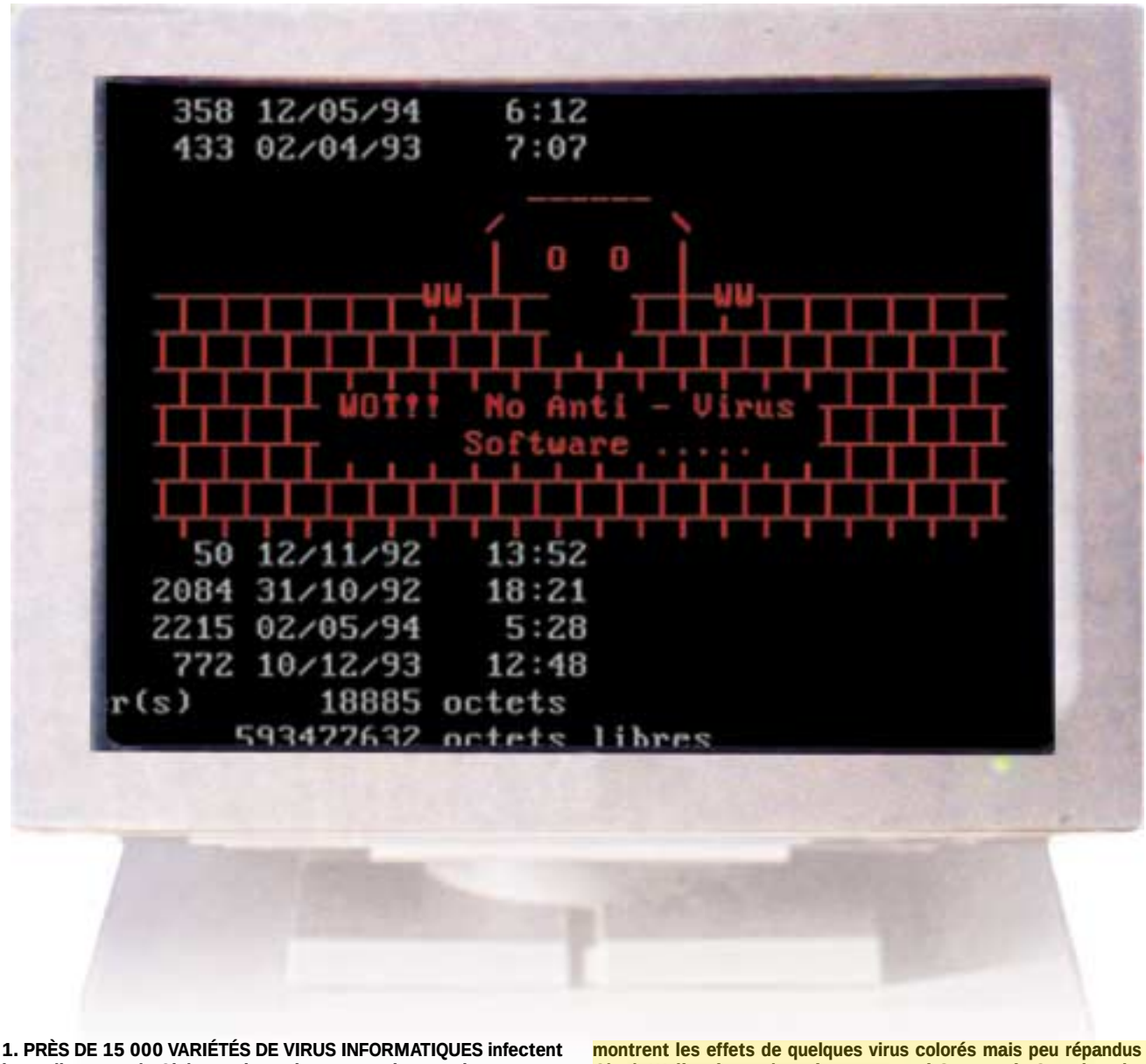
nateur est allumé et dont les programmes sont exécutés automatiquement. Habituellement, le secteur de démarrage contient les instructions de chargement du système d'exploitation, le système qui gère le fonctionnement de l'ordinateur et qui permet notamment l'affichage des données ou la lecture d'ordres tapés par l'utilisateur. Une fois installé, un tel virus peut contaminer toute disquette non protégée en écriture introduite dans le lecteur. Il infecte aussi le disque dur, de sorte qu'il se trouve chargé dans la mémoire vive de l'ordinateur à chaque redémarrage. Les virus de démarrage sont très efficaces et, bien que moins de 1 000 souches différentes existent, ils sont pour le moment plus répandus que les virus qui infectent les programmes exécutables (30 pour cent des infections).

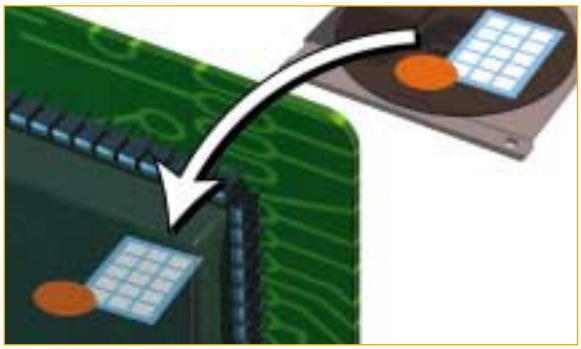
La troisième catégorie, les virus de macros, sont indépendants des systèmes d'exploitation, de sorte qu'ils infectent aussi bien des ordinateurs compatibles PC que des *Macintosh* ; ils infectent des fichiers de données plutôt que des programmes. Beaucoup de tableurs, de programmes de bases de données et de traitement de texte peuvent exécuter des séquences de commandes nommées «macros», qui automatisent des tâches fastidieuses : certaines macros de traitement de texte placent automatiquement un mot long ou une expression toute entière quand l'utilisateur tape seulement quelques lettres ; des macros de tableurs effectuent de longs calculs. Des concepteurs de virus ont programmé des macros qui se recopient dans d'autres documents. De tels virus se propagent beaucoup plus vite que les autres formes de virus, parce que de nombreuses personnes s'échangent des fichiers de données, lorsque, par exemple, ils rédigent un document en commun. Le premier virus de macros détecté, un virus nommé *Concept*, fut trouvé fin 1995 dans un document créé par le programme de traitement de texte *Word*, et c'est aujourd'hui l'un des virus les plus répandus (dix pour cent des infections), avec un nouvel arrivant, *CAP.A*, qui représente 20 pour cent des infections. En tout, on a recensé plus de 1 500



Jana Brenning

1. PRÈS DE 15 000 VARIÉTÉS DE VIRUS INFORMATIQUES infectent les ordinateurs du Globe, mais quelques centaines seulement sont répandues. Les écrans reproduits ci-dessus et sur la page ci-contre montrent les effets de quelques virus colorés mais peu répandus : *Chad*, *Walker* («marcheur») et *Rescue* («Secours»). Certains virus sont inoffensifs, mais d'autres détruisent irrémédiablement les don-

Le cycle d'un virus qui infecte les programmes



Lorsqu'un utilisateur lance un programme infecté, l'ordinateur copie le programme du disque, où il est stocké et inactif, dans la mémoire vive, où il peut être exécuté.

Le programme viral s'exécute en premier, tandis que le programme infecté reste au repos.

Le virus se recopie dans une zone de la mémoire vive séparée du programme, de sorte qu'il peut rester actif même après que l'utilisateur a lancé d'autres logiciels.

virus de macros, responsables de la moitié de toutes les attaques virales.

En plus des séquences qui assurent la recopie, les virus contiennent des séquences variées : certains virus impriment un message ou affichent une image ; d'autres effacent des programmes ou des données. Même ceux qui ne sont potentiellement pas nuisibles peuvent créer des dégâts quand ils se placent dans des configurations différentes de celle où ils avaient été créés. Par exemple, le virus *Form*, qui ne produit habituellement qu'un léger cliquetis chaque mois, écrit sur une partie du disque qui est inoccupée dans les vieux ordinateurs, mais qui contient des données cruciales dans les nouvelles machines, où les répertoires sont agencés différemment.

Techniques immunitaires

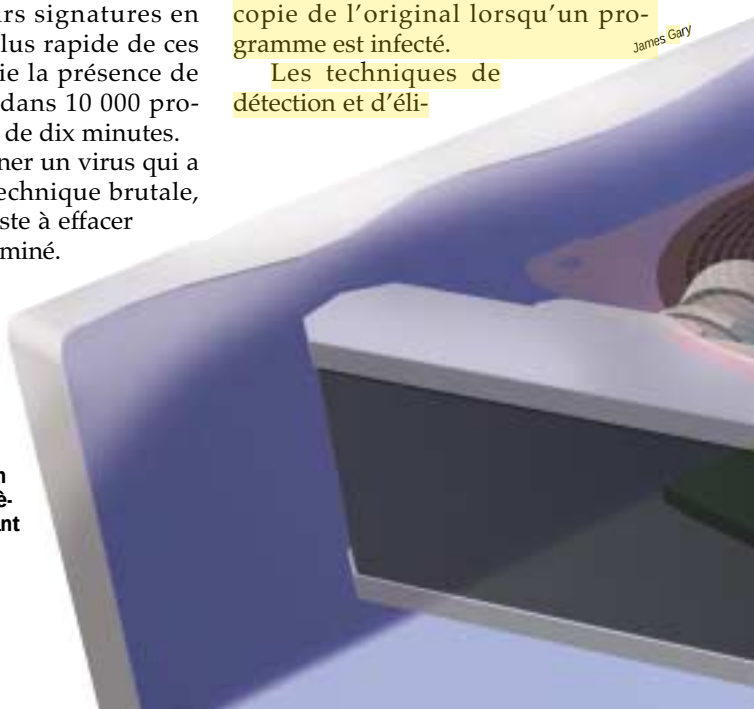
Les logiciels contre les virus sont apparus peu après les virus. Des programmes généraux de détection de virus surveillent si le comportement d'un ordinateur est modifié par la présence d'un virus (par exemple, si le virus modifie certains fichiers importants ou des parties de la mémoire) et cherchent périodiquement des modifications suspectes des programmes. Ils détectent les virus sans les connaître, mais ils peuvent aussi déclencher de fausses alarmes, car des activités normales de l'ordinateur ressemblent parfois à celles de virus en action.

En revanche, des programmes d'analyse recherchent dans les fichiers, dans les secteurs de démarrage ou dans la mémoire de l'ordinateur, des morceaux de programmes (nommés aussi signatures virales) caractéristiques de virus déjà connus. Pour rester efficaces, ils doivent être mis à jour régulièrement, mais ils ne déclenchent que rarement de fausses alarmes. Ces programmes ont la même efficacité que les récepteurs biologiques du système immunitaire : ces derniers reconnaissent les protéines virales en se liant à de courtes séquences (8 à 15 acides aminés seulement, contre des milliers pour la protéine virale complète) ; de même, les signatures virales reconnues par les programmes d'analyse sont très courtes, de 16 à 30 octets (un octet représente huit bits), parmi les quelques milliers qui constituent un virus informatique complet. La recherche de petits segments, au lieu du virus complet, accélère l'analyse, d'autant que des virus différents partagent parfois la même signature. La plupart des programmes d'analyse utilisent des algorithmes issus des techniques d'appariement en biologie, qui cherchent plusieurs signatures en même temps. Le plus rapide de ces programmes vérifie la présence de 10 000 signatures dans 10 000 programmes en moins de dix minutes.

Comment éliminer un virus qui a été détecté? Une technique brutale, mais efficace, consiste à effacer le programme contaminé. La technique est identique à celle qui est utilisée par certains types de cellules immunitaires, qui détruisent les cellules infectées ; mais si les cellules du corps sont aisément remplacées, il n'en est pas de même des programmes et des documents informatiques. Les programmes antiviraux perfectionnés essaient plutôt de réparer les fichiers infectés. Cette tâche est facilitée par le fait que les virus informatiques ne se transmettent que s'ils n'éveillent pas l'attention de l'utilisateur, de sorte qu'ils laissent leur programme hôte intact.

Lorsqu'un programme d'analyse détecte un fichier infecté, il exécute habituellement une ordonnance détaillée, fournie par ses concepteurs, afin d'ôter le code viral et de reconstruire une copie opérationnelle du programme original. D'autres techniques de désinfection générale fonctionnent aussi bien sur des virus connus que sur des virus inconnus. Nous avons mis au point un programme qui élabore un résumé mathématique (nommé somme de contrôle) de chacun des programmes du système, de sorte que l'on peut reconstituer une copie de l'original lorsqu'un programme est infecté.

Les techniques de détection et d'éli-



James Gary

2. SUR LE CHAMP DE BATAILLE NUMÉRIQUE, des programmes antiviraux recherchent les programmes malfaisants (virus, vers ou chevaux de Troie) et réparent les dégâts qu'ils causent. Les nombreux types de virus informatiques qui existent peuvent être reconnus à leur action et à leur structure caractéristique. Les programmes antiviraux protègent aussi les programmes ordinaires en les analysant et en prévenant les utilisateurs de tout changement.