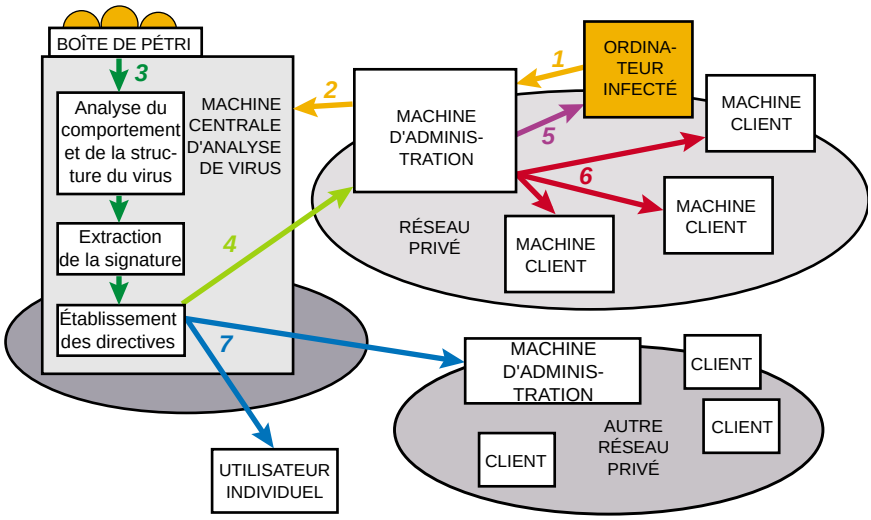

Jeffrey O. Kephart

6. DANS LES RÉSEAUX, des systèmes immunitaires informatiques empêcheront la prolifération des virus. Un ordinateur infecté envoie une copie du programme suspect à une machine d'administration *(1)* qui, à son tour, envoie ce programme, sous forme codée, à une machine centrale d'analyse de virus *(2)*. Cette machine cultive le virus dans une «boîte de Pétri» informatique, où il analyse son fonctionnement et sa structure *(3)*. Les recommandations qui en résultent sont renvoyées vers la machine d'administration *(4)*, qui les renvoie tout d'abord vers l'ordinateur infecté *(5)*, puis vers les autres machines du réseau local *(6)*. Les autres abonnés du monde entier reçoivent périodiquement des remises à jour d'antiviraux qui les protègent des nouveaux virus *(7)*.

en quantités égales, et leur nombre croissait légèrement. Puis, les virus de programmes sont devenus moins fréquents, tandis que le nombre de virus de secteur de démarrage continuait à augmenter. Entre fin 1992 et fin 1995, ces derniers régnèrent sans partage. Pourquoi les virus de programmes se sont-ils éteints?

Nous supposons qu'ils ont été bloqués par l'avènement du système d'exploitation *Windows 3.1*, une amélioration du système MS-DOS utilisé sur les ordinateurs compatibles PC à partir de 1992 : en présence de certains virus qui infectent les programmes, le système *Windows 3.1* se bloque, de sorte que les utilisateurs se sont débarrassés des virus (parfois en vidant le contenu du disque dur et en installant à nouveau tous les logiciels), même quand ils ignoraient que leurs problèmes provenaient d'un virus. En revanche, les virus de démarrage coexistent pacifiquement avec *Windows 3.1*, ils ne gênent pas leur hôte avant que l'infection ne se déchaîne.

L'utilisation générale de *Windows 95*, un autre système d'exploitation, a provoqué le brusque déclin des virus de démarrage. Ce système d'exploitation prévient l'utilisateur de la plupart des changements survenant dans la zone de démarrage, si bien que les virus ne peuvent s'y développer. Lors de notre recensement, nous avons observé quelques virus de démarrage spécifiques à *Windows 95* et à d'autres systèmes d'exploitation à 32 bits, mais ils ont peu de chances de se multiplier.

Aujourd'hui, l'ère des virus de macros a commencé. Ces virus, attachés aux fichiers de données, sont échangés plus fréquemment que les virus attachés aux programmes : ils se transmettent plus rapidement que les autres virus. À l'heure des réseaux, des programmes de courrier électronique et de transfert de fichiers élaborés permettent de partager des programmes et des documents plus rapidement et plus facilement que naguère, ce qui amplifie le problème.

Les virus de macros sont aussi les premiers qui exploitent la tendance croissante à l'interopérabilité des ordinateurs : un virus qui infecte des fichiers DOS ne met pas en danger un *Macintosh*, par exemple, parce que les instructions de copie des systèmes DOS diffèrent de celles des *Macintosh* ; en revanche, un virus de macros peut infecter n'importe quel ordinateur du moment qu'il possède un programme vulnérable. Le fait que le traitement de texte *Word* fonctionne sur une grande variété d'ordinateurs permet à *Concept*, ainsi qu'à d'autres virus de macros, de franchir les frontières entre systèmes.

Aujourd'hui, les virus se déplacent d'un ordinateur à un autre quand les utilisateurs s'échangent volontairement et manuellement des disquettes ou d'autres supports numériques ; on parvient à enrayer les épidémies, car même les virus les plus efficaces mettent des mois, voire des années, pour se propager. Dans les réseaux, les virus se propagent beaucoup plus vite. En 1988 déjà, Robert Tappan Morris avait lancé le «vers de l'Internet», un programme qui exploitait les défauts de sécurité du système d'exploitation UNIX et qui a envahi des centaines d'ordinateurs sur toute la Terre en moins d'une journée.

Un système immunitaire numérique

Les nouvelles techniques de chargement automatique des programmes et des données aggravent le problème. Les programmes de courrier électronique permettent l'envoi de textes ou de feuilles de calcul à des messages : lorsque l'on ouvre le document attaché, le programme adapté s'ouvre, et tous les virus de macros contenus dans le document sont exécutés. Plus grave encore, des «agents intelligents», c'est-à-dire des programmes qui parcourent le réseau à la place des utilisateurs, enverront périodiquement des courriers électroniques et ouvriront automatiquement les documents attachés ; les virus se propageront à des vitesses bien supérieures à celles d'aujourd'hui.

Ces changements de l'écosystème numérique imposent la recherche rapide d'une parade automatique aux problèmes posés par les virus. Les Sociétés *IBM*, *Symantec* et *McAfee* mettent au point des techniques d'analyse et d'éradication automatiques des nouveaux virus. Chez *IBM*, nous créons une sorte de système immunitaire pour les réseaux. De même que le système immunitaire des vertébrés crée des cellules qui reconnaissent et combattent de nouveaux agents pathogènes après quelques jours d'exposition, un système immunitaire informatique peut donner, en quelques minutes, des directives pour reconnaître et éradiquer des virus nouveaux. Dans notre prototype, des ordinateurs compatibles PC, connectés par un réseau à un ordinateur central, exécutent tous le programme *AntiVirus* d'*IBM*. Pour détecter la présence d'un virus, le programme *AntiVirus* utilise diverses méthodes heuristiques : il observe des modifications du comportement de l'ordinateur, recherche des modifications

suspectes des programmes ou analyse des signatures ; il utilise le réseau pour envoyer tout programme suspect à un ordinateur d'administration du réseau.

À la réception d'un programme potentiellement infecté, l'ordinateur d'administration l'envoie à un ordinateur d'analyse de virus qui se comporte comme une «boîte de Pétri» numérique : les programmes de cette machine de test piègent le virus à l'aide de programmes spécialement conçus, nommés «leurres», qui sont exécutés, copiés ou manipulés. Cette phase est particulièrement utile pour faire se découvrir les virus polymorphes. Ces virus sont des virus de macros dont les lignes de programme sont cryptées, de sorte qu'un logiciel antiviral classique est en général incapable de reconnaître sa signature. De plus, lorsqu'ils se dupliquent, les virus polymorphes utilisent un code de chiffrement généré aléatoirement : les signatures sont modifiées à chaque copie. Pour se propager, un virus doit infecter des programmes qui sont souvent utilisés, si bien que l'activité des leurres fait ressortir le code du virus. Ainsi le virus se découvre, et on peut l'éradiquer. Pendant cette phase, on peut aussi comprendre d'autres caractéristiques du virus.

Les leurres infectés sont analysés par d'autres éléments du système immunitaire, qui extraient la signature du virus et fournissent des directives pour le détecter et l'enlever. À partir d'un programme infecté, l'analyseur de virus met généralement moins de cinq minutes pour engendrer ses directives. La machine d'analyse envoie cette information à l'ordinateur qui a demandé de l'aide ; ce dernier incorpore l'information dans une base de données permanente contenant les remèdes à utiliser pour les virus connus. Il peut alors localiser et enlever toutes les copies du virus, et il est définitivement protégé de futures rencontres.

Lorsque l'ordinateur infecté est relié à d'autres machines par l'intermédiaire d'un réseau local, il est tout à fait possible que le virus les ait également envahis. Aussi les nouvelles directives de surveillance et d'éradication sont-elles envoyées automatiquement aux ordinateurs voisins, de sorte que chaque machine peut vérifier immédiatement la présence éventuelle du nouveau virus. Puisque les virus informatiques utilisent le réseau pour se répandre rapidement, l'utilisation du réseau fournit l'antidote aux machines qui en ont besoin. En envoyant aux clients d'un site infecté les dernières directives, on peut, en principe, immuniser très rapidement toute la population des ordinateurs contre l'émergence d'un nouveau virus.

Malgré les efforts, les virus informatiques cohabiteront avec nos ordinateurs. Chaque type de virus évoluera à sa façon, mais, collectivement, la coévolution des virus informatiques et des techniques antivirales se poursuivra comme, en biologie, le font les parasites et leurs hôtes. Ces deux composantes évolueront aussi en réaction aux changements de l'environnement informatique. Par exemple, les agents logiciels itinérants devront être protégés des ordinateurs qu'ils traversent, tout comme ces derniers de la malveillance de certains agents logiciels. Peut-être les virus et les systèmes immunitaires informatiques sont-ils les précurseurs d'un riche écosystème de vie artificielle où les proies et les prédateurs vivront, mourront et coopéreront.

Jeffrey KEPHART, Gregory SORKIN, David CHESS et Steve WHITE travaillent au Centre de recherche Thomas Watson de la Société *IBM*, à Yorktown Heights.

Rogue Programs : Viruses, Worms and Trojan Horses, sous la direction de Lance J. Hoffman, Van Nostrand Reinhold, 1990.

Frederick B. COHEN, *A Short Course on Computer Viruses*, deuxième édition, John Wiley & Sons, 1994.

Robert SLADE, *Robert Slade's Guide to Computer Viruses*, Springer-Verlag, 1994.

Jeffrey O. KEPHART, Gregory B. SORKIN, William C. ARNOLD, David M. CHESS, Gerald J. TESAURO et Steve R. WHITE, *Biologically Inspired Defenses against Computer Viruses*, in *Proceedings of the 14th International Joint Conference on Artificial Intelligence*, Montréal, 20-25 août 1995, Morgan Kaufmann Publishers, Inc.

Mark LUDWIG, *Du virus à l'antivirus : guide d'analyse*, Éditions Dunod, 1997.

Des liens vers de nombreux sites qui traitent des virus sont sur notre site Web : http://www.pourlascience.com