Aperçu des
MALWARES

Malware == **Mal**icious soft**ware**

Apparition dans les années 70-80 avec **Brain** (1986) sur IBM PC.

Il pouvait remplacer le secteur boot d'une disquette par une copie du virus.

```
Displacement ──────── Hex codes ──────── ASCII value
0000(0000)  FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20  -0J04↕•◘↑0
0016(0010)  20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F        Welcome to
0032(0020)  20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20   the Dungeon
0048(0030)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050)  20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20  (c) 1986 Basit
0096(0060)  26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74  & Amjad (put) Lt
0112(0070)  64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20  d.
0128(0080)  20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20   BRAIN COMPUTER
0144(0090)  53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49  SERVICES.. 730 NI
0160(00A0)  5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41  ZAM BLOCK ALLAMA
0176(00B0)  20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20   .IQBAL TOWN
0192(00C0)  20 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F            LAHOR
0208(00D0)  45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E  E-PAKISTAN..PHON
0224(00E0)  45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 3B  E :430791,443248
0240(00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20  ,280530.
```

Amjad Farooq (gauche) and Basit (droite) Alvi

Le virus (virus)

Ce sont des logiciels auto-réplicatifs contenant souvent (mais pas toujours) du code malveillant.

Ils insèrent le code dans d’autres programmes grâce à l’action de la victime.

Il peut engendrer des problèmes, certains sont invisibles, d'autres plus embêtant.

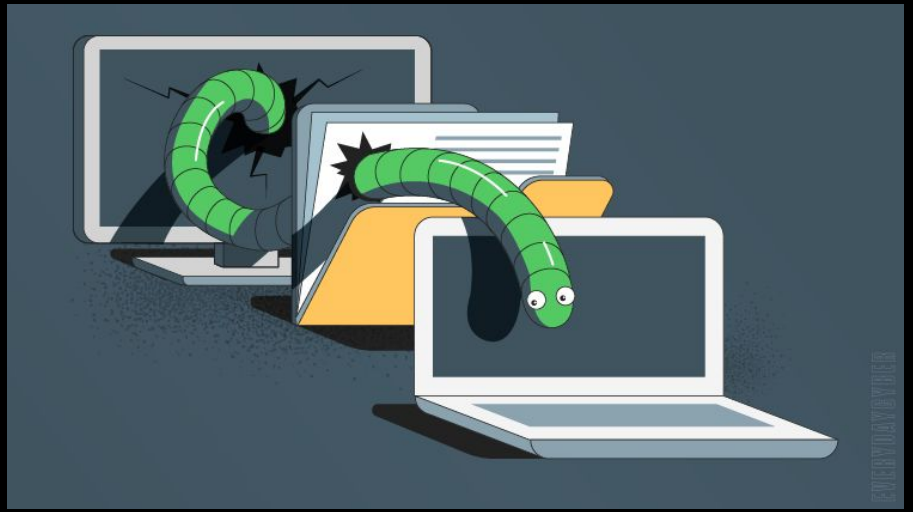
Ils se répandent via le réseau, l’échange de données numériques ou encore les périphériques de stockage.

Le ver (worm)

Il se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

Il a la capacité de se dupliquer une fois qu'il a été exécuté.

C’est un programme autonome donc contrairement au virus, le ver se propage **sans avoir besoin de se lier à d'autres programmes exécutables et aussi d’une action de la victime.**



Le rançongiciel (ransomware)

Il prend en otage des données personnelles en chiffrant ces données, les rendant illisibles et inutilisables.

Le rançonneur demande au propriétaire des fichiers chiffrés d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Le “cheval de Troie” (Trojan Horse)

Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante.

Son but est de faire entrer cette fonctionnalité malveillante sur l'ordinateur et de l'installer à l'insu de l'utilisateur.

Il ne doit pas être confondu avec les virus ou autres parasites

La “trousse administrateur pirate” (rootkit ou “kit”)

C’est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès à une machine à tout moment et avec le niveau de privilège le plus haut possible.

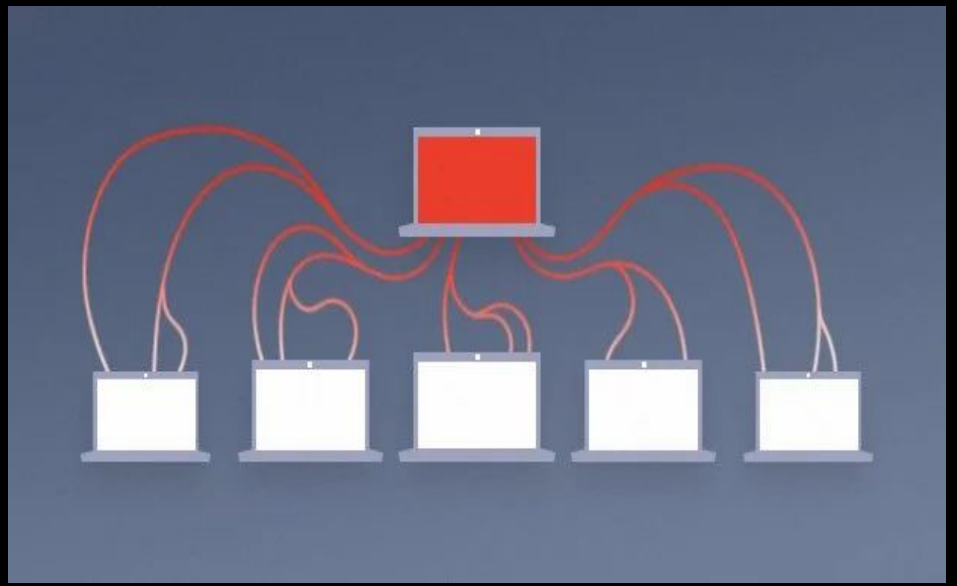
Contrairement à d’autres logiciels malveillants, il se veut le plus discret possible.

Ils peuvent être assez dangereux car ils peuvent opérer au niveau du noyau. Et deviennent donc très difficilement détectables.

Le “réseau de robots” (botnet)

Ce sont des machines avec des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches. (machine zombie)

Divers usages: phishing - diffusion de malware - DDoS - spam - minage de cryptomonnaie - Vol - exploitation de la puissance de calcule - etc.



Le logiciel espion (spyware)

Il a pour but de collecter et transférer des informations (identifiants, mot de passe, images, caméras, sons, touches du clavier, etc) sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance