Verisign : 'Les serveurs .com sont susceptibles de tomber'!...

Les attaques DoS (Denial of Service) se multiplient et selon Verisign les serveurs, déjà régulièrement ciblés sont devenus les cibles principales des cybercriminels. *« Avec l'explosion des connexions haut débit, les attaques DoS se multiplient «* estime Verisign, le groupe qui administre les noms de domaines en .com. Les groupes de criminels qui vendent « des outils de hacking » (ndlr : type Mpack) en ligne sont très nombreux, et pour Verisign ils menacent l'intégrité de la Toile, car chaque année, de plus en plus d'ordinateurs zombies passent sous leur contrôle, via des réseaux de Botnet. Inquiétant constat, car Verisign indique que si ses serveurs étaient victimes d'une attaque DoS massive cela pourrait provoquer une gigantesque panne des .com. Autrement dit, toute une partie du Net ne serait plus accessible. Interrogé par nos confrères de*silicon.com*, Ken Silva, le chef de la sécurité de VeriSign explique : *« Nous avons déjà essuyé plusieurs tentatives d'attaques sur nos serveurs. Le but des hackers est clair, ils veulent faire tomber le net. »* Silva explique que les attaques DoS sont particulièrement difficiles à détecter et encore plus dures à tracer. Les groupes les plus actifs sont en Russie, en Chine et en Roumanie. Par contre, rien ne prouve l'implication des gouvernements. *« Nous multiplions nos efforts pour empêcher ces attaques, mais malheureusement avec l'actuelle course au haut débit que se livrent les opérateurs un black-out total est à craindre. »* Actuellement, Verisign est en train de mettre à jour son in frastructure. Ce projet est baptisé Titan. Au programme de ce rafraîchissement de l'écosystème de nouveaux outils afin de gérer plus finement les serveurs notamment au niveau de l'utilisation du CPU et de l'allocation dynamique de mémoire. Enfin, Silva estime que les fournisseurs d'accès doivent apprendre à mieux surveiller leurs réseaux.