L’état de la sécurité informatique

Linux Gazette n°96 — Novembre 2003

David Dorgan

L’état actuel de la sécurité informatique est consternant. Il y a des virus en permanence. Il y a ceux qui s’attaquent à votre courrier électronique, parfois il s’agit d’un réseau irc, voire d’une simple « inondation » du trafic. Bref, la situation devient incontrôlable et je n’ai pas vu une seule entreprise spécialisée dans la « sécurité informatique » apporter de l’aide. Elles ne font qu’aggraver la situation : il y a en ce moment un nombre incalculable d’hôtes infectés et, une fois qu’un utilisateur est touché, vous risquez de l’être aussi. Le récent bogue d’openssh a été le premier à être présenté au Defcon de cette année, et il était supposé être connu de « certains cercles » depuis plus d’un an...

J’ai rapidement perdu mes illusions sur la sécurité informatique. Il semble s’agir d’une bataille qui est loin d’être gagnée. Chaque fournisseur d’antivirus offre la « panacée », et la plupart des utilisateurs acceptent cela. Un exemple : il y a eu récemment quelques « épidémies virales », et maintenant un grand nombre de machines est infecté. Le virus lançait des requêtes **ping** sur une multitude d’hôtes avant de les contaminer. En réalité, il essayait seulement d’infecter ceux qui répondaient, causant une attaque de déni de service (DoS) sur les sites des fournisseurs d’anti-virus et rendant la mise à jour de ceux-ci très difficile. Le site proposant le correctif de Microsoft était quant à lui très ralenti compte-tenu de la demande...

Il y a certains problèmes avec les antivirus.

- Ils résolvent les problèmes d’hier, NON ceux d’aujourd’hui.
- Même si vous êtes à jour, ils ne vous protègent pas d’un virus personnalisé à votre intention, que tout le monde pourrait créer TRÈS facilement.
- Ce sont des palliatifs, ils NE traitent PAS la racine du problème.

Maintenant, après cette récente vague de panique, circulent quelques prétendus « patchs internet » qui dissimulent en fait des virus sous forme de fichier `.exe` sur lequel certaines personnes NAÏVES cliquent. Elles peuvent bien sûr peuvent plaider l’ignorance... il n’y a PAS plus de responsabilité chez l’utilisateur final en informatique qu’il n’y en a sur le fournisseur à propos de la qualité d’un logiciel. À vrai dire, pour avoir une idée de la négligence de certaines entreprises, visitez cette page sur les trous de sécurité d’Internet Explorer non corrigés (http://www.pivx.com/larholm/unpatched/).

Presque tout cela pourrait être évité par un minimum d’effort. En programmation, POURQUOI UTILISER `STRCPY` si vous utilisez le C. Si vous enseignez ce langage dans un collège, NE LAISSEZ PERSONNE L’UTILISER ! Empêchez quiconque de s’en servir dans la phase de test du code. Si quelqu’un est assez stupide pour utiliser `strcpy` en entrée utilisateur par exemple, imaginez la quantité possible de situations de concurrence (race conditions), de débordements de tampon (format string overflows) etc.

En tant qu’utilisateur final, ne cliquez pas sur les fichiers exécutables. Ne le faites pas. Ne demandez pas pourquoi, même s’ils semblent provenir d’un ami. Ne lancez ni les fichiers `.pif`, `.bat` ou `.src`. Pourquoi utiiser des documents Word ? HTML est une plate-forme portable, agréable, etc.

Les choses vont empirer avant de s’améliorer. Imaginez 1 000 virus du style sobig en liberté, et non pas un seul. Imaginez beaucoup plus d’ordinateurs infectés et des logiciels inefficaces répondant à chacun, sur des listes de diffusion de plus 10 000 connectés. L’avenir de l’informatique sécurisée ne viendra pas d’entreprises comme celles que nous connaissons, c’est une certitude, et je le crois vraiment après les quelques déclarations sans objet de quelques-uns des leaders du marché des anti-virus.

Paru dans le n°96 de la Linux Gazette de Novembre 2003.

Traduction française par Simon Depiets <`2df@tuxfamily.org`>.

Relecture de la traduction française par Joëlle Cornavin <`jcornavi CHEZ club TIRET internet POINT fr`>.