COMMENT SURVIVRE À UN HOLD-UP

Un guide pratique et concret pour survivre à pratiquement toutes les menaces, des effractions de compte venues du dark web aux attaques de malwares.

Voici la dure réalité du monde numérique constamment connecté d'aujourd'hui : à l'instant où vous réalisez que votre banque pourrait être victime d'un hold-up, il est déjà trop tard. Les voleurs numériques d'aujourd'hui sont déjà loin quand vous prenez conscience de leur passage.

Voici notre guide de survie pour vous protéger avant que cela ne se produise.

Les braqueurs de banque d'aujourd'hui ne sont plus les mêmes qu'il y a 10 ans, tout comme vos clients, d'ailleurs. Cela fait longtemps que les voleurs, comme les clients, ne se déplacent plus jusqu'à votre agence. Si bien qu'il est quasiment impossible de tenir les malfaiteurs à distance de vos coffres. Quasiment.

Si vous voulez remporter la partie, vous devez en comprendre les joueurs. Si vous parvenez à penser comme les braqueurs modernes, vous saurez vous en protéger avant qu'ils n'arrivent et ne détruisent vos systèmes, vos finances et votre réputation. En bref, pour survivre à un hold-up au 21e siècle, vous devez penser comme un hacker.

La menace invisible

Les voleurs d'aujourd'hui sont plus discrets, plus fourbes. Imaginez que quelqu'un vous menace à 10 000 kilomètres de distance. Tout du moins, c'est ce que le voleur d'aujourd'hui essaie de vous faire croire avant d'usurper une adresse IP sur trois continents tout en installant des scripts de cryptominage un peu partout dans le monde. Les seules choses qui relient directement le voleur à votre banque sont des câbles et un mot de passe.

Bienvenue dans l'ère numérique, où les menaces les plus graves sont souvent invisibles et où l'argent n'est plus le seul mobile. Ces voleurs installent clandestinement des malwares qui exploitent des vulnérabilités critiques, puis dérobent des données financières, la propriété intellectuelle et autres actifs numériques en toute discrétion, tout en compromettant votre position de conformité et en détruisant votre marque et votre réputation.

Aujourd'hui, les attaques ciblées sophistiquées comme le détournement SWIFT de 2016 vous poussent à rehausser constamment le niveau de vos défenses. Au cours de ce cyberbraquage sans précédent, les malfaiteurs ont envoyé des messages frauduleux via le système SWIFT à la Réserve fédérale américaine à New York pour tenter de transférer près d'un milliard de dollars depuis un compte de la Banque du Bangladesh. Ils sont parvenus à détourner 81 millions de dollars de la Réserve fédérale américaine vers des comptes illégaux aux Philippines. La majeure partie de la somme n'a jamais été récupérée.

Aujourd'hui, ces vols représentent près de 43 % des cyberattaques.

Malgré tout le temps, l'argent et les efforts que vous avez investis dans des murs plus solides et des caméras plus performantes, les cybermenaces n'ont fait que s'accentuer. Une grande banque multinationale, par exemple, subit encore les conséquences d'une faille massive survenue lorsqu'une ancienne employée d'Amazon Web Services (AWS) est parvenue à voler le nombre record de 100 millions de comptes client et de demandes de carte de crédit grâce à un défaut dans la configuration du pare-feu d'une application web.

Et ce n'est que la partie visible de l'iceberg. D'innombrables autres banques et institutions de crédit sont frappées chaque jour par des milliers de failles créées par des cybercriminels. Ces attaques sont invisibles, destructrices et très rarement signalées, ou même détectées.

La question est donc : êtes-vous prêt à survivre à un hold-up

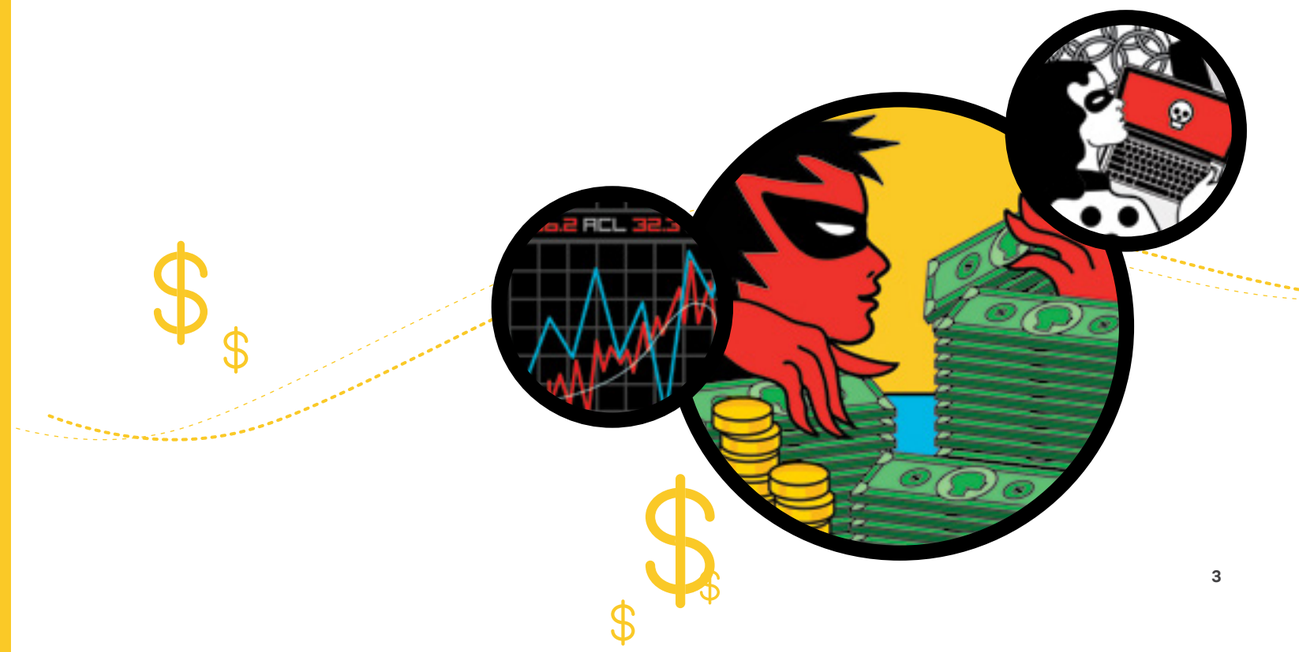
Sachez qui est votre ennemi et quelles sont ses tactiques

Voici quelques-uns des adversaires que vous rencontrerez presque certainement :

- Syndicats criminels organisés et dispersés
- Cyberespions et malfaiteurs agissant pour des États-nations
- Hacktivistes politiques et saboteurs
- Pirates amateurs ayant accès à des kits de malwares largement répandus
- Malfaiteurs motivés par l'argent et utilisant des méthodes sophistiquées reposant sur l'IA

Si les grandes organisations de cybercriminalité et les attaques médiatisées proviennent majoritairement de Chine, de Russie et du nord-est de l'Europe, les pirates sont issus de bien d'autres régions et brouillent de mieux en mieux les pistes.

Ce guide est conçu pour vous aider à survivre efficacement à 10 des plus grandes menaces, identifiées par les équipes de recherche et les experts industriels de Splunk. Mais avant de pouvoir survivre à une attaque, vous devez savoir qui sont vos adversaires, comment vous préparer et quoi faire pour réduire le risque d'être visé par des cybercriminels.



Attaques par hameçonnage

Anatomie d'une attaque par hameçonnage

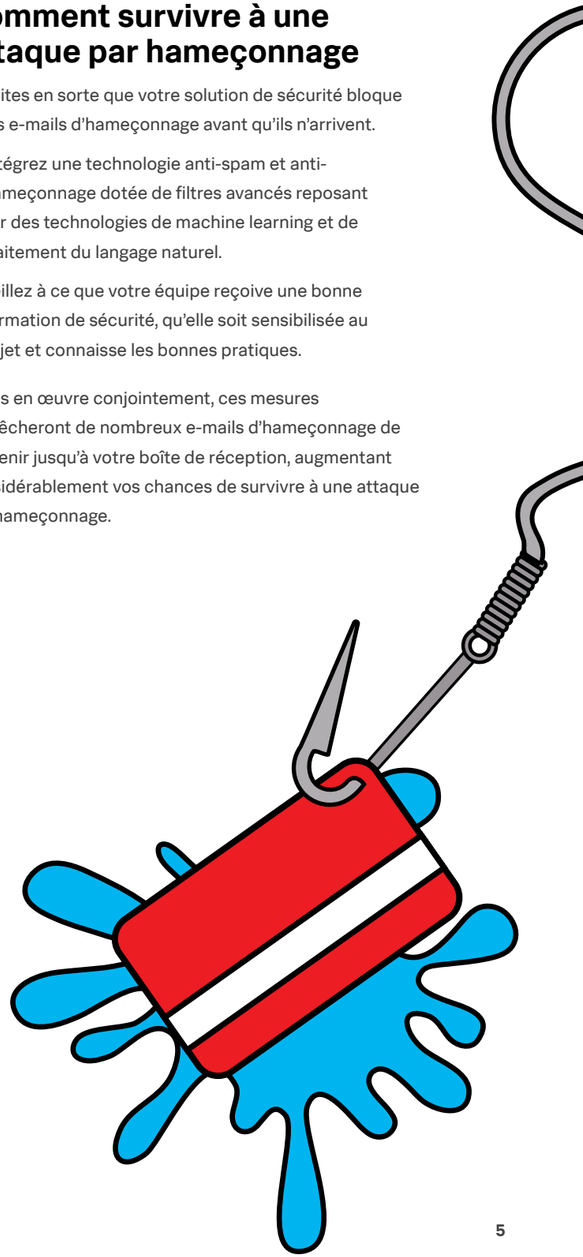
Une attaque par hameçonnage incite les clients ou les employés d'une banque à cliquer sur un lien malveillant qui les conduit généralement à un faux site pour qu'ils saisissent des informations personnellement identifiables telles qu'un numéro de compte bancaire, des informations de carte de crédit ou des mots de passe. L'hameçonnage parvient à la victime par e-mail, messagerie instantanée ou autre moyen de communication.

- **Qui en sont les auteurs :** En raison de la simplicité et de la disponibilité des kits d'hameçonnage, même des pirates possédant des compétences techniques limitées sont en mesure de lancer des campagnes d'hameçonnage. Les auteurs de ces campagnes sont variés, allant du pirate isolé à l'organisation cybercriminelle.
- **D'où viennent-ils :** Il y a quelques dizaines d'années seulement, une grande partie des attaques par hameçonnage provenait du Nigeria ; elles étaient surnommées « arnaques 419 » en référence au paragraphe du code pénal nigérien qui les condamne. Aujourd'hui, les attaques par hameçonnage proviennent du monde entier et en particulier des « BRIC » (Brésil, Russie, Inde et Chine) selon l'Institut InfoSec.
- **Leur objectif :** Faites preuve de vigilance, ces faux sites sont souvent très convaincants, mais les pirates se tiennent prêts à récolter toutes les informations que vous y saisirez. Ils peuvent également lancer des malwares visant à dérober des fonds sur votre compte, des informations personnellement identifiables ou d'autres ressources critiques.
- **Méthode d'exécution :** Vous êtes généralement leurré par un e-mail dont l'auteur usurpe l'identité d'une personne que vous connaissez (un collègue ou un supérieur, par exemple) et qui vous demande d'ouvrir une pièce jointe malveillante ou de cliquer sur un lien conduisant à une page quasiment identique au site légitime qu'elle imite.

Comment survivre à une attaque par hameçonnage

- Faites en sorte que votre solution de sécurité bloque les e-mails d'hameçonnage avant qu'ils n'arrivent.
- Intégrez une technologie anti-spam et anti-hameçonnage dotée de filtres avancés reposant sur des technologies de machine learning et de traitement du langage naturel.
- Veillez à ce que votre équipe reçoive une bonne formation de sécurité, qu'elle soit sensibilisée au sujet et connaisse les bonnes pratiques.

Mises en œuvre conjointement, ces mesures empêcheront de nombreux e-mails d'hameçonnage de parvenir jusqu'à votre boîte de réception, augmentant considérablement vos chances de survivre à une attaque par hameçonnage.



Fraude à la facture

Anatomie d'une fraude à la facture

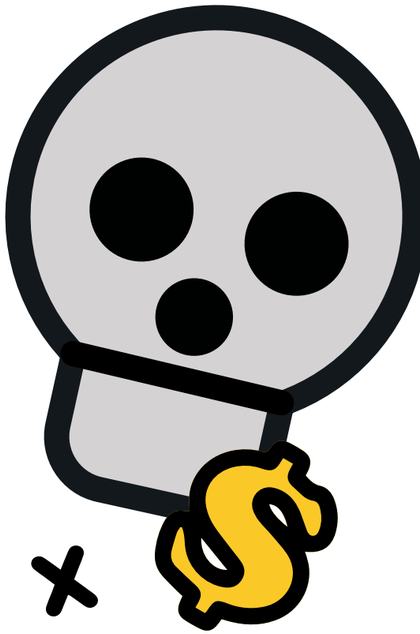
La fraude à la facture ou fraude au paiement, désigne tout type de transaction falsifiée ou illégale au cours de laquelle le cybercriminel détourne des fonds de vos clients. Et ces stratagèmes fonctionnent : selon les données les plus récentes de la FTC, les particuliers ont signalé environ 1,48 milliards de dollars de pertes dues à la fraude en 2018, soit une augmentation de 406 millions de dollars par rapport à 2017.

- **Qui en sont les auteurs :** Des criminels organisés possédant les ressources, la bande passante et la technologie nécessaires pour créer des factures frauduleuses imitant parfaitement les vraies. Comme l'hameçonnage, la fraude à la facture vise généralement une population d'individus aussi nombreuse qu'aléatoire.
- **D'où viennent-ils :** Comme dans le cas de l'hameçonnage, les organisations derrière ce type de fraude viennent du monde entier, y compris des États-Unis.
- **Leur objectif :** Tromper un grand nombre d'utilisateurs en les incitant à payer de façon répétée des sommes minimes ou raisonnables afin qu'ils ne s'aperçoivent pas de l'escroquerie.
- **Méthode d'exécution :** Dans ce scénario, les criminels envoient des factures frauduleuses à l'apparence authentique demandant à vos clients de transférer des fonds depuis leur compte. Sachant que beaucoup de vos clients utilisent régulièrement des services numériques payants, les pirates s'appuient sur le fait que leurs victimes peuvent avoir des raisons de penser que cette fausse facture correspond bien à des services utilisés. Vos clients procèdent alors à un transfert de fonds ou un paiement par carte de crédit pour régler la « facture ».

Comment survivre à la fraude à la facture

- Commencez par automatiser le traitement des factures et le workflow de paiement.
- Mettez en œuvre une solution de sécurité capable de détecter et signaler les aberrations dans les factures de vos clients, afin d'être alerté en cas d'activité suspecte.

Gagner en visibilité sur vos workflows de traitement des factures en repérant les différences mineures vous donnera une longueur d'avance quand il s'agira de survivre à la fraude à la facture.



Attaques de harponnage

Anatomie d'une attaque de harponnage

Type particulier d'hameçonnage, le harponnage consiste à envoyer un e-mail spécifique et personnalisé à un destinataire soigneusement sélectionné pour l'inciter, ou inciter ses employés, à fournir des données financières ou propriétaires, ou bien à donner l'accès à son réseau.

- **Qui en sont les auteurs :** Des individus comme des organisations. Toutefois, de nombreuses tentatives de harponnage sont le fruit d'organisations criminelles appuyées par un gouvernement et disposant des ressources nécessaires pour faire des recherches sur leurs cibles et contourner des filtres de sécurité robustes. Le groupe russe de cyberespionnage Fancy Bear, par exemple, a utilisé des techniques de harponnage pour cibler des comptes d'e-mail en lien avec la campagne présidentielle d'Hillary Clinton en 2016, John Podesta et Colin Powell, ancien secrétaire d'État américain. L'attaque du groupe a été détaillée dans la version expurgée du « Rapport d'enquête sur l'ingérence russe dans l'élection présidentielle de 2016 » de Robert Mueller, daté de 2019.
- **D'où viennent-ils :** Si les auteurs viennent du monde entier, les attaques complexes de harponnage de ces dernières années étaient basées en Europe de l'Est. L'année dernière, les agents fédéraux américains ont arrêté trois Ukrainiens impliqués dans l'organisation cybercriminelle FIN7, liée au piratage de plus de 3 600 entreprises sur le territoire américain et au vol de plus de 15 millions de cartes de crédit et de débit.
- **Leur objectif :** Le harponnage vise les personnes qui ont accès à des informations sensibles ou constituent un maillon faible dans le réseau. Si vous êtes une cible de grande valeur, comme un membre de la direction ou du conseil d'administration de l'entreprise, vous êtes particulièrement vulnérable car vous avez accès à des systèmes critiques et à des informations propriétaires de la société.
- **Méthode d'exécution :** Les criminels font des recherches pour vous identifier et cerner votre position au sein de votre institution financière à l'aide de réseaux sociaux comme LinkedIn. Ils usurpent ensuite des adresses pour vous envoyer des messages parfaitement personnalisés, à l'aspect authentique, afin d'infiltrer votre infrastructure et vos systèmes. Une fois que les pirates ont accès à votre environnement, ils tentent de mettre en œuvre des plans plus sophistiqués encore.

Comment survivre à une attaque de harponnage

- Commencez par déployer des filtres robustes contre le spam et l'hameçonnage.
- Mettez en œuvre des technologies de machine learning et de traitement du langage naturel pour détecter les messages de harponnage les plus sophistiqués et personnalisés.

En raison de leur nature extrêmement personnelle et ciblée, ces attaques sont souvent plus difficiles à détecter et à bloquer. Mais les attaques de harponnage présentent des vulnérabilités, et tout comme les attaques par hameçonnage classiques, il s'agit de savoir ce que l'on cherche et d'être préparé.

Fraude à la facture en entreprise

Anatomie de la fraude à la facture en entreprise

Les tentatives de fraude à la facture en entreprise cherchent à vous faire payer une facture falsifiée, mais convaincante, adressée à votre institution financière. En réalité, les fonds versés vont à des fraudeurs qui imitent vos fournisseurs.

- **Qui en sont les auteurs :** Si une partie de la fraude à la facture en entreprise est le fait d'escrocs isolés, la majorité provient d'organisations disposant des ressources requises pour faire des recherches sur votre banque et créer une expérience de facturation crédible.
- **D'où viennent-ils :** On rencontre des organisations de fraude utilisant des fausses factures dans le monde entier. La fraude à la facture a coûté 93 millions de livres (122,8 millions de dollars américains) aux entreprises britanniques l'année dernière, avec 3 280 cas d'escroquerie employant des factures ou des mandats, selon un rapport récent. Il existe également des milliers de cercles de fraude répartis sur tout le territoire américain : la Floride, le Michigan et le Nevada affichaient en 2018 les nombres les plus élevés de signalement de fraudes selon la Federal Trade Commission américaine.
- **Leur objectif :** Le mobile est simple : c'est l'argent. Ces pirates cherchent généralement à facturer un montant raisonnable afin d'éviter d'éveiller les soupçons, 1 500 dollars par exemple. Mais en répétant ces escroqueries des centaines ou des milliers de fois, les chiffres grossissent rapidement.
- **Méthode d'exécution :** Dans ce scénario, vous recevez des fausses factures qui tentent de vous dérober de l'argent en espérant que vous ne fassiez pas attention à vos processus de règlement. Les pirates choisissent leur cible en fonction de la taille de votre entreprise, de son emplacement et de vos fournisseurs. Armés de ces informations, ils créent des contrefaçons de factures à l'aspect parfaitement légitime. En espérant que votre service des règlements soit en retard, ils envoient des fausses factures assorties d'une mention telle que « Somme due depuis 90 jours, règlement immédiat ! »

Comment survivre à la fraude à la facture en entreprise

- Gardez le contrôle sur vos processus de règlement en instaurant une visibilité complète.
- Trouvez des solutions vous donnant des renseignements immédiats sur toutes les factures délictueuses et autres failles de processus.
- Mettez en place des technologies qui feront la lumière sur toute activité frauduleuse ou suspecte.

Les fraudeurs parviennent à leurs fins en comptant sur votre manque de visibilité sur votre workflow de règlement, ou simplement sur votre inattention. Ne les laissez pas faire et vous survivrez à la fraude à la facture en entreprise.

Attaques au point d’eau

Anatomie d’une attaque au point d’eau

Dans l’attaque au point d’eau, vos adversaires ciblent les sites web que vos employés et vous visitez fréquemment (d’où son nom) et les infectent avec des malwares conçus pour infiltrer votre réseau et voler des données ou des actifs financiers. Plus spécifiquement, les cybercriminels utilisent souvent la technique de l’attaque zero-day.

- **Qui en sont les auteurs :** Il s’agit souvent d’organisations structurées, bénéficiant parfois du soutien d’un gouvernement, possédant les ressources et les capacités nécessaires pour faire des recherches minutieuses sur votre institution et savoir quels sites vous utilisez.
- **D’où viennent-ils :** S’ils peuvent venir du monde entier, la majorité des cybercriminels derrière ces attaques sont basés dans des régions où les organisations menaçantes se multiplient, comme la Russie et la Chine. 2014 nous en donne un célèbre exemple : un groupe de pirates basé en Chine a exploité deux vulnérabilités zero-day pour injecter du code malveillant sur le site de Forbes, infectant tous les visiteurs de Forbes.com.
- **Leur objectif :** Le but est d’infecter votre système informatique avec un exploit zero-day pour obtenir l’accès à votre réseau afin d’en tirer un gain financier ou de voler des informations propriétaires.
- **Méthode d’exécution :** Dans un premier temps, les adversaires vont déterminer quels sites web vous visitez fréquemment, puis rechercher des faiblesses à exploiter. En tirant parti de ces vulnérabilités, les pirates compromettent les sites web en question puis attendent, sachant que votre prochaine visite n’est qu’une question de temps. Le site web va ensuite infecter votre réseau et leur permettre d’y accéder, avant de se déplacer latéralement vers d’autres systèmes.

Comment survivre à une attaque au point d’eau

- Donnez-vous les moyens d’inspecter proactivement les sites populaires à la recherche de malwares, puis de détecter et bloquer les sites web compromis.
- Mettez régulièrement à jour la sécurité de votre site web, surveillez les tentatives d’infiltration et inspectez votre site pour détecter les logiciels illicites qui y seraient installés.
- Configurez vos navigateurs pour qu’ils émettent automatiquement des alertes en cas de malware.

Les attaques au point d’eau sont particulièrement fourbes car elles peuvent exploiter n’importe quelle vulnérabilité d'un site populaire pour infecter les utilisateurs. Toutefois, en surveillant régulièrement vos systèmes de sécurité et en les tenant à jour, vous ferez déjà beaucoup pour vous prémunir contre les attaques au point d’eau.

Attaque par cryptojacking

Anatomie d'une attaque par cryptojacking

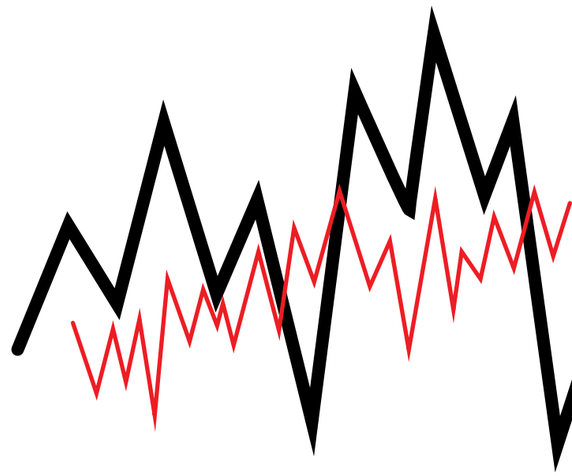
Le cryptojacking est une méthode d'attaque par laquelle un pirate cible et détourne vos systèmes informatiques à l'aide d'un malware qui se cache dans vos machines puis exploite leur puissance de calcul pour miner des cryptomonnaies comme le Bitcoin ou l'Ethereum… à vos frais.

- **Qui en sont les auteurs :** De nos jours, le cryptojacking ne nécessite pas de compétences techniques importantes. Des kits de cryptojacking sont disponibles sur le dark web pour une trentaine de dollars. C'est un point d'accès facile pour les pirates qui cherchent à s'enrichir rapidement, car cette méthode permet de générer beaucoup d'argent avec des risques relativement faibles. Lors d'une attaque, une banque européenne a observé des schémas de trafic inhabituels sur ses serveurs, des processus nocturnes plus lents que d'habitude et l'arrivée en ligne de nouveaux serveurs sans explication : tout cela était le fait d'un employé qui avait installé un système de cryptominage.
- **D'où viennent-ils :** Du monde entier.
- **Leur objectif :** Créer de la cryptomonnaie à l'aide de vos ressources informatiques.
- **Méthode d'exécution :** Pour mettre en œuvre leurs attaques par cryptojacking, les pirates procèdent notamment en envoyant un lien malveillant dans un e-mail d'hameçonnage, vous incitant à télécharger le code de cryptominage directement sur votre ordinateur. Une autre méthode consiste à intégrer du code JavaScript dans une page web que vous visitez (attaque de type « drive-by »). Lorsque vous vous rendez sur la page, le code malveillant qui doit miner la cryptomonnaie est automatiquement téléchargé sur votre machine. Le code de cryptominage s'exécute silencieusement à l'arrière-plan sans que vous n'en ayez connaissance, et le ralentissement d'une machine peut être le seul signe du problème.

Comment survivre à une attaque par cryptojacking

- Commencez par vérifier que vous pouvez superviser l'intégralité de votre réseau pour détecter les activités malveillantes.
- Vous devez pouvoir distinguer les activités malveillantes des autres types de communications.

À terme, cette visibilité et cet éclairage contribueront à tenir les pirates pratiquant le cryptominage à distance de vos réseaux, ou au moins à les empêcher de faire trop de dégâts, ce qui vous permettra de survivre à une attaque par cryptojacking.



Vol d’identité

Anatomie du vol d’identité

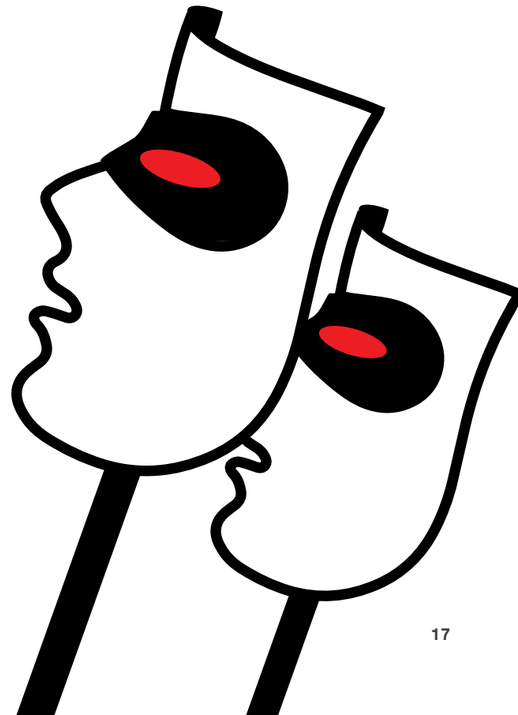
Le vol d’identité consiste à dérober votre identité afin d’obtenir l’accès à tous vos comptes ainsi qu’à leurs privilèges.

- **Qui en sont les auteurs :** Les pirates qui visent votre institution financière sont généralement de grandes organisations structurées et spécialisées, qui ont les moyens d’effectuer des recherches sur des comptes à forte valeur et de contourner les défenses de sécurité standards.
- **D’où viennent-ils :** Des organisations cybercriminelles sont basées dans le monde entier, mais on observe des points chauds dans des pays comme la Russie.
- **Leur objectif :** Les cybercriminels veulent accéder à vos comptes. Une fois vos identifiants volés, ils peuvent réinitialiser vos mots de passe, vous interdire l’accès, accéder à vos données sensibles et à d’autres ordinateurs du réseau, ou oblitérer intégralement vos informations critiques. De plus, ils peuvent obtenir un accès distant aux systèmes en utilisant des mots de passe légitimes pour se connecter à des services cloud grand public utilisés pour des opérations et des communications commerciales.
- **Méthode d’exécution :** Pour vous inciter, vos employés et vous-même, à remettre vos identifiants à votre insu, les pirates recourent souvent à des techniques d’hameçonnage. Ils peuvent toutefois les obtenir par d’autres moyens, comme la force brute ou en achetant des informations de compte sur le dark web, ce qui leur donne ainsi la possibilité d’effectuer facilement des transferts frauduleux sur les comptes volés.

Comment survivre au vol d’identité

- Commencez par un système robuste d’authentification capable de détecter les activités suspectes d’hameçonnage.
- Proposez des formations régulières sur la solidité des mots de passe et les bonnes pratiques de sécurité.

Si les voleurs d’identité disposent de multiples méthodes pour obtenir vos informations personnelles, la mise en œuvre des bonnes pratiques fera pencher la balance en votre faveur.



Injection d'identifiants

Anatomie de l'injection d'identifiants

Dans le cas de l'injection d'identifiants, les cybercriminels utilisent des identifiants volés (souvent des noms d'utilisateur et des mots de passe récoltés à la suite d'une fuite de données) pour accéder à des comptes supplémentaires en automatisant des milliers, voire des millions de demandes de connexion ciblant votre application web.

- **Qui en sont les auteurs :** Des pirates isolés ou organisés ayant accès à des outils dédiés de vérification de compte et à de nombreux proxys pour éviter que leurs adresses IP ne soient mises sur liste noire. Les malfaiteurs moins doués finissent parfois par se trahir en tentant d'infiltrer un grand nombre de comptes à l'aide de robots, produisant involontairement un scénario de déni de service distribué (DDoS).
- **D'où viennent-ils :** Les proxys dissimulent la localisation des pirates utilisant la méthode de l'injection d'identifiants. On les rencontre pourtant dans le monde entier, en particulier dans les points chauds de la cybercriminalité.
- **Leur objectif :** Ils cherchent un moyen facile d'accéder à vos comptes sensibles, tout simplement en s'y connectant. Et cela fonctionne parce qu'ils comptent sur le fait que vos collègues et vous utilisiez les mêmes identifiants et mots de passe pour accéder à de multiples services. En cas de succès, un identifiant peut déverrouiller des comptes hébergeant des informations financières et propriétaires, et c'est ainsi qu'ils obtiennent les clés du royaume.
- **Méthode d'exécution :** Les pirates ont seulement besoin d'avoir accès à des identifiants de connexion, à un outil automatisé et à des proxys pour mettre en œuvre une attaque par injection d'identifiants. Ils récupèrent une grande quantité de noms d'utilisateur et de mots de passe glanés lors de failles majeures puis « injectent » ces identifiants à l'aide d'outils automatisés dans les interfaces de connexion d'autres sites.

Comment survivre à l'injection d'identifiants

- Commencez par activer l'authentification multifacteurs sur les actifs critiques de votre entreprise.
- Vérifiez que vous avez des solutions de protection par mot de passe.
- Proposez des formations régulières sur la robustesse des mots de passe et les bonnes pratiques.

L'injection d'identifiants n'est qu'une question de chiffre pour les cybercriminels : jouez la carte de la sécurité en modifiant régulièrement les mots de passe et en mettant en place des solutions robustes d'authentification afin de les empêcher de prendre l'avantage et survivre à une attaque par injection d'identifiants.

Attaques internes

Anatomie d'une attaque interne

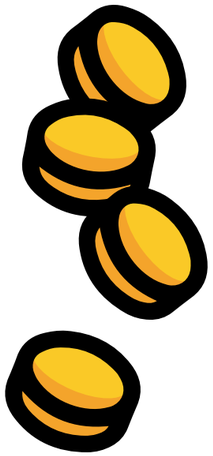
Une attaque interne, ou menace interne, est une agression malveillante menée par un membre de l'organisation ayant accès au système informatique, au réseau et aux ressources de votre banque.

- **Qui en sont les auteurs :** Des employés de votre entreprise ayant de mauvaises intentions, ou des cyberespions se faisant passer pour des sous-traitants, des tiers ou des télétravailleurs. Ils peuvent aussi bien travailler pour leur propre compte que pour celui d'un gouvernement, d'une organisation criminelle ou d'une entreprise concurrente.
- **D'où viennent-ils :** Les attaques internes proviennent de votre organisation. Même s'il s'agit de prestataires indépendants ou de sous-traitants situés ailleurs dans le monde, ces malfaiteurs disposent d'un certain niveau d'accès légitime à vos systèmes et vos données.
- **Leur objectif :** Les auteurs d'attaques internes cherchent souvent à obtenir des informations et des ressources confidentielles, propriétaires ou sensibles, que ce soit pour un bénéfice personnel ou pour fournir des renseignements à un concurrent. Ils peuvent également tenter de saboter votre entreprise en perturbant les systèmes, causant des pertes de productivité, de rentabilité et de réputation.
- **Méthode d'exécution :** Ces initiés malveillants ont un atout de poids : ils ont déjà un accès autorisé au réseau, aux informations et aux actifs de votre institution. Comme ils disposent souvent de comptes ayant accès aux systèmes ou aux données critiques, ils peuvent facilement les localiser, contourner les contrôles de sécurité et les exfiltrer de la société.

Comment survivre à une attaque interne

- Mettez en œuvre des solutions donnant une visibilité sur toute l'activité du réseau.
- Supervisez les accès des utilisateurs.
- Contrôlez et actualisez régulièrement les autorisations, en particulier celles qui concernent les informations sensibles et les actifs critiques.

Comme les malfaiteurs de cette catégorie opèrent dans l'ombre, vous devez faire la lumière sur leurs activités néfastes pour survivre à une attaque interne.



Attaques par virement

Anatomie d'une attaque par virement

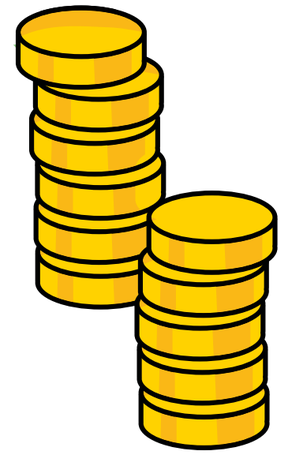
Les attaques par virement sont des stratagèmes sophistiqués visant à exécuter des paiements frauduleux d'un montant élevé via le réseau international de transfert d'argent SWIFT. Dépassant largement la fraude au transfert ordinaire, ces attaques touchent de préférence des banques implantées dans des marchés émergents, disposant d'infrastructures de cybersécurité et de contrôles opérationnels limités.

- **Qui en sont les auteurs :** On trouve historiquement des organisations cybercriminelles internationales ou nationales fortement structurées, comme APT 38 et le Lazarus Group, derrière les grandes attaques par virement. Ces groupes disposent de l'infrastructure et des ressources nécessaires pour mener ces assauts complexes et aux dimensions multiples. Une chose à savoir : dans des institutions armées de systèmes plus robustes, ces attaques par virement impliquant des sommes considérables nécessitent vraisemblablement la complicité d'acteurs internes pour obtenir l'accès aux systèmes.
- **D'où viennent-ils :** On ne sait pas clairement qui se cache derrière le Lazarus Group et APT 38, certains rapports indiquent qu'ils pourraient avoir des liens avec la Corée du Nord.
- **Leur objectif :** Ces organisations cybercriminelles poursuivent un seul objectif : l'argent. En très grande quantité.
- **Méthode d'exécution :** Les malfaiteurs emploient des malwares sophistiqués pour contourner vos systèmes de sécurité locaux. À partir de là, ils accèdent au réseau de messagerie SWIFT et envoient des messages frauduleux pour initier des transferts monétaires à partir des comptes de grandes banques.

Comment survivre à une attaque par virement

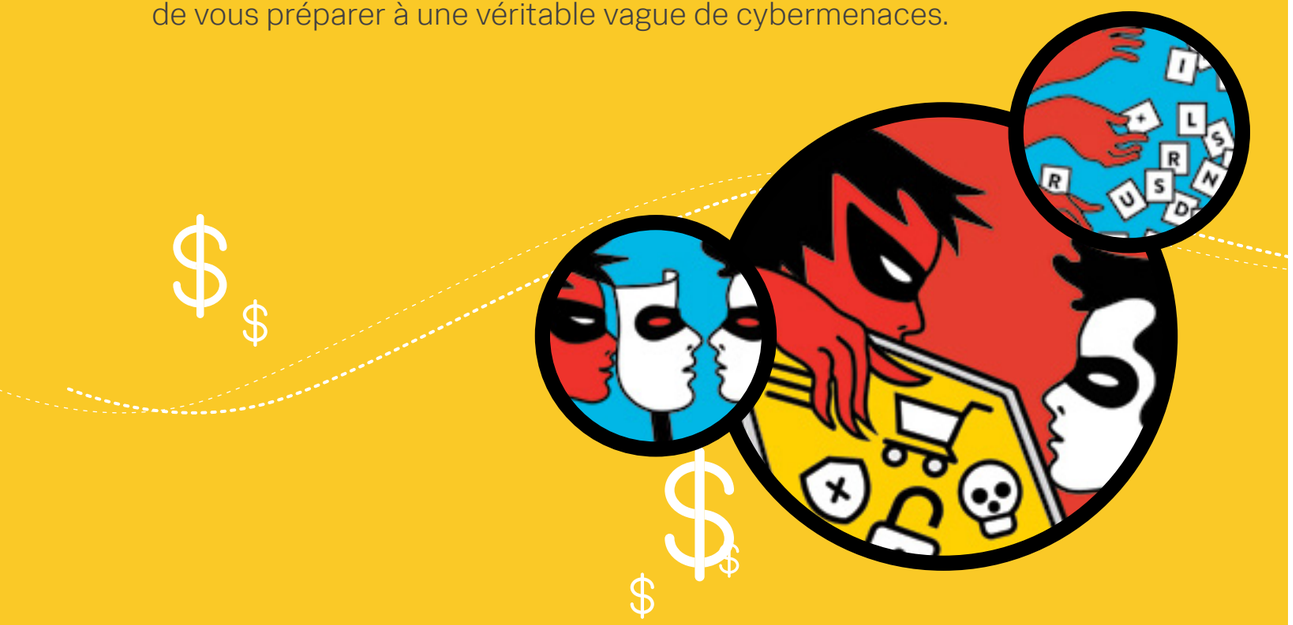
- Commencez par anticiper en cartographiant proactivement les voies d'accès diverses et nombreuses que les malfaiteurs peuvent emprunter pour accéder à vos systèmes.
- Déterminez les points prioritaires dans votre infrastructure de détection et de réponse de sécurité.
- Identifiez, au sein de votre réseau, les voies de déplacement latéral accessibles à un pirate ayant compromis un poste de travail ou un serveur.

Face à la sophistication technologique de cet adversaire, vous devrez faire des efforts pour garder une longueur d'avance. Anticipez les prochains mouvements des cybercriminels et placez des défenses de sécurité adaptées sur leur parcours : c'est comme cela que vous aurez le plus de chances d'éviter une attaque par virement pouvant faire apparaître votre institution financière à la une des journaux. Pour résumer, votre meilleure défense consiste à penser comme un voleur pour survivre à une attaque par virement.



Les trois clés pour survivre à un hold-up

Les braqueurs d'aujourd'hui ne portent ni masque, ni armes, et pourtant ils parviennent à leurs fins. Pour survivre, vous n'avez pas d'autre choix que de prendre des mesures et de vous préparer à une véritable vague de cybermenaces.



Voici les trois règles d'or pour survivre à ces menaces qui évoluent rapidement :

1. **Adoptez une approche basée sur les risques de la cybersécurité.** Poser de plus gros verrous sur les portes ne suffit pas à empêcher les voleurs d'entrer : pour protéger votre réseau tout en poursuivant vos activités, vous avez besoin de systèmes et d'opérations nouvelle génération, capables de détecter les cybermenaces avant qu'elles ne se transforment en hold-up. Cette approche vous permettra de surmonter :
   - **Les attaques systématiques :** Une technologie de sécurité robuste au niveau des points de terminaison, englobant protection des données, protection contre les menaces, sécurité de la couche réseau et analyses centralisées, va détecter les attaques les plus systématiques et fréquentes, puis prendre les mesures nécessaires pour empêcher les pirates de faire des ravages dans vos systèmes. La majeure partie de cette détection sera automatisée.
   - **Les attaques complexes :** Au moins, ces menaces à plusieurs phases vous donnent le temps de détecter une activité anormale ou un accès non autorisé (vous pourrez déceler les opérations de reconnaissance des intrus). Plusieurs étapes peuvent séparer la première intrusion de l'attaque finale des cybercriminels, ce qui vous laisse le temps d'agir avant qu'ils ne frappent.
2. **La formation est indispensable.** C'est là que vous pouvez vraiment commencer à penser comme un pirate et mettre vos connaissances à l'épreuve. Ce livre est un excellent point de départ. Vous pouvez également lancer une campagne interne générant de faux e-mails d'hameçonnage pour entraîner vos employés à détecter les stratagèmes sophistiqués et à les signaler aux administrateurs de sécurité. En plus d'être un bon exercice de sensibilisation, confier une part de la responsabilité de détection aux utilisateurs internes accélère efficacement la réponse aux attaques d'hameçonnage et de harponnage.
3. **Ne sous-estimez pas l'importance du partage des informations.** En cas d'attaque de grande envergure, vous devrez réagir rapidement pour éviter que l'incident ne se propage de façon exponentielle. C'est pour cela que le partage des informations sur les cybermenaces (CTI) est un outil essentiel pour combattre les attaques. Heureusement, vous avez accès à un riche écosystème de mécanismes et d'organismes de partage des informations. Le Centre d'analyse et de partage des informations des services financiers (FS-ISAC) est un consortium industriel dont le but est d'aider les institutions financières à anticiper, à réduire les risques et à répondre aux cybermenaces. Des homologues de confiance dans votre secteur d'activité et les forces de l'ordre sont également vos alliés dans cet effort de partage des CTI.

   Outre les alertes qui signalent les menaces immédiates et imminentes, le partage des tactiques, techniques et procédures (TTP) employées par les pirates va devenir un outil essentiel pour renforcer votre position de sécurité. En partageant des renseignements sur l'évolution des menaces et les organisations criminelles connues, vous agirez concrètement pour vous protéger de ces adversaires. Le partage des CTI constitue en outre un outil puissant pour avertir les institutions en cas de menace interne.

Aussi impressionnantes soient-elles, les solutions ponctuelles traditionnelles, qui prennent en charge des menaces spécifiques comme les malwares, ne suffisent plus à vous protéger dans l'ère nouvelle des cyberattaques. Aujourd'hui, les données machine détiennent les clés de la détection des menaces et de la protection des actifs. Pour garder vos actifs numériques en sécurité, vous devrez mettre en place un plan d'orchestration et d'automatisation. Il vous permettra de vous adapter plus rapidement et, muni d'armes de cybersécurité modernes, d'arrêter les braqueurs de banque d'aujourd'hui et de survivre à un hold-up.

Vous voulez en savoir plus pour apprendre à survivre à un hold-up ? Rendez-vous sur www.splunk.com/bankrobbery

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

2019-splunk-sec-how-to-survive-a-bank-robbery-104-eb