Comment combattre les virus informatiques

JEFFREY KEPHART • GREGORY SORKIN • DAVID CHESS • STEVE WHITE

La biologie éclaire le comportement des virus informatiques et aide à concevoir des parades.

Naguère, les épidémies redoutées étaient la peste, le choléra ou la grippe espagnole. À l'ère des autoroutes de l'information, les œuvres de fiction grouillent de virus informatiques qui se dupliquent et détruisent les ordinateurs à travers les réseaux. Si les virus infectent effectivement un nombre croissant d'ordinateurs, ils ne sont pas la menace que dépeignent les auteurs de science-fiction. Est-ce pour cette raison qu'ils n'ont pas encore été beaucoup étudiés par les informaticiens?

Leur notoriété est due à une particularité qu'ils partagent avec les véritables virus : ils se lient à un système dont ils utilisent les ressources pour se répliquer (les virus biologiques se lient à une cellule, les virus informatiques à un programme ou à un ordinateur). Leurs effets sont variables : certains virus informatiques sont inactifs, d'autres gênants, et d'autres encore désastreux. À la manière des virus biologiques qui infectent les individus d'une communauté, les virus informatiques se déplacent de programme en programme, d'ordinateur en ordinateur

Avec mes collègues du Centre de recherche *IBM* de Yorktown Heights nous avons trouvé qu'une analogie avec la biologie aide à comprendre les épidémies de ces virus et à élaborer des défenses. En utilisant les outils mathématiques mis au point ces dernières décennies par les épidémiologistes, nous avons compris certains facteurs qui gouvernent leur vitesse de propagation. Nos découvertes de méthodes de détection efficaces de ces virus et des relations entre virus doivent beaucoup aux techniques de recherche d'homologie mises au point en biologie moléculaire. De surcroît, nous avons trouvé des parades contre ces logiciels dangereux en nous inspirant du système immunitaire des vertébrés et de sa remarquable capacité à repousser et à détruire des agents pathogènes.

Le plus ancien ancêtre des virus informatiques n'a existé que théoriquement : en 1940, John von Neumann étudie l'autoréplication des automates cellulaire. Si l'idée de programmes capables d'infecter des ordinateurs date de 1970, le premier cas d'infection répertorié date du mois d'octobre 1987, lorsqu'un petit programme nommé *Brain* («cerveau») apparut sur plusieurs dizaines de disquettes à l'Université du Delaware. Aujourd'hui, les virus infectent au moins un million d'ordinateurs par an, et les utilisateurs dépensent chaque année plusieurs centaines de millions de francs en réparations et en logiciels antiviraux.

La plupart des virus s'attaquent à des micro-ordinateurs de type PC, c'est-à-dire des compatibles avec les ordinateurs *IBM*. Près de 15 000 virus ont déjà vu le jour, et six nouveaux virus apparaissent quotidiennement. Heureusement, seuls quelques-uns d'entre eux se sont disséminés.

Il existe trois types principaux de virus : les virus qui contaminent les programmes exécutables, les virus de secteur de démarrage et les virus de macros. Environ 85 pour cent des souches virales contaminent des programmes, comme des tableurs ou des jeux, mais cela ne représente que 20 pour cent des infections. Lorsque l'utilisateur exécute un programme infecté, les lignes du programme viral s'exécutent en premier et se copient dans la mémoire vive de l'ordinateur, de façon à se recopier toutes seules, dans un autre programme qui sera lancé plus tard. Une fois installé dans la mémoire, le virus redonne le contrôle au programme infecté, si bien que l'utilisateur ne peut déceler sa présence. Lorsque le programme infecté atteint un autre ordinateur par l'intermédiaire d'une disquette ou d'un réseau, le cycle d'infection recommence.

Les virus de secteur de démarrage représentent cinq pour cent de l'ensemble des virus connus. Ils résident dans une zone des disquettes ou des disques durs qui est lue quand l'ordi-