# Le DRDoS, nouvelle menace qui peut paralyser le Web

Depuis quelques semaines, les spécialistes de la sécurité ont détecté plus de 1.500 attaques visant les serveurs de noms, des ordinateurs spécialisés qui accompagnent le trafic Web en dirigeant l'internaute vers ses destinations.

Ces attaques d'un nouveau genre ont déjà fait des victimes: en particulier des sites commerciaux, des opérateurs Internet et des sociétés d'infrastructure en ont été la cible, mais leurs internautes n'ont pas pu (encore) en mesurer les réels effets. En s'attaquant aux serveurs '*root*' (racine) avec cette technique du '*distributed reflector denial-of-service*', les pirates paralysent le Net sans que leur attaque soit détectable par l'utilisateur, et pire encore sans qu'il soit nécessaire qu'ils attaquent directement les sites. Selon Ken Silva, directeur de la sécurité chez VeriSign, ces attaques n'ont touché que 6 % du million de **serveurs de noms** qui alimentent le réseau Internet. En revanche, avec un taux de 8 gigabits par seconde, les attaques ont démontré une parfaite maîtrise de l'électronique de la part de leurs auteurs. Mais le plus inquiétant, c'est l'effet potentiel de ces attaques. Pour Ken Silva, le danger est comparable à celui de l'**attaque d'octobre 2002** qui avait paralysé **neuf des treize serveurs '*root*'** qui gèrent le trafic Internet. On avait frisé la catastrophe mondiale ! A l'époque, VeriSign avait autopsié deux des serveurs, mais les machines avaient révélé? qu'elles n'étaient pas affectées. Mais aujourd'hui, « *ce pourrait être l'ouragan 'Katrina' de l'Internet*« , affirme Ken Silva. L'*US Computer Emergency Readness Team*, un partenaire du département américain de la sécurité intérieure (*Homeland Security Department*), a averti en décembre dernier les ingénieurs réseaux de configurer proprement leurs serveurs de nom afin de se protéger des attaques. Le danger est sérieux, des 'hackers' très bien informés ont trouvé là le moyen de paralyser le Web et les e-mails sans s'attaquer directement aux sites. Et sans que les serveurs Web, leurs systèmes de protection, et les internautes eux-mêmes soient directement attaqués et disposent de la moindre latitude.