



## « Ils attaquent toutes les trois semaines »

**NICOLAS WOIRHAYE**, ingénieur au Laboratoire d'expertises en sécurité informatique (Lexsi)

**Existe-t-il une parade à ces attaques venues de Russie ?**

■ **Nicolas Woirhaye.** Les parades ne sont pas universelles car les ordinateurs peuvent être infectés en consultant un site quelconque. La meilleure solution, c'est d'avoir équipé son ordinateur de logiciels antivirus et de les mettre à jour régulièrement. Ils sont d'autant plus efficaces que les virus sont répandus et, lorsque ces virus sont rares, ces logiciels sont moins actifs. Toutes les victimes de cette affaire en France ont été piégées car elles ne possédaient aucun système de protection.

**Quelle solution préconisez-vous ?**

Les banques ont réagi depuis l'année 2005 pour faire face à ces attaques. Elles ont mis en place la technique du clavier virtuel. Le client ne saisit plus son mot de passe sur le clavier mais le choisit grâce à la souris sur une page affichée sur l'écran. Cette technique permet de contourner les virus qui pistent les frappes sur le clavier. Nous avons identifié sur des réseaux de messagerie instantanés des forums où l'on observe ces pirates. La France est victime d'une alerte environ toutes les trois semaines de la part de pirates russes. Notre rôle est d'anticiper ces at-



Nicolas Woirhaye. (DR.)

taques et de prévenir les organismes bancaires.

**Mais est-ce efficace ?**

Nous nous trouvons face à une concurrence sans fin entre les techniques des pirates et les banques. Nous avons des exemples de piratages de cla-

viers virtuels sur des établissements anglais et américains. Mais cela reste marginal.

**Comment sont structurés ces réseaux de pirates ?**

Ce sont des réseaux très atomisés avec une grande expertise technique où chacun se répartit les rôles. Il y a, d'un côté, ceux qui conçoivent les logiciels, ceux qui éditent les mails ou contaminent les pages du Net, ceux encore qui recrutent les hébergeurs d'argent et ceux qui le récupèrent. C'est une façon de brouiller les pistes.

**Y a-t-il des réseaux plus spécialisés ?**

La mode est aux attaques sur les comptes-titres bien plus fournis que les comptes des particuliers. C'est la spécialité des réseaux brésiliens qui jouent plutôt chez eux. On en est à 200 millions d'euros détournés selon les estimations. Les Russes ciblent le monde tandis que les Roumains ou les Bulgares préfèrent les Etats-Unis.

**PROPOS RECUEILLIS PAR J.-M.D.**