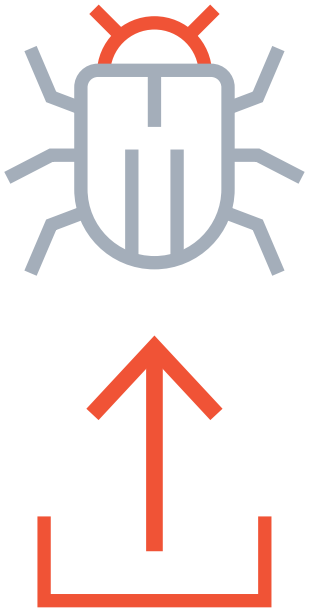
- Votre site Web est-il vraiment sécurisé ? De quand date sa dernière mise à jour ?
- Avez-vous des formulaires sur votre site ? Comment vous prémunissez-vous contre les attaques par formulaire ?
- Autorisez-vous l'envoi de fichiers sur votre site Web ? Comment les sécurisez-vous contre les malwares ?

L'activation de HTTPS ne suffit pas à sécuriser un site. Elle permet seulement d'éviter qu'un pirate espionne quelqu'un lorsqu'il se connecte à votre site Web pour lui voler ses identifiants. Les cybercriminels peuvent toujours utiliser les attaques par force brute dans le cadre d'un site HTTPS pour essayer d'en deviner les bons identifiants.

Adjoindre un CAPTCHA ou le service reCAPTCHA aux formulaires de connexion de votre site n'est pas suffisant non plus, dans la mesure où il est facile d'automatiser et de contourner ces services.

La limitation du nombre de connexions dans un intervalle de temps donné ou par IP est une autre mesure de sécurité facile à contourner, à l'aide d'attaques dites « low-and-slow » et de divers systèmes d'automatisation.

Si vous acceptez l'envoi de fichier, vous avez un autre problème à prendre en compte. Il arrive assez souvent qu'un pirate tente de pirater un site Web en y envoyant un virus ou un malware de type ransomware.



3. Accès à l'infrastructure

Depuis le début de la pandémie de COVID-19, de nombreuses entreprises s'appuient sur un VPN pour donner accès à leurs applications hébergées en interne. Cette pratique est utilisée lorsqu'il n'existe pas de solution de remplacement basée sur du SaaS pour certaines applications auto-hébergées. La fourniture d'un accès VPN à domicile est le seul moyen de maintenir l'activité de l'entreprise. Cependant, en l'absence d'une gestion sérieuse des identités et des accès, cette approche est une véritable bombe à retardement : de nombreux identifiants déjà volés sont susceptibles d'avoir les mêmes noms d'utilisateur et mots de passe que ceux utilisés pour l'accès à votre infrastructure. Le risque pour votre réseau, vos applications et vos données est alors sérieux.

4. Déplacements latéraux

Après avoir compromis votre application ou votre infrastructure à partir d'identifiants volés, les pirates essaieront d'entrer plus en profondeur dans votre réseau et, à partir de là, de lancer d'autres attaques. Voici donc le quatrième vecteur d'attaque à prendre en compte. Posez-vous les questions suivantes :

- Votre réseau d'entreprise est-il divisé en segments correctement isolés ?
- Avez-vous activé une authentification multifacteur pour l'accès à votre réseau ?

Segmenter correctement son réseau requiert beaucoup de temps et de travail. Il est bien plus facile de trouver des raisons de relier deux segments entre eux, en permettant l'accès à l'un depuis l'autre. Mais en fin de compte, on en arrive à rendre son réseau accessible par des moyens que l'on n'avait pas voulus.

L'authentification multifacteur ajoute une importante couche supplémentaire de protection qui contribue à empêcher les pirates d'accéder au réseau.

Barracuda

Comment une attaque par ransomware exploite les vulnérabilités d'une application

Voici un autre scénario (fictif, mais tout à fait possible) que les pirates peuvent suivre pour exploiter les applications mal sécurisées et réussir leur attaque par ransomware. Il s'agit de profiter de la nouvelle popularité dont jouissent les extensions de codes promo pour tenter une arnaque bien connue.

Étape 1

Le pirate crée un site qui imite un vrai site Web de codes promo. Il usurpe un site de codes promo bien connu et y parvient assez facilement grâce aux techniques d'usurpation de domaine et de web scraping, c'est-à-dire d'extraction automatique des données. Nous appellerons ce faux site le « site Web X ».

Étape 2

Le pirate recherche la présence d'une ou plusieurs vulnérabilités répertoriées au top 10 de l'OWASP pour voler les identifiants d'un vrai site Web professionnel mais mal protégé, que nous appellerons le « site Web Y ». Le cybercriminel exploite les défaillances d'authentification et l'exposition de données sensibles pour récolter des identifiants et d'autres informations sensibles sur le site Web Y.

Étape 3

Le pirate utilise les identifiants volés pour lancer une attaque par credential stuffing contre un site e-commerce légitime, que nous appellerons le « site Web Z ». Il s'agit d'une attaque automatisée, qui peut s'exécuter lentement sur plusieurs semaines. Son objectif est de tenter d'associer les identifiants volés aux comptes existants sur ce site.

Étape 4

Dès lors qu'une correspondance est trouvée et que le pirate parvient à se connecter au compte de la victime, le compte de cette dernière est utilisé pour publier des avis sur les produits les plus vendus du site Web Z. En voici un exemple : « Ce produit est génial ! Pour profiter de ce code de réduction et économiser 50 %, cliquez ici. » Le lien de la réduction redirige le visiteur vers le site Web X créé lors de la première étape.

Barracuda

Étape 5

Les victimes potentielles se connectent au site Web Z, cliquent sur l'évaluation du produit et suivent le lien vers le site Web X, sans se rendre compte qu'elles sont redirigées vers un site frauduleux, à moins qu'elles n'observent attentivement le nom de domaine, l'URL, le certificat et d'autres détails du site. Les internautes qui tombent dans le piège entrent ensuite leurs coordonnées pour pouvoir bénéficier du code de réduction. Le pirate connaît désormais l'adresse de quelqu'un qui attend un e-mail de ce site Web. Il vient de gagner la confiance de la victime, qui baisse donc la garde.

Étape 6

La victime reçoit un e-mail personnalisé concernant le produit et le code de réduction, accompagné d'une pièce jointe qu'elle doit installer pour pouvoir en profiter. Il peut s'agir d'un fichier exécutable ou d'une extension de navigateur qui utilise JavaScript pour mener l'attaque. Étant donné que l'e-mail est entièrement personnalisé et attendu par son destinataire, il a peu de chances d'être bloqué par les systèmes de défense traditionnels. Bien que son système d'exploitation lui déconseille l'installation d'exécutables non fiables, la victime, ayant déjà baissé la garde, clique dessus

.

Barracuda

Étape 7

La victime installe la pièce jointe, et l'attaque par ransomware est lancée. Une fois le fichier exécutable installé, plusieurs types d'attaques peuvent être menés : infecter le MBR (Zone amorce), chiffrer la table du système de fichiers ou même empêcher le système d'exploitation de démarrer. Peu de temps après, une demande de paiement est envoyée à la victime. Le pirate tentera probablement d'étendre cette attaque pour récolter d'autres identifiants et d'autres données disponibles sur le réseau. Une fois cette opération terminée, le ransomware chiffrera les données du réseau.

Dans cet exemple, l'attaque par ransomware aboutit uniquement parce que les vulnérabilités des différentes applications web ont permis le déroulement de ce scénario convaincant, à savoir le web scraping d'un site légitime à l'étape 1, le vol d'identifiants à l'étape 2, le « credential stuffing » à l'étape 3, l'avis frauduleux et l'URL malveillante aux étapes 4 et 5, puis l'installation de l'exécutable à l'étape 7. Si les applications avaient été sécurisées efficacement, l'attaque n'aurait jamais abouti.

Barracuda

Comment sécuriser vos applications et vos accès

Sécurisez votre réseau

Empêchez les ransomware de se propager sur votre réseau grâce à la segmentation du réseau et à la prévention des intrusions. Procurez-vous une solution de pare-feu nouvelle génération qui remplit les critères suivants :

- Apporte une sécurité multicouche capable de bloquer les menaces avancées, y compris les attaques de type zero-day
- Comprend une technologie de prévention des intrusions et de sandboxing des malwares
- Fournit une puissante segmentation du réseau afin d'éviter les déplacements latéraux au sein du réseau

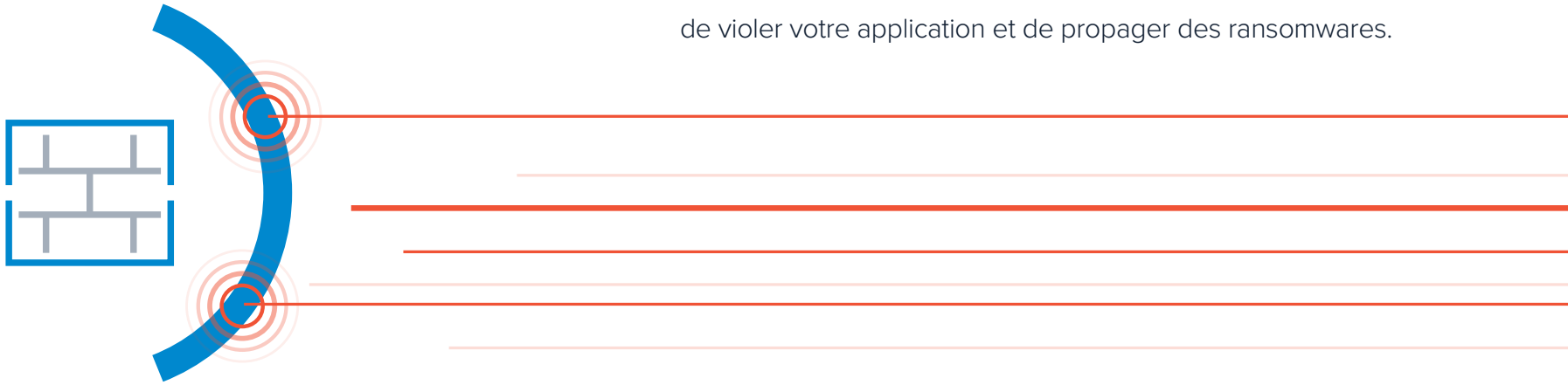
Sécurisez l'accès à vos applications

Vous vous devez de sécuriser l'accès à vos applications à l'aide d'une solution d'accès réseau zero trust (ZTNA) qui permet un accès sécurisé aux applications et aux charges de travail depuis n'importe quel appareil et emplacement.

Procurez-vous une solution qui remplit les critères suivants :

- Vérifie en permanence que seule la bonne personne, munie du bon appareil, peut accéder aux ressources de l'entreprise
- Fait respecter un contrôle d'accès basé sur les rôles et les attributs pour accorder un accès avec le moins de privilèges possible

En bloquant les accès non autorisés, un ZTNA empêche les pirates de violer votre application et de propager des ransomwares.



Sécurisez vos applications Web

L'une des meilleures manières de sécuriser vos applications est d'utiliser un web application firewall (WAF) pour protéger vos logiciels, vos utilisateurs et leurs données, où qu'ils se trouvent. Ainsi, les attaques de bots et les attaques par déni de service seront bloquées et vous aurez une vision bien plus précise de ce qui se passe. Procurez-vous une solution qui dispose des fonctionnalités suivantes :

Facile à déployer et à adapter à votre environnement

Seul un WAF que vous pouvez configurer en fonction de votre environnement pourra vous assurer une protection complète.

Évolutif

Le développement de votre activité, la transformation numérique, ainsi que d'autres facteurs peuvent accroître vos besoins en matière d'applications et de sites Web. Votre WAF doit pouvoir évoluer en même temps que votre entreprise.

Protection globale contre les menaces avancées

Un bon WAF saura vous protéger tout au moins contre les vulnérabilités classées au Top 10 de l'OWASP et les attaques DDoS de la couche application. Pour bénéficier d'une protection complète, optez pour une solution efficace contre les attaques zero-day, le credential stuffing (bourrage d'identifiants), les fuites de données, les bots malveillants, etc.

Facile à mettre à jour

Le firmware du WAF doit être mis à jour régulièrement pour sécuriser votre appareil et améliorer ses performances. Il est préférable de choisir une solution hébergée qui se met à jour automatiquement, sans l'intervention de votre administrateur.

Information continue sur les menaces

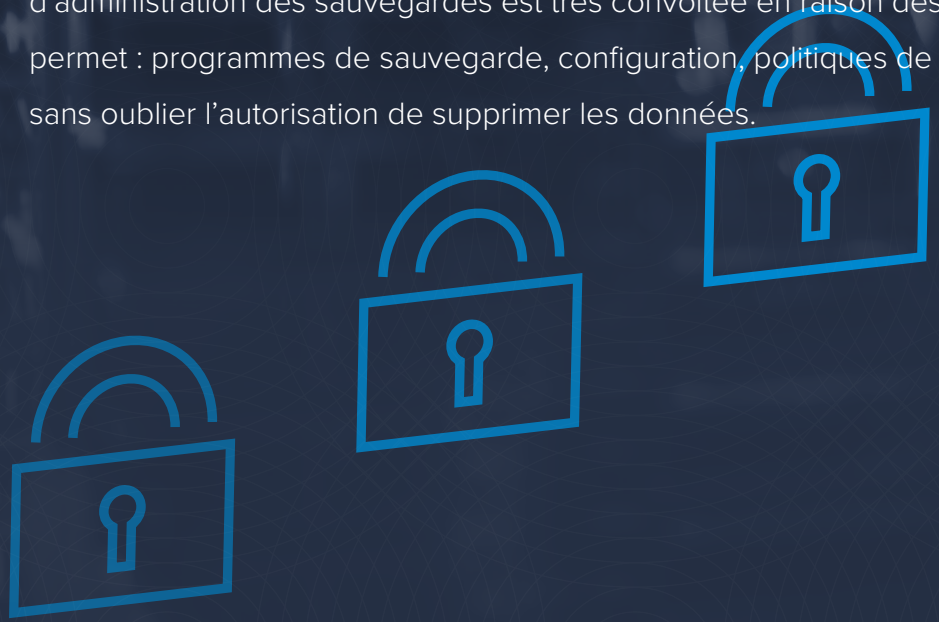
De nouvelles attaques, capables de se propager dans le monde entier en quelques heures, sont mises au point tous les jours. Votre WAF doit pouvoir en être informé en temps réel et utiliser l'apprentissage automatique pour s'adapter aux variants.

En bloquant les vulnérabilités des applications Web ainsi que les menaces zero-day les plus courantes, un bon web application firewall empêche les ransomwares de se frayer un chemin dans vos systèmes.

Troisième étape : sauvegardez vos données

Toute stratégie de protection contre les ransomwares digne de ce nom doit commencer par une réflexion sur la sauvegarde et la reprise après sinistre. Le problème, c'est que les criminels en ont bien conscience.

Les solutions de sauvegarde sont particulièrement scrutées par les cybercriminels pendant cette phase d'exploration du réseau. La console d'administration des sauvegardes est très convoitée en raison des accès qu'elle permet : programmes de sauvegarde, configuration, politiques de rétention, sans oublier l'autorisation de supprimer les données.



Barracuda

Les cybercriminels s'attaquent également à l'espace de stockage pour tenter de supprimer votre serveur de sauvegarde principal ainsi que toute copie secondaire que vous avez créée pour la récupération d'urgence. Après s'être emparés des mots de passe Active Directory pour empêcher les utilisateurs de se connecter à leur compte, ils lancent l'attaque. Ils viennent de prendre le contrôle.

Par ailleurs, trop d'utilisateurs restent encore convaincus que leurs données stockées dans le cloud sont protégées des attaques par ransomware, à tort.

Prenons un exemple simple : un enfant qui navigue sur Internet sur une tablette ou un ordinateur alors qu'il étudie depuis son domicile peut aisément être trompé par un lien malveillant. Or, si cet appareil est connecté et synchronisé à OneDrive par le biais de son compte Office 365 scolaire, un fichier ransomware peut alors être automatiquement téléchargé sur OneDrive et chiffrer les données et fichiers stockés par l'établissement sur le cloud Microsoft.

Vous devez voir la reprise après sinistre comme une part essentielle et stratégique de votre infrastructure. Testez-la régulièrement, en conditions réelles. Il ne suffit pas de vérifier que les sauvegardes sont exécutées : un tel test suppose de procéder à de vraies restaurations de données.

Barracuda

Il arrive aussi que SharePoint, Exchange et d'autres sources de données soient touchés. À noter également que si des lecteurs réseau sont rattachés à des bibliothèques de documents dans Office 365 à l'aide de la fonctionnalité « Ouvrir avec l'Explorateur », le ransomware pourra rechercher des fichiers sur les lecteurs connectés et les infecter.

Même les données dans le cloud ou en SaaS peuvent se retrouver chiffrées par un ransomware. Microsoft garantit la disponibilité du service mais vous recommande de sauvegarder vos données à l'aide d'une solution de sauvegarde tierce. Vos données sont peut-être sauvegardées dans Microsoft Office 365 mais Office 365 n'est pas conçu pour restaurer des instances complètes comme il peut être nécessaire de le faire après une attaque par ransomware.

Vous avez donc besoin de défendre et d'isoler correctement vos données sauvegardées. Réfléchissez à la fréquence à laquelle les systèmes doivent être reproduits en miroir et à la vitesse à laquelle vous pouvez restaurer les systèmes depuis ces images.

Il faut vous assurer que la restauration des systèmes depuis les sauvegardes peut effectivement avoir lieu, dans un délai raisonnable et à partir de données suffisamment récentes. Aussi, il vous faut prendre le contrôle de la situation et vous en occuper pour de bon. Vous ne pouvez pas vous contenter de consulter les journaux pour vérifier que les données sont répliquées assez souvent et de manière suffisamment fidèle.

Barracuda

Il faut effectuer de vrais exercices pour prouver que les systèmes fonctionnent comme prévu. Vous pouvez sélectionner un service, voire une seule application, plutôt que d'arrêter l'ensemble de votre infrastructure mais il est essentiel de pouvoir avoir une confiance absolue dans sa capacité à rétablir les systèmes rapidement.

C'est votre filet de sécurité. Dans l'hypothèse où tout le reste aurait échoué, si vous disposez d'une sauvegarde vraiment à jour et sécurisée alors les criminels ne peuvent rien contre vous.

Vous devez voir la reprise après sinistre comme une part essentielle et stratégique de votre infrastructure. Testez-la régulièrement, en conditions réelles. Il ne suffit pas de vérifier que les sauvegardes sont exécutées : un tel test suppose de procéder à de vraies restaurations de données.

Barracuda

Comment choisir votre solution de sauvegarde

Pour prévenir les risques associés aux ransomwares, équipez-vous d'une solution de sauvegarde complète, qui propose les avantages suivants :

Stockage immuable

Même s'ils accèdent à vos sauvegardes, les cybercriminels ne pourront ni modifier ni supprimer vos données.

Cloud protégé par air gap

Conservez une copie de votre sauvegarde sur un cloud sécurisé basé sur un réseau isolé.

Authentification multifacteur (MFA)

Sécurisez les comptes et les identifiants qui permettent d'accéder à votre sauvegarde.

Redondance

Dupliquez vos sauvegardes sur site et sur le cloud et transférez-les vers un autre emplacement.

Contrôle d'accès basé sur les rôles

Appliquez le principe du privilège minimum pour chaque utilisateur ayant accès au système de sauvegarde.

Barracuda

Conclusion

Même si votre entreprise dispose d'une cyberassurance ou de ressources suffisantes pour payer la rançon, il est extrêmement risqué de miser sur cette option pour tenter de récupérer vos données. Rien ne vous garantit que les pirates déchiffreront vos données une fois la rançon payée, et quand bien même ils le feraient, il ne faut pas oublier que selon une étude récente, 80 % des entreprises qui choisissent de payer se font attaquer à nouveau.

Même si vous avez fait tout ce que nous avons évoqué précédemment, vous serez quand même attaqué. Même avec la meilleure protection possible, se préparer au pire relève du bon sens. Les criminels peuvent investir des millions pour s'introduire dans vos systèmes. Le seul moyen raisonnable de se préparer est de partir du principe qu'un jour, ils y parviendront.

Vous devez réfléchir à ce qui se passera, ce jour-là. Vous avez besoin d'un plan pour ne pas avoir à payer la rançon.

- ☐ Qui fait partie de votre équipe de réponse aux ransomwares ?
- ☐ Qui doit répondre si un problème a lieu un week-end ou un jour férié ?
- ☐ Qui s'en occupe ?
- ☐ Quand en informerez-vous vos clients et vos fournisseurs ?
- ☐ Qui vous assiste sur le plan juridique ?
- ☐ Devez-vous prévenir une autorité de réglementation ou la police ?
- ☐ Devez-vous faire appel à un spécialiste en relations publiques dès le départ ?

Comparez cela à un exercice d'évacuation en cas d'incendie : on ne se prépare pas quand le bureau est déjà en proie aux flammes. Néanmoins, les attaques actuelles les plus courantes évoluent en permanence. C'est pourquoi votre stratégie et vos techniques de défense doivent être régulièrement mises à jour. Téléchargez notre liste de contrôle anti-ransomware pour vous aider à élaborer un plan.

Barracuda

Préparez-vous à répondre aux attaques

Vous devez réfléchir à ce qui se passera au moment où l'attaque sera identifiée et si l'attaque vire à la violation. Pouvez-vous la contenir ou la restreindre à une partie de votre infrastructure en bloquant le trafic réseau ? Avez-vous besoin de mettre provisoirement certains systèmes hors ligne ? Si oui, qui en prend la responsabilité ?

Dans ces circonstances, tout est question de rapidité. Une rapidité qui est la clé. Vous ne pouvez pas vous permettre d'attendre que votre directeur technique vous rappelle. Tout le monde doit tout de suite savoir quoi faire.

Si tout se déroule suffisamment vite, vous pourrez peut-être même empêcher le chiffrement de se faire. Vous avez également besoin d'un plan pour vérifier rapidement l'ensemble de vos systèmes, afin de vous faire une idée précise de la situation.

De nos jours, les pirates ont tendance à utiliser plusieurs types d'attaques simultanément. Alors que vous essayez par exemple de gérer une attaque par déni de service, une attaque par ransomware se produit ailleurs. Une fois que vous avez compris ce qui s'est passé et où l'attaque a eu lieu, vous pouvez commencer à réfléchir à ce que vous devez faire pour éradiquer le malware et rétablir vos systèmes.

Une fois vos systèmes et vos données restaurés, que ce soit à l'aide d'une sauvegarde ou en isolant l'attaque suffisamment tôt, et une fois que vous avez vérifié qu'il n'y a pas de données corrompues ou manquantes, il est temps de lancer l'analyse.

Évaluez l'efficacité de votre réponse face à une véritable attaque. Analysez ce qui a bien fonctionné, ce qui a reposé sur un coup de chance et ce qui s'est avéré insuffisant. Envisagez des manières d'améliorer et d'intervenir plus rapidement la prochaine fois.

Si vous avez mis en place les systèmes appropriés, vous aurez une grande quantité de données d'analyse sur lesquelles vous appuyer. Il y aura peut-être même de quoi alimenter le travail d'enquête de la police. Quelles que soient vos données, vous devez prendre le temps de faire un compte-rendu à l'équipe d'intervention et voir quelles leçons tirer de l'épisode.

Insistons sur le fait que l'intervention ne peut être uniquement technologique : c'est aussi une affaire de personnes et de procédures. Faut-il revoir la formation du personnel ? Votre équipe d'intervention était-elle fonctionnelle ou doit-elle être renforcée ?

Barracuda

Restez informé

Les stratégies de défense actuelles se doivent d'être dans l'action et non dans la simple réaction. Ce dont vous avez besoin, c'est de la meilleure transparence possible quant à vos systèmes de sécurité. Vous devez observer ce qui se passe, à quel moment et à quelle fréquence. Vous devez être attentif à la situation de vos confrères. En effet, les pirates qui utilisent des ransomwares ciblent souvent des marchés verticaux ou des zones géographiques spécifiques. Vous devez également vous tenir informé des dernières menaces, tendances ou informations de votre secteur, à l'aide de ressources telles que le blog de Barracuda.

Les données sont essentielles à la réussite de votre stratégie de sécurité, car la position ou le profil de votre entreprise seront probablement amenés à évoluer. Vous devez vous tenir prêt et informé pour effectuer tout changement qui s'avérerait nécessaire. La sécurité en tant que service peut vous débarrasser de la pénible tâche consistant à suivre les évolutions, ce qui est particulièrement utile dans un contexte où la cybersécurité évolue plus vite que jamais.

Pour certaines entreprises à la position très active ou au profil de risque élevé, il peut être nécessaire d'employer du personnel à plein temps pour des tâches de veille technologique afin d'être informé à l'avance d'attaques potentielles.

Mais dans la plupart des entreprises, il n'est pas nécessaire d'aller si loin. Choisissez le bon partenaire et mettez en place les bases de la sécurité. Dans la vraie vie, et contrairement à ce que l'on peut voir au cinéma ou à la télé, les pirates ne sont pas des génies du mal passionnés par l'idée de déjouer les systèmes de sécurité les plus élaborés au monde. Pour l'essentiel, il s'agit de gens qui cherchent à se faire de l'argent facile en profitant d'une entreprise négligente, qui n'a pas fait attention ou n'a pas investi dans la sécurité appropriée.

Suivre ces trois étapes (protéger ses identifiants, sécuriser ses accès et applications Web et sauvegarder ses données) n'est pas une garantie absolue contre les attaques par ransomware. C'est en revanche la garantie que vous n'aurez pas à payer de rançon pour récupérer vos données.

Barracuda en quelques mots

Rendre le monde plus sûr est notre objectif chez Barracuda. nous pensons que chaque entreprise doit se doter de solutions cloud, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives qui s'adaptent à la croissance de nos clients.

Plus de 200 000 entreprises à travers le monde font confiance à Barracuda pour les protéger — elles restent sereines face aux risques qui sont toujours là — et peuvent se concentrer sur le développement de leur activité. Pour en savoir plus, rendez-vous sur fr.barracuda.com.

Barracuda
Your journey, secured.