TOP 5

des menaces de cybersécurité

splunk>

Sommaire

Avant-propos

Aujourd'hui plus que jamais, la cybersécurité est essentielle pour notre avenir. Après tout, elle assure la protection de toutes les technologies dont nous dépendons aujourd'hui : des services bancaires et de l'e-commerce au développement de médicaments et de vaccins, ou plus simplement pour assurer le fonctionnement de nos services de streaming préférés.

Pourtant, suite aux migrations massives vers le cloud et à la transformation numérique, de nombreuses organisations n'ont pas encore réussi à optimiser leurs opérations de sécurité à cause de plusieurs défis de taille : un paysage des menaces en évolution constante qui nous oppose à des malfaiteurs créatifs et bien financés ; la complexité croissante des environnements hybrides et multicloud ; les équipes de sécurité qui s'enlisent dans des tâches monotones et des processus manuels interminables ; et enfin les silos de données causés par la prolifération d'outils utilisés au sein de nos organisations, source d'inefficacité et d'angles morts.

Ces quatre défis soulignent une réalité : la sécurité est une question de données. C'est pourquoi une approche orientée données de la sécurité est essentielle : nous procurer les bonnes informations au bon moment et assurer le lien entre les outils et les équipes au milieu du bruit et de la complexité. Une solution orientée analyse s'appuyant sur la visibilité de bout en bout et exploitant le machine learning (ML) est nécessaire pour réussir. Ces fonctionnalités avancées offrent une vision complète sur votre environnement, mais permettent aussi de diminuer l'intervention humaine dans les opérations et de passer à une cyberdéfense automatisée et renforcée.

Comment ? En formant et en contextualisant des ensembles de données extrêmement complexes, en réagissant plus rapidement aux menaces grâce à l'automatisation du tri, de l'investigation et de la réponse aux alertes, et en détectant les comportements anormaux grâce à des modèles et à des algorithmes de ML prêts à l'emploi. Tout cela aide les organisations à améliorer leur cyberrésilience, c'est-à-dire leur capacité à anticiper et à s'adapter aux compromissions ou aux attaques ciblant leurs ressources, afin de pouvoir automatiser plus efficacement leurs opérations de sécurité et protéger leur activité, tout en stimulant la croissance et l'innovation.

Chez Splunk, les possibilités offertes par les données pour assurer un avenir plus serein et sûr nous enthousiasment. Mais pour y arriver, nous devons être fin prêts. Nous devons savoir ce qui nous attend, notamment les menaces qui rôdent. C'est pourquoi nous avons créé cet e-book qui recense les plus grandes menaces de cybersécurité : pour que vous puissiez mieux identifier les différents types d'attaques, réduire les risques et renforcer votre organisation.

Gary Steele
PDG, Splunk Inc.

Il nous faudra encore un bon moment avant de pouvoir véritablement mesurer l'impact de la pandémie sur le paysage mondial de la sécurité de l'information (InfoSec). Pendant cette période, il s'est produit plus d'événements et d'évolutions qu'au cours de la carrière de nombreux professionnels de la sécurité avant 2020. Il faut se rendre à l'évidence : les défis auxquels nous faisons face sont plus importants que jamais.

Le syndrome de la « Grande démission » et les classiques burn out noircissent encore un peu plus le tableau, au moment où le monde de la sécurité a plus que jamais besoin d'attirer et de fidéliser les talents. Et ceux qui tiennent encore bon sont submergés d'alertes. Ils doivent consacrer trop de leur temps à des tâches manuelles répétitives, qui ne font qu'affecter encore un peu plus leur moral. De plus, ils manquent d'informations et de visibilité sur les données dont ils ont besoin pour comprendre les plus grandes menaces pesant sur votre organisation.

Mais l'espoir demeure. La plupart des plateformes d'opérations de sécurité n'ont pas réussi à gérer la sécurité en tant que problème de données, et c'est dans ce domaine que des solutions existent pour les professionnels de la sécurité.

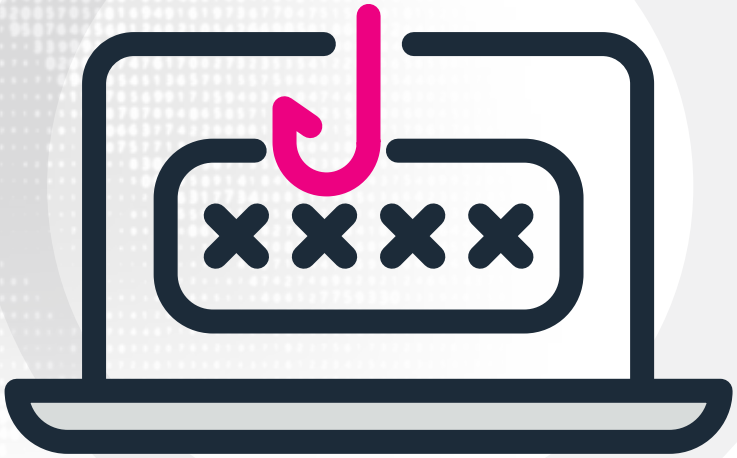
La capacité à mettre en place une réponse de cybersécurité efficace est directement liée à la quantité et à la qualité des données collectées, analysées et exploitées dans la lutte pour réduire les risques commerciaux.

Se rendant compte que l'avenir est incertain, les organisations investissent pour renforcer leur résilience, résister aux dernières menaces et en sortir grandies. Dans ce contexte, résilience est synonyme de avec flexibilité, rapidité, préparation, et proactivité. Les organisations résilientes disposent d'une base solide de technologies et de données, qui leur permet de traiter rapidement n'importe quel problème.

Les équipes de sécurité résilientes mettent en place des solutions de cybersécurité pour protéger chaque aspect de l'entreprise, stimuler l'innovation et renforcer l'organisation. Les équipes résilientes relèvent les défis en plaçant les données au cœur de toutes leurs activités. Et cela se traduit dans leurs résultats. Les opérations de sécurité orientées données peuvent réduire les risques de failles de sécurité, de vol de propriété intellectuelle et de fraude jusqu'à 70 %.

C'est pour cela qu'il est important de savoir quelles sont les menaces pour votre organisation et c'est précisément ce que nous allons vous expliquer dans cet e-book. D'après les recherches de la Splunk Threat Research Team, nous allons vous présenter 50 des plus grandes menaces de cybersécurité, et quelques menaces supplémentaires, pour aider les professionnels de la sécurité à sécuriser les environnements dans lesquels nous travaillons au quotidien.

Appropriation de compte



L'appropriation de compte est considérée comme l'un des moyens les plus nuisibles d'accéder à un compte utilisateur. L'attaquant se fait généralement passer pour un client, un utilisateur ou un employé authentique, et obtient finalement l'accès aux comptes de la personne dont il usurpe l'identité. Plus effrayant encore, les informations d'identification des utilisateurs peuvent provenir du deep web et être exploitées sur des sites d'e-commerce à l'aide de bots et d'autres outils automatisés de saisie rapide et facile.

FitBit a même été victime de ce type d'attaque lorsque des pirates ont exposé les informations d'identification des comptes clients, modifié l'e-mail avec lequel ils se sont inscrits, puis appelé le service clientèle pour se plaindre du dispositif et obtenir un remplacement sous garantie.

Appropriation de compte

Ce que vous devez savoir :

Par rapport à un simple vol de carte ou d'informations d'identification, l'appropriation de compte est plus subreptice et permet à l'attaquant d'utiliser la carte dérobée au maximum avant de se faire repérer pour activité suspecte. Les banques, les grandes places de marché et les services financiers comme PayPal en sont des cibles courantes, et tout site web nécessitant une connexion est exposé à ce type d'attaque.

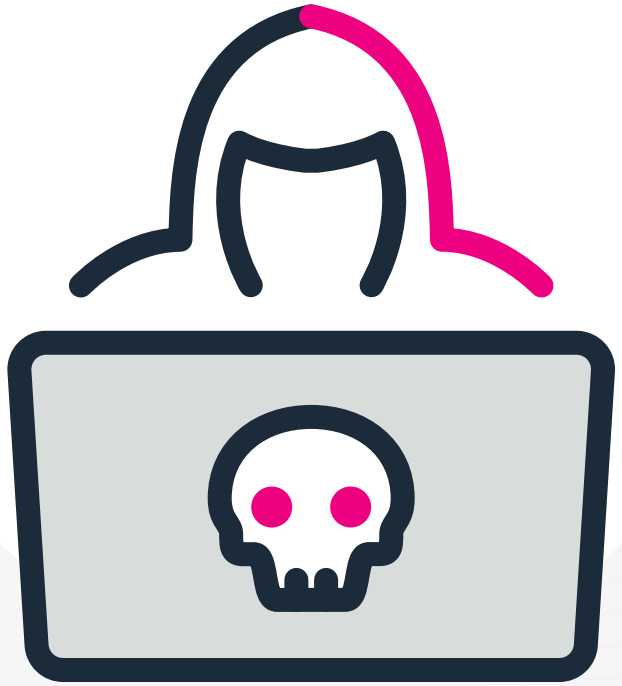
Comment l'attaque se produit :

Les plus courantes incluent les applications avec vérification en un clic basées sur un proxy, les attaques de botnet par force brute, le phishing et les logiciels malveillants. D'autres méthodes incluent la fouille de poubelle pour trouver des informations personnelles dans le courrier jeté et l'achat pur et simple de listes de « Fullz », un terme d'argot désignant des ensembles complets d'informations d'identification vendus sur le marché noir. Une fois le profil de la victime acheté ou créé, un voleur d'identité peut utiliser les informations pour déjouer un système d'authentification basé sur les connaissances.

D'où provient l'attaque :

Un volume énorme de nos transactions, financières et autres, s'opère en ligne. Pour les cybercriminels, l'acquisition d'informations d'identification et d'informations personnelles (comme les numéros de sécurité sociale, les adresses de domicile, les numéros de téléphone, les numéros de carte de crédit et autres informations financières) est une activité lucrative, qu'ils choisissent de vendre les informations acquises ou de les utiliser à leur propre compte. En tant que telles, ces types d'attaques peuvent provenir de n'importe où dans le monde.

Menaces persistantes avancées



Lors de l'une des failles de sécurité les plus importantes de l'histoire des États-Unis, l'attaque contre l'Office of Personnel Management (OPM), des experts de la sécurité ont découvert que des malfaiteurs parrainés par le gouvernement chinois avaient utilisé une menace persistante avancée.

L'attaque contre l'OPM a compromis plus de 4 millions de dossiers, y compris des informations sur les employés actuels, anciens et potentiels du gouvernement fédéral, ainsi que les membres de leur famille, des contacts étrangers et même des informations psychologiques.

Menaces persistantes avancées

Ce que vous devez savoir :

Une menace persistante avancée (APT) est une menace dissimulée très élaborée sur un système ou un réseau informatique dans lequel un utilisateur non autorisé parvient à entrer par effraction, à éviter la détection et à obtenir des informations pour des motifs commerciaux ou politiques. Généralement menée par des criminels ou des États-nations, elle vise principalement le gain financier ou l'espionnage politique. Alors que l'on continue d'associer les APT à des États-nations qui tentent de voler des secrets gouvernementaux ou industriels, les cybercriminels sans affiliation particulière ont également recours aux APT pour dérober des données ou de la propriété intellectuelle.

Comment l'attaque se produit :

Une APT a généralement recours à des tactiques très avancées, y compris la collecte d'une grande quantité d'informations, et à des méthodes moins sophistiquées pour s'insérer dans le système (logiciel malveillant et harponnage, p. ex.). Diverses méthodologies sont utilisées pour compromettre la cible et pour conserver l'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 apprenant quels comptes disposent des autorisations appropriées, puis en les exploitant pour compromettre les actifs. Les pirates qui ont recours à l'APT installeront également des programmes de porte dérobée (comme des chevaux de Troie) sur les ordinateurs compromis de l'environnement exploité. Cette installation a pour but de leur assurer de pouvoir revenir, même si les informations d'identification sont modifiées ultérieurement.

D'où provient l'attaque :

La plupart des groupes d'APT sont affiliés ou sont des agents gouvernementaux d'États souverains. Un APT peut également être un pirate professionnel travaillant à temps plein pour les personnes précitées. Ces organisations de piratage parrainées par l'État possèdent généralement les ressources et la capacité nécessaires pour étudier de près leur cible et déterminer le meilleur point d'entrée.

Attaques Amazon Web Services (AWS)

Le nombre d'attaques créatives sur les environnements virtuels a explosé avec l'essor du cloud computing. Et en tant que l'un des plus grands fournisseurs de services cloud, Amazon Web Services a très clairement connu son lot de menaces.

Plusieurs vulnérabilités menacent la sécurité des fournisseurs cloud. Par exemple, une entreprise de marketing numérique n'a pas protégé par mot de passe son bucket Amazon S3 lorsqu'elle a fait faillite. Cette erreur a permis l'exposition des données personnelles de 306 000 personnes.

La fuite a dévoilé 50 000 fichiers, soit 32 Go de noms, prénoms, localisations, adresses e-mails, numéros de téléphone et de mots de passe non chiffrés de clients tels que Patrón Tequila.

Attaques Amazon Web Services (AWS)

Ce que vous devez savoir :

Le modèle de « responsabilité partagée » d'Amazon indique qu'AWS est responsable de l'environnement extérieur aux machines virtuelles mais que le client est responsable de la sécurité à l'intérieur du conteneur S3.

Cela signifie que les menaces qui profitent de vulnérabilités engendrées par de mauvaises configurations et des erreurs de déploiement sont devenues un problème encore plus important depuis que les entreprises ont adopté en masse les technologies cloud et que les organisations sont responsables de la sécurisation de leur environnement. Et d'autres menaces pèsent également sur les clients AWS.

Comment l'attaque se produit :

Une attaque sur une instance AWS peut survenir de bien des façons. La transition rapide vers le cloud entraînée par la pandémie de COVID-19 a augmenté le nombre de menaces pour les fournisseurs cloud.

Il est important de faire preuve de vigilance pour des activités qui peuvent être aussi banales qu'un comportement suspect au sein d'un environnement AWS. D'autres activités à suivre sont l'accès aux données S3 depuis un lieu inhabituel ou par un utilisateur inconnu.

Il est également important de superviser et de contrôler les accès à l'infrastructure AWS de l'organisation. La détection des connexions suspectes à l'infrastructure AWS constitue un bon point de départ pour les investigations. Des actions telles que les comportements abusifs liés à des informations d'identification compromises, peuvent entraîner des pertes financières directes car les utilisateurs sont facturés pour toutes les instances EC2 créées par le malfaiteur.

D'où provient l'attaque :

En raison de la diversité des services hébergés sur AWS et des nouveaux types de menaces cloud apparaissant chaque jour, ces attaques peuvent pratiquement venir de n'importe où et de n'importe qui.

Jeton d'accès aux applications

Pawn Storm, un groupe d'espionnage actif et agressif, a recours à différentes stratégies pour obtenir des informations de leurs cibles. L'une de ces méthodes consistait notamment à détourner l'authentification ouverte (OAuth) dans les schémas d'ingénierie sociale avancés pour cibler des utilisateurs de haut niveau de la messagerie web gratuite.

Le groupe a également lancé des attaques de phishing agressives contre des organisations telles que la Convention nationale démocrate (DNC), l'Union chrétienne-démocrate d'Allemagne (CDU), le parlement et le gouvernement de Turquie, le parlement du Monténégro, l'Agence mondiale antidopage (AMA), Al Jazeera et bien d'autres encore.

Ils continuent d'utiliser plusieurs applications malveillantes qui détournent les jetons d'accès OAuth pour accéder aux comptes de messagerie cibles, notamment Gmail et Yahoo Mail.

Jeton d’accès aux applications

Ce que vous devez savoir :

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

Comment l’attaque se produit :

Les attaquants peuvent utiliser des jetons d’accès aux applications pour contourner le processus d’authentification habituel 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 informations d’identification.

D’où provient l’attaque :

Les jetons d’accès compromis peuvent être utilisés comme étape initiale pour compromettre d’autres services. Par exemple, si un jeton autorise l’accès à la messagerie principale d’une victime, l’attaquant peut potentiellement obtenir un accès à tous les autres services auxquels la cible s’abonne en déclenchant des routines de mot de passe oublié. L’accès direct à l’API via un jeton réduit à néant l’efficacité d’un deuxième facteur d’authentification et peut être insensible aux contre-mesures telles que la modification des mots de passe.

Fraude au paiement

Zelle est un service financier qui permet aux clients d'envoyer facilement de l'argent à leurs amis et à leur famille. Pourtant, les caractéristiques qui font de Zelle un service rapide et efficace pour le transfert de fonds sont *aussi* exploitées par des cyber-voleurs à des fins pécuniaires. Les pirates et les escrocs utilisent le système pour dérober des fonds aux consommateurs dans le cadre de stratagèmes de fraude aux paiements, vidant parfois l'intégralité de comptes bancaires.

Ce que vous devez savoir :

La fraude au paiement englobe tout type de transaction frauduleuse ou illégale dans laquelle le cybercriminel détourne les fonds de consommateurs. Et ces mécanismes fonctionnent : selon les données récentes de la FTC, les consommateurs ont déclaré plus d'un milliard de dollars de perte en lien avec des plaintes pour fraude de janvier 2021 à mars 2022.

Comment l'attaque se produit :

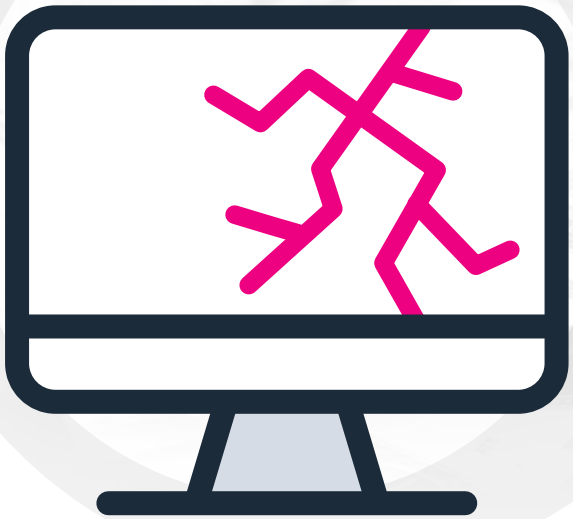
Cette attaque amène un grand nombre d'utilisateurs à payer à plusieurs reprises des sommes d'argent faibles ou raisonnables afin qu'ils ne remarquent pas l'arnaque. Dans ce stratagème, les attaquants envoient des factures frauduleuses à l'apparence authentique demandant aux clients de transférer des fonds à partir de leurs comptes.

Sachant que la plupart des clients utilisent régulièrement des services numériques payants, les attaquants comptent sur le fait que leurs cibles supposeront à tort que la facture frauduleuse concerne un service qu'ils utilisent réellement. Les consommateurs initient alors un transfert de fonds ou un paiement par carte de crédit pour payer la fausse « facture ».

D'où provient l'attaque :

Les organisations de fraude au paiement sont issues du monde entier, y compris des États-Unis. Elles proviennent généralement d'attaquants disposant des ressources, de la bande passante et de la technologie nécessaires pour créer des factures frauduleuses qui semblent réelles. Comme l'hameçonnage, la fraude au paiement cible généralement une population large et aléatoire d'individus.

Attaque par force brute



Lors d'une attaque par force brute désormais tristement célèbre, plus de 90 000 comptes PlayStation et Sony Online Entertainment ont été compromis en 2011. Les pirates ont tenté d'innombrables combinaisons de nom d'utilisateur et de mot de passe à partir d'un tiers non identifié et ont fini par piller les informations personnelles des comptes des membres.

En 2013, le Club Nintendo, désormais supprimé, a également été victime du même type d'attaque : des pirates ont exécuté une attaque coordonnée contre plus de 15 millions de membres et sont parvenus à s'introduire dans plus de 25 000 comptes de membres du forum. Tous les comptes compromis ont été suspendus jusqu'à ce que l'accès ait été restitué aux propriétaires légitimes, mais la réputation de la marque avait déjà été entachée.

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, un serveur ou un compte protégé par mot de passe, car l'attaquant essaie simplement des combinaisons de noms d'utilisateur et de mots de passe jusqu'à réussir à entrer (si tant est qu'il y parvienne ; un mot de passe à six caractères a des milliards de combinaisons potentielles).

Comment l'attaque se produit :

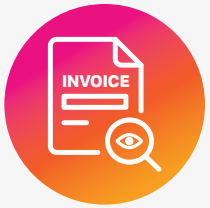
L'attaque par force brute la plus basique est une attaque par dictionnaire, dans laquelle l'attaquant utilise systématiquement un dictionnaire ou une liste de mots et en teste chaque entrée jusqu'à ce qu'il trouve une correspondance. Certains vont même jusqu'à ajouter aux mots des symboles et des chiffres, ou utiliser des dictionnaires spéciaux avec des mots de passe divulgués et/ou couramment utilisés. Et s'ils n'ont ni le temps ni la patience, des outils automatisés pour exécuter des attaques par dictionnaire rendent cette tâche beaucoup plus rapide et moins fastidieuse.

D'où provient l'attaque :

Grâce à sa facilité et à sa simplicité, l'attaque par force brute permet aux pirates et cybercriminels avec peu ou pas d'expérience technique d'essayer d'accéder au compte d'un individu. Les personnes à l'origine de ces campagnes disposent de suffisamment de temps ou de puissance pour parvenir à leurs fins.

Fraude à la facture

Même les plus grandes entreprises technologiques ne sont pas à l'abri de subir une fraude à la facture. Selon une étude du magazine Fortune, Facebook et Google ont été sans le savoir victimes d'un vaste stratagème de fraude à la facture. Le fraudeur, un Lituanien connu sous le nom d'Evaldas Rimasauskas, a créé des factures imitant celles d'un grand fabricant asiatique qui faisait fréquemment affaire avec les deux entreprises pour les amener à payer pour des fournitures informatiques fictives. Pendant deux ans, le fraudeur a dupé les deux géants de la technologie en leur faisant débourser des dizaines de millions de dollars. Au moment où les entreprises ont compris ce qu'il se passait, Evaldas Rimasauskas se serait enfui avec plus de 100 millions de dollars.



Ce que vous devez savoir :

La fraude à la facture consiste à tenter de duper et de faire payer à ses victimes une facture frauduleuse (mais convaincante) adressée à votre entreprise. En réalité, les fonds iront à des imposteurs imitant des fournisseurs. Ces pirates factureront généralement un montant raisonnable afin de ne pas attirer les soupçons. Mais exécutées des centaines ou des milliers de fois, ces escroqueries rapportent rapidement de gros montants.

Comment l'attaque se produit :

Dans le cadre de cette attaque, les malfaiteurs envoient de fausses factures à leurs victimes pour tenter de leur dérober de l'argent en espérant qu'elles ne prêtent pas attention à leur comptabilité fournisseurs. Les pirates choisissent leurs cibles en fonction de la taille de leur entreprise, de leur emplacement et des fournisseurs auxquels elles font appel, puis créent de fausses factures d'apparence légitime. Dans l'espoir que le département comptabilité fournisseurs de la victime soit surchargé, ils envoient de fausses factures très urgentes, comme « 90 jours en retard, à payer immédiatement ! »

D'où provient l'attaque :

Bien que de nombreux escrocs aient recours aux fausses factures, bon nombre d'entre elles proviennent de réseaux frauduleux qui disposent de l'organisation et des ressources nécessaires pour faire des recherches sur l'institution bancaire de la victime et créer une expérience de facturation qui semble réelle. Les réseaux frauduleux qui commettent des fraudes à la facture se trouvent un peu partout dans le monde.

Gestion de l'accès au cloud

Le passage au cloud présente d'innombrables avantages, qu'il s'agisse de favoriser la collaboration ou de permettre aux employés de travailler depuis presque n'importe où dans le monde. L'importance de cette flexibilité a été illustrée tout au long de la pandémie de COVID-19.

Mais le passage à un service basé sur le cloud peut comporter un certain nombre de risques, souvent dus à l'erreur humaine.

Wyze Labs, une entreprise spécialisée dans les produits domestiques intelligents à bas prix, en a fait l'expérience. Une violation qui aurait pu s'avérer prolifique a eu lieu dans la start-up lorsqu'un employé a créé une base de données pour l'analyse des utilisateurs en supprimant accidentellement les protocoles de sécurité nécessaires, exposant ainsi une base de données contenant des informations personnelles sur les clients.

Gestion de l'accès au cloud

Ce que vous devez savoir :

La gestion des autorisations est de plus en plus importante afin d'éviter une violation basée sur le cloud à votre entreprise. Une sécurité laxiste ou inexistante (ou dans ce cas, des contrôles de sécurité mal configurés) peut facilement compromettre la sécurité de vos données et exposer votre organisation à une quantité inutile de risques, y compris des dommages importants à la réputation de votre marque.

Comment l'attaque se produit :

Elle a généralement lieu en raison d'une mauvaise communication, d'un manque de protocole, d'une configuration par défaut non sécurisée et d'une mauvaise documentation. Une fois que l'attaquant exploite la vulnérabilité pour s'insérer dans votre environnement cloud, il peut utiliser des privilèges pour accéder à d'autres points d'entrée distants, rechercher des applications et des bases de données non sécurisées ou des contrôles réseau faibles. Ils peuvent alors exfiltrer les données sans être détectés.

D'où provient l'attaque :

La mauvaise gestion et la mauvaise configuration d'un environnement cloud ne sont pas considérées comme des actes malveillants en soi et, comme on l'a vu, se produisent généralement en raison d'une erreur humaine.

Cloud mining

Le cloud mining n'a pas besoin de combustible pour avancer. Pour en avoir la preuve, ne cherchez pas plus loin que chez Tesla. Le constructeur de voitures électriques a été victime d'une attaque de cloud mining lorsque des pirates ont profité d'une console Kubernetes non sécurisée pour voler la puissance de traitement informatique de l'environnement cloud de Tesla afin de miner des cryptomonnaies.

Ce que vous devez savoir :

Le cloud mining est une activité intentionnellement compliquée et gourmande en ressources. Sa complexité a été conçue pour garantir la stabilité du nombre de blocs extraits chaque jour. Il est donc tout à fait normal que des mineurs à la fois ambitieux et sans scrupules fassent de l'accumulation de la puissance de calcul des grandes entreprises (une pratique connue sous le nom de cryptojacking) une priorité absolue.

Comment l'attaque se produit :

Depuis l'explosion de sa popularité à l'automne 2017, le cryptomining attire de plus en plus l'attention des médias. Les attaques sont passées des exploitations de navigateurs et téléphones mobiles à celle des services cloud d'entreprise, tels qu'Amazon Web Services, Google Cloud Platform (GCP) et Microsoft Azure.

Il est difficile de déterminer avec exactitude l'ampleur de la pratique, car les pirates font continuellement évoluer leur capacité à échapper à la détection, notamment en utilisant des points de terminaison non répertoriés, en modérant leur utilisation du processeur et en cachant l'adresse IP du pool de minage derrière un réseau de distribution de contenu gratuit (CDN).

Lorsque des mineurs dérobent une instance cloud, ils créent souvent des centaines de nouvelles instances dont les coûts peuvent devenir astronomiques pour le titulaire du compte. Il est donc essentiel de superviser ses systèmes et d'y rechercher les activités suspectes pouvant indiquer qu'un réseau a été infiltré.

D'où provient l'attaque :

La cryptomonnaie étant une ressource mondiale, les attaques peuvent provenir de n'importe où. Au lieu de se concentrer sur l'origine des attaques, il est essentiel de superviser les instances de cloud computing et d'y rechercher les activités liées au cryptojacking et au cloud mining, telles que les nouvelles instances de cloud provenant de régions inédites, les utilisateurs qui lancent un nombre anormalement élevé d'instances ou les instances de calcul lancées par des utilisateurs jamais vus auparavant.

Commande et contrôle

La première panne de réseau électrique d'un pays due à une cyberattaque s'est produite le 23 décembre 2015. Les détails du piratage sont résumés dans les moindres détails par Wired. Vers 15 h 30, heure locale, un employé du centre de contrôle de Prykarpattyaoblenergo a vu le curseur de sa souris se déplacer sur l'écran.

Le curseur fantomatique a flotté vers les commandes numériques des disjoncteurs d'un poste et a commencé à les mettre hors ligne. Près de 30 postes sont ensuite tombés en panne et 230 000 habitants de l'ouest de l'Ukraine ont été contraints de passer une soirée dans le froid et le noir, par des températures inférieures à zéro.

Commande et contrôle

Ce que vous devez savoir :

Une attaque par commande et contrôle se produit lorsqu'un pirate informatique s'empare d'un ordinateur pour envoyer des commandes ou des logiciels malveillants à d'autres systèmes du réseau. Dans certains cas, l'attaquant procède à des activités de reconnaissance, en se déplaçant latéralement sur le réseau pour collecter des données sensibles.

Dans d'autres, les pirates utilisent cette infrastructure pour lancer de véritables attaques. L'une des principales fonctions de cette infrastructure est d'établir des serveurs qui communiqueront avec des implants sur les points de terminaison compromis. Ces attaques sont également souvent appelées attaques C2 ou C&C.

Comment l'attaque se produit :

La plupart des pirates s'insèrent dans le système par le biais d'e-mails de phishing et en installant des logiciels malveillants. Ils établissent ainsi un canal de commande et contrôle utilisé pour transférer les données entre le point de terminaison compromis et l'attaquant. Ces canaux relaient les commandes vers le point de terminaison compromis et la sortie de ces commandes vers l'attaquant.

D'où provient l'attaque :

D'importantes attaques par commande et contrôle ont été perpétrées depuis la Russie, l'Iran et même les États-Unis. Ces attaquants peuvent se trouver n'importe où ; l'important pour eux étant que vous ne sachiez pas d'où ils viennent.

La communication étant essentielle, les pirates informatiques utilisent des techniques conçues pour masquer la véritable nature de leur correspondance. Ils tenteront souvent de consigner leurs activités le plus longtemps possible sans être détectés, en s'appuyant sur diverses techniques pour communiquer sur ces canaux tout en conservant un profil bas.

Informations d'identification compromises

En 2020, Marriott International a subi une faille de sécurité massive en raison d'une compromission d'informations d'identification. Cette faille a touché les comptes de 5,2 millions de clients Marriott, révélant leurs coordonnées, leur sexe, leur date de naissance et les informations relatives à leur compte fidélité. Le malfaiteur a utilisé les identifiants de deux employés de Marriott, vraisemblablement obtenus grâce à un mélange de phishing et de bourrage d'informations d'identification, pour récupérer les informations de clients Marriott pendant un mois avant d'attirer les soupçons.

Informations d'identification compromises

Ce que vous devez savoir :

La plupart des individus utilisent encore l'authentification à facteur unique pour s'identifier (une véritable aberration dans le domaine de la cybersécurité). Et bien que des exigences plus strictes commencent à être imposées aux mots de passe (comme le nombre de caractères, la combinaison de symboles et de chiffres et les intervalles de renouvellement), les utilisateurs finaux continuent à utiliser les mêmes identifiants sur leurs différents comptes, plateformes et applications, sans les mettre à jour périodiquement.

Ce type d'approche permet 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.

Comment l'attaque se produit :

Un mot de passe, une clé ou autre identifiant découvert peut être utilisé par un acteur malveillant pour obtenir un accès non autorisé aux informations et aux ressources (d'un seul compte à une base de données entière).

Un acteur malveillant peut alors exploiter un compte de confiance au sein de l'organisation ciblée pour y opérer sans être détecté et exfiltrer des données sensibles sans déclencher d'alerte. Les méthodes courantes de collecte d'identifiants incluent l'utilisation de renifleurs de mots de passe, les campagnes de phishing ou les attaques par logiciels malveillants.

D'où provient l'attaque :

Les identifiants compromis représentent un énorme vecteur d'attaque en donnant aux auteurs de la menace un moyen d'accéder aux appareils informatiques, aux comptes protégés par mot de passe et à l'infrastructure réseau d'une entreprise avec une certaine facilité. Souvent organisés, ces acteurs visent une entreprise ou une personne en particulier. Et ils ne sont pas toujours externes à l'entreprise et peuvent parfaitement être une menace interne possédant un certain niveau d'accès légitime aux systèmes et aux données de l'entreprise.

Dumping d'informations d'identification

Disney+ a enregistré 10 millions d'utilisateurs et le cours de son action a atteint un niveau record peu de temps après. Mais cette gloire s'est rapidement estompée lorsque bon nombre de ces abonnés enthousiastes ont commencé à se plaindre du verrouillage de leurs comptes. Quelques jours après le lancement, les identifiants Disney+ étaient mis en vente pour à peine trois dollars.

Disney a déclaré que le site n'avait pas été piraté ; les utilisateurs qui ont trouvé leurs informations d'identification en ligne auraient été victimes d'une pratique courante (mais notoirement mauvaise) – utiliser le même mot de passe sur plusieurs sites – et ont ensuite été victimes d'une attaque de dumping d'informations d'identification.

Dumping d'informations d'identification

Ce que vous devez savoir :

Le dumping d'informations d'identification fait simplement référence à une attaque qui repose sur la collecte d'informations d'identification sur un système ciblé. Même si les informations ne sont pas en texte brut (elles sont souvent hachées ou chiffrées), un attaquant peut toujours extraire les données et les déchiffrer hors ligne sur son propre système. C'est pourquoi on désigne cette attaque par le terme « dumping ».

Souvent, les pirates tentent de voler les mots de passe des systèmes qu'ils ont déjà compromis. Le problème s'amplifie lorsque les utilisateurs réutilisent le même mot de passe sur plusieurs comptes à travers plusieurs systèmes.

Comment l'attaque se produit :

Les informations d'identification obtenues de cette manière incluent généralement celles d'utilisateurs privilégiés, qui peuvent donner accès à des informations et à des opérations système plus sensibles. Les pirates ciblent souvent diverses sources pour extraire les informations d'identification, y compris le gestionnaire de comptes de sécurité (SAM), l'autorité de sécurité locale (LSA), le NTDS des contrôleurs de domaine ou les fichiers de préférences de stratégie de groupe (GPP).

Une fois qu'ils ont obtenu des informations d'identification valides, les attaquants les utilisent pour se déplacer facilement sur un réseau cible, découvrir de nouveaux systèmes et identifier les actifs d'intérêt.

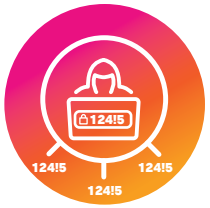
D'où provient l'attaque :

Le dumping d'informations d'identification peut provenir de n'importe où. Et comme nous commettons tous l'erreur de recycler les mots de passe, ces informations peuvent être vendues pour de futures attaques.

Attaque par réutilisation d'informations d'identification

L'attaque de Dunkin Donuts de 2019 compte parmi les attaques de réutilisation d'informations d'identification les plus notables. Et au grand dam de la chaîne de la côte est, ce fut la *deuxième* attaque en deux mois. Cette fois, les malfaiteurs sont allés jusqu'à vendre des milliers de comptes sur le dark web. Ils vendaient les informations d'identification des utilisateurs, y compris les noms d'utilisateur et les mots de passe, aux plus offrants, qui pouvaient ensuite les tester sur d'autres sites web de consommateurs jusqu'à obtenir un bon résultat.

Attaque par réutilisation d'informations d'identification



Ce que vous devez savoir :

La réutilisation d'informations d'identification est un problème répandu dans les entreprises et les bases d'utilisateurs. De nos jours, la plupart des utilisateurs possèdent des dizaines (voire des centaines) de comptes et doivent se souvenir d'innombrables mots de passe qui répondent à toutes sortes d'exigences rigoureuses. En conséquence, ils recyclent constamment le même mot de passe, dans l'espoir de mieux gérer et mémoriser les informations d'identification de tous leurs comptes. Sans surprise, cela peut entraîner des problèmes de sécurité majeurs lorsque lesdites informations d'identification sont compromises.

Comment l'attaque se produit :

En théorie, l'attaque en elle-même est simple, directe et étonnamment furtive (si l'authentification à deux facteurs n'est pas activée). Une fois les informations d'identification d'un utilisateur volées, le coupable peut tester le même nom d'utilisateur et le même mot de passe sur d'autres sites Web de consommateurs ou bancaires jusqu'à ce qu'ils obtiennent une correspondance, d'où l'expression « attaque par réutilisation d'informations d'identification ».

Cependant, le premier accès est un peu plus compliqué. Pour obtenir des informations privilégiées, les attaquants commencent généralement par une tentative de phishing en utilisant des e-mails et des sites Web qui semblent légitimes pour duper l'utilisateur et lui faire dévoiler ses informations d'identification.

D'où provient l'attaque :

Il peut s'agir d'une attaque ciblée, dans laquelle la personne 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 informations personnelles de l'utilisateur dans le monde de la cybercriminalité.

Bourrage d'informations d'identification

Citrix Systems, une entreprise basée à Fort Lauderdale, s'est retrouvée à réaliser une investigation en profondeur sur une grave violation de réseau qui s'était produite en 2019 et soldée par le vol de documents commerciaux par des pirates. Le FBI pensait que la violation avait donné lieu à une « pulvérisation de mots de passe », autrement connue sous le nom de bourrage d'informations d'identification, une attaque grâce à laquelle les pirates informatiques tentent d'accéder à distance à un grand nombre de comptes à la fois. Selon un formulaire 10-K déposé auprès de la Securities and Exchange Commission des États-Unis, Citrix pensait que les pirates avaient tenté d'infiltrer les systèmes de l'entreprise pour accéder aux comptes Content collaboration de ses clients.

Bourrage d'informations d'identification

Ce que vous devez savoir :

Avec le bourrage d'informations d'identification, les cybercriminels utilisent des informations d'identification de compte volées (souvent des noms d'utilisateur et mots de passe obtenus à partir d'une violation de données) pour accéder à des comptes supplémentaires en automatisant des milliers ou des millions de demandes de connexion dirigées contre une application web. Ils cherchent un moyen facile d'accéder aux comptes sensibles, tout simplement en s'y connectant. Et cela fonctionne parce qu'ils comptent sur le fait que les gens utilisent les mêmes identifiants et mots de passe pour accéder à de multiples services. S'ils parviennent à leurs fins,un jeu d'identifiants peut déverrouiller des comptes contenant des informations financières et privées et leur donner les clés de presque tout.

Comment l'attaque se produit :

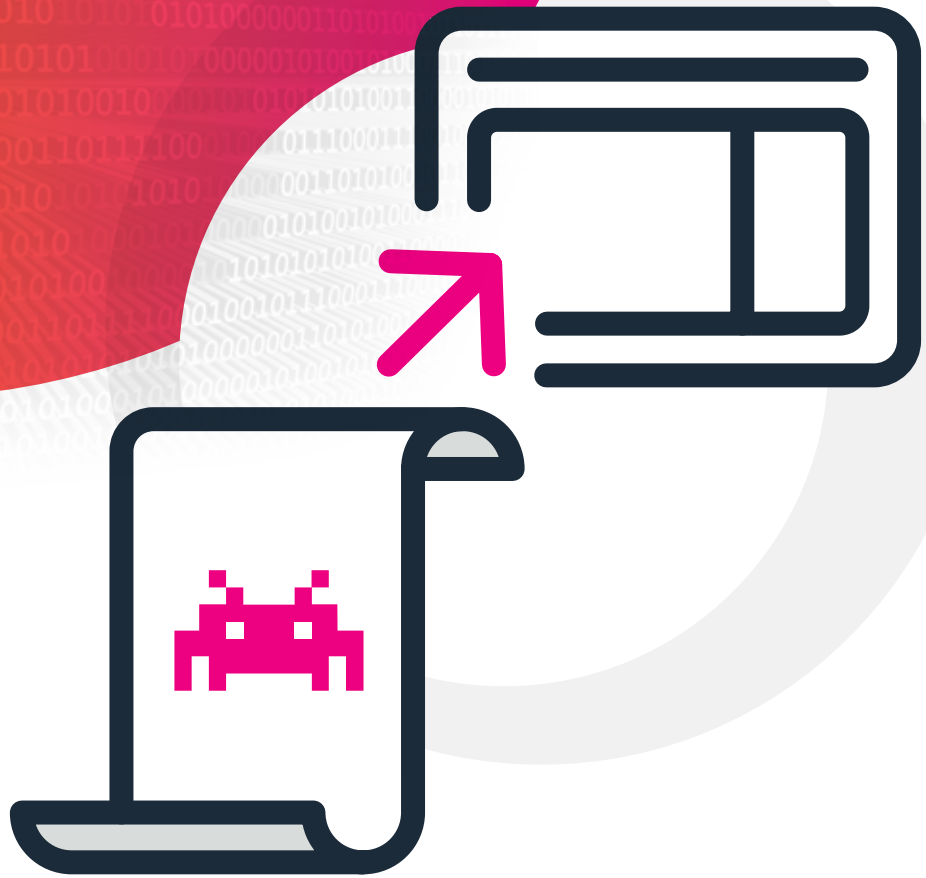
Les pirates ont seulement besoin d'accéder aux informations d'identification, à un outil automatisé et à des proxys pour mener une attaque par bourrage d'informations d'identification. Ils vont puiser dans un cache de noms d'utilisateur et de mots de passe, glanés à partir de violations massives de données d'entreprise et utiliser des outils automatisés pour « bourrer » ces informations d'identification dans les informations de connexion d'autres sites.

D'où provient l'attaque :

Les proxys masquent la localisation des auteurs d'attaque par bourrage d'informations d'identification, ce qui complique leur détection. Mais ils peuvent se retrouver partout dans le monde, en particulier dans les lieux stratégiques de cybercriminalité organisée. Souvent, les attaquants sont des pirates informatiques indépendants et organisés ayant accès à des outils de vérification de compte dédiés et à de nombreux proxys qui empêchent de bloquer leurs adresses IP.

Des malfaiteurs moins sophistiqués peuvent finir par se trahir en tentant d'infiltrer un grand nombre de comptes via des bots, créant par inadvertance un scénario d'attaque par déni de service (DDoS).

Script intersites



En janvier 2019, une vulnérabilité XSS a été découverte dans le client Steam Chat exploité par Valve, une société de jeux informatiques avec plus de 90 millions d'utilisateurs actifs, dont un certain nombre aurait pu être attaqué jusqu'à ce que le bogue soit révélé.

Les attaques de type Cross-Site Scripting (XSS) sont un type d'attaque dans laquelle des scripts malveillants sont injectés dans des sites Web inoffensifs et fiables. Conceptuellement, il s'agit d'une attaque similaire à une injection SQL dans laquelle un code malveillant est saisi dans un formulaire pour accéder à la base de données du site. La seule différence avec le XSS, c'est que le code malveillant est conçu pour s'exécuter dans le navigateur d'un autre visiteur du site et permettre à l'attaquant de voler les cookies utilisateur, lire les identifiants de session, modifier le contenu d'un site Web ou rediriger un utilisateur vers un site malveillant.

Script intersites

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 qui permettent à ces attaques de réussir sont répandues et apparaissent partout où une application Web génère une entrée utilisateur sans la valider ou l'encoder.

Le navigateur de l'utilisateur final n'a aucun moyen de savoir qu'il ne doit pas faire confiance au script, qui s'exécute automatiquement. Étant donné qu'il pense que le script provient d'une source fiable, il peut accéder aux cookies, aux jetons de session ou à d'autres informations sensibles conservées par le navigateur. Ces scripts sont même capables de réécrire le contenu de la page HTML.

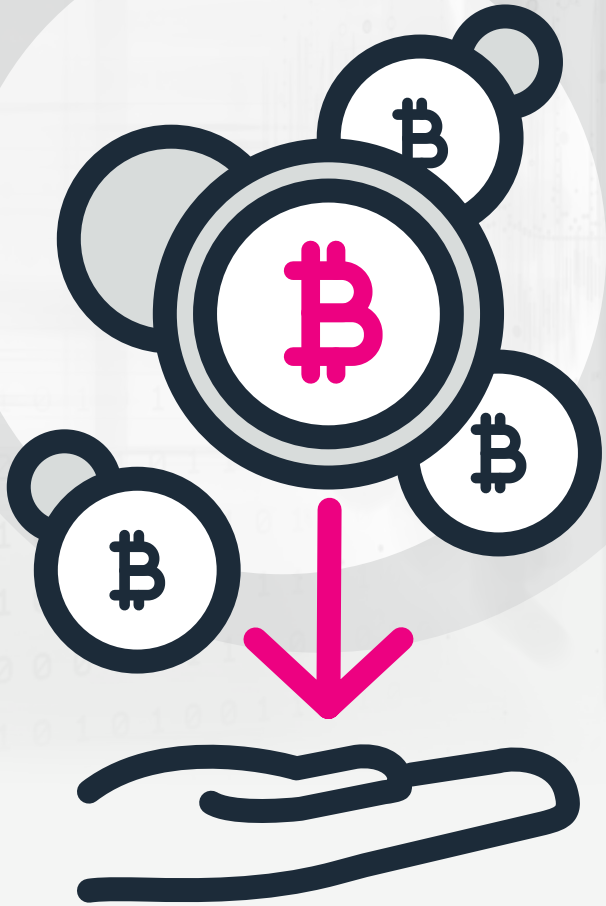
Comment l'attaque se produit :

Il existe deux types d'attaques XSS : stockées et réfléchies. Les attaques XSS stockées se produisent lorsqu'un script injecté est stocké dans un emplacement fixe sur le serveur, comme un message ou un commentaire de forum. Chaque utilisateur qui arrive sur la page infectée sera affecté par l'attaque XSS. Avec le XSS réfléchi, le script injecté est fourni à un utilisateur en réponse à une demande, comme une page de résultats de recherche.

D'où provient 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, et la base de données Common Vulnerabilities and Exposures répertorie près de 14 000 vulnérabilités associées aux attaques XSS.

Attaque de cryptojacking



Des pirates informatiques ont compromis de nombreux sites web du gouvernement australien avec des logiciels malveillants qui ont forcé les ordinateurs des visiteurs à miner secrètement de la cryptomonnaie sans leur autorisation. L'attaque de cryptojacking a débuté lorsque des pirates ont exploité une vulnérabilité d'un plug-in de navigateur populaire dans le cadre d'une violation de sécurité mondiale plus importante. L'attaque a affecté le site officiel du parlement du Victoria, le tribunal civil et administratif du Queensland et la page d'accueil du Queensland Community Legal Center, entre autres, ainsi que le National Health Service du Royaume-Uni et le site de surveillance de la protection des données du Royaume-Uni.

Ce que vous devez savoir :

Le cryptojacking est une attaque par laquelle un pirate informatique cible et détourne les systèmes informatiques avec des logiciels malveillants qui se cachent sur un appareil et exploitent sa puissance de traitement pour extraire des cryptomonnaies (comme le Bitcoin ou l'Ethereum) aux dépens de la victime. La mission du pirate est de créer de la cryptomonnaie avec les ressources informatiques d'une autre personne.

Comment l'attaque se produit :

L'une des méthodes courantes utilisées pour exécuter les attaques de cryptojacking consiste à envoyer, dans un e-mail de phishing, un lien malveillant incitant les utilisateurs à télécharger le code de cryptominage directement sur leur ordinateur. Une autre méthode consiste à intégrer un bout de code JavaScript dans une page web que l'utilisateur visite, connue sous le nom d'attaque drive-by. Lorsque vous visitez la page, un code malveillant destiné à extraire la cryptomonnaie se télécharge automatiquement sur la machine. Le code de cryptominage fonctionne alors silencieusement en arrière-plan et à l'insu de l'utilisateur, la lenteur anormale de l'ordinateur pouvant être la seule indication du problème.

D'où provient l'attaque :

Ces attaques proviennent du monde entier car le cryptojacking ne nécessite pas de compétences techniques importantes. Des kits de cryptojacking sont disponibles sur le deep web pour à peine 30 dollars ; une condition négligeable pour les pirates désireux de gagner de l'argent rapidement en prenant relativement peu de risques. Dans le cadre d'une attaque, une banque européenne a observé des schémas de trafic inhabituels sur ses serveurs, des processus nocturnes plus lents que la moyenne et des serveurs en ligne inexpliqués, tous attribués à un membre du personnel malhonnête ayant installé un système de cryptominage.

Données des référentiels d'informations

Le groupe de hackers APT28 aurait compromis la campagne d'Hillary Clinton, le Comité national démocrate (DNC) et le Comité de campagne du Congrès démocrate (DCCC) pendant la campagne présidentielle contre Donald Trump. Ils ont également ciblé des gouvernements d'Europe de l'Est, des organisations militaires et en lien avec la sécurité, y compris l'OTAN (Organisation du traité de l'Atlantique Nord).

Le groupe utilise un ensemble complexe d'outils et de stratégies pour accéder subrepticement à des référentiels d'informations et contrôler et voler des données. APT28 a collecté des informations à partir des services Microsoft SharePoint au sein des réseaux cibles.

Données des référentiels d'informations

Ce que vous devez savoir :

Les référentiels d'informations sont des outils qui permettent le stockage d'informations, comme Microsoft SharePoint et Atlassian Confluence. Les référentiels d'informations facilitent généralement la collaboration ou le partage d'informations entre les utilisateurs et stockent une grande variété de données qui peuvent tenter les attaquants. Les pirates informatiques peuvent exploiter les référentiels d'informations pour accéder à des informations précieuses et les extraire.

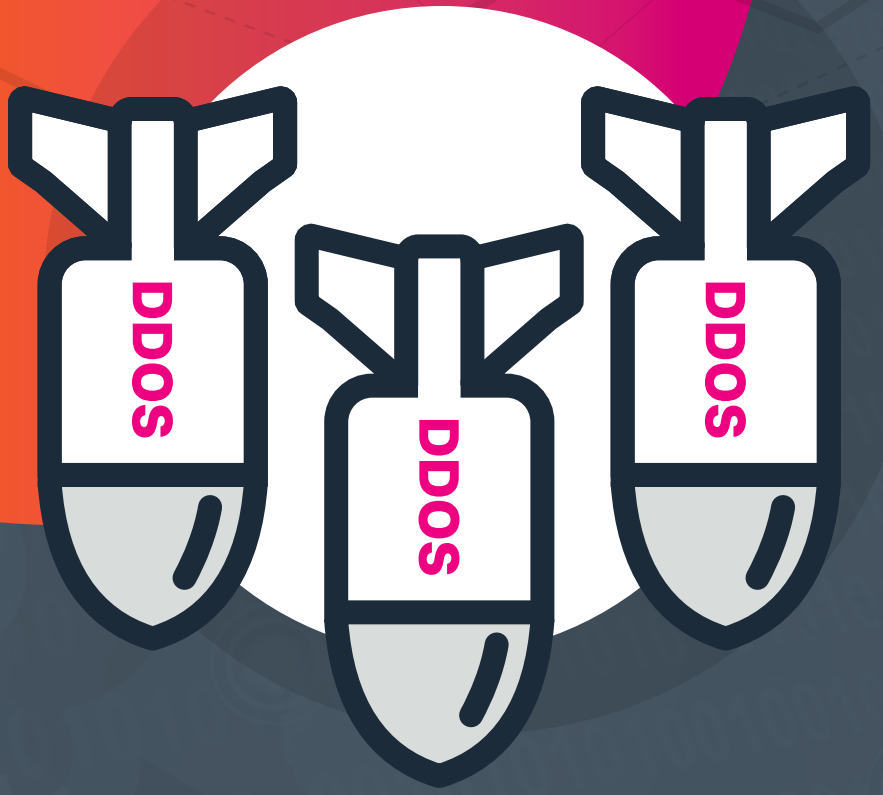
Comment l'attaque se produit :

Les référentiels d'informations ont souvent une grande base d'utilisateurs et la détection des violations peut s'avérer compliquée. Les attaquants peuvent collecter des informations à partir de référentiels de stockage partagés et hébergés dans une infrastructure cloud ou des applications de logiciel en tant que service (SaaS).

D'où provient l'attaque :

Des attaquants comme APT28 ciblent les agences gouvernementales, les sites de réservation d'hôtels, les sociétés de télécommunications et informatiques. Il convient au minimum de superviser étroitement et de signaler les accès aux référentiels d'informations effectués par des utilisateurs privilégiés (comme les administrateurs de domaine Active Directory, d'entreprise ou de schéma), car ces types de comptes ne doivent généralement pas être utilisés pour accéder aux référentiels d'informations. Une infrastructure supplémentaire de stockage et d'analyse des journaux sera probablement nécessaire pour renforcer les capacités de détection.

Attaque DDoS



À ce jour, l'une des plus grandes attaques par déni de service distribué (DDoS), sinon la plus importante, s'est produite en 2018 contre le système de gestion de code en ligne populaire GitHub. GitHub a été touché par un assaut de trafic qui, à son apogée, a atteint un rythme de 1,3 téraoctet par seconde, envoyant des paquets à un rythme de 126,9 millions par seconde. L'attaque était non seulement massive, mais elle battait tous les records. Dans le cadre de cette attaque, les botmasters ont inondé les serveurs memcached de requêtes falsifiées, ce qui leur a permis d'amplifier leur attaque de 50 000 fois. La bonne nouvelle ? GitHub n'a pas été pris au dépourvu. Les administrateurs ont été alertés de l'attaque et celle-ci a été stoppée après 20 minutes.

Ce que vous devez savoir :

Dans le cadre d'une attaque DDoS, des pirates, hacktivistes ou cyberespions tentent de supprimer des sites Web, de ralentir et de bloquer les serveurs cibles et de rendre le service en ligne indisponible en les inondant de trafic provenant de plusieurs sources. Comme leur nom l'indique, les attaques DDoS sont des attaques par force brute largement distribuées visant à semer le chaos et provoquer la destruction. Ces attaques ont souvent tendance à cibler des sites populaires ou très médiatisés, tels que les banques, sites d'information et gouvernementaux, pour empêcher ou dissuader les entreprises cibles de publier des informations importantes ou les affaiblir financièrement.

Comment l'attaque se produit :

L'objectif des acteurs malveillants à l'origine des attaques DDoS est de semer le chaos chez leurs cibles, saboter les sites et services Web, nuire à la réputation de la marque et provoquer des pertes financières en empêchant les utilisateurs d'accéder à un site Web ou à une ressource réseau. DDoS exploite des centaines ou des milliers d'ordinateurs « bots » infectés situés partout dans le monde. Connues sous le nom de réseaux de bots, ces armées d'ordinateurs compromis exécutent simultanément l'attaque pour lui garantir une efficacité optimale.

Le pirate ou le groupe de pirates qui contrôle ces ordinateurs infectés devient alors un botmaster, qui infecte les systèmes vulnérables avec des logiciels malveillants (souvent des chevaux de Troie). Lorsqu'un nombre suffisant de périphériques est infecté, le botmaster leur donne l'ordre d'attaquer et les serveurs et réseaux cibles sont bombardés de demandes de service qui les saturent et provoquent leur arrêt.

D'où provient l'attaque :

Comme leur nom l'indique, les attaques DDoS sont distribuées, ce qui signifie que le flux de trafic entrant qui cible le réseau de la victime provient de nombreuses sources. Les pirates informatiques à l'origine de ces attaques peuvent donc littéralement provenir de n'importe où dans le monde. Qui plus est, leur nature distribuée ne permet pas de déjouer ces attaques en sécurisant ou en bloquant simplement une seule source.

Désactivation des outils de sécurité

Pour accéder à des systèmes, les pirates informatiques exploitent parfois les outils destinés à protéger les organisations. Lors de sa première sortie en 1985, Microsoft Windows s'est imposé comme le système d'exploitation de prédilection partout dans le monde. Et si sa part de marché a diminué ces dernières années, il n'en reste pas moins une force dominante par rapport à son lointain concurrent, Apple OSX. En raison de son adoption massive et de sa vulnérabilité aux attaques de type logiciel malveillant et bots, notamment, Windows est le terrain de jeu de prédilection des pirates.

C'est en partie pourquoi Microsoft a décidé d'installer un programme anti-spyware et antivirus natif, appelé Windows Defender, avec le lancement de Windows Vista. Malheureusement, Microsoft n'a pas anticipé que les pirates s'attaqueraient à l'outil censé protéger ses utilisateurs.

Une attaque par cheval de Troie connue sous le nom de Novter (ainsi que Nodersok ou encore Divergent) a neutralisé les fonctionnalités de protection en temps réel de Windows Defender. Une fois désactivé, le cheval de Troie téléchargeait des logiciels malveillants supplémentaires sur le système.

Désactivation des outils de sécurité

Ce que vous devez savoir :

Les pirates utilisent diverses techniques pour éviter d'être détectés et agir sans barrières. Ils doivent souvent modifier la configuration des outils de sécurité, tels que les pare-feu, pour les contourner ou les désactiver explicitement pour empêcher leur exécution.

Comment l'attaque se produit :

Les signes de cette attaque sont ceux que laissent les pirates qui tentent de désactiver divers mécanismes de sécurité. Ils vont essayer d'accéder aux fichiers du registre qui contiennent une grande partie de la configuration de Windows et de divers autres programmes. Les pirates peuvent également tenter de fermer les services liés à la sécurité.

Les attaquants peuvent également tenter diverses astuces pour empêcher l'exécution de programmes spécifiques, telles que l'ajout de certificats qui ajoutent les outils de sécurité à une blacklist pour empêcher ces outils de protection de s'exécuter.

D'où provient l'attaque :

Une attaque centrée sur la désactivation des outils de sécurité peut provenir de n'importe où, car ces types d'attaques peuvent cibler une liste presque infinie d'outils. L'attaque de Nodersok, par exemple, a principalement attaqué des utilisateurs de PC aux États-Unis et au Royaume-Uni (81 %).

Amplification DNS

En février 2022, des pirates ont lancé des attaques par déni de service distribué (DDoS) par amplification DNS à grande échelle par l'intermédiaire de Mitel, une entreprise de communication commerciale internationale. L'attaque a pilonné entre autres des institutions financières, des FAI haut-débit, des entreprises logistiques et de jeux vidéo. Capables de marteler les systèmes sur une durée pouvant atteindre 14 heures, avec un facteur d'amplification record de pratiquement 4,3 milliards, ces attaques DDoS peuvent couper les communications vocales et d'autres services d'organisations entières avec un simple paquet réseau malveillant.

Ce que vous devez savoir :

Même si les attaques DDoS par amplification DNS existent depuis longtemps, les techniques d'exploitation continuent d'évoluer. Cette attaque est similaire au piratage DNS dans le sens où elle exploite le répertoire Internet en sabotant sa configuration. Mais la façon dont elle se produit est légèrement différente.

En règle générale, une attaque par amplification DNS implique l'envoi d'une petite quantité d'informations vers un service réseau vulnérable qui le pousse à répondre avec un volume de données largement supérieur. En dirigeant cette réponse vers une victime, l'attaquant peut relativement facilement faire travailler les machines d'autres personnes pour inonder les réseaux d'une cible choisie hors ligne.

Comment l'attaque se produit :

Lors d'une attaque par amplification DNS, l'attaquant inonde un site web avec une quantité telle de fausses requêtes de recherche DNS qu'il consomme la bande passante du réseau jusqu'à ce que le site soit en échec. Tandis que le piratage DNS dirige le trafic vers un autre site, une attaque par amplification DNS empêche quant à elle le chargement du site.

La différence entre les deux attaques est encore illustrée par le terme « amplification ». Dans cette attaque, les pirates créent les requêtes DNS de manière à ce qu'elles nécessitent une réponse plus intensive. Un pirate peut par exemple demander plus que le nom de domaine. L'attaquant peut également baser sa requête sur l'intégralité du domaine (requête ANY), et demander le domaine ainsi que le sous-domaine, les serveurs de messagerie, les serveurs de sauvegarde, les alias, etc.

Imaginez maintenant que plusieurs de ces requêtes « ANY » arrivent en même temps. Le trafic amplifié qu'elles génèrent est alors suffisant pour mettre le site hors ligne.

D'où provient l'attaque :

Similaire à une attaque par piratage DNS, la nature relativement primitive de cette attaque implique qu'elle peut provenir de n'importe où dans le monde, qu'il s'agisse de pirates informatiques d'un État-nation ou d'un loup solitaire.

Piratage DNS

Un jeudi matin de 2017, les lecteurs de WikiLeaks se sont réveillés en s'attendant à trouver le dernier secret d'État publié sur le site web de divulgation. À la place, ils ont découvert le message d'un collectif de pirates appelé OurMine annonçant qu'ils contrôlaient le domaine.

Le fondateur de Wikileaks, Julian Assange, a rapidement communiqué sur Twitter pour préciser que l'attaque n'était pas un piratage traditionnel, mais une attaque ciblant le DNS (Domain name system).

Ce que vous devez savoir :

On dit souvent que le DNS est le talon d'Achille d'Internet, ou le répertoire d'Internet, car il joue un rôle essentiel dans le routage du trafic Web. Le DNS est le protocole utilisé convertir les noms de domaine en adresses IP. Il s'avère efficace pour sa fonction prévue. Mais le DNS est notoirement vulnérable aux attaques, notamment en raison de sa nature distribuée. Le DNS repose sur des connexions non structurées entre des millions de clients et de serveurs via des protocoles intrinsèquement non sécurisés.

La gravité et l'ampleur de l'importance de la sécurisation du DNS contre les attaques sont indéniables. Les retombées d'un DNS compromis peuvent être désastreuses. Non seulement les pirates peuvent faire tomber toute une entreprise, mais ils peuvent également intercepter des informations confidentielles, des e-mails et des informations d'identification.

La Cybersecurity and Infrastructure Security Agency (CISA) du département américain de la Sécurité intérieure a soulevé des inquiétudes concernant certaines attaques de piratage DNS de grande ampleur contre les infrastructures, aux États-Unis et à l'étranger.

Comment l'attaque se produit :

Dans cette attaque, les pirates informatiques exploitent la façon dont DNS communique avec un navigateur Internet. Le système agit comme un annuaire téléphonique en traduisant un domaine (comme NYTimes.com) en une adresse IP. Le DNS recherche et trouve le serveur global qui héberge ce site et dirige ensuite le trafic vers celui-ci. L'attaque se produit lorsqu'un pirate parvient à interrompre la recherche DNS, puis à mettre le site hors ligne ou rediriger le trafic vers un site contrôlé par le pirate.

D'où provient l'attaque :

Il n'existe pas de profil unique d'auteur de piratage DNS, principalement parce qu'il peut suffire d'une simple attaque d'ingénierie sociale, dans laquelle un individu appelle un fournisseur de domaine et le dupe pour qu'il modifie une entrée DNS.

Certaines des attaques de piratage DNS les plus importantes ont été attribuées à des collectifs de piratage tels que OurMine dans l'affaire Wikileaks, ou l'Armée électronique syrienne dans les piratages du New York Times et du Washington Post.

DNS Tunneling

Ces dernières années, un groupe de pirates connu sous le nom d'OilRig lance régulièrement des attaques contre des gouvernements et des entreprises du Moyen-Orient à l'aide de divers outils et méthodes. Un élément essentiel de leurs efforts pour perturber les opérations quotidiennes et exfiltrer les données consiste à maintenir une connexion entre leur serveur de commande et contrôle et le système qu'ils attaquent par le biais d'un tunnel DNS.

Ce que vous devez savoir :

Souvent, le trafic qui passe par le DNS n'est pas supervisé, car il n'est pas conçu pour le transfert de données. Cela qui le rend vulnérable à plusieurs types d'attaques, notamment le DNS tunneling, qui se produit lorsqu'un attaquant encode des données malveillantes dans une requête DNS : une chaîne complexe de caractères au début d'une URL.

Le DNS tunneling peut être utilisé à des fins honnêtes : les fournisseurs de logiciels antivirus l'utilisent pour envoyer des profils de logiciels malveillants mis à jour aux clients en arrière-plan, par exemple. Étant donné qu'il peut être utilisé de façon légitime, il est important que les entreprises supervisent minutieusement leur trafic DNS et autorisent uniquement le trafic de confiance sur le réseau.

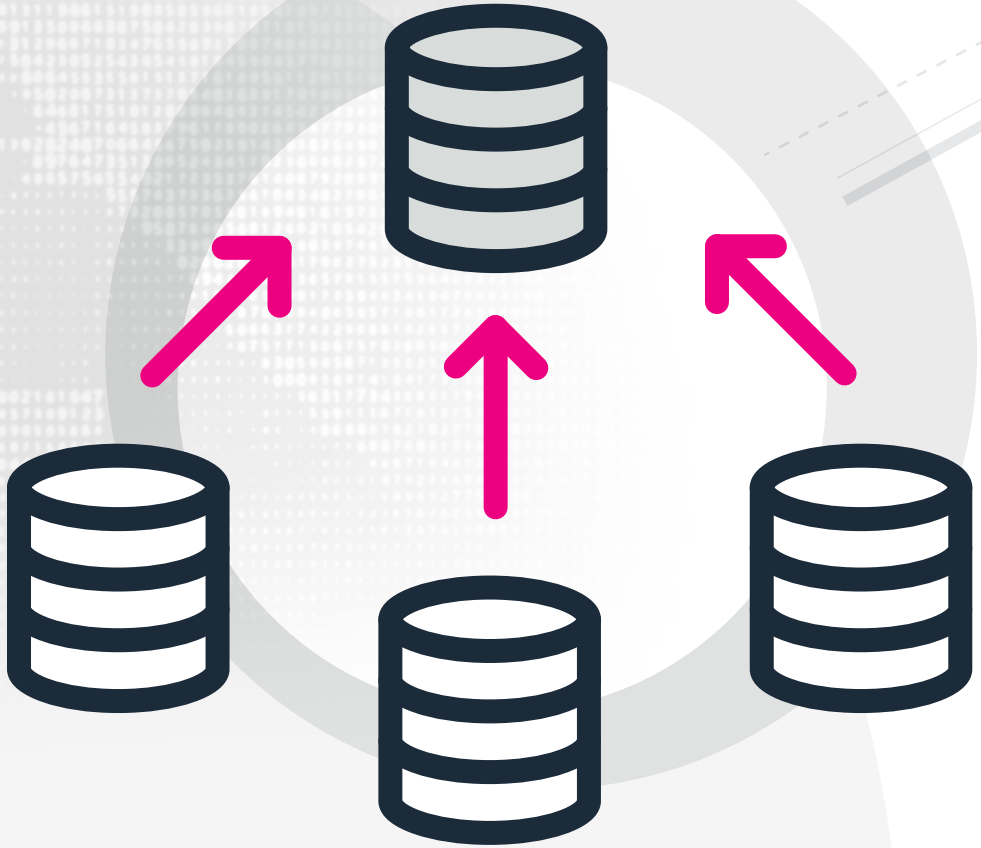
Comment l'attaque se produit :

Avec le DNS tunneling, un attaquant peut contourner les systèmes de sécurité (en créant des tunnels en dessous ou autour d'eux, pour ainsi dire) en redirigeant le trafic vers son propre serveur et en établissant une connexion au réseau d'une entreprise. Une fois activée, cette connexion permet d'exfiltrer des données et de mener des attaques par commande et contrôle ainsi qu'un certain nombre d'autres attaques.

D'où provient l'attaque :

Bien qu'il existe des outils de DNS tunneling facilement téléchargeables, les attaquants qui ne veulent pas se contenter de contourner le paywall d'un hôtel ou d'une compagnie aérienne pour accéder à Internet nécessitent des connaissances plus sophistiquées. De plus, DNS ayant été uniquement conçu pour résoudre les adresses Web, il s'agit d'un système très lent pour le transfert de données.

Attaque DoS



Il y a pratiquement 20 ans, un pirate 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 de nombreux acteurs majeurs comme CNN, eBay, Amazon et Yahoo. Selon les rapports, Mafiaboy s'est introduit dans des dizaines de réseaux pour installer des logiciels malveillants conçus pour inonder les cibles de trafic d'attaques. Étant donné que de nombreux sites n'étaient pas préparés à un tel assaut, l'attaque a duré environ une semaine tandis que les organisations ciblées luttaient pour comprendre ce qui s'était passé et comment revenir en ligne. Mafiaboy a finalement été arrêté et condamné à la détention dans un centre pour mineurs.

Vingt ans plus tard, les attaques DoS (dont beaucoup sont des DDoS) continuent d'augmenter et font partie des attaques les plus courantes auxquelles est confronté environ un tiers de l'ensemble des entreprises.

Ce que vous devez savoir :

Dans le cadre d'une attaque DoS, les cyberattaquants rendent une machine ou un réseau inaccessible à ses utilisateurs prévus. Les attaques DoS peuvent être exécutées en inondant les réseaux de trafic ou en envoyant des informations qui déclenchent un ralentissement du système, voire une interruption de service globale. À l'instar des attaques DDoS, les attaques DoS ont tendance à se concentrer sur des entreprises de premier plan ou sur des sites Web publics populaires tels que les banques, le commerce électronique, les médias ou les institutions gouvernementales. Les attaques DoS privent les utilisateurs légitimes du service auquel ils souhaitent accéder et causent des dommages considérables à la victime, en raison des coûts de sécurité et de nettoyage, de l'atteinte à la réputation, de la perte de revenus et de la perte de clientèle.

Comment l'attaque se produit :

Les attaques DoS se produisent de l'une des deux manières suivantes : en inondant ou en générant une interruption de service sur un réseau ciblé. Dans les attaques par inondation, les cybercriminels bombardent les ordinateurs des victimes avec plus de trafic qu'ils ne sont capables de gérer pour provoquer un ralentissement ou un arrêt complet. Les attaques par inondation incluent les attaques par débordement de tampon, les attaques par inondation ICMP et par inondation SYN.

D'autres attaques DoS exploitent des vulnérabilités qui provoquent une interruption du système cible. Dans ces attaques, les acteurs malveillants exploitent les vulnérabilités du système avec des logiciels malveillants qui provoquent ensuite une interruption ou perturbent gravement le système.

D'où provient l'attaque :

Les attaques DoS peuvent provenir de n'importe où dans le monde. Les attaquants sont capables de masquer facilement leurs allées et venues afin de submerger les ordinateurs des victimes, d'exécuter des logiciels malveillants ou d'accomplir d'autres méfaits sans craindre d'être détectés.

Attaque de téléchargement furtif

En janvier 2020, les visiteurs du légendaire magazine en ligne et blog Boing Boing ont vu un faux overlay Google Play Protect leur demandant de télécharger ce qui était en fait un APK malveillant qui installait un cheval de Troie bancaire sur les appareils Android. Pour les utilisateurs Windows, il apparaissait sous la forme d'une (fausse) page d'installation d'Adobe Flash qui distribuait d'autres programmes malveillants. Le système de gestion du contenu de Boing Boing avait été piraté. Même si le visiteur ne tombait pas dans le piège, les téléchargements furtifs étaient automatiquement lancés par du JavaScript intégré à la page. Bien que Boing Boing ait réussi à détecter l'attaque et à supprimer le script relativement vite, le site compte cinq millions d'utilisateurs uniques, dont l'ancien président des États-Unis Barack Obama, et les conséquences auraient pu être désastreuses.

Attaque de téléchargement furtif

Ce que vous devez savoir :

Un téléchargement furtif fait référence au téléchargement involontaire de code malveillant sur un ordinateur ou un appareil mobile qui expose les utilisateurs à différents types de menaces. Les cybercriminels ont recours aux téléchargements furtifs pour voler et collecter des informations personnelles, injecter des chevaux de Troie bancaires ou introduire des kits d'exploitation ou d'autres logiciels malveillants sur les appareils des utilisateurs. Pour vous protéger contre les téléchargements furtifs, vous devez régulièrement mettre à jour ou corriger les systèmes en installant les dernières versions des applications, des logiciels, des navigateurs et des systèmes d'exploitation. Il est également conseillé d'éviter les sites web non sécurisés ou potentiellement malveillants.

Comment l'attaque se produit :

Ce qui rend les téléchargements furtifs différents, c'est que les utilisateurs n'ont pas besoin de cliquer sur quoi que ce soit pour lancer le téléchargement. Le simple fait d'accéder ou de naviguer sur un site Web peut l'activer. Le code malveillant est conçu pour télécharger des fichiers malveillants sur l'appareil de la victime à l'insu de l'utilisateur. Un téléchargement furtif abuse d'applications, de navigateurs ou même de systèmes d'exploitation non sécurisés, vulnérables ou obsolètes.

D'où provient l'attaque :

La montée en puissance des kits de téléchargement furtif préconfigurés permet aux pirates de n'importe quel niveau de compétence de lancer ce type d'attaques. En fait, ces kits peuvent être achetés et déployés sans que le pirate écrive son propre code ou établisse sa propre infrastructure pour exfiltrer des données ou commettre d'autres abus. Étant donné la facilité avec laquelle ces attaques peuvent être exécutées, elles peuvent provenir de virtuellement n'importe où.

Menaces internes

La revanche… c'est une histoire vieille comme le monde. En 2022, un spécialiste IT a été inculpé pour avoir prétendument piraté le serveur d'une organisation de santé de Chicago. Il avait eu accès au serveur car il y avait travaillé en tant que contractuel, et il avait un mobile. L'organisation lui avait en effet refusé un emploi et quelques mois plus tard, il avait été licencié de l'entreprise IT contractante. Cet acte de vengeance personnelle a entraîné une cyberattaque qui a grandement perturbé les examens médicaux, les traitements et les diagnostics de nombreux patients.

Ce que vous devez savoir :

Une attaque interne est une attaque malveillante perpétrée par des employés ayant un accès autorisé au réseau, aux ressources et au système informatique d'une organisation. Dans le cadre de cette attaque, l'objectif des attaquants consiste souvent à voler des informations et des actifs classifiés, exclusifs ou autrement sensibles, soit à des fins personnelles, soit pour les communiquer à des concurrents. Ils peuvent également tenter de saboter votre entreprise avec des perturbations du système qui entraînent une perte de productivité, de rentabilité et de réputation.

Comment l'attaque se produit :

Les employés malveillants ont l'avantage de disposer d'un accès autorisé au réseau, aux informations et aux actifs d'une organisation. Ils peuvent posséder des comptes qui leur donnent accès à des systèmes ou des données critiques, ce qui leur permet de les localiser facilement, de contourner les contrôles de sécurité et de les envoyer à l'extérieur de l'entreprise.

D'où provient l'attaque :

Les auteurs de ces attaques internes peuvent être des employés malintentionnés de l'organisation ou des cyber-espions se faisant passer pour des sous-traitants, des tiers ou des télétravailleurs. Ils sont capables de travailler de manière autonome ou avec des États-nations, réseaux criminels ou entreprises concurrentes. Bien qu'il puisse également s'agir de fournisseurs ou de prestataires distants situés dans le monde entier, ils disposent en règle générale d'un certain niveau d'accès légitime aux systèmes et données de l'organisation.

Menaces IoT

Après qu'une fuite de données a mis au jour les informations personnelles de plus de 3 000 utilisateurs de Ring, un fournisseur de sécurité à domicile appartenant à Amazon, les malfaiteurs ont profité de la fuite et ont piraté les sonnettes vidéo et les caméras de surveillance des domiciles de nombreuses personnes. Dans le cadre d'un recours collectif en 2020, des dizaines de personnes ont indiqué avoir été victimes de harcèlement, de menaces et de chantage via leurs appareils Ring. Des experts affirment que ces attaques recensées ne sont que la partie émergée de l'iceberg, puisque Ring a vendu plus de 1,4 million de sonnettes vidéo rien qu'en 2020. Depuis, Ring a mis en place un cryptage vidéo de bout en bout pour se prémunir contre de futurs piratages, mais étant donné l'omniprésence des appareils IoT, il ne s'agit certainement pas de la dernière attaque de ce type.

Ce que vous devez savoir :

On estime qu'il existe environ 13,1 milliards de dispositifs IoT connectés dans le monde ; un nombre qui devrait passer à 30 milliards d'ici 2030. Le manque courant d'infrastructure de sécurité de ces dispositifs crée des vulnérabilités flagrantes dans le réseau qui augmentent de façon exponentielle la surface d'attaque et la rendent vulnérable aux logiciels malveillants. Les attaques lancées sur des dispositifs IoT incluent notamment des menaces DDoS, des ransomwares et des attaques par ingénierie sociale.

Comment l'attaque se produit :

Les pirates informatiques et les États-nations malveillants peuvent exploiter les vulnérabilités des dispositifs IoT connectés avec des logiciels malveillants sophistiqués pour accéder à un réseau afin de superviser les utilisateurs ou de voler la propriété intellectuelle, des données classifiées ou d'identification personnelle et d'autres informations critiques. Une fois qu'ils ont infiltré un système IoT, les pirates peuvent également utiliser leur nouvel accès pour se déplacer latéralement vers d'autres appareils connectés ou pour accéder à un plus grand réseau à diverses fins malveillantes.

D'où provient l'attaque :

Les attaques peuvent provenir de n'importe où dans le monde. Mais comme de nombreux secteurs verticaux tels que le gouvernement, l'industrie et la santé déploient une infrastructure IoT sans sécurité appropriée, ces systèmes sont la cible d'attaques par des États-nations hostiles et des organisations de cybercriminalité sophistiquées. Contrairement aux attaques contre les infrastructures technologiques, les attaques contre les systèmes civiques ou de santé connectés peuvent entraîner des perturbations généralisées, un climat de panique et la mise en danger d'individus.

Menaces IoMT

En raison de la prévalence et de la complexité des attaques contre les organisations de soins de santé, et du risque pour la confidentialité et la sécurité des patients, les fournisseurs sont la cible de critiques en matière de sécurité des dispositifs médicaux. Après des attaques telles que l'attaque du ransomware WannaCry, les législateurs ont souligné la gravité des problèmes de cybersécurité qui affectent les logiciels et équipements hérités. La FDA a également émis de nouvelles recommandations pour les fabricants de dispositifs, mais les entreprises ne sont pas contraintes de les suivre, car il ne s'agit pas de mandats légaux.

Ce que vous devez savoir :

L'Internet des objets médicaux (IoMT) a révolutionné les soins de santé tels que nous les connaissons, notamment pendant la pandémie de COVID-19. L'IoMT a le pouvoir de générer d'innombrables opportunités pour diagnostiquer, traiter et gérer la santé et le bien-être d'un patient, et constitue la clé pour réduire les coûts tout en améliorant la qualité des soins. Cependant, à mesure que le nombre d'appareils connectés augmente inéluctablement, le risque de cybersécurité s'accroît également. Depuis 2020, plus de 25 % des cyberattaques ciblant les prestataires de soins de santé impliquent l'IoMT.

Comment l'attaque se produit :

Étant donné que les technologies numériques vieillissent plus rapidement que leurs homologues physiques (qui ont généralement un long cycle de vie), les équipements et logiciels obsolètes créent, pour les hôpitaux et les patients, de graves vulnérabilités en matière de cybersécurité. Actuellement, les fabricants n'autorisent pas les clients à dépanner et réparer leurs propres appareils, et vont même jusqu'à annuler les garanties s'ils le font. Ajoutez à cela le manque de chiffrement, des information d'identification codées en dur et des contrôles de sécurité laxistes, et vous comprendrez pourquoi les organisations de soins de santé ne peuvent pas faire grand-chose pour atténuer les risques liés aux appareils hérités.

D'où provient l'attaque :

Les attaquants IoMT ont la capacité et les ressources pour identifier les prestataires de santé avec une position de sécurité ambiguë, une mauvaise visibilité des actifs et des stocks, et des systèmes et appareils obsolètes.

Virus macro

Le virus Melissa, l'un des incidents dus à un virus les plus connus de tous les temps apparu à la fin des années 90, n'était autre qu'un virus macro. Un ordinateur infecté par Melissa piratait le système de messagerie Microsoft Outlook de l'utilisateur et envoyait des messages chargés de virus aux 50 premières adresses de sa liste de diffusion. Le virus s'est propagé à une vitesse incroyable et a provoqué des dommages impressionnants dans le monde entier : environ 80 millions de dollars pour le nettoyage et la réparation des systèmes et réseaux infectés. Bien que l'âge d'or des virus macro soit révolu, ces attaques persistent, et elles ne ciblent plus uniquement Windows : de récentes attaques ont également pris pour cible des utilisateurs de Mac.

Virus macro

Ce que vous devez savoir :

Un virus macro est un virus informatique écrit dans un langage macro identique à celui que l'on utilise pour les applications logicielles. Certaines applications, telles que Microsoft Office, Excel et PowerPoint, permettent d'intégrer des programmes de macros dans des documents de sorte que les macros s'exécutent automatiquement à l'ouverture du document. Elles déclenchent un mécanisme distinct par lequel des instructions informatiques malveillantes peuvent se propager. C'est l'une des raisons pour lesquelles il peut être dangereux d'ouvrir des pièces jointes imprévues ou des e-mails provenant d'expéditeurs non reconnus. De nombreux programmes antivirus sont capables de détecter les virus macro, mais leur comportement peut encore être difficile à repérer.

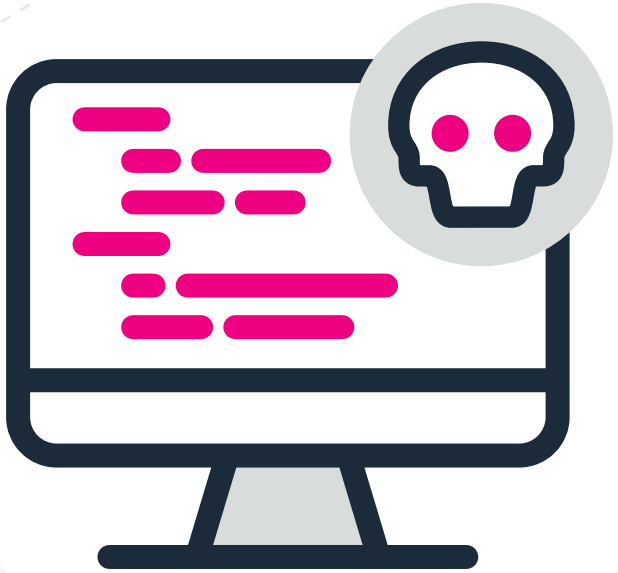
Comment l'attaque se produit :

Les virus macro se propagent souvent par le biais d'e-mails de phishing contenant des pièces jointes intégrant le virus. Comme l'e-mail semble provenir d'une source crédible, de nombreux destinataires l'ouvrent. Lorsqu'elle est exécutée, la macro infectée peut accéder à tous les autres documents de l'ordinateur de l'utilisateur et les infecter. Les virus macro se propagent chaque fois qu'un utilisateur ouvre ou ferme un document infecté. Ils s'exécutent sur des applications et non sur des systèmes d'exploitation. Les méthodes les plus courantes de propagation des virus macro sont le partage de fichiers sur un disque ou un réseau et l'ouverture d'un fichier joint à un e-mail.

D'où provient l'attaque :

Si les virus macro ne font plus partie des attaques malveillantes les plus en vogue, principalement parce que les logiciels antivirus sont davantage aptes à les détecter et à les désactiver, ils représentent toujours une menace importante. Une recherche rapide sur Google sur « macro virus » vous donnera des instructions pour créer des virus macro et des outils qui aident les non-programmeurs à créer ces virus. En théorie, toute personne disposant d'un accès Internet peut facilement créer un virus macro.

PowerShell malveillant



Les séquences d'attaques qui exploitent le très populaire PowerShell sont de plus en plus répandues auprès des cybercriminels et des groupes de cyberespionnage en raison de leur capacité à propager des virus sur un réseau facilement. De célèbres malfaiteurs tels que APT29 (ou Cozy Bear) utilisent des scripts PowerShell pour réunir des informations essentielles pour appuyer des cyberattaques encore plus sophistiquées. En 2020, le célèbre groupe de pirates APT35 (ou Charming Kitten) a utilisé Powershell dans le cadre d'une attaque par ransomware ciblant une organisation caritative pour réunir et exfiltrer des données d'un gouvernement local américain.

PowerShell malveillant

Ce que vous devez savoir :

PowerShell est un outil de ligne de commande et de script développé par Microsoft et basé sur .NET (prononcé « dot net »), qui permet aux administrateurs et utilisateurs de modifier les paramètres système ainsi que d'automatiser les tâches. L'interface de ligne de commande (ILC) offre une gamme d'outils et de la flexibilité, ce qui en fait un shell et un langage de script populaires. Les acteurs malveillants ont également reconnu les avantages de PowerShell : agir sans être détecté sur un système en tant que point de terminaison de code et effectuer des actions en coulisses.

Comment l'attaque se produit :

Étant donné que 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 points de terminaison de code, la logique derrière ce type d'attaque est parfaitement claire. Il est facile (d'autant plus pour les attaquants) d'accéder au système et de s'y implanter. Les logiciels malveillants n'ont pas besoin d'être installés pour s'exécuter ou exécuter le script malveillant. Ce qui signifie que le pirate peut contourner sans effort les moyens de détection, esquiver l'analyse des fichiers exécutable et faire des ravages à sa guise.

D'où provient l'attaque :

Ce type d'attaque est plus sophistiqué que les autres méthodes et est généralement exécuté par un pirate informatique qui sait exactement ce qu'il fait (par opposition à un amateur qui pourrait recourir à des attaques par force brute). Toujours furtifs dans leur approche, ils sont capables de brouiller les pistes et savent se déplacer latéralement sur un réseau.

Attaque de l'homme du milieu

Début 2022, Microsoft a découvert une campagne d'hameçonnage ciblant les utilisateurs d'Office365. Les attaquants ont falsifié une page d'identification d'Office 365 pour collecter des identifiants pour utilisation et détournement ultérieurs. Pour ce faire, les malfaiteurs utilisent un kit d'hameçonnage Evilginx2, un framework d'attaque de l'homme du milieu (MITM) utilisé pour récupérer des identifiants de connexion et des cookies de session, pour contourner l'authentification à deux facteurs et ainsi pirater le processus d'authentification. Microsoft a ajouté à son article de blog : « Veuillez noter qu'il ne s'agit pas d'une vulnérabilité de l'authentification multifacteurs (MFA) ; comme les attaques d'hameçonnage AiTM volent les cookies de session, le malfaiteur est authentifié sur une session au nom de l'utilisateur, peu importe la méthode d'identification utilisée par ce dernier. »

Attaque de l'homme du milieu

Ce que vous devez savoir :

L'attaque MITM ou AiTM (adversary-in-the-middle) consiste à mettre en place un serveur proxy qui intercepte la session d'identification de la victime afin que le malfaiteur puisse s'insérer en tant que relais entre les deux parties ou systèmes, gagnant accès ou dérobant ainsi des informations confidentielles. Ce type d'attaque permet à un acteur malveillant d'intercepter, d'envoyer et de recevoir des données destinées à une autre personne (ou qui ne sont pas destinées à être envoyées du tout) sans qu'aucune des parties externes ne s'en aperçoive à temps.

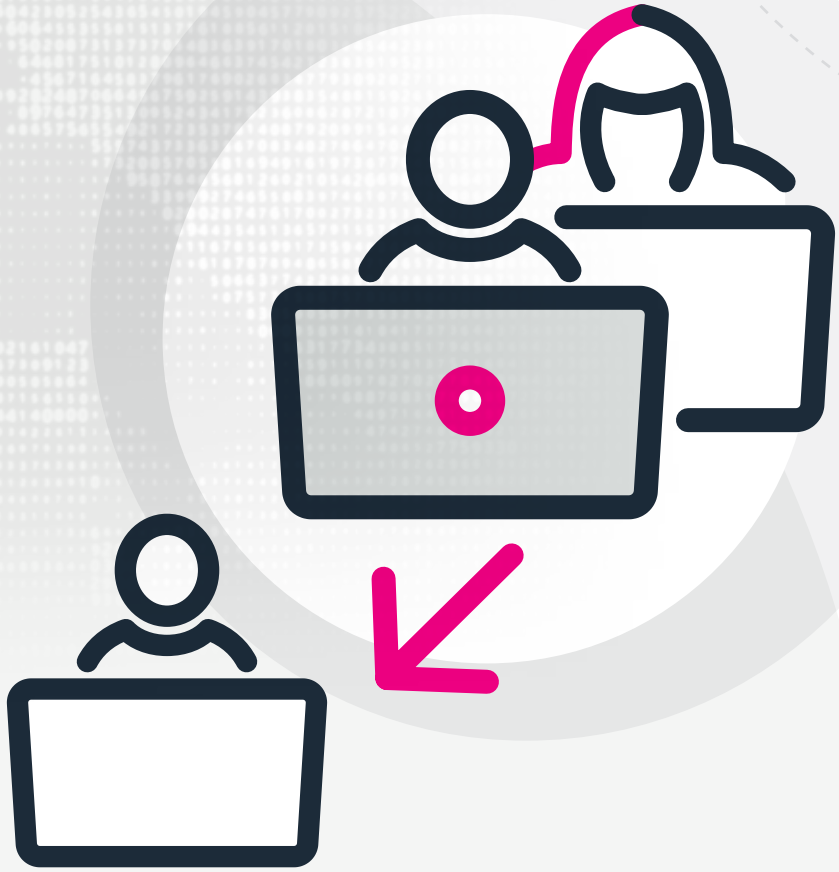
Comment l'attaque se produit :

Pratiquement n'importe qui peut exécuter une attaque de l'homme du milieu. Depuis l'implémentation de HTTPS Everywhere, ces types d'attaques sont toutefois plus difficiles à exécuter, et donc plus rares. Lors d'une attaque MITM, le pirate informatique se trouve entre l'utilisateur et le site Web réel (ou un autre utilisateur) et transmet les données entre eux pour exfiltrer les données qu'il souhaite de l'interaction.

D'où provient l'attaque :

Les améliorations apportées aux technologies de sécurité ayant compliqué l'exécution des attaques MITM, les seuls groupes qui les tentent sont des pirates informatiques sophistiqués ou des acteurs étatiques. En 2018, la police néerlandaise a découvert quatre membres du groupe de hackers russe Fancy Bear stationnés à l'extérieur de l'Organisation pour l'interdiction des armes chimiques en Hollande, tentant une infiltration de type MITM pour dérober les informations d'identification des employés. Plus tard dans la même année, les gouvernements américain et britannique ont publié des avertissements concernant des acteurs parrainés par l'État russe qui ciblaient activement les routeurs dans les foyers et les entreprises à des fins d'exfiltration MITM.

Attaque par mascarade



Nombre d'entre nous n'ont pas oublié quand Target a subi une violation massive de données de cartes de crédit touchant plus de 40 millions de comptes clients. L'investigation menée par l'état a révélé que les attaquants ont volé les informations d'identification du fournisseur de services CVC de Target, Fazio Mechanical Services. Après avoir utilisé les détails du fournisseur tiers pour accéder à l'application Web interne de Target, ils ont installé des logiciels malveillants sur le système et capturé des noms, numéros de téléphone, numéros de carte de crédit, codes de vérification de carte de crédit, ainsi que d'autres informations hautement sensibles.

Attaque par mascarade

Ce que vous devez savoir :

Une attaque par mascarade se produit lorsqu'un acteur malveillant utilise une identité falsifiée ou légitime (mais volée) pour obtenir un accès non autorisé à la machine d'un individu ou au réseau d'une entreprise à l'aide d'informations d'identification légitimes. Selon le niveau d'accès fourni par les autorisations, les attaques par mascarade peuvent donner aux attaquants l'accès à un réseau entier.

Comment l'attaque se produit :

Une attaque par mascarade peut se produire après le vol d'informations d'identification d'utilisateurs ou via l'authentification sur des machines et dispositifs non protégés ayant accès au réseau cible.

D'où provient l'attaque :

Lorsqu'ils sont des initiés, les attaquants peuvent obtenir un accès en usurpant les domaines de connexion ou en utilisant des enregistreurs de frappe pour voler des informations d'authentification légitimes. Les attaques peuvent également se produire physiquement en profitant de cibles qui laissent des machines sans supervision, comme quand un collègue accède à l'ordinateur portable d'un autre pendant son absence. De manière générale, les méthodes d'authentification faibles qui peuvent être dupées par des parties externes sont généralement à l'origine du problème.

Attaque Spectre et Meltdown

La plupart des attaques de cybersécurité exploitent une vulnérabilité, telle qu'une erreur de codage ou une mauvaise conception. Mais toutes les attaques ne se valent pas. En 2018, deux chercheurs de Google ont découvert un nouveau type d'attaque qui a affecté tous les fabricants de puces informatiques et potentiellement exposé des milliards aux attaques Spectre et Meltdown.

Attaque Spectre et Meltdown

Ce que vous devez savoir :

L'attaque Spectre et Meltdown 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 sur l'isolement de la mémoire pour protéger les informations d'un utilisateur. Un « meltdown » fait référence à la rupture des barrières de protection entre un système d'exploitation et un programme, tandis qu'un « spectre » fait référence à celles qui isolent les informations de deux applications.

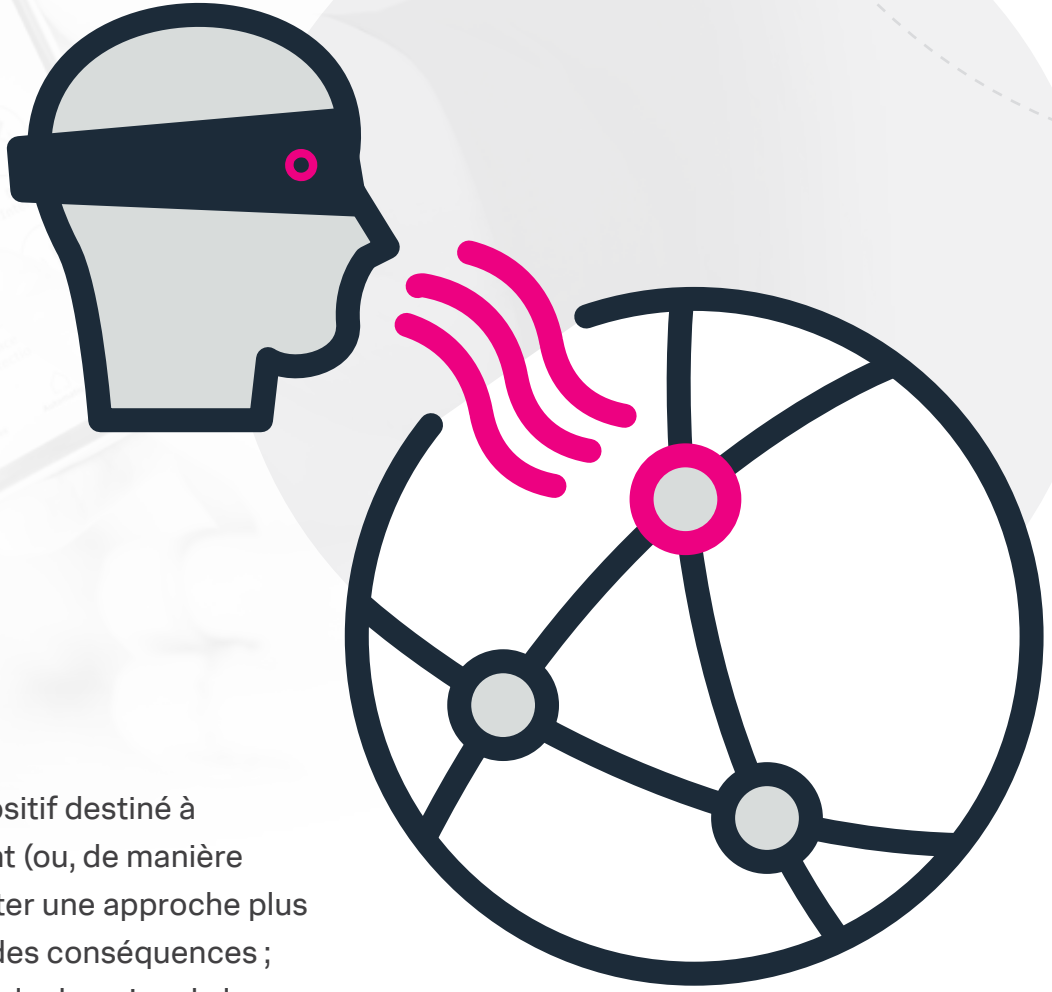
Comment l'attaque se produit :

Une attaque Spectre et Meltdown exploite les vulnérabilités critiques des processeurs modernes qui permettent involontairement d'accéder aux données stockées en mémoire. L'attaque brise la norme informatique selon laquelle les programmes ne sont pas autorisés à lire les données d'autres programmes. Les informations que les attaquants ciblent généralement sont les mots de passe stockés dans les gestionnaires de mots de passe ou les navigateurs, ainsi que les e-mails, dossiers financiers et informations personnelles telles que les photos et messages instantanés. Mais cette attaque ne se limite pas aux ordinateurs personnels. Elle peut cibler presque tous les dispositifs dotés d'un processeur, comme un téléphone portable ou une tablette.

D'où provient l'attaque :

L'attaque Spectre et Meltdown peut provenir de presque n'importe où, et les recherches se sont pour l'instant principalement concentrées sur la nature unique de cette attaque, et non sur ses auteurs.

Reniflage de réseau



Les serrures intelligentes sont un nouveau type de dispositif destiné à protéger votre habitation *et* à faciliter l'entrée en cliquant (ou, de manière plus appropriée, en appuyant) sur un bouton. Mais adopter une approche plus futuriste pour fortifier votre demeure peut avoir de lourdes conséquences ; c'est du moins ce qu'ont découvert des chercheurs dans le domaine de la sécurité. Une serrure intelligente, commercialisée un peu à tort comme la « serrure la plus intelligente de tous les temps », pourrait être interceptée via le trafic réseau entre l'application mobile et la serrure. Plus effrayant encore, cette interception peut être effectuée à l'aide de dispositifs de détection de réseau peu coûteux et facilement disponibles.

Reniflage de réseau

Ce que vous devez savoir :

Le reniflage de réseau, également connu sous le nom de reniflage de paquets, correspond à la capture, la supervision et l'analyse en temps réel des données qui circulent dans un réseau. Assistés par du matériel, des logiciels ou une combinaison des deux, les acteurs malveillants utilisent des outils de reniflage pour épier les données non chiffrées des paquets réseau, telles que les informations d'identification, les e-mails, les mots de passe, les messages et autres informations sensibles.

Comment l'attaque se produit :

À l'instar des scénarios de mise sur écoute dans lesquels un individu écoute les appels téléphoniques pour obtenir des données sensibles, le reniflage de réseau fonctionne en arrière-plan et épie silencieusement les informations échangées entre les entités d'un réseau. Pour ce faire, les attaquants placent un renifleur sur un réseau en installant un logiciel ou un matériel branché sur un appareil qui lui permet d'intercepter et d'enregistrer 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 sur le réseau avant d'être détectés.

D'où provient l'attaque :

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

Mais il peut également être initié par des pirates qui le font par malveillance ou des États-nations cherchant à voler des éléments de propriété intellectuelle. Comme les ransomware, les renifleurs de réseau peuvent être injectés dans le réseau en incitant la bonne personne à cliquer sur le bon lien. Les menaces internes ayant accès à du matériel sensible pourraient également être un vecteur d'attaque.

Redirection ouverte

En 2022, on a découvert qu'une énième campagne d'hameçonnage ciblant les utilisateurs de Facebook avait permis de récupérer des centaines de millions d'identifiants. La technique utilisée était courante : un lien est envoyé par message privé depuis un compte Facebook compromis. Ce lien effectue ensuite toute une série de redirections, généralement vers des pages de malvertising pour accumuler des vues et des clics (et des revenus pour le malfaiteur), pour finalement arriver sur une fausse page. Même si la technique de redirection d'hôte, aussi appelée redirection ouverte, n'a rien de nouveau, l'ampleur de cette campagne est remarquable. Des experts ont découvert que, sur les 400 pages exploitées, l'une avait reçu à elle seule 2,7 millions de visiteurs en 2021 et 8,5 millions au total en juin 2022. Lors d'un entretien avec des experts, l'attaquant s'est vanté d'avoir récolté 150 $ toutes les 1 000 visites d'utilisateurs Facebook américains, ce qui équivaudrait à un profit de 59 millions de dollars.

Redirection ouverte

Ce que vous devez savoir :

Les attaques par redirection d'hôte sont très répandues et de plus en plus subversives, car les pirates redoublent de créativité pour tromper leurs cibles. Les attaquants utilisent la redirection d'URL pour gagner la confiance de l'utilisateur avant de frapper immanquablement. Ils utilisent généralement des URL intégrées, un fichier .htaccess ou des tactiques de phishing afin de rediriger le trafic vers un site Web malveillant.

Comment l'attaque se produit :

Le pirate informatique peut envoyer un e-mail de phishing contenant une copie de l'URL du site Web à la victime sans méfiance. Si le site semble légitime, les utilisateurs peuvent partager par inadvertance des informations personnelles en remplissant les invites ou les formulaires qui s'affichent. Les attaquants peuvent passer au niveau supérieur en incorporant de faux domaines de commande et contrôle dans des logiciels malveillants et en hébergeant du contenu malveillant sur des domaines qui imitent fidèlement les serveurs d'entreprises.

D'où provient l'attaque :

Les origines de cette attaque ne sont pas aussi importantes que la cible. Cette attaque vise 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 de simplicité (elle peut être aussi simple que l'enregistrement d'un nom de domaine), elle peut provenir de presque n'importe où.

Pass the Hash

La fameuse violation de plus de 40 millions de comptes clients de Target a partiellement abouti grâce à la célèbre technique d'attaque appelée Pass the Hash (PtH). Les pirates ont eu recours au PtH pour accéder à une variable de hachage NT qui leur permettrait de se connecter au compte administrateur Active Directory sans le mot de passe en texte brut, leur donnant ainsi les privilèges nécessaires pour créer un nouveau compte administrateur de domaine et l'ajouter au groupe d'administrateurs de domaine. Cet enracinement dans le système leur a donné la possibilité de voler des informations personnelles et des détails de carte de paiement aux clients de Target.

Pass the Hash

Ce que vous devez savoir :

Pass the Hash permet à un attaquant d'authentifier le mot de passe d'un utilisateur avec le hachage NTLM ou LanMan sous-jacent au lieu du mot de passe en texte brut associé. Une fois que le pirate possède un nom d'utilisateur valide et les valeurs de hachage de son mot de passe, il peut sans problème accéder au compte de l'utilisateur et exécuter des actions sur des systèmes locaux ou distants. Essentiellement, les hachages remplacent les mots de passe d'origine à partir desquels ils ont été générés.

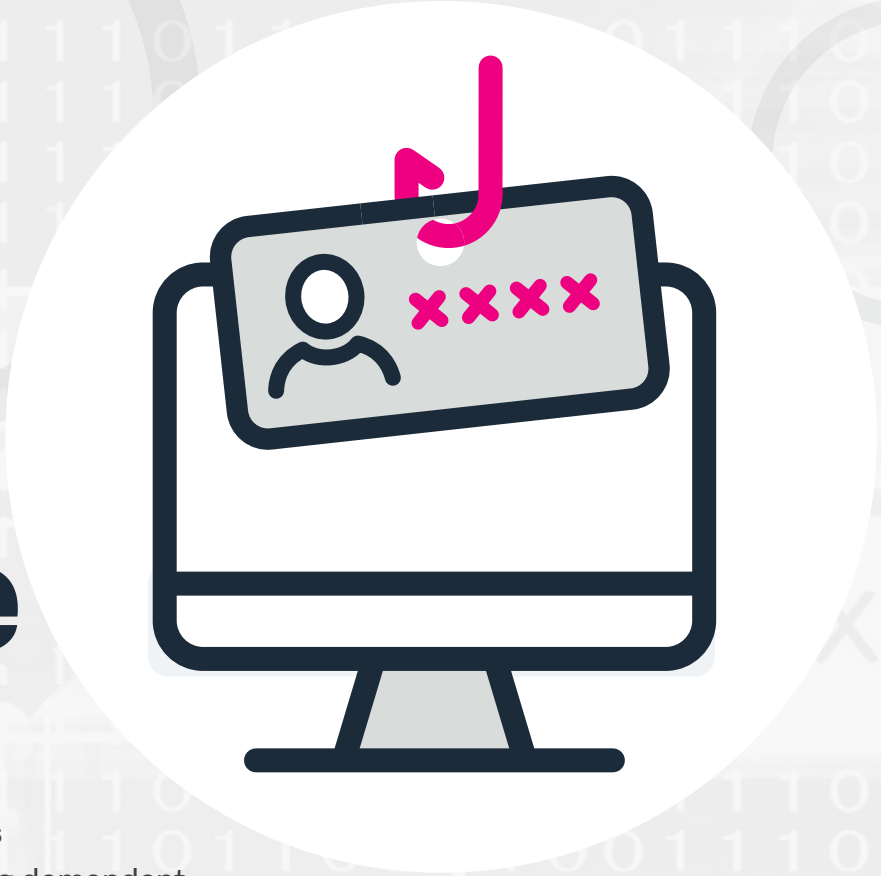
Comment l'attaque se produit :

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, mais envoyé sous la forme de hachage en réponse à un schéma d'authentification de type stimulation-réponse. Lorsque cela se produit, les hachages de mot de passe valides pour le compte utilisé sont capturés à l'aide d'une technique d'accès aux informations d'identification.

D'où provient l'attaque :

Ce type d'attaque est plus sophistiqué que les autres méthodes et est généralement exécuté par des groupes de hackers. Ces malfaiteurs sont souvent organisés et ciblent une entreprise ou une personne spécifique dans un but politique ou financier.

Hameçonnage



Plusieurs attaques de phishing se démarquent des autres, notamment l'attaque désormais tristement célèbre à l'encontre de Sony. Les pirates informatiques ont exécuté l'attaque en envoyant des e-mails de phishing demandant la vérification des identifiants Apple aux ingénieurs système, administrateurs réseau et autres employés sans méfiance disposant d'informations d'identification système. Les attaquants ont subtilisé des gigaoctets de fichiers comprenant des e-mails, des rapports financiers et des copies numériques de films récemment sortis. Qui plus est, les acteurs malveillants ont ensuite déployé sur les ordinateurs des postes de travail de Sony des logiciels malveillants qui ont effacé les disques durs. Quelques semaines plus tard, le FBI a officiellement désigné le gouvernement nord-coréen comme le cerveau de l'attaque.

Hameçonnage

Ce que vous devez savoir :

Une attaque de phishing incite les clients, les utilisateurs ou les employés des banques à cliquer sur un lien malveillant qui les redirige souvent vers un faux site où ils saisissent des informations d'identification personnelle telles que des numéros de compte bancaire, des informations de carte de crédit ou des mots de passe, transmises par e-mail, messagerie instantanée ou un autre moyen de communication. Attention : bien que ces faux sites paraissent convaincants, les attaquants récolteront toutes les informations que vous leur soumettez. Ils peuvent aussi lancer des logiciels malveillants visant à voler des fonds sur vos comptes, des informations d'identification personnelle sur les clients ou d'autres actifs critiques.

Comment l'attaque se produit :

En règle générale, vous recevez un e-mail semblant provenir de quelqu'un que vous connaissez (un message qui semble provenir d'un responsable ou d'un collègue, par exemple) et qui vous invite à ouvrir des pièces jointes malveillantes ou à cliquer sur des liens qui vous dirigent vers des pages web pratiquement identiques à celles de sites légitimes.

D'où provient l'attaque :

Il y a à peine quelques décennies, un grand nombre d'attaques de phishing provenaient du Nigeria dans le cadre de ce que l'on appelait la fraude 419 (ou scam 419), en raison de la désignation de cette fraude dans le code pénal nigérian. Aujourd'hui, les attaques de phishing proviennent du monde entier, et selon l'Institut InfoSec, bon nombre d'entre elles se produisent dans les pays BRIC (Brésil, Russie, Inde et Chine). En raison de la simplicité et de la disponibilité des kits de phishing, même les pirates avec des compétences techniques minimales ont la possibilité de lancer des campagnes de phishing. Les personnes à l'origine de ces campagnes vont des pirates informatiques isolés aux cybercriminels organisés.

Charges utiles d'hameçonnage

L'un des plus grands cybercrimes de tous les temps, avec le plus grand nombre d'accusés inculpés pour le même crime, a été celui que le FBI a baptisé Operation Phish Phry. L'attaque a entraîné une enquête internationale pour hameçonnage après avoir ciblé des centaines de détenteurs de clients bancaires et de cartes de crédit, qui ont reçu des e-mails contenant des liens vers de faux sites web financiers d'apparence authentique. Sur le site, les victimes étaient invitées à saisir leurs numéros de compte et leurs mots de passe dans des formulaires frauduleux.

Charges utiles d'hameçonnage

Ce que vous devez savoir :

Malgré sa simplicité, l'hameçonnage reste la cybermenace la plus répandue et la plus dangereuse. En effet, les recherches montrent que jusqu'à 91 % de toutes les attaques abouties sont initiées par un e-mail d'hameçonnage.

Ces e-mails utilisent des domaines frauduleux, des techniques d'extraction d'e-mails, des noms de contacts familiers insérés 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 néfaste ou à saisir des informations personnelles sensibles que les auteurs peuvent alors intercepter. La « charge utile » fait référence aux données transmises qui constituent le message. Les en-têtes et les métadonnées ne sont envoyés que pour permettre la livraison de la charge utile à la bonne personne.

Comment l'attaque se produit :

Cette attaque présente un schéma d'attaque typique : dans un premier temps, l'attaquant envoie un e-mail d'hameçonnage et le destinataire télécharge le fichier joint, qui est généralement un fichier .docx ou .zip contenant un fichier .lnk. Ensuite, le fichier .lnk exécute un script PowerShell et enfin, le script Powershell exécute un shell inversé pour faire aboutir l'attaque.

D'où provient l'attaque :

Étant donné que cette attaque ne nécessite pas un haut niveau de sophistication et que l'hameçonnage est au centre de la plupart des cyberattaques, elle peut provenir de n'importe où dans le monde. L'opération Phish Phry en est un parfait exemple. Lors de cette attaque, le FBI a arrêté plus de 50 individus en Californie, au Nevada et en Caroline du Nord, tout en inculpant environ 50 citoyens égyptiens en lien avec l'attaque.

Harponnage

De nos jours, les responsables d'attaque de harponnage ciblent non seulement des victimes plus importantes, mais ils s'inspirent également de l'escroquerie sentimentale, en appâtant leurs victimes avec des profils attirants pour leur faire télécharger des malwares sur leurs ordinateurs. En 2021, des chercheurs ont dévoilé une attaque par malware ciblé et ingénierie sociale qui a duré plusieurs années et l'ont attribuée au célèbre groupe cybercriminel TA456, lié à l'État iranien. À l'aide d'un faux profil sur les réseaux sociaux nommé « Marcella Flores », TA456 a noué une relation romantique avec un employé d'une petite filiale d'une entreprise de défense aérospatiale. Le malfaiteur en a profité quelques mois plus tard pour envoyer un fichier de malware via une chaîne d'e-mails professionnels à des fins de reconnaissance. Une fois le malware, baptisé LEMPO, infiltré dans la machine, il a exfiltré des données hautement confidentielles pour les envoyer au malfaiteur, tout en masquant sa localisation pour éviter toute détection.

Harponnage

Ce que vous devez savoir :

Sous-ensemble de l'hameçonnage, le harponnage se produit lorsque des cybercriminels ciblent des victimes de manière sélective avec un e-mail spécifique et personnalisé pour inciter les employés ou les personnes à divulguer des données financières ou exclusives ou à déverrouiller l'accès au réseau. Les harponnages ciblent les individus qui ont accès à des informations sensibles ou des maillons faibles du réseau. Les cadres dirigeants, les membres de comité de direction ou les administrateurs disposant de privilèges élevés sont des cibles de choix car ils ont accès à des systèmes critiques et à des informations confidentielles.

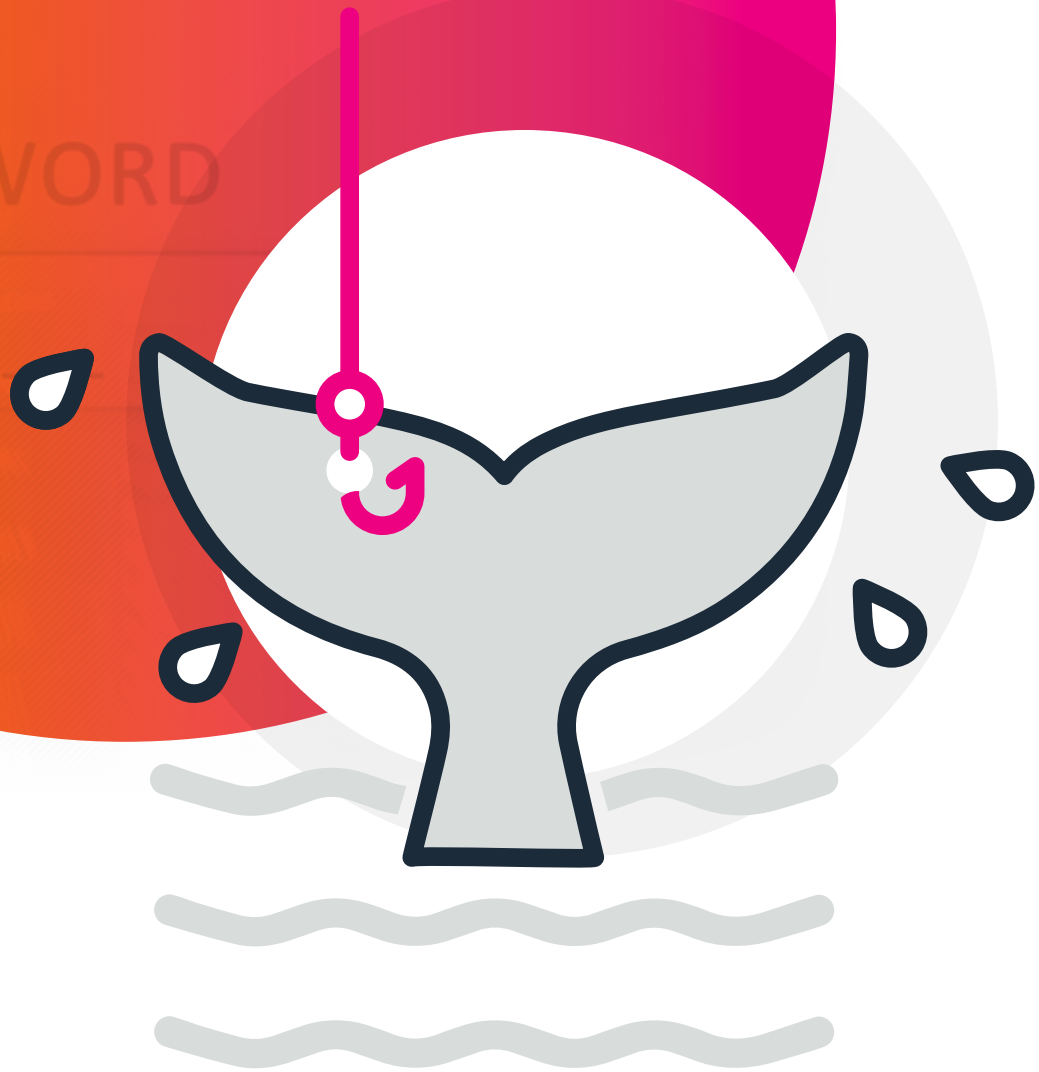
Comment l'attaque se produit :

Les harponneurs font des recherches pour identifier des cibles et leurs postes à l'aide de réseaux sociaux tels que LinkedIn. À partir de là, ils créent de fausses adresses pour envoyer des messages hautement personnalisés et d'apparence authentique afin d'infiltrer l'infrastructure et les systèmes de la cible. Une fois que les pirates ont accès à l'environnement, ils tentent de mettre en œuvre des stratagèmes encore plus élaborés.

D'où provient l'attaque :

À l'origine de cette attaque, on retrouve tant des individus que des organisations. Toutefois, de nombreuses tentatives de harponnage sont le fruit d'organisations criminelles appuyées par un gouvernement et disposant des ressources nécessaires pour faire des recherches sur leurs cibles et contourner des filtres de sécurité robustes.

Whaling



Pourquoi s'attaquer au petit poisson quand on peut viser la baleine ? En 2020, le fonds de spéculation australien Levitas Capital l'a découvert à ses dépens lorsque des pirates ont lancé une attaque de whaling furtive ciblant directement l'un des fondateurs. Les malfaiteurs ont réussi à accéder au réseau du fonds spéculatif après avoir envoyé au dirigeant un faux lien Zoom qui installe des malwares lorsque l'on y accède. Le code malveillant permettait aux attaquants d'infiltrer le compte de messagerie ciblé et par la suite de créer de fausses factures adressées au fiduciaire et à l'administrateur tiers du fonds, qui a ensuite approuvé des demandes de virement pour un montant de 8,7 millions de dollars dérobés. Les fausses factures demandaient également de verser 1,2 million de dollars à un fonds d'investissement privé suspect : Unique Star Trading. Les pertes furent si importantes et préjudiciables que Levitas Capital fut contraint de mettre la clé sous la porte.

Whaling

Ce que vous devez savoir :

Une attaque de whaling consiste à cibler une personne haut placée, par exemple un PDG. La cible est toujours une personne spécifique, alors qu'un e-mail d'hameçonnage peut viser n'importe qui dans une entreprise. Les pirates informatiques s'attaquent aussi généralement à des cibles connues, car elles peuvent posséder des informations importantes ou sensibles.

Comment l'attaque se produit :

La technique utilisée dans une attaque de whaling est une pratique d'hameçonnage classique. La cible reçoit un e-mail d'apparence authentique l'invitant généralement à cliquer sur un lien contenant un code malveillant ou menant à un site Web qui demande des informations sensibles, telles qu'un mot de passe.

D'où provient l'attaque :

L'hameçonnage est le point d'entrée le plus courant d'une cyberattaque, ce qui signifie qu'une attaque de whaling peut provenir de n'importe où dans le monde.

L'attaque de Levitas Capital, par exemple, a été attribuée à un collectif de cybercriminels de plusieurs régions, avec des paiements envoyés à Bank of China et United Overseas Bank à Singapour.

Compromission d'utilisateur privilégié

Début 2022, le groupe de cybercriminels Lapsus$, supposément géré par un adolescent d'Oxford, s'est vanté publiquement d'avoir réussi à pirater Okta, un fournisseur de services d'authentification unique utilisé par des milliers d'organisations et gouvernement du monde entier. Lapsus$ a eu accès à un compte administratif Okta de niveau « Super User » via un technicien de support tiers et a pu accéder à son ordinateur portable pendant cinq jours, avec un accès privilégié à certains systèmes d'Okta. Le groupe cybercriminel a communiqué à propos de l'attaque sur son compte Telegram, allant même jusqu'à publier des captures d'écran montrant les systèmes d'Okta. Mais le groupe ne ciblait pas véritablement Okta : il ciblait ses milliers de clients. Une semaine plus tard, le groupe de pirates avait 15 000 followers de plus sur son compte Telegram, laissant craindre d'autres attaques.

Compromission d'utilisateur privilégié

Ce que vous devez savoir :

Il est communément admis que de nombreuses violations de données majeures trouvent leur origine dans l'abus d'identifiants privilégiés. Il s'agit de comptes disposant de privilèges élevés, par exemple des utilisateurs avec des droits d'administrateur de domaine ou d'accès de niveau root. Les attaquants utilisent de plus en plus les identifiants d'utilisateurs privilégiés pour accéder aux ressources et aux informations d'une organisation et exfiltrer des données confidentielles. Un attaquant qui réussit à mettre la main sur les identifiants d'utilisateurs privilégiés peut prendre le contrôle de l'infrastructure d'une organisation pour modifier les paramètres de sécurité, exfiltrer des données, créer des comptes utilisateurs et bien plus encore, tout en paraissant légitime, et donc en étant plus difficile à détecter.

Comment l'attaque se produit :

Les attaquants essaient de mettre la main sur des identifiants de comptes privilégiés en employant des techniques d'ingénierie sociale, en envoyant des messages d'hameçonnage, en utilisant des malwares ou en réalisant des attaques « pass the hash ». Les organisations ouvrent leurs réseaux pour faire face à l'essor du télétravail. Elles doivent donc mettre en place un système complexe d'accès à distance utilisé par leurs fournisseurs et prestataires. Nombre de ces connexions, y compris au cloud, se font au moyen de comptes hautement privilégiés, et la supervision et le contrôle de tous ces accès est difficile, ce qui laisse bon nombre d'ouvertures aux malfaiteurs.

Une fois armés des identifiants, les attaquants s'introduisent dans les systèmes et dérobent tout ce qu'ils peuvent, comme les clés SSH, les certificats et les hashes d'administration de domaine. Et il suffit d'une seule compromission d'identifiants pour provoquer une grave violation de données susceptible de mener une organisation à sa ruine.

D'où provient l'attaque :

Étant donné qu'elle permet d'obtenir un accès important et difficile à détecter à toutes sortes de privilèges, la compromission d'utilisateur est très attrayante et couramment employée dans le cadre de différentes cyberattaques : cyberespionnage d'État-nation à des fins politiques ou cybercrime à caractère financier par des groupes tels que Lapsus$.

Ransomware

Selon la société de cybersécurité Emsisoft, en 2019, les attaques par ransomware ont touché au moins 948 agences gouvernementales, institutions scolaires et prestataires de soins de santé aux États-Unis, pour un coût potentiel supérieur à 7,5 milliards de dollars.

Dans le secteur médical, les effets potentiels de ces types d'attaques incluent le transfert de patients vers d'autres hôpitaux et l'impossibilité d'accéder aux dossiers médicaux (voire leur destruction définitive). Les centres de dispatching des urgences doivent s'appuyer sur des cartes imprimées et des registres papier pour suivre les équipes sur le terrain. Lorsque l'attaque touche les administrations, les services d'urgence locaux peuvent être perturbés. Et selon le procureur de Manhattan Cyrus Vance Jr., l'effet des ransomwares pourrait être aussi dévastateur et coûteux qu'une catastrophe naturelle comme l'ouragan Sandy.

Ce que vous devez savoir :

Un ransomware est une attaque dans laquelle un hôte infecté chiffre les données d'une victime et les garde en otage jusqu'à ce qu'elle paie une rançon à l'attaquant. Les récentes attaques par ransomware ont démontré que les pirates informatiques menacent de divulguer ou de vendre les données volées, augmentant ainsi considérablement les dommages potentiels de ce type d'attaque.

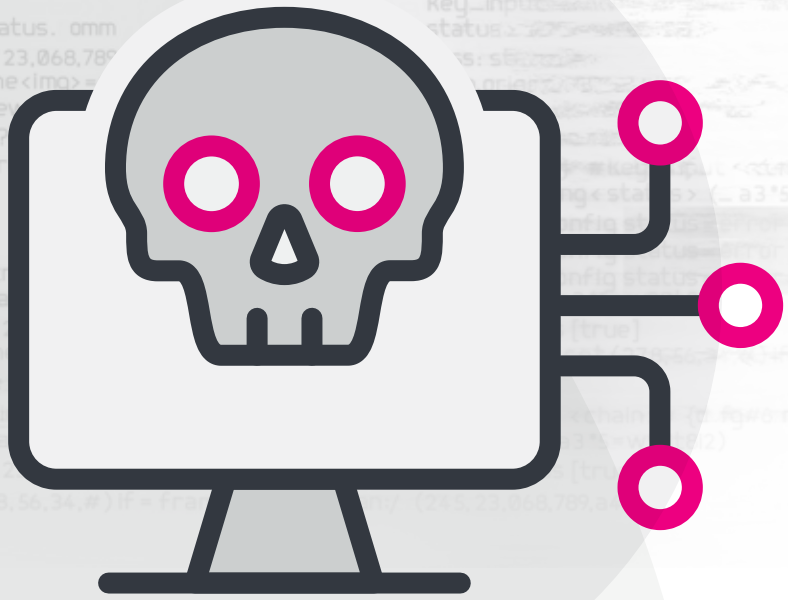
Il existe d'innombrables types de ransomwares, mais certains groupes sont particulièrement néfastes. Un gang bien connu, Blackmatter, a ciblé un certain nombre d'organisations essentielles à l'économie et aux infrastructures américaines, notamment du secteur agroalimentaire. Ryuk est un autre type de ransomware dont il faut se méfier. En 2019, Ryuk détenait le record de rançon la plus élevée avec 12,5 millions de dollars.

Comment l'attaque se produit :

Les attaquants peuvent déployer des ransomwares dans des entreprises et chez des particuliers via des campagnes de harponnage et de téléchargements furtifs, ainsi que via une exploitation traditionnelle basée sur des services à distance. Une fois le logiciel malveillant installé sur la machine de la victime, il présente une fenêtre contextuelle à l'utilisateur ou le dirige vers un site web l'informant que ses fichiers sont chiffrés et pourront être déchiffrés s'il paie la rançon.

D'où provient l'attaque :

Les ransomwares sont généralement l'œuvre de groupes de cybercriminels avancés : rester anonyme après avoir extorqué des gouvernements ou de grandes entreprises nécessite un certain degré de sophistication technologique. Cependant, depuis l'arrivée des cryptomonnaies, qui simplifient les transactions anonymes, la population générale est plus exposée aux attaques de ransomware.



Ransomware-as-a-Service

Le Ransomware-as-a-Service (RaaS) a été créé à des fins d'extorsion grâce au chiffrement ou au vol de données. L'auteur du ransomware met le logiciel à disposition de clients appelés affiliés, qui l'utilisent pour prendre en otage les données de leurs victimes, et ce avec très peu de compétence technique. WannaCry a mené l'une des plus vastes attaques RaaS à ce jour, avec plus de 400 000 ordinateurs infectés dans 150 pays. WannaCry a infiltré des réseaux à l'aide de la vulnérabilité EternalBlue dans l'implémentation par Microsoft du protocole Server Message Block (SMB). Cyberattaque à l'origine développée par la National Security Agency (NSA) américaine, l'agence n'a pas alerté Microsoft à propos des vulnérabilités et les a gardées secrètes pendant plus de cinq ans avant que la violation ne force l'agence à reconnaître le problème.

Ce que vous devez savoir :

Le RaaS est un modèle commercial entre opérateurs de ransomware et affiliés dans le cadre duquel des affiliés paient pour lancer des attaques par ransomwares développés par des opérateurs. Des kits RaaS permettent aux affiliés ne disposant pas des compétences ou n'ayant pas le temps de développer leur propre ransomware d'être opérationnels rapidement et à moindre coût. Un kit RaaS peut inclure une assistance 24 h/24, 7 j/7, des offres groupées, des avis d'utilisateurs, des forums et d'autres fonctionnalités identiques à celles proposées par des prestataires SaaS légitimes.

Comment l'attaque se produit :

Les ransomwares constituent un risque permanent pour les entreprises : un hôte infecté chiffre des données critiques et les prend en otage jusqu'à ce que la victime verse une rançon au malfaiteur. Les attaquants peuvent déployer des ransomware dans des entreprises via des campagnes de harponnage et de téléchargements furtifs, ainsi que via une exploitation traditionnelle basée sur des services à distance.

D'où provient l'attaque :

Étant donné que les kits RaaS sont simples à utiliser et faciles à trouver sur le dark web, où ils sont mis en avant, cette attaque peut provenir d'un pirate lambda ayant suffisamment d'argent pour acheter un kit.

Sécurité des routeurs et des infrastructures

Cisco a été victime d'une attaque des routeurs et des infrastructures au cours de laquelle un « implant » de routeur, appelé SYNful Knock, a été détecté dans 14 routeurs de quatre pays différents. SYNful Knock est un type de malware persistant qui permet à l'attaquant de prendre le contrôle d'un appareil et de compromettre son intégrité avec une image de logiciel Cisco IOS modifiée. Mandiant le décrit comme le fait d'avoir différents modules activés via le protocole HTTP et déclenchés par des paquets TCP créés sur l'appareil.

Sécurité des routeurs et des infrastructures

Ce que vous devez savoir :

L'ajout d'implants dans les routeurs est rare, on estime d'ailleurs en grande partie que leur nature et leur utilisation ne sont que théoriques. Cependant, de récents rapports de fournisseurs signalent plusieurs cas. Le vecteur d'infection initial ne semble pas exploiter de vulnérabilité zero-day. On estime que les identifiants sont soit ceux par défaut, soit découverts par l'attaquant dans le but d'installer la porte dérobée. Toutefois, la position du routeur dans le réseau en fait une cible idéale pour repénétrer le réseau ou l'infecter davantage.

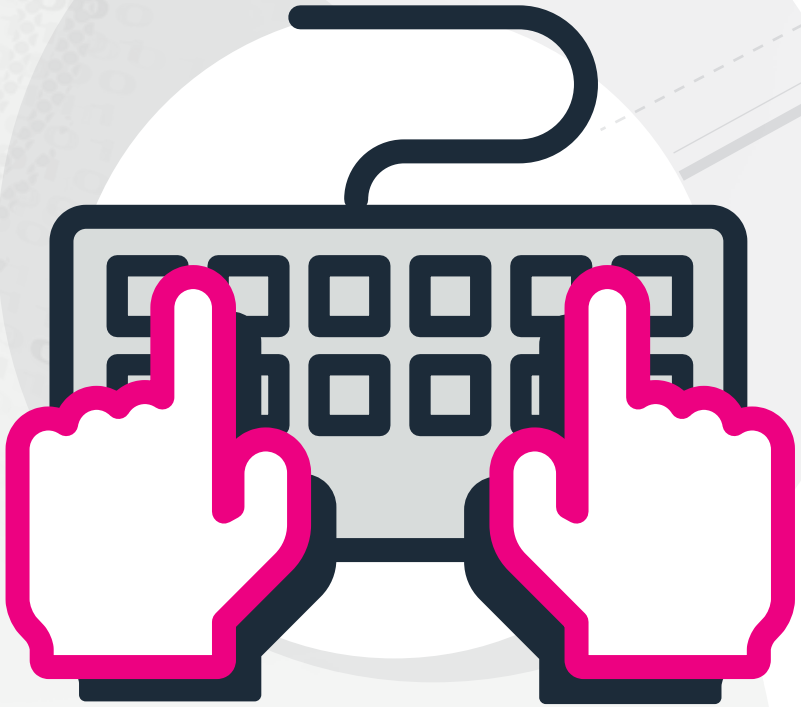
Comment l'attaque se produit :

Les périphériques réseau, comme les routeurs et les commutateurs, sont des ressources bien souvent négligées et exploitables par les malfaiteurs pour saboter une entreprise. Ils compromettent les périphériques réseau et peuvent ensuite obtenir un accès direct à l'infrastructure interne de l'entreprise. Ils augmentent ainsi la surface d'attaque et peuvent accéder aux services et données privés.

D'où provient l'attaque :

Les malfaiteurs montrent une propension à cibler ces périphériques essentiels afin de détourner et de rediriger le trafic réseau, flasher des systèmes d'exploitation avec une porte dérobée et exécuter des algorithmes cryptographiques affaiblis pour déchiffrer plus facilement le trafic réseau.

Informatique fantôme



Les applications de logiciel en tant que service sont devenues de plus en plus rapides et faciles à utiliser, et les employés peuvent désormais télécharger des solutions qui les aident à exécuter leurs tâches sur leurs postes de travail. Cependant, bon nombre d'entre eux utilisent ces applications sans trop se soucier de la sécurité. Il n'est donc pas surprenant qu'une étude Forbes Insights 2019 intitulée « Perception Gaps in Cyber Resilience: Where Are Your Blind Spots? » (Écarts de perception dans la cyber-résilience : où se situent les angles morts ?) ait révélé que plus d'une entreprise sur cinq a été victime d'un cyberincident provenant d'une ressource informatique non autorisée (ou « fantôme »).

Ce que vous devez savoir :

L'informatique fantôme fait référence aux applications et infrastructures informatiques que les employés utilisent à l'insu et/ou sans le consentement du service informatique de leur entreprise. Celles-ci peuvent inclure du matériel, des logiciels, des services web, des applications cloud et d'autres programmes.

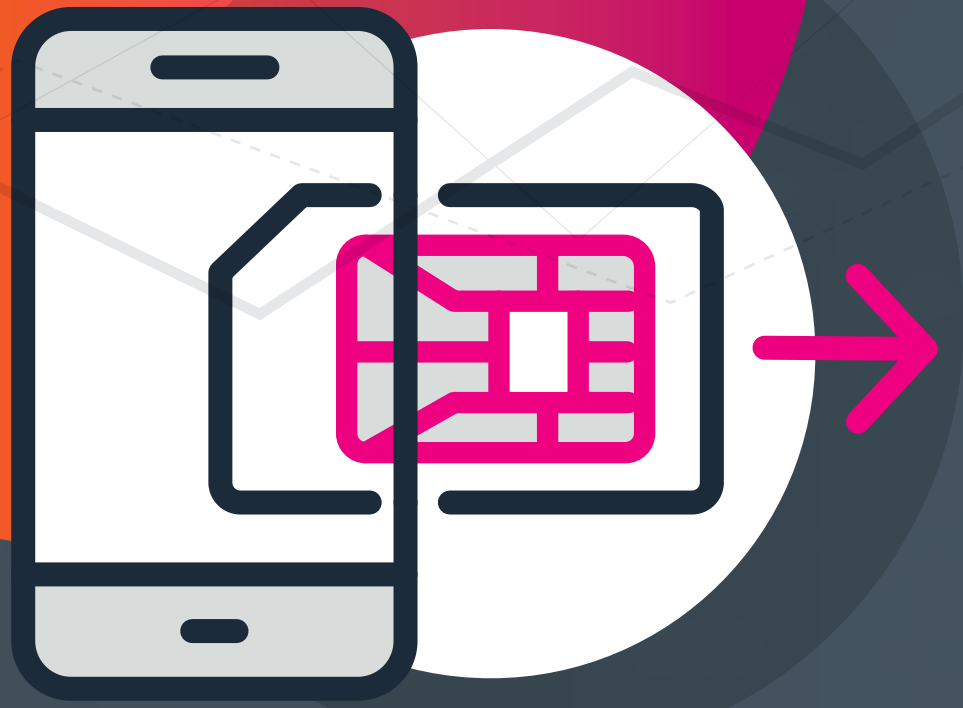
En général, les employés bien intentionnés téléchargent et utilisent innocemment ces applications pour gagner en facilité et en efficacité dans leur travail. Ce phénomène est si répandu que Gartner avait estimé qu'en 2020, un tiers de toutes les attaques de cybersécurité en entreprise proviendraient de ressources informatiques fantômes. Étant donné que les utilisateurs accèdent majoritairement à ces applications en passant sous le radar, ils ouvrent souvent involontairement la porte aux menaces internes, aux violations de données et de conformité.

Comment l'attaque se produit :

Comme son nom l'indique, la nature secrète de l'informatique fantôme est due au fait que les employés partagent ou stockent des données sur des services cloud non autorisés et préparent le terrain à une multitude de risques de sécurité et de conformité. Les violations peuvent se produire lorsque les employés téléchargent, partagent ou stockent des données critiques ou réglementées dans des applications informatiques fantômes sans solutions de sécurité et de prévention des pertes de données (DLP) appropriées. Les informations exposées constituent alors une cible facile pour les menaces internes et le vol de données, et peuvent également conduire à des violations de conformité onéreuses. En outre, les applications peuvent elles-mêmes présenter des vulnérabilités et des failles de sécurité au niveau des points de terminaison.

D'où provient l'attaque :

Dans ce cas, la menace provient de l'intérieur d'une entreprise. Les employés qui utilisent des applications informatiques fantômes le font souvent pour contourner une politique prohibitive ou pour travailler plus rapidement, pas nécessairement pour mettre leurs employeurs et leurs collègues en danger. Cependant, ils laissent finalement la porte grande ouverte aux initiés malveillants ou aux pirates 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, faisaient face à un déluge de messages profondément offensants, envoyés par un groupe de pirates informatiques appelé « Chuckling Squad ». Le groupe a eu recours à l'usurpation de carte SIM pour prendre le contrôle du numéro de téléphone de Jack Dorsey, puis a utilisé un service de text-to-tweet acquis par Twitter pour publier les messages. Bien que les messages aient été visibles en ligne moins de dix minutes, des millions de personnes ont été exposées aux tweets offensants.

Ce que vous devez savoir :

L'usurpation de carte SIM (SIMjacking, SIM swap scam, port-out scam, SIM splitting et SIM swapping en anglais) est un type d'appropriation de compte qui cible généralement une faiblesse dans l'authentification à deux facteurs ou la vérification en deux étapes dans laquelle le deuxième facteur est un message texte (SMS) ou un appel vers un téléphone mobile. En termes simples, l'usurpation de carte SIM se produit lorsqu'un malfaiteur se fait passer pour sa cible auprès de son fournisseur de téléphonie mobile afin de voler son numéro de téléphone en le faisant transférer sur une autre carte SIM, déjà en la possession du pirate informatique.

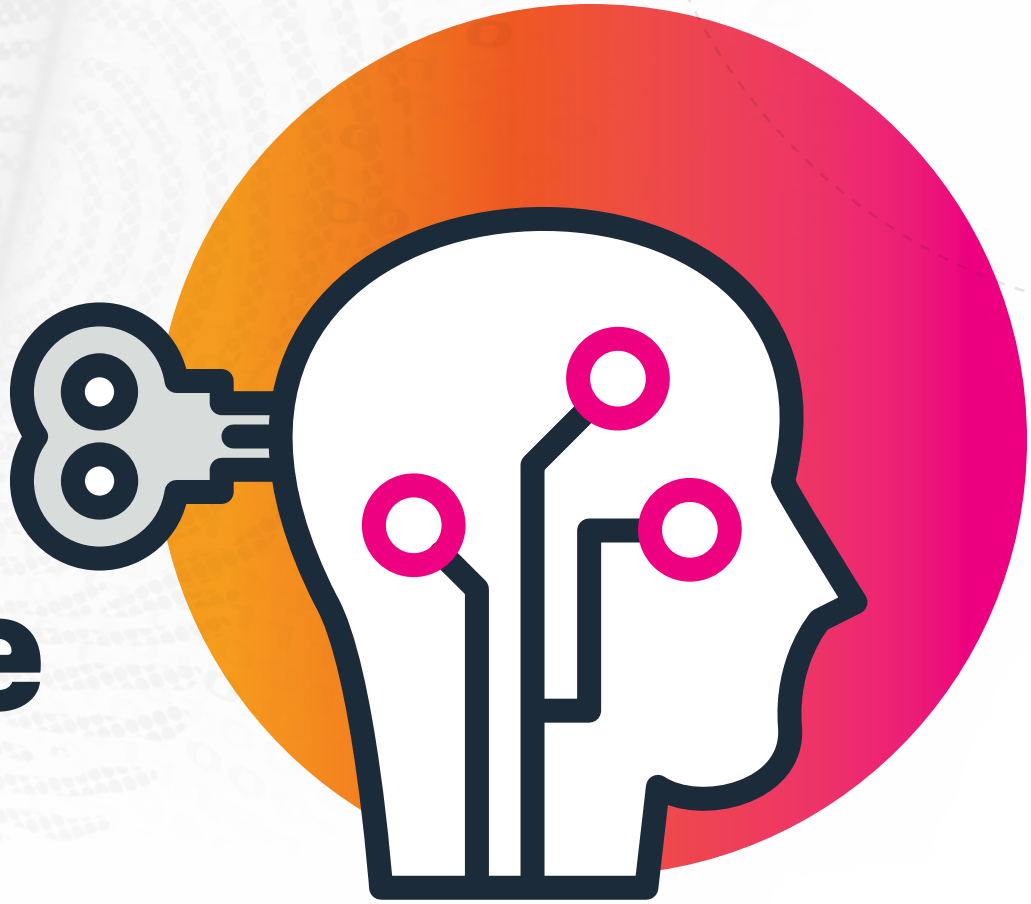
Comment l'attaque se produit :

Un pirate appelle la ligne d'assistance d'un fournisseur de services mobiles en se faisant passer pour sa cible afin de déclarer la perte de sa carte SIM. Pour ce faire, il aura au préalable obtenu une partie des informations personnelles (adresse, mots de passe ou SSN) de leur cible grâce à l'un des nombreux piratages de bases de données menés au cours de la dernière décennie. N'ayant aucun moyen de savoir que la personne à l'autre bout du fil n'est pas la bonne, l'employé du fournisseur de services procède au changement. Immédiatement, ce numéro de téléphone, la clé associée à tant d'éléments de notre vie numérique, tombe entre les mains du malfaiteur.

D'où provient l'attaque :

Les usurpateurs de cartes SIM cherchent généralement à extorquer aux victimes des choses de grande valeur (comme des bitcoins ou autres portefeuilles de cryptomonnaie, ou des comptes de réseaux sociaux de grande valeur) ou à nuire à leur réputation, comme la Chuckling Squad l'a fait avec Jack Dorsey. Ces pirates peuvent provenir de n'importe où dans le monde, et peuvent être membres de groupes organisés ou des acteurs solitaires.

Attaque d'ingénierie sociale



Le film « Arrête-moi si tu peux » (2002) relate l'histoire réelle de l'un des spécialistes en ingénierie sociale les plus accomplis de tous les temps. Dans le film, Leonardo DiCaprio interprète un dénommé Frank W. Abagnale, Jr., un homme qui a exécuté diverses escroqueries de grande envergure, s'est rendu coupable de fraude bancaire et a usurpé l'identité de diverses personnalités, dont un médecin et un pilote. Le succès d'Abagnale reposait sur sa capacité à convaincre ses victimes de l'authenticité de ses contrefaçons, qu'il s'agisse de chèques, de diplômes ou d'identités. Abagnale était un escroc actif dans les années 60 et 70, mais la pratique de l'ingénierie sociale a continué de se développer et reste, pour les pirates et fraudeurs, un outil puissant pour accéder à des systèmes fermés dans le monde entier.

Ce que vous devez savoir :

L'ingénierie sociale est le terme utilisé pour désigner un large éventail d'activités malveillantes exécutées par manipulation psychologique pour amener 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 contrecarrer qu'une intrusion basée sur des logiciels malveillants.

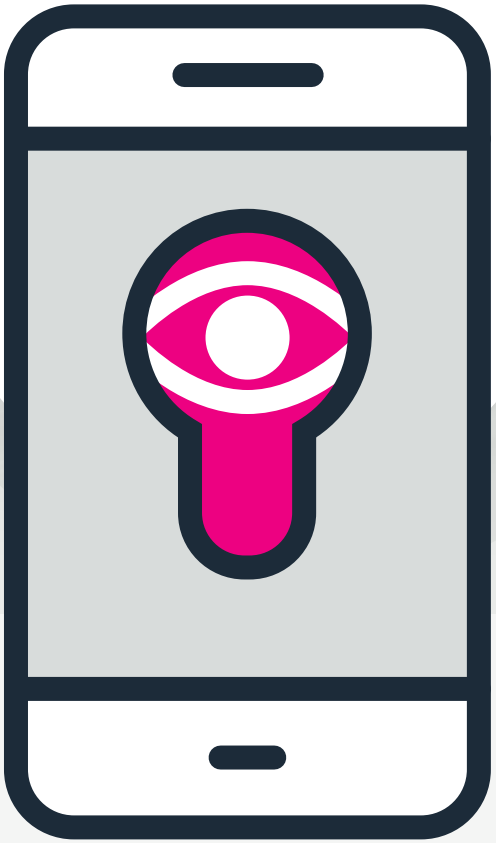
Comment l'attaque se produit :

Les attaques d'ingénierie sociale se présentent sous de nombreuses formes différentes et peuvent être exécutées partout où une interaction humaine est impliquée. Un auteur va commencer, par exemple, par se renseigner sur la victime visée pour recueillir les informations de base nécessaires pour poursuivre l'attaque, telles que les points d'entrée potentiels et les protocoles de sécurité faibles. Ensuite, il gagne la confiance de la victime et l'incite à commettre des actes contraires aux pratiques de sécurité, telles que la révélation d'informations sensibles ou l'octroi d'un accès à des ressources critiques.

D'où provient l'attaque :

L'ingénierie sociale peut prendre plusieurs formes et avoir de nombreuses motivations différentes. Le plus souvent, elle se présente sous la forme d'e-mails d'hameçonnage. D'autres formes incluent le faux-semblant, dans lequel l'attaquant crée un bon prétexte pour voler des données importantes ; l'appâtage et la contrepartie, dans lesquels l'attaquant offre à la victime une chose qu'il souhaite en échange d'informations d'identification ; et le talonnage, dans lequel un attaquant accède à une zone restreinte d'une entreprise en suivant un employé authentifié au passage des portes sécurisées.

Spywares



Ce n'est un secret pour personne : les attaques par spyware se produisent toujours à une fréquence alarmante. Et si vous êtes un acteur médiatisé, vous êtes vraisemblablement une cible encore plus attrayante. En mai 2021, les autorités ont annoncé que des malfaiteurs avaient ciblé les téléphones portables du Président du gouvernement espagnol Pedro Sánchez et de la Ministre de la Défense Margarita Robles dans le cadre de plusieurs attaques exploitant le spyware Pegasus, aboutissant à un vol massif de données sur les deux appareils et semant le chaos au sein des systèmes gouvernementaux et des administrateurs espagnols.

Spywares

Ce que vous devez savoir :

Un spyware, ou logiciel espion, est un type de logiciel malveillant qui vise à collecter des données personnelles ou organisationnelles, à suivre ou à vendre l'activité web d'une victime (par exemple, recherches, historique et téléchargements), à capturer les informations de compte bancaire et même à voler l'identité de la cible. Il existe plusieurs types de spywares, et chacun utilise une tactique unique pour suivre la victime.
En fin de compte, les spywares peuvent prendre le contrôle d'un appareil, exfiltrer des données ou envoyer des informations personnelles à une autre entité inconnue sans connaissance ni consentement préalable.

Comment l'attaque se produit :

Les logiciels espions peuvent s'installer sur l'appareil d'une victime par divers moyens, mais s'implanteront généralement dans un système en dupant la cible ou en exploitant les vulnérabilités existantes. Cela peut se produire lorsqu'un utilisateur accepte négligemment une invite ou une fenêtre contextuelle aléatoire, télécharge un logiciel ou des mises à niveau à partir de sources non fiables, ouvre des pièces jointes provenant d'expéditeurs inconnus ou pirate des films et de la musique.

D'où provient l'attaque :

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

Injection SQL

Le langage SQL (Structured Query Language), est le langage de programmation standard utilisé pour communiquer avec les bases de données relationnelles, des systèmes qui assurent la prise en charge sur l'Internet de l'ensemble des sites Web et applications basés sur les données. Un attaquant peut tirer parti de ce système très courant en saisissant une requête SQL spécifique dans un formulaire (en l'injectant dans la base de données), après quoi il pourra accéder à la base de données, au réseau et aux serveurs. Les attaques par injection SQL sont encore très populaires. Pas plus tard qu'en août 2020, la Freepik Company a révélé une violation de données affectant les identifiants de plus de huit millions d'utilisateurs suite à une injection SQL dans une base de données globale d'icônes personnalisables ayant permis aux pirates de dérober les identifiants et les informations personnelles des utilisateurs.

Injection SQL

Ce que vous devez savoir :

L'injection SQL est un type d'attaque par injection utilisée pour 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 entrées des utilisateurs ne sont pas correctement filtrées.

Comment l'attaque se produit :

Une attaque par injection SQL consiste en l'insertion ou « injection » d'une requête SQL via les données d'entrée du client vers l'application. Une attaque par injection SQL fructueuse peut lire des données sensibles de la base de données, modifier des données de la base de données, exécuter des opérations d'administration sur la base de données, récupérer le contenu d'un fichier présent sur le système de fichiers du SGBD et, dans certains cas, émettre des commandes vers le système d'exploitation.

D'où provient 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. La recherche du terme « injection » dans la base de données des vulnérabilités et expositions courantes renvoie 15 000 résultats.

Attaque de la chaîne logistique

Les attaques SolarWinds, que certains experts ont qualifié de pire série d'attaques de cybersécurité de l'histoire, sont l'exemple parfait des dégâts qu'une attaque de la chaîne logistique peut infliger. En 2020, des pirates experts, qui auraient été mandatés par les services de renseignements russes, ont compromis le logiciel SolarWinds. Ils y ont intégré un malware qui a ensuite été déployé via une mise à jour, leur donnant un accès dérobé au réseau de tous les clients de la plateforme SolarWinds Orion. Jusqu'à 18 000 clients, dont des entreprises du Fortune 500 et plusieurs agences gouvernementales américaines, ont ainsi installé des mises à jour qui les ont rendus vulnérables aux pirates. Comme Tim Brown, Vice-président de la sécurité chez SolarWinds, l'a récemment confié : « Il s'agit véritablement de votre pire cauchemar. »

Attaque de la chaîne logistique

Ce que vous devez savoir :

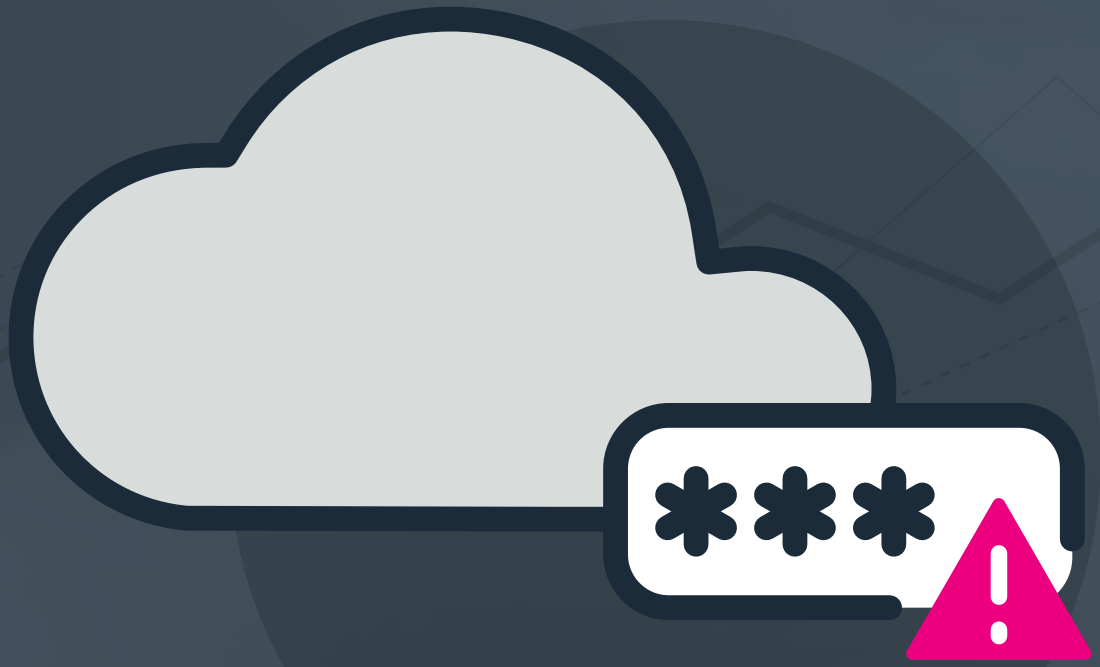
Une attaque de la chaîne logistique est une puissante cyberattaque qui peut traverser les défenses de sécurité les plus sophistiquées par l'intermédiaire de fournisseurs tiers légitimes. Comme les fournisseurs ont besoin d'accéder à des données sensibles pour s'intégrer aux systèmes internes de leurs 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.

Comment l'attaque se produit :

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 provient l'attaque :

Les attaques de la chaîne logistique sont des attaques sophistiquées à grande échelle réalisées par des pirates experts, souvent parrainées par des États-nations et motivées par une idéologie, bien que l'appât du gain reste un facteur de motivation majeur.



Activités d'authentification cloud suspectes

Aujourd'hui plus que jamais, la gestion des accès et des identités (IAM) est devenue un rouage essentiel de la sécurité cloud. Rien qu'en 2022, 84 % des organisations ont été victimes de violations liées à l'identité, 96 % d'entre elles indiquant que la violation aurait pu être évitée ou minimisée en mettant en place des systèmes de sécurité basés sur l'identité.

Sans les bonnes technologies et politiques, (par ex. modèle Zero Trust et gestion des fournisseurs), l'identification des comportements anormaux via l'authentification et l'autorisation peut s'avérer très difficile. De ce fait, ces attaques passent souvent inaperçues, car l'authentification d'un malfaiteur peut paraître identique à celle d'un utilisateur légitime en fonction de l'étendue du framework IAM mis en place (si tant est qu'il y en ait un).

Activités d'authentification cloud suspectes

Ce que vous devez savoir :

Les organisations doivent aller au-delà de la sécurité réseau afin de mieux protéger et authentifier l'identité de leurs utilisateurs. Jusqu'à récemment, c'était cependant beaucoup plus facile à dire qu'à faire. Certaines technologies ne disposaient tout simplement pas des fonctionnalités d'intégration nécessaires, limitant la capacité des organisations à superviser de manière centralisée la sécurité globale de leurs ressources.

Il existe maintenant d'innombrables technologies centrées sur le contrôle des accès, comme l'authentification multifacteurs (MFA). Pour éviter les authentifications illégales sur les applications cloud, aucun utilisateur ou appareil, qu'il soit externe ou interne à l'organisation, ne doit être implicitement approuvé, et l'accès à toutes les ressources doit être explicitement et systématiquement authentifié et autorisé.

Comment l'attaque se produit :

La menace ou le malfaiteur peut facilement pénétrer le réseau ou le périmètre lorsqu'il n'y a pas de framework IAM ou que celui utilisé n'est pas optimal, et lorsqu'une organisation s'appuie toujours sur la sécurité des réseaux et des points de terminaison. Dans les deux cas, comme les contrôles d'accès sont laxistes, le malfaiteur peut facilement s'identifier avec les identifiants volés sans être détecté, puis se déplacer latéralement dans le réseau et dans les systèmes connectés. Il peut alors compromettre des actifs et provoquer des dommages irréparables, sans aucun obstacle.

D'où provient l'attaque :

Entre le nombre croissant d'attaques de phishing, l'augmentation du nombre d'identités utilisateurs et la croissance constante de l'adoption du cloud, ce type d'attaque peut venir de partout, notamment de fournisseurs tiers, d'employés, de télétravailleurs et de contractuels.

Activités de stockage cloud suspectes

D'après le rapport 2022 Verizon Data Breach Investigations Report (DBIR), 82 % des violations impliquent un « élément humain », avec une progression des « erreurs diverses » en raison d'une mauvaise configuration du stockage cloud. Le rapport Les données sensibles dans le cloud révèle également que la majorité des professionnels IT et de la sécurité (67 %) stockent des données sensibles dans des environnements cloud publics, un tiers des participants affirmant qu'ils n'étaient pas (ou peu) confiants dans leur capacité à protéger des données sensibles dans le cloud.

Ce type d'erreur technique et professionnelle, qu'elle implique une base de données mal configurée ou des équipes de sécurité sans le savoir-faire nécessaire, est exactement ce pour quoi les comptes cloud sont devenus une cible de choix 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, bien souvent au hasard, les malfaiteurs ont tout le loisir de trouver et d'exploiter des vulnérabilités connues et inconnues. Cela est d'autant plus vrai que les entreprises ont dû migrer vers le cloud à la va-vite, en configurant mal ou en compromettant potentiellement certains contrôles de sécurité.

Pour ne rien arranger, les actifs et les applications doivent être sécurisés conformément au modèle de responsabilité partagée, qui indique que les fournisseurs de services cloud (CSP) couvrent certains éléments, processus et fonctions, mais que les clients sont ensuite responsables de la sécurisation de leur code, de leurs données propriétaires et de leurs autres actifs importants, d'après la Cloud Security Alliance (CSA). Mais lorsque cette responsabilité n'est pas assumée, les pirates ne tardent pas à arriver.

Comment l'attaque se produit :

Une attaque sur le stockage cloud survient lorsqu'un malfaiteur parvient à mettre le pied dans l'infrastructure cloud d'une organisation en raison de paramètres de sécurité incorrects, laxistes ou inexistants. Une fois à l'intérieur, il commence à désactiver certains contrôles tels que la supervision des accès. Il peut créer de nouveaux comptes pour bénéficier d'un accès durable, tout en exécutant des commandes qui ne sont pas habituelles pour le type d'utilisateur ou système en question. Il peut également modifier les politiques de certains buckets de stockage, de façon à ce que les fichiers d'une organisation soient accessibles au public, entraînant ainsi une exfiltration des données. Heureusement, il s'agit là exclusivement d'événements notables faciles à suivre et à identifier dans les logs d'audit du CSP.

D'où provient l'attaque :

Elle peut par exemple survenir si un développeur exécute une instance obsolète d'une application ou d'une fonction cloud. Elle pourrait encore contenir des vulnérabilités connues et corrigées depuis dans les versions suivantes. Mais puisqu'il s'agit d'une version antérieure, les malfaiteurs peuvent l'utiliser comme point d'entrée avant de se déplacer latéralement au sein de l'environnement cloud.

Activité Okta suspecte

Okta est souvent la porte d'entrée d'applications et de comptes professionnels, et les pirates en sont bien conscients. S'il est exploité, un défaut de l'authentification unique (SSO) permet aux pirates de dérober les identifiants de comptes existants pour réaliser toutes sortes d'activités non autorisées : accès, persistance, élévation de privilèges et contournement de défense. Une fois les identifiants compromis, les malfaiteurs peuvent ensuite contourner les contrôles d'accès pour accéder aux VPN, à Outlook Web Access et aux protocoles de bureau à distance. Ils peuvent également utiliser des identifiants compromis pour augmenter leurs privilèges sur certains systèmes ou accéder à des zones restreintes du réseau, tout en utilisant des malwares pour dérober des informations et/ou masquer leur présence. Dans un scénario d'attaque, les pirates peuvent prendre le contrôle de comptes inactifs d'employés ayant quitté l'organisation et utiliser leurs identifiants pour accéder à des systèmes critiques pour voler des données et des identités.

Ce que vous devez savoir :

Okta est le plus grand fournisseur d'authentification unique, permettant aux utilisateurs de s'identifier une fois auprès d'Okta pour pouvoir ensuite accéder à différentes applications web. Ces applications sont assignées aux utilisateurs et permettent aux administrateurs de gérer de manière centralisée quels utilisateurs sont autorisés à accéder à quelles applications. Okta fournit également une journalisation centralisée afin d'aider à comprendre comment et par qui les applications sont utilisées.

Même si la SSO est un véritable confort pour les utilisateurs, elle constitue également une opportunité pour les malfaiteurs. Si un pirate arrive à accéder à Okta, il a alors accès à toutes sortes d'applications.

Comment l'attaque se produit :

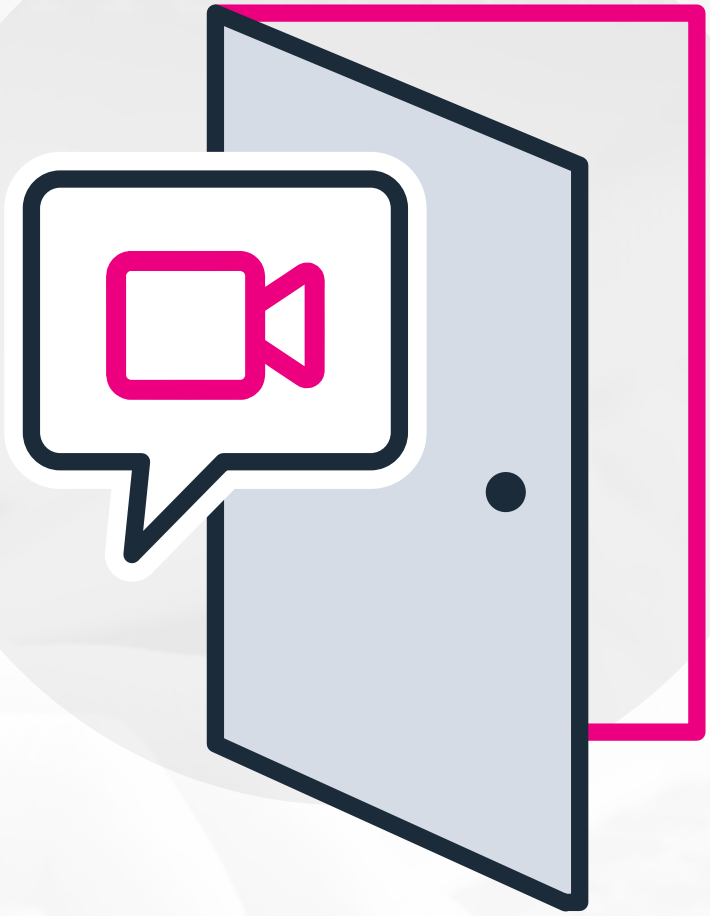
Une fois exploitée, la vulnérabilité permet de réaliser une attaque par bourrage d'identifiants, lors de laquelle le malfaiteur obtient les noms d'utilisateur et les mots de passe depuis différentes sources telles que des sites piratés, des attaques de phishing et des sites de dépôt de mots de passe. En menant des attaques par force brute à l'aide d'outils automatisés, le malfaiteur teste ces identifiants à grande échelle sur une multitude de sites web pour voir si certains identifiants permettent d'accéder au site. À partir de là, les malfaiteurs peuvent lancer tout type d'attaques, notamment des campagnes de spam ou de phishing, accéder à des informations personnellement identifiables et sensibles, et ponctionner financièrement les comptes dérobés.

Les attaques par pulvérisation de mots de passe, qui sont essentiellement des attaques par force brute, envoient de nombreux noms d'utilisateurs dans un programme automatisé qui essaie ensuite de deviner les mots de passe qui y sont associés. Comme son nom l'indique, cette attaque repose sur une technique de « pulvérisation » dans l'espoir qu'une des combinaisons nom d'utilisateur/mot de passe soit la bonne. Et une seule suffit.

D'où provient l'attaque :

Ces attaques peuvent concrètement venir de partout. Bien qu'il soit possible de les relier à des réseaux cybercriminels sophistiqués, elles peuvent également être menées par des pirates isolés moins organisés ayant accès à des outils automatisés capables de réaliser un grand nombre d'attaques par force brute à la fois.

Processus Zoom suspects



Le géant de la vidéoconférence Zoom fait office de plus grande plateforme de communication vidéo professionnelle ces dernières années. Son utilisation a drastiquement augmenté avec l'essor soudain du télétravail, en grande partie attribué aux confinements suite à la pandémie de COVID-19. Cependant, parallèlement à l'explosion de popularité de Zoom, les failles sur les systèmes Windows et macOS ont fait l'objet d'une plus grande attention de la part des malfaiteurs, qui se sont de plus en plus appuyés sur ce vecteur d'attaque pour accéder illégalement et augmenter leurs privilèges sur les systèmes ciblés, notamment en exploitant une fonction de validation de bibliothèque locale de Zoom pour prendre le contrôle de la webcam et du micro d'une victime qui ne se doute de rien. Des scénarios d'attaque plausibles impliquent par exemple l'utilisation des privilèges acquis illégalement pour espionner les utilisateurs ciblés, que ce soit dans le cadre de leur vie privée ou pendant des réunions importantes au cours desquelles des informations confidentielles sont échangées.

Processus Zoom suspects

Ce que vous devez savoir :

Ces failles d'élévation de privilèges locaux exploitent l'architecture logicielle de Zoom. Ces exploits peuvent être utilisés par un malfaiteur local qui dispose déjà d'un accès physique à un ordinateur vulnérable. Une fois les bugs exploités, les malfaiteurs peuvent obtenir un accès continu à différentes fonctions de l'ordinateur d'une victime, ce qui leur permet d'installer des ransomwares, des chevaux de Troie, des spywares et beaucoup d'autres types de code malveillant dans les systèmes ciblés à des fins répréhensibles.

Comment l'attaque se produit :

Une des méthodes utilisées pour effectuer cette attaque exploite le programme d'installation de Zoom pour installer Zoom sur MacOS sans interaction de l'utilisateur. Dans ce scénario, un malfaiteur local avec des privilèges d'utilisateur peu élevés peut injecter un malware dans le programme d'installation de Zoom pour obtenir des privilèges root qui lui permettent d'accéder au système d'exploitation Mac sous-jacent, ce qui facilite l'exécution de malwares ou de spywares sans le consentement de l'utilisateur ou à son insu.

Un autre bug exploite une faille dans la fonction de validation de bibliothèque locale de Zoom. Un malfaiteur peut charger une bibliothèque tierce malveillante dans l'espace de processus/d'adresse de Zoom. Elle hérite alors automatiquement de tous les droits d'accès de Zoom et prend le contrôle de la caméra et du micro à l'insu ou sans le consentement de l'utilisateur.

D'où provient l'attaque :

Ce qui rend cette vulnérabilité unique est le fait que le malfaiteur a besoin d'un accès physique à l'ordinateur de la victime pour exploiter ses failles multiples. Cette attaque provient donc de l'intérieur ou de pirates ayant accès à un ordinateur perdu ou volé. Un autre scénario d'attaque implique une infection par malware réalisée par un pirate à distance, mais avec un accès préexistant au système ciblé, vraisemblablement grâce à une première infection par malware.

Mauvaise configuration du système

Une petite erreur peut avoir de graves conséquences. Nissan North America en a fait l'expérience après que le code source des outils internes et applis mobiles a été divulgué en ligne en raison d'une mauvaise configuration d'un système. L'incident a été attribué à un serveur Git laissé vulnérable sur Internet avec le nom d'utilisateur et le mot de passe par défaut d'un administrateur, qui a ensuite été prévenu de la fuite par une source anonyme. La fuite contenait entre autres les données relatives au code source des applis mobiles, des outils d'acquisition et de fidélisation des clients, des outils et des données d'étude de marché, du portail de logistique des véhicules et des services connectés des véhicules de Nissan NA.

Mauvaise configuration du système

Ce que vous devez savoir :

Très répandues, les erreurs de configuration peuvent mettre les entreprises en danger en raison des contrôles de sécurité mal configurés (ou même absents). Cela peut se produire à presque tous les niveaux de la pile informatique et de sécurité, allant du réseau sans fil de l'entreprise aux applications Web et serveur, en passant par le code personnalisé.

Comment l'attaque se produit :

L'origine de ce type d'attaque provient généralement de correctifs manquants, de l'utilisation de comptes par défaut, de services inutiles, d'une configuration par défaut non sécurisée ou d'une mauvaise documentation. Elle peut prendre la forme d'une erreur de définition dans l'en-tête de sécurité d'un serveur web, ou d'un accès administrateur resté activé par défaut pour certains niveaux d'employés. Cette attaque peut également se produire lorsque des pirates informatiques s'implantent dans des applications obsolètes contenant des erreurs de configuration inhérentes dues à leur ancienneté.

D'où provient l'attaque :

Une mauvaise configuration n'est pas considérée comme un acte malveillant en soi, elle est au contraire principalement due à une erreur humaine. Cependant, les attaquants qui soupçonnent du laxisme dans la configuration de la pile informatique d'une entreprise savent où chercher.

Typosquattage

Noblox.js est un wrapper pour l'API Roblox, une fonction largement utilisée par de nombreux gamers pour automatiser les interactions avec la plateforme de jeu populaire Roblox. Le logiciel semble également attirer une nouvelle population. En 2021, des pirates ont lancé une attaque de typosquattage via le package noblox.js en uploadant des packages très similaires contenant des ransomwares sur un dépôt de bibliothèques JavaScript open source, puis en distribuant les fichiers infectés via un service de messagerie. Cependant, depuis septembre 2021, le joueur Josh Muir et d'autres luttent activement contre ces malfaiteurs, en essayant d'empêcher la prolifération de ransomwares via le package noblox.js et d'autres librairies de code, et de déjouer les nouvelles attaques à l'encontre de la communauté des joueurs.

Typosquattage

Ce que vous devez savoir :

Le typosquattage est une attaque d'hameçonnage dans laquelle les attaquants profitent de noms de domaine couramment mal orthographiés. Souvent, le coupable ne cherche pas réellement à mener une attaque, mais espère plutôt qu'une entreprise, une marque ou une personne lui rachètera le domaine. Mais il arrive également que des voleurs créent des domaines malveillants qui ressemblent étroitement à ceux des marques légitimes.

Comment l'attaque se produit :

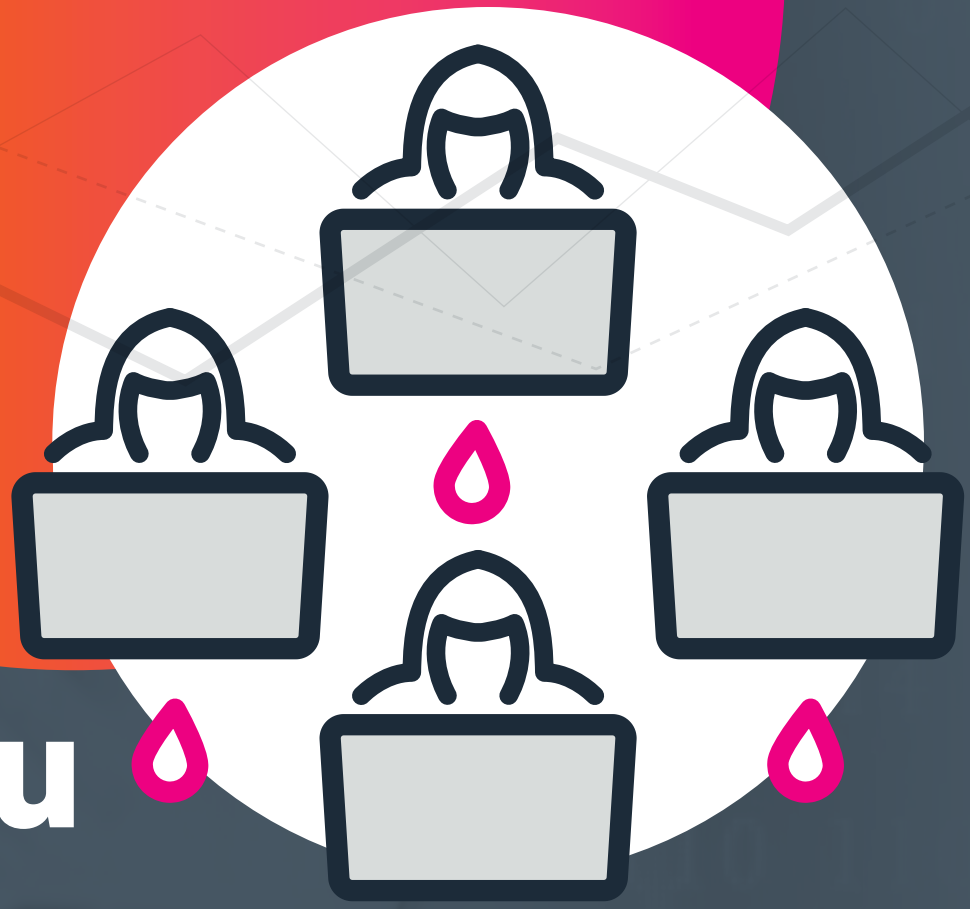
Ce type d'attaque n'est pas sophistiqué. Elle est si simple qu'un jeune de 14 ans peut enregistrer un domaine puis installer du code malveillant dessus. La forme malveillante de cette attaque implique généralement un pirate informatique utilisant de faux domaines pour amener les utilisateurs à interagir avec une infrastructure malveillante.

Même pour les utilisateurs au courant de ces risques, l'erreur humaine fait partie de la vie. La plupart des malfaiteurs ne le savent que trop bien et chercheront systématiquement à en profiter : comme l'hameçonnage avec des adresses similaires, ils intègrent de faux domaines de commande et contrôle dans des malwares et hébergent du contenu malveillant sur des domaines qui imitent fidèlement vos serveurs d'entreprise.

D'où provient l'attaque :

Les origines de cette attaque ne sont pas aussi importantes que la cible. Cette attaque vise 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 suffit simplement d'enregistrer un nom de domaine), elle peut provenir de presque n'importe où.

Attaque de point d'eau



Dans ce qui est devenu une attaque de point d'eau célèbre, un fournisseur d'installations de traitement des eaux et des eaux usées a malencontreusement hébergé du code malveillant sur son site internet, entraînant le piratage de l'usine de traitement d'eau d'Oldsmar en 2021. Les cybercriminels derrière l'attaque semblaient avoir une cible bien précise en tête : le code malveillant découvert sur le site du fournisseur semblait également cibler d'autres compagnies des eaux de Floride. Probablement sans grande surprise, le site avait été visité depuis un navigateur situé dans la ville d'Oldsmar le jour du piratage. Le site internet ne lançait pas de code d'exploit, mais injectait à la place un malware qui fonctionnait comme un script de fingerprinting et d'énumération de navigateur conçu pour récolter des informations sur les visiteurs du site, notamment le système d'exploitation, le type de navigateur, le fuseau horaire et la présence d'une caméra et d'un micro. Ces informations étaient ensuite envoyées sur une base de données à distance hébergées sur un site d'appli Heroku qui stockait également le script.

Attaque de point d'eau

Ce que vous devez savoir :

Comme son nom l'indique, une attaque de point d'eau est une attaque dans laquelle l'ordinateur de l'utilisateur est compromis en visitant un site Web infecté par un logiciel malveillant conçu pour infiltrer son réseau et voler des données ou des actifs financiers. Il s'agit essentiellement d'une attaque zero-day ; l'objectif étant d'infecter le système informatique pour accéder au réseau et en tirer un gain financier ou des informations exclusives.

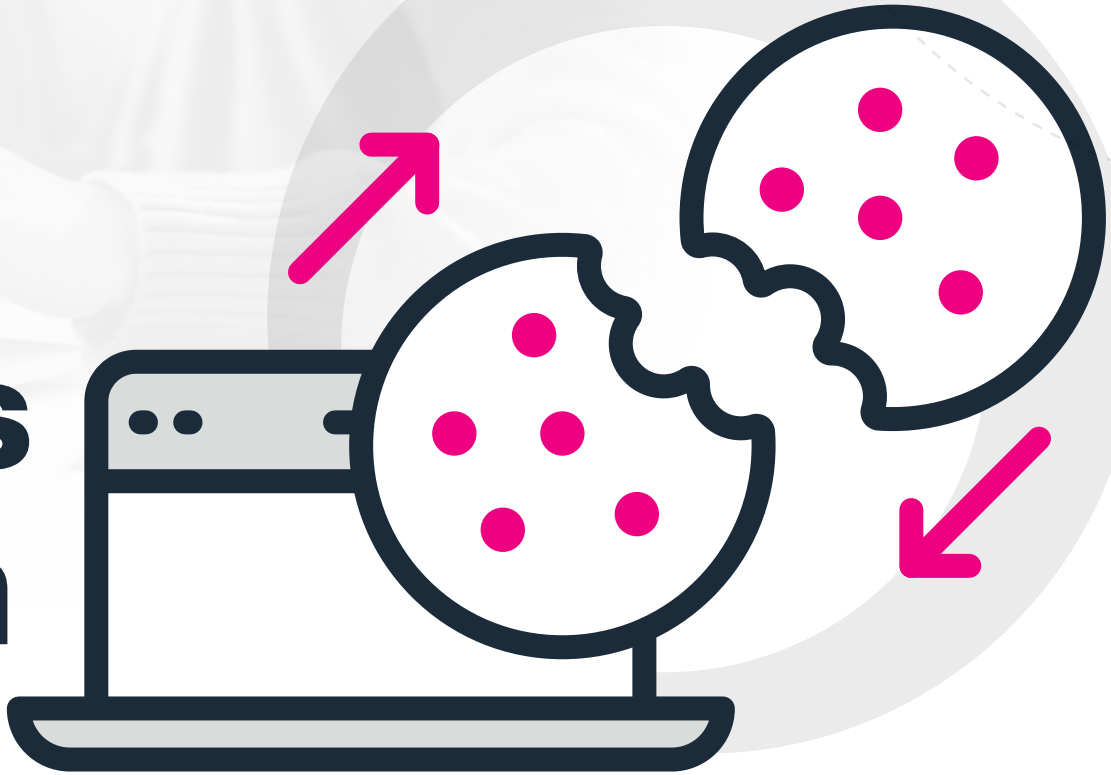
Comment l'attaque se produit :

Les attaquants commencent par dresser le profil de leur cible afin de déterminer les sites Web qu'ils visitent fréquemment et, à partir de là, cherchent des vulnérabilités. Ils les exploitent et compromettent ces sites web, puis attendent, sachant que l'utilisateur en question finira tôt ou tard par les visiter. Le site Web compromis infectera à son tour le réseau de l'utilisateur et permettra aux attaquants d'accéder à l'intégralité de son système et de se déplacer latéralement vers d'autres systèmes.

D'où provient l'attaque :

Bien qu'ils viennent de partout, de nombreux cybercriminels à l'origine de cette attaque sont originaires de pays où prospèrent des groupes de hackers organisés, comme la Russie, l'Europe de l'Est et la Chine. En 2018, une attaque de point d'eau a été attribuée au groupe de pirates chinois connu sous le nom de « Lucky Mouse » (ou Iron Tiger, EmissaryPanda, APT 27 et Threat Group 3390), ayant pour habitude de mener de nombreux types d'attaques, dont des attaques de point d'eau, ciblant les secteurs du gouvernement, de l'énergie et de la fabrication.

Vol de cookies de session web



Presque toutes les applications web que nous utilisons, des réseaux sociaux et plateformes de streaming aux services cloud et applications financières, fonctionnent avec des cookies d'authentification. Bien que ces cookies améliorent grandement notre expérience sur le Web, ils représentent également une vulnérabilité dont les malfaiteurs peuvent abuser de manière efficace. Fin 2019, un groupe de pirates plus ou moins liés s'est fait un nom en exécutant des malwares de vol de cookies pour pirater plusieurs chaînes YouTube, puis en dupant les propriétaires des chaînes au moyen d'offres factices pour faire de la publicité pour des arnaques aux cryptomonnaies ou en vendant les comptes au plus offrant.

Vol de cookies de session web

Ce que vous devez savoir :

Lorsqu'un attaquant parvient à voler un cookie de session, il peut effectuer toutes les actions que l'utilisateur d'origine est autorisé à accomplir. Pour les entreprises, le danger réside dans le fait que les cookies peuvent être utilisés pour identifier les utilisateurs authentifiés dans les systèmes d'authentification unique et donner potentiellement à l'attaquant un accès à toutes les applications Web que la victime peut utiliser, comme les systèmes financiers, les dossiers des clients ou les systèmes métiers contenant potentiellement de la propriété intellectuelle confidentielle.

Comment l'attaque se produit :

Lorsqu'un utilisateur accède à un service et valide son identité, un cookie est enregistré sur sa machine pour une durée prolongée afin de lui éviter de devoir saisir ses informations d'identification à maintes reprises. Des acteurs malveillants peuvent dérober des cookies de session Web via un logiciel malveillant, puis l'importer dans un navigateur qu'ils contrôlent. Tant que le cookie de session est actif, ils peuvent ainsi utiliser le site ou l'application en tant qu'utilisateur. Une fois connecté au site, un attaquant peut accéder à des informations sensibles, lire des e-mails ou effectuer des actions que le compte de la victime est autorisé à effectuer.

D'où provient l'attaque :

Le vol de cookies est généralement accompli par des logiciels malveillants qui copient les cookies de la victime et les envoient directement à l'attaquant. Le logiciel malveillant peut atterrir sur la machine de la victime de plusieurs manières abordées dans cet ouvrage, comme l'hameçonnage, les virus macro, les scripts intersites, etc.
De nombreux pirates réalisant des vols de cookies font partie de réseaux plus vastes en Russie et en Chine. Les auteurs de l'attaque contre YouTube faisaient par exemple partie d'un groupe de pirates fréquentant un forum russe.

Cyber-braquage

Même si le réseau SWIFT a subi moins d'attaques depuis le tristement célèbre braquage de 2016, les cybercriminels n'hésitent pas à utiliser les virements bancaires de manière innovante pour lancer des cyberattaques malveillantes et/ou lucratives. En 2018 par exemple, Frank Krasovec, un propriétaire de franchises Domino's Pizza en Chine, a perdu 450 000 $ lorsqu'un fraudeur est parvenu à prendre le contrôle de son adresse e-mail et à convaincre son assistante de lui virer de l'argent sur un compte à Hong Kong à deux reprises. Plus récemment en 2020, des malfaiteurs ont ciblé un directeur de banque à Hong Kong via un appel au cours duquel ils ont imité la voix d'un responsable qu'il connaissait grâce à une technologie de clonage de voix par IA. Le cybercriminel imitant le responsable a prétendu que son entreprise réalisait une acquisition et a demandé le virement de 35 millions de dollars vers un autre compte. Généralement précédés par une attaque de phishing ou par malware, les cyber-braquages permettent le virement de sommes d'argent conséquentes rapidement.

Ce que vous devez savoir :

Les cyber-braquages, ou attaques sur les transferts bancaires, sont des stratagèmes sophistiqués qui envoient des paiements frauduleux de grande valeur via des réseaux de virement internationaux. Dépassant bien souvent la fraude au transfert bancaire ordinaire, les attaquants ciblent les banques des marchés émergents ayant une infrastructure de cybersécurité ou des contrôles opérationnels limités ou dupent des cibles haut placées grâce à des arnaques de phishing élaborées et crédibles. Ces syndicats de la cybercriminalité ne visent qu'une seule chose : l'argent. Et en grande quantité.

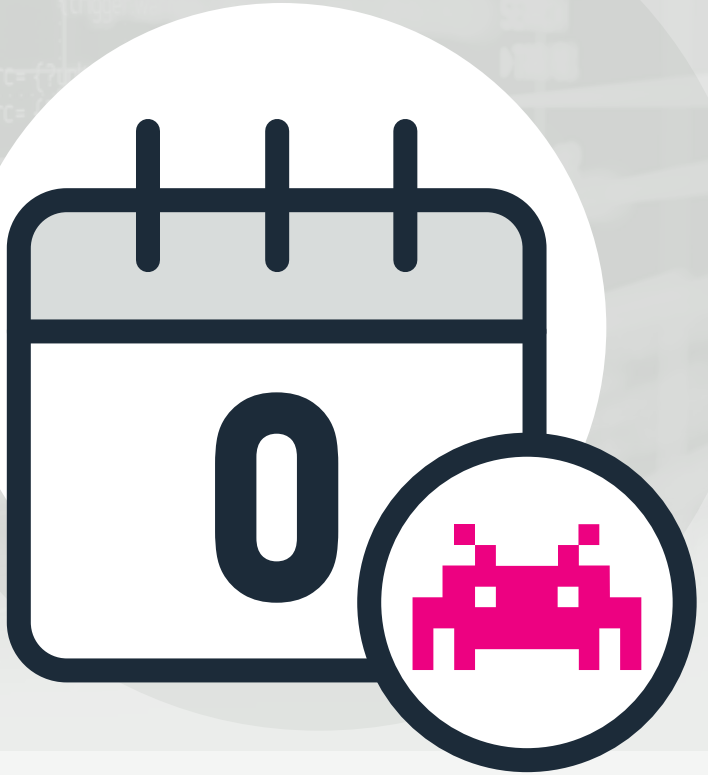
Comment l'attaque se produit :

Dans un scénario d'attaque, les cybercriminels utilisent 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 de fonds à partir de comptes de banques plus importantes. Dans un autre scénario d'attaque, les malfaiteurs déploient des campagnes de harponnage ciblées crédibles afin de convaincre des parties prenantes de virer des sommes d'argent conséquentes sur leurs comptes.

D'où provient l'attaque :

On trouve historiquement des organisations cybercriminelles internationales ou nationales fortement structurées, comme APT 38 et 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. Bien qu'on ne sache pas exactement qui se cache derrière ces groupes, certains rapports indiquent qu'ils pourraient avoir des liens avec la Corée du Nord. Cependant, des cyber-braquages élaborés ont également été attribués à des groupes cybercriminels chinois et nigérians. Attention : les cyber-braquages de grande valeur dans des institutions dotées de systèmes plus robustes requièrent probablement l'implication d'initiés pour accéder aux systèmes.

Exploitation zero-day



Il n'est pas surprenant que le nombre de failles zero-day continue d'augmenter. Mais 2021 aura été l'année de tous les records : les cybercriminels ont exploité 58 nouvelles vulnérabilités zero-day, contre 25 en 2020 et 21 en 2019. Et les enjeux sont de plus en plus élevés à mesure que les systèmes critiques deviennent de plus en plus connectés. Ces dernières années, les pirates ont exploité des vulnérabilités zero-day pour compromettre les serveurs de Microsoft et installer des spywares complexes sur des smartphones à des fins d'espionnage ciblant des journalistes, des politiciens et des défenseurs des droits de l'Homme. En août 2021 par exemple, une vulnérabilité zero-day baptisée « PwnedPiper » a été découverte dans les systèmes de tubes pneumatiques utilisés par les hôpitaux pour transporter des analyses de sang, des échantillons de test et des médicaments. Elle permettait aux malfaiteurs d'exploiter des failles dans le logiciel de panneau de commande, tout en ouvrant la porte à des mises à jour de firmware non autorisées et non chiffrées.

Ce que vous devez savoir :

À la base, 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 (ou immédiatement) après son lancement officiel. Le terme « zéro » fait référence au fait que ces vulnérabilités sont exploitées le jour-même.

Comment l'attaque se produit :

Une attaque zero-day se produit une fois la vulnérabilité exploitée. Si la nature de la vulnérabilité affecte la façon dont l'attaque est mise en œuvre, les attaques zero-day suivent néanmoins un schéma. Dans un premier temps, le pirate (ou un groupe de pirates qui collaborent) analyse la base du code à la recherche de vulnérabilités. Une fois qu'il a trouvé la faille, il crée un code qui exploite la vulnérabilité. Il infiltre le système (en utilisant une ou plusieurs des méthodes décrites dans cet ouvrage) et l'infecte avec son code malveillant, puis lance l'attaque.

D'où provient l'attaque :

La prévalence de la technologie a entraîné une croissance exponentielle des attaques zero-day. Bien que ces attaques puissent provenir de partout, elles sont souvent menées par des États-nations ou des régions composées de nombreux réseaux et d'infrastructures cybercriminels.
De récents rapports affirment que la majorité des vulnérabilités zero-day exploitées en 2021 peut être attribuée à des groupes de pirates chinois.

En savoir plus.

Découvrez comment votre organisation peut se protéger face à d'innombrables menaces et moderniser son SOC à l'aide de la solution d'opérations de sécurité orientée données de Splunk.

splunk> turn data into doing®