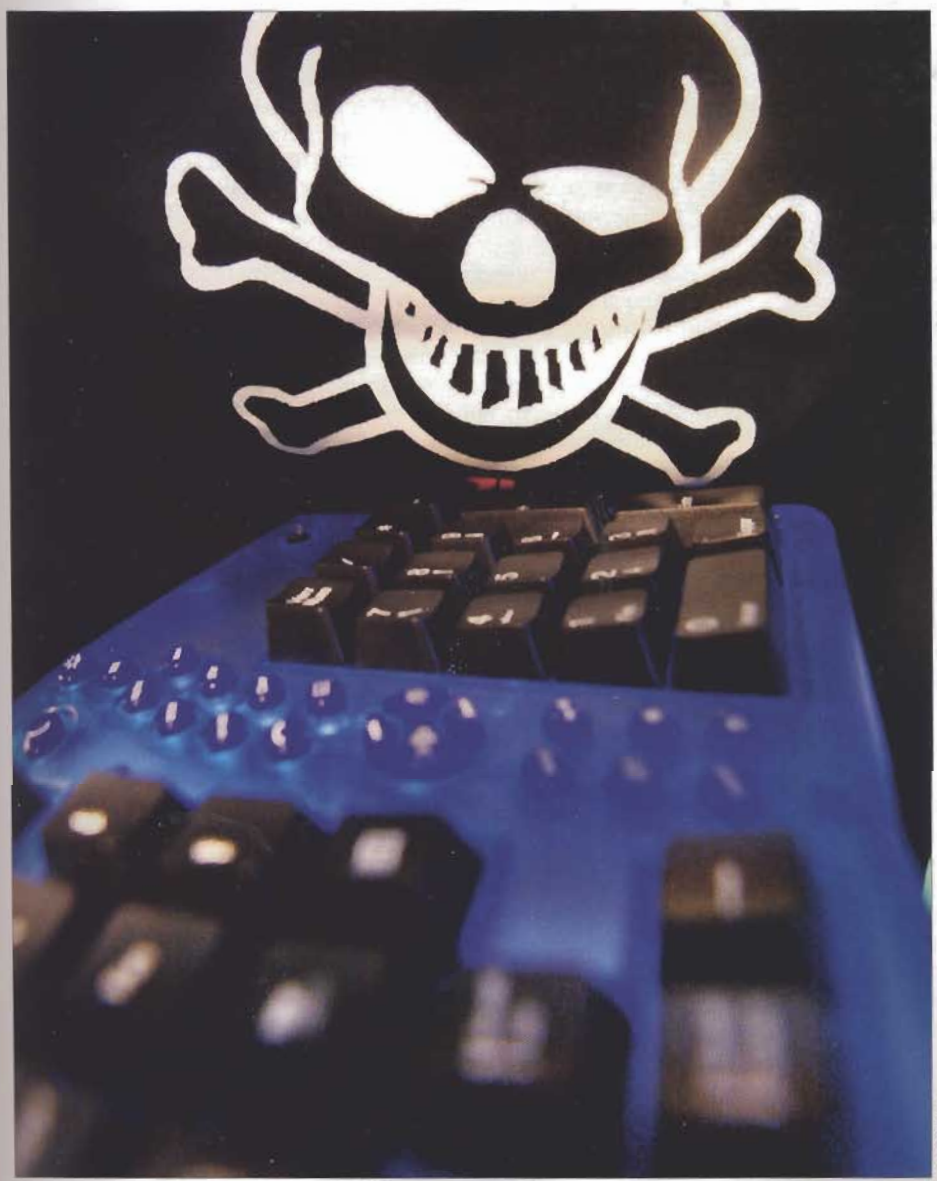
Les nouveaux virus transforment nos ordinateurs en zombies au service d'entreprises criminelles ou terroristes. Une piraterie très organisée.

Les antivirus sont-ils vraiment efficaces ?



JOEL SAGET/AFP

Porte dérobée, cheval de Troie... Les stratégies des pirates informatiques se sont sophistiquées.

Fini le bon vieux temps où les virus « se contentaient » d'afficher des messages amusants sur nos écrans ou, au pire, écrasaient les données de nos disques durs; où des pirates (« hackers ») fanfarons infiltraient pour la gloire des serveurs réputés imprenables. Aujourd'hui, les virus sont au service d'organisations crapuleuses, voire terroristes. Leur stratégie : prendre le contrôle de votre machine. Via internet, le pirate asservit des milliers d'ordinateurs personnels ou d'entreprises grâce à un virus de sa fabrication. Il constitue ainsi de redoutables « botnets », réseaux de machines dites « zombies », prêts à obéir à ses ordres.

Dans cette guerre secrète, le simple particulier devient à la fois victime et complice malgré lui. Car les botnets servent à toutes sortes d'opérations illicites, notamment le vol d'informations personnelles comme les coordonnées bancaires. Mais aussi le stockage sur votre machine de photos pédophiles, de plans d'action terroristes... Ou encore l'attaque massive de sites institutionnels. Ces derniers mois, l'Estonie a ainsi accusé la Russie d'avoir attaqué ses sites gouvernementaux. Peu de temps après, c'était au tour de la France, de l'Allemagne et des Etats-Unis d'être pris pour cibles, en apparence depuis la Chine. En septembre, en pleine crise de l'Ossétie du Sud, la Géorgie dénonçait des pirates russes. Dans tous les cas, les commanditaires peuvent difficilement être identifiés. ●●●

Le coin du spécialiste

L'art des virus indétectables

Si l'une des priorités de l'Esat est de former des spécialistes en informatique et électronique, les chercheurs de l'école préparent aussi l'armée aux menaces numériques. *« Notre objectif est d'anticiper ces menaces en concevant des programmes malveillants le plus sophistiqués possible »*, explique Eric Filiol.
Pour cela, les militaires de l'Esat utilisent notamment des technologies de programmation inspirées de problèmes mathématiques très difficiles à résoudre. Ils ont ainsi construit, à titre de concept de laboratoire, un virus utilisant la cryptographie. Le programme se chiffre lui-même, c'est-à-dire qu'il réécrit son code informatique d'origine sous forme chiffrée. Pour s'exécuter, le code viral doit disposer de sa clé de chiffrement, une sorte de sésame, un énorme mot de passe numérique pouvant aligner plusieurs dizaines de chiffres. Mais quand le virus est installé sur l'ordinateur, il « jette » sa clé ! Il oublie son propre mot de passe. Il ne peut alors plus théoriquement s'exécuter, ni accéder à son code source, sauf à essayer toutes les clés possibles dans l'espoir de retrouver la bonne. L'astuce est alors de concevoir ce virus chiffré de manière à ce qu'il soit capable de récupérer sa clé au bout de quinze minutes de calculs et d'essais. Même le plus obstiné des antivirus ne passe pas un tel laps de temps à analyser un programme chiffré pour savoir ce qu'il y a réellement dedans. Il ne peut pas non plus le rejeter systématiquement, car beaucoup de logiciels légitimes utilisent le chiffrement, par exemple pour la protection des droits d'auteur. Le virus, par contre, a tout son temps. Une fois sur le disque dur, il réalise sa propre analyse pour retrouver sa clé. Il n'utilise que très peu de mémoire et une part infime de la puissance de calcul de l'ordinateur. L'utilisateur ne se rend compte de rien.
Quinze minutes plus tard, le virus a sa clé, il se déchiffre et son code peut s'exécuter.

●●● Ces milliers de zombies servent aussi à saturer les serveurs de sites commerciaux en s'y connectant simultanément à une date et une heure précises. Le site attaqué n'étant plus accessible aux internautes, le pirate n'a plus qu'à exiger une rançon. Autre usage : les botnets se louent à l'heure pour l'envoi massif de spams commerciaux, ces courriels indésirables qui proposent sans cesse des copies de montres de luxe, du Viagra, etc.
« Avec ces nouvelles techniques virales, il faut accepter l'idée que nous ne contrôlons pas forcément les agissements de nos ordinateurs personnels ! », avertit Eric Filiol. Lieutenant-colonel dans l'armée de terre, l'homme est surtout un spécialiste international des menaces informatiques et le directeur du laboratoire de Virologie et de Cryptologie de l'Ecole supérieure et d'application des transmissions (Esat), près de Rennes, et du laboratoire de Cryptologie et Virologie opérationnel de l'Ecole supérieure d'informatique électronique automatique de Laval (ESIEA). Autant dire que les codes malveillants, les « malwares », c'est-à-dire les virus, vers, chevaux de Troie et autres programmes malicieux qui naviguent d'ordinateur en ordinateur, il connaît. Mieux, ses laboratoires se sont spécialisés dans l'étude des plus redoutables, ceux que l'on ne pourra jamais détecter et donc éradiquer *(lire encadré ci-dessus)*.

Protéger la machine sans la ralentir

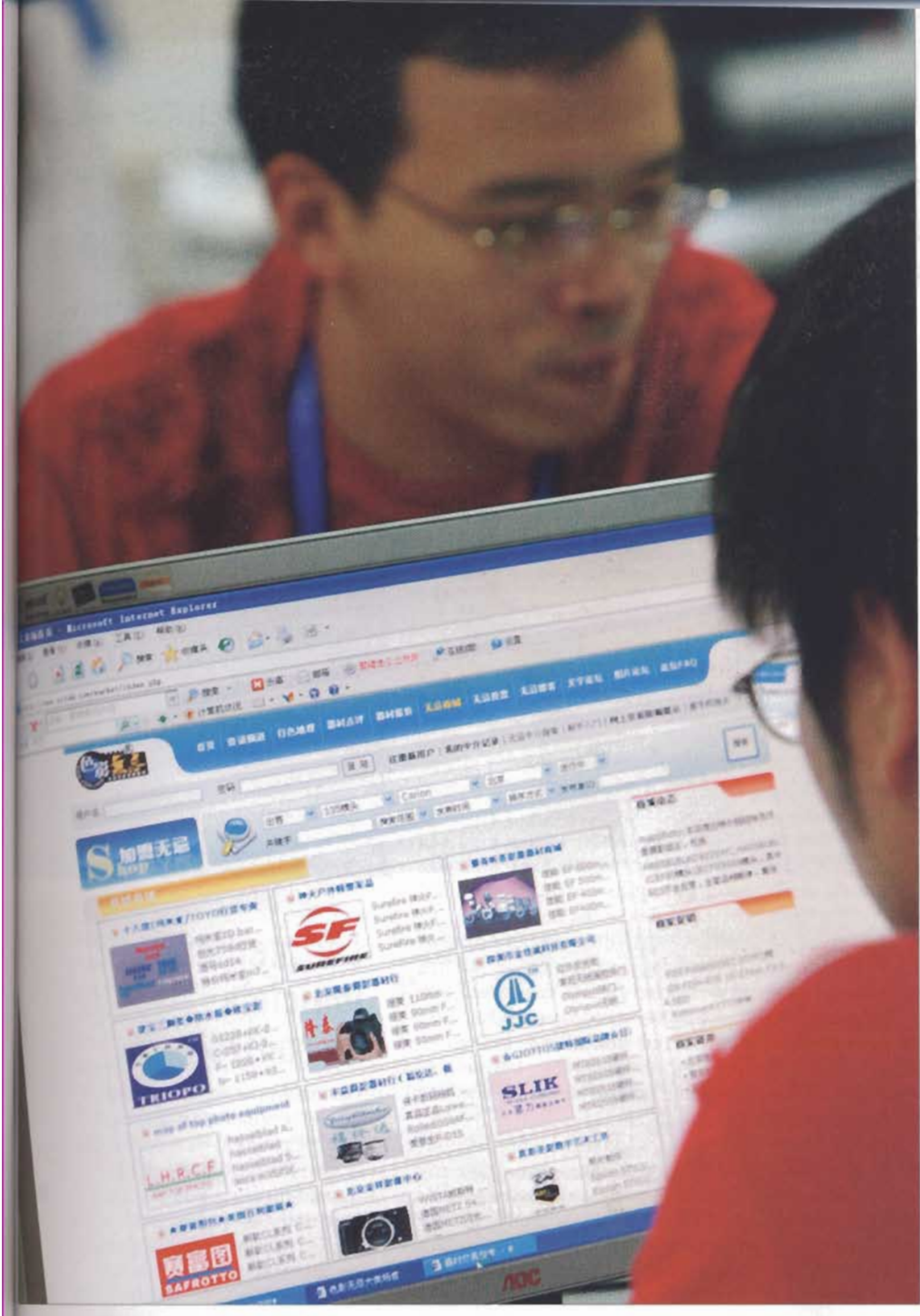
Eric Filiol ne cache pas son pessimisme sur la lutte antivirale : *« Il a été démontré que la détection absolue est une impossibilité mathématique. Aucun programme ne peut prétendre protéger efficacement une machine. »* Pourtant, du côté des éditeurs d'antivirus, le discours commercial laisse entendre le contraire. *« Détecte et élimine automatiquement tous les types de virus »*, *« Empêche les menaces inconnues de pénétrer dans votre ordinateur »*, *« Les malwares, issus de la navigation sur internet, des envois de courrier électronique, des discussions par chat, seront détectés et éradiqués »*, peut-on lire dans les argumentaires de vente de fabricants renommés !
De quoi faire sourire Eric Filiol : *« Les éditeurs sont forcés de trouver un compromis entre sécurité et ergonomie. Ils doivent protéger la machine sans trop la ralentir en puisant dans sa mémoire et les capacités de calcul du processeur. Finalement, l'ergonomie passe avant la sécurité. »* Et c'est normal, car personne n'accepterait que l'antivirus bloque l'ordinateur pendant deux minutes pour analyser chaque nouvelle page web affichée.
Fluidité de fonctionnement oblige, les antivirus suivent prioritairement une stratégie de détection simple consistant à faire des recherches de « signatures », c'est-à-dire à repérer des bouts du fameux code source (langage dans lequel l'informaticien écrit son programme) ayant un aspect viral. Problème : la qualité de la détection dépend de la taille de la chaîne de caractères que l'éditeur choisit de faire analyser par son produit. Plus elle est longue, plus la détection est efficace, mais plus elle mobilise les ressources de la machine et donc la ralentit.
Une stratégie complémentaire de détection, dite heuristique ou comportementale, consiste à rechercher les programmes malveillants non plus à partir de leur code, mais à partir de leur comportement. Par exemple, ouverture et fermeture fréquente des fichiers, des accès sur le réseau, tentatives régulières d'écrire sur le disque dur... *« Nos produits font d'abord une analyse du code puis, si ce code est suspect, ils analysent son comportement pour voir s'il appartient à une famille de codes malveillants connus »*, explique Marc Blanchard (1), *« virus doctor »* chez Kaspersky, l'un des principaux fabricants d'antivirus. Malheureusement, l'ana-

TROIS CONSEILS DE SÉCURITÉ

1. MISES À JOUR : faire des mises à jour régulières de ses applications car elles corrigent les vulnérabilités exploitées par les virus.

2. LOGICIELS PIRATÉS : proscrire l'usage de versions piratées des logiciels payants car, outre un risque de poursuites, elles ne peuvent bénéficier des mises à jour et donc des corrections de vulnérabilité.

3. ISOLATION : utiliser deux disques durs amovibles ou deux ordinateurs différents, l'un pour surfer sur internet et l'autre, complètement isolé du réseau, sur lequel conserver les données importantes. C'est la parade la plus efficace. Eviter aussi d'utiliser des clés USB et des DVD dont l'origine n'est pas sûre.



APITEP/ENG KIOON

lyse comportementale ne peut être poussée très loin, toujours pour des questions de fluidité. Elle ne garantit pas une protection totale.

La preuve la plus frappante se trouve sur le site internet *www.virus.gr* dont le responsable, Antony Petrakis, conserve l'une des plus grosses collections au monde de virus (plusieurs centaines de milliers), sans cesse enrichie. Régulièrement, il publie les résultats d'un test des antivirus du marché sur cette collection. Aucun n'atteint les 100 % de virus détectés. Sur les 49 produits évalués lors de la dernière session, en juin 2008, les scores variaient de 99,05 à 0 %! Certains éditeurs réputés passaient même en dessous des 90 %. Pourtant, tous les virus pris en compte sont théoriquement connus, puisqu'ils apparaissent dans cette collection. « *Le fait est qu'aucun logiciel ne détecte tous les virus, et aucun ne les détectera jamais* », commente simplement Antony Petrakis. « *Mais attention, même s'il faut être conscient que l'antivirus n'offre qu'une protection limitée, il reste indispensable* », insiste Eric Filiol.

OLIVIER HERTEL

A plusieurs reprises, la Chine a été accusée par le gouvernement américain d'avoir dirigé des attaques contre ses systèmes informatiques.

1. Le blog de Marc Blanchard : marc-blanchard.com

AA Lexique

VIRUS : terme générique qualifiant les menaces informatiques. Au sens propre, c'est un programme qui a pour but de s'insérer dans des fichiers ou des programmes hôtes. En ouvrant le fichier ou le programme contaminé, on active le virus qui déclenche des actions nuisibles.

VER (WORM) : l'hôte est le disque dur d'un ordinateur. Le ver n'a donc pas besoin d'un fichier ou d'un programme hôte. La machine peut être elle-même vulnérable ou servir de relais pour contaminer d'autres machines.

PORTE DÉROBÉE (BACKDOOR) : un ordinateur comporte 65 535 ports qui sont autant d'ouvertures vers le monde extérieur. Par exemple, le port 80 sert à la navigation sur internet. Une « porte dérobée » ouvre l'un de ces ports pour que le pirate contrôle l'ordinateur à distance.

ZOMBIE : quand une porte dérobée est ouverte, le pirate peut installer un logiciel appelé aussi « botnet », qui étudie l'adresse IP de l'ordinateur, c'est-à-dire son numéro d'identification lorsqu'il est connecté à l'internet. Ce numéro, donné par le fournisseur d'accès, change régulièrement. Le robot utilise la porte dérobée pour informer le pirate de ces changements. Avec l'adresse IP et la porte dérobée, l'ordinateur est complètement sous contrôle. On parle alors de machine zombie, souvent reliée à des milliers d'autres zombies, aux ordres d'une organisation criminelle.

BOTNET : logiciel robot qui s'exécute seul et de manière automatique, ou réseau de machines zombies.

CONTAMINATION : elle peut se faire par l'ouverture d'un courriel, la connexion d'une clé USB, le lancement d'un DVD... Mais depuis quelque temps, c'est l'infestation par la navigation sur internet qui est à la mode. Il peut suffire d'ouvrir une page d'un site, même officiel, pour charger un ver.