ISBN 978-0-660-45951-6
CAT D96-9/2022F-PDF

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Introduction à l'**environnement** de **cybermenace**

2023
2024

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Centre de la sécurité des télécommunications
1929, chemin Ogilvie
Ottawa (Ontario) K1J 8K6
cse-cst.gc.ca

ISBN 978-0-660-45951-6
CAT D96-9/2022F-PDF

À propos du présent document

Le présent document décrit les concepts pertinents aux discussions relatives aux activités de cybermenace dans le contexte canadien et sert de point de référence aux publications du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Il transmet des connaissances de base sur l'environnement de cybermenace, notamment sur les auteurs de cybermenace et leurs motivations, le degré de sophistication, les techniques, les outils et l'exposition aux cybermenaces.

Prière de consulter le glossaire du Centre pour la cybersécurité[1] pour trouver des termes additionnels, ainsi que sa page de conseils[2] pour de plus amples discussions sur l'environnement de cybermenace.

[1] https://cyber.gc.ca/fr/glossaire
[2] https://cyber.gc.ca/fr/orientation

Cybermenace

Une **cybermenace** est une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient, ou à perturber le monde numérique en général.

Par **environnement de cybermenace**, on entend l'espace virtuel où les auteurs de cybermenace mènent des activités malveillantes. Il comprend les réseaux, les dispositifs et les processus qui sont connectés à Internet et qui peuvent être la cible d'auteurs de cybermenace, ainsi que les méthodes utilisées par ces auteurs pour atteindre les systèmes.

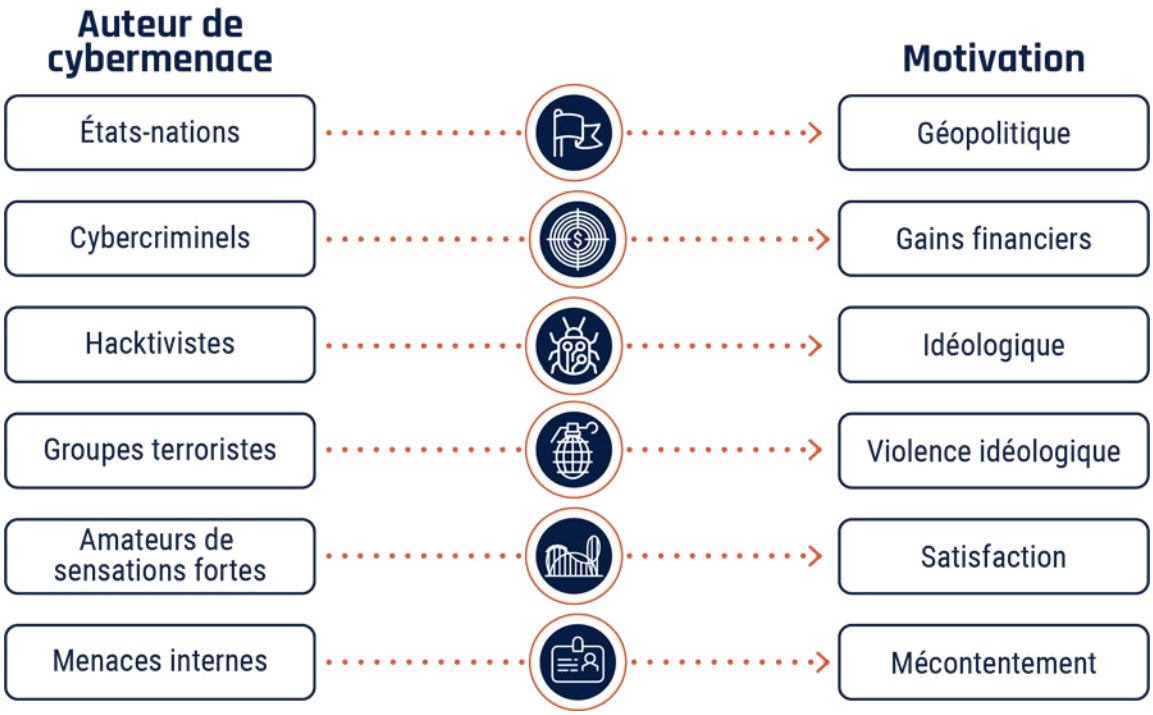
Auteurs de cybermenace

Les **auteurs de cybermenace** sont des groupes ou des personnes qui, dans un but malveillant, cherchent à exploiter les lacunes dans un système d'information, ou à tirer avantage des exploitants de ce système pour obtenir un accès non autorisé ou encore porter préjudice aux données, aux dispositifs, aux systèmes et aux réseaux des victimes, y compris l'authenticité de l'information vers ces systèmes et en provenance de ceux-ci. L'universalisation d'Internet fait en sorte que les auteurs de menace peuvent se trouver n'importe où dans le monde et toujours compromettre la sécurité des systèmes d'information au Canada.

Types d'auteurs de cybermenace et leurs motivations

On peut catégoriser les auteurs de cybermenace selon leur motivation et, dans une certaine mesure, selon leur degré de sophistication sur le plan technique. Les auteurs de menace cherchent à obtenir l'accès aux dispositifs et aux réseaux pour différentes raisons, par exemple, pour le siphonnement de la puissance de traitement, l'exfiltration ou la manipulation de l'information, la dégradation du rendement d'un réseau et l'extorsion à l'endroit du propriétaire. Certains auteurs de menace mènent des activités de cybermenace contre des personnes ou des organisations précises, alors que d'autres agissent de façon opportuniste pour cibler des systèmes vulnérables. Or, chaque catégorie d'auteurs de cybermenace est animée par une motivation principale.

Figure 1 : Auteurs de cybermenace



Degré de sophistication sur le plan technique

Les auteurs de cybermenace n'ont pas les mêmes capacités et le même degré de sophistication sur le plan technique. Ils tirent parti d'un large éventail de ressources, de formations et de soutien pour mener leurs activités. Ils peuvent agir seuls ou faire partie d'une organisation plus large (p. ex. le programme de renseignement d'un État-nation ou un groupe du crime organisé). Les auteurs de menace disposant de moyens sophistiqués ont parfois recours à des outils et à des techniques facilement accessibles parce que ceux-ci sont quand même efficaces pour une tâche donnée ou qu'ils rendent le processus d'attribution d'une activité plus difficile, par exemple, en tirant parti des outils de sécurité commerciaux utilisés par les chercheurs en sécurité.

Les **auteurs de menaces persistantes avancées (MPA)** sont des auteurs de cybermenace utilisant des méthodes grandement sophistiquées et possédant un niveau de compétence très élevé. Ils sont en mesure d'utiliser des techniques avancées pour mener des campagnes complexes et prolongées afin de réaliser leurs objectifs stratégiques. Cette dénomination est généralement réservée à des États-nations et à des groupes du crime organisé très compétents.

Les **auteurs de cybermenace parrainés par des États** travaillent pour le compte d'un État-nation précis et ont recours à des activités de cybermenace principalement pour mener à bien leurs objectifs géopolitiques. Ils possèdent souvent les moyens les plus sophistiqués en raison des ressources et du personnel à leur disposition, et des efforts de planification et de coordination qu'ils peuvent déployer. Les États-nations qui n'ont pas développé de cyberprogrammes peuvent avoir recours à des cyberoutils commerciaux et à un bassin mondial de talents en pleine croissance pour assurer la mise en œuvre d'activités de cybermenace sophistiquées. Certains États-nations entretiennent également des relations opérationnelles avec des membres du crime organisé.

Parmi les activités des auteurs de cybermenace parrainés par des États, notons l'espionnage contre des gouvernements, des organisations et des personnes; le prépositionnement dans les systèmes essentiels ou la perturbation de ceux-ci; ou l'établissement de réseaux d'appareils compromis pour permettre de poursuivre les activités de cybermenace. Les auteurs de cybermenace parrainés par des États peuvent aussi se livrer à des activités motivées par l'appât du gain.

Les **cybercriminels** sont principalement motivés par le gain financier et le degré de sophistication de leurs méthodes varie beaucoup. Les groupes du crime organisé peuvent souvent disposer de fonctions de planification et de soutien, ainsi que de capacités techniques spécialisées susceptibles de faire de nombreuses victimes. Les marchés en ligne servant à la vente d'outils et de services illicites ont rendu la cybercriminalité plus accessible et ont permis aux cybercriminels de mener des activités plus complexes et sophistiquées.

Les activités de cybermenace des **hacktivistes** sont motivées par des considérations idéologiques et sont généralement moins sophistiquées que celles d'auteurs de cybermenace parrainés par des États ou de groupes du crime organisé. Ces auteurs, tout comme les **groupes terroristes** et les **amateurs de sensations fortes**, ont souvent recours à des outils accessibles à grande échelle qu'il est facile de déployer avec des compétences techniques limitées. Bien que leurs actions n'aient souvent aucune conséquence durable sur leurs cibles, abstraction faite du tort causé à leur réputation, ces auteurs sont parvenus, par le passé, à infliger des dommages physiques et financiers à leurs cibles.

Les **menaces internes** proviennent des personnes qui travaillent dans l'organisation. Elles sont particulièrement dommageables puisque ces personnes ont accès aux réseaux internes qui sont protégés par des périmètres de sécurité. Les menaces internes peuvent être associées à l'un des types d'auteurs de menace mentionnés précédemment et peuvent également inclure des employés mécontents.

CYBEROUTILS COMMERCIAUX

Les fournisseurs commerciaux vendent des outils et des services qui permettent aux clients d'installer des maliciels, d'intercepter des communications et de voler de l'information provenant d'appareils ciblés. Les cyberoutils commerciaux sont souvent présentés à titre d'outils destinés aux services de police, mais ce ne sont pas tous les fournisseurs qui font preuve de discernement quant aux acheteurs de leurs produits. Les auteurs de cybermenace peuvent tirer parti des cyberoutils commerciaux pour accroître la sophistication de leurs activités de menace.

Exposition aux cybermenaces

L**'exposition aux cybermenaces** fait référence à tous les services et systèmes d'information qu'un auteur de cybermenace peut exploiter en tentant de compromettre une personne, une organisation ou un réseau. Elle comprend tous les terminaux exposés à Internet, y compris les réseaux, les ordinateurs personnels, les appareils mobiles, les dispositifs de l'Internet des objets (IdO) et les serveurs, en plus des processus qui communiquent avec des systèmes d'information connectés à Internet ou qui dépendent de ceux-ci. L'exposition d'une personne à des menaces repose également sur la quantité de renseignements personnels qui sont partagés avec des services et des fournisseurs en ligne; plus une personne partage ses renseignements personnels et financiers, plus ces renseignements deviennent vulnérables au vol ou à une exposition découlant d'une atteinte à la protection des données. Plus l'exposition aux cybermenaces d'une personne, d'une organisation ou d'un réseau est grande, plus il devient difficile d'assurer sa sécurité.

Le nombre de terminaux connectés à Internet augmente de façon importante chaque année, ce qui s'explique en grande partie par le déploiement de dispositifs qui composent l'IdO et l'Internet industriel des objets (IIoT pour *Industrial IoT*).[3] Des dispositifs grand public et médicaux connectés, comme les systèmes de sécurité à domicile, les voitures et les stimulateurs cardiaques, sont de plus en plus courants, tout comme les technologies opérationnelles (TO) connectées, qui consistent en du matériel et des logiciels intégrés dans les dispositifs servant à détecter ou à provoquer un changement dans le monde physique.

Des services, des dispositifs et des données peuvent tous être ciblés par des auteurs de cybermenace pour obtenir l'accès initial à un environnement. Les chaînes d'approvisionnement comprennent de plus en plus le transfert de renseignements numériques en plus du transport des marchandises. Depuis 2020, un nombre accru d'organisations ont adopté des technologies comme des logiciels infonuagiques, une infrastructure infonuagique et des produits de type plateforme-service pour augmenter leur efficacité dans un environnement de travail hybride où certains employés travaillent de la maison alors que d'autres travaillent sur place. Les accords de services gérés comprennent souvent pour les fournisseurs un niveau d'accès élevé aux réseaux de leurs clients. La confiance et le flux d'information entre les organisations procurent aux auteurs de menace les moyens nécessaires pour compromettre les cibles, en compromettant d'abord une tierce partie.

Figure 2 : Terminaux

Un terminal est un appareil connecté à un réseau, ce qui comprend, entre autres, les ordinateurs personnels, les appareils mobiles, les dispositifs IdO et les serveurs.

[3] https://www.statista.com/topics/2637/internet-of-things/#dossierKeyfigures

Cibles, répercussions et activités de cybermenace

Cibles des activités de cybermenace

Les auteurs de cybermenace peuvent mener des activités malveillantes contre tout ce qui peut être connecté à Internet ou s'y trouver, y compris des dispositifs, de l'information, des ressources financières, des opinions et des réputations :

- Les **dispositifs** impliquent des technologies connectées. Il peut s'agir de téléphones cellulaires ou d'ordinateurs, de serveurs et de technologies opérationnelles qui contrôlent les processus industriels. Une fois compromis, ces dispositifs peuvent servir à faciliter des activités de cybermenace.
- Le terme **information** fait référence à la propriété intellectuelle, à d'autres renseignements commerciaux sensibles et à des renseignements personnels. Elle peut également comprendre des renseignements financiers importants comme des détails ou des identifiants bancaires.
- Les **ressources financières** comprennent des actifs tels que des devises numériques et des actifs numériques, notamment la cryptomonnaie. Les auteurs de cybermenace ciblent souvent des Canadiens en ayant recours à la fraude et à des escroqueries visant à convaincre les victimes d'envoyer de l'argent à un auteur de menace pour éviter des sanctions ou pour recevoir une récompense fictive. Les activités de cybermenace visant les institutions financières et les systèmes financiers peuvent être menées dans le but de voler des sommes beaucoup plus importantes.
- Il est possible, par des activités d'influence en ligne, d'influencer des **opinions** et de nuire à la **réputation**. Ces activités font appel à de la mésinformation, à de la désinformation ou à de la malinformation. Les auteurs de menace peuvent cibler des personnes ou un discours social plus général en influençant des événements précis comme des élections ou en menant des campagnes d'influence constante pour exposer des faits favorables à leurs objectifs géopolitiques.

Répercussions des activités de cybermenace

Répercussions sur la vie privée des Canadiens

Les Canadiens mettent considérablement des renseignements personnels sur Internet et dépendent de dispositifs connectés à Internet pour les communications, les finances, le divertissement, le confort et la sécurité. Lorsque ces renseignements se retrouvent en ligne, ils deviennent vulnérables aux actions des auteurs de cybermenace. Ces auteurs volent également des renseignements financiers et médicaux, ainsi que d'autres renseignements personnels qu'ils vendent en ligne ou utilisent dans le cadre de cybercrimes. Les importantes atteintes à la protection des données qui touchent les entreprises ont de graves répercussions sur leurs clients. Ces atteintes révèlent des renseignements personnels pouvant servir à d'éventuels crimes.

Répercussions sur la sécurité financière des Canadiens

Lorsque des auteurs de menace obtiennent les identifiants de connexion des Canadiens, les détails relatifs à leurs cartes de crédit et d'autres renseignements personnels, ils se servent de ces renseignements pour voler de l'argent, commettre une fraude ou les vendre sur les marchés de la cybercriminalité. Ces criminels ciblent également les systèmes de point de vente (PDV) utilisés par les entreprises en installant des maliciels afin de voler l'information des clients, de nuire aux activités de l'entreprise, d'effectuer des achats frauduleux, de manipuler les prix et de provoquer d'autres formes de perturbation.

Les Canadiens sont ciblés par des fraudes en ligne. Les auteurs de cybermenace rendent les escroqueries pertinentes et attrayantes en associant leurs cyberfraudes à des événements d'actualité. Les élections, la période des impôts et les nouvelles qui font l'actualité ont toutes servi de toile de fond pour la cybercriminalité.

Répercussions sur la santé économique du Canada

Les activités de cybermenace entraînent des dépenses imprévues pour les organisations, dont des montants attribués à des rançons ou des fonds volés, des pertes en raison de l'interruption des opérations, des coûts nécessaires pour assurer la sécurité des réseaux, l'atteinte à la réputation et la perte de clients qui en découle, et sans oublier le vol de propriété intellectuelle et de renseignements sensibles.

Ces coûts sont un fardeau sur les ressources limitées des organisations et ils diminuent leur compétitivité. Ils sont en fait un fardeau sur l'ensemble de l'économie canadienne.

Les auteurs de cybermenace ciblent les entreprises canadiennes afin de voler de précieux renseignements commerciaux. Le vol de ces renseignements peut entraîner des conséquences financières à court et à long terme pour les victimes, notamment des impacts sur la compétitivité à l'échelle internationale et sur la réputation des victimes.

Répercussions sur la confiance des Canadiens

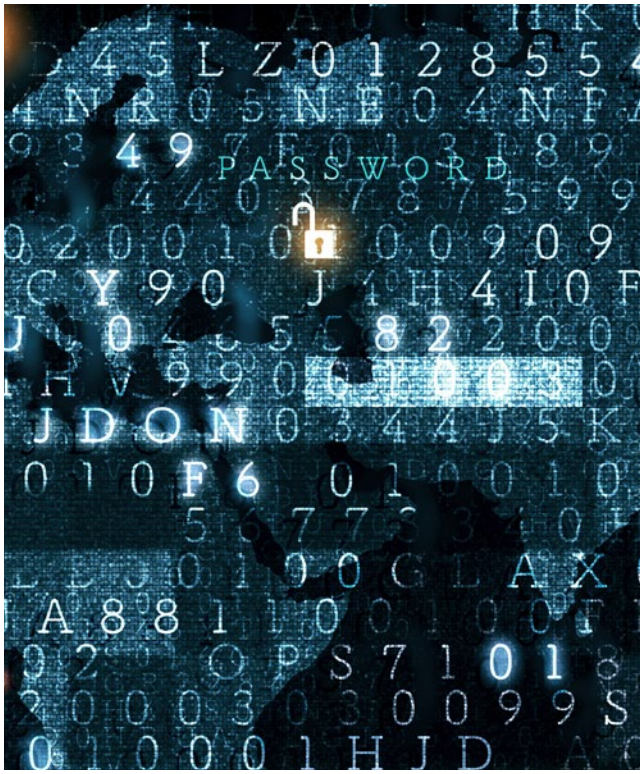
En diffusant de l'information trompeuse et potentiellement nuisible, les auteurs de cybermenace polluent l'espace d'information en ligne, ce qui rend difficile pour les Canadiens de séparer la vérité des mensonges. Une telle situation peut influencer le discours civil, les choix des décideurs politiques et avoir une répercussion sur la réputation des politiciens et des dirigeants.

Les auteurs de cybermenace exploitent les relations de confiance entre les organisations en ciblant les systèmes de paiement en ligne et en personne ou les vulnérabilités de la chaîne d'approvisionnement, ou encore en tirant profit de l'accès privilégié que détiennent les fournisseurs de services gérés (les entreprises qui fournissent des services de technologies de l'information [TI] et qui assurent la maintenance des réseaux de leurs clients.)

Répercussions sur la sécurité des Canadiens

Lorsque les auteurs de cybermenace ciblent des processus physiques d'une industrie ou des services essentiels connectés à Internet, comme ceux que l'on retrouve dans les secteurs des soins de santé et des transports, des perturbations peuvent provoquer des répercussions sur la sécurité des Canadiens. Pour ce qui est des particuliers, les activités de cybermenace visant des dispositifs IdO domestiques et personnels, y compris des dispositifs médicaux comme des stimulateurs cardiaques, risquent d'avoir des répercussions sur la sécurité physique.

Des harceleurs et des partenaires violents peuvent tirer avantage des vulnérabilités des dispositifs IdO personnels pour voler les renseignements recueillis par les moniteurs d'activité physique et les technologies intelligentes dans une maison afin d'identifier et de localiser les victimes ou de contrôler ouvertement leurs dispositifs dans le but de les intimider.



Façon de procéder des auteurs de cybermenace

Les auteurs de cybermenace poursuivent leurs objectifs en exploitant les vulnérabilités techniques, en ayant recours au piratage psychologique, et en créant, en diffusant ou en amplifiant un contenu en ligne erroné ou trompeur pour influencer le comportement et les croyances de certaines personnes.

L'**exploitation de vulnérabilités** consiste à profiter des lacunes ou des défauts dans la conception, la mise en œuvre, l'exploitation ou la gestion d'un système TI, d'un dispositif ou d'un service, collectivement appelées les **vulnérabilités**. Les auteurs de menace utilisent des exploits pour tirer parti des vulnérabilités et déployer des charges de virus qui leur permettent d'accéder à une activité malveillante sur le système d'une victime, de la contrôler, de la détruire ou de l'utiliser pour faciliter d'autres activités malveillantes. Ils peuvent avoir recours à des outils qui exploitent directement des vulnérabilités techniques précises, tandis que les auteurs dotés de moyens sophistiqués peuvent investir dans des ressources pouvant les aider à découvrir de nouvelles vulnérabilités, jusqu'à présent inconnues; c'est ce que l'on appelle le **jour zéro**, dans les systèmes cibles. Alors que les vulnérabilités du jour zéro ne sont pas connues des propriétaires de systèmes TI ou de logiciels, les auteurs de cybermenace ciblent également des vulnérabilités connues, tirant ainsi avantage des protocoles de sécurité faibles et des systèmes non corrigés.

Le **piratage psychologique** consiste à exploiter la confiance des gens qui utilisent les TI. Cette exploitation se fait en se basant sur des caractéristiques propres aux humains comme l'insouciance et la confiance. Les auteurs de menace ont recours au piratage psychologique pour inciter des gens à communiquer de l'information sensible ou à autoriser accidentellement l'accès à un système, à un réseau ou à un dispositif. Le piratage psychologique est aujourd'hui une tactique très répandue dans le cadre des activités de cybermenace. La compromission de courriel d'affaires (BEC pour *business email compromise*), ou fraude du faux PDG, est l'une des fraudes liées au piratage psychologique les plus courantes et coûteuses. Lors d'une telle fraude, les auteurs de menace se font passer pour des cadres supérieurs ou des tiers de confiance pour inciter les victimes à transférer directement des fonds. Le piratage psychologique est aussi souvent utilisé conjointement avec l'exploitation de vulnérabilités. Par exemple, les auteurs de menace créent des courriels d'hameçonnage et de harponnage contenant des liens ou des fichiers malveillants. Lorsque les victimes cliquent sur ces liens ou fichiers, des exploits sont activés qui permettent à l'auteur de menace d'accéder au système de la victime.

Les auteurs de cybermenace étrangers peuvent également manipuler les médias sociaux, la publicité légitime et les outils d'échange d'information pour mener des campagnes d'**influence étrangère en ligne** en vue d'affecter de façon générale des événements à l'échelle nationale comme des élections, un recensement ou des campagnes de santé publique, ainsi que des débats publics. L'influence étrangère en ligne se produit lorsque des auteurs de cybermenace étrangers parviennent secrètement à créer, à diffuser ou à amplifier la mésinformation, la désinformation ou la malinformation pour influencer les croyances ou les comportements de citoyens d'un autre pays. Ils tirent avantage de leur compréhension du fonctionnement des médias traditionnels et des médias sociaux – et de la façon dont les personnes consomment l'information – pour diffuser leur message à un vaste auditoire, et à un coût relativement bas. Ils peuvent y parvenir en se faisant passer pour des fournisseurs d'information légitimes, en piratant des comptes dans les médias sociaux ou en créant des sites Web et de nouveaux comptes. Les auteurs de menace peuvent également tirer parti de la technologie pour créer un contenu synthétique comportant du texte, des images ou des vidéos et ainsi promouvoir leurs messages ou provoquer des perturbations.

Identification des activités de cybermenace

Par **attribution**, on entend l'action de déterminer avec précision qui est l'auteur de menace responsable d'un ensemble particulier d'activités. L'attribution d'une activité à un auteur de cybermenace est importante pour plusieurs raisons, notamment pour assurer la défense d'un réseau, appliquer la loi, prendre des mesures dissuasives et préserver des relations extérieures. Or, cette attribution peut s'avérer difficile puisque de nombreux auteurs de cybermenace ont recours à l'obscurcissement pour éviter que des activités ne leur soient attribuées.

Par **obscurcissement**, on entend les outils et les moyens que les auteurs de menace utilisent pour dissimuler leur identité, leurs objectifs, leurs techniques et même leurs victimes. Pour éviter de laisser aux responsables de la sécurité des indices susceptibles de les aider à attribuer l'activité, les auteurs de menace emploient des outils et des techniques facilement accessibles ou des outils qui permettent de transmettre secrètement l'information sur Internet.

Les auteurs de menace sophistiqués peuvent également mener des **opérations sous faux pavillon**. Cette technique consiste à imiter les activités connues d'autres auteurs de menace dans l'espoir que les responsables de la sécurité attribuent faussement l'activité à quelqu'un d'autre. Par exemple, un État-nation pourrait employer un outil utilisé par des cybercriminels ou par d'autres États-nations dans l'espoir qu'une activité leur soit attribuée.

La capacité des auteurs de cybermenace de dissimuler leurs actions dépend du degré de sophistication de leurs méthodes et de leur motivation. En règle générale, les États-nations et les cybercriminels compétents arrivent plus habilement à pratiquer l'obscurcissement que d'autres auteurs de cybermenace.

Annexe : Glossaire

Vous trouverez ci-dessous une liste non exhaustive des outils et des techniques couramment utilisés par les auteurs de menace. Par souci de simplicité, les éléments sont affichés par ordre alphabétique et non en fonction de leur fréquence ou de leur incidence.

Activité d'influence étrangère en ligne (Online foreign influence activity)

Une **activité d'influence étrangère en ligne** est un instrument courant qui permet à des adversaires de poursuivre leurs principaux intérêts, notamment la sécurité nationale, la prospérité économique et des objectifs idéologiques. Les campagnes d'influence en ligne peuvent tenter d'avoir un impact sur le discours civil, d'influencer les choix des décideurs politiques, d'aggraver la friction dans les sociétés démocratiques ou de nuire à la réputation de personnalités publiques comme les politiciens. Les activités d'influence étrangère en ligne exploitent souvent la mésinformation, la désinformation et la malinformation.

Mésinformation (Misinformation)

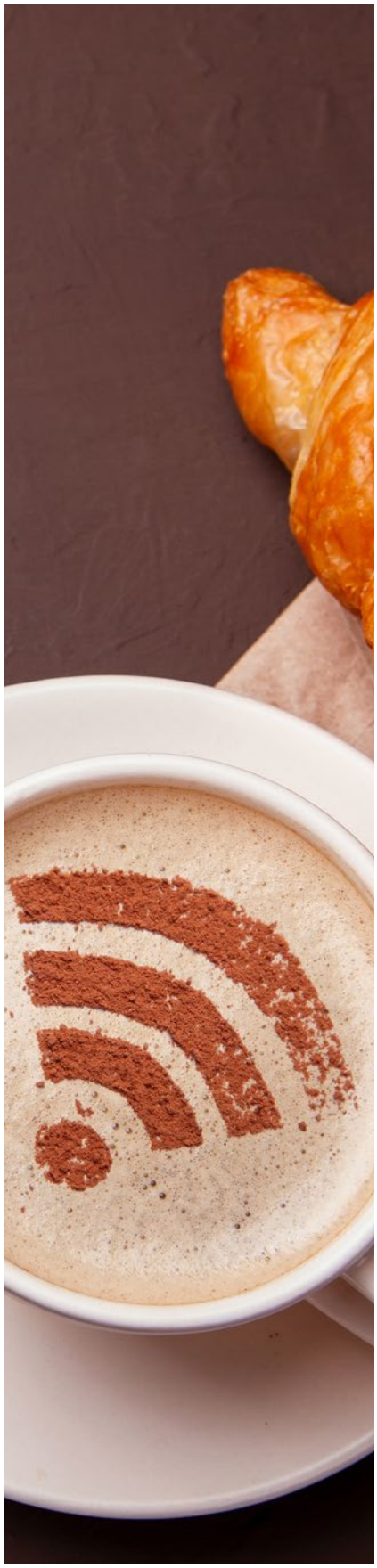
La **mésinformation** désigne le fait de diffuser intentionnellement une fausse information sans avoir de mauvaises intentions.

Désinformation (Disinformation)

Par **désinformation**, on entend le fait de diffuser intentionnellement une fausse information dans le but de manipuler ou de tromper des personnes, des organisations et des États ou bien de leur faire du tort.

Malinformation (Malinformation)

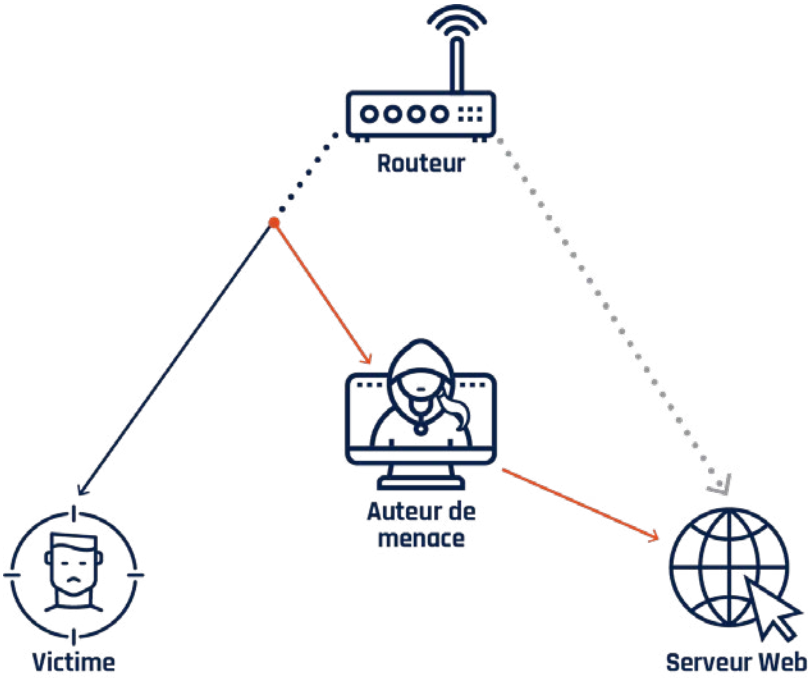
La **malinformation** désigne le fait de diffuser de l'information qui repose sur un fait, mais qui est souvent exagérée de façon à tromper ou même à causer des préjudices.



Attaque de l'intercepteur (Person-in-the-middle attack)

L'**attaque de l'intercepteur** est une technique qui consiste à intercepter les communications entre deux parties, comme un utilisateur et un serveur Web, à l'insu de la victime. Celle-ci croit avoir établi une connexion directe et sécurisée avec un site Web. L'attaque de l'intercepteur permet aux auteurs de menace de surveiller les communications, de réacheminer le trafic, de modifier l'information, d'installer des maliciels et d'obtenir des renseignements nominatifs ou de l'information sensible. Elle peut être réalisée au moyen de diverses techniques : l'hameçonnage, le détournement de domaine, le typosquattage, l'écoute électronique par réseau Wi-Fi et le détournement SSL.

Figure 3 : Attaque de l'intercepteur



Détournement SSL (SSL hijacking)

Le **détournement SSL (*Secure Sockets Layer*)** est une technique par laquelle un auteur de menace intercepte et redirige une connexion non sécurisée entre une victime et un serveur tentant d'établir une connexion sécurisée. La connexion sécurisée est alors fournie par l'auteur de menace plutôt que par le site Web prévu, ce qui lui permet d'intercepter et de compromettre les communications à l'insu de la victime (voir « attaque de l'intercepteur »). Le détournement SSL n'a pas pour objet de porter atteinte à la sécurité fournie par le protocole SSL, mais bien de compromettre la connexion entre les parties non chiffrée et chiffrée de la communication.

Écoute électronique par réseau Wi-Fi (Wi-Fi eavesdropping)

Un auteur de menace utilise l'**écoute électronique par réseau Wi-Fi** pour installer ce qui semble être un point d'accès Wi-Fi légitime dans une zone publique. Les utilisateurs qui se connectent à un tel point d'accès, que l'on appelle souvent un point d'accès malveillant ou indésirable, peuvent alors être victimes d'une attaque de l'intercepteur. Par ailleurs, les auteurs de menace peuvent être en mesure d'intercepter du trafic Web non chiffré sur des réseaux Wi-Fi publics non sécurisés. Une telle activité permet à un auteur de menace de surveiller les communications et d'obtenir des renseignements nominatifs ou de l'information sensible.

Attaque hors sol (Living off the land)

Une **attaque hors sol** se produit lorsqu'un auteur de menace utilise uniquement les outils disponibles par les processus légitimes des systèmes de la victime pour mener à bien une cyberactivité malveillante, plutôt que de déployer un maliciel. Les auteurs de cybermenace se servent d'outils préexistants dans un système pour se fondre dans les opérations normales d'un dispositif ou du réseau de la victime et ainsi éviter d'être détectés.

Cassage de mot de passe (Password cracking)

Le **cassage de mot de passe** fait référence à des techniques qui permettent aux auteurs de cybermenace d'avoir un accès direct à un compte en devinant ou en déchiffrant le mot de passe.

Force brute (Brute force)

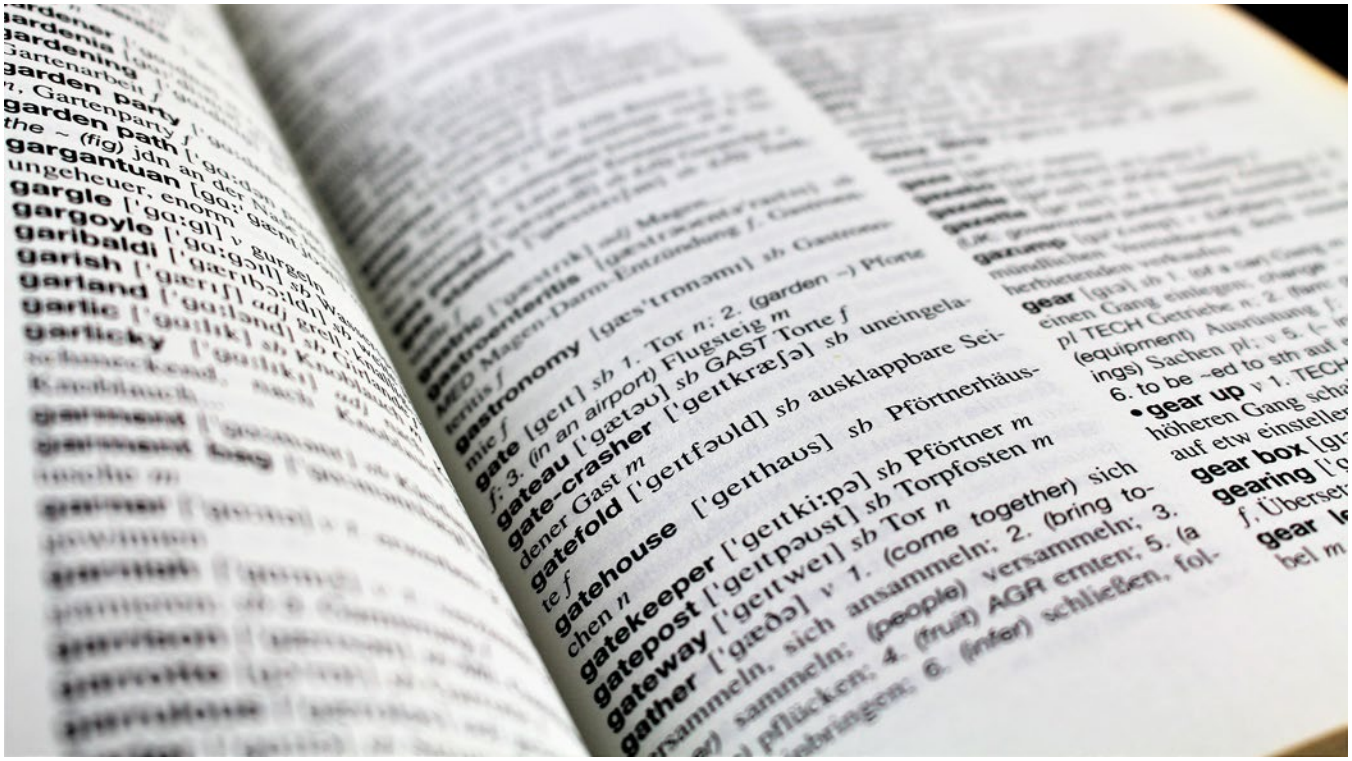
Une attaque par **force brute** consiste à utiliser un nombre exhaustif de mots de passe générés aléatoirement pour tenter de deviner le bon mot de passe et d'accéder au compte. Le cassage de mot de passe par force brute est la méthode la moins efficace, particulièrement dans le cas des mots de passe complexes.

Bourrage d'identifiants (Credential stuffing)

Une **attaque par bourrage d'identifiants** est une manœuvre consistant à utiliser des listes de combinaisons de noms d'utilisateur et de mots de passe compromis afin d'accéder frauduleusement à des comptes en ligne. Les auteurs de cybermenace ont recours à ces listes pour lancer des demandes de connexion automatisées à grande échelle dans l'espoir que l'une des combinaisons corresponde à un compte existant auquel ils pourront avoir accès.

Attaque par dictionnaire (Dictionary attack)

Les **attaques par dictionnaire** mettent à profit des listes exhaustives de mots et de mots de passe fréquemment utilisés, qui comprennent souvent des fautes d'orthographe et diverses permutations qui tiennent compte des exigences en matière de complexité des mots de passe.



Déni de service (Denial of service)

Un **déni de service (DoS pour *Denial of Service*)** désigne une activité visant à rendre un service (p. ex. un site Web, un serveur, un réseau, un dispositif IdO) inutilisable ou à ralentir l'exploitation et les fonctions d'un système.

Attaque par inondation (Flooding attack)

Une **attaque par inondation** est la forme la plus courante de déni de service. Elle se produit lorsqu'un auteur de menace envoie à répétition des demandes de connexion au serveur ciblé, mais qu'il ne parvient pas à établir la connexion. Ces procédures de connexion incomplètes occupent et consomment toutes les ressources disponibles du serveur. Ainsi, le serveur ne parvient plus à traiter ni le trafic ni les demandes de connexion légitimes.

Attaque par arrêt de service (Crash attack)

Les **attaques par arrêt de service** sont moins répandues que les attaques par inondation. Les auteurs de menace s'en servent pour exploiter une vulnérabilité dans le but de provoquer une panne de système pour ainsi en empêcher l'accès.

Déni de service distribué (Distributed denial of service)

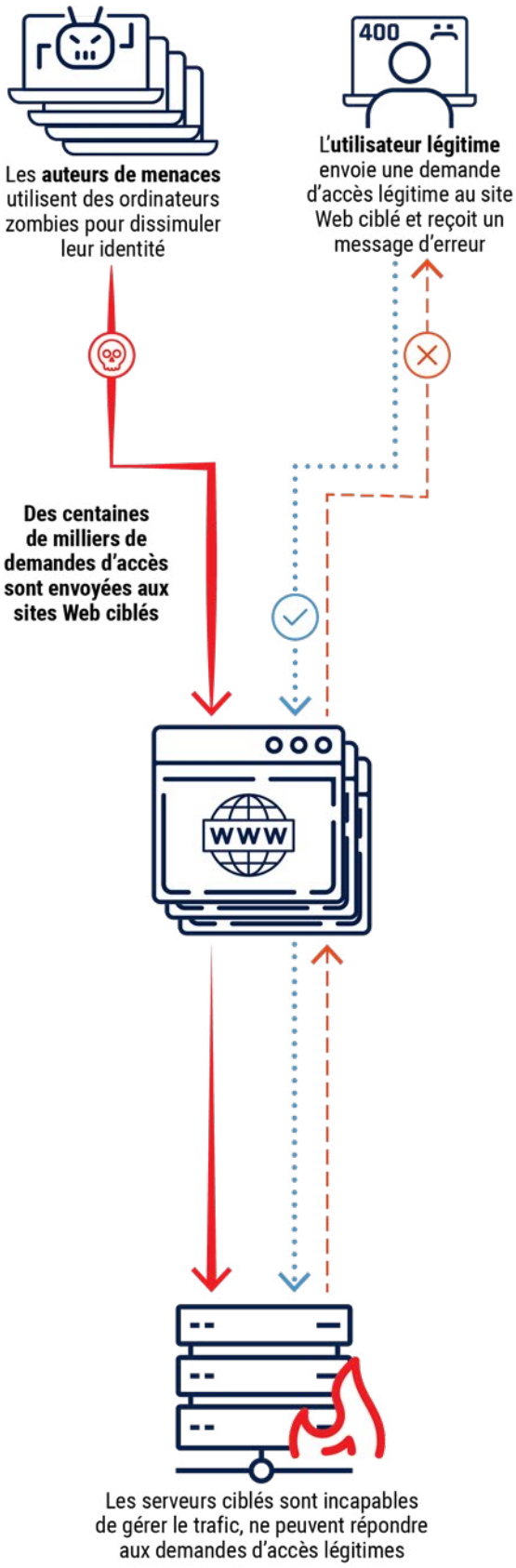
Une **attaque par déni de service distribué (DDoS pour *Distributed Denial of Service*)** est une attaque par déni de service qui provient de plusieurs machines à la fois. Ces machines peuvent être contrôlées par un groupe d'auteurs de menace travaillant ensemble ou faire partie d'un réseau de zombies agissant sous le contrôle d'un seul auteur de menace. Les DDoS sont plus puissants, ce qui complique davantage la tâche d'identification de la véritable source de l'attaque.

Exploit et trousse d'exploit

(Exploit and exploit kit)

Un **exploit** est un code malveillant qui tire avantage d'une vulnérabilité non corrigée. Une **trousse d'exploit** est une collection d'exploits qui ciblent les applications logicielles non sécurisées. Les trousses d'exploit sont adaptées de manière à chercher des vulnérabilités précises et à exécuter l'exploit correspondant à la vulnérabilité relevée. Si un utilisateur visite un site Web hébergeant une trousse d'exploit, celle-ci comparera son référentiel d'exploits aux applications logicielles qui se trouvent sur le dispositif de l'utilisateur et déploiera l'exploit correspondant à la vulnérabilité décelée.

Figure 4 : Déni de service distribué



Injection de code (Code injection)

L'**injection de code** est une technique qui consiste à insérer du code malveillant dans un programme informatique en exploitant une faille dans les instructions d'une fonction du programme ou dans la façon dont ce programme interprète les données saisies. Les deux techniques d'injection de code souvent utilisées sont l'**injection de script intersites (XSS pour *Cross-Site Scripting*)** et l'**injection SQL (*Structured Query Language*)**.

- L'**injection XSS** est une méthode d'injection de code au moyen de laquelle un auteur de menace insère et exécute un programme malveillant dans une application Web en contournant les mécanismes de validation des données saisies. Le programme malveillant est exécuté dans le navigateur des utilisateurs qui accèdent à l'application Web infectée. Le code injecté par XSS peut être une exécution unique ou être utilisé pour permettre une activité malveillante ultérieure.
- L'**injection SQL** récupère ou modifie le contenu d'une base de données SQL en insérant du code dans des formulaires Web destinés à saisir des données dans les bases de données SQL ou à les interroger. Ces bases de données peuvent contenir des renseignements nominatifs ou de l'information sensible.

Exploitation du jour zéro (Zero-day exploit)

Une **vulnérabilité du jour zéro** est une vulnérabilité dont l'existence est inconnue du fournisseur, ce qui signifie que son risque n'a pas été atténué par un correctif. Un **exploit du jour zéro** est une attaque dirigée vers une vulnérabilité du jour zéro. Lorsqu'un correctif a été mis au point, la vulnérabilité n'est plus considérée comme étant du jour zéro.

Exploit sur le Web (Web-based exploit)

Les **exploits sur le Web** visent à compromettre les utilisateurs lorsqu'ils naviguent, ou tentent de naviguer, sur des pages Web précises. Ces exploits fonctionnent en compromettant ou en se faisant passer pour un site Web que les victimes cherchent à visiter. Ce faisant, les victimes subissent elles-mêmes une compromission, ou il y a une exploitation des vulnérabilités du système qui dirigent les utilisateurs à la bonne page Web.

Attaque par téléchargement furtif (Drive-by exploit)

Par **attaque par téléchargement furtif**, on entend le code malveillant qu'un auteur de cybermenace installe sur un site Web à l'insu de l'hôte dans le but de compromettre les dispositifs des utilisateurs qui le consultent.

Détournement de formulaire (Formjacking)

Le **détournement de formulaire** consiste à injecter du code malveillant dans un formulaire de page Web, comme une page de paiement, pour le compromettre et voler les détails relatifs aux cartes de crédit ainsi que d'autres renseignements que les utilisateurs entrent sur ces pages.

Détournement de domaine (Pharming)

Le **détournement de domaine** est une technique qui consiste à rediriger le trafic d'un site Web légitime vers un site malveillant. Pour réaliser cette supercherie, les auteurs de menace modifient les paramètres système de l'utilisateur ou exploitent les vulnérabilités logicielles du serveur du système d'adressage par domaines (DNS pour *Domain Name System*) qui assure la correspondance entre les adresses URL et les adresses IP. Contrairement au typosquattage (voir ci-dessous), une technique qui tire avantage des fautes de frappe de l'utilisateur pour le rediriger vers un site Web illégitime, le détournement de domaine peut rediriger l'utilisateur malgré le fait qu'il ait tapé la bonne adresse URL. Au premier coup d'œil, le site Web illégitime peut sembler légitime, alors qu'il sert en réalité à installer un maliciel et à obtenir des renseignements nominatifs ou de l'information sensible.

Typosquattage (Typo-squatting)

Le **typosquattage** est une technique qui consiste à enregistrer des noms de domaines graphiquement apparentés à une adresse de domaine légitime, mais pouvant facilement être confondus. Cette technique, appelée également détournement d'adresse URL, elle permet aux auteurs de menace de rediriger un utilisateur ayant fait une erreur au moment de saisir l'adresse d'un site Web vers un domaine en apparence similaire sous leur contrôle. Le nouveau domaine peut alors servir à installer un maliciel et à obtenir des renseignements nominatifs ou de l'information sensible. Des techniques d'hameçonnage peuvent également être utilisées pour attirer les utilisateurs vers une adresse URL détournée.

Attaque par embuscade (Watering hole)

Une **attaque par embuscade** consiste à compromettre au moyen d'un exploit un site Web consulté fréquemment par des personnes précises en vue de les infecter.

Maliciel (Malware)

Un **maliciel** (abréviation des mots « malveillant » et « logiciel ») désigne tout logiciel ou code conçu pour infiltrer ou endommager un système informatique. Le terme « charge de virus » fait référence aux actions réalisées par un logiciel malveillant lorsqu'il se trouve dans un système ou dans le réseau d'une victime (p. ex. un rançongiciel qui chiffre des fichiers ou l'installation de portes dérobées qui permettent un accès à distance).

Publiciel (Adware)

Un **publiciel** (abréviation des mots « publicitaire » et « logiciel ») peut infecter un ordinateur lorsqu'il est téléchargé dans le cadre du téléchargement d'un autre programme ou d'une attaque par téléchargement furtif sur le Web. Son objectif principal est de générer des revenus en offrant de la publicité en ligne adaptée. Un logiciel publicitaire basé sur un navigateur et sur une application fait le suivi et la collecte de l'information liée aux utilisateurs et aux dispositifs, dont les données de localisation. Les publiciels peuvent mener à l'exploitation des paramètres de sécurité, des utilisateurs et des systèmes.

Balise (Beacon)

Les **balises** sont des signaux envoyés par un maliciel. Elles tentent de se connecter à l'infrastructure de commande d'un auteur de menace après s'être infiltrées dans l'environnement ciblé. Les balises avisent l'auteur de menace qu'il a réussi à compromettre le système et lui permettent d'envoyer des commandes supplémentaires au maliciel.

Minage clandestin (Cryptojacking)

Le **minage clandestin** permet à un auteur de menace d'exploiter secrètement le dispositif d'une victime (p. ex. un ordinateur, un appareil mobile ou un dispositif IdO) dans le but de miner de la cryptomonnaie sans autorisation. Pour accroître son efficacité (c.-à-d. ses revenus), l'auteur de menace peut faire appel à un réseau de zombies composé de dispositifs compromis. Les logiciels malveillants utilisés à cette fin sont généralement téléchargés lors de la consultation d'un site Web compromis, à l'installation d'une application ou par hameçonnage. Par **cryptominage** ou minage de cryptomonnaie, on entend le processus par lequel des programmes informatiques utilisent la puissance de calcul d'ordinateurs pour générer ou « miner » de la cryptomonnaie, activité pour laquelle le mineur reçoit, pour ses services, une fraction de la cryptomonnaie minée.

Rançongiciel (Ransomware)

Un **rançongiciel** est un programme malveillant qui permet de bloquer l'accès à un ordinateur ou à un dispositif et à son fonctionnement; l'accès au système n'est rendu qu'après le versement d'une rançon. Les auteurs de menace accomplissent cet acte au moyen du chiffrement, mais ils peuvent également avoir recours à diverses méthodes d'extorsion, comme le fait de déployer des attaques DDoS, de menacer des partenaires et des clients ou de menacer de publier des renseignements de nature sensible. Un rançongiciel est généralement installé au moyen d'un cheval de Troie ou d'un ver déployé par hameçonnage ou à la consultation d'un site Web compromis.

Certains cybercriminels se livrent à des campagnes de rançongiciel de type **chasse au gros gibier**. Ils concentrent ainsi leurs activités sur de grandes organisations comme des fournisseurs d'infrastructures essentielles, des gouvernements ou des grandes entreprises, qui doivent éviter que leurs réseaux soient perturbés et qui sont prêts à payer de lourdes rançons pour rétablir rapidement leurs opérations.

Dissimulateur d'activité (Rootkit)

Un **dissimulateur d'activité** est une application malveillante conçue pour fournir à un auteur de menace un accès racine ou administrateur privilégié aux logiciels et aux systèmes qui se trouvent sur le dispositif d'un utilisateur. Un dissimulateur d'activité fournit un accès complet, y compris la capacité de modifier les logiciels utilisés pour détecter les maliciels.

Espiogiciel (Spyware)

Les **espiogiciels** (abréviation des mots « espion » et « logiciel ») sont des logiciels malveillants utilisés pour recueillir et transmettre les activités numériques et les données personnelles de l'utilisateur à son insu et sans sa permission. Ils peuvent être utilisés dans le cadre de plusieurs activités, notamment l'enregistrement de la frappe, l'accès au microphone et à la caméra Web, la surveillance des activités de l'utilisateur et de ses habitudes de navigation, et la capture des noms d'utilisateurs et des mots de passe. Un espiogiciel qui est utilisé pour faciliter la violence, les abus ou le harcèlement de partenaires intimes est appelé **logiciel traqueur.**

Cheval de Troie (Trojan)

Un **cheval de Troie** est un programme malveillant déguisé en logiciel légitime ou qui y est intégré.

Virus (Virus)

Un **virus** est un programme exécutable et reproductible qui insère son propre code dans des programmes légitimes dans le but de causer des dommages sur l'ordinateur hôte (p. ex. en supprimant des fichiers et des programmes ou en corrompant les systèmes d'exploitation et de stockage).

Effaceur (Wiper)

Les **effaceurs** sont des maliciels conçus pour détruire entièrement le disque dur des dispositifs infectés. Les effaceurs peuvent se faire passer pour un rançongiciel en vue de dissimuler l'intention du maliciel et de rendre l'attribution encore plus difficile.

Ver (Worm)

Un **ver** est un programme informatique capable de se reproduire indépendamment par lui-même et de se propager sur d'autres ordinateurs afin de drainer les ressources du système. Tout comme un virus, un ver peut propager un code pouvant endommager son hôte (p. ex. supprimer des fichiers, envoyer des documents par courriel ou saturer la bande passante).

Ordinateur zombie et réseau de zombies (Bots and botnets)

Un **ordinateur zombie**, ou zombie, est un dispositif connecté à Internet (p. ex. un ordinateur, un appareil mobile ou un dispositif IdO) et infecté par un maliciel à l'insu du propriétaire, qu'un auteur de menace peut contrôler à distance afin de mener des opérations illicites. Ensemble, ces dispositifs compromis forment un **réseau de zombies** coordonné par un auteur de menace. Les réseaux de zombies se répandent généralement en sondant l'environnement en ligne dans le but de trouver des dispositifs vulnérables susceptibles d'accroître la puissance informatique et d'ajouter de nouvelles capacités. Ils servent à des fins diverses, telles que pour mener une attaque par déni de service distribué (DDoS pour *Distributed Denial of Service*), propager des rançongiciels et des maliciels, lancer des campagnes publicitaires frauduleuses, envoyer des pourriels, détourner le trafic, voler des données, ou encore pour manipuler, enflammer et censurer les médias sociaux et le contenu de plateformes Web de manière à influencer les débats publics.

Piratage psychologique (Social engineering)

Le **piratage psychologique** est une pratique qui permet d'obtenir de l'information sensible en manipulant des utilisateurs légitimes, souvent par téléphone ou Internet. Les techniques de piratage psychologique visent à convaincre la cible d'envoyer un paiement dans un compte contrôlé par l'auteur de menace ou de recueillir de l'information pour entreprendre d'autres activités de menace.

Hameçonnage (Phishing)

L'**hameçonnage** est une technique courante par laquelle les auteurs de menace se font passer pour une entité fiable dans le but d'inciter un grand nombre de destinataires à fournir de l'information les concernant, comme des justificatifs d'ouverture de session, de l'information bancaire et d'autres renseignements nominatifs. L'hameçonnage est une technique de piratage psychologique qui consiste essentiellement à usurper des courriels et des messages textes. Les utilisateurs tombent dans le piège dès qu'ils ouvrent des pièces jointes malveillantes ou cliquent sur les liens intégrés.

Mystification (Spoofing)

La **mystification** est une technique utilisée pour dissimuler ou falsifier un site Web, une adresse courriel ou un numéro de téléphone de manière à ce qu'il semble provenir d'une source fiable. Après avoir reçu un message d'hameçonnage, la victime peut être invitée à fournir de l'information personnelle, financière ou sensible, ou à cliquer sur un lien ou une pièce jointe, ce qui permettra d'infecter le dispositif en y installant un maliciel.

Harponnage (Spear phishing)

Le **harponnage** est une technique qui consiste à envoyer un message d'hameçonnage personnalisé à un groupe précis de destinataires ou à un seul destinataire. Basée sur le piratage psychologique, cette technique utilise des détails destinés à convaincre la victime que le message provient d'une source digne de confiance. La **chasse à la baleine** est un type de harponnage qui vise les cadres supérieurs et les autres destinataires de grande notoriété disposant d'autorisations et d'accès privilégiés.

Figure 5 : Hameçonnage et harponnage

Compromission de courriel d'affaires (Business email compromise)

La **compromission de courriel d'affaires**, ou fraude du faux PDG, est l'une des fraudes liées au piratage psychologique les plus courantes et coûteuses qui cible les organisations. Elle implique des courriels conçus pour convaincre un employé d'une entreprise ciblée de transférer directement des fonds aux auteurs de cybermenace. Pour ce faire, les auteurs se font passer pour des cadres supérieurs ou des tiers de confiance.

Porte dérobée (Backdoor)

Une **porte dérobée** est un point d'entrée dans le système ou l'ordinateur d'un utilisateur, qui permet de contourner contrôles d'accès et mesures d'authentification habituels. Les auteurs de menace qui disposent d'un tel accès à distance peuvent voler l'information, installer des maliciels ou contrôler les processus et procédures du dispositif. Les portes dérobées peuvent être le résultat d'un maliciel ou d'une autre cyberactivité malveillante, mais elles sont aussi souvent créées délibérément et sans intention de nuire, aux fins de dépannage, de mise à jour logicielle ou de maintenance système. Les auteurs de menace peuvent utiliser ces portes dérobées légitimes à des fins malveillantes.

Reconnaissance (Reconnaissance)

Reconnaissance, ou **recon**, désigne les activités menées par un auteur de menace pour lui permettre d'obtenir des renseignements et d'identifier des vulnérabilités dans le but de faciliter d'éventuelles compromissions. Les auteurs de menace opportunistes peuvent scruter Internet à la recherche d'hôtes ayant des vulnérabilités non sécurisées et les cibler. Lorsqu'une cible est sélectionnée, l'auteur peut mener des recherches supplémentaires sur celle-ci, dont des recherches de source ouverte sur l'entreprise, les employés ou l'infrastructure. Parmi les techniques plus directes, notons l'accès à la cible au moyen de trafic Internet malveillant ou en utilisant le piratage psychologique pour soutirer des renseignements.