

Les virus



Table des matières

Origine/Définition	3
Principe de fonctionnement	4
Ses différents types	5
Sources	6

Origine/Définition

Les virus appartiennent à la catégorie des logiciels malveillants. Ils sont généralement intégrés dans des fichiers contaminés. Une fois le fichier téléchargé et ouvert, la machine de son hôte est infectée, puis il se réplique et se diffuse avant de s'attaquer au système.

Les virus informatiques sont apparus dans les années 1980 à la suite d'une expérience menée par les premiers programmeurs. Ils ont été créés par des chercheurs et passionnés d'informatique qui souhaitaient comprendre les mécanismes de propagation et d'interaction des programmes à travers les réseaux. Certains virus ont été créés pour démontrer des concepts techniques ou pour tester des failles dans les systèmes. Au fil du temps, les virus ont évolué pour inclure des objectifs plus nuisibles, tels que la destruction de données, l'espionnage et même l'extorsion financière. En conséquence, ils sont devenus un outil privilégié des cybercriminels et ont donné naissance à un ensemble complexe de menaces informatiques visant à voler des informations personnelles ou à endommager les infrastructures.

Principe de fonctionnement

Les virus informatiques se propagent sur les systèmes et les réseaux en infectant les fichiers. Lorsqu'un fichier est lancé, un virus devient actif. Il utilise la propre structure du programme pour se diffuser à l'insu de l'utilisateur. Selon le type de virus, il peut altérer ou détruire des données, modifier les paramètres du système ou ouvrir des portes dérobées. Certains virus sont conçus pour se propager automatiquement via des médias externes, tandis que d'autres peuvent rester inactifs pendant un certain temps avant d'être déclenchés. Les virus peuvent être difficiles à détecter et à supprimer car ils disposent de mécanismes permettant de contourner les logiciels de sécurité.

Les virus informatiques peuvent provenir de diverses sources et exploiter les comportements et les vulnérabilités des utilisateurs ou du système. Il s'agit de l'une des sources d'infection les plus courantes téléchargées à partir de sites Web, de logiciels ou de courriers électroniques. Les réseaux sociaux et les plateformes de messagerie instantanée sont souvent utilisés comme terrain fertile pour les virus, car ils peuvent se propager sous forme de liens ou de fichiers apparemment innocents.

Ils peuvent se transmettre d'un ordinateur à un autre en utilisant divers supports de stockage. Il existe des failles dans les logiciels et les systèmes d'exploitation qui peuvent être exploitées par des virus, surtout lorsque ces systèmes ne sont pas régulièrement mis à jour. Les réseaux Wi-Fi non sécurisés peuvent être utilisés pour propager certains virus.

Ses différents types

Parmi ses types les plus connues, on retrouve :

- Les boot sector : Ces virus sont gravés directement sur un support amovible bootable (disque dur, CD-ROM, clé USB...). Ils exécutent des instructions en MBR une fois le support utilisé.
- Les virus non-résidents : Ces virus ne restent pas enregistrés sur la mémoire de la machine hôte.
- Les virus résidents : A l'inverse des virus non-résidents, ceux-ci vont rester actifs en permanence dans la mémoire de la machine hôte tant qu'elle reste allumée.
- Les virus furtifs : Similaires aux autres virus, sa spécificité est sa capacité à ne pas être détectés par les antivirus en se détachant du fichier d'origine. Il n'affecte pas la taille du fichier contaminé et est difficile à détecter, sauf avec un antivirus puissant.
- Les virus polymorphes : Il affecte les performances de sa machine hôte en corrompant les données.
- Les virus flibustiers : Ces virus modifient la signature des antivirus pour les rendre inefficaces.

Sources

<https://guardia.school/boite-a-outils/quest-ce-quun-virus-informatique-definition-et-fonctionnement.html>

<https://fr.norton.com/blog/malware/what-is-a-computer-virus>

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/virus-informatiques#:~:text=Un%20virus%20est%20un%20programme,informations%20personnelles%20qu%27il%20contient.>

https://fr.wikipedia.org/wiki/Virus_du_secteur_d%27amorçage

<https://www.securiteinfo.com/attaques/malwares-virus-spam-logiciels-indesirables/virus.shtml#:~:text=Un%20virus%20non-résident%20est,la%20mémoire%20de%20l%27ordinateur.>

<https://www.kaspersky.fr/resource-center/definitions/stealth-virus>

<https://www.malwarebytes.com/fr/polymorphic-virus>

<https://web.maths.unsw.edu.au/~lafaye/CCM/virus/virus.htm#:~:text=On%20appelle%20«%20rétrovirus%20»%20ou%20«,afin%20de%20les%20rendre%20inopérants.>