Noël à UltraDNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 décembre 2009

https://www.bortzmeyer.org/noel-a-ultradns.html

Les services du fournisseur d'hébergement DNS UltraDNS, filiale de NeuStar, ont été complètement interrompus mercredi 23, apparemment suite à une attaque par déni de service. Avec UltraDNS, est tombé le service DNS de plusieurs gros clients notamment Amazon et Walmart.

Comme d'habitude, il n'y a pas beaucoup de détails techniques disponibles. Et tout ce qui est publié n'est pas forcément correct. Il semble bien que l'attaque était une DoS contre les serveurs DNS d'UltraDNS et, si c'est bien le cas, il pourrait s'agir de la première attaque DoS réussie contre un service DNS complètement "*anycasté*". En l'absence d'autres informations, il est toutefois difficile d'en déduire quelle technique exacte a été utilisée. Le marketing ultra-agressif <http://www.merit.edu/mail.archives/nanog/2006-11/msg00247.html> d'UltraDNS, et notamment leur habitude détestable d'appeler directement les Directions Générales, en crachant sur le logiciel libre et en expliquant au Directeur que son équipe technique utilise des logiciels gratuits d'amateurs, fait que beaucoup de gens ne pleureront pas sur les malheurs de ce fournisseur. Les concurrents directs d'UltraDNS ne se sont pas privés de rappeller cette attaque réussie <https://press.verisign.com/easyir/customrel.do?easyirid=AFC0FF0DB5C560D3&version=live&prid=674084&releasejsp=custom_97>. Mais il faut quand même se rappeler que les attaques par déni de service sont les plus difficiles à contrer, qu'il existe une offre assez vaste <http://www.gdata.fr/security-labs/actualite/news-details/article/1330-economie-souterraine-g-data.html> de mercenaires prêts à travailler pour n'importe qui et que personne n'a encore la solution miracle contre cette vulnérabilité.

Quelles étaient les motivations de l'attaque ? Certains se sont étonnés que les attaquants ne soient pas sensibles à la magie de Noël. Mais c'est sans doute justement la proximité de cette date qui est responsable. Noël est depuis longtemps une opération commerciale et non plus la célébration de la naissance du barbu palestinien qui voulait que tout le monde s'aime. Des entreprises comme Amazon font une bonne part de leur chiffre d'affaires dans les jours précédant Noël. C'est donc logiquement à ce moment que les extorsions se font, de même que les sites Web de paris en ligne reçoivent ces demandes au moment du Super Bowl. Le plus probable est donc qu'Amazon a refusé de payer et que les gangsters ont attaqué l'entreprise par son point le plus faible (Amazon n'a, bien à tort, qu'un seul fournisseur DNS en tout et pour tout).

Quelques articles sur le sujet :

— Rich Miller dans Datacenter KNowledge <http://www.datacenterknowledge.com/archives/2009/12/23/dns-issues-cause-downtime-for-major-sites/>,
— Tom Krazit sur Cnet <http://news.cnet.com/8301-30684_3-10421567-265.html>.