GLOSSAIRE CYBERSECURITE

Adware, Publiciel	Il s'agit d'une fonction intégrée dans un logiciel afin d'afficher de la publicité. L'intention est malveillante à partir du moment où cette fonction est cachée et agit sans que l'éditeur du logiciel ne vous ait prévenu. Cela peut être le cas notamment si vous téléchargez gratuitement un logiciel normalement payant (jeu, plug-in vidéo, etc.). Couplé à des logiciels espions, un adware peut même vous envoyer de la publicité ciblée.
Antivirus	C'est un logiciel qui détecte et neutralise les logiciels malveillants (malwares). Pour protéger efficacement un équipement, un antivirus doit être toujours allumé, et à jour, car de nouveaux malwares émergent régulièrement.
Backdoor, Porte dérobée	Il s'agit d'un accès dissimulé qui permet à un pirate de se connecter à votre équipement à votre insu. Cet accès peut être caché dans un logiciel ou prendre l'aspect d'un petit équipement connecté physiquement (et très discrètement) à votre ordinateur.
Bitcoin, BTC	Le bitcoin (ou BTC) est la cryptomonnaie la plus répandue.
Chapeau blanc, White hat	C'est un "hacker éthique", c'est-à-dire un expert de la sécurité informatique dont les intentions sont bienveillantes.
Chapeau gris, Grey hat	C'est un hacker qui agit sans mauvaise intention. Sa principale motivation est de prouver son habileté afin d'être reconnu par ses pairs, quitte à braver la loi.
Chapeau noir, Black hat	C'est un cybercriminel qui agit dans le but de nuire ou de faire du profit (espionnage, vol et revente d'information, manipulation, chantage, extorsion, demande de rançon, etc.).
Cheval de Troie, Trojan horse	Il s'agit d'une fonctionnalité malveillante cachée dans un logiciel qui semble tout à fait normal. Une fois installé, le cheval de Troie permet au pirate d'utiliser furtivement l'ordinateur à distance, de dérober des informations, de filmer ou d'écouter l'utilisateur à son insu.
Chiffrement	C'est un procédé qui rend les données incompréhensibles, sauf pour la personne qui détient la clé de déchiffrement. Tout fichier peut être chiffré. Il existe de nombreux logiciels de chiffrement et certains sont même intégrés aux logiciels de messagerie afin de sécuriser l'envoi d'e-mails sensibles.

Cible d'opportunité	Il s'agit d'une personne que les pirates n'avaient pas forcément prévus de prendre pour cible, mais qui se trouve sur leur chemin et leur permet d'atteindre un objectif plus grand, par "rebond". C'est comme ça qu'ils parviennent à approcher des cibles stratégiques et à s'octroyer des droits de plus en plus élevés sur les réseaux dont ils prennent le contrôle.
Cible stratégique	C'est une personne que les pirates ont choisi d'attaquer, par exemple parce qu'elle est importante dans la société, détient des informations sensibles, dispose des droits d'accès particulièrement élevés, etc. Avant d'atteindre leur cible, les pirates vont apprendre à la connaître, se renseigner sur son entourage, sa famille, son emploi du temps... jusqu'à ses goûts personnels.
Clé Wifi	C'est le mot de passe qui permet de se connecter au réseau Wifi. Il existe différents types de clé Wifi. Les clés "WEP" et "WPA" sont les moins sécurisées. Pour votre box à la maison, privilégiez une clé "WPA2", beaucoup plus robuste.
Cryptomonnaie, cybermonnaie	Ce terme regroupe les monnaies "alternatives" qui sont échangées en ligne afin de réaliser des transactions sans passer par les monnaies officielles. Les cryptomonnaies font l'objet d'échanges directs et ne dépendent pas d'une banque centrale. Leur statut juridique varie d'un pays à un autre : parfois interdites, parfois institutionnalisées, elles ne sont pas encore reconnues comme de vraies monnaies. La cryptomonnaie la plus répandue est le "bitcoin".
Déni de service, Denial of Service, DOS	On parle de déni de service lorsqu'un système (un serveur de messagerie par exemple) n'arrive plus à remplir correctement sa fonction. C'est le but de certaines actions de sabotage qui consistent à noyer les serveurs de requêtes pour les ralentir ou les bloquer, paralysant l'activité de l'entreprise. Lorsque les requêtes sont lancées depuis plusieurs sources, on parle de "déni de service distribué", en anglais "distributed denial of service" (DDOS).
Double authentification	C'est un système qui vérifie que vous êtes bien vous, à travers 2 canaux séparés. C'est le cas par exemple pour les paiements en ligne qui demandent de saisir les informations bancaires ET un code temporaire envoyé par SMS. La double-authentification augmente grandement le niveau de sécurité.
Filtre de confidentialité	Il s'agit d'un écran de protection qui s'installe par-dessus votre écran d'ordinateur ou de smartphone, le rendant illisible à toute personne qui regarde de côté. Ce dispositif très simple empêche le "piratage visuel" : un équipement indispensable dans les transports et les lieux publics !
Fraude au Président	La Fraude au Président consiste à se faire passer pour le dirigeant d'une société, le plus souvent pour donner l'ordre de réaliser des virements bancaires. Cette escroquerie fréquente repose sur l'usurpation d'identité, l'ingénierie sociale, la manipulation et l'abus de confiance.

Hacker	Ce mot anglais désigne de façon large tout spécialiste en informatique qui cherche à contourner les dispositifs de sécurité. C'est un terme très généraliste, qui regroupe autant les cybercriminels que les pirates bienveillants qui contribuent à renforcer la sécurité des failles qu'ils détectent. Il désigne avant tout la compétence, pas la moralité.
Hacktiviste	C'est un "hacker-activiste", c'est-à-dire une personne qui utilise le piratage informatique pour défendre une cause ou une idéologie politique, sociétale ou environnementale, quitte à transgresser la loi.
HTTPS	Cet acronyme permet de reconnaître les sites web sécurisés, contrairement à ceux dont l'adresse ne contient que "http://" sans le "s". HTTPS signifie "Hypertext Transfer Protocol Secure", c'est-à-dire qu'il protège l'intégrité et la confidentialité des données qui sont échangées entre le serveur et vous. Ce protocole est particulièrement important pour tous les sites sur lesquels vous pouvez être amené à saisir des données sensibles (site bancaire, achat en ligne, etc.).
Ingénierie sociale, Social Engineering	C'est un terme très large qui regroupe toutes les techniques utilisées par les pirates pour manipuler psychologiquement leur cible. On parle d'ingénierie sociale dès qu'il s'agit de se renseigner sur une personne (via son entourage ou les réseaux sociaux), de la cibler en fonction de ses passions, d'exploiter ses faiblesses psychologiques, d'abuser de sa confiance, pour obtenir de sa part une information, de l'argent, un bien, une mise en relation vers une autre cible ou le déclenchement d'un action malveillante.
IP	Une adresse IP (Internet Protocol) est un numéro unique qui permet d'identifier votre équipement (PC, smartphone...) sur un réseau, et donc sur Internet. Le fait qu'un pirate connaisse votre adresse IP est dangereux car cela lui permet de cibler spécifiquement votre équipement pour y accéder ou pour lancer une attaque en faisant croire qu'elle vient de vous.
Keylogger	C'est un programme qui espionne l'utilisateur en enregistrant les touches saisies au clavier.
Malware, Logiciel malveillant	Ce terme regroupe tous les programmes malveillants au sens large : virus, ver, cheval de Troie, ransomware, adware, rootkit, key logger, rogue, backdoor...
Phishing, Hameçonnage	Le phishing consiste à vous envoyer un e-mail qui ressemble à un "vrai e-mail", mais qui sert à récupérer vos données personnelles ou à installer un malware. Il semble provenir d'un expéditeur de confiance (votre banque, les impôts...) ou d'un contact personnel (famille, ami), avec un objet rédigé de façon à attirer votre attention ("Votre compte va expirer", "Regarde cette vidéo"...). Il contient un lien, qui renvoie vers un site sur lequel vous allez saisir vos données en pensant être sur le site officiel. Il peut aussi contenir une pièce jointe qui infectera votre équipement si vous l'ouvrez. La meilleure façon de s'en prémunir est de se connecter directement au site officiel sans cliquer dans l'e-mail.

Ransomware, Rançongiciel	C'est un programme malveillant qui bloque l'accès à vos propres données, les chiffre pour les rendre illisibles, ou menace de les détruire... tant que vous ne payez pas une rançon.
RAT	Un "Remote Administration Tool", ou "outil d'administration à distance", est un programme qui permet de prendre totalement le contrôle d'un ordinateur à distance. Il peut s'agit d'un programme légitime, par exemple si une personne pilote son propre équipement à distance, ou si elle a donné son accord à un tiers, comme un prestataire de télémaintenance. Pour un pirate, l'installation d'un RAT à l'insu de l'utilisateur est un très bon moyen de pénétrer furtivement dans un système d'information et d'y rester.
RGPD	Le Règlement Général de la Protection des Données est une directive européenne qui protège l'utilisation des données personnelles (nom, numéro de téléphone, n° de carte bleue, etc. et bien sûr les données sensibles comme les empreintes digitales, les données de santé...). Les organismes qui traitent ces données doivent respecter des règles strictes, et les citoyens qui confient leur données ont des droits.
Rogue	Parfois appelés également "scareware", les rogues sont de faux logiciels de sécurité qui servent en réalité à diffuser des programmes malveillants. Ils prennent par l'exemple l'apparence d'avertissements ("Votre ordinateur est infecté, cliquez-ici pour résoudre le problème") et vont jusqu'à vous faire payer le téléchargement d'un faux logiciel antivirus.
Rootkit	Il s'agit d'un ensemble d'outils logiciels que le pirate installe discrètement sur un ordinateur pour agir ensuite. Si le rootkit est bien fait et s'avère indétectable, il agit comme une "cape d'invisibilité" : le pirate peut alors utiliser différents types de malwares pour contrôler l'ordinateur à distance, enregistrer la saisie au clavier, subtiliser des données ou installer d'autres programmes... sans éveiller le moindre soupçon.
Shadow IT	Ce terme désigne les systèmes, programmes, applications... qui sont utilisés dans l'entreprise sans que la Direction des Systèmes d'Information n'en soit informée. Il peut s'agir de clouds privés, de logiciels officieux, de macros dans des fichiers Excel, ou encore de matériel personnel apporté sur le lieu de travail ou connecté à l'environnement de l'entreprise. Le Shadow IT fait actuellement partie des risques cyber les plus répandus.
Screenshooter	C'est un programme qui espionne l'utilisateur en réalisant des captures d'écran à intervalles réguliers ou en continu.
URL	Une URL est une adresse web qui permet d'accéder à une ressource sur Internet (un site, une vidéo, une image...). L'URL d'un site est visible dans la barre d'adresse de votre navigateur ("http://www...") ou au survol de la souris sur un lien cliquable. Le fait de vérifier que l'URL à laquelle vous accédez est bien légitime est un très bon réflexe sécurité pour éviter de se retrouver sur un site potentiellement malveillant. "URL" est un acronyme anglais qui signifie "Uniform Resource Locator".

Usurpation d'identité	C'est le fait de se faire passer pour quelqu'un d'autre. Dans le monde numérique, les techniques sont nombreuses : un pirate peut usurper votre adresse e-mail, votre numéro de téléphone, votre pseudo sur un réseau social, etc.
Ver, Worm	C'est un programme malveillant qui, une fois lancé, se propage automatiquement dans un réseau sans que l'utilisateur n'ait besoin d'agir.
Virus	C'est un programme malveillant caché dans un document d'apparence légitime. Il a besoin d'une action humaine pour se propager.
VPN	Un VPN est un Réseau Privé Virtuel (Virtual Private Network), c'est-à-dire un logiciel qui cache votre adresse IP et chiffre vos données. C'est un dispositif de protection particulièrement utile si vous vous connectez à un réseau public, afin d'éviter que vos données ne circulent en clair et qu'une personne malveillante ne connaisse votre adresse IP.

© Dæsign - Ces contenus sont protégés par le droit d'auteur. Leur reproduction est interdite sans l'accord préalable de Daesign. La reproduction sur un support papier demeure autorisée aux conditions suivantes : usage non commercial, respect de l'intégrité des documents reproduits (ni modifications, ni altérations), citation claire et lisible du copyright Dæsign.