linéairement jusqu'à atteindre un plateau ; ensuite, ils continuent d'apparaître à un rythme constant dans les ordinateurs, et quelquefois ils disparaissent complètement.

Afin de comprendre ces caractéristiques, nous avons utilisé des modèles mathématiques élaborés par les épidémiologistes. Les modèles les plus simples prédisent l'évolution d'une infection à partir d'un petit nombre de paramètres : le «taux de naissance», c'est-à-dire la vitesse à laquelle les individus malades infectent les autres, et le «taux de mortalité», la vitesse à laquelle un individu malade meurt ou est guéri. Lorsque le quotient de ces deux quantités est inférieur à un seuil, l'infection disparaît rapidement. Plus ce quotient est élevé et plus, en l'absence de mesures prophylactiques ou de réactions immunitaires, le nombre de personnes infectées augmente rapidement.

Toutefois, cette théorie simple ne rend pas bien compte de l'évolution des virus informatiques, car elle stipule que, sauf quand le quotient des naissances et des morts est proche de la valeur critique, les virus disparaissent ou se propagent à toute la population. Or, de nombreux virus infectent une très faible proportion de la population et restent à ce niveau. Pourquoi cette évolution? Parce que la théorie suppose qu'un individu a la même chance de contaminer n'importe quel autre individu de la population à risque. En informatique, ce n'est pas le cas, et l'on doit compliquer la théorie pour décrire la structure en groupes fermés de la population qui utilise les ordinateurs : en moyenne, chaque personne ne partage des logiciels et des données qu'avec un petit nombre de personnes, et tous les échanges prennent place à l'intérieur de groupes. Si Philippe échange des logiciels avec Pascale et Pascale avec Françoise, alors, il est raisonnable de penser que Philippe et Françoise peuvent échanger des virus.

Des simulations informatiques ont montré que la proximité des contacts ralentit la croissance des épidémies conformément à nos observations. Des échanges peu fréquents réduisent la probabilité d'une épidémie et abaissent le niveau du plateau, mais n'expliquent pas complètement les données.

L'évolution en action

De même que les disettes, les campagnes de santé publique ou les migrations modifient le cours des épidémies biologiques, des changements de l'environnement informatique sont responsables de plusieurs époques distinctes dans l'histoire de la virologie informatique. Jusqu'en 1992, les virus infectant les programmes ou les secteurs de démarrage se trouvaient

Les virus de messagerie électronique

La croissance rapide du réseau Internet accroît proportionnellement les menaces liées au contenu des messageries électroniques, et plus particulièrement, aux virus informatiques. Un message électronique qui transite sur le réseau peut être séparé en trois parties : l'en-tête, le corps du message et les fichiers attachés. La principale cible des virus informatiques est le fichier attaché. Ces fichiers sont soit des programmes exécutables, soit des documents. Aujourd'hui, on se prémunit contre ce type d'infection informatique par deux approches principales : la protection répartie et la protection centralisée.

Dans la protection répartie, chaque poste susceptible de recevoir un message est protégé. La plupart des programmes antiviraux du marché disposent de modules de surveillance. Ces derniers détectent la présence du virus lorsque les éléments attachés sont exécutés ou ouverts. Malheureusement, cette méthode n'empêche pas la propagation du virus sur l'ensemble des postes des destinataires de messages : si, sur certains postes infectés, le virus n'est pas éradiqué, l'épidémie peut s'étendre. De surcroît, la détection n'intervient qu'à l'ouverture du fichier. Dès lors, un fichier attaché infecté pourra être transmis d'un utilisateur à l'autre sans qu'aucune alerte soit donnée.

Certains programmes antiviraux possèdent des modules spécifiques pour la messagerie électronique. Ces programmes décomposent le message et l'analysent sans ouvrir ni exécuter le fichier attaché. Si cette détection précoce évite l'épidémie, elle dépend du type de messagerie électronique et n'empêche pas la propagation d'un virus infecté à de nombreux utilisateurs. Ainsi, une note de service envoyée à l'ensemble du personnel d'une société entraînera de nombreuses alertes.

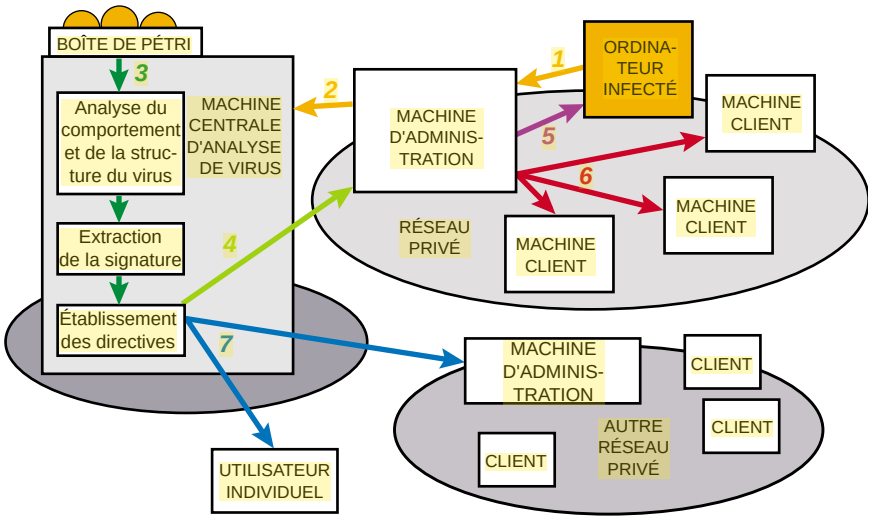
L'autre approche, nommée protection centralisée, consiste à utiliser une machine de contrôle. Tous les messages qui transitent passent par cette machine. À leur arrivée, les messages sont décomposés et décompressés (les fichiers attachés sont souvent compressés). Sur la machine centrale, des logiciels antivirus éradiquent alors les éventuels virus avant de faire suivre le message. Cette solution a l'avantage d'être préventive et centralisée : la note de service infectée envoyée à l'ensemble du personnel sera bloquée avant d'atteindre ses destinataires. Malheureusement, ces solutions ne fonctionnent qu'avec certains types de messageries.

La dernière approche qui s'apparente également à de la protection centralisée, n'est pas préventive : elle consiste à analyser tous les messages présents sur une machine centrale. Cette machine centrale, ou serveur de messagerie, vérifie l'innocuité des messages avant qu'ils ne parviennent à l'utilisateur. Cette solution est encore peu répandue, mais elle présente l'intérêt d'être économique en terme de ressource mémoire et de système.

Quelle que soit la solution mise en œuvre, l'utilisation de l'Internet et des messageries électroniques doit se faire avec une extrême prudence. Sans protection adéquate, quelques règles élémentaires de conduite peuvent éviter le pire : ne pas ouvrir un message en provenance d'un expéditeur inconnu, ne pas exécuter de programmes ni ouvrir de document attaché sans en connaître l'origine et le but, sauvegarder sur disquette les zones et les fichiers sensibles.

Sans ces précautions, le *surf and buy* («se promener sur l'Internet et acheter») peut rapidement se transformer par un *surf and die* («se promener» sur l'Internet et mourir) pour les disques durs et les informations des internautes non avertis.

Stéphane BOUCHÉ, Société *OMNISET*



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