

Internet

Petits nuisibles

Thomas Engel

Je vous ai parlé dans un des derniers numéros des petits auxiliaires utiles; c'est maintenant le tour des petits nuisibles: je vais approfondir quelque peu le sujet des virus informatiques.

Que sont les virus informatiques?

Les virus qui peuvent infecter un PC sont des fragments de code de programmation. Ceux d'entre eux qui se reproduisent et se répandent partout sont souvent appelés des virus. Peu importe que le virus puisse faire quelque chose ou non. Malheureusement, nombre d'entre eux sont programmés de telle sorte qu'ils endommagent le logiciel, le système d'exploitation, voire même le matériel d'un PC. D'autres s'attaquent aux données stockées sur l'ordinateur, aux mots de passe enregistrés, aux informations bancaires: ils peuvent espionner n'importe quelles informations!

Les virus au sens propre du terme ne peuvent pas se propager tout seuls: il leur faut un intermédiaire (fichier image, fichier texte, programme, etc.) pour pouvoir se répandre.

De plus en plus de ces programmes peuvent utiliser des liaisons réseau pour se propager. On les nomme «vers» (*Worms*).

D'où viennent les virus informatiques?

Comme déjà indiqué, ce sont de petits segments de code de programmation. Ils n'arrivent pas de nulle part: ils sont écrits (programmés) par des êtres humains. Il peut y avoir différentes motivations à leur programmation. Certains programmeurs veulent juste s'amuser un petit peu et ils créent des virus qui ne font pas de dégâts pour la plupart. D'autres par contre ont des intentions délictueuses et désirent capturer ou détruire des données de manière ciblée.

Quels sont les différents types de virus?

Comme dans bien d'autres domaines, il y a aussi pour les virus informatiques d'innombrables variantes. Certains ne causent pas de dommages, d'autres font des dégâts considérables. On connaît plus de 60 000 virus, la plupart pour les ordinateurs DOS (systèmes tournant sous Windows). Ils peuvent se répartir ainsi:

Virus Boot: ils infectent le secteur d'amorçage (*Boot Sector*).

Virus de fichiers: ils infectent les fichiers exécutables.

Macrovirus: ils infectent les applications qui traitent les documents contenant des macros intégrées.



Virus de scripts: on les trouve sous forme de scripts et non dans le code machine. Ils sont donc traités pas à pas et s'attaquent de préférence aux serveurs web.

Comment attrape-t-on les virus?

Avant tout, je voudrais tordre le cou à une légende souvent entendue: il n'y a pas que des virus DOS. D'autres systèmes d'exploitation comme Mac, Linux ou Unix en sont aussi les victimes. Malheureusement, les utilisateurs de ces systèmes ont souvent l'impression qu'ils ne sont pas concernés par les virus et n'utilisent en conséquence aucun programme de protection. Un ordinateur Windows sans programme antivirus ne détecte pas non plus de virus! Cela signifie-t-il qu'il n'y en a pas?

Comment attrape-t-on donc des virus? Comme déjà mentionné, les virus ne sont rien d'autre que de petits programmes. Chaque fois que des données arrivent dans l'ordinateur, elles peuvent contenir des virus, quel que soit le chemin employé pour y parvenir: internet, clé USB, cédérom ou autre. Aujourd'hui, le type des données ne joue aucun rôle. Les virus peuvent se cacher dans des images, du texte, de la musique, des fichiers programmes ou dans n'importe quel autre type de fichiers. Il n'est plus nécessaire d'ouvrir ou de traiter ces fichiers: les virus peuvent démarrer tous seuls, s'installer, se copier ou se dissimuler.



Comment protéger son PC des virus?

Utilisez toujours un programme antivirus récent et à jour. Il doit être installé comme *On-Access-Scanner* (c'est-à-dire qu'il surveille en permanence tous les flux de données sur le PC) et comme *On-Demand-Scanner* (pour contrôler périodiquement toutes les données se trouvant dans le PC).

Tenir toujours à jour le système d'exploitation et les programmes installés (*Service Packs*, *Patches* ou *Hot Fixes*).

Ne jamais télécharger et, surtout, ne jamais installer de programmes douteux.

Ne jamais ouvrir de courriels provenant d'expéditeurs inconnus! N'ouvrir que les pages internet connues et officielles. Ne jamais ouvrir de pages dont les abréviations de pays sont du genre *.ru* ou *.tv*, car de très nombreux virus proviennent de ces régions.

Pour les travaux habituels sur le PC, ne jamais s'annoncer comme administrateur, mais comme utilisateur à droits limités. Ce sont en particulier les droits d'écriture et d'installation de programmes qui doivent être limités.

Définitions

Maliciel (Malware): programmes (virus, vers, etc.) qui peuvent avoir des effets néfastes.

Vers informatiques (Computer Worms): programmes autonomes qui peuvent s'activer et se propager tout seuls, sans intermédiaires. Ils sont aussi nommés virus car la différence entre vers et virus est très labile.

Chevaux de Troie (Trojan Horses): ils se présentent comme des programmes utiles, mais ils font des dégâts en arrière-plan.

Virus Boot: ce sont des virus qui infectent le secteur d'amorçage (*Boot Sector*) d'un disque ou d'une disquette. Ce secteur contient les programmes exécutés immédiatement au démarrage du PC. Ces virus peuvent donc agir sur le système d'exploitation à son démarrage. Pour des motifs techniques, il n'en existe plus guère, car le secteur d'amorçage est très petit.

A suivre...

