
Les 50 plus grandes
menaces de
cybersécurité
splunk>

Sommaire

Avant-propos

Aujourd'hui plus que jamais, la cybersécurité est essentielle pour notre avenir. En effet, c'est elle qui protège tout ce sur quoi nous comptons aujourd'hui. Pensez à la banque, à l'e-commerce et au développement de médicaments et de vaccins qui sauvent des vies, bien sûr, mais aussi à des choses plus simples, comme nos services de streaming vidéo préférés.

Cependant et à cause notamment des migrations massives vers le cloud et d'une transformation numérique généralisée, de nombreuses organisations n'ont toujours pas atteint leurs objectifs en termes d'opérations de sécurité, et ce en raison de plusieurs défis majeurs : un paysage de menaces en constante évolution, qui nous confronte à des malfaiteurs créatifs et bien financés ; la complexité croissante des environnements hybrides et multicloud ; des équipes de sécurité enlisées dans une liste interminable de tâches monotones et chronophages ; et des silos de données dus à la prolifération des outils au sein de nos organisations, qui entraînent des pertes d'efficacité et des angles morts.

Ces quatre défis se combinent pour former une seule réalité : la sécurité est un problème de données. C'est pourquoi il est primordial d'adopter une approche de la sécurité centrée sur les données, qui fournira les bonnes informations au bon moment et connectera les outils et les équipes, malgré le bruit et la complexité. Une solution basée sur l'analyse, s'appuyant sur une visibilité de bout en bout et alimentée par le machine learning (ML), est la clé du succès des organisations. Ces capacités avancées ne délivrent pas seulement une image complète de votre environnement, elles allègent également la part de l'intervention humaine et de diagnostics de base dans les opérations, pour aboutir à une défense de sécurité automatisée et renforcée.

Comment ? En rassemblant et en contextualisant toute une série d'ensembles de données très complexes, en traitant les menaces plus rapidement grâce à l'automatisation du tri, de l'investigation et de la réponse aux alertes, et en localisant les comportements anormaux grâce à des modèles et des algorithmes de ML prêts à l'emploi. Tout cela aide les organisations à améliorer leur cyberrésilience, qui est la capacité à anticiper et à s'adapter aux compromissions et aux attaques ciblant les ressources numériques. Elles pourront ainsi automatiser plus efficacement les opérations de sécurité et protéger leurs activités, tout en stimulant la croissance et l'innovation.

Chez Splunk, nous envisageons avec enthousiasme les possibilités offertes par les données pour un avenir meilleur *et plus sûr*. Mais pour y arriver, nous devons nous préparer. Nous devons savoir à quoi nous sommes confrontés et connaître les menaces qui planent. C'est pourquoi nous avons créé ce livre blanc sur les menaces de cybersécurité : nous voulons vous aider à identifier les différents types d'attaques, à atténuer les risques et à rendre votre entreprise encore plus forte.

Gary Steele
PDG de Splunk

Il faudra peut-être un certain temps avant que nous ne comprenions pleinement l'impact que les années de pandémie ont eu sur le paysage mondial de la sécurité de l'information (InfoSec). Il s'est passé bien plus de choses au cours de cette période que ce que de nombreux professionnels de la sécurité avaient pu voir dans toute leur carrière avant 2020. C'est une réalité : les défis auxquels nous sommes confrontés sont plus grands que jamais.

La « Grande démission », mais aussi le burn-out, malheureusement bien connu, viennent encore compliquer la tâche au moment où le monde de la sécurité a justement besoin d'attirer et de retenir les meilleurs talents. Ceux qui n'ont pas encore succombé sont submergés d'alertes. Ils consacrent trop de temps à des tâches manuelles répétitives qui usent leur moral. Ils n'ont pas suffisamment accès aux données indispensables pour comprendre les plus grandes menaces.

Mais il y a des raisons d'espérer. La plupart des plateformes d'opérations de sécurité n'ont pas réussi à aborder la sécurité en tant que problème de données avant tout. Et c'est là que réside l'opportunité pour les professionnels de la sécurité.

La capacité à mettre en place une réponse de cybersécurité résiliente est directement liée à la quantité et à la qualité des données collectées, analysées et exploitées dans la lutte pour réduire les risques de l'entreprise.

Conscientes que l'avenir est incertain, les organisations axent leurs investissements sur la résilience pour résister aux nouvelles menaces, rebondir et devenir plus fortes. Dans ce contexte, la résilience est synonyme de flexibilité. Les organisations résilientes disposent de solides fondations de données et de technologies, ce qui leur permet de faire face immédiatement aux perturbations qui surviennent.

Les équipes de sécurité résilientes fournissent des solutions de cybersécurité qui protègent tous les aspects de l'entreprise, stimulent l'innovation et donnent à l'organisation des moyens inédits. Elles relèvent les défis en mettant les données au cœur de tout ce qu'elles font. Et les résultats sont là. Les opérations de sécurité centrées sur les données réduisent le risque de violation, de vol d'adresse IP et de fraude jusqu'à 70 %.

On comprend alors pourquoi il est utile de savoir quelles menaces rechercher – et en quoi ce livre peut vous aider. Sur la base des travaux de l'équipe Splunk de recherche sur les menaces, nous présentons les 50 plus grandes menaces de cybersécurité, afin d'aider les professionnels de la sécurité à mieux nous protéger.

Appropriation de compte

Le piratage de compte est considéré comme l'un des moyens les plus nuisibles d'accéder au compte d'un utilisateur. L'adversaire se fait généralement passer pour un client, un utilisateur ou un employé authentique, pour finalement accéder aux comptes de la personne dont il usurpe l'identité.

Pendant la seule année 2022, 84 % des organisations ont été victimes de violations liées à l'identité, et 96 % d'entre elles ont déclaré que la violation aurait pu être évitée ou minimisée en mettant en œuvre une sécurité centrée sur l'identité.

Sans les technologies et politiques appropriées (comme le Zero Trust et la gestion des fournisseurs), il peut être extrêmement difficile d'identifier les comportements anormaux des utilisateurs. Ces attaques passent donc souvent inaperçues, car l'authentification fournie par un acteur malveillant peut ressembler à celle d'un utilisateur légitime, selon l'étendue du cadre de gestion des identités et des accès (IAM) en place (quand il y en a un).

Appropriation de compte

Ce que vous devez savoir :

Contrairement au simple vol de badge ou d'identifiants, le piratage du compte est plus subtil : il permet à l'adversaire de faire un grand usage des informations d'identification avant que l'activité suspecte ne soit signalée. Les banques, les grandes places de marché et les services financiers comme PayPal sont couramment la cible de ces attaques, et tout site web nécessitant une connexion peut l'être également.

Les organisations doivent abandonner l'approche axée sur la sécurité du réseau pour mieux protéger et contrôler les identités des utilisateurs. Jusqu'à récemment, certaines technologies n'offraient tout simplement pas les capacités d'intégration nécessaires, empêchant les organisations de centraliser la supervision de la sécurité globale de leurs ressources. Il existe maintenant de nombreuses technologies de contrôle d'accès, à commencer par l'authentification multifacteurs (MFA).

Pour éviter une authentification illégitime sur les applications cloud, aucun utilisateur ou appareil, qu'il soit interne ou externe à l'organisation, ne doit faire l'objet d'une confiance implicite, et l'accès à toutes les ressources doit être explicitement et continuellement authentifié et autorisé.

Déroulement de l'attaque :

Parmi les méthodes les plus courantes, citons les applications en un clic basées sur un proxy, les attaques de botnet par force brute, le phishing et les logiciels malveillants. Certains malfaiteurs n'hésitent pas à fouiller dans les poubelles pour trouver des informations personnelles dans le courrier, ou tout simplement à acheter des listes de « Fullz », un terme d'argot désignant des liasses complètes d'identifiants vendues sur le marché noir. Une fois le profil de la victime acheté ou construit, le voleur d'identité peut utiliser les informations pour déjouer un système d'authentification basé sur la connaissance.

Un adversaire peut facilement franchir le périmètre ou pénétrer le réseau lorsque le framework IAM est insuffisant ou faible, et lorsqu'une organisation s'appuie toujours sur la sécurité du réseau et des terminaux. Dans les deux cas, du fait du laxisme des contrôles d'accès et d'identité, l'attaquant peut facilement se connecter avec les identifiants volés sans être détecté, pour finalement se déplacer librement sur le réseau.

D'où vient l'attaque :

Une part considérable de nos transactions, financières et autres, s'effectue en ligne. Pour les cybercriminels, l'acquisition d'identifiants de compte et d'informations personnelles (numéros de sécurité sociale, adresses postales, numéros de téléphone, numéros de carte de crédit et autres informations financières) est une activité lucrative, qu'il s'agisse ensuite de vendre les informations acquises ou de les utiliser pour leur propre profit.

Avec la multiplication des attaques de phishing, le nombre croissant d'identités d'utilisateurs et l'adoption toujours plus rapide du cloud, ce type d'attaque peut provenir de n'importe où, y compris de fournisseurs tiers, d'employés, de télétravailleurs et de sous-traitants.

Menaces persistantes avancées

Lors d'une célèbre attaque, une menace persistante avancée chinoise (APT) a mené au piratage de 25 comptes Microsoft Exchange au sein de diverses agences américaines. L'attaque a permis au groupe APT de forger un accès à « plusieurs types d'applications Azure Active Directory, y compris toutes les applications prenant en charge l'authentification des comptes personnels, telles que SharePoint, Teams, OneDrive, les applications des clients utilisant la fonctionnalité de 'connexion avec Microsoft', et applications multi-utilisateurs dans certaines conditions, » selon les rapports.

Menaces persistantes avancées

Ce que vous devez savoir :

Une menace persistante avancée (APT) est une menace discrète et très sophistiquée présente sur un système informatique ou un réseau ; un utilisateur non autorisé parvient à s'introduire par effraction en échappant à toute détection, et à obtenir des informations pour des motifs commerciaux ou politiques. Généralement menées par des groupes criminels ou des États-voyous, ces campagnes ont pour objectif principal le gain financier ou l'espionnage politique. Si les APT restent associées à des acteurs étatiques désireux de s'approprier des secrets gouvernementaux ou industriels, des cybercriminels sans affiliation particulière utilisent également les APT pour voler des données ou de la propriété intellectuelle.

Déroulement de l'attaque :

Une APT s'appuie généralement sur des tactiques très avancées et la collecte d'une grande quantité d'informations, ou mise sur des méthodes moins sophistiquées pour s'implanter dans le système (logiciels malveillants et spear phishing, notamment). Diverses méthodologies permettent de compromettre la cible et de conserver un accès.

Le plan d'attaque le plus courant consiste à passer d'un seul ordinateur à un réseau entier en lisant une base de données d'authentification, en identifiant les comptes qui possèdent les autorisations appropriées, puis en les exploitant pour compromettre les actifs. Les acteurs APT installent aussi des portes dérobées (ou des chevaux de Troie) sur les ordinateurs compromis au sein de l'environnement exploité. Ils s'assurent ainsi de pouvoir revenir, même en cas de modification des identifiants.

D'où vient l'attaque :

La plupart des groupes APT sont affiliés au gouvernement d'États souverains, quand ils n'en sont pas directement les agents. Une APT peut aussi être le fruit d'un hacker professionnel travaillant à temps plein pour une administration. Ces organisations de piratage parrainées par l'État disposent généralement d'importantes ressources qui leur permettent de faire des recherches approfondies sur leur cible pour déterminer le meilleur point d'entrée.

Attaques d'Amazon Web Services (AWS)

Le nombre d'attaques créatives visant les environnements virtuels a explosé avec l'essor du cloud computing. Et en tant que fournisseur majeur de services cloud, Amazon Web Services connaît son lot de menaces.

Plusieurs vulnérabilités menacent la sécurité des fournisseurs de cloud. Une entreprise de marketing numérique, par exemple, a omis de protéger par mot de passe son bucket Amazon S3 lorsqu'elle a cessé ses activités. Cette erreur a provoqué la fuite des données de 306 000 personnes.

Elle a libéré 50 000 fichiers, soit 32 Go de noms, d'adresses, d'adresses e-mail, de numéros de téléphone et de mots de passe hachés, provenant de clients tels que Patrón Tequila.

Attaques d'Amazon Web Services (AWS)

Ce que vous devez savoir :

Le modèle de « responsabilité partagée » d'Amazon précise qu'AWS est responsable de l'environnement qui entoure la machine virtuelle, mais que le client est responsable de la sécurité à l'intérieur du conteneur S3.

Les menaces qui tirent parti des vulnérabilités créées par des erreurs de configuration et de déploiement sont devenues un problème majeur à l'heure où les entreprises adoptent les technologies cloud à grande vitesse, car l'organisation qui utilise AWS est responsable de la sécurisation de son environnement. Et le nombre de menaces ciblant les clients AWS est impressionnant.

Déroulement de l'attaque :

Une attaque contre une instance AWS peut se produire de plusieurs manières. Il est important de rester vigilants face à des activités qui se résument parfois à un comportement suspect au sein d'un environnement AWS. On supervisera notamment les accès à S3 provenant d'emplacements et d'utilisateurs inconnus.

Il est également important de contrôler qui a accès à l'infrastructure AWS d'une organisation. La détection des connexions suspectes fournit en effet un bon point de départ pour les investigations. Certains comportements abusifs permis par la compromission d'identifiants, par exemple, peuvent avoir des conséquences financières directes, car toutes les instances EC2 créées par l'attaquant seront facturées à l'entreprise cliente.

D'où vient l'attaque :

En raison de la diversité des services hébergés sur AWS et des nouveaux types de menaces cloud qui apparaissent quotidiennement, ces attaques peuvent pratiquement provenir de n'importe où et de n'importe qui.

Jeton d’accès aux applications

Un acteur malveillant actif et inconnu a utilisé différentes stratégies pour obtenir et exploiter des informations auprès de cibles clés. Une méthode consistait à abuser des jetons d’authentification ouverte (OAuth) ciblant les référentiels d’organisations de premier plan, dont l’infrastructure de production de Github npm et des applications intégrées aux produits cloud Heroku et Travis-CI.

Jeton d’accès aux applications

Ce que vous devez savoir :

Avec un jeton d’accès OAuth, un pirate informatique peut utiliser l’API REST accordée par l’utilisateur pour réaliser des opérations telles que la recherche d’e-mails et l’énumération de contacts. Dans le cas d’un service de messagerie basé sur le cloud, une fois qu’un jeton d’accès OAuth est accordé à une application malveillante, celle-ci peut potentiellement obtenir un accès à long terme aux fonctionnalités du compte d’utilisateur si elle reçoit un jeton « d’actualisation » permettant l’accès en arrière-plan.

Déroulement de l’attaque :

Les adversaires peuvent utiliser des jetons d’accès aux applications pour contourner le processus d’authentification et accéder à des comptes, des informations ou des services restreints sur des systèmes distants. Ces jetons sont généralement volés aux utilisateurs et utilisés à la place des identifiants de connexion.

D’où vient l’attaque :

Les jetons d’accès compromis peuvent être utilisés comme première étape pour compromettre d’autres services. Par exemple, si un jeton accorde l’accès à l’e-mail principal d’une victime, l’attaquant peut étendre son accès à tous les autres services auxquels la cible est abonnée en déclenchant des routines de mot de passe oublié. L’accès direct à l’API via un jeton annule l’efficacité d’un deuxième facteur d’authentification, et peut contourner des contre-mesures telles que la modification des mots de passe.

Fraude à la facture

Paypal est un service financier et un système de paiement en ligne qui permet à ses clients d'envoyer et de recevoir facilement de l'argent. Pourtant, les fonctionnalités qui rendent Paypal aussi rapide et efficace quand il s'agit de transférer des fonds sont *également* exploitées par des pirates pour s'enrichir. Les pirates et les escrocs utilisent le système pour voler des fonds à des consommateurs en employant des stratagèmes de fraude aux paiements ; certains parviennent à vider entièrement des comptes bancaires.

Fraude à la facture

Ce que vous devez savoir :

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 des clients. Et ces stratagèmes fonctionnent : selon des données récentes de la FTC, les particuliers ont signalé environ 8,8 milliards de dollars de pertes dues à la fraude en 2022, soit une augmentation de plus de 30 % par rapport à l'année précédente.

Déroulement de l'attaque :

Cette attaque trompe un grand nombre d'utilisateurs afin de leur faire payer des sommes minimes ou raisonnables afin qu'ils ne s'aperçoivent pas de l'escroquerie. Dans ce scénario, les criminels envoient des factures frauduleuses à l'apparence authentique demandant aux clients de transférer des fonds depuis leur compte.

Sachant que la plupart des 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. Les consommateurs procèdent alors à un transfert de fonds ou un paiement par carte de crédit pour régler la « facture ».

D'où vient l'attaque :

Les organisations derrière ce type de fraude viennent du monde entier, y compris des États-Unis. Elles sont souvent l'œuvre de malfaiteurs possédant les ressources, la bande passante et la technologie nécessaire 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.

Attaque par force brute

Les attaques par force brute peuvent cibler toutes sortes de services ; un exemple récent implique, par exemple, le protocole RDP (Windows Remote Desktop Protocol). Entre début 2020 et aujourd'hui, Microsoft a enregistré une augmentation significative des attaques par force brute ciblant le RDP, qui s'explique par le grand nombre de points de terminaison exposés. Les acteurs malveillants parviennent ainsi à exploiter des mots de passe faibles ou courants pour obtenir un accès non autorisé à un large éventail de systèmes.

Attaque par force brute

Ce que vous devez savoir :

Une attaque par force brute vise à obtenir des informations personnelles, en particulier des noms d'utilisateur et des mots de passe, en utilisant une approche par tâtonnements. C'est l'un des moyens les plus simples d'accéder à une application, à un serveur ou à un compte protégé par mot de passe : l'attaquant essaie simplement des combinaisons de noms d'utilisateur et de mots de passe jusqu'à ce qu'il finisse par entrer (*s'il y parvient*, car n'oublions pas qu'un mot de passe à six caractères offre des milliards de combinaisons potentielles).

Déroulement de l'attaque :

L'attaque par force brute la plus élémentaire est l'attaque par dictionnaire. L'adversaire essaie systématiquement tous les mots d'un dictionnaire ou d'une liste, jusqu'à ce qu'il obtienne un résultat. Il peut ajouter des symboles et des chiffres aux mots, ou utiliser des dictionnaires spéciaux contenant des mots de passe divulgués et/ou couramment utilisés. Et s'il n'a ni le temps ni la patience, il existe des outils automatisés qui peuvent rendre cette tâche beaucoup plus rapide et moins fastidieuse.

D'où vient l'attaque :

En raison de la simplicité de l'attaque par force brute, des cybercriminels qui n'ont que peu ou pas d'expérience technique peuvent essayer d'accéder au compte de quelqu'un. Les personnes qui mènent ces campagnes ont suffisamment de temps ou de puissance de calcul pour y arriver.

Compromission de l'adresse e-mail d'entreprise

La compromission du courrier électronique d'entreprise (BEC), similaire à la fraude aux factures professionnelles, a évolué au fil des années, notamment avec l'augmentation des appels vidéo depuis la pandémie de COVID-19. L'attaque est souvent menée par des malfaiteurs qui se font passer pour des contacts professionnels légitimes et envoient de fausses invitations à des réunions. Selon un rapport, la division IC3 du FBI a « reçu un nombre accru de plaintes de BEC dans lesquelles des plateformes de réunion virtuelle étaient utilisées pour demander aux victimes d'effectuer des transferts de fonds non autorisés vers des comptes frauduleux ».

Compromission de l'adressee-mail d'entreprise

Ce que vous devez savoir :

La compromission d'adresse e-mail d'entreprise consiste à tenter d'inciter les victimes à payer une facture frauduleuse (mais convaincante) adressée à leur organisation. En réalité, les fonds parviennent à des imposteurs qui ont pris l'apparence de fournisseurs. Dépassant largement la fraude ordinaire, ces attaques touchent de préférence des banques implantées dans des marchés émergents, disposant d'infrastructures de cybersécurité et de contrôles opérationnels limités, ou bien visent des cibles de premier plan au moyen de techniques de phishing sophistiquées et crédibles. Ces organisations cybercriminelles poursuivent un seul objectif : l'argent. En grande quantité.

Déroulement de l'attaque :

Les cybercriminels peuvent utiliser des logiciels malveillants sophistiqués pour contourner les systèmes de sécurité locaux. À partir de là, ils accèdent à un réseau de messagerie et envoient des messages frauduleux pour initier des transferts monétaires à partir des comptes de grandes banques. Autre approche : les acteurs malveillants peuvent mener des campagnes de spear phishing pour convaincre leurs victimes de transférer d'importantes sommes d'argent vers leurs comptes. Ils leur envoient de fausses factures dans l'espoir qu'elles ne respectent pas trop étroitement les processus de règlement des créances.

Les pirates choisissent des cibles en fonction de la taille de l'entreprise, de sa localisation et de ses fournisseurs utilisés, et ils créent de fausses factures qui semblent légitimes. En espérant que le service des règlements des créances de la victime soit en retard, ils envoient des fausses factures assorties d'une mention telle que « Somme due depuis 90 jours, règlement immédiat ! »

D'où vient l'attaque :

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 la banque de la victime et créer une expérience de facturation crédible. On rencontre des organisations de fraude utilisant des fausses factures dans le monde entier.

On trouve historiquement des organisations cybercriminelles internationales ou nationales fortement structurées, comme APT 38 et le Lazarus Group, derrière les grandes attaques par transfert. Ces groupes disposent de l'infrastructure et des ressources nécessaires pour mener des assauts complexes et aux multiples dimensions. On ne sait pas clairement qui se cache derrière ces groupes, mais certains rapports indiquent qu'ils pourraient avoir des liens avec la Corée du Nord. Mais des groupes de hackers chinois et nigérians se sont également révélés être à l'origine d'attaques élaborées utilisant le virement bancaire. Une mise en garde : dans des institutions armées de systèmes plus robustes, ces attaques par transfert impliquant des sommes considérables nécessitent généralement la complicité d'acteurs internes pour obtenir l'accès aux systèmes.

Cryptominage dans le cloud

Le cryptominage dans le cloud ne requiert pas grand-chose. Si vous voulez une preuve, regardez simplement du côté de Github. Le référentiel cloud de code logiciel a été victime d'une attaque de cryptominage : des acteurs malveillants ont mené une vaste opération de freejacking ciblant 30 comptes GitHub, 2 000 comptes Heroku et 900 comptes Buddy, mais aussi 130 images Docker Hub. Ils ont ainsi abusé d'un grand nombre de comptes gratuits avec un minimum d'effort humain.

Ce que vous devez savoir :

Le cryptominage est une activité intentionnellement difficile et consommatrice de ressources. Sa complexité a un objectif : garantir que le nombre de blocs extraits chaque jour reste stable. On comprend donc que des mineurs ambitieux, mais sans scrupules, cherchent à détourner la puissance de calcul des grandes entreprises pour l'exploiter – une pratique connue sous le nom de crypto-détournement.

Déroulement de l'attaque :

Le cryptominage attire de plus en plus l'attention des médias depuis que sa popularité a explosé à l'automne 2017. Les attaques, qui ciblaient au départ les vulnérabilités des navigateurs et des téléphones mobiles, visent aujourd'hui les services cloud d'entreprise comme Amazon Web Services, Google Cloud Platform (GCP) et Microsoft Azure.

Il est difficile de déterminer exactement à quel point cette pratique s'est répandue, car les pirates informatiques perfectionnent continuellement leur capacité à échapper à la détection. Ils utilisent notamment des points de terminaison non répertoriés, modèrent leur utilisation du processeur et masquent l'adresse IP du pool de minage derrière un réseau de diffusion de contenu (CDN) gratuit.

Lorsque les mineurs volent une instance cloud, créant souvent des centaines de nouvelles instances, les coûts peuvent devenir astronomiques pour le titulaire du compte. Il est donc essentiel de superviser les systèmes pour détecter les activités suspectes pouvant trahir une infiltration de réseau.

D'où vient l'attaque :

Comme les cryptomonnaies s'échangent dans le monde entier, les attaques peuvent provenir de n'importe où. Plutôt que de se concentrer sur l'origine des attaques, il est essentiel de superviser les instances de cloud computing pour rechercher les activités liées au crypto-détournement et au cryptominage : nouvelles instances cloud provenant de régions inconnues auparavant, lancement d'un nombre anormalement élevé d'instances par un même utilisateur ou création d'instances de calcul par des utilisateurs inconnus auparavant.

Attaque de commande et contrôle

Cobalt Strike est un outil commercial de test d'intrusion. Les professionnels de la cybersécurité l'utilisent pour simuler des comportements menaçants avancés et évaluer la posture de sécurité d'une organisation. Il propose différentes fonctionnalités et permet par exemple de mener des activités de reconnaissance, d'exploitation et de post-exploitation ; sa charge utile « Beacon » est l'un de ses grands atouts.

Ces dernières années, cette charge utile a été utilisée pour mener des opérations de commande et contrôle (C2) sur des hôtes compromis, et permettre ainsi des communications furtives, des mouvements latéraux et diverses techniques d'attaque en mémoire. Si Cobalt Strike est un outil légitime destiné aux opérations des équipes rouges et à la simulation de menaces, des acteurs malveillants sont parvenus à utiliser des versions crackées de ce logiciel dans des cyberattaques en profitant de ses puissantes fonctionnalités et de sa grande discrétion.

Attaque de commande et contrôle

Ce que vous devez savoir :

Une attaque de commande et contrôle se produit lorsqu'un pirate prend le contrôle d'un ordinateur afin d'envoyer des commandes ou des logiciels malveillants à d'autres systèmes du réseau. Dans certains cas, l'attaquant effectue des activités de reconnaissance en se déplaçant latéralement sur le réseau pour recueillir des données sensibles. Ce type d'attaques gagne constamment en popularité : le nombre de serveurs de commande et de contrôle (C2) a en effet augmenté de 30 % dans la seule année 2022.

Dans d'autres contextes, les pirates peuvent utiliser cette infrastructure pour lancer de véritables attaques. L'une des fonctions essentielles de cette infrastructure est d'établir des serveurs qui vont communiquer avec des implants sur les points de terminaison compromis. Ces attaques sont souvent appelées attaques C2 ou C&C.

Déroulement de l'attaque :

La plupart des pirates prennent pied dans un système au moyen d'e-mails d'hameçonnage puis installent des logiciels malveillants. Ils établissent ainsi un canal de commande et contrôle qui sert à transmettre des données entre le point de terminaison compromis et l'attaquant. Ces canaux relaient les commandes au point de terminaison compromis et renvoient le résultat de ces commandes à l'adversaire.

D'où vient l'attaque :

On a recensé d'importantes attaques de commande et contrôle en provenance de Russie, d'Iran et même des États-Unis. Ces attaquants peuvent venir de n'importe où, mais ils ne veulent pas que vous le sachiez.

La communication jouant un rôle clé dans ces attaques, les pirates utilisent des techniques conçues pour dissimuler la véritable nature de leurs échanges. Ils essaieront souvent de consigner leurs activités aussi longtemps que possible sans être détectés, en s'appuyant sur une variété de techniques pour communiquer tout en faisant profil bas.

Identifiants compromis

Group-IB, un leader mondial de la cybersécurité, a subi une violation massive de données en 2023. L'attaque coordonnée a compromis des dizaines de milliers de comptes avec des identifiants ChatGPT enregistrés. Sans surprise, ce robot conversationnel basé sur un grand modèle de langage a gagné en popularité auprès des organismes cybercriminels, en particulier pour obtenir un accès non autorisé à des comptes et exposer des informations sensibles, dans le cadre de campagnes de grande envergure ciblant les entreprises et leurs salariés.

Identifiants compromis

Ce que vous devez savoir :

La plupart des gens utilisent encore l'authentification à facteur unique pour s'identifier (ce qui fait froncer les sourcils à la plupart des professionnels de la cybersécurité). Certes, on commence à appliquer des exigences plus strictes en matière de mot de passe (nombre de caractères, combinaison de symboles et de chiffres et intervalles de renouvellement), mais les utilisateurs finaux continuent de réutiliser les mêmes identifiants sur différents comptes, plateformes et applications, sans les mettre à jour périodiquement.

Ces pratiques permettent aux adversaires d'accéder plus facilement au compte d'un utilisateur, et un certain nombre de violations actuelles sont dues à ces campagnes de collecte d'identifiants.

Déroulement de l'attaque :

Une fois découvert, un mot de passe, une clé ou un autre type d'identifiant peut être utilisé par un acteur malveillant pour obtenir un accès non autorisé à des informations et des ressources. La violation peut toucher un compte isolé comme une base de données entière.

En s'appuyant sur un compte de confiance au sein d'une organisation ciblée, un acteur malveillant peut opérer sans être détecté et exfiltrer des données sensibles sans déclencher de signal d'alarme. Les méthodes couramment employées pour collecter des identifiants sont les renifleurs de mots de passe, le phishing et les logiciels malveillants.

D'où vient l'attaque :

Les identifiants compromis représentent un vecteur d'attaque pour les acteurs malveillants qui veulent accéder à des ordinateurs, à des comptes protégés par mot de passe et à l'infrastructure réseau d'une organisation avec une relative facilité. Les auteurs sont souvent organisés et visent une organisation ou une personne spécifique. Et ils ne viennent pas toujours de l'extérieur : il peut s'agir de menaces internes ayant un certain niveau d'accès légitime aux systèmes et aux données de l'entreprise.

Déversement d'identifiants

Un nouveau ransomware nommé Trigona a récemment été identifié. Il cible Windows à l'aide de méthodes uniques et utilise spécifiquement l'outil Mimikatz pour réaliser diverses tâches en lien avec les identifiants et extraire des données sensibles de Windows : la mémoire Windows, le processus Local Security Authority Subsystem Service (LSASS) et le registre. Mimikatz extrait et sauvegarde les identifiants dans un fichier, compilant aussi bien des noms d'utilisateur et des mots de passe que des hachages et des tickets Kerberos.

Déversement d'identifiants

Ce que vous devez savoir :

Le déversement d'identifiants désigne simplement une attaque qui repose sur la collecte d'identifiants auprès d'un système ciblé. Même s'ils ne sont pas en texte brut – ils sont le plus souvent stockés sous forme de hash ou chiffrés, un adversaire peut toujours extraire les données et casser le chiffrement hors ligne sur ses propres systèmes. C'est pourquoi on parle de « déversement ».

Les pirates tentent souvent de voler les mots de passe de systèmes qu'ils ont déjà compromis. Le problème s'amplifie lorsque les utilisateurs répliquent le même mot de passe sur plusieurs comptes et plusieurs systèmes.

Déroulement de l'attaque :

Les informations d'identification obtenues de cette manière incluent généralement celles d'utilisateurs privilégiés, qui ont accès à des informations et à des opérations système plus sensibles. Les pirates ciblent souvent plusieurs sources pour extraire des identifiants : gestionnaire de comptes de sécurité (SAM), autorité de sécurité locale (LSA), NTDS des contrôleurs de domaine ou fichiers de préférence de stratégie de groupe (GPP).

Lorsque des malfaiteurs ont obtenu des identifiants valides, ils les utilisent pour se déplacer facilement sur un réseau ciblé, découvrir de nouveaux systèmes et identifier les actifs qui les intéressent.

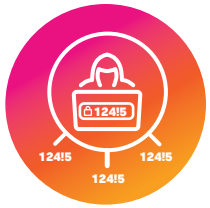
D'où vient l'attaque :

Le déversement d'identifiants peut provenir de n'importe où. Et parce que nous avons tous, un jour ou l'autre, recyclé des mots de passe, ces informations peuvent être vendues pour faciliter de futures attaques.

Attaque par réutilisation des identifiants

La violation Paypal de 2022 est un excellent exemple d'attaque par réutilisation des identifiants. Malheureusement pour le système de paiement en ligne, elle a compromis plus de 30 000 comptes en l'espace de quelques mois. Les acteurs malveillants ont eu accès à des données personnelles, notamment les « nom, adresse, numéro de sécurité sociale, numéro d'identification fiscale individuel et/ou date de naissance », selon un e-mail envoyé par Paypal à la suite de l'attaque.

Attaque par réutilisation des identifiants



Ce que vous devez savoir :

La réutilisation des identifiants est un problème omniprésent dans toute entreprise ou base d'utilisateurs. De nos jours, la plupart des utilisateurs ont des dizaines (voire des centaines) de comptes et doivent mémoriser d'innombrables mots de passe répondant à toutes sortes d'exigences strictes. Ils sont donc tentés de réutiliser le même mot de passe à plusieurs reprises, dans l'espoir de mieux mémoriser leurs identifiants sur tous leurs comptes. Sans surprise, cela peut entraîner des problèmes de sécurité majeurs lorsque les identifiants en question sont compromis.

Déroulement de l'attaque :

En théorie, l'attaque elle-même est simple, directe et étonnamment furtive (si l'authentification à deux facteurs n'est pas activée). Une fois les identifiants d'un utilisateur dérobés, le coupable peut essayer le même nom d'utilisateur et le même mot de passe sur d'autres sites web grand public ou bancaires jusqu'à ce qu'il obtienne une correspondance – d'où la précision « réutilisation » dans « attaque par réutilisation des identifiants ».

La première entrée est toutefois un peu plus compliquée. Pour obtenir des informations privilégiées, les attaquants commencent généralement par une tentative de phishing, en utilisant des e-mails et des sites web d'apparence légitime pour duper l'utilisateur et l'inciter à fournir ses identifiants.

D'où vient l'attaque :

Il peut s'agir d'une attaque ciblée : l'auteur connaît la victime et souhaite accéder à ses comptes pour des raisons personnelles, professionnelles ou financières. L'attaque peut également provenir d'un parfait inconnu qui a acheté les identifiants de l'utilisateur sur un réseau cybercriminel clandestin.

Cross-Site Scripting

Une vulnérabilité de script intersites (XSS) a été récemment découverte dans Zimbra, une suite logicielle collaborative. Cette faille permettait aux acteurs malveillants de voler les informations sensibles des utilisateurs en menant une attaque ciblée.

Les attaques XSS désignent un type d'injection dans lequel des scripts malveillants sont injectés dans des sites web autrement inoffensifs et fiables. Le concept est le même que l'injection SQL, qui consiste à saisir du code malveillant dans un formulaire pour accéder à la base de données du site. Mais dans le cas du XSS, le code malveillant est conçu pour s'exécuter dans le navigateur d'un autre utilisateur pour dérober ses cookies, lire les identifiants de session, modifier le contenu du site web ou le rediriger vers un site malveillant.

Cross-Site Scripting

Ce que vous devez savoir :

Les attaques XSS se produisent lorsqu'un attaquant utilise une application web pour envoyer un code malveillant, généralement sous la forme d'un script côté navigateur, à un autre utilisateur final. Les failles sur lesquelles reposent ces attaques sont répandues et se produisent partout où une application web génère une entrée d'un utilisateur sans la valider ni l'encoder.

Le navigateur de l'utilisateur final n'a aucun moyen de savoir que le script ne doit pas être approuvé, et l'exécute automatiquement. Parce qu'il pense que le script provient d'une source fiable, il le laisse accéder aux cookies, aux jetons de session et autres informations sensibles conservées par le navigateur. Ces scripts peuvent même réécrire le contenu de la page HTML.

Déroulement de l'attaque :

Il existe deux types d'attaques XSS : stockées et réfléchies. On parle d'attaque XSS stockée lorsqu'un script injecté est stocké sur le serveur à un emplacement fixe – un message de forum ou un commentaire, par exemple. Chaque utilisateur qui visite la page infectée sera affecté par l'attaque XSS. Dans une attaque XSS réfléchie, le script injecté est servi à un utilisateur en réponse à une requête, comme une page de résultats de recherche.

D'où vient l'attaque :

Bien que les attaques XSS ne soient plus aussi courantes qu'auparavant, principalement en raison des améliorations apportées aux navigateurs et à la technologie de sécurité, elles sont encore suffisamment répandues pour se classer parmi les dix principales menaces répertoriées par l'Open Web Application Security Project. La base de données Common Vulnerabilities and Exposures répertorie près de 14 000 vulnérabilités associées aux attaques XSS.

Attaque par crypto-détournement

En juillet 2023, des cyberpirates ont exploité les workloads cloud de près de 200 instances, extrayant secrètement des cryptomonnaies à l'insu des utilisateurs. Cette attaque par crypto-détournement a été lancée en chargeant discrètement des charges utiles sans fichier dans la mémoire du système cible, échappant ainsi à toute détection.

Attaque par crypto-détournement

Ce que vous devez savoir :

Le crypto-détournement est une méthode d'attaque par laquelle un pirate cible et détourne des systèmes informatiques à l'aide d'un malware qui se cache dans les machines puis exploite leur puissance de calcul pour miner des cryptomonnaies comme le Bitcoin ou l'Ethereum… aux frais de la victime. Le pirate cherche à créer des cryptomonnaies rentables à partir des ressources informatiques d'un tiers.

Déroulement de l'attaque :

Pour mettre en œuvre une attaque par crypto-détournement, les malfaiteurs procèdent notamment en envoyant un lien malveillant dans un email d'hameçonnage, incitant l'utilisateur à télécharger le code de cryptominage directement sur son ordinateur. Une autre méthode consiste à intégrer du code JavaScript dans une page web visitée par l'utilisateur (attaque de type « drive-by »). Lorsque vous vous rendez sur la page, le code malveillant qui doit miner la cryptomonnaie est automatiquement téléchargé sur la machine. Le code de cryptominage s'exécute silencieusement à l'arrière-plan et à l'insu de l'utilisateur, et le ralentissement d'une machine peut être le seul signe du problème.

D'où vient l'attaque :

Ces attaques viennent du monde entier car le crypto-détournement ne nécessite pas de compétences techniques importantes. On trouve en effet des kits prêts à l'emploi sur le dark web pour seulement 30 $; c'est un ticket d'entrée très peu coûteux pour les pirates qui veulent gagner rapidement de l'argent en courant relativement peu de risques.

Amplification DNS

En février 2022, des malfaiteurs ont lancé des attaques massives et amplifiées par déni de service distribué (DDoS) par l'intermédiaire de Mitel, une entreprise mondiale de communications d'entreprise. L'attaque a frappé des institutions financières, des FAI haut débit, des sociétés de logistique et de jeux et bien d'autres organisations encore. Capables de soutenir des attaques DDoS pendant 14 heures, avec un facteur d'amplification record de près de 4,3 milliards contre un, des campagnes de ce type peuvent couper les communications vocales et d'autres services à l'échelle d'organisations entières, avec un seul paquet réseau malveillant.

Amplification DNS

Ce que vous devez savoir :

Même si l'amplification DNS, qui est un type d'attaque DDoS, existe depuis longtemps, les techniques d'exploitation ne cessent d'évoluer. L'attaque s'apparente au détournement DNS dans la mesure où elle exploite l'annuaire Internet en altérant sa configuration. Mais la méthode des attaques est légèrement différente.

Une attaque par amplification DNS implique généralement l'envoi d'une petite quantité d'informations à un service réseau vulnérable, qui répond en renvoyant une quantité de données beaucoup plus importante. En dirigeant cette réponse vers une victime, un attaquant peut, au prix d'un effort relativement faible, obliger les machines de tiers à inonder la cible de leur choix jusqu'à ce qu'elle tombe.

Déroulement de l'attaque :

Lors d'une attaque par amplification DNS, l'adversaire inonde un site web de fausses requêtes DNS qui dévorent la bande passante du réseau jusqu'à ce que le site tombe. Alors que le piratage DNS dirigerait le trafic vers un autre site, une attaque par amplification DNS empêche le site de se charger.

Le terme d'« amplification » souligne bien la différence entre les deux méthodes. Dans cette attaque, les requêtes DNS des pirates requièrent une réponse plus longue. Ils peuvent, par exemple demander plus qu'un simple nom de domaine, et réclamer l'intégralité du domaine, appelé « enregistrement ANY », qui englobe le domaine et les sous-domaines, les serveurs de messagerie, les serveurs de sauvegarde, les alias et bien plus encore.

Imaginez maintenant que plusieurs de ces requêtes « ANY » arrivent en même temps. Ce trafic amplifié est suffisant pour mettre le site hors ligne.

D'où vient l'attaque :

À l'instar du détournement DNS, cette attaque relativement primitive peut provenir de n'importe quelle région du monde, et être menée aussi bien par des pirates au service d'un État-voyou que par un loup solitaire.

Détournement DNS

Fin 2022, Celer Network, protocole d'interopérabilité et pont inter-chaînes, a été victime d'une attaque de détournement DNS. Son interface utilisateur cBridge redirigeait les utilisateurs vers des contrats de phishing sur Avalanche, Ethereum et Polygon pour épuiser leur compte.

Détournement DNS

Ce que vous devez savoir :

Le DNS, une sorte de répertoire téléphonique, est souvent considéré comme le talon d'Achille d'Internet car il joue un rôle essentiel dans le routage du trafic web. Le DNS est le protocole utilisé pour rapprocher les noms de domaine des adresses IP. Et il remplit parfaitement sa fonction. Mais le DNS est notoirement vulnérable, en partie à cause de sa nature distribuée. Il repose sur des connexions non structurées entre des millions de clients et de serveurs et utilise des protocoles intrinsèquement non sécurisés.

Les enjeux de la sécurisation du DNS contre les attaques sont considérables. Les conséquences d'une compromission peuvent être désastreuses. Les pirates peuvent mettre une entreprise entière dans l'incapacité d'exercer ses activités, mais aussi intercepter des informations confidentielles, des e-mails et des identifiants de connexion.

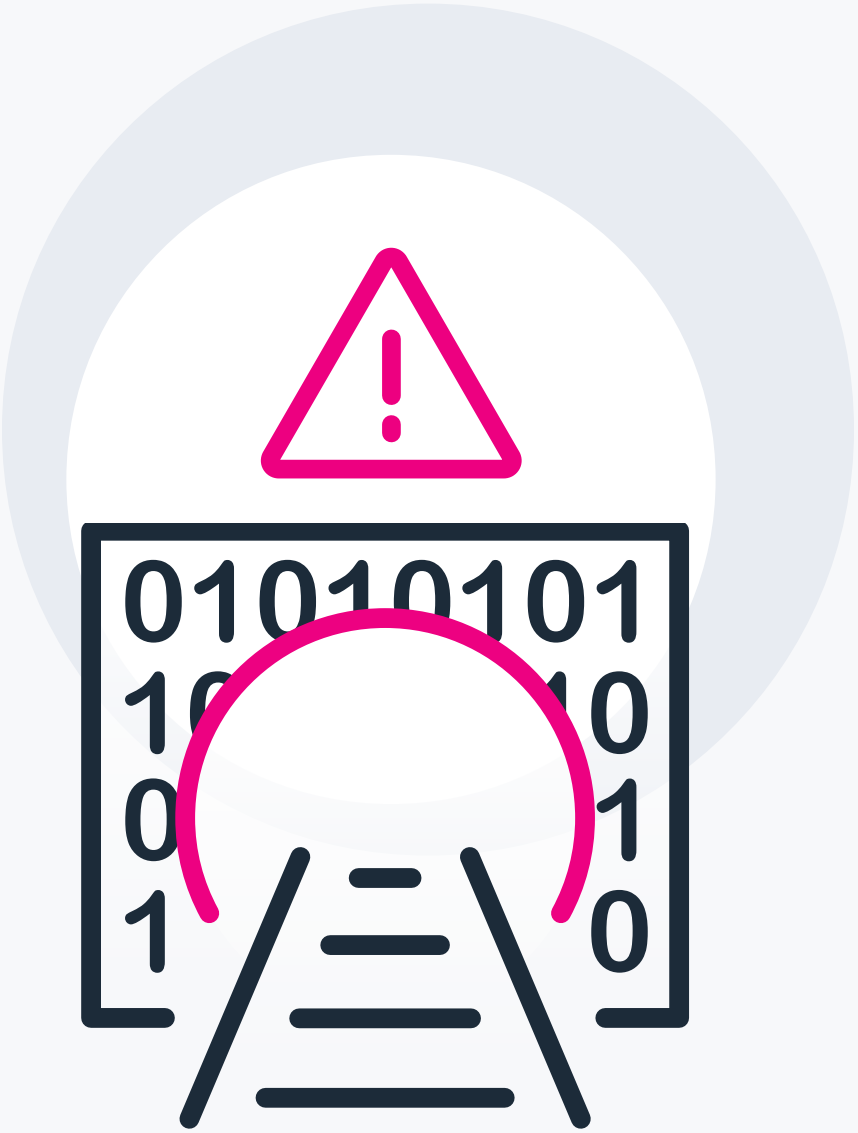
Déroulement de l'attaque :

Les pirates exploitent la façon dont DNS communique avec un navigateur Internet. Le système DNS agit comme un annuaire téléphonique : il traduit un nom de domaine, comme NYTimes.com, en adresse IP. Le DNS recherche ensuite quel serveur mondial héberge ce site, puis y dirige le trafic. Pour mener son attaque, le pirate informatique parvient à perturber la recherche DNS, puis à mettre le site hors ligne ou à rediriger le trafic vers un site qu'il contrôle.

D'où vient l'attaque :

Il n'existe pas de profil type du pirate de DNS, en grande partie parce que l'attaque peut prendre appui sur une simple opération d'ingénierie sociale : le malfaiteur appelle un fournisseur de domaine et le manipule pour qu'il modifie une entrée DNS.

Tunnelage DNS



Au cours des dernières années, un groupe de pirates informatiques connu sous le nom d'OilRig a lancé une série d'attaques contre plusieurs administrations et entreprises au Moyen-Orient en utilisant divers outils et méthodes. Pour perturber les opérations quotidiennes et exfiltrer les données, ce groupe doit impérativement établir une connexion durable entre son serveur de commande et de contrôle et le système qu'il attaque à l'aide du tunnelage DNS.

Tunnelage DNS

Ce que vous devez savoir :

Le protocole qui traduit les URL que nous saisissons dans un navigateur web en adresses IP numériques s'appelle le système de noms de domaine, ou DNS. Vous pouvez le voir comme l'annuaire téléphonique d'Internet. Bien souvent, le trafic qui transite par le DNS n'est pas supervisé, car ce protocole n'est pas conçu pour le transfert de données. Il est donc vulnérable à plusieurs types d'attaques, notamment le tunnelage DNS, qui consiste à encoder des données malveillantes dans une requête DNS, une chaîne complexe de caractères placée devant une URL.

Le tunnelage DNS a des usages légitimes : les fournisseurs de logiciels antivirus l'utilisent pour envoyer des mises à jour de profils de logiciels malveillants aux clients en arrière-plan, par exemple. Pour cette raison, les organisations doivent superviser minutieusement leur trafic DNS et autoriser uniquement le trafic digne de confiance à circuler sur le réseau.

Déroulement de l'attaque :

Avec le tunnelage DNS, un adversaire peut contourner les systèmes de sécurité (créer un tunnel, autrement dit) en redirigeant le trafic vers son propre serveur, de façon à établir une connexion au réseau d'une organisation. Cette connexion active ouvre la porte à plusieurs types d'attaque : commande et contrôle, exfiltration de données et bien d'autres.

D'où vient l'attaque :

On trouve des outils de tunnelage DNS facilement téléchargeables. Toutefois, des pirates qui souhaitent faire plus que contourner la page de paiement d'un hôtel ou d'une compagnie aérienne pour accéder gratuitement à Internet auront besoin de connaissances plus sophistiquées. Et comme le DNS a été conçu uniquement pour résoudre les adresses web, ce système est très lent quand il s'agit de transférer des données.

Attaque DoS

Il y a près de vingt ans, un hacker de 16 ans connu sous le nom de Mafiaboy a lancé l'une des attaques par déni de service (DoS) les plus célèbres et mis hors ligne plusieurs sites majeurs, notamment CNN, eBay, Amazon et Yahoo. Selon certaines informations, Mafiaboy aurait infiltré des dizaines de réseaux afin d'installer des logiciels malveillants conçus pour inonder les cibles de trafic d'attaque. Comme beaucoup de sites n'étaient pas préparés à ce type d'attaque, l'opération a duré près d'une semaine : les organisations ciblées ne parvenaient pas à comprendre ce qui s'était passé et comment rétablir leurs systèmes. Mafiaboy a finalement été arrêté et condamné à la détention en centre pour mineurs.

Vingt ans plus tard, les attaques DoS – dont beaucoup sont des attaques par déni de service distribué (DDoS) orchestrées par des pirates informatiques, des hacktivistes ou des cyberespions pour détruire des sites web et des services en ligne – sont en augmentation et restent l'une des formes d'attaque les plus courantes qui ciblent les entreprises. Les attaques DDoS sont en effet en hausse de 150 % en 2022 à l'échelle mondiale.

Attaque DoS

Ce que vous devez savoir :

Dans une attaque DoS, les pirates rendent une machine ou un réseau inaccessible à ses utilisateurs prévus. Les attaques DoS peuvent être exécutées soit en inondant les réseaux de trafic, soit en envoyant des informations qui déclenchent un ralentissement ou un effondrement complet du système. Comme dans le cas des attaques DDoS, les attaques DoS ont tendance à se concentrer sur des organisations de premier plan ou possédant des sites web populaires et publics, comme les banques, l'e-commerce, les médias ou les institutions gouvernementales. Les attaques DoS privent les utilisateurs légitimes du service auquel ils souhaitent accéder et causent des dommages importants à la victime, en raison des coûts de remise en sécurité et de nettoyage, des dommages à la réputation, des pertes de revenus et de l'attrition des clients.

Déroulement de l'attaque :

Les attaques DoS se produisent de deux manières : en inondant un réseau ou en provoquant son effondrement. Lors d'attaques par inondation, les cybercriminels bombardent les serveurs des victimes de trafic en quantité impossible à gérer, ce qui les ralentit, quand ils ne provoquent pas leur arrêt complet. Les attaques par débordement de tampon, par inondation ICMP et par inondation SYN entrent dans cette catégorie.

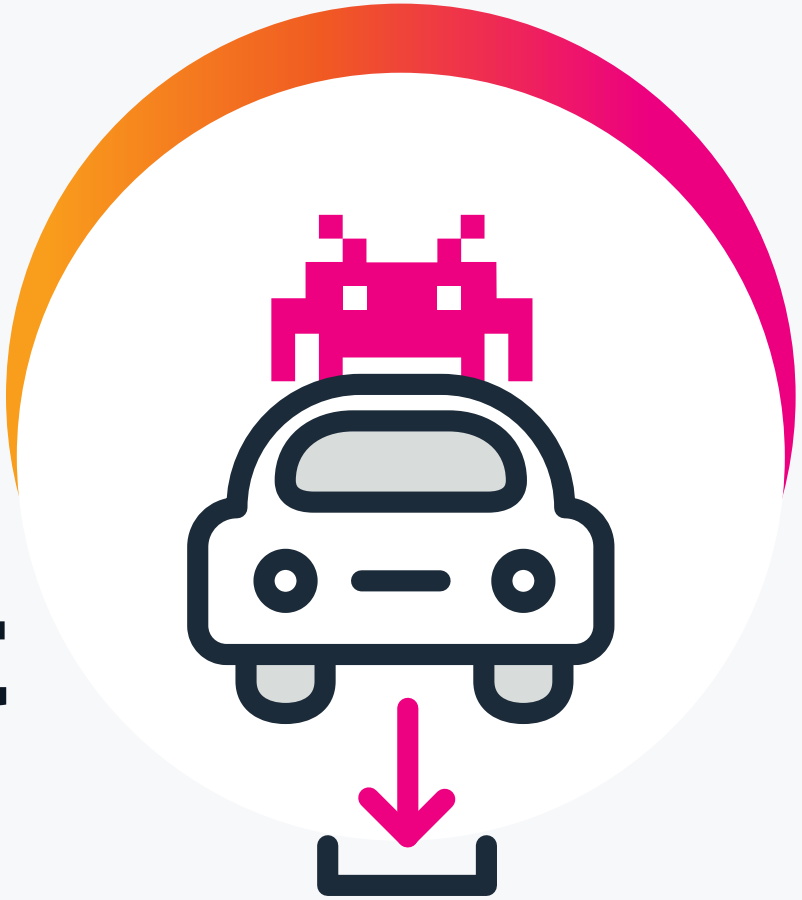
Les acteurs malveillants à l'origine des attaques DDoS visent à faire des ravages chez leurs cibles, à saboter les installations web, à nuire à la réputation des marques et à provoquer de lourdes pertes financières en empêchant les utilisateurs d'accéder à un site web ou à une ressource réseau. Le DDoS exploite des centaines, voire des milliers d'ordinateurs « robots » infectés répartis dans le monde entier. Connues sous le nom de botnets, ces armées d'ordinateurs compromis exécutent l'attaque de façon coordonnée pour une efficacité totale.

D'où vient l'attaque :

Les attaques DoS peuvent provenir de n'importe quelle région du monde. Parce qu'ils peuvent facilement masquer leur localisation, les adversaires submergent les ordinateurs des victimes, lancent des logiciels malveillants et multiplient les actes néfastes en toute sérénité : ils ne seront pas détectés.

Comme leur nom l'indique, les attaques DDoS sont distribuées : le flot de trafic entrant qui cible le réseau de la victime provient de nombreuses sources différentes. Les pirates qui mènent ces attaques peuvent littéralement venir de n'importe où dans le monde. De plus, du fait de leur nature distribuée, elles sont impossibles à arrêter en sécurisant ou en bloquant une source.

Attaque par téléchargement furtif



En janvier 2020, les visiteurs du légendaire magazine et blog Boing Boing se sont retrouvés face à une fausse surcouche Google Play Protect les invitant à télécharger ce qui était en réalité un APK malveillant qui installait un cheval de Troie bancaire sur les appareils Android. Pour les utilisateurs de Windows, il s'agissait d'une (fausse) page d'installation d'Adobe Flash qui distribuait d'autres programmes malveillants. Le système de gestion de contenu de Boing Boing avait été piraté. Même quand le visiteur ne mordait pas à l'hameçon, des téléchargements parallèles étaient automatiquement lancés par le JavaScript intégré à la page. Même si Boing Boing est parvenu à détecter l'attaque et à supprimer le script assez rapidement, l'impact aurait pu être désastreux sur ce site aux cinq millions d'utilisateurs uniques – parmi lesquels l'ancien président Barack Obama.

Attaque par téléchargement furtif

Ce que vous devez savoir :

Le téléchargement furtif désigne le téléchargement involontaire de code malveillant sur un ordinateur ou un appareil mobile, exposant les utilisateurs à différents types de menaces. Les cybercriminels utilisent le téléchargement furtif pour voler et collecter des informations personnelles, injecter des chevaux de Troie bancaires, des kits d'exploitation ou d'autres logiciels malveillants sur les appareils des utilisateurs. Pour vous protéger des téléchargements furtifs, appliquez régulièrement les mises à jour et les correctifs aux applications, aux logiciels, aux navigateurs et aux systèmes d'exploitation. Il est également recommandé de rester à l'écart des sites web non sécurisés ou potentiellement malveillants.

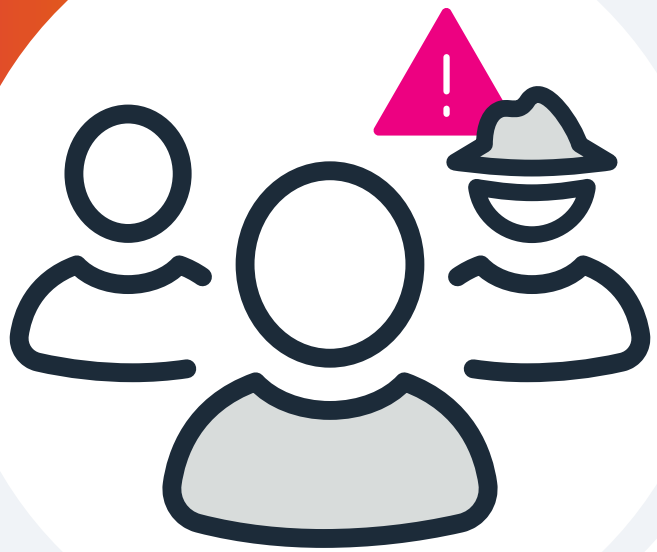
Déroulement de l'attaque :

Le téléchargement furtif se distingue en ce que les utilisateurs n'ont pas besoin de cliquer sur quoi que ce soit pour lancer le téléchargement. Il suffit en effet à la victime de consulter un site web ou de le parcourir pour activer le téléchargement. Les fichiers malveillants sont alors déposés sur l'appareil de la victime à son insu. Le téléchargement furtif tire parti d'applications, de navigateurs ou même de systèmes d'exploitation non sécurisés, vulnérables ou obsolètes.

D'où vient l'attaque :

La multiplication des kits de téléchargement furtif prêts à l'emploi permet aux pirates de tout niveau de compétences de lancer ce type d'attaques. En effet, un malfaiteur peut acheter et déployer ces kits sans écrire son propre code ni créer sa propre infrastructure pour exfiltrer des données ou commettre d'autres abus. En raison de leur extrême simplicité, ces attaques peuvent provenir de pratiquement n'importe où.

Menaces internes



La vengeance. Une histoire vieille comme le monde. En 2022, un informaticien a été inculpé sur des soupçons de piratage du serveur d'un établissement de santé de Chicago. Il avait eu accès au serveur parce qu'il était sous-traitant et il avait un mobile. On lui avait refusé un emploi au sein de l'organisation et, quelques mois plus tard, il avait été licencié par l'entreprise informatique sous-traitante. Cet acte de représailles individuel a pris la forme d'une cyberattaque qui a considérablement perturbé les examens médicaux, le traitement et le diagnostic de nombreux patients. Le pirate risque jusqu'à 10 ans de prison fédérale s'il est reconnu coupable.

Menaces internes

Ce que vous devez savoir :

Une attaque 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. 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 informations 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.

Déroulement de l'attaque :

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.

D'où vient l'attaque :

Les attaques internes peuvent provenir d'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 travailler pour leur propre compte ou pour celui d'un gouvernement, d'une organisation criminelle ou d'une entreprise concurrente. Même s'il s'agit de prestataires indépendants ou de sous-traitants situés ailleurs dans le monde, ces malfaiteurs disposent généralement d'un certain niveau d'accès légitime aux systèmes et aux données de votre organisation.

Menaces IoT

Après qu'une fuite de données a exposé les informations personnelles de plus de 3 000 utilisateurs de Ring, un fournisseur de sécurité domestique appartenant à Amazon, des pirates sont parvenus à détourner les sonnettes vidéo et les caméras intelligentes des maisons des utilisateurs touchés. Des milliers d'organisations restent exposées à des risques à cause de leur équipement Ring. Et les chercheurs pensent que ces attaques documentées ne représentent que la partie émergée de l'iceberg. Le chiffrement vidéo de bout en bout a depuis été introduit pour protéger les appareils Ring contre de futurs piratages, mais avec l'omniprésence croissante des appareils IoT, cette attaque ne sera pas la dernière.

Ce que vous devez savoir :

Il y a environ 15,14 milliards d'appareils IoT connectés à l'échelle mondiale selon les estimations – et ce nombre devrait passer à 30 milliards d'ici 2030. Ces appareils manquent souvent d'infrastructure de sécurité, ce qui crée des vulnérabilités flagrantes dans le réseau et agrandit de manière exponentielle la surface d'attaque pour les logiciels malveillants. Différents types d'attaques peuvent être lancées via des appareils IoT : attaques DDoS, ransomwares et ingénierie sociale.

Déroulement de l'attaque :

Les pirates et les États-voyous malveillants peuvent exploiter les vulnérabilités des appareils IoT connectés à l'aide de logiciels sophistiqués pour accéder à un réseau. L'objectif : superviser les utilisateurs ou voler de la propriété intellectuelle, des données classifiées ou personnellement identifiables, et autres informations critiques. Une fois qu'ils ont infiltré un système IoT, les pirates peuvent ensuite se déplacer latéralement vers d'autres appareils connectés ou accéder à un réseau plus vaste à diverses fins malveillantes.

D'où vient l'attaque :

Les attaques peuvent provenir de n'importe quelle région du monde. Mais comme de nombreux secteurs verticaux tels que les administrations, la fabrication et la santé déploient une infrastructure IoT sans les protections de sécurité adéquates, ces systèmes sont la cible d'attaques d'États-voyous hostiles et d'organisations cybercriminelles sophistiquées. Contrairement aux attaques visant les infrastructures technologiques, les attaques qui ciblent les systèmes civiques ou de santé connectés peuvent entraîner des perturbations généralisées et des situations de crise, et même mettre des personnes en danger.

Virus macro

L'un des virus les plus tristement célèbres de tous les temps, le virus Melissa de la fin des années 90, n'était autre qu'un macrovirus. Un PC infecté par Melissa détournait le système de messagerie Microsoft Outlook de l'utilisateur et envoyait des messages contaminés aux 50 premières adresses de ses listes de diffusion. Le virus s'est propagé à une vitesse incroyable et a causé des dégâts considérables dans le monde entier : on estime que le nettoyage et la réparation des systèmes et réseaux touchés a coûté 80 millions de dollars. L'âge d'or du virus macro est peut-être révolu, mais ces attaques persistent et ne ciblent plus uniquement Microsoft Windows : des attaques récentes visent également les utilisateurs de Mac.

Virus macro

Ce que vous devez savoir :

Un virus macro est un virus informatique écrit dans le langage macro qui est utilisé dans les applications logicielles. Certaines applications (Microsoft Office, Excel et PowerPoint) permettent d'intégrer des programmes de macros dans des documents de façon à ce qu'elles soient exécutées automatiquement à l'ouverture du document, fournissant un mécanisme pour la propagation d'instructions informatiques malveillantes. C'est l'une des raisons pour lesquelles il peut être dangereux d'ouvrir des pièces jointes inattendues ou des e-mails provenant d'expéditeurs non reconnus. De nombreux programmes antivirus peuvent détecter les virus macro, mais leur comportement reste parfois difficile à détecter.

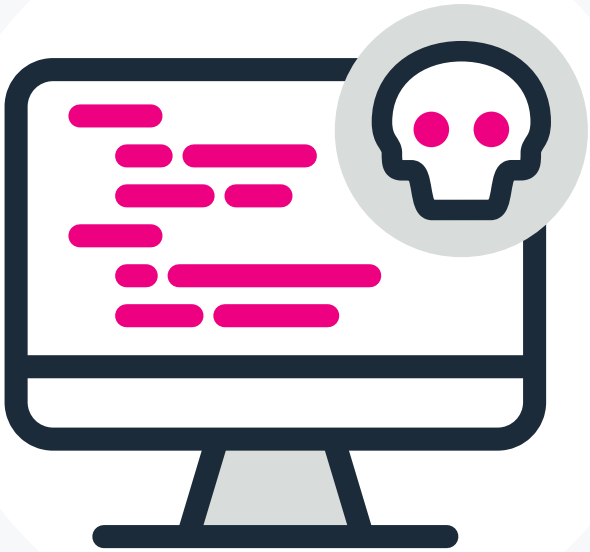
Déroulement de l'attaque :

Les virus macro se propagent souvent via des e-mails de phishing contenant des pièces jointes virales. Comme l'e-mail semble provenir d'une source crédible, de nombreux destinataires l'ouvrent sans hésitation. Une fois que la macro infectée est exécutée, elle peut accéder à tous les autres documents de l'ordinateur de l'utilisateur et les contaminer. Les virus macro se propagent chaque fois qu'un utilisateur ouvre ou ferme un document infecté. Ils fonctionnent dans des applications et non dans les systèmes d'exploitation. Les virus macro se propagent principalement via le partage de fichiers sur un disque ou un réseau et des pièces jointes à un e-mail.

D'où vient l'attaque :

Certes, les virus macro ne sont plus aussi prisés pour mener des attaques malveillantes – principalement parce que les logiciels antivirus parviennent bien mieux à les détecter et les désactiver. Pourtant, ils représentent toujours une menace majeure. Il suffit de chercher « virus macro » rapidement sur Google pour trouver des instructions sur leur création et des outils qui aident les non-codeurs à en fabriquer. En théorie, toute personne ayant accès à Internet peut facilement créer un virus macro.

Powershell malveillant



PowerShell est extrêmement populaire, et les séquences d'attaques qui l'exploitent sont tout aussi séduisantes pour les grands groupes de cybercriminalité et de cyberespionnage, car elles facilitent la propagation des virus sur un réseau. Des acteurs malveillants notoires tels que le groupe APT29 (alias Cozy Bear) emploient des scripts PowerShell pour recueillir des informations critiques qui vont éclairer des cyberattaques plus sophistiquées encore. En 2020, le célèbre groupe de menace APT35 (alias « Charming Kitten ») a exploité Powershell dans le cadre d'une attaque de ransomware visant une organisation caritative, ainsi que pour récolter et exfiltrer des données d'une administration locale américaine.

Powershell malveillant

Ce que vous devez savoir :

PowerShell est un outil de ligne de commande et de script développé par Microsoft et reposant sur .NET (qu'on prononce « dot net »). Il permet aux administrateurs et aux utilisateurs de modifier des paramètres système et d'automatiser des tâches. L'interface en ligne de commande (CLI), très souple, offre une large gamme d'outils, ce qui en fait un shell et un langage de script populaires. Les pirates ont, eux aussi, bien cerné les avantages de PowerShell : en tant que terminal de code, il leur permet d'opérer sans être détecté sur un système et d'agir en coulisses.

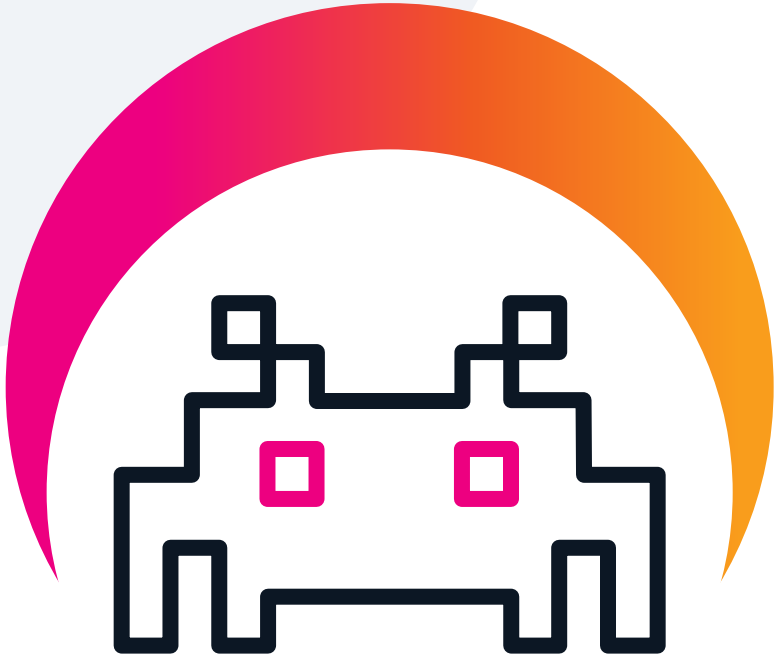
Déroulement de l'attaque :

Comme PowerShell est un langage de script qui s'exécute sur la majorité des machines d'entreprise, et que la plupart des entreprises ne supervisent pas les terminaux de code, la logique derrière ce type d'attaque est parfaitement claire. Il est facile d'obtenir l'accès à un système et de s'y enraciner. Nul besoin d'installer un logiciel malveillant pour exécuter le script nuisible. Pour le pirate, c'est un moyen simple d'éviter toute détection en contournant les analyses de fichiers exécutables, pour ensuite semer le chaos à sa guise.

D'où vient l'attaque :

Plus sophistiqué que les autres méthodes, ce type d'attaque est généralement le fait d'un pirate informatique qui sait exactement ce qu'il fait (contrairement à un amateur qui pourrait recourir à des attaques par force brute). Toujours furtif dans son approche, il sait brouiller les pistes et se déplacer latéralement sur un réseau.

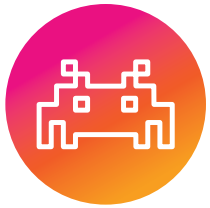
Logiciels malveillants



Identifié pour la première fois en 2014 comme cheval de Troie bancaire ciblant les particuliers, Emotet a su se réinventer pour devenir une menace persistante et omniprésente, *autant* dans le secteur public que dans le privé. Selon un rapport du ministère de la Sécurité intérieure, Emotet est l'un des logiciels malveillants les plus coûteux et les plus destructeurs – on parle de plus d'un million de dollars d'impact par incident.

Emotet a attaqué des agences gouvernementales en France, au Japon, au Canada et en Nouvelle-Zélande, mais aussi des entreprises du secteur privé, notamment dans les secteurs de la pharmacologie, de la fabrication, des technologies et des services financiers. Les forces de l'ordre américaines et européennes ont perturbé les activités du réseau Emotet en février 2021 en interrompant les communications et sa capacité à se propager. Emotet a fait son retour en 2023 et repris ses activités douteuses.

Logiciels malveillants



Ce que vous devez savoir :

Différents types de logiciels malveillants permettent de mener des activités d'espionnage, d'installer des portes dérobées de contrôle administratif et d'accéder à distance, sans entrave et sans autorisation, à l'appareil d'une cible. Une fois que les pirates ont pris le contrôle des machines en question, ils peuvent installer et supprimer des programmes, détourner des webcams, manipuler des fichiers et récolter des identifiants et autres données sensibles. Ils peuvent également usurper l'identité d'utilisateurs légitimes pour installer sans peine des logiciels malveillants supplémentaires, et ainsi compromettre d'autres ordinateurs et appareils sur le réseau.

Déroulement de l'attaque :

Les logiciels malveillants, distribués via des tactiques de phishing avancées, sont conçus pour dérober des informations sensibles telles que des identifiants, prendre des captures d'écran, accéder à la webcam et à l'audio des ordinateurs, les géolocaliser et enregistrer les frappes au clavier. L'une de leurs tactiques de phishing les plus courantes consiste à inciter les utilisateurs à ouvrir un fichier présenté sous forme de document Microsoft Office, principalement PowerPoint et Word. Les adversaires déploient des ransomwares auprès des entreprises par le biais de campagnes de harponnage et de téléchargements furtifs, mais aussi, de façon plus traditionnelle, en exploitant des failles dans des services à distance.

D'où vient l'attaque :

Compte tenu de la popularité et de l'omniprésence des logiciels malveillants, cette tactique est aussi insidieuse que courante. Si vous voyez un e-mail suspect accompagné d'une pièce jointe dans votre boîte de réception, vérifiez qu'il provient d'un expéditeur de confiance avant de l'ouvrir. Vous éviterez peut-être de libérer ce qui pourrait être un logiciel malveillant sur votre réseau.

Attaque de l'homme du milieu (MITM)

Début 2022, Microsoft a découvert une campagne de phishing ciblant les utilisateurs d'Office 365. Les attaquants ont présenté une fausse page de connexion 365 et collecté des informations d'identification pour en faire une utilisation frauduleuse par la suite. Pour ce faire, les attaquants ont utilisé un kit de phishing Evilginx2. Ce framework d'attaque de l'homme du milieu (MITM), utilisé pour acquérir des identifiants de connexion et des cookies de session, permet aux pirates de contourner l'authentification à deux facteurs afin de détourner le processus d'authentification. Dans son article de blog, Microsoft précise : « Notez qu'il ne s'agit pas d'une vulnérabilité inhérente à la MFA ; le phishing AiTM vole les cookies de session et l'attaquant ouvre une session authentifiée au nom de l'utilisateur, quelle que soit la méthode de connexion utilisée par ce dernier. »

Attaque de l'homme du milieu (MITM)

Ce que vous devez savoir :

L'attaque MITM, également connue sous le nom d'adversary-in-the-middle (AiTM), consiste à mettre en place un serveur proxy qui intercepte la session de la victime. L'acteur malveillant agit alors comme un relais entre les deux parties ou systèmes, et peut ainsi consulter et/ou voler des informations sensibles. Ce type d'attaque permet d'intercepter, d'envoyer et de recevoir des données destinées à quelqu'un d'autre – ou qui ne sont pas destinées à être envoyées du tout – sans qu'aucune des parties extérieures ne le sache, jusqu'à ce qu'il soit trop tard.

Déroulement de l'attaque :

L'attaque de l'homme du milieu est à la portée de n'importe qui ou presque. Mais depuis la généralisation d'HTTPS, elle est devenue plus difficile à exécuter et se fait donc plus rare Dans une attaque MITM, le pirate se place entre l'utilisateur et le site web (ou l'autre utilisateur) et assure la transmission des données tout en exfiltrant celles qui l'intéressent.

D'où vient l'attaque :

Dans la mesure où l'amélioration des technologies de sécurité a rendu les attaques MITM plus difficiles à exécuter, les seuls groupes qui les tentent sont des pirates sophistiqués ou des acteurs parrainés par des états. En 2018, la police néerlandaise a découvert quatre membres du groupe de pirates russe Fancy Bear garés devant l'Organisation pour l'interdiction des Armes Chimiques en Hollande ; ils tentaient une infiltration MITM pour voler les identifiants des employés. Plus tard cette année-là, les gouvernements américain et britannique ont publié des mises en garde indiquant que des acteurs parrainés par l'État russe ciblaient activement les routeurs des particuliers et des entreprises à des fins d'exfiltration MITM.

Attaque par mascarade

Les fraudeurs se font souvent passer pour des représentants d'éditeurs de logiciels afin d'inciter les utilisateurs peu avertis à télécharger des logiciels malveillants déguisés en pièces jointes dans des e-mails. Récemment, Microsoft et Adobe ont été particulièrement employés comme prétexte. « Les fraudeurs envoient à leurs victimes un fichier Microsoft OneNote en pièce jointe à un e-mail, et le téléchargement des logiciels malveillants se déclenche dès que quelqu'un l'ouvre, » a expliqué Avast, célèbre éditeur de logiciels antivirus et de sécurité, début 2023. Depuis, les attaques par mascarade continuent de se multiplier.

Attaque par mascarade

Ce que vous devez savoir :

On parle d'attaque par mascarade lorsqu'un acteur malveillant utilise une identité falsifiée ou réelle, mais volée, pour obtenir un accès non autorisé à la machine d'une personne ou au réseau d'une organisation via une identification légitime. Selon le niveau d'accès fourni par les autorisations, les attaques par mascarade peuvent donner aux pirates l'accès à l'ensemble d'un réseau.

Déroulement de l'attaque :

Une attaque par mascarade peut se produire après un vol d'identifiants ou au moyen d'une authentification sur des machines et des appareils non protégés ayant accès au réseau cible.

D'où vient l'attaque :

En interne, les attaquants peuvent obtenir l'accès en usurpant les domaines de connexion ou en utilisant des enregistreurs de frappe pour voler des identifiants légitimes. Les attaques peuvent également s'appuyer sur un accès physique à une machine laissée sans surveillance — un collègue qui accède à l'ordinateur de quelqu'un d'autre pendant son absence, par exemple. De manière générale, le problème trouve souvent son origine dans des méthodes d'authentification faibles qui peuvent être exploitées par des parties externes.

Attaque Meltdown et Spectre

La plupart des attaques de cybersécurité exploitent une vulnérabilité, comme une erreur de code ou de conception. Mais toutes les attaques ne se valent pas. Deux chercheurs de Google ont découvert un nouveau type d'attaque qui a touché tous les fabricants de puces informatiques. Ce sont potentiellement des milliards de personnes qui ont été exposées à Meltdown et Spectre.

Attaque Meltdown et Spectre

Ce que vous devez savoir :

L'attaque Meltdown et Spectre exploite les vulnérabilités des processeurs informatiques. Ces vulnérabilités permettent aux attaquants de voler presque toutes les données en cours de traitement sur l'ordinateur. Cette attaque frappe au cœur de la sécurité informatique, qui repose normalement sur l'isolation de la mémoire pour protéger les informations d'un utilisateur. La partie « Meltdown », fait référence à la rupture de toute barrière de protection entre le système d'exploitation et un programme, tandis que « Spectre » désigne la rupture de la frontière entre deux applications qui ne doivent normalement pas échanger d'informations.

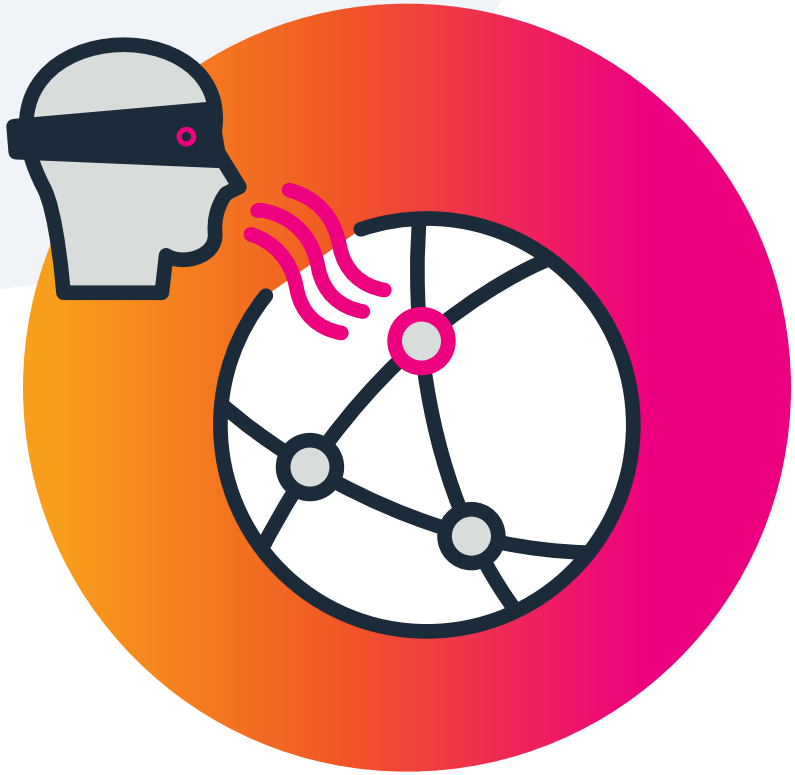
Déroulement de l'attaque :

L'attaque Meltdown et Spectre exploite des vulnérabilités critiques présentes dans les processeurs modernes, et qui ouvrent un accès non prévu aux données stockées en mémoire. Cette attaque brise une norme de l'informatique, à savoir que les programmes ne sont pas autorisés à lire les données d'autres programmes. Les informations généralement ciblées par les pirates sont les mots de passe stockés dans un gestionnaire de mots de passe ou un navigateur, mais aussi les e-mails, les dossiers financiers et les informations personnelles comme les photos et les messages instantanés. Mais cette attaque ne vise pas seulement des ordinateurs personnels. Elle peut cibler tous les appareils dotés d'un processeur ou presque, y compris les téléphones mobiles et les tablettes.

D'où vient l'attaque :

Une attaque Meltdown et Spectre peut provenir de n'importe où, et jusqu'à présent, la plupart des recherches se sont attachées à cerner la nature unique de cette attaque plutôt qu'à identifier les auteurs.

Reniflage de réseau



Les serrures connectées sont conçues pour protéger votre maison et permettre d'y accorder l'accès en un clic, ou sur simple pression d'un bouton. Mais adopter cette approche futuriste pour protéger votre maison peut avoir de graves conséquences, comme l'ont découvert des chercheurs en sécurité. Le trafic réseau d'une serrure connectée, vendue de façon un peu abusive comme la « serrure la plus intelligente jamais conçue », peut être intercepté entre l'application mobile et la serrure elle-même. Et ce qui est le plus effrayant, c'est qu'il suffit pour cela d'utiliser des dispositifs de détection de réseau, peu coûteux et faciles à se procurer.

Reniflage de réseau

Ce que vous devez savoir :

Le reniflage de réseau, également connu sous le nom de reniflage de paquets, désigne la capture, la supervision et l'analyse en temps réel des données circulant au sein d'un réseau. Que ce soit via le matériel, le logiciel ou une combinaison des deux, les acteurs malveillants utilisent des outils de détection pour espionner les données non chiffrées des paquets réseau : informations d'identification, e-mails, mots de passe, messages et autres informations sensibles.

Déroulement de l'attaque :

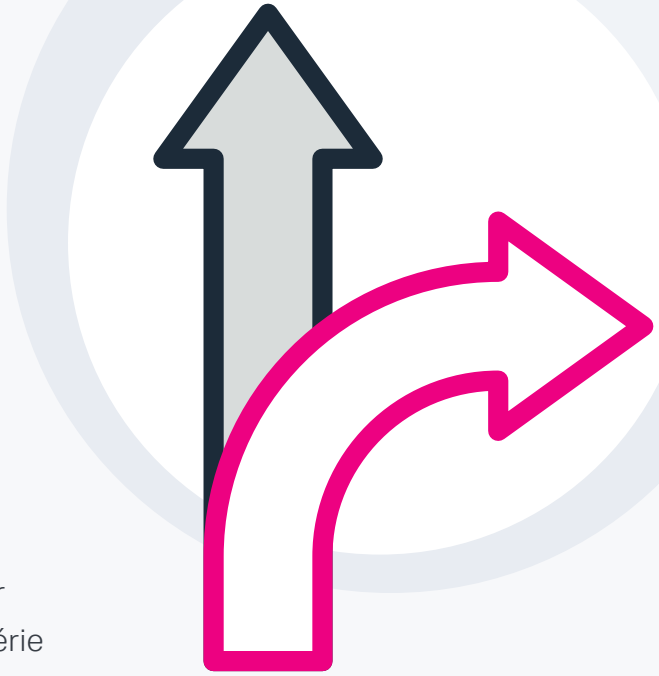
Tout comme dans les scénarios d'écoute téléphonique, le reniflage de réseau opère en arrière-plan, écoutant silencieusement les échanges d'informations entre les entités d'un réseau. Pour y parvenir, les malfaiteurs placent un renifleur sur un réseau en installant un logiciel ou un dispositif matériel connecté à un appareil qui lui permet d'intercepter et de consigner le trafic sur le réseau filaire ou sans fil auquel l'appareil hôte a accès. En raison de la complexité inhérente à la plupart des réseaux, les renifleurs peuvent rester longtemps présents sur le réseau avant d'être détectés.

D'où vient l'attaque :

Le reniflage de réseau est souvent effectué légalement par des organisations telles que les FAI, les agences de publicité, les agences gouvernementales et autres qui ont besoin de superviser le trafic réseau.

Mais il peut également être le fait de pirates « pour s'amuser » ou d'États-voyous cherchant à dérober des secrets industriels. Comme les ransomwares, les renifleurs de réseau peuvent être injectés dans le réseau en demandant à la personne visée de cliquer sur le lien adéquat. Les acteurs internes ayant accès à du matériel sensible peuvent également être un vecteur d'attaque.

Redirection ouverte



En 2022, on a découvert qu'une nouvelle campagne de phishing ciblant les utilisateurs de Facebook avait permis d'obtenir des centaines de millions d'identifiants. La technique utilisée était assez ordinaire : un lien, envoyé par message privé à partir d'un compte Facebook compromis, effectuait une série de redirections, souvent via des pages de publicité malveillantes, pour accumuler des vues et des clics (et donc des revenus pour l'adversaire), avant d'arriver sur une fausse page. La technique de redirection d'hôte, également connue sous le nom de redirection ouverte, n'a rien de nouveau, mais l'envergure de cette campagne est remarquable. Les chercheurs ont découvert que l'une des 400 pages de destination de phishing avait comptabilisé à elle seule 2,7 millions de visiteurs en 2021 et 8,5 en juin 2022. Dans un entretien avec des chercheurs, le pirate s'est vanté de gagner 150 dollars pour chaque millier de visites d'utilisateurs américains de Facebook, ce qui porterait le total de ses recettes à 59 millions de dollars.

Redirection ouverte

Ce que vous devez savoir :

Les attaques par redirection d'hôte sont très courantes et de plus en plus dangereuses, car les pirates informatiques font preuve d'une créativité croissante pour attirer leurs cibles. Les attaquants utilisent la redirection d'URL pour gagner la confiance d'un utilisateur avant de frapper. Ils emploient généralement des URL intégrées, un fichier .htaccess ou des tactiques de phishing pour rediriger le trafic vers un site web malveillant.

Déroulement de l'attaque :

Le pirate peut envoyer un e-mail de phishing contenant une imitation de l'URL du site web à sa victime. Si le site web semble légitime, les utilisateurs peuvent partager par inadvertance des informations personnelles en répondant aux messages et en remplissant les formulaires qui s'affichent. Les pirates peuvent passer au niveau supérieur en intégrant de faux domaines de commande et contrôle à des logiciels malveillants et en hébergeant du contenu nuisible sur des domaines imitant fidèlement les serveurs d'entreprise.

D'où vient l'attaque :

L'origine de cette attaque n'a pas autant d'importance que sa cible. Cette attaque cible généralement les internautes non avertis qui ne remarqueront pas qu'il manque une lettre ou deux à l'URL de leur domaine préféré. Et comme cette attaque se targue d'être simple (il peut parfois suffire d'enregistrer un nom de domaine), elle peut provenir de presque n'importe où.

Pass the hash

Le succès de la célèbre faille de Target, qui a permis aux pirates d'accéder à 40 millions de comptes clients, a reposé en grande partie sur une technique bien connue, appelée « Pass the hash » (PtH). Les pirates ont utilisé PtH pour accéder à un jeton de hachage NT qui devait leur permettre de se connecter au compte de l'administrateur Active Directory sans le mot de passe en clair. Ils ont ainsi obtenu les privilèges nécessaires pour créer un nouveau compte d'administrateur de domaine, puis l'ajouter au groupe Administrateurs de domaine. Cet ancrage dans le système leur a permis de voler les données personnelles et les informations des cartes de paiement des clients de Target.

Pass the hash

Ce que vous devez savoir :

Le passage de hash permet à un attaquant d'authentifier le mot de passe d'un utilisateur avec le hash NTLM ou LanMan sous-jacent plutôt que le mot de passe en clair. Une fois que le pirate a un nom d'utilisateur valide ainsi que les valeurs de hash de son mot de passe, il peut accéder au compte de l'utilisateur sans problème et effectuer des actions sur des systèmes locaux ou distants. Essentiellement, les hash remplacent les mots de passe d'origine à partir desquels ils ont été générés.

Déroulement de l'attaque :

Sur les systèmes utilisant l'authentification NTLM, le mot de passe ou la phrase secrète d'un utilisateur n'est jamais soumis en texte clair. Au lieu de cela, il est envoyé sous forme de hash en réponse à un schéma d'authentification défi-réponse. Lorsque cela se produit, les hashes de mot de passe valides pour le compte utilisé sont capturés à l'aide d'une technique d'accès aux identifiants.

D'où vient l'attaque :

Ce type d'attaque est plus sophistiqué que d'autres méthodes et est généralement le fait de groupes de menaces hautement organisés et motivés, qui visent une organisation ou une personne spécifique, dans un but politique ou financier.

Phishing

En juin 2022, Twilio, une plateforme d'engagement client, a connu sa deuxième faille majeure. Les pirates informatiques du groupe « 0ktapus », responsables des deux incidents, ont réussi à accéder aux données des clients en utilisant le phishing (hameçonnage) vocal : l'un d'eux s'est fait passer pour le service informatique de Twilio au téléphone afin de tromper un employé. Pensant parler à un représentant légitime, l'employé a fourni au groupe criminel les informations de connexion de l'entreprise. Cette violation a abouti à la consultation non autorisée d'un nombre limité de coordonnées clients.

Phishing

Ce que vous devez savoir :

Une attaque par hameçonnage incite des consommateurs, des utilisateurs ou des employés 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 communication. Faites preuve de vigilance : ces faux sites sont souvent très convaincants, mais les pirates s'apprêtent 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.

Déroulement de l'attaque :

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.

D'où vient l'attaque :

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. 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.

Charges utiles de phishing

Attribuée au groupe de menaces TA866, une attaque de phishing unique en son genre a fait son apparition : une charge utile malveillante préliminaire prend des captures d'écran des appareils des victimes. Cela permet aux attaquants d'évaluer la valeur potentielle de la victime et de décider s'il peut être rentable de déployer d'autres logiciels malveillants. À ce jour, cette campagne a ciblé plus de 1 000 organisations aux États-Unis et en Allemagne.

Ce que vous devez savoir :

Malgré sa simplicité, le phishing reste la cybermenace la plus répandue et la plus dangereuse. En effet, des recherches montrent que jusqu'à 91 % des attaques réussies ont pour point de départ un e-mail de phishing.

Ces e-mails utilisent des domaines frauduleux, des techniques de moissonnage d'e-mails, des noms de contacts familiers en tant qu'expéditeurs et d'autres tactiques pour inciter les cibles à cliquer sur un lien malveillant, à ouvrir une pièce jointe avec une charge utile nuisible, ou à saisir des informations personnelles sensibles qui seront interceptées. La « charge utile » désigne les données néfastes qui constituent le véritable message. Les en-têtes et les métadonnées n'ont pour seul but que de faciliter la livraison de la charge utile.

Déroulement de l'attaque :

Cette attaque a un modèle d'attaque classique : tout d'abord, l'attaquant envoie un e-mail de phishing et le destinataire télécharge la pièce jointe, qui correspond généralement à un fichier .docx ou .zip avec un fichier .lnk intégré. Ensuite, le fichier .lnk exécute un script PowerShell qui, lui, exécute un shell inversé et assure le succès de l'exploitation.

D'où vient l'attaque :

Comme cette attaque ne nécessite pas un haut niveau de sophistication technique, et comme le phishing est au cœur de la plupart des cyberattaques, elle peut provenir de n'importe où dans le monde.

Spear Phishing (harponnage)

De nos jours, les harponneurs ne ciblent pas seulement les plus gros poissons : s'inspirant des escroqueries amoureuses, ils attirent leurs victimes avec de faux profils attrayants pour les inciter à télécharger des logiciels malveillants sur leurs ordinateurs. Les chercheurs ont identifié une attaque d'ingénierie sociale et de malware ciblée qui dure depuis des années et qui est le fait du célèbre acteur menaçant TA456, lié à l'État iranien. À l'aide d'un faux profil de réseau social « Marcella Flores », TA456 a noué une relation amoureuse factice avec un employé d'une filiale d'un petit entrepreneur de défense aérospatiale. Quelques mois plus tard, l'attaquant est passé à l'action en envoyant un gros fichier malveillant via une chaîne de communication utilisant l'e-mail d'entreprise dans le but d'effectuer une reconnaissance. Une fois que le malware, baptisé LEMPO, a infiltré la machine, il a exfiltré des données et renvoyé des informations hautement sensibles au pirate, tout en dissimulant sa localisation pour échapper à toute détection.

Spear Phishing (harponnage)

Ce que vous devez savoir :

Type particulier d'hameçonnage, le spear phishing, ou 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 au réseau. Le spear phishing vise les personnes qui ont accès à des informations sensibles ou constituent un maillon faible dans le réseau. Les cibles de grande valeur, comme les membres de la direction ou du conseil d'administration d'une entreprise, ou bien les administrateurs bénéficiant de privilèges élevés, sont particulièrement vulnérables, car elles ont accès à des systèmes critiques et à des informations confidentielles.

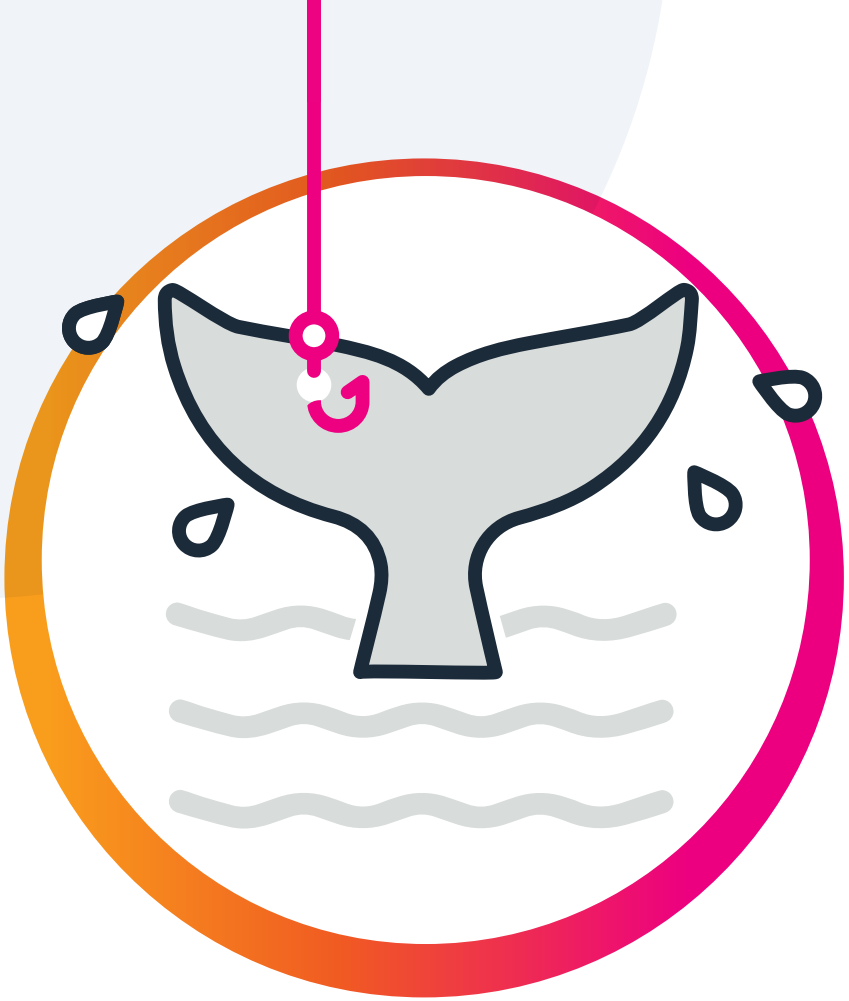
Déroulement de l'attaque :

Les criminels font des recherches pour identifier les cibles et cerner leur position professionnelle à l'aide de réseaux sociaux comme LinkedIn. Ils usurpent ensuite des adresses pour leur envoyer des messages parfaitement personnalisés, à l'aspect authentique, afin d'infiltrer leur infrastructure et leurs systèmes. Une fois que les pirates ont accès à l'environnement, ils tentent de mettre en œuvre des plans plus sophistiqués encore.

D'où vient l'attaque :

Elle peut être le fait d'individus ou d'organisations. Toutefois, de nombreuses tentatives d'hameçonnage ciblé 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.

Whaling (harponnage de baleine)



Pourquoi se contenter des petits poissons quand on peut viser une baleine ? Le fonds spéculatif australien Levitas Capital l'a découvert à ses dépens quand des pirates ont lancé une attaque furtive visant directement l'un des fondateurs. Les malfaiteurs ont accédé au réseau du hedge fund après avoir envoyé au dirigeant un faux lien Zoom qui installait un logiciel malveillant lorsqu'on cliquait dessus. Le code malveillant a permis aux attaquants d'infiltrer le compte de messagerie ciblé et de créer de fausses factures à l'intention du fiduciaire de fonds et de l'administrateur tiers, qui ont lancé et approuvé des demandes de transfert d'argent, pour un montant total de 8,7 millions de dollars. Parmi les fausses factures, il y avait une demande de paiement de 1,2 million de dollars à la société de capital-investissement suspecte Unique Star Trading. Les pertes ont été si considérables que l'entreprise a finalement été contrainte de fermer définitivement ses portes.

Whaling (harponnage de baleine)

Ce que vous devez savoir :

On parle de whaling lorsque les pirates s'attaquent à une cible unique et de grande valeur, comme le PDG d'une société de services financiers. La cible est toujours une personne spécifique, alors qu'un e-mail de phishing peut s'en prendre à n'importe qui dans une entreprise. Si les pirates s'attaquent à des cibles de premier plan, c'est aussi parce qu'elles peuvent posséder des informations importantes ou sensibles.

Déroulement de l'attaque :

La technique utilisée lors d'une attaque de whaling relève du phishing classique. La cible reçoit un e-mail d'apparence authentique qui lui demande généralement de cliquer sur un lien. Ce lien contient un code malveillant ou mène à un site web qui demande des informations sensibles telles qu'un mot de passe.

D'où vient l'attaque :

Le phishing est le point d'entrée le plus courant d'une cyberattaque, si bien qu'une attaque de whaling peut provenir de n'importe où dans le monde.

L'attaque de Levitas Capital, par exemple, était le fait d'un collectif de cybercriminels de diverses régions, et les paiements étaient envoyés à la Bank of China et à la United Overseas Bank à Singapour.

Compromission d'utilisateur privilégié

En 2022, le groupe de piratage criminel Lapsus$, prétendument dirigé par un adolescent d'Oxford, en Angleterre, s'est vanté publiquement d'avoir réussi à pirater Okta, un fournisseur d'authentification unique utilisé par des milliers d'organisations et d'administrations dans le monde. Lapsus$ a eu accès à un compte administratif « super utilisateur » pour Okta via un technicien de support tiers. Pendant cinq jours, les pirates ont ainsi pu accéder à l'ordinateur portable de l'employé, qui avait notamment un accès privilégié à certains systèmes Okta. Le groupe cybercriminel a divulgué des informations sur l'attaque sur sa chaîne Telegram, allant même jusqu'à publier des captures d'écran montrant qu'il se trouvait dans les systèmes d'Okta. Pourtant, il ne visait pas précisément Okta : les véritables cibles étaient les 15 000 clients d'Okta. Une semaine plus tard, le groupe de hackers a ajouté 15 000 abonnés à sa chaîne Telegram, faisant craindre de nouvelles attaques imminentes.

Compromission d'utilisateur privilégié

Ce que vous devez savoir :

Il est largement admis que de nombreuses violations graves de données peuvent être attribuées à l'abus d'identifiants privilégiés. Il s'agit de comptes disposant de privilèges élevés, comme des droits d'administration sur un domaine ou des privilèges root. Les adversaires utilisent de plus en plus les identifiants d'utilisateurs privilégiés pour accéder aux ressources et aux informations d'une organisation et exfiltrer des données sensibles. Un pirate qui accède aux identifiants d'un utilisateur privilégié peut contrôler l'infrastructure d'une organisation et modifier les paramètres de sécurité, exfiltrer des données, créer des comptes utilisateurs et plus encore, tout en apparaissant légitime, et donc plus difficile à détecter.

Déroulement de l'attaque :

Les pirates tentent d'obtenir un accès à des comptes privilégiés en utilisant des techniques d'ingénierie sociale, des messages d'hameçonnage, des malwares ou des attaques par passage de hash. Les organisations ont ouvert leurs réseaux pour répondre aux besoins d'une main-d'œuvre de plus en plus mobile et distante, et mis un réseau complexe d'accès à distance à la disposition de leurs fournisseurs et prestataires de services. Bon nombre de ces connexions, y compris vers le cloud, sont accessibles à l'aide d'identifiants de compte privilégié. Il est extrêmement difficile de trouver, contrôler et superviser toutes ces connexions – une manne pour les malfaiteurs.

Une fois armés des identifiants, les attaquants entrent et se saisissent de tout ce qui peut être intéressant : clés SSH, certificats, hash d'administration de domaine. Et il suffit d'un seul compte pour entraîner une violation de données majeure et mettre une organisation à genoux.

D'où vient l'attaque :

Parce qu'elle offre aux cybercriminels un accès aussi large que discret à toutes sortes de données, la compromission d'utilisateurs privilégiés est très attrayante et couramment employée dans des cyberattaques de toutes sortes, du cyberespionnage national motivé par une idéologie politique à la cybercriminalité sophistiquée à but lucratif, avec des groupes comme Lapsus$.

Ransomwares

Selon la société de cybersécurité Emsisoft, les attaques par ransomware ont touché au moins 948 agences gouvernementales, établissements d'enseignement et organismes de santé aux États-Unis en 2019, pour un coût dépassant potentiellement les 7,5 milliards de dollars.

Ces attaques ont de lourdes conséquences dans le secteur médical : les patients doivent être redirigés vers d'autres hôpitaux, les dossiers médicaux deviennent inaccessibles (quand ils ne sont pas définitivement perdus) et les centres de répartition des urgences doivent s'appuyer sur des cartes imprimées et des registres papier pour suivre les intervenants d'urgence sur le terrain. Quand les gouvernements sont touchés, les services d'urgence locaux peuvent être perturbés. Et selon Cyrus Vance Jr. du Manhattan D.A., l'effet d'un ransomware peut être aussi dévastateur et coûteux qu'une catastrophe naturelle comme l'ouragan Sandy.

Ce que vous devez savoir :

Une attaque par ransomware (ou rançongiciel) infecte un hôte, chiffre les données de la victime et les retient en otage jusqu'à ce qu'elle verse une rançon. Au cours de récentes attaques de ransomware, les pirates ont menacé de divulguer ou de vendre les données volées, augmentant considérablement les dommages potentiels de ce type d'attaque.

Il existe d'innombrables types de ransomwares, mais certains groupes sont particulièrement néfastes. Un gang bien connu, Blackmatter, a ciblé un certain nombre d'organisations essentielles à l'économie et à l'infrastructure des États-Unis, notamment dans l'industrie agroalimentaire. Ryuk doit également faire l'objet d'une supervision étroite. En 2019, Ryuk était l'auteur de la demande de rançon la plus élevée de l'histoire, avec 12,5 millions de dollars.

Déroulement de l'attaque :

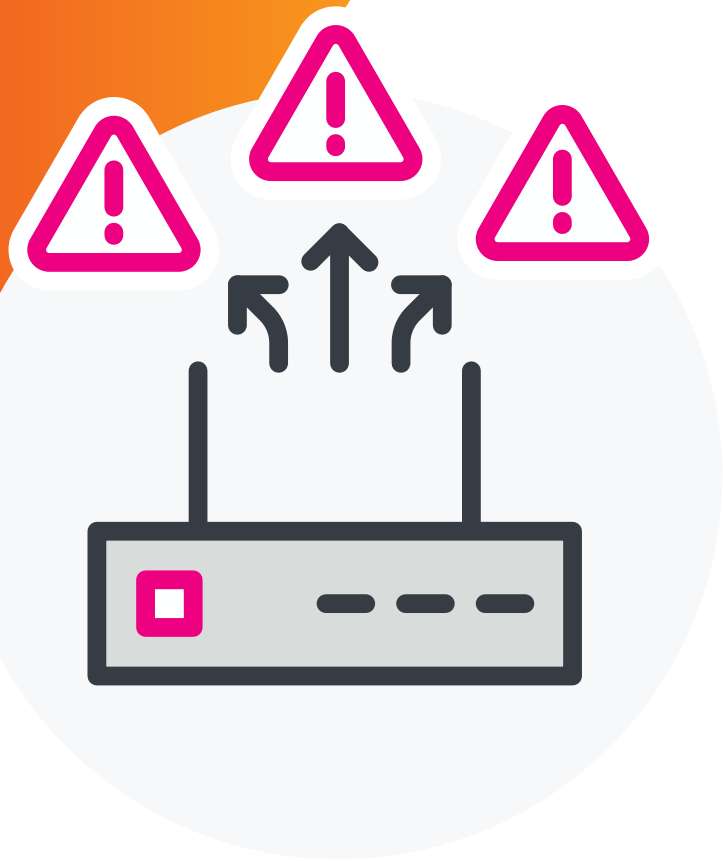
Les adversaires déploient des ransomwares auprès des entreprises et des particuliers par le biais de campagnes de harponnage et de téléchargements furtifs, mais aussi, de façon plus traditionnelle, en exploitant des failles dans des services à distance. Une fois le logiciel malveillant installé sur la machine de la victime, il présente une fenêtre à l'utilisateur ou le dirige vers un site web, où il est informé que ses fichiers sont chiffrés et peuvent être libérés s'il paie la rançon.

Le ransomware en tant que service (RaaS), quant à lui, est un modèle commercial impliquant des opérateurs de ransomware et des affiliés ; ces derniers paient pour lancer des attaques de ransomware élaborées par les opérateurs. Les kits RaaS permettent aux affiliés qui n'ont pas les compétences ou le temps nécessaires pour développer leur propre variante de ransomware, de devenir rapidement opérationnels, à moindre coût. Un kit RaaS peut s'accompagner d'une assistance 24 h/24 et 7 j/7, d'offres groupées, d'avis d'utilisateurs, de forums et d'autres options semblables à celles que proposent les fournisseurs SaaS légitimes.

D'où vient l'attaque :

Les ransomwares étaient habituellement l'œuvre de groupes de cybercriminels sophistiqués, qui restent anonymes après avoir extorqué des gouvernements ou de grandes entreprises. Cependant, depuis l'arrivée des cryptomonnaies, qui simplifient les transactions anonymes, le grand public est plus exposé aux attaques de ransomwares.

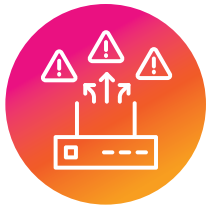
Comme les kits RaaS sont relativement simples à utiliser et très faciles à trouver sur le dark web, où ils font l'objet de grandes campagnes publicitaires, ce type d'attaque peut être le fait de n'importe quel pirate débutant disposant des fonds nécessaires à l'achat d'un kit.



Attaques contre les routeurs et l'infrastructure

Cisco a été victime d'une attaque de routeur et d'infrastructure au cours de laquelle un « implant », surnommé SYNful Knock, aurait été identifié dans 14 routeurs, répartis dans quatre pays différents. SYNful Knock est un malware persistant qui permet à un attaquant de prendre le contrôle d'un périphérique et de compromettre son intégrité en lui appliquant une image logicielle Cisco IOS modifiée. D'après la description de Mandiant, il comprend différents modules activés via le protocole HTTP et déclenchés par des paquets TCP contrefaits envoyés à l'appareil.

Attaques contre les routeurs et l'infrastructure



Ce que vous devez savoir :

Les implants de routeur sont rares et ont longtemps été considérés comme purement théoriques. Cependant, de récents avis des fournisseurs signalent des observations dans le monde réel. On pense que les attaquants accèdent à ces appareils en identifiant des vulnérabilités connues ou en ciblant les appareils avec des mots de passe par défaut ou faibles, simples à deviner. La position du routeur dans le réseau en fait une cible idéale pour une implantation durable et pour propager une infection.

Déroulement de l'attaque :

Les périphériques réseau, tels que les routeurs et les switches, sont rarement considérés comme des ressources visées par des adversaires pour compromettre une entreprise. Les attaquants infectent les périphériques réseau et peuvent ensuite obtenir un accès direct à l'infrastructure interne de l'entreprise, ce qui augmente efficacement la surface d'attaque et ouvre la porte aux services et aux données privés.

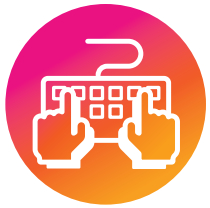
D'où vient l'attaque :

Les acteurs des menaces avancées ont montré une propension à cibler ces actifs critiques pour siphonner et rediriger le trafic réseau, flasher les systèmes d'exploitation infiltrés et mettre en œuvre des algorithmes de chiffrement affaiblis pour déchiffrer plus facilement le trafic réseau.

Shadow IT

Parce qu'elles sont très rapides et faciles à utiliser, les applications SaaS (Software as a Service) sont particulièrement prisées par les employés qui peuvent les installer sur leur poste de travail. Mais nombreux sont ceux qui utilisent ces applications sans se soucier de la sécurité. On ne sera donc pas surpris d'apprendre qu'une étude de Forbes Insights, intitulée « Écarts de perception de la cyber-résilience : qu'est-ce qui pourrait mal tourner ? », a révélé que plus d'une organisation sur cinq avait été confrontée à un cyberincident en lien avec une ressource informatique non autorisée, « fantôme » ou « shadow IT ».

Shadow IT



Ce que vous devez savoir :

Le shadow IT désigne les applications et les infrastructures informatiques que les employés utilisent à l'insu et/ou sans le consentement du service IT de leur organisation. Il peut s'agir de matériel, de logiciels, de services web, d'applications cloud et d'autres types de programmes. En général, les employés sont bien intentionnés ; ils téléchargent et utilisent ces applications en toute bonne foi, pour rendre leur travail plus facile ou plus efficace. Ce phénomène est à ce point répandu que Gartner avait estimé qu'un tiers des attaques de cybersécurité en entreprise pourrait lui être attribué. Parce que les utilisateurs accèdent à ces applications sans le faire savoir, ils ouvrent souvent involontairement la porte aux menaces internes, aux violations de données et aux infractions de conformité.

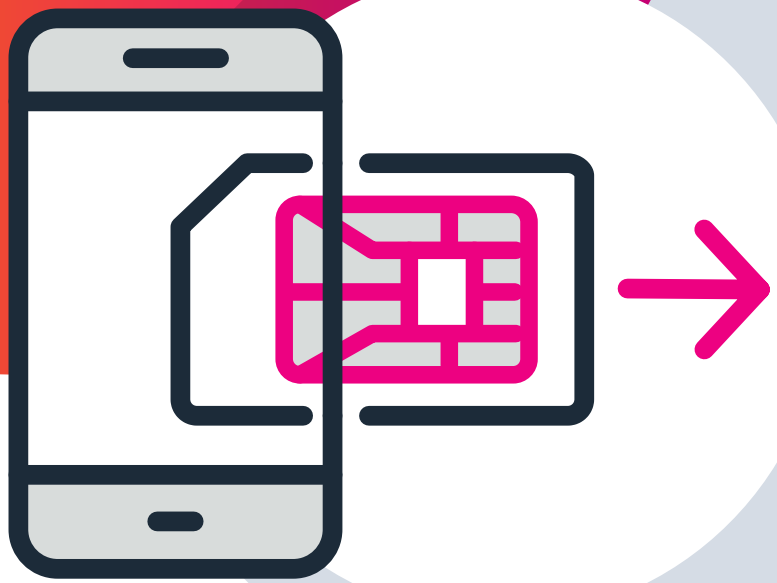
Déroulement de l'attaque :

Parce que le shadow IT est discret par nature, les employés partagent ou stockent des données sur des services cloud non autorisés, ouvrant la voie à une multitude de risques de sécurité et de conformité. Le risque de violation émerge lorsque les employés téléchargent, partagent ou stockent des données critiques ou réglementées dans des applications non validées, sans la protection de solutions appropriées de sécurité et de prévention des pertes de données (DLP). Les informations exposées sont une proie facile pour les menaces internes comme les tentatives de vol de données, ce qui peut entraîner des violations de conformité coûteuses. Rappelons également que les applications elles-mêmes peuvent présenter de nombreuses vulnérabilités au niveau des points de terminaison, ainsi que des failles de sécurité.

D'où vient l'attaque :

Cette fois, la menace provient de l'intérieur d'une organisation. Les employés qui recourent au shadow IT le font souvent pour contourner une politique restrictive ou pour accomplir leur travail plus rapidement, et non pas pour mettre en danger leurs employeurs et leurs collègues. Mais le résultat est qu'ils ouvrent grand la porte aux malveillances internes ou externes qui cherchent à exploiter les failles de sécurité de ces systèmes.

Simjacking



Le 30 août 2019, les 4,2 millions d'abonnés du PDG de Twitter, Jack Dorsey, ont été exposés à un flux de messages profondément offensants, pour lequel il faut remercier un groupe de pirates informatiques appelé « Chuckling Squad ». Le groupe a eu recours au simjacking pour prendre le contrôle du numéro de téléphone de Dorsey, puis a utilisé un service de SMS acquis par Twitter pour publier les messages. Les messages offensants sont restés visibles en ligne pendant moins de dix minutes, mais des millions de personnes y ont été exposées.

Simjacking

Ce que vous devez savoir :

Le Simjacking (également connu sous le nom d'échange de cartes SIM, port-out ou fractionnement de carte SIM) entre dans la catégorie du piratage de compte et cible généralement une faiblesse dans l'authentification à deux facteurs ou la vérification en deux étapes, lorsque le deuxième facteur est un SMS ou un appel émis vers le téléphone mobile. En termes simples, on parle de simjacking lorsqu'un pirate usurpe l'identité d'une cible auprès d'un fournisseur de téléphonie mobile afin de voler son numéro de téléphone portable en le transférant sur une autre carte SIM (qui est déjà en possession du pirate informatique).

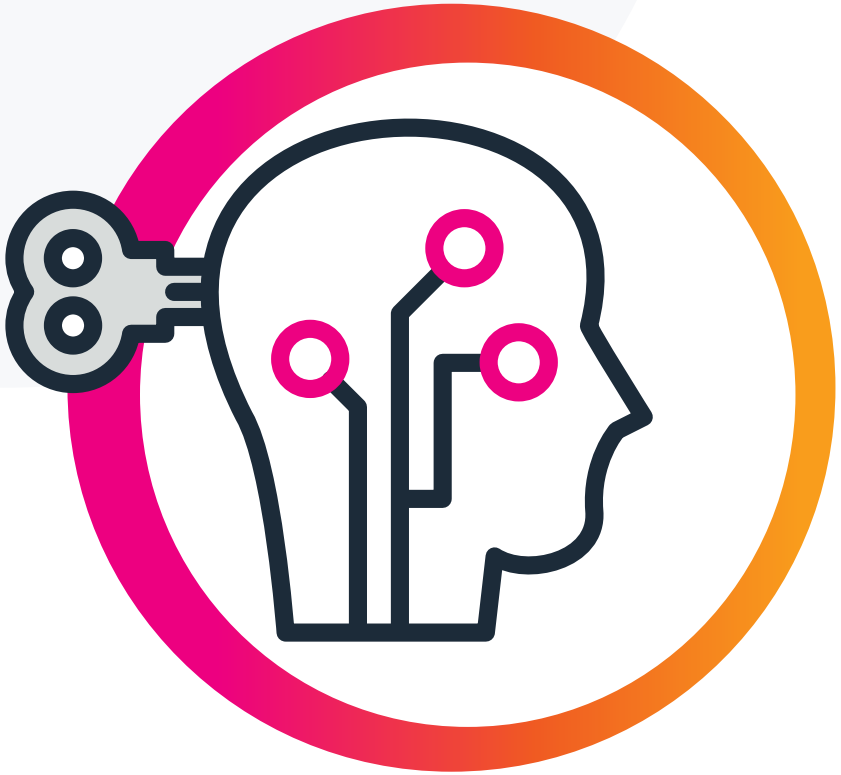
Déroulement de l'attaque :

Le pirate appelle la ligne d'assistance d'un fournisseur de services mobiles ; il se fait passer pour la cible et dit qu'il a perdu sa carte SIM. Il peut confirmer son identité car il a acquis une partie des informations personnelles de la cible (adresse, mots de passe ou numéro de sécurité sociale) via l'un des nombreux piratages de bases de données de la dernière décennie. L'employé du fournisseur de services, n'ayant aucun moyen de savoir que la personne à l'autre bout de la ligne n'est pas celle qu'elle prétend être, effectue le changement. Instantanément, ce numéro de téléphone (qui est la clé d'une grande partie de la vie numérique) est sous le contrôle de l'attaquant.

D'où vient l'attaque :

Les simjackers cherchent généralement à extorquer une ressource de grande valeur – un portefeuille de Bitcoin ou autre cryptomonnaie, ou bien un compte de réseau social important – ou à nuire à la réputation de leur victime, comme l'a fait Chuckling Squad avec Jack Dorsey. Membres de groupes organisés ou acteurs solitaires, ces pirates peuvent être basés n'importe où dans le monde.

Attaque d'ingénierie sociale



En juillet 2022, CoinsPaid, un système de paiement par cryptomonnaie a perdu 37 millions de dollars suite à une attaque d'ingénierie sociale. Les malfaiteurs ont présenté une fausse offre d'emploi à un employé existant, mais l'ont d'abord incité à installer un logiciel malveillant sur son ordinateur d'entreprise. « Vous pensez peut-être qu'une telle tentative d'installer un logiciel malveillant sur l'ordinateur d'un employé est trop grossière, mais les pirates avaient passé six mois à collecter toutes sortes d'informations sur CoinsPaid, nos collaborateurs, la structure de notre entreprise, etc. », a expliqué un représentant de l'entreprise.

Attaque d'ingénierie sociale

Ce que vous devez savoir :

L'ingénierie sociale désigne un large éventail d'activités malveillantes qui exploitent la manipulation psychologique et visent à inciter les utilisateurs à commettre des erreurs de sécurité ou à divulguer des informations sensibles. Ce qui rend l'ingénierie sociale particulièrement dangereuse, c'est qu'elle repose sur l'erreur humaine, plutôt que sur les vulnérabilités des logiciels et des systèmes d'exploitation. Les erreurs commises par des utilisateurs légitimes sont beaucoup moins prévisibles, ce qui les rend plus difficiles à identifier et à déjouer qu'une intrusion basée sur un logiciel malveillant.

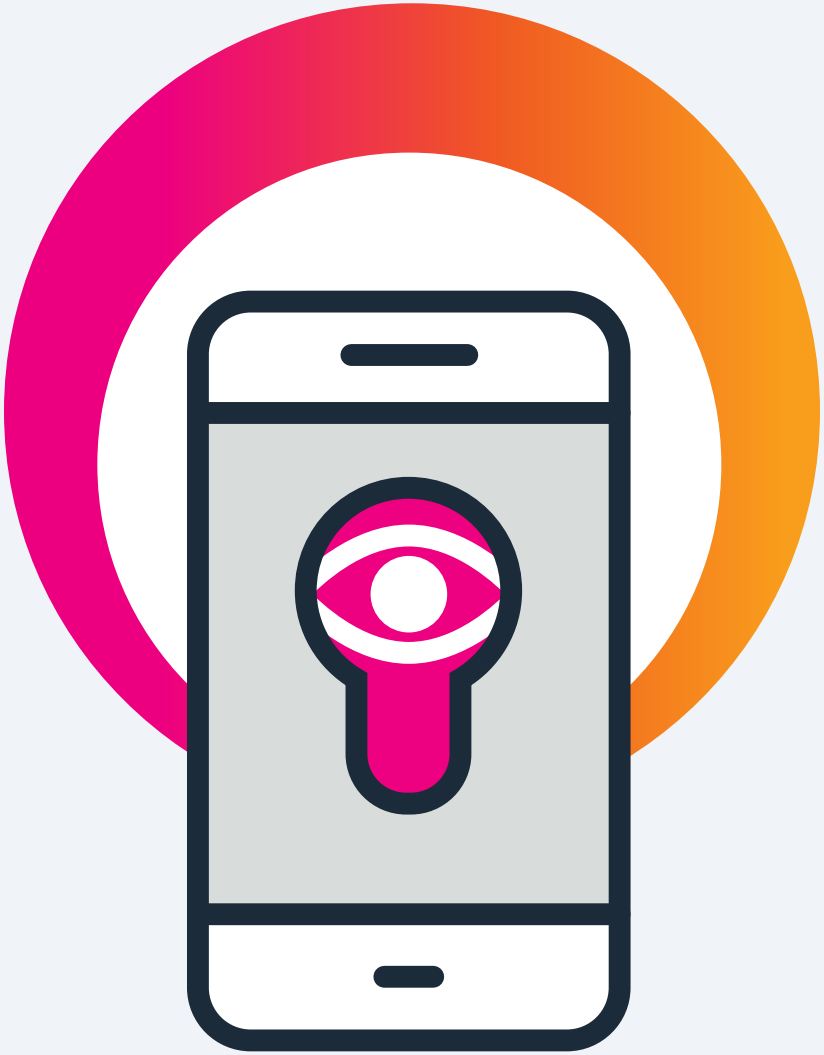
Déroulement de l'attaque :

Les attaques d'ingénierie sociale se présentent sous de nombreuses formes et peuvent être menées partout où une interaction humaine est impliquée. Un exemple d'attaque d'ingénierie sociale : le pirate commence par se renseigner sur la victime visée pour recueillir les informations de base nécessaires (points d'entrée potentiels, protocoles de sécurité faibles) pour poursuivre l'attaque. Ensuite, il gagne la confiance de la victime et l'incite à agir de manière contraire aux pratiques de sécurité, par exemple en révélant des informations sensibles ou en accordant l'accès à des ressources critiques.

D'où vient l'attaque :

L'ingénierie sociale peut prendre de nombreuses formes et avoir diverses sources et motivations. Le plus souvent, elle se présente sous la forme d'e-mails de phishing, mais pas seulement. Dans le faux-semblant, l'attaquant crée un bon prétexte pour voler des données importantes. Citons aussi l'appâtage et le quid pro quo, dans lesquels l'attaquant offre à la victime quelque chose de désirable en échange d'identifiants de connexion ; ou encore le talonnage, dans lequel un attaquant accède à une zone restreinte d'une entreprise en passant derrière un employé authentifié lorsqu'il passe les portes sécurisées.

Logiciels espions



Ce n'est un secret pour personne : les attaques de logiciels espions continuent de se produire à une fréquence alarmante. Mais une personnalité de premier plan est beaucoup plus exposée. Des responsables politiques ont annoncé que des acteurs malveillants avaient ciblé les téléphones portables du Premier ministre espagnol Pedro Sánchez et de la ministre de la Défense Margarita Robles lors de plusieurs attaques exploitant le logiciel Pegasus. Le résultat : un vol de données important sur les deux appareils et des ravages chez les administrateurs espagnols et dans les systèmes gouvernementaux.

Logiciels espions

Ce que vous devez savoir :

Un logiciel espion est un logiciel malveillant qui vise à collecter des données personnelles ou organisationnelles, à suivre ou à vendre l'activité web d'une victime (ses recherches, son historique et ses téléchargements), à capturer des informations sur les comptes bancaires et même à voler l'identité d'une cible. Il existe plusieurs types de logiciels espions, et chacun utilise une tactique unique pour suivre sa victime. En bout de ligne, les logiciels espions peuvent prendre le contrôle d'un appareil, exfiltrer des données ou envoyer des informations personnelles à une autre entité inconnue, à l'insu de leur propriétaire et sans son consentement.

Déroulement de l'attaque :

Les logiciels espions peuvent être installés sur l'appareil d'une victime par divers moyens, mais ils s'implantent généralement en dupant la cible ou en exploitant les vulnérabilités existantes. L'infection peut se produire lorsqu'un utilisateur clique négligemment dans un pop-up aléatoire, télécharge un logiciel ou une mise à jour à partir d'une source non fiable, ouvre des pièces jointes à des e-mails d'expéditeurs inconnus ou pirate des films et de la musique.

D'où vient l'attaque :

Grâce aux kits de logiciels criminels, désormais facilement disponibles, ce type d'attaque peut provenir de n'importe qui et de n'importe où. Mais le plus souvent, elles sont le fait d'organisations malveillantes cherchant à vendre les informations de leurs victimes à des tiers.

Injection SQL

Le langage de requête structuré, ou SQL (parfois prononcé « sequel »), est le langage de programmation standard utilisé pour communiquer avec les bases de données relationnelles, ces systèmes qui prennent en charge tous les sites web et applications basés sur les données sur Internet. Un pirate peut tirer parti de ce système (très courant) en saisissant une requête SQL spécifique dans le formulaire (autrement dit, en l'injectant dans la base de données), après quoi le pirate informatique peut accéder à la base de données, au réseau et aux serveurs. Et les attaques par injection SQL restent une méthode d'attaque très populaire. En août 2020, par exemple, la Freepik Company a divulgué une violation de données affectant les identifiants de plus de 8 millions d'utilisateurs à la suite d'une injection SQL dans une base de données mondiale d'icônes personnalisables. Cette attaque a permis aux malfaiteurs de dérober les identifiants et les informations personnelles des utilisateurs.

Injection SQL

Ce que vous devez savoir :

L'injection SQL vise à manipuler ou détruire des bases de données à l'aide d'instructions SQL malveillantes. Les instructions SQL contrôlent la base de données de votre application web et peuvent être utilisées pour contourner les mesures de sécurité si les saisies utilisateur ne sont pas correctement filtrées.

Déroulement de l'attaque :

Une attaque par injection SQL consiste à insérer ou « injecter » une requête SQL via les données d'entrée du client vers l'application. Un exploit d'injection SQL réussi peut lire des données sensibles de la base de données, modifier les données de la base de données, exécuter des opérations d'administration sur la base de données, récupérer le contenu d'un fichier donné présent sur le système de fichiers du SGBD et, dans certains cas, envoyer des commandes au système d'exploitation.

D'où vient l'attaque :

Étant donné qu'une grande partie d'Internet repose sur des bases de données relationnelles, les attaques par injection SQL sont extrêmement courantes. Rechercher « injection » dans la base de données Common Vulnerabilities and Exposures renvoie 15 000 résultats.

Attaques de la chaîne logistique

Les attaques SolarWinds, que certains experts qualifient de pire série d'attaques de cybersécurité de l'histoire, offrent un excellent exemple des dommages que peut infliger une attaque de la chaîne logistique. En 2020, des attaquants sophistiqués qu'on soupçonne d'avoir agi sur l'injonction des services de renseignement russes, ont compromis le logiciel SolarWinds. Ils lui ont intégré un logiciel malveillant qui a ensuite été déployé via une mise à jour du produit et a installé une porte dérobée indétectable dans les réseaux de tous clients de la plateforme SolarWinds Orion. Jusqu'à 18 000 clients ont installé les mises à jour qui les ont rendus vulnérables, y compris des sociétés Fortune 500 et plusieurs agences du gouvernement américain. Comme l'a déclaré Tim Brown, Vice-président de la sécurité chez SolarWinds, « c'est vraiment votre pire cauchemar ».

Attaques de la chaîne logistique

Ce que vous devez savoir :

Une attaque de la chaîne logistique est une puissante cyberattaque qui peut traverser les défenses de sécurité les plus sophistiquées par l'intermédiaire de fournisseurs tiers légitimes. Comme les fournisseurs ont besoin d'accéder à des données sensibles pour s'intégrer aux systèmes internes de leurs clients, les cyberattaques qui les visent exposent aussi souvent les données de leurs clients. Et comme les fournisseurs stockent les données sensibles de nombreux clients, une seule attaque de la chaîne logistique permet à des pirates d'accéder aux données sensibles de nombreuses entreprises, dans de nombreux secteurs. La gravité des attaques de la chaîne logistique ne saurait être surestimée. Et la récente vague d'attaques de ce genre laisse penser que cette méthode est aujourd'hui à la mode parmi les acteurs étatiques.

Déroulement de l'attaque :

Une attaque de la chaîne logistique utilise des processus légitimes et fiables pour obtenir un accès complet aux données des entreprises en ciblant le code source du logiciel, les mises à jour ou les processus de compilation d'un fournisseur. Ces attaques sont difficiles à détecter car elles se produisent en décalage par rapport à la surface d'attaque. Les fournisseurs compromis transmettent alors involontairement des programmes malveillants au réseau de leurs clients. Les victimes peuvent être atteintes par le biais de mises à jour de logiciels tiers, d'installeurs d'applications ou de programmes malveillants présents sur des appareils connectés. Une mise à jour logicielle peut infecter des milliers d'entreprises avec un minimum d'efforts de la part des pirates, qui disposent désormais d'un accès « légitime » pour se déplacer latéralement dans leurs réseaux.

D'où vient l'attaque :

Les attaques de la chaîne logistique sont des attaques sophistiquées à grande échelle perpétrées par des acteurs de haut profil, souvent parrainés par des États-nations et motivés par des idéologies, bien que le gain financier soit également une motivation importante.

Activités de stockage cloud suspectes

Selon le Rapport d'investigations sur les fuites de données (DBIR) 2022 de Verizon, 82 % des violations impliquent un « élément humain », et les « erreurs diverses » liées aux mauvaises configurations de stockage cloud sont en hausse. Le rapport Données sensibles dans le cloud révèle également que la majorité (67 %) des professionnels de la sécurité et de l'informatique stockent des données sensibles dans des environnements de cloud public. Pourtant, un tiers des répondants disent avoir peu ou pas du tout confiance dans leur capacité à protéger les données sensibles dans le cloud.

Ce type de négligence technique et professionnelle – qu'il s'agisse d'un défaut de configuration dans une base de données ou d'un manque de savoir-faire des équipes de sécurité – est précisément la raison pour laquelle les comptes cloud sont devenus une cible privilégiée à l'ère du télétravail.

Activités de stockage cloud suspectes

Ce que vous devez savoir :

Maintenant que les données sont largement dispersées dans le cloud, trop souvent de façon erratique d'ailleurs, les attaquants ont mille et une opportunités de trouver et d'exploiter des vulnérabilités connues et inconnues. C'est particulièrement le cas à l'heure où les organisations migrent précipitamment vers le cloud et risquent de ce fait de mal configurer certains contrôles de sécurité.

Pour compliquer encore les choses, les actifs et les applications doivent être sécurisés selon le modèle de responsabilité partagée : les fournisseurs de services cloud (CSP) couvriront certains éléments, processus et fonctions, mais le client est ensuite responsable de sécuriser ses données propriétaires, son code et tout autre actif important, conformément à l'Alliance de sécurité du cloud (CSA). Mais lorsque l'on se soustrait à cette responsabilité, les pirates informatiques profitent inévitablement de la situation.

Déroulement de l'attaque :

Dans une attaque contre le stockage cloud, un acteur malveillant prend pied dans l'infrastructure cloud de l'organisation en profitant de paramètres de sécurité incorrects, laxistes ou inexistants. Une fois à l'intérieur, ils désactivent certains contrôles, comme la supervision des accès. Ils peuvent créer de nouveaux comptes pour obtenir un accès durable, mais aussi exécuter des commandes inhabituelles pour le type d'utilisateur ou de système en question. Ils peuvent également modifier les politiques de certains compartiments de stockage pour rendre les fichiers d'une organisation accessibles au public et exfiltrer les données. Heureusement, il s'agit à chaque fois d'événements notables, faciles à suivre et à identifier dans les journaux d'audit du CSP.

D'où vient l'attaque :

Pour donner un exemple, ce type d'attaque peut se produire si un développeur exécute une instance obsolète d'une fonction ou d'une application cloud. Cette instance pourrait contenir des vulnérabilités connues, qui ont depuis été corrigées dans une version ultérieure. Mais si une version ancienne du programme est présente, les adversaires peuvent l'utiliser comme point d'entrée avant de se déplacer latéralement dans l'environnement cloud.

Typosquatting

Noblox.js est un wrapper pour l'API Roblox, une fonction utilisée par de nombreux joueurs pour automatiser les interactions avec la célèbre plateforme de jeu Roblox. Et le logiciel semble attirer un nouveau public. En 2021, des pirates ont lancé des attaques de typosquatting via le paquet noblox.js en important des paquets aux noms similaires et chargés de ransomwares dans un registre de bibliothèques JavaScript open source, puis en distribuant les fichiers infectés via un service de messagerie. Mais depuis septembre 2021, le joueur Josh Muir et plusieurs autres ont activement poursuivi les pirates et tenté d'empêcher la prolifération des ransomwares via le paquet noblox.js et d'autres bibliothèques de codes, et d'éviter d'autres attaques contre la communauté des joueurs.

Typosquatting

Ce que vous devez savoir :

Le typosquatting est une attaque de phishing dans laquelle les attaquants utilisent des noms de domaine ressemblant à un ou deux caractères près à un nom de domaine connu. Bien souvent, les coupables ne cherchent pas réellement à mener une attaque : ils espèrent plutôt que l'entreprise, la marque ou la personne visée leur rachètera le domaine. Mais il arrive aussi qu'ils créent des domaines malveillants qui ressemblent beaucoup à ceux de marques légitimes.

Déroulement de l'attaque :

Cette démarche n'a rien de sophistiqué : un jeune de 14 ans peut tout à fait enregistrer un domaine et y installer du code malveillant. Dans la forme malveillante de l'attaque, un pirate informatique tente généralement d'utiliser de faux domaines pour inciter les utilisateurs à interagir avec une infrastructure malveillante.

Même pour les utilisateurs qui connaissent bien ces risques, l'erreur humaine est toujours possible, et la plupart des malfaiteurs le savent très bien. Ils essaieront forcément d'en profiter, en menant des campagnes de phishing basées sur des adresses similaires, en intégrant des domaines contrefaits de commande et contrôle à des logiciels malveillants, et en hébergeant du contenu malveillant sur des domaines qui imitent fidèlement les serveurs d'entreprise.

D'où vient l'attaque :

L'origine de cette attaque n'a pas autant d'importance que sa cible. Cette attaque cible généralement les internautes non avertis qui ne remarqueront pas qu'il manque une lettre ou deux à l'URL de leur domaine préféré. Et comme cette attaque est extrêmement simple (il peut parfois suffire d'enregistrer un nom de domaine), elle peut provenir de presque n'importe où.

Attaques au point d'eau

Dans ce qui est devenu un classique de l'attaque au point d'eau, l'exploitant d'une installation d'épuration et de traitement des eaux usées de Floride a hébergé par inadvertance un code malveillant sur son site web, qui a été à l'origine du piratage de l'usine d'épuration d'Oldsmar en 2021. Les cybercriminels à l'origine de l'attaque semblaient viser un public bien précis : le code malveillant retrouvé sur le site de l'exploitant ciblait d'autres services de traitement des eaux de Floride et, sans surprise, avait été consulté par un navigateur de la ville d'Oldsmar le jour du piratage. Le site web n'a pas lancé de code d'exploitation : il a plutôt injecté un logiciel malveillant qui fonctionnait comme un script d'énumération et de relevé d'empreinte digitale, afin de glaner diverses informations auprès des visiteurs du site – système d'exploitation, type de navigateur, fuseau horaire et présence d'une caméra et d'un microphone. Ces informations étaient ensuite envoyées à une base de données distante hébergée sur un site d'application Heroku qui stockait également le script.

Attaques au point d'eau

Ce que vous devez savoir :

Dans l'attaque au point d'eau, vos adversaires compromettent l'ordinateur d'un utilisateur au moment où il visite un site web infecté par des malwares conçus pour infiltrer votre réseau pour voler des données ou des actifs financiers. Il s'agit essentiellement d'une attaque zero-day : le but est d'infecter votre système informatique pour obtenir l'accès à votre réseau afin d'en tirer un gain financier ou de voler des informations propriétaires.

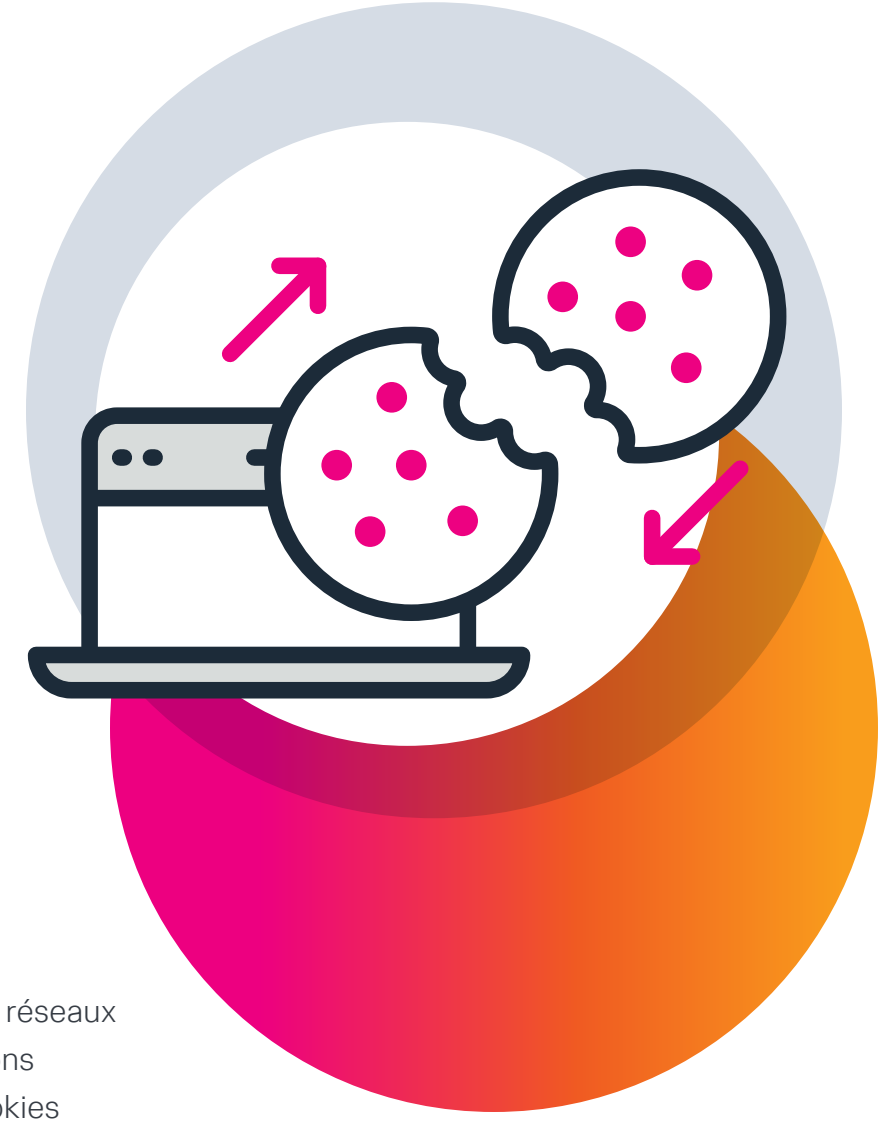
Déroulement de l'attaque :

Dans un premier temps, les adversaires vont déterminer quels sites web les utilisateurs visitent fréquemment, puis rechercher des faiblesses à exploiter. En exploitant les failles identifiées, 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 puis de se déplacer latéralement vers d'autres systèmes.

D'où vient l'attaque :

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, l'Europe de l'Est et la Chine. En 2018, une attaque au point d'eau d'envergure nationale a été attribuée au groupe de menace chinois connu sous le nom de LuckyMouse (alias Iron Tiger, EmissaryPanda, APT 27 ou encore Groupe de menace 3390), connu pour cibler les secteurs de l'administration, de l'énergie et de la fabrication par différents types d'attaques, y compris des assauts au point d'eau.

Vol de cookies de session web



Presque toutes les applications web que nous utilisons, qu'il s'agisse de réseaux sociaux, de plateformes de streaming, de services cloud ou d'applications financières, fonctionnent avec des cookies d'authentification. Si les cookies facilitent considérablement notre expérience sur le Web, ils créent également une vulnérabilité qui peut être exploitée avec beaucoup d'impact. Fin 2019, un groupe de pirates informatiques disparates s'est fait un nom en exécutant un logiciel de vol de cookies pour détourner diverses chaînes YouTube. Ils attiraient ensuite les propriétaires sans méfiance avec de fausses offres pour diffuser des escroqueries basées sur les cryptomonnaies ou vendre les comptes au plus offrant.

Vol de cookies de session web

Ce que vous devez savoir :

Lorsqu'un attaquant réussit à voler des cookies de session, il peut réaliser toutes les opérations que l'utilisateur d'origine est autorisé à entreprendre. C'est particulièrement dangereux en entreprise, car les cookies peuvent être utilisés pour reconnaître des utilisateurs dans les systèmes d'authentification unique. Celui qui se les approprie a potentiellement accès à toutes les applications web que la victime peut utiliser : systèmes financiers, dossiers des clients et systèmes commerciaux contenant des secrets industriels potentiels.

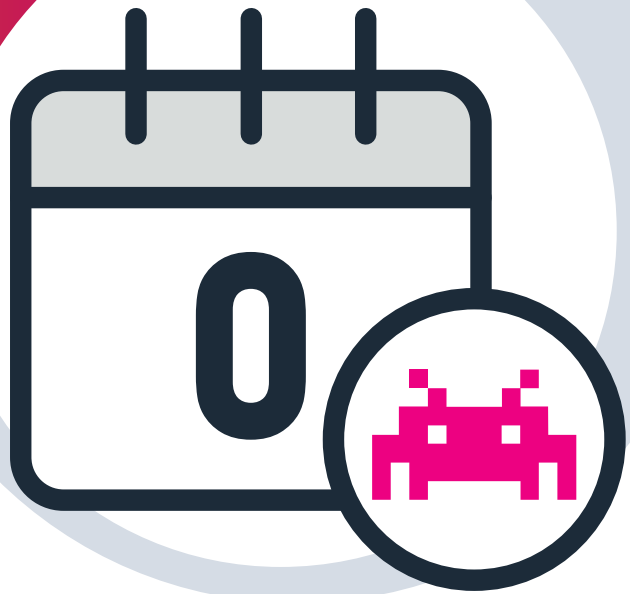
Déroulement de l'attaque :

Quand un utilisateur accède à un service et valide son identité, un cookie est stocké sur sa machine pendant une période prolongée afin qu'il n'ait pas à se reconnecter régulièrement. Un malfaiteur peut voler des cookies de session web à l'aide de logiciels malveillants, puis les importer dans un navigateur qu'il contrôle afin d'utiliser le site ou l'application aussi longtemps que le cookie de session est actif. Une fois connecté au site, il peut accéder à des informations sensibles, lire des e-mails ou effectuer toutes les opérations entrant dans le champ d'autorisation du compte de la victime.

D'où vient l'attaque :

Le vol de cookies est généralement réalisé par le biais de logiciels malveillants qui copient les cookies de la victime et les envoient directement à l'attaquant. Le logiciel malveillant peut être installé sur la machine de la victime par différents moyens que nous avons déjà vus : phishing, virus macro, XSS, etc. De nombreux pirates se livrant au vol de cookies appartiennent à de vastes réseaux basés en Russie et en Chine. On a ainsi découvert que les acteurs à l'origine de l'attaque de YouTube, par exemple, faisaient partie d'un groupe de pirates connectés via un forum russophone.

Exploit zero-day



Il n'est pas surprenant que le nombre de failles zero-day continue d'augmenter. Mais tous les records ont été battus en 2021 : au total, ce sont 58 nouvelles menaces zero-day qui ont été exploitées, contre 25 en 2020 et 21 en 2019. Et il est clair que les enjeux augmentent avec les systèmes critiques qui deviennent toujours plus connectés. Ces dernières années, des pirates ont utilisé des menaces d'attaque zero-day pour compromettre les serveurs Microsoft et installer des logiciels espions avancés sur les smartphones afin d'espionner des journalistes, des politiciens et des militants des droits de l'homme.

Exploit zero-day

Ce que vous devez savoir :

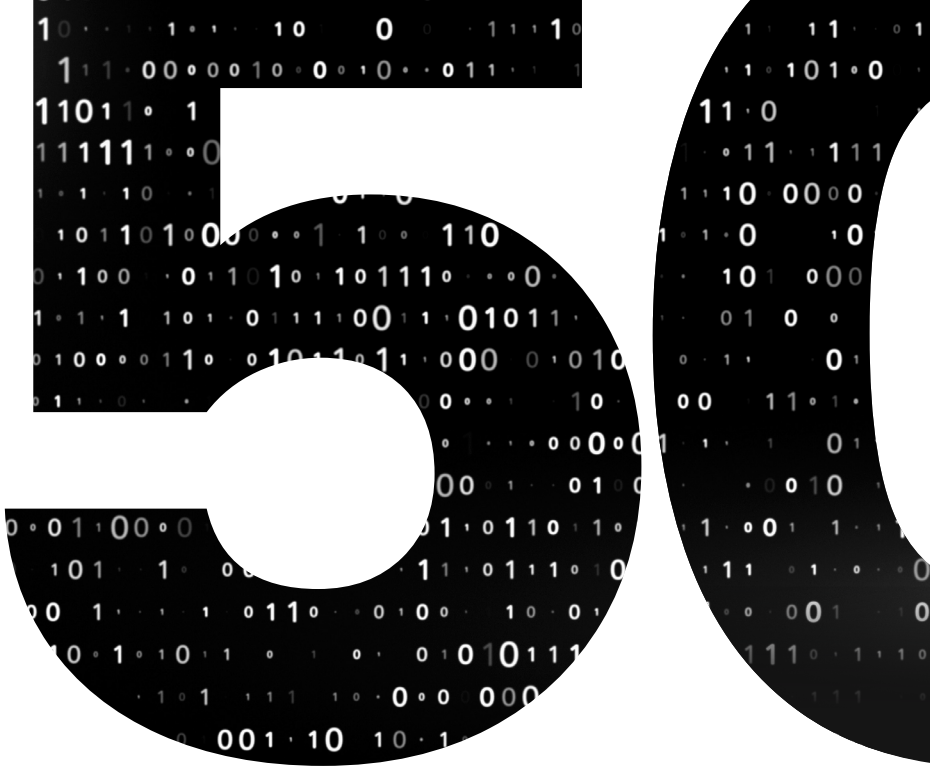
Au départ, une vulnérabilité zero-day est une faille. Il s'agit d'une faiblesse au sein d'un logiciel ou d'un réseau informatique dont les pirates profitent peu de temps après son lancement, voire immédiatement après. Son nom fait référence au fait que ces vulnérabilités sont souvent exploitées le jour même.

Déroulement de l'attaque :

L'attaque zero-day se produit dès que la vulnérabilité est exploitée. La nature de la vulnérabilité influera sur la mise en œuvre de l'attaque, mais on observe un modèle récurrent. Tout d'abord, le pirate (ou le groupe de pirates) analyse la base de code à la recherche de vulnérabilités. Une fois qu'il a trouvé la faille, il crée un code qui exploite la vulnérabilité. Il infiltre ensuite le système (en utilisant une ou plusieurs des méthodes décrites ici) et l'infecte avec son code malveillant avant de lancer l'exploit.

D'où vient l'attaque :

La généralisation de la technologie a entraîné une croissance exponentielle des attaques zero-day. Ces attaques peuvent apparemment être lancées de n'importe où, mais elles proviennent souvent d'États-voyous ou de régions qui abritent d'importants réseaux cybercriminels.



En savoir plus.

Découvrez comment contrecarrer d'innombrables menaces et **moderniser votre SOC** grâce à la **sécurité axée sur l'analyse de Splunk**.

23-337536-Splunk-Top 50 Cybersecurity Threats-EB-110

splunk>