Lexique du parfait hacker

Dans un environnement marqué par un développement technologique constant et une digitalisation des pratiques, les attaques informatiques ne cessent aujourd'hui de croître que ce soit dans la sphère professionnelle ou privée, avec des conséquences souvent très sérieuses pour les données personnelles.

Derrière elles se cachent des petits êtres mystérieux, les pirates informatiques ou « *hackers* », qui semblent faire preuve d'une inventivité sans cesse renouvelée, tant est si bien que la question pour les entreprises ou les particuliers n'est plus « *Est-ce que je vais être attaqué un jour* » mais plutôt « *Quand vais-je être attaqué ?* ».

C'est pourquoi, afin de vous aider à naviguer en eaux troubles et de mieux comprendre les termes employés par les experts de la cybersécurité, nous vous proposons un petit lexique des termes les plus souvent utilisés lors de ces « *cyber attacks* ».

Backdoor (porte dérobée) : Moyen d'accès non autorisé, dissimulé dans un programme, qui permet à un utilisateur malveillant de s'introduire dans un système informatique.

> **Exemple** : création d'un nouveau compte administrateur avec un mot de passe choisi par un pirate

Canular (hoax) : Information fausse, périmée ou invérifiable qui est propagée spontanément par les internautes. Se présentant essentiellement sous forme écrite, comme un courrier électronique, elle invite en général l'internaute à faire suivre l'information à tous ses contacts, ce qui entraîne une réaction en chaîne.

> **Exemples :**
> - alertes à un virus ou à une disparition d'enfant
> - promesses de bonheur
> - chaînes de solidarité

Cheval de Troie : Logiciel malveillant faisant référence à l'Iliade d'Homère qui, sous une apparence légitime, exécute des actions nuisibles à l'insu de l'utilisateur. En introduisant une « *porte dérobée* » sur un ordinateur, le cheval de Troie permet ainsi à un pirate informatique de prendre le contrôle de cet ordinateur à distance, de voler les mots de passe enregistrés, de copier des données et d'exécuter des actions nuisibles.

> **Exemple :** un pirate envoie un mail à la personne dont il cherche à infiltrer l'ordinateur et met son « *cheval* » en pièce jointe. Si l'utilisateur ouvre ce fichier, le mouchard s'installe alors en toute discrétion sur la machine, souvent dissimulé dans un fichier ou programme qui fonctionne tout à fait normalement, comme un jeu par exemple

Déni de service : Attaque par saturation qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société. Si cette technique n'altère pas le contenu du site Internet de la société, elle le paralyse toutefois pendant plusieurs heures, bloquant ainsi son accès aux internautes.

Deepfake : Vidéo truquée très réaliste réalisée grâce à l'intelligence artificielle. Similaires aux infox (voir ci-dessous), cette technique consiste à superposer des images vidéos déjà existantes sur d'autres.

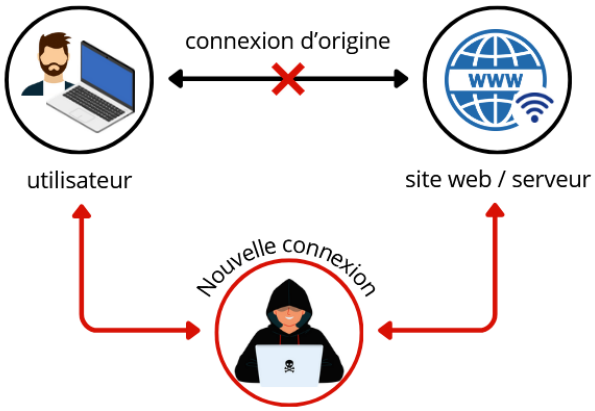
Drive by Download : Téléchargement non désiré, réalisé à l'insu de l'utilisateur, par exemples lors de la visite d'un site Web, de l'ouverture d'une pièce jointe dans un mail, ou lors d'un clic sur une pop-up sur un site malveillant.

Faille : Vulnérabilité dans un système informatique permettant à un pirate informatique de porter atteinte au fonctionnement normal dudit système, à sa confidentialité ou à l'intégrité des données qu'il contient.

Faux support technique : Type de fraude qui consiste à effrayer les victimes en leur faisant croire que leur équipement est défaillant ou victime d'un problème technique grave.
Très souvent, le faux technicien installera un logiciel à distance qui lui permettra de prendre le contrôle des appareils de ses victimes et d'y voler leurs mots de passe et documents.

Homme du milieu (attaque de l'homme du milieu) : Attaque qui consiste pour un hacker à se placer en position d'interception sur le réseau

> **Exemple :** récupération de l'adresse MAC du routeur afin de récupérer les communications



Infox (Fake news): Fausses informations diffusées dans le but de manipuler ou de tromper l'opinion.

Logiciel malveillant ou malware : Programme développé dans le but de nuire à, ou au moyen, d'un système informatique ou d'un réseau. Il peut prendre la forme d'un virus ou d'un vers informatique.

Mail bombing (Bombardement de courriels) : Envoi d'un nombre considérable d'emails (plusieurs milliers par exemple) à un destinataire unique dans une intention malveillante. Il aboutit en général soit à saturer la boite aux lettres de la victime soit à rendre impossible l'utilisation par ce dernier de son adresse électronique.

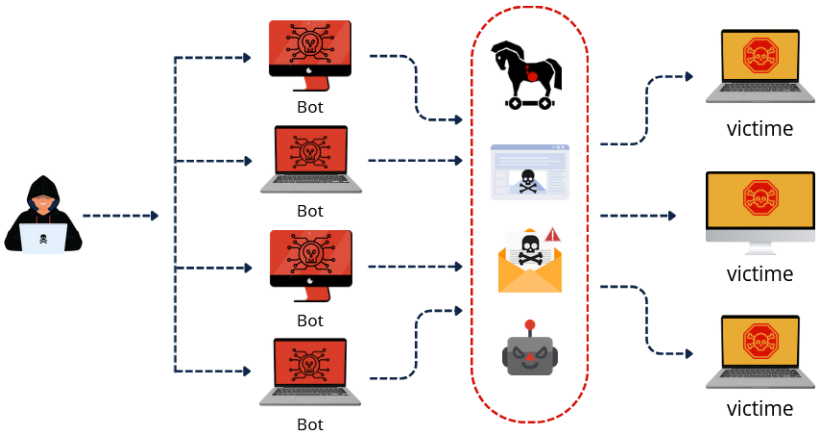
Patch : Morceau de code que l'on ajoute à un logiciel pour remédier à un problème (correction d'un bug par exemple).

Piratage de compte : Accès à un compte (bancaire, administrateur, profil sur les réseaux sociaux, etc.) après avoir « *cracker* » le mot de passe le protégeant.

Phishing (hameçonnage) : Vol d'identité ou d'informations confidentielles (codes d'accès, coordonnées bancaires, etc.) par subterfuge. Les escrocs se font le plus souvent passer pour un organisme de confiance (organisme bancaire, Paypal, etc.) et invitent les usagers, par courrier électronique, à visiter le site frauduleux - qui ressemble au site authentique – et à partager des informations sensibles.

Ransomware (Rançongiciel) : Logiciel malveillant qui prend en otage les données contenues dans un système informatique puisqu'il chiffre et bloque les fichiers contenus sur un ordinateur et n'envoie la clé permettant le déchiffrement que lorsque l'utilisateur a payé une rançon.

Réseau de machines zombies ou botnet : Réseau de machines infectées et contrôlées par un pirate à distance. Ce dernier peut alors transmettre des ordres aux machines du botnet et les actionner à sa guise.



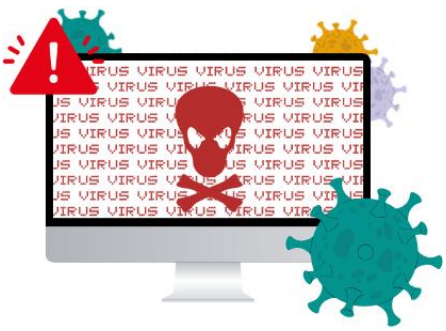
Scan : Pratique frauduleuse, le plus souvent originaire d'Afrique de l'Ouest et notamment du Nigéria, qui consiste à extorquer de l'argent à des internautes en leur faisant miroiter une somme d'argent.

> **Exemple :** e-mail émanant d'un soi-disant riche héritier africain qui se trouve dans une situation de détresse ou d'urgence prétextant un compte en banque bloqué. Si l'internaute accepte de l'aider à récupérer son argent, il lui promet alors en échange de créditer son compte d'une somme faramineuse.

Spamming : Envoi massif de messages électroniques non souhaités dans un but promotionnel ou publicitaire à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact mais dont il a récupéré les informations de façon irrégulière.

Usurpation de compte : Forme de vol d'identité où des pirates accèdent à un compte, une application ou encore un service en ligne en se faisant passer pour une personne après avoir réussi à subtiliser les identifiants de cette dernière.

Virus informatique : Programme ou morceau de programme malveillant qui s'attache à un fichier légitime dans l'espoir que l'utilisateur ou le système l'exécute, afin de lui permettre de se propager dans un système informatique (ordinateur, serveur, appareil mobile, etc.) et souvent d'en atteindre les données, la mémoire et/ou le réseau.



La propagation d'une machine à une autre se fait par échange de fichiers infectés par le biais d'une messagerie, de portes dérobées, d'une page Internet frauduleuse, de clés USB, d'un partage de fichiers, etc.

Ver informatique : Virus qui se propage de manière quasi autonome (sans intervention humaine directe) via le réseau. Il utilise une faille dans le système pour se copier là où il ne devrait pas pour ensuite propager son code, à l'insu des utilisateurs, au plus grand nombre de cibles et infecter le réseau (récupération du carnet d'adresses, envoi de copies…).

Vishing : Issue de la contraction de *« voice* » (voix) et « *phishing* », cette arnaque par appel téléphonique ou message vocal a pour objectif d'obtenir les données bancaires ou personnelles de la victime, en se faisant passer pour une source fiable.

> **Exemple :** les appels provenant d'un numéro affichant le nom d'une banque ou d'un service visant à obtenir les codes d'autorisation pour effectuer un virement