PrimaryCare 2002;2:705

Virus informatiques: nouvelles du front

Angel Vilaseca

Fin octobre – début novembre 2002, l'on a pu assister à une vraie pluie de virus e-mail. Il s'agissait du ver W32.Klez, que j'ai reçu à un ou plusieurs exemplaires par jour pendant cette période.

Fort heureusement, ce ver (un ver ou «worm» est un type de virus dont la particularité est de se répandre à l'intérieur d'un système – Internet dans ce cas – en se multipliant à l'infini) est efficacement reconnu et intercepté par l'antivirus du serveur de mon pourvoyeur d'accès, Bluewin en l'occurrence. Ce service est offert gracieusement et activé par défaut. Chaque fois que vous recevez un e-mail avec un attachement infecté, il l'élimine et vous avertit, ainsi que le correspondant qui vous l'a envoyé (à son insu).

Mais comme c'était prévisible, toute cuirasse à son défaut. C'est ainsi que fin octobre j'ai reçu un e-mail d'un collègue. Le mail paraissait à première vue tout à fait normal. L'antivirus du provider n'avait rien signalé. Ma méfiance ainsi endormie (et moi-même à moitié, il devait en effet être quelque chose comme 23 h.) j'ai cliqué sur l'attachement pour l'ouvrir et ... rien ne s'est passé en apparence. C'est déjà mauvais signe. En regardant l'e-mail de plus près, j'ai vu qu'il était daté du mois de juillet, que l'adresse e-mail du collègue était bidon et que l'attachement que j'avais allègrement ouvert était un fichier binaire de type indéterminé. C'était suffisamment inquiétant pour que je mette en route mon antivirus.

Peine perdue: Mon ordinateur était désormais infecté et mon antivirus ne fonctionnait plus. Il avait été corrompu par le virus, qui à l'évidence savait taper là où ça fait mal.

J'essaie de réinstaller l'antivirus: Echec. Le virus est là qui m'en empêche. En essayant d'utiliser mon ordinateur pour quelques travaux urgents, je remarque qu'il m'est impossible d'écrire un texte comportant un caractère avec accent circonflexe. Au lieu d'écrire ô, j'obtiens ^ ^o et ce avec n'importe lequel des programmes installés dans mon ordinateur. L'auteur du virus serai-il francophobe? …

Le salut est venu de mon ami, l'excellent Docteur Bruce Brinkley qui a trouvé sur le site web de Symantec (le producteur de Norton Antivirus http://www.symantec.com/) un petit programme avec son mode d'emploi, téléchargeables gratuitement.

Il suffit de lancer ce programme qui sait où se cache le virus et va l'éliminer sans coup férir.

L'auteur de mes déboires était le virus «Bugbear». Il se distingue des bestioles habituelles par le fait qu'il va regarder dans la machine où il se terre, les titres d'anciens e-mails envoyés et les envoie une nouvelle fois, infectés, à leur destinataire original, avec le titre d'origine. Les virus plus anciens prenaient comme titre un bout de texte pris au hasard, ce qui pouvait alerter le destinataire. Avec Bugbear, ce dernier ne se méfie plus. En outre, le nom de l'expéditeur est conservé, mais l'adresse e-mail est bidon, ainsi l'expéditeur (involontaire!) n'est pas alerté par les mails de mise en garde. On n'arrête pas le progrès …

En ce qui me concerne, afin d'éviter la répétition de tels épisodes, je ne vais plus sur Internet qu'avec un client e-mail tournant sous Linux et équipé d'un firewall. Pour l'instant, c'est une bonne parade, économique et à large spectre. En effet:

1 Un virus écrit pour Windows ne peut affecter un système d'exploitation Linux (c'est un peu l'équivalent de la barrière inter-espèces pour les virus biologiques).
2 L'accès aux fichiers-système de Linux est obligatoirement régi par un mot de passe, choisi par vous et que le virus ne connaît donc évidemment pas. Ceci rend Linux beaucoup plus résistant aux virus que Windows.
3 Il n'existe actuellement que peu de virus Linux, contre des centaines de milliers pour Windows, sans compter les nouveaux qui apparaissent chaque jour.