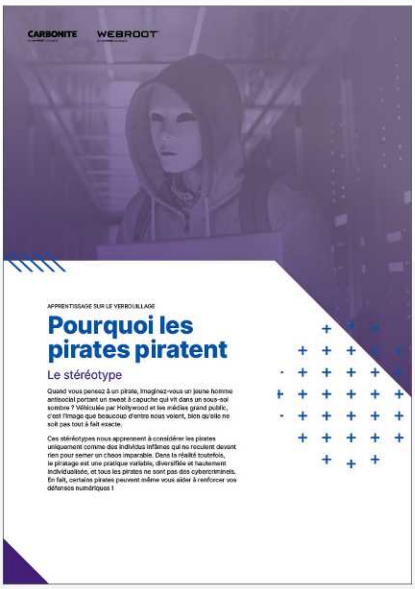
APPRENTISSAGE SUR LE VERROUILLAGE

Pourquoi les pirates piratent

Introduction

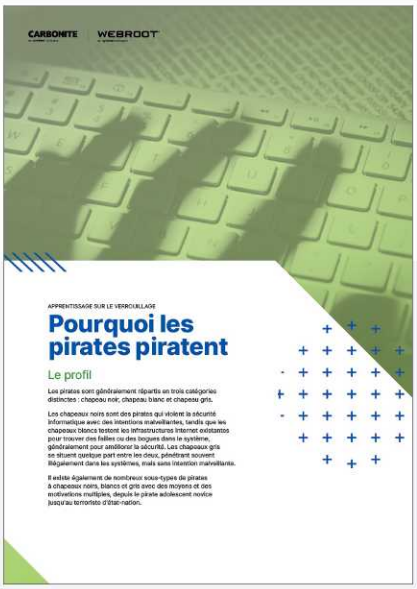
À mesure que la cybersécurité se complique, les criminels du monde entier s'adaptent. Leurs méthodes vous rendent vulnérable et de nombreuses organisations sont en danger. Rester informé sur cet aspect en constante évolution est vital. Dans cet eBook éducatif, nous explorons l'esprit des pirates et nous ouvrons la fenêtre sur leur monde. Découvrez pourquoi il est important de démystifier les stéréotypes courants, de vous informer sur leurs méthodes et leurs motivations et de découvrir qui ils ciblent le plus. Les experts en sécurité informatique Tyler Moffitt, Kelvin Murray et Grayson Milbourne vous aident à naviguer dans les eaux incertaines d'aujourd'hui et vous donnent des conseils sur la façon de verrouiller votre entreprise et de protéger vos clients contre les menaces permanentes.

C'est de votre responsabilité qu'il s'agit !
Webroot.com/LockdownLessons



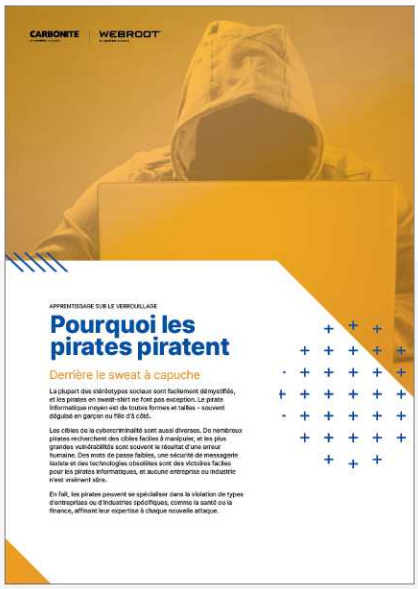
Le stéréotype

À quoi ressemble un pirate ? Les stéréotypes nous incitent à considérer les pirates uniquement comme des individus infâmes qui ne reculent devant rien pour semer un chaos imparable, mais la réalité est bien différente. Découvrez la vérité qui se cache derrière les stéréotypes et pourquoi vous devriez faire attention.



Le profil

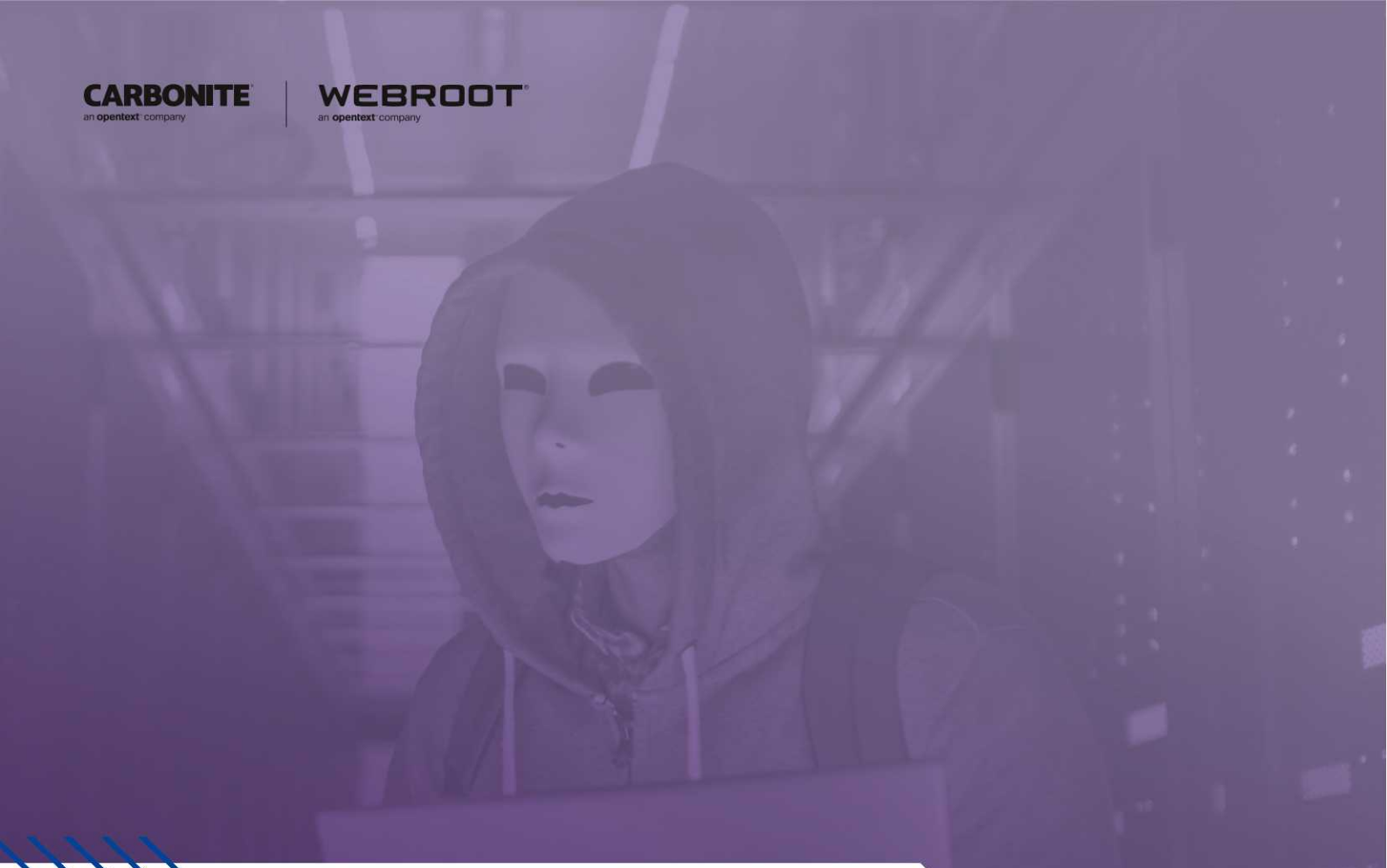
Que recherchent les pirates ? Les pirates sont généralement répartis en trois catégories distinctes : chapeau noir, chapeau blanc et chapeau gris. Leurs méthodes et leurs motivations varient, en allant du gain financier à la perturbation, et certains piratent même pour le plaisir. Découvrez pourquoi c'est important pour votre entreprise.



Derrière le sweat à capuche

Qui sont les cibles des pirates ? Comprendre pourquoi les pirates informatiques en veulent à votre entreprise et quelles méthodes ils utilisent pour s'introduire dans vos systèmes peut vous aider à contrecarrer les attaques avant qu'elles ne se produisent.

CARBONITE an opentext company | WEBROOT an opentext company



APPRENTISSAGE SUR LE VERROUILLAGE

Pourquoi les pirates piratent

Le stéréotype

Quand vous pensez à un pirate, imaginez-vous un jeune homme antisocial portant un sweat à capuche qui vit dans un sous-sol sombre ? Véhiculée par Hollywood et les médias grand public, c'est l'image que beaucoup d'entre nous voient, bien qu'elle ne soit pas tout à fait exacte.

Ces stéréotypes nous apprennent à considérer les pirates uniquement comme des individus infâmes qui ne reculent devant rien pour semer un chaos imparable. Dans la réalité toutefois, le piratage est une pratique variable, diversifiée et hautement individualisée, et tous les pirates ne sont pas des cybercriminels. En fait, certains pirates peuvent même vous aider à renforcer vos défenses numériques !

L'histoire du pirate hollywoodien

Le portrait moderne d'un pirate a été forgé par des films et des émissions de télévision populaires qui perpétuent le mythe du jeune génie informatique imprudent qui peut tout pirater.

Les origines de ce stéréotype remontent en fait aux années 1960, avec la comédie britannique « The Italian Job ». Grâce au succès du film, le stéréotype a continué d'évoluer au cours des décennies suivantes jusqu'à ce qu'une représentation plus précise apparaisse enfin en 2015.

« The Italian Job » (1969)

Un voleur reçoit l'aide d'un groupe de pirates informatiques comptant parmi les plus infâmes de Grande-Bretagne pour voler des lingots d'or. C'était l'une des premières représentations hollywoodiennes du piratage en tant que commerce glamour et rentable.

« WarGames » (1983)

Un lycéen pirate un ordinateur militaire et active accidentellement l'arsenal nucléaire américain. L'un des premiers films à envisager les conséquences mondiales dévastatrices d'une seule cyberattaque.

« Hackers » (1995)

Un groupe de pirates adolescents doit prouver qu'un sinistre superhacker les accuse de détournement de fonds. Une des premières représentations célèbres d'une femme pirate, interprétée par Angelina Jolie.

« The Matrix » (1999)

Un pirate informatique découvre que toute vie sur terre n'est peut-être qu'une façade élaborée. Ce film a contribué à véhiculer le stéréotype du « génie informatique » du piratage rapide que nous connaissons aujourd'hui.

« Mr. Robot » (2015)

Un jeune programmeur travaille comme ingénieur en cybersécurité le jour et comme pirate justicier la nuit. Ce film est considéré comme l'une des représentations fictives les plus précises des vrais pirates.

Réalité contre fiction

Hollywood dépeint souvent les pirates comme des justiciers vertueux ou des terroristes pervers. Cette fausse idée courante romance le piratage tout en occultant les vrais dangers ; cependant, des représentations précises peuvent également entraîner des problèmes dans le monde réel. Après la diffusion de « WarGames » en 1983, le gouvernement américain a signé le Computer Fraud and Abuse Act pour dissuader les pirates de reproduire les attaques présentées dans le film.

Alors que les cinéastes et les acteurs prennent des libertés avec leurs représentations, le stéréotype du « pirate hollywoodien » offre un petit aperçu des motivations réelles des pirates, comme l'espionnage, le vol, la perturbation et même l'altruisme.

Démystifier les stéréotypes des pirates

Les pirates ont plusieurs casquettes et leurs moyens et motivations sont multiples. L'un des plus grands mythes sur les pirates est que la plupart d'entre eux sont des génies de l'informatique, alors qu'en réalité, de nombreux pirates utilisent des logiciels au code élémentaire pour concevoir des virus ou s'introduire dans des systèmes avec peu ou pas de connaissances en programmation.

Mythe : tous les pirates sont des « méchants » qui volent des informations.

Vérité : les pirates informatiques sont des personnes qui utilisent des ordinateurs, des réseaux ou d'autres technologies et compétences pour accéder aux systèmes informatiques pour différentes raisons.

Mythe : tous les pirates sont des hommes.

Vérité : le pirate moyen est un homme de moins de 35 ans[1], mais il y en a de tout âge, sexe ou origine ethnique.

Mythe : tous les pirates sont des loups solitaires.

Vérité : les pirates sont coordonnés et travaillent au sein d'un vaste réseau complexe. Ils sont souvent rémunérés, prennent des vacances fixes, reçoivent des primes et sont engagés dans des contrats de vente incluant des portails de revendeurs et de la location de composants. Il est courant que les pirates soient impliqués dans des groupes ou des organisations de plus grande envergure.

Mythe : les pirates doivent travailler vite.

Vérité : les pirates ne regardent généralement pas la pendule, et beaucoup adoptent une approche lente et méthodique pour obtenir ce qu'ils veulent.

Mythe : le piratage brasse peu d'argent.

Vérité : le coût moyen d'une violation de données est de 3,92 millions $[2] et 71 % des violations sont motivées par l'argent. Le pirate moyen peut gagner jusqu'à 40 fois le salaire moyen d'un développeur de logiciel.[1]

Mythe : les pirates n'attaquent que les grandes entreprises.

Vérité : les PME sont des cibles de choix. Plus de 70 % des cyberattaques ciblent les petites entreprises[3] et les MSP détiennent la palme en ce qui concerne l'accès aux données.

En réalité, tous les pirates ne veulent pas ruiner votre entreprise. Les motivations des pirates varient entre la perturbation et le gain financier en passant par le simple amusement.

« Les cybercriminels utilisent l'automatisation pour assurer le travail d'une équipe complète de pirates ! Les cyberattaques basées sur l'IA peuvent frapper plusieurs entreprises à la fois, et aucune entreprise n'est trop grande ou trop petite pour être une cible. »

Tyler Moffitt
Analyste principal de la recherche sur les menaces, Webroot

En comprenant mieux les véritables méthodes et motivations qui se cachent derrière les mythes, vous pouvez apprendre à verrouiller votre entreprise et à protéger vos clients contre les plus grandes menaces d'aujourd'hui.

[1] HackerOne. « The 2019 Hacker Report » (août 2019)
[2] Intelligence de sécurité. « 2019 Cost of a Data Breach Report » (juillet 2019)
[3] Verizon. « 2019 Data Breach Investigations Report » (mai 2019)

CARBONITE an opentext company | WEBROOT an opentext company

APPRENTISSAGE SUR LE VERROUILLAGE

Pourquoi les pirates piratent

Le profil

Les pirates sont généralement répartis en trois catégories distinctes : chapeau noir, chapeau blanc et chapeau gris.

Les chapeaux noirs sont des pirates qui violent la sécurité informatique avec des intentions malveillantes, tandis que les chapeaux blancs testent les infrastructures Internet existantes pour trouver des failles ou des bogues dans le système, généralement pour améliorer la sécurité. Les chapeaux gris se situent quelque part entre les deux, pénétrant souvent illégalement dans les systèmes, mais sans intention malveillante.

Il existe également de nombreux sous-types de pirates à chapeaux noirs, blancs et gris avec des moyens et des motivations multiples, depuis le pirate adolescent novice jusqu'au terroriste d'état-nation.

Pirates à chapeaux noirs, blancs et gris

Pourquoi classer les pirates en fonction de la couleur de leur chapeau ? L'analogie rappelle les westerns américains des années 30 et 40, lorsque les gentils portaient des chapeaux de cow-boy blancs et les méchants, des noirs. Bien qu'il s'agisse d'une simplification à outrance, l'archétype du chapeau nous aide à définir différents groupes de pirates en fonction de leur comportement et de leurs motivations.

Chapeaux noirs

Aussi connus sous le nom de cybercriminels ou d'acteurs de menaces, les pirates à chapeau noir violent la sécurité informatique avec une intention malveillante ou pour un gain personnel.

Les chapeaux noirs talentueux tirent profit non seulement du ciblage des entreprises et des particuliers, mais aussi de la vente de leurs outils à des pirates informatiques moins techniquement capables (« pirates adolescents »), tels que les ransomwares sous forme de service ou les kits d'exploitation à louer. Les chapeaux noirs sont généralement hautement qualifiés, mais ne sous-estimez pas les débutants. Ils peuvent facilement atteindre une grosse cible avec les bons outils.

Pourquoi piratent-ils ? Le gain financier est la principale motivation des pirates à chapeau noir et le piratage peut être très rentable. Les chapeaux noirs gagnent généralement de l'argent par le vol, la fraude, l'extorsion et d'autres moyens néfastes.

Chapeaux blancs

Également connus sous le nom de pirates éthiques, les chapeaux blancs testent l'infrastructure Internet existante pour rechercher des failles ou trouver des bogues dans un système.

Les chapeaux blancs ont toujours été essentiels pour garantir la sécurité du réseau des organisations. Ils travaillent souvent en tant qu'employés ou consultants, généralement pour les gouvernements et les grandes entreprises, bien que certains s'associent à des MSP et des sociétés de sécurité pour aider les PME. Plus de 300 000 pirates à chapeau blanc environ sont enregistrés dans le monde.[1]

Pourquoi piratent-ils ? Les motivations du chapeau blanc varient, mais l'argent et l'altruisme figurent en tête de liste. Le pirate éthique certifié (Certified Ethical Hacker) gagne en moyenne 91 000 $ par an.[2] Les « primes pour bogues » constituent pour les chapeaux blancs un moyen légal de gagner de l'argent et d'être reconnus.

Chapeaux gris

Les pirates à chapeau gris sont ceux dont les pratiques de piratage peuvent violer des normes éthiques, mais généralement sans intention malveillante.

À l'instar des chapeaux blancs, les chapeaux gris piratent souvent les systèmes informatiques pour informer l'administrateur ou le propriétaire que son réseau présente une ou plusieurs vulnérabilités, qui doivent être corrigées. Cependant, contrairement aux chapeaux blancs, les pirates à chapeau gris peuvent ne pas travailler pour une entreprise officielle et peuvent choisir d'extorquer des victimes, en proposant de supprimer des bogues pour une somme modique.

Pourquoi piratent-ils ? Les chapeaux gris sont peut-être moins malveillants que leurs homologues à chapeau noir, mais l'argent reste un facteur de motivation majeur, même si certains piratent pour s'amuser ou pour améliorer leurs compétences en programmation.

Sous-types de pirates

Entre le chapeau blanc le plus altruiste et le chapeau noir profondément sinistre, il existe un large éventail de personnages pirates, guidés par leurs intentions de piratage.

Pirates adolescents

Fréquemment associés au stéréotype du « pirate au sweat à capuche », les pirates adolescents sont des novices en programmation dotés de certaines connaissances en écriture de code mais manquant de savoir-faire. Ils utilisent généralement des logiciels gratuits et open source, faciles à trouver sur le Dark Web, pour infiltrer les réseaux, et ils peuvent porter des chapeaux noirs, blancs ou gris.

Hacktivistes

Les hacktivistes sont des pirates à chapeau gris dont le principal objectif est d'attirer l'attention du public sur une question politique ou sociale par le biais de la perturbation. Deux des stratégies hacktivistes les plus courantes consistent à voler et à exposer des informations sensibles ou à lancer une attaque par déni de service distribué (DDoS). L'un des groupes hacktivistes les plus connus est Anonymous, tristement célèbre pour avoir immobilisé le site Web de la CIA.

Chapeaux rouges

Les chapeaux rouges sont des chapeaux à nuance de gris plus blanche dont le seul objectif est de bloquer ou de détruire les efforts des pirates à chapeau noir. Considérés comme les « justiciers » du monde des pirates, les chapeaux rouges tenteront d'arrêter les attaques malveillantes avec leurs propres outils plutôt que de signaler la violation.

État-nation

Les pirates de l'état-nation sont ceux qui se livrent à l'espionnage, à l'ingénierie sociale ou à l'intrusion informatique dans le but d'acquérir des informations classifiées ou de demander d'importantes rançons. Soutenus par les gouvernements, ils sont souvent sophistiqués et bien formés.

Initié malveillant

Un initié peut être un employé mécontent actuel ou ancien qui vole ou détruit des informations, ou une personne embauchée par un concurrent pour voler des secrets commerciaux. Les données les plus précieuses pour un initié malveillant sont les noms d'utilisateur et les mots de passe, qui peuvent ensuite être vendus sur le Dark Web pour générer un bénéfice considérable.

Comprendre les sous-types de pirate peut vous aider à identifier les menaces potentielles ainsi que les opportunités d'exploitation du piratage pour protéger votre entreprise.

« Alors que cela n'était pas le cas il y a des années, la plupart des chapeaux noirs piratent maintenant pour un gain financier parce qu'il y a beaucoup d'argent à gagner dans le piratage. Même les chapeaux blancs qui utilisent leurs pouvoirs pour le bien peuvent faire des bénéfices. »

Tyler Moffitt
Analyste principal de la recherche sur les menaces, Webroot

Les pirates peuvent cibler n'importe quelle entreprise pour n'importe quelle raison ! Comprendre leurs méthodes et leurs motivations peut vous aider à verrouiller votre entreprise et à protéger vos clients.

[1] HackerOne. « The 2019 Hacker Report » (août 2019)
[2] PayScale. « Certified Ethical Hacker (CEH) Salary Data » (décembre 2019)

CARBONITE
an opentext company

WEBROOT
an opentext company

APPRENTISSAGE SUR LE VERROUILLAGE

Pourquoi les pirates piratent

Derrière le sweat à capuche

La plupart des stéréotypes sociaux sont facilement démystifiés, et les pirates en sweat-shirt ne font pas exception. Le pirate informatique moyen est de toutes formes et tailles - souvent déguisé en garçon ou fille d'à côté.

Les cibles de la cybercriminalité sont aussi diverses. De nombreux pirates recherchent des cibles faciles à manipuler, et les plus grandes vulnérabilités sont souvent le résultat d'une erreur humaine. Des mots de passe faibles, une sécurité de messagerie laxiste et des technologies obsolètes sont des victoires faciles pour les pirates informatiques, et aucune entreprise ou industrie n'est vraiment sûre.

En fait, les pirates peuvent se spécialiser dans la violation de types d'entreprises ou d'industries spécifiques, comme la santé ou la finance, affinant leur expertise à chaque nouvelle attaque.

Cibles du viol : les astuces du métier

Dans le même esprit que le stéréotype actuel du sweat à capuche, les petites et moyennes entreprises croient en une fausse idée dangereuse selon laquelle les pirates informatiques ne ciblent que les grandes organisations, alors qu'en fait, toute entreprise qui gère des informations personnellement identifiables (PII), des comptes bancaires, des données de santé et d'autres informations sensibles est vulnérable. La simple vérité est que la majorité de l'argent du crime provient de PME des principaux secteurs verticaux. Alors, qui constitue une cible ?

Fournisseurs de services gérés

Les MSP détiennent de nombreuses données précieuses pour plusieurs clients de tous les secteurs, ce qui en font des cibles de choix. Le saut d'île en île est une technique de piratage courante dans laquelle les pirates passent d'une entreprise à une autre via des identifiants de connexion volés. Les MSP et leurs clients PME sont tous deux des cibles potentielles de ces attaques.

Organisations de santé

Les hôpitaux, les bureaux de physiothérapie, les pédiatres, les chiropraticiens et autres cabinets de soins de santé sont des cibles faciles pour la cybercriminalité en raison de leurs pratiques de sécurité chaotiques et parfois laxistes.
Les données médicales et la recherche sont très précieuses pour l'acquéreur intéressé. Sur le Dark Web, les dossiers des patients à eux seuls peuvent se vendre jusqu'à 1 000 $ ou plus.[1]

Municipalités, infrastructures et services publics

Les villes peuvent également être victimes de cyberattaques. Non seulement la quantité massive de données stockées dans les systèmes urbains est attrayante, mais les pirates peuvent également lancer des attaques de ransomware perturbatrices, en fermant les infrastructures ou les services publics jusqu'à ce qu'ils soient payés. De nombreuses villes utilisent encore des anciens systèmes obsolètes qui sont vulnérables aux logiciels malveillants ou aux ransomwares.

Organismes gouvernementaux

Les gouvernements locaux et nationaux sont les principales cibles des cybercriminels, en particulier des terroristes d'état-nation, pour diverses raisons. Les petits gouvernements et les agences locales génèrent des tonnes d'informations sensibles, tandis que les grands gouvernements peuvent être victimes de perturbations à l'échelle nationale.

Institutions financières

Les banques, les coopératives de crédit et autres institutions financières sont depuis longtemps la cible des pirates informatiques en raison de la multitude de données et d'argent présents. En fait, en 2018, plus de 25 % de toutes les attaques de logiciels malveillants ciblaient des banques - plus que tout autre secteur.[2]
En outre, l'automatisation a permis aux cybercriminels d'exécuter des attaques avancées contre les institutions financières à grande échelle.

Célébrités, politiciens et grandes marques

Les hacktivistes, qui sont politiquement, économiquement ou socialement motivés, recherchent des célébrités, des politiciens et d'autres organisations de premier plan comme cibles. Ils peuvent même tenter d'embarrasser des personnalités publiques ou des entreprises en volant et en diffusant des données sensibles, exclusives ou classifiées pour perturber le public, ou pour un profit financier privé via le chantage.

Comment se protéger contre les pirates malveillants

La seule condition préalable pour devenir une cible est d'avoir quelque chose que les pirates veulent, ce qui met toutes les entreprises en danger. Heureusement, la sensibilisation aux menaces et une approche proactive de la sécurité peuvent contribuer grandement à assurer la sécurité de votre entreprise.

Pensez comme un pirate

La sensibilisation à la sécurité est un élément essentiel d'une cybersécurité efficace. En fait, les propres recherches de Webroot ont révélé que la formation sur la sensibilisation à la sécurité réduisait de 70 % les clics sur les liens de phishing lorsqu'elle est dispensée avec régularité. Comprendre les pratiques et les motivations des pirates peut vous aider à prévoir les menaces potentielles et à contrecarrer les attaques.

Verrouillez d'abord votre entreprise

Les bonnes couches de sécurité peuvent vous protéger contre les menaces de tous côtés. Découvrez les vidéos éducatives gratuites de Webroot, les podcasts et les guides de cybersécurité de notre **Centre de ressources sur les leçons de verrouillage** pour découvrir comment la cybersécurité en couches peut profiter à votre entreprise.

Tirez parti de la détection automatisée des menaces

Au fur et à mesure que les attaques modernes deviennent de plus en plus complexes et sont automatisées à grande échelle, votre entreprise deviendra plus ciblée. La meilleure façon de lutter contre les attaques ciblées est de corriger rapidement et automatiquement les menaces qui aboutissent. Détection et réponse automatisées (ADR) Les solutions améliorent la précision de la détection et la vitesse de réponse, qui sont essentielles contre les attaques.

Protégez vos clients

Vos clients peuvent être sous-équipés pour gérer une violation. Les MSP occupent une position unique pour offrir aux clients PME une formation complète et de haute qualité sur la sensibilisation à la sécurité, ainsi qu'une expertise en cybersécurité et une protection automatisée. Les PME qui cherchent à renforcer leur sécurité devraient également chercher à s'associer aux MSP et à d'autres fournisseurs de sécurité gérés pour sécuriser leurs propres réseaux et systèmes.

Alors que les moyens et les motivations des pirates sont multiples, pour les chapeaux noirs et autres intrus malveillants, c'est votre entreprise qui détient les clés du royaume. Il vous appartient de connaître leurs méthodes et de protéger votre entreprise et vos clients contre les menaces avancées.

« Une des plus grandes tendances de ces dernières années est la spécialisation des pirates criminels. »

Kelvin Murray
Chercheur principal sur les menaces, Webroot

Comprendre pourquoi les pirates informatiques en veulent à votre entreprise et quelles méthodes ils utilisent pour s'introduire dans vos systèmes peut vous aider à contrecarrer les attaques avant qu'elles ne se produisent.

[1] CBS News. « Hackers are stealing millions of medical records – and selling them on the dark web. » (février 2019)
[2] Forrester. « The Total Economic Impact of the IntSights External Threat Protection Suite. » (octobre 2019)
[3] Webroot. « Webroot 2019 Threat Report. » (février 2019)

Conclusion

Bien que les pirates informatiques soient diversifiés et que le piratage en tant que profession soit plus complexe qu'on ne le pense, les cibles des cyberattaques restent cohérentes. La réalité est que chaque entreprise constitue une cible potentielle de piratage malveillant - y compris vous et vos clients ! Les cyberattaques contre les MSP et les PME sont en augmentation, ce qui oblige à se protéger contre tous les types de menaces. Verrouiller votre entreprise commence par une formation sur les pirates et leurs méthodes, mais cela ne s'arrête pas là. Protégez vos clients avec les solutions de cybersécurité les plus avancées qui peuvent aider à combler les failles de sécurité et à éliminer rapidement les menaces.

N'attendez pas pour protéger votre entreprise !

Ce que vous ne savez pas peut vous blesser. Les cyberattaques contre les MSP et les PME sont en augmentation. Démarrez un essai gratuit de Webroot et voyez par vous-même comment nos solutions peuvent vous aider à prévenir les menaces et à maximiser la croissance.

Contactez-nous pour en savoir plus – Webroot – Zone EMOA

E-mail : France-smbc@opentext.com

Téléphone : +33 (0)1 47 96 55 41

À propos de Webroot et de Carbonite

Les sociétés Carbonite, Webroot et OpenText exploitent le Cloud et l'intelligence artificielle pour fournir des solutions complètes de cyber-résilience aux entreprises, aux particuliers et aux fournisseurs de services gérés. La cyber-résilience signifie pouvoir rester opérationnel, même face aux cyberattaques et à la perte de données. C'est pourquoi nous avons uni nos forces pour fournir des solutions de protection des postes et des réseaux, de sensibilisation à la sécurité et de sauvegarde des données et de reprise après sinistre, ainsi que des services de renseignement sur les menaces utilisés par les principaux fournisseurs de technologies du marché dans le monde entier. Nous exploitons la puissance de l'apprentissage automatique pour protéger des millions d'entreprises et de particuliers, et sécuriser le monde connecté. Webroot et Carbonite sont implantés en Amérique du Nord, en Europe, en Australie et en Asie. Découvrez la cyber résilience sur carbonite.com et webroot.com.