Internet sous la menace d'une nouvelle forme d'attaques via les DNS

- Informatique - Internet -

Date de mise en ligne : jeudi 16 mars 2006

Spyworld Actu

Une technique spécifique de dénis de service amplifie l'attaque en exploitant la fonction récursive des serveurs de noms de domaine.

L'US-CERT (United States Computer Emergency Readiness Team), une initiative gouvernementale visant à protéger l'infrastructure Internet américaine publiait, mi-décembre 2005, un document (à télécharger au format PDF) intitulé La menace continue des dénis de service introduite par la récursivité DNS (The Continuing Denial of Service Threat Posed by DNS Recursion).

Les chercheurs de l'US-CERT y notaient qu'ils avaient "été alertés d'une hausse d'attaques par saturation de service [DDoS ,ndlr] à partir de requêtes DNS récursives falsifiées". Des attaques préoccupantes dans la mesure où "tous les systèmes communiquant sur Internet doivent permettre le trafic DNS".

Petite explication technique. Lorsqu'un internaute saisit une adresse web dans son navigateur, le système (son ordinateur) commence par interroger un serveur de nom de domaine (DNS pour Domain Name Server) chargé de traduire l'adresse en clair (www.vnunet.fr par exemple) en adresse numérique dite IP (propre aux ordinateurs). Schématiquement, si le DNS ne trouve pas la correspondance entre l'adresse web et le numéro IP, il interroge un DNS lui faisant autorité et ainsi de suite jusqu'à obtention d'une réponse (ou d'une "non réponse") qui sera renvoyée à l'auteur initial de la requête. Du moins, seuls les serveurs qui acceptent la récursivité des requêtes autorisent le transfert des requêtes non résolues par le DNS principal.

Une requête falsifiée (spoofed) usurpe une adresse IP afin de cacher la localisation originale de la requête (et donc de l'attaque). Du coup, le DNS interrogé renvoit sa réponse à un ordinateur (la cible de l'attaquant) qui ne l'a de fait pas sollicité. Et, selon l'US-CERT, un attaquant peut envoyer des milliers de requêtes récursives falsifiées afin de "générer un raz-de-marée de réponse DNS" dont les flux pourraient atteindre plusieurs gigabits/s de transferts de données. De quoi mettre à plat plus d'un serveur.

75 % des serveurs DNS en mode récursif

"Les attaques de DNS par récursivité sont essentiellement une amplification des attaques par déni de service", estime l'US-CERT. D'autant que ce type d'attaque se répercute sur le trafic général d'Internet affectant serveurs de nom racines, routeurs, backbone et autres composantes du réseaux. L'Associated Press a rapporté, aujourd'hui, qu'une attaque de ce type s'est produite sur un DNS situé en Afrique du Sud. Ce qui a mis à mal des sites web commerciaux et des fournisseurs d'accès durant plusieurs semaines.

Pour se protéger, l'US-CERT conseille de couper la fonction de récursivité des serveurs DNS ou de les restreindre aux seuls domaines dignes de confiance. Paradoxalement, interdire la récursivité des serveurs limiterait considérablement la communication en ligne (faute de pouvoir trouver les sites Web demandés). C'est probablement pour cela que, selon une récente étude réalisé par le constructeur InfoBlox, 75 % des 1,3 million de serveurs DNS "interrogés" fonctionnent en mode récursif. De quoi faire tomber Internet ?

Post-scriptum :

http://www.vnunet.fr/actualite/rese...