

Semaine du jeudi 25 mars 2004 - n°2055 - Notre époque

Opinions  
Éditos  
Forums

## Guerre électronique

## Internet : les virus attaquent

Finis le temps des petits malins qui créaient des virus informatiques pour rigoler. Aujourd'hui, l'infection des ordinateurs est devenue une affaire de professionnels

Effarant: aujourd'hui, en moyenne, chaque ordinateur connecté à internet est victime d'une tentative d'intrusion toutes les 12 secondes, au lieu de toutes les 30 minutes voici seulement deux ans. Des milliers de virus et de vers informatiques de plus en plus sophistiqués, porteurs d'un «code malicieux», circulent à toute vitesse sur le réseau. Et cherchent à s'insinuer dans chaque machine, via un courriel contaminé dans 99% des cas. Si bien que *«la durée de vie d'un ordinateur non protégé n'est plus que de quelques minutes»*, constate Marc Blanchard, directeur de l'Esac (European Scientific Antivirus Center). En clair, si vous vous branchez sans aucune protection, et que vous ouvrez sans discernement les «fichiers joints» de vos courriels, votre ordinateur sera très vite inutilisable: il faudra réinstaller tous vos logiciels, et faire le deuil de vos fichiers. Stéphane Bouché (société SecuServe) se souvient: *«Le 26 janvier dernier, à 2 heures du matin, le taux d'infestation des courriels électroniques que nous filtrons pour nos clients est passé subitement de 0,31% à 33%: une multiplication par 1000!»*

C'était l'irruption du désormais célèbre Mydoom A, qui s'est décliné ensuite dans ses versions B, C, D, E, F... Dans la foulée, Bagle, Netsky, Sober et quelques autres sont venus prendre le relais. Les spécialistes ont été particulièrement interloqués par Bagle, qui, en l'espace de dix jours, a successivement muté sous la forme de quinze virus de plus en plus difficiles à détecter et à combattre. Car dès qu'une parade est trouvée, une nouvelle version apparaît. Bagle a ainsi diffusé son code malicieux sous la forme d'un fichier compressé crypté (invisible pour les logiciels antivirus), avec une clé d'ouverture dissimulée dans un texte d'accompagnement aguicheur. Puis dans une image. Aux dernières nouvelles, les laboratoires spécialisés cherchent toujours l'antidote.

D'autres virus savent se tapir incognito dans la machine infectée, qui ne présente alors aucun symptôme du mal, mais ils se reconnectent périodiquement sur le site internet de leur concepteur. Ceci leur permet de changer d'apparence et d'attendre l'ordre de se manifester – par exemple pour moucharder les numéros d'une carte de crédit ou d'un compte bancaire, lorsque ceux-ci auront été composés sur le clavier à l'occasion d'une transaction en ligne. Entre-temps, ils se seront propagés à beaucoup d'autres machines, via les carnets d'adresses, en procédant à des usurpations d'identité qui brouillent les pistes.

Cette sophistication extrême a convaincu les spécialistes, comme Stéphane Bouché ou Marc Blanchard, que *«les créateurs actuels de virus ne sont plus des personnes isolées»*. Et de regretter le bon vieux temps, l'époque où on avait affaire à des hackers, des *«adolescents boutonneux plus ou moins surdoués, excités seulement par la performance technique»*. Aujourd'hui, les amateurs ont passé la main. La création de virus est un boulot d'équipes professionnelles animées par des objectifs économiques, ou par l'intention de nuire dans un but précis. Parmi les victimes, le géant Microsoft avait l'an

## MARS 2004

semaine 1	semaine 2
semaine 3	semaine 4
semaine 5	

## Les Archives

► Rechercher

## Le Kiosque

dernier promis une prime de 250000 dollars à quiconque lui permettrait d'identifier la provenance des virus MSBlast et Sobig. Stéphane Le Hir, PDG de Kaspersky Lab France, va jusqu'à dire: «*Internet est une parfaite zone de non-droit, et on assiste à sa prise en main par des organisations criminelles. Lesquelles peuvent très bien travailler en sous-main pour des entreprises ayant pignon sur rue.*»

Cette nouvelle guerre électronique peut s'exprimer de plusieurs façons. Il peut s'agir de faire de la propagande pour une cause. Ou bien de paralyser une société ou une organisation: c'est le *mail bombing*, l'avalanche instantanée, colossale. Beaucoup d'entreprises l'ont expérimentée, de la part d'un concurrent, d'un client ou d'un employé mécontents. Il peut s'agir aussi de dérober de l'information: Microsoft s'est ainsi fait récemment siphonner le «code source», cœur de ses logiciels les plus diffusés, lequel code source est donc tombé entre des mains anonymes qui savaient ce qu'elles cherchaient, et qu'on n'imagine pas bienveillantes. Il peut s'agir enfin de décourager des pratiques nuisibles à certains. Par exemple, observe Stéphane Le Hir, on a repéré un virus spécifiquement conçu pour détruire les fichiers MP3 – format sous lequel sont stockés les films ou programmes musicaux piratés. Pour le plus grand bonheur des industries victimes de ces piratages.

Pour juguler les épidémies, Kaspersky – l'une des sociétés championnes de la lutte – est contrainte d'offrir à ses clients une remise à jour des antivirus toutes les trois heures! Comme toutes ses consœurs, elle plaide bien sûr non coupable: les vendeurs d'antivirus ne créent pas les virus et n'y auraient d'ailleurs aucun intérêt, puisque cela multiplie les interventions alors que les clients ont déjà payé. «*Les virus sont clairement devenus des outils de nuisance*», assure le patron de Kaspersky. Mais comme leurs diffuseurs se cachent souvent en haute mer, sur d'anciennes plates-formes pétrolières échappant à toute juridiction, on n'est pas près d'assister à leur éradication. Au point que Stéphane Le Hir se demande si «*l'internet tel qu'on le connaît n'est pas condamné à une disparition prochaine*»...

**Fabien Gruhier**

### Envoyer cet article à un(e) ami(e)

Dans la rubrique "Notre époque" :

- Vilnius : une justice si lointaine
- Mini-tyrans
- Le ruban noir
- Foot : retour gagnant
- Règlements de comptes entre gendarmes
- Les chercheurs se radicalisent
- Sécheresse sous influence
- Sedna, l'astre du froid
- Educateurs ou indicateurs?
- Le polytechnicien des rues



**Retour à l'index**

▲ Haut de page

© Le Nouvel Observateur 2003/2004

Conformément à la loi "Informatique et Liberté" n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous nous engageons à informer les personnes qui fournissent des données nominatives sur notre site de leurs droits, notamment de leur droit d'accès et de rectification sur ces données nominatives. Nous nous engageons à prendre toutes précautions afin de préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers.

Droits de [reproduction](#) et de [diffusion](#) réservés © **Le Nouvel Observateur** 2003

**Usage strictement personnel.** L'utilisateur du site reconnaît avoir pris connaissance de la [licence](#) de droits d'usage, en accepter et en respecter les dispositions.

La fréquentation de ce site est contrôlée et certifiée par [Diffusion Contrôlée](#)