De l'Antivirus à l'exploit Zero-day:

les 20 termes de cybersécurité que vous devez connaître

NordVPN®

“

La cybersécurité est désormais liée à chacune de nos activités sur Internet. Par ailleurs, la « vie en ligne » est devenue un terme normal ancré dans notre société. Par extension, les menaces relatives à la cybercriminalité ne peuvent être négligées où une certaine éducation est essentielle pour préserver notre bien-être. Chaque internaute profite ainsi de bases théoriques... C'est pourquoi la compréhension de termes (de A à Z) relatifs à la cybersécurité est cruciale.

Troy Hunt

Troy Hunt - Membre du conseil consultatif de NordVPN, directeur régional de Microsoft et lauréat du prix dédié à la sécurité des développeurs, blogueur sur troyhunt.com, conférencier international dans le domaine de la sécurité Web et auteur de nombreux ouvrages axés sur la sécurité de haut niveau pour les développeurs Web sur Pluralsight.

Préface

Le domaine de la cybersécurité ne vous est pas familier ? Cet e-book est idéal pour développer vos connaissances. Afin d'argumenter cette affirmation, voyons le fonctionnement habituel des choses.

Vous avez été confronté au terme « spyware » et vous souhaitez comprendre ce phénomène ? Très souvent, vos recherches sur Internet se résumeront par des explications techniques et complexes telles que :

> Un spyware est un type de logiciel malveillant qui surveille l'appareil d'une victime afin d'extraire des données sensibles à son insu. Exemples de spywares : adwares, keyloggers et chevaux de Troie.

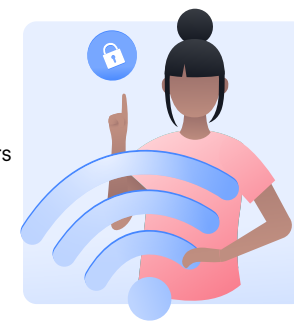
Certes, cette définition est précise. Toutefois, celle-ci n'est pas très utile. Désormais, de nombreuses questions pourront traverser votre esprit. Comment fonctionnent ces spywares ? Quelles données sont considérées comme sensibles et dans quelle mesure devriez-vous vous inquiéter de leur sécurité ? Qu'est-ce qu'un enregistreur de frappe (ou keylogger) ? Est-il question d'un enregistrement de mots spécifiques ?

Nous privilégions une approche différente

Plutôt que de vous donner des définitions techniques, nous allons vous expliquer comment la cybersécurité peut affecter votre vie en vous fournissant des comparaisons accessibles et pertinentes. Ce glossaire se veut donc incomplet, et ce choix est volontaire. Notre e-book est avant tout destiné à « aiguiser votre appétit » lors de votre apprentissage.
Si vous recherchez des explications techniques plus détaillées concernant la sécurité en ligne, n'hésitez pas à consulter notre blog sur NordVPN.com/-blog. Celui-ci traite de nombreuses thématiques de fonds mais aussi les plus populaires.

Table of contents:

3 Antivirus
4 Botnet
5 Texte chiffré
6 Violation de données
7 Chiffrement de bout en bout
8 Pare-feu
9 Hacker
11 Adresse IP
12 Cryptojacking
13 Enregistreur de frappe
14 Bombe logique
15 Attaque de l'homme du milieu
16 Réseau
17 Phishing
18 Ransomware
19 Ingénierie sociale
21 Authentification à deux facteurs
22 VPN
23 Wi-Fi
24 Exploit Zero-day



A

Antivirus

Vous avez un nouvel e-mail. Sujet : **je t'aime**
En consultant ce courrier électronique, vous retrouvez une déclaration d'amour rédigée par un admirateur anonyme. Par ailleurs, vous remarquez également une photo. Curieux, vous cliquez sur la pièce jointe... Et téléchargez un virus à votre insu.

Votre antivirus analyse immédiatement ces données avant de les placer en quarantaine. Par chance, il s'agissait d'un « vieux » virus et sa signature était déjà enregistrée dans la base de données de votre logiciel.

S'il est question d'un virus « récent » et absent dans cette base de données, votre antivirus peut utiliser d'autres outils pour procéder à sa détection. En effet, il surveille votre ordinateur lors de chaque activité suspecte et inhabituelle. Si un programme tente de contourner votre antivirus, ou s'exécute au démarrage sans autorisation ou télécharge d'autres données indésirables, votre logiciel entre en action.

Par ailleurs, votre antivirus n'est pas exclusivement dédié aux virus. En effet, il existe différents types de logiciels malveillants tels que les chevaux de Troie (Trojans), ransomwares, keyloggers... Leur objectif ? Tenter de compromettre ou violer l'accès de vos appareils.

Aujourd'hui, le terme « antivirus » désigne différents outils dédiés à la protection des appareils connectés face aux malwares.

Termes associés: virus, malware, logiciel anti-malware, Cheval de Troie (Trojan), ver informatique, logiciel publicitaire (adware).

B

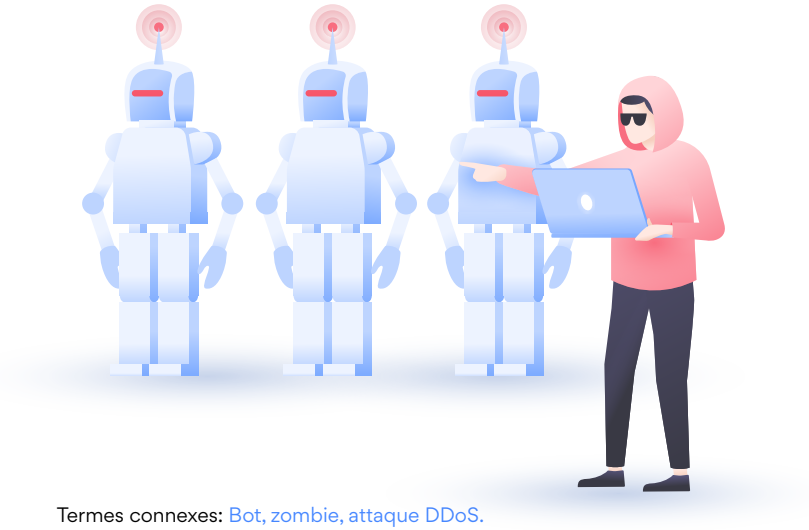
Botnet

Vous ouvrez votre navigateur avant d'entrer l'adresse URL de votre site web favori. Par surprise, vous découvrez que celui-ci est en panne... Et la raison de ce phénomène vous échappera très souvent.

Bien que cela puisse être surprenant, il est ici question de « zombies » ... Ou plutôt de Bots, pour être exact. Brièvement, ceux-ci font référence à un essaim d'appareils infectés procédant à l'envoi de centaines de milliers de requêtes de connexions vers ce site Web afin de le submerger.

Cette attaque est communément appelée DDoS (attaque par déni de service). Les pirates utilisent parfois des botnets à d'autres fins néfastes telles que le spam par e-mail ou la création de faux trafic sur Internet.

Vos appareils peuvent également faire partie d'un botnet en répondant secrètement aux commandes des cybercriminels. En pratique, il peut être difficile d'identifier ce phénomène depuis votre équipement. Toutefois, des performances légèrement réduites ou une surchauffe peuvent confirmer cette situation.



Termes connexes: Bot, zombie, attaque DDoS.

C

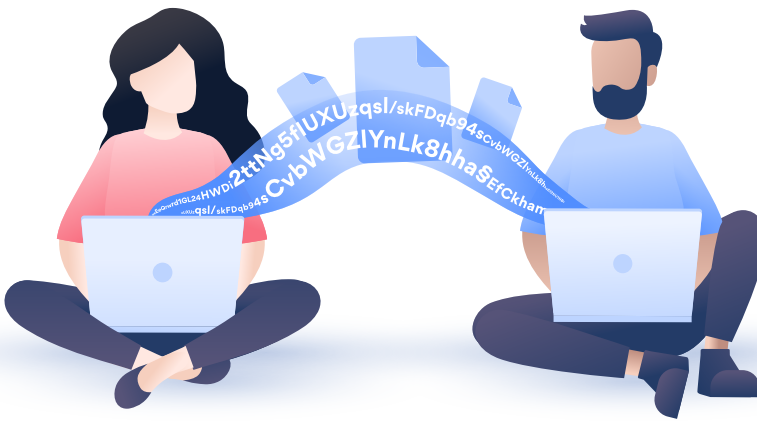
Texte chiffré

Vous ouvrez votre application de messagerie et tapez : « Désolé les gars, je ne peux pas venir ce soir. J'ai un mal d'estomac. »

C'est ce qu'on appelle du texte en clair. Il s'agit d'un contenu non chiffré qui peut être intercepté et lu par un espion en ligne.
C'est aussi ce que l'on appelle un mensonge, si vous êtes en pleine forme, mais qu'un bon film sous la couette est votre priorité.
Par chance, vous utilisez une application de messagerie sécurisée. Celle-ci applique un algorithme complexe afin de transformer votre « mensonge » en texte chiffré.

> "ueEeQrwrd1GL24HWDi2ttNg5fIUXUzqsIFqb94^Ef2NU1NBrD
> rPb84wbReVnclTP2AgnMCkhaHC3UrfR8VWxh3jWWh+0WE"

Ceci s'appelle le chiffrement en action. Le texte en clair est transformé en texte chiffré via une clé sécurisée (chiffrement). Les applications de messagerie utilisées par vos amis détiennent cette clé indispensable pour déchiffrer votre contenu. En revanche, les espions en ligne ne disposent pas de cette clé et ne peuvent pas accéder à vos messages.



Termes associés: chiffrement, message chiffré, texte en clair, déchiffrement.

D

Violation de données

Vous avez une discussion de groupe avec un groupe d'amis proches. Un jour, vous constatez que des captures d'écran concernant ces messages circulent sur les réseaux sociaux. Mauvaise nouvelle : vous venez de subir une violation de données.

Une violation de données se produit lorsque des données sensibles tombent entre les mains d'un individu aux intentions malveillantes.

Comment cela s'est-il produit ? Un hacker serait parvenu à intercepter vos messages privés ou est-il question d'une récupération interne à votre groupe ? Peut-être que le colocataire de Marc s'est connecté à ce chat en ligne alors que celui-ci n'était pas à proximité de son ordinateur portable. Cet homme vous a toujours semblé suspect... Mais vous n'aurez sans doute jamais le fin mot de l'histoire.
Ce type de situation concerne également les données d'entreprise parfois violées par les hackers.

En effet, les entreprises collectent de grandes quantités de données - parfois des informations personnelles d'internautes. Malheureusement, certaines de ces entreprises sont piratées et les données récupérées sont divulguées. Voilà pourquoi vous pourriez retrouver vos identifiants et mots de passe divulgués sur Internet.
Vérifiez régulièrement si vos comptes n'ont pas été compromis lors d'une violation de données en utilisant haveibeenpwned.com.

Termes associés: divulgation involontaire d'informations, fuite de données, déversement de données, récupération de données.

Chiffrement de bout en bout

Une personne vous a confirmé cette information : « Nous allons mettre en œuvre le chiffrement de bout en bout ! » Cependant, comment interpréter ces termes ? Brièvement, le chiffrement de bout en bout élimine les intermédiaires. Imaginez vos données comme une note sur un papier. Avant de l'envoyer, vous prenez soin de placer votre message dans une enveloppe qui le protégera des regards indiscrets. Ce processus évoque une méthode essentielle : le chiffrement.

Lors de l'envoi de votre message, un tiers (par exemple, le service de messagerie instantanée que vous utilisez) ouvre cette enveloppe, analyse vos données avant de les envoyer à votre destinataire.

Ce schéma résume le fonctionnement d'Internet - des intermédiaires sont évoqués lors de chaque interaction.

Le chiffrement de bout en bout supprime ces intermédiaires. En d'autres mots, seuls votre destinataire et vous-même seront capables d'accéder au contenu partagé.

Termes associés: message chiffré, texte brut, texte en clair.

F

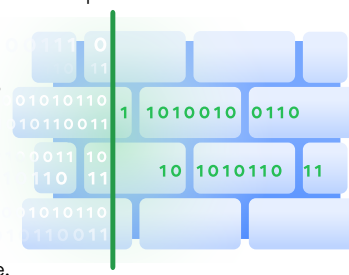
Pare-feu

Vous faites la queue (comme tout le monde) pour accéder à votre boîte de nuit favorite. Lorsque vous arrivez près du videur, celui-ci vous annonce " Aucune entrée ". Vous faites demi-tour et rentrez chez vous avec regret – vous ne ferez pas la fête ce soir.

Le videur applique des règles afin d'autoriser ou non les entrées. Celles-ci ne sont pas arbitraires, mais dépendent des politiques de chaque boîte de nuit et des circonstances extérieures. Par exemple, la boîte de nuit est pleine ou bien une soirée privée se déroule à l'intérieur, seront de parfaits exemples.

En suivant des principes similaires, un pare-feu se situe entre votre réseau local et Internet. En tant que « videur numérique », cet outil applique des règles afin de vérifier si le trafic est satisfaisant pour relier votre réseau.

Un pare-feu autorise le trafic provenant de sources ou d'adresses IP fiables. Vous n'êtes pas sur la liste ? Désolé trafic, mais vous pouvez faire demi-tour et rentrer chez vous. Cette comparaison résume le fonctionnement d'un pare-feu afin de protéger votre réseau du trafic Internet malveillant et préserver votre système.



H

Hacker

Les hackers : toujours plus représentés dans les films, ils sont parfois mystérieux, dangereux ou encore antisocial. Ces internautes sont des hors-la-loi numériques et vivent en dehors de la société. Ils piratent le Pentagone en moins de 5 minutes. Impressionnant !
Ne vous méprenez pas, c'est clairement de la fiction. Les hackers sont des individus lambdas et chaque personne a ses propres motivations. Certains aiment le défi intellectuel qu'est celui d'infiltrer des réseaux. D'autres, appelés hackers au chapeau noir ("black hat"), agissent avec malice. Ceux-ci compromettent les systèmes à des fins personnelles afin de voler des données, de l'argent ou des crypto-monnaies, perturber les réseaux et causer des dégâts aussi variés qu'inquiétants.

De nombreuses entreprises et gouvernements emploient des pirates informatiques. Ceux-ci testent la sécurité de leurs systèmes informatiques en tentant des intrusions numériques. Ces analyses portent un nom : les tests de pénétration. Les méthodes appliquées pourront alors varier (digitales ou physiques).

Un pirate au chapeau blanc ("white hat") peut, par exemple, entrer dans le bâtiment d'une entreprise en suivant un employé. La politesse est généralement de mise – ces salariés ouvrent les portes aux autres, et ce, même aux personnes externes à l'entreprise. Après une intrusion, un pirate peut voler des disques durs contenant des données sensibles, accéder à des ordinateurs sans surveillance ou tout simplement les compromettre (avec des enregistreurs de frappe, par exemple).

Pourriez-vous être concerné par ces situations de piratage ?

Tout dépend de vos mesures de sécurité. Cependant, certains hackers extrêmement qualifiés sont capables d'accéder aux réseaux les plus sécurisés. La bonne nouvelle : ceux-ci privilégieront probablement des cibles plus « juteuses » que votre compte Steam.

Habituellement, vous ne serez pas directement impactés par les méfaits des pirates informatiques (cf. « violation de données »).

En revanche, vous pourrez vous méfier des escrocs qui créent de faux sites web afin de propager des liens malveillants (cf. « phishing »). En saisissant votre mot de passe depuis l'un de ces domaines, vous divulguerez vos identifiants à un escroc.

Termes associés: hacker chapeau gris, hacker chapeau noir, hacker chapeau blanc, intrusion, tests d'intrusion.

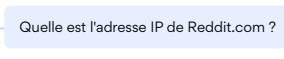
I

Adresse IP

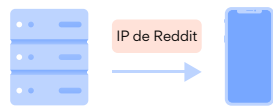
Votre smartphone dispose d'une adresse IP (Protocole Internet) attribuée par votre réseau. Ce processus concerne également votre ordinateur portable, Smart TV ou d'autres équipements connectés à Internet. Aucun appareil ne pourrait fonctionner en ligne sans appliquer ce processus. Pourquoi cela ?

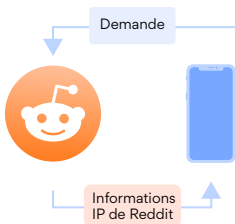
Imaginons que vous souhaitez combler du temps perdu. Vous sortez votre téléphone et inscrivez « Reddit.com » dans la barre de votre navigateur.

Votre smartphone n'a pourtant aucune connaissance de « Reddit.com ». Les nombres (et non les mots) font référence à sa « langue maternelle ». Pour accéder à Reddit, votre téléphone envoie une requête : « Quelle est l'adresse IP de Reddit.com ? »



Cette question est adressée à un serveur spécial (base de données d'adresses IP). Le serveur identifie l'adresse IP de Reddit avant de l'indiquer à votre smartphone.





Par la suite, votre téléphone envoie une requête à l'adresse IP de Reddit. Le site web en question renvoie ses informations à l'adresse IP de votre téléphone.

Enfin, la page principale de Reddit se charge sur votre écran. Pourtant, rien ne suscite votre intérêt et vous décidez de quitter le navigateur.

J

Cryptojacking

Votre ordinateur travaille à plein régime et son ventilateur fonctionne activement. Tout paraît si lent et vous devez patienter pour charger une simple page web.

Comment expliquer ce phénomène ? Un pirate informatique pourrait avoir « détourné » votre équipement connecté afin de miner une cryptomonnaie.

Vous aurez probablement déjà entendu parler du cryptomining. Brièvement, il s'agit ici de réception de crypto-monnaie en échange de calculs complexes assurés par votre ordinateur. Toutefois, ces calculs consomment une puissance informatique considérable. Celle-ci est généralement trop importante pour que le cryptomining soit rentable.

Pour résoudre cette problématique, les pirates détournent des appareils afin de miner à leur place une crypto-monnaie. Ce type d'attaque (appelée cryptojacking) évoque l'utilisation de logiciels malveillants ou d'une ligne de codes via une page web. Les victimes se demandent alors pourquoi leur ordinateur est si brûlant après quelques minutes d'utilisation.

P.S. Nous l'avouons, le classement du cryptoJacking depuis la lettre J pourrait vous surprendre. Néanmoins, la lettre J est un véritable désert dans le domaine de la cybersécurité... Nous en avons donc abusé.

Termes associés: cryptomining, cryptomining malveillant.

K

Enregistreur de frappe

Vous rédigez un article dans la bibliothèque pour votre cours d'économie. Vous avez du retard et la batterie de votre ordinateur portable est déchargée. Problème : vous avez laissé le cordon d'alimentation à la maison.

Une fille sympathique est assise à vos côtés. Vous souhaitez lui emprunter son ordinateur portable - 5 minutes vous suffiront pour terminer votre article. Cette demoiselle est ravie de vous aider. Vous prenez son ordinateur portable, avant de vous connectez à votre service cloud afin de terminer votre exposé dédié aux politiques antitrust menées lors des années 90.

Lorsque vous rentrez chez vous, vous constatez que votre messagerie et certains de vos comptes en ligne ont été piratés. Que s'est-il passé ?

La fille que vous avez rencontrée disposait d'un keylogger sur son ordinateur portable. Brièvement, cet outil enregistre les frappes au clavier. Le Keylogger a enregistré chaque mot que vous avez indiqué, y compris le mot de passe de votre service cloud.

Malheureusement, vous utilisez un mot de passe similaire via votre service cloud et votre messagerie. La pirate est donc parvenue à accéder à votre compte de messagerie principal (voilà pourquoi il est vivement déconseillé de réutiliser des mots de passe). Par ailleurs, cette fille rencontrée a réinitialisé les mots de passe de vos autres comptes.

Les keyloggers ne sont que rarement des filles à l'allure amicale. Habituellement, ceux-ci prennent la forme d'outils matériels que les pirates associent à des ordinateurs non protégés. Il peut également s'agir d'outils logiciels utilisés illégalement ou légalement. Certaines entreprises, par exemple, installent des enregistreurs de frappe depuis leurs ordinateurs afin de surveiller leurs employés.
Termes associés: logiciels espions, spywares.

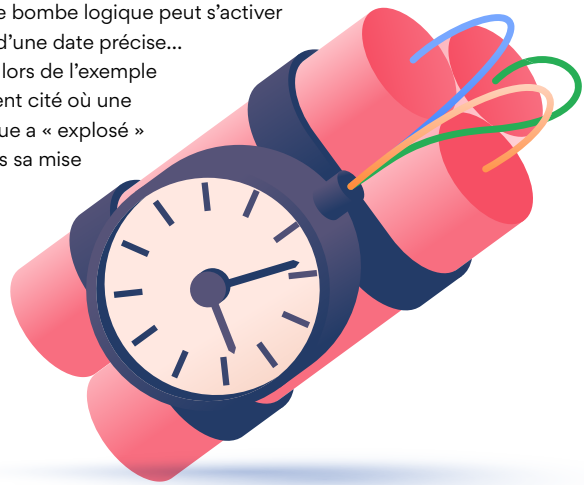
L

Bombe logique

Vous êtes au travail, cinq minutes avant la deadline imposée par votre client. Vous rédigez à toute allure quand tout se bloque. Vous ne pouvez plus accéder au réseau interne ou à un fichier distant. A votre insu, votre travail semble fini pour aujourd'hui.

Le lendemain, certaines rumeurs vous surprennent. Il s'agirait d'un ancien employé... Un informaticien mécontent ayant volontairement fermé le réseau interne. Comment expliquer cette situation si cet individu a été licencié il y a six mois et n'avait plus accès aux systèmes de l'entreprise ?

Lors de son dernier jour de travail, ce salarié licencié a laissé une bombe logique sur le réseau interne de son entreprise. Brièvement, il s'agit d'un code malveillant qui s'active lorsque certaines conditions sont remplies (par exemple, lorsque le PDG se connecte à un système sensible). Une bombe logique peut s'activer en fonction d'une date précise... Tout comme lors de l'exemple précédemment cité où une bombe logique a « explosé » six mois après sa mise en place.



Termes associés: bombe à retardement, time bomb, attaque d'initié

M

Attaque de l'homme du milieu

Vous êtes dans un café et vous vous connectez au Wi-Fi public. Vous venez d'envoyer un e-mail destiné à un entrepreneur en lui demandant son numéro de compte bancaire. Vous obtenez le numéro, payez les frais et profitez de cet instant pour savourer un petit café.

Deux jours plus tard, l'entrepreneur vous contacte et vous questionne : « Quand serai-je payé ? »

Comment ?

Vous vous revoyez alors dans le café du coin. Malheureusement, un hacker est arrivé avant vous avant de préparer un point d'accès jumeau nommé « Coffee shop wifi GRATUIT ». En croyant qu'il s'agit d'un réseau légitime, vous vous y êtes connecté. Dès cet instant, le pirate peut surveiller votre trafic Internet.

Vous avez été victime d'une attaque appelée « homme du milieu ».

Le pirate a intercepté votre e-mail et vous a envoyé son propre numéro de compte bancaire. Celui-ci a reçu vos fonds, tandis que l'entrepreneur attend toujours les honoraires.

Gardez à l'esprit que le Wi-Fi public est un point d'accès dangereux. Même s'il n'est pas configuré par un pirate informatique, il ne vous sera pas possible de vérifier si celui-ci est correctement configuré. Un hacker se cache peut-être derrière chacune de vos interactions. Utiliser un VPN avant de vous connecter à un Wi-Fi public est donc essentiel.

Termes associés: evil twin, attaque jumelle, Wi-Fi honeypot

N

Réseau

Vos appareils sont associés à un réseau. Celui-ci fait également partie d'un réseau plus grand, puis d'un autre encore plus grand... Et ainsi de suite. Ce schéma porte un nom : Internet. Peu importe votre profil et la nature de votre connexion, vous utiliserez cet espace digital.

Le réseau le plus proche de vous est appelé LAN (réseau local). Celui-ci fait référence à un groupe d'appareils interconnectés depuis un emplacement physique similaire. En d'autres mots, lorsque vous vous connectez à votre routeur domestique, vous vous connectez à votre réseau local.

Très souvent, votre réseau domestique sera relativement petit et dénombrera jusqu'à 10 appareils connectés (ou plus si vous êtes un adepte de la domotique, la technologie est si attrayante et passionnante). Un réseau local peut également concerner chaque équipement d'une entreprise ou couvrir un domaine scolaire avec des milliers d'appareils interconnectés.

Termes associés: Internet, LAN.

P

Phishing

Vous recevez un e-mail de votre banque. Avec stupeur, vous remarquez que celui-ci est un avertissement – une personne a tenté de retirer de l'argent de votre compte. Vous consultez alors cette phrase : « Veuillez envoyer votre identifiant et votre mot de passe IMMÉDIATEMENT afin de confirmer votre identité ».

Effrayant, n'est-ce pas ? Toutefois, vous ne devriez pas agir sans aucune réflexion.

Si vous vérifiez soigneusement l'expéditeur, vous constaterez probablement qu'il ne s'agit pas de votre banque, mais d'un internaute malveillant. Ne répondez pas et ne cliquez sur aucun lien dans l'e-mail. Appelez directement votre banque afin de faire le point sur cet e-mail inquiétant.

Ce type d'escroqueries peut prendre plusieurs formes et porte un nom : le phishing. Ces messages ou e-mails évoquent la peur et l'urgence afin d'extraire des données confidentielles. Autre exemple : vous vous connectez à un faux site web semblable à celui de votre université. Vous entrez votre identifiant et mot de passe... Et ceux-ci sont transmis à un pirate.

Comment préserver votre cybersécurité ? En 2 mots : restez prudent. Méfiez-vous des messages louches incitant la peur ou promettant quelque chose de « trop beau pour être vrai ». Le message sera toujours semblable à « il vous suffit de cliquer ici pour réclamer votre prix ».

Arrêtez, analysez et revérifiez. Ne cliquez jamais sur un lien si l'URL semble illégitime. En général, ne saisissez ni ne divulguez jamais votre mot de passe si vous estimez qu'un e-mail est douteux.

R

Ransomware

Vous allumez votre ordinateur pour naviguer sur le web et... Attendez, qu'est-ce que c'est ? Votre écran est bloqué et affiche un message inquiétant : « Vos fichiers ont été chiffrés par NarutoRun Hacker Group. Vous avez une semaine pour transférer 500 € en Bitcoins vers notre portefeuille électronique ou vos fichiers seront perdus à tout jamais. Rasengan ! »
Ce message ressemble à une comédie mal écrite, mais l'humour n'est absolument pas au rendez-vous. Un ransomware est un logiciel malveillant qui chiffre les données d'une victime. Seuls les pirates informatiques à l'origine de cette attaque peuvent déchiffrer vos fichiers grâce à leur clé unique (Il existe de nombreux protocoles de chiffrement pratiquement infaillibles sans la clé de déchiffrement). Cf. texte chiffré / chiffrement de bout en bout
Il est vivement déconseillé de payer ce type de rançon. En effet, votre argent (plus probablement vos crypto-monnaies généralement imposées par les pirates) ne servirait qu'à entretenir les criminels. Privilégiez plutôt certains conseils efficaces face aux ransomwares :

- Ne téléchargez jamais depuis des sites web douteux. N'ouvrez aucun lien, e-mail ou message suspect. Voir : hameçonnage (phishing).
- Sauvegardez périodiquement vos données sensibles.
- Mettez à jour vos applications et logiciels (en particulier vos logiciels dédiés à la cybersécurité).
- Utilisez des mots de passe complexes.

S

Ingénierie sociale

Aux aurores, vous êtes réveillé par votre smartphone. Votre correspondant explique poliment qu'il est technicien chez LiteNet, votre fournisseur d'accès à Internet. D'après ses dires, une panne de réseau a été confirmée, et celle-ci aurait éventuellement entraîné une perte de données mineure.

« Pourriez-vous fournir les quatre derniers chiffres de votre numéro de carte de crédit afin d'entamer des vérifications en fonction d'enregistrements sur nos serveurs ? »

Encore endormi, vous fournissez ces données bancaires avant de repartir dans vos rêves. Vous vous réveillez ensuite deux heures plus tard, vous prenez un copieux petit-déjeuner et constatez avec effroi que vous avez été piraté.

La personne qui vous a contacté n'était pas un technicien, mais un ingénieur social - un escroc expert en manipulation psychologique et doué pour inciter ses victimes à effectuer une action spécifique ou à révéler des données sensibles.

Résumons ce qu'il s'est passé. Un escroc vous a réveillé aux aurores, s'est présenté pour apaiser vos soupçons (en évoquant LiteNet, le fournisseur d'accès Internet le plus populaire de votre région) avant d'employer un jargon technique (parfois sans significations) afin de sembler légitime.

Ensuite, cet individu a contacté votre FAI en usurpant votre identité pour mentionner l'oubli d'un mot de passe. Il a fourni les quatre derniers chiffres de votre numéro de carte de crédit afin de confirmer votre identité et réinitialiser votre mot de passe - y compris celui-ci de votre messagerie.

LiteNet est un faux fournisseur Internet fictif que nous avons inventé pour cet exemple. Toutefois, de nombreuses entreprises peuvent réinitialiser votre mot de passe par téléphone uniquement en indiquant les quatre derniers chiffres de votre carte de crédit. Il est alors essentiel de fournir le moins d'informations sensibles lors de votre inscription et affirmer explicitement que vous ne souhaitez divulguer aucune information personnelle par téléphone.

Les ingénieurs sociaux utilisent de nombreuses techniques pour manipuler les internautes... Et certaines d'entre elles sont sophistiquées et brutales. Un escroc peut envoyer un millier de faux e-mails dans l'espoir de trouver quelques victimes caractérisées par un manque de précaution. Celles-ci répondront avec les coordonnées de leur carte de crédit ou leurs mots de passe.
Cf. hameçonnage (phishing).

T

Authentification à deux facteurs

Vous vous connectez à Twitter sur le téléphone de votre ami car votre smartphone est resté chez vous. Puisqu'il s'agit d'un nouvel appareil, vous devez confirmer votre connexion via une application d'authentification. Qui se trouve sur votre téléphone. Qui est actuellement chez vous.

Voici un exemple typique de cybersécurité catch-22 !

Certes, ce système peut engendrer de légers inconvénients, mais l'authentification à deux facteurs (2FA) vous garantit une protection supplémentaire non-négligeable. Si vous rencontrez des difficultés pour accéder à votre compte sans votre smartphone, les pirates rencontreront ces mêmes difficultés.

Généralement, les deux facteurs font référence à :

Une information personnelle (un mot de passe ou code PIN) ou quelque chose que vous possédez (un téléphone, livre de codes ou vos données biométriques).

Aucun système n'est infaillible, mais le 2FA améliore la sécurité de vos comptes à un niveau supérieur comparé aux autres internautes. Les cybercriminels sont souvent opportunistes. Au lieu de tenter de contourner le 2FA, ceux-ci privilégieront d'autres cibles... De préférence un internaute qui utilise ABCDEFG comme mot de passe.

Vous l'aurez compris, l'activation du 2FA depuis chaque service compatible est vivement conseillées. Cette solution optimise votre sécurité en ligne sans évoquer d'inconvénients majeurs.

Termes associés: authentification multifacteur.

V

VPN

Vous naviguez, vous scrollez, vous surfez. Lors de chaque connexion, vous laissez derrière-vous certaines de vos empreintes. Votre fournisseur de services Internet a accès à votre activité en ligne. En d'autres mots, votre FAI peut identifier chaque site web que vous visitez grâce aux adresses IP récoltées.
Outre votre confidentialité, votre sécurité en ligne est également remise en cause. Certains sites web n'utilisent pas de protocole de communication sécurisé et la plupart des applications ne divulguent pas leurs solutions relatives à la cybersécurité. Vous devrez alors accorder aveuglément votre confiance... Mais à quel prix ?
Un VPN (réseau privé virtuel) est un outil capable de diriger toute votre activité en ligne via un serveur sécurisé, chiffrer vos données et modifier votre adresse IP ainsi que votre emplacement virtuel. Certes, cela peut sembler technique aux premiers abords. Toutefois, les VPN sont des outils accessibles à tous.

Cependant, tous les VPN ne sont pas forcément recommandables. Un réseau privé virtuel achemine l'ensemble de votre trafic depuis ses serveurs. Celui-ci peut donc collecter vos données afin de les vendre au plus offrant. Rassurez-vous, la majorité des VPN les plus populaires évoquent des services transparents et ne conservent aucun historique de navigation (no-log). Aucune vente ou divulgation à des tiers ne pourra vous inquiéter.
NordVPN, par exemple, vous propose une politique de non-conservation des données personnelles. Nos services sont régulièrement évalués par l'un des quatre plus grands cabinets d'audit dans le monde.

Termes associés: bombe à retardement, menace d'initié.

W

Wi-Fi

Vous êtes dans votre chambre d'hôtel et naviguez grâce au Wi-Fi gratuit. Quelques étages plus bas, un hacker espionne votre activité en ligne. Inquiétant, n'est-ce pas ?

Le Wi-Fi public est une solution particulièrement dangereuse. En effet, les cybercriminels peuvent utiliser de nombreuses méthodes pour exploiter et compromettre ces accès.

Lorsqu'un routeur est mal configuré, un pirate peut observer le trafic Internet de chaque personne connectée au hotspot concerné. Le pirate peut également injecter des logiciels malveillants dans le stockage interne de votre équipement depuis un réseau commun.

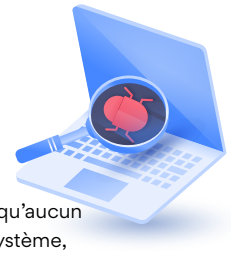
Par ailleurs, un hacker peut créer de faux hotspots – accès jumeau – et vous inciter à vous y connecter. Cf. Attaque de l'homme du milieu.
Votre sécurité sera caractérisée par :

La configuration et les mesures de sécurité appliquées depuis le réseau Wi-Fi de l'hôtel.
Les pratiques des sites web que vous visitez et des applications que vous utilisez.
Vos pratiques personnelles concernant la cybersécurité.

Habituellement, il est impossible de vérifier le niveau de sécurité d'un réseau public. Evitez donc d'accéder à vos données personnelles lorsque vous y êtes connecté. Pourquoi ne pas utiliser vos données mobiles (4G) ou activer un VPN ?
PS : Si vous organisez un événement, ne vous reposez pas sur le Wi-Fi fourni par le lieu choisi car celui-ci est rarement sécurisé. Configurer correctement un point d'accès Wi-Fi est souvent complexe et nécessite des connaissances techniques spécifiques. Il est préférable d'embaucher des professionnels si vous ne disposez pas de compétences techniques. Toutefois, votre travail est tout aussi important - vous devez communiquer avec vos invités ! Informez chaque participant à propos de vos points d'accès gratuits et prévenez-les que les autres hotspots évoqueront des risques, et ce, même s'ils semblent légitimes.
Termes associés : envoi de logiciels malveillants, sniffer Wi-Fi.

Z

Exploit Zero-day



Vous avez mis à jour votre logiciel, installé un antivirus et activé votre pare-feu. Vous pensez alors qu'aucun pirate informatique ne peut s'introduire dans votre système, n'est-ce pas ?
Si seulement tout était si simple.

Les réseaux informatiques, logiciels et le matériel sont créés par des individus. Naturellement, l'erreur est humaine et la considération de tous types de scénarios est impossible... Et les vulnérabilités sont probables. Les pirates exploitent ces failles et recherchent le maillon le plus faible du système afin de le compromettre.
Dès qu'une vulnérabilité est découverte, celle-ci est corrigée. En d'autres mots, les mises à jour que vous installez depuis vos applications ou votre système font majoritairement référence à des correctifs pour les vulnérabilités nouvellement découvertes.

(Naturellement, certaines vulnérabilités ne peuvent pas être corrigées. Les humains, et non les machines, sont les maillons les plus faibles en matière de cybersécurité. Cf. ingénierie sociale)

Une vulnérabilité zero-day est inconnue du fournisseur et n'évoque donc pas de corrections. Ces termes font référence au nombre de jours disposé par un fournisseur pour corriger ladite vulnérabilité – c'est-à-dire zéro jour. Une attaque basée sur cette vulnérabilité est appelée « exploit zero-day » ou « attaque zero-day ».

Ainsi, même si vous gardez votre système sécurisé, corrigé et mis à jour, un exploit zero-day peut le compromettre depuis une vulnérabilité jusque-là inconnue. Une vigilance constante sera donc la seule et unique solution pour préserver votre sécurité. Naviguez avec précaution, utilisez des mots de passe complexes et ne cliquez jamais sur un lien si celui-ci vous semble douteux.

En appliquant ces recommandations, vous minimiserez les risques tout en incitant les pirates à rechercher des cibles plus « accessibles ».

Termes associés: vulnérabilité zero-day, attaque zero-day.