# Les pirates ont trois longueurs d'avance sur leurs cibles

*Plus rapides et souvent insiders, ils s'attaquent à des entreprises qui hésitent à porter plainte.*

**Jean-Louis Richard**

Soudain, l'on reparle de la sécurité sur Internet. Cette fois il ne s'agit pas de la sûreté des transactions – elle a alimenté tout un débat l'année passée –, mais de l'attaque par déni de service, encore appelée attaque par saturation *(voir l'encadré en page 16)*. Les huit sites parmi les plus fréquentés du réseau qui en ont été les victimes, ont cessé de fonctionner pendant plusieurs heures. Ce type de criminalité, contre laquelle il n'existe, à l'heure actuelle, aucune protection, semble à la portée de n'importe quel adolescent un peu dégourdi. Des kits de piratage circulent depuis quelques mois sur le réseau. Quelques gamins ingénieux ont donc le pouvoir de faire trembler les entreprises les plus puissantes de la nouvelle économie. Internet n'est-il pas un outil effrayant? *L'agefi* a interrogé deux spécialistes, Solange Ghernaouti-Hélie, professeur à HEC-Lausanne et Arnaud Dufour, consultant en stratégies Internet.

**A-t-on une idée de l'identité et des motivations des cyber-pirates qui ont frappé ces derniers jours?**

Arnaud Dufour: Non. D'ailleurs, il sera très difficile au FBI de démasquer l'origine des attaques. Ce que l'on peut dire aujourd'hui, c'est que le e-commerce a des ennemis. On retrouve sur le réseau des groupuscules résolument opposés au développement commercial d'Internet. Tout comme les pirates, ils ont leurs propres sites et communiquent sur leurs opinions et leurs opinions.

Solange Ghernouati-Hélie: Ces cyber-délinquants agissent d'autant plus facilement qu'ils éprouvent un sentiment de relative impunité. D'une part, ils commettent leurs méfaits à distance, d'autre part, le cadre juridique qui traite de ces questions comporte encore des lacunes. Surtout, les victimes portent rarement plainte.

**Comment se fait-il que les entreprises hésitent à porter plainte?**

Arnaud Dufour: Parce que cela serait interprété comme un aveu de déficience du système informatique. Il y a quelques années, lorsque plusieurs banques s'étaient plaintes de malversations chez elles, des clients ont eu peur que des données les concernant ne s'échappent. Ils ont préféré partir chez des concurrents. Alors, depuis, tout le monde reste très discret. Les informations et les données sur la

●●● SUITE PAGE 16

# Les pirates ont trois longueurs d'avance

▸ délinquance électronique sont rares.

**La sécurité Internet est-elle correctement prise en compte dans les entreprises ?**

Solange Ghernouati-Hélie: Le phénomène Internet n'est que la pointe de l'iceberg. En fait, c'est la maîtrise de l'ensemble des risques informatiques qu'il faut considérer. Pour beaucoup d'entreprises, le phénomène Internet a eu un effet de révélateur sur l'importance à attacher à la sécurité des systèmes informatiques. Force est de constater que cette sécurité est souvent mise en place au coup par coup, lorsqu'un problème a été identifié. Il faudrait bien mieux adopter une démarche globale sur la gestion des risques.

Arnaud Dufour: Les points faibles des entreprises sont la formation et la discipline des utilisateurs des systèmes informatiques. Les négligences font le bonheur des pirates. En général, ils sont très bien informés: environ 80% sont des proches de l'entreprise: soit des employés, soit des personnes ayant bénéficié d'une complicité.

En plus, les pirates ont un avantage structurel. Presque tous les logiciels présentent des points de défaillance, provenant soit de par leur conception, soit de leur mauvaise configuration par l'utilisateur. Nombreux sont les informaticiens qui, découvrant de tels points faibles, les publient sur Internet. L'éditeur du logiciel va bien sûr se précipiter pour proposer une rectification. En attendant, les pirates ont tout loisir de chercher à utiliser à leur profit la défaillance, désormais connue de tous. En plus, il faut dire que certains responsables de l'informatique hésitent à mettre leurs logiciels à jour de peur qu'une erreur ne se glisse lorsque le système est arrêté pour modification. Pour eux, c'est toujours un moment délicat.

**N'est-il pas troublant que le plus grand danger provienne des employés?**

Arnaud Dufour: Ce chiffre de 80% est en fait plutôt rassurant. L'entreprise agressée n'est en général pas la victime de quelque chose qui la dépasse totalement ou d'un pirate qui frappe on ne sait pourquoi depuis l'autre bout de la planète. Les cas de sabotage impliquent la plupart du temps des problèmes humains. Une vengeance après un licenciement est un cas typique ●

## Il n'y a pas de parade contre le déni de service

La Chine, après les événements de Tiananmen, a été la première à expérimenter le déni de service. Les associations de défense des droits de l'Homme avaient submergé les fax du gouvernement avec leurs protestations. Ceux-ci, incapables de reconnaître les vrais messages de ceux destinés à les «polluer», ont été rendus inutilisables. L'attaque qui a visé cette semaine les plus grands sites Internet est de même nature.

Depuis peu, les pirates ont à disposition des logiciels d'assaut capables de pénétrer des ordinateurs tiers (esclaves) et d'y installer des systèmes à retardement. Au moment voulu, ces derniers ordonneront aux ordinateurs esclaves de se connecter avec le site visé pour lui déverser un flot d'informations destiné à le submerger. Les sites sont à l'heure actuelle incapables de faire le tri entre les connections correspondant à un trafic normal et celles ayant des intentions hostiles. Quant au logiciel d'assaut, il a soin d'effacer toutes les traces qui permettraient de le localiser. Pour dérangeantes qu'elles soient, elles empêchent tout le trafic et toute connexion, ces attaques restent (techniquement) bénignes: elles n'endommagent pas le site, ni les informations qui s'y trouvent.

Les experts en sécurité estiment que ce genre d'attaques risque de se multiplier à l'avenir, ce qui fait promet déjà de beaux jours aux entreprises de sécurité. Celles-ci se sont offert hier leur second jour de forte hausse. WatchGuard s'est déjà appréciée de près de 100%. ISS Group ou Axent Technologies, entre autres, étaient aussi en forte progression.