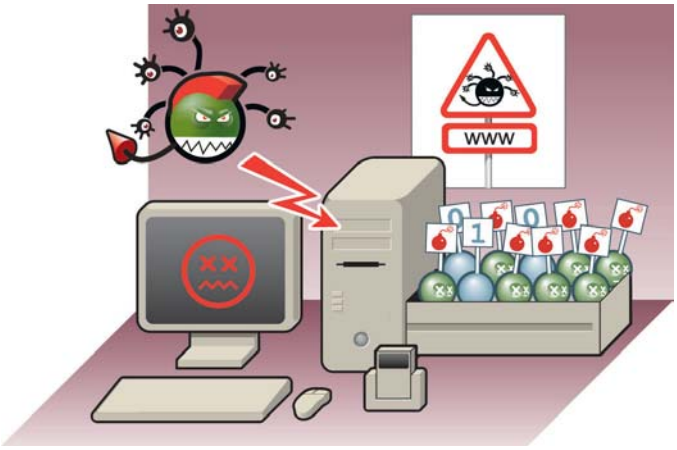
Vers Virus

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Ce document traite des virus et des vers qui ont pour vocation d'infecter une machine, comme un ordinateur ou un serveur, à l'insu des utilisateurs pour y exécuter un logiciel illicite, et se propager d'une machine à une autre. Les virus et les vers peuvent concerner toute personne, lors des échanges d'informations par courrier électronique, par transferts via des médias ou en téléchargeant des logiciels, documents ou tout autre type de fichiers depuis Internet. Sont décrits dans ce document les principes de fonctionnement et de propagation des virus et des vers, les impacts possibles ainsi que les mesures préventives.

Table des matières



1 C'est quoi ?

Un virus est un logiciel ou un morceau de logiciel qui, pour pouvoir se propager, s'attache à tout type de fichier ou autre logiciel, et qui a pour vocation l'infection et sa propagation d'une machine à une autre, à l'insue des utilisateurs.

Un ver est un logiciel très similaire à un virus. Cependant et contrairement au virus, un ver n'a pas besoin de l'intervention humaine pour infecter une machine. Il dispose d'un « moteur » (automatisme) qui lui permet de délivrer et d'exécuter automatiquement son code puis, par la suite, de chercher des nouvelles machines cibles à infecter.

2 Qui est concerné ?

Tous les citoyens, PME et administrations, échangeant des informations par courrier électronique, par transferts via des médias tels que disquettes, CD-ROMs, memory sticks, mais également en téléchargeant des logiciels, documents ou tout autre type de fichiers depuis Internet.

Le simple fait de connecter sa machine à Internet ou à un autre réseau de communication peut être dans certains cas suffisant pour infecter sa machine.

3 Comment cela fonctionne ?

La majorité des virus et des vers sont cachés dans des fichiers ou logiciels ayant des extensions de type .exe, .bin, .com, .vbs, .js et similaires.

Il y a plusieurs années, la propagation des virus et des vers se faisait principalement par disquettes. Internet a introduit de nouveaux mécanismes de distribution beaucoup plus rapides. Notamment à cause de l'utilisation massive du courrier électronique, de la mise a disposition de nouveaux médias et logiciels et du nombre croissant de machines connectées à Internet. Les virus et les vers se propagent de plus en plus vite. La rapidité d'infection et de propagation ne cesse également d'augmenter.

Aujourd'hui plus de 60.000 cas différents ont été identifiés, et plus de 400 sont créés chaque mois selon l'International Computer Security Association (ICSA).

Un autre effet plus inquiétant réside dans le fait que les créateurs de virus et de vers informatiques les ont fait changer d'apparence au fil des années. Aujourd'hui, on en trouve différents types tel que des macro virus, des flash worms et des virus multipartites.

Un virus s'active, en général, si l'utilisateur exécute le fichier ou le logiciel dans lequel le virus est intégré. Par exemple, en cliquant sur un fichier attaché à un courrier électronique (email).

suite au verso

Vers Virus

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

Un ver infecte une machine sans intervention humaine, il essaye d'exploiter des vulnérabilités (veuillez aussi consulter le document «Définition des vulnérabilités») du système d'exploitation (OS) ou des logiciels installés pour infecter la machine. Une fois que le ver se trouve sur une machine, son code est automatiquement exécuté. Un ver dispose, en général, d'un mécanisme lui permettant de rechercher de nouvelles machines cibles à infecter et se propage donc automatiquement. Par exemple en surfant sur Internet.

Exemples :

Morris worm - Le Morris Worm du nom de son créateur «Robert Morris» a été un des premiers vers (1988) à se propager rapidement sur Internet et à infecter des millions de machines.

Iloveyou - Virus qui s'est fortement propagé en 2000 sous forme de courrier électronique qui demandait à l'utilisateur d'ouvrir une soi-disant lettre d'amour se trouvant dans un fichier attaché.

Blaster - Ver qui s'est fortement propagé durant l'été 2003 et qui a en quelques jours infecté des millions de machines connectées à Internet. Plusieurs mois après, beaucoup de machines étaient encore infectées par Blaster sans que leur propriétaire ne s'en rende compte.

4 Pourquoi se protéger ?

Les virus et les vers constituent une menace considérable pour tous les utilisateurs de systèmes informatiques et peuvent causer des pertes importantes, nécessitant une protection efficace afin d'éviter :

pertes financières directes

- destruction de données cruciales,
- mise hors service de tout le système informatique,
- ...

perte de réputation

- divulgation d'informations hautement confidentielles,
- ...

perte de temps

- élimination des virus ou vers du système informatique,
- efforts pour rétablir les données détruites,
- empêcher une propagation continue,
- ...

5 Comment se protéger ?

Pour vous protéger contre une infection virale ou un ver, il existe trois mesures préventives principales qui sont :

- Utilisez un(des) logiciel(s) de type anti-virus et pare-feu (firewall) sur votre machine. Il est important de tenir à jour régulièrement votre logiciel anti-virus afin de vous protéger contre l'apparition de nouveaux virus et vers. (Veuillez aussi consulter les documents : «Anti-virus» et «Firewall»).

Citoyens : vous pouvez acheter ces logiciels dans les grandes surfaces commerciales. Ces produits donnent souvent droit à des mises à jour gratuites de plusieurs mois à quelques années.

- Evitez d'ouvrir des courriers électroniques (e-mails), logiciels ou tout autre fichier dont le sujet ou le contenu vous semble inhabituel voire anormal.

- Appliquez régulièrement les patchs de votre système d'exploitation (OS) et autres logiciels installés, qui permettent de vous protéger dans la majorité des cas contre la propagation et l'infection des virus et des vers. (Veuillez aussi consulter le document : «Patch»).

Grâce à ces trois mesures préventives, vous pourrez éviter bon nombre de problèmes sur votre machine.

D'une manière générale nous vous conseillons d'appliquer les mesures suivantes :

- Assurez un contrôle d'accès individuel aux applications.
- Maintenez un système de sauvegarde performant. (Veuillez aussi consulter le document : «Backup»).
- Protégez physiquement vos machines. (Veuillez aussi consulter le document : «Sécurité physique»).
- Tenez-vous informé sur les nouvelles menaces. (Veuillez aussi consulter le document : «Définitions des Menaces»)

www.cases.lu