# Tous les types de malwares

Définition malware: Un malware est un logiciel malveillant conçu pour causer des dommages à un ordinateur, un réseau ou un système d'information. Les malwares peuvent être utilisés pour voler des informations confidentielles, détruire des fichiers, prendre le contrôle d'un système à distance ou pour lancer des attaques contre des sites Web ou des réseaux.

[source](https://www.mcafee.com/fr-fr/antivirus/malware.html)

## Virus

Un virus se présente généralement sous la forme d'une pièce jointe à un e-mail contenant une charge utile de virus, en d'autres termes la partie du logiciel malveillant qui exécute l'action malveillante. Une fois que la victime a ouvert le fichier, l'équipement est infecté.

## Logiciel rançonneur (ransomware)

Le ransomware est l'un des types de logiciel malveillant les plus rentables, et donc l'un des plus populaires pour les cybercriminels. Ce logiciel malveillant s'installe lui-même sur l'ordinateur d'une victime, chiffre ses fichiers, puis demande une rançon (généralement en Bitcoins) pour restituer ces données à l'utilisateur.

## Faux logiciel de sécurité (scareware)

Les cybercriminels ont recours à des tactiques fondées sur la peur en faisant croire à des victimes que leur ordinateur ou smartphone a été infecté pour les convaincre d'acheter une application factice. Lors d'une escroquerie au scareware, un message alarmant peut s'afficher lors de la navigation sur le Web, typiquement « Avertissement : votre ordinateur est infecté ! » ou encore « Vous avez un virus ! ». Les cybercriminels se servent de ces programmes et de pratiques publicitaires déloyales pour effrayer les utilisateurs et les inciter à acheter des applications non autorisées.

## Ver

Les vers sont capables de se dupliquer d'un ordinateur à l'autre, généralement en exploitant une faille de sécurité dans un logiciel ou un système d'exploitation et n'ont pas besoin de l'intervention de l'utilisateur pour fonctionner. Contrairement au virus, il n’a pas besoin d’une application pour fonctionner, il est indépendant.

## Logiciel espion (spyware)

Un logiciel espion est un programme installé sur votre ordinateur, généralement à votre insu, qui capture et transmet des informations personnelles ou des habitudes et des détails de navigation Internet à son utilisateur. Les logiciels espions permettent aux personnes qui s'en servent de surveiller toutes les formes de communication sur l'équipement ciblé. Les logiciels espions sont souvent utilisés par les forces de l'ordre, les agences gouvernementales et les organisations de sécurité de l'information pour tester et surveiller les communications au sein d'un environnement sensible ou lors d'une enquête. Cependant, les logiciels espions sont également mis à la disposition des consommateurs, permettant aux personnes qui en font l'acquisition d'espionner leur conjoint, leurs enfants ou leurs employés.

## Cheval de Troie

[src](https://www.kaspersky.fr/resource-center/threats/zeus-trojan-malware)

Les chevaux de Troie se font passer pour des applications inoffensives, incitant les utilisateurs à les télécharger et à les utiliser. Une fois opérationnels, ils peuvent alors voler des données personnelles, bloquer un équipement, espionner les activités de l'utilisateur, ou même lancer une attaque. Souvent orienté sur un seul type d’OS.

## Logiciel publicitaire

Les programmes de logiciels publicitaires diffusent des publicités indésirables auprès des utilisateurs et affichent généralement des publicités clignotantes ou des fenêtres contextuelles lorsque vous effectuez une certaine action. Les logiciels publicitaires sont souvent installés en échange d'un autre service, comme par exemple le droit d'utiliser un programme sans le payer.

## Logiciel malveillant sans fichier

Un logiciel malveillant sans fichier est un type de logiciel malveillant qui utilise des programmes légitimes pour infecter un ordinateur. Les attaques de logiciels malveillants sans fichier visant le Registre ne laissent ni fichier de logiciel malveillant à analyser ni processus malveillant à détecter. Un logiciel malveillant sans fichier ne repose pas sur des fichiers et ne laisse aucune empreinte, ce qui le rend difficile à détecter et à supprimer.

## Logiciels espions

Les logiciels espions sont des programmes qui collectent des informations sur l'utilisateur à son insu, comme les mots de passe ou les habitudes de navigation sur le Web.

## Botnets

Les botnets sont des réseaux d'ordinateurs infectés par des logiciels malveillants et contrôlés à distance par un attaquant. Ils peuvent être utilisés pour lancer des attaques DDoS ou pour effectuer des activités illégales.

## Rootkits

Les rootkits sont des programmes malveillants qui se cachent dans le système d'exploitation et sont souvent très difficiles à détecter. Ils peuvent être utilisés pour accéder à distance au système de l'utilisateur ou pour exécuter des programmes malveillants.

## Backdoors

Les backdoors sont des portes dérobées laissées ouvertes par les développeurs de logiciels, qui peuvent être utilisées par des attaquants pour accéder au système de l'utilisateur à son insu.

# Symptôme commun des malwares

[src](https://www.kaspersky.fr/blog/les-10-symptomes-dune-infection-malware/1437/#:~:text=Un%20mauvais%20fonctionnement%20de%20vos,que%20vous%20%C3%AAtes%20victimes%20d)

Des bugs inattendus

Votre système est lent ...

Un disque dur anormalement actif ...

Des fenêtres étranges ...

D'étranges avertissements ...

Un mauvais fonctionnement de vos programmes ...

L'activité de votre réseau sans fil ...

Les e-mails inconstants ...

Des adresses IP blacklistées ...

Une désactivation inattendue de l'anti-virus …

# Les méthodes d’infection de malwares

[src](https://encyclopedia.kaspersky.fr/knowledge/how-malware-penetrates-systems/), [src](https://learn.microsoft.com/fr-fr/security-updates/security/20200343)

## Ingénierie sociale

Les types d’attaques d’ingénierie sociale

Il existe différents types d’attaques d’ingénierie sociale. Il est important de comprendre la définition de l’ingénierie sociale ainsi que le fonctionnement de celle-ci. Une fois que le modus operandi général est défini, il est beaucoup plus facile de reconnaître des attaques d’ingénierie sociale.

### Technique de l’appât

La technique de l’appât consiste à créer un piège, par exemple une clé USB contenant des logiciels malveillants. Lorsque quelqu’un est curieux de voir ce qui se trouve sur la clé, il connecte celle-ci à son lecteur USB, ce qui entraîne la contamination du système. Il existe en fait une clé USB qui permet de détruire les ordinateurs. Une fois insérée, elle se charge avec l’énergie du lecteur USB et la libère sous forme d’une surtension féroce, endommageant ainsi l’appareil dans lequel elle a été insérée. (Une telle clé USB coûte 54 dollars.)

### Prétexte

Cette attaque utilise un prétexte pour attirer l’attention et inciter la victime à fournir des informations. Par exemple, un sondage sur Internet peut sembler tout à fait innocent au début, mais peut ensuite demander les détails d’un compte bancaire. Une personne munie d’un porte-bloc pourrait également se présenter et vous dire qu’elle effectue un contrôle des systèmes internes. Toutefois, il se peut qu’elle ne soit pas la personne qu’elle prétend être et qu’elle cherche à vous voler des informations précieuses.

### Hameçonnage

Les attaques d’hameçonnage utilisent un email ou un message textuel qui prétend provenir d’une source fiable et qui demande des informations. Un exemple bien connu : un email est prétendument envoyé par une banque, qui veut que ses clients confirment leurs informations de sécurité et qui dirige les utilisateurs vers un faux site où leurs informations d’identification seront enregistrées. Le harponnage vise une seule personne au sein d’une entreprise. Cette pratique consiste à envoyer un email censé provenir d’un cadre supérieur de l’entreprise et qui demande des informations confidentielles.

### Quid pro quo

L’expression dit : « échange équitable n’est pas vol ». Toutefois, il s’agit bien d’un vol dans ce cas-ci. De nombreuses attaques d’ingénierie sociale font croire aux victimes qu’elles obtiennent quelque chose en échange des données ou de l’accès qu’elles fournissent. Les « faux logiciels de sécurité » fonctionnent de cette manière. Ils promettent aux utilisateurs une mise à jour pour corriger un problème de sécurité urgent, alors qu’en fait, ce sont les logiciels eux-mêmes qui représentent la menace de sécurité.

### Envoi de spams et piratage de messageries électroniques

Ce type d’attaque implique le piratage des comptes de messageries ou des réseaux sociaux d’une personne pour accéder à ses contacts. Les contacts peuvent recevoir un message indiquant que cette personne a été agressée et qu’elle a perdu toutes ses cartes de crédit. Ensuite, elles seront invitées à effectuer un virement sur un compte de transfert d’argent. Ou encore, une personne qui prétend être un ami peut envoyer une « vidéo à voir obligatoirement » qui redirige vers un logiciel malveillant ou vers un cheval de Troie enregistreur de frappe.

### Exploitation ou chasse

Il faut savoir que certaines attaques d’ingénierie sociale sont beaucoup plus développées. La plupart des stratégies que nous avons décrites sont une forme de « chasse ». En bref, il s’agit d’entrer, de saisir l’information et de sortir.

## Techniques d’installation

Les cybercriminels peuvent utiliser des techniques qui introduisent de manière dissimulée un code malveillant dans un système en exploitant des vulnérabilités dans les fonctionnalités de sécurité du système d’exploitation ainsi que dans ses logiciels. Les vulnérabilités permettent au ver ou au cheval de Troie de pénétrer dans l’ordinateur de la victime et de s’exécuter eux-mêmes.

## Usage simultané des techniques d’installation et des méthodes d’ingénierie sociale

Les cybercriminels utilisent souvent les deux méthodes simultanément : l’ingénierie sociale pour attirer l’attention des potentielles victimes et des moyens techniques afin d’augmenter les probabilités d’infiltration d’un objet infecté dans le système ciblé.

# Type d’attaque

## Man-in-the-middle

[src](https://www.pandasecurity.com/fr/mediacenter/securite/attaque-man-in-the-middle/)

Une attaque de l’homme du milieu (MITM) est un [type de cyberattaque](https://www.pandasecurity.com/fr/mediacenter/securite/types-de-cybercriminalite/) où les attaquants interceptent une conversation ou un transfert de données existant, soit en écoutant, soit en se faisant passer pour un participant légitime. Pour la victime, il semblera qu’un échange standard d’informations est en cours, mais en s’insérant au « milieu » de la conversation ou du transfert de données, l’attaquant peut discrètement détourner des informations.

L’objectif d’une attaque MITM est de récupérer des données confidentielles telles que des détails de compte bancaire, des numéros de carte de crédit ou des informations de connexion, qui peuvent être utilisées pour commettre d’autres crimes comme le vol d’identité ou les transferts de fonds illégaux. Parce que les attaques MITM sont menées en temps réel, elles passent souvent inaperçues jusqu’à ce qu’il soit trop tard.

## Empoisonnement SEO

[src](https://blog.avast.com/fr/seo-poisoning)

Être infecté par un malware, n’implique pas seulement de cliquer sur un fichier. Très souvent, les pirates mettent en place tout un écosystème dans le seul but de vous pousser à cliquer. C’est la technique utilisée lors de l’empoisonnement SEO. Les recherches innocentes que vous menez peuvent vous pousser à cliquer sur des liens infectés.

Tout commence par un pirate qui crée de nombreux faux contenus sur Internet, des contenus qui vont copier ou se servir de la réputation d’un site web authentique. Ces faux contenus contiennent un malware et sont pensés pour arriver en tête des résultats sur les moteurs de recherche. Pour ce faire, les pirates travaillent en duo : l’un pose une question sur un forum, l’autre lui « répond » en postant un lien contenant le malware.

## Man-in-the-mobile

[src](https://securityintelligence.com/man-in-the-mobile-attacks-single-out-android/)

Une fois installé, le logiciel malveillant mobile capture tout le trafic SMS, y compris les codes d'autorisation de transaction envoyés par la banque à la victime, et les transmet aux fraudeurs. Cela permet aux criminels d'initier des transferts frauduleux et de capturer les codes de sécurité nécessaires pour contourner les systèmes d'autorisation hors bande par SMS utilisés par de nombreuses banques européennes.

# WIFI

[Définition](https://www.netspotapp.com/fr/blog/all-about-wifi/what-is-wifi.html#Spectre_radio_WiFi)

## Hacker un wifi

Attaque par brute-force

Réseau libre

# Hardware

## [Faille mémoire](https://fr.wikipedia.org/wiki/Mart%C3%A8lement_de_m%C3%A9moire)

Les condensateurs gardes en mémoire de l’électricité, donc sur la base de cette erreur, en accédant à plusieurs reprise a ROW HAMMER

MeltDown

Détruit l’isolation entre la mémoire et les applications non autorisées.

Spectre

# Vocabulaire

## [IMSI-Catcher](https://fr.wikipedia.org/wiki/IMSI-catcher)

MRC = Méthode de raisonnement cyber

Spectre rompt l'isolement entre les différentes applications. Il permet à un attaquant de tromper des programmes sans erreur, qui suivent les meilleures pratiques, pour qu'ils divulguent leurs secrets. En fait, les contrôles de sécurité desdites meilleures pratiques augmentent en fait la surface d'attaque et peuvent rendre les applications plus sensibles à Spectre