Les développeurs Linux victimes d'une attaque DDoS

Les développeurs réunis cette semaine lors de la conférence Linux Plumbers de Santa Fe (Nouveau Mexique) ont été victimes d'une attaque par déni de service distribué (DDoS), rapporte *ZDNet.com*.

L'attaque qui a débuté le 1er novembre, n'émane pas d'un réseau d'objets connectés compromis, comme celle qui a ciblé le fournisseur de services DNS Dyn le mois dernier, mais d'une attaque DDoS de type SYN *flood*, plus classique. James Bottomley, un ingénieur d'IBM Research et mainteneur du noyau Linux du sous-système SCSI, a confirmé l'information.

H...ACK

Une attaque par déni de service SYN *flood* émet de multiples demandes incomplètes de synchronisation de paquets TCP vers un serveur.

Elle casse le processus de connexion TCP en trois étapes, celles du *« three-way handshake »* (SYN, SYN-ACK et ACK), en ne renvoyant pas de confirmation (ACK). Le serveur attend la réponse qui ne vient pas, les ressources peuvent être saturées et les connexions Internet rendues impossibles.

Une telle attaque informatique, connue depuis plus de 20 ans, est censée être aisément évitable. Mais il semble que le FAI à l'oeuvre lors de la conférence de développeurs Linux n'a pas suivi les recommandations de l'IETF (Internet Engineering Task Force) en la matière.

Lire aussi :

DDoS : Le botnet IoT Mirai a bien participé au raid contre Dyn
48 caractères pour planter les distributions Linux

crédit photo © AndreAnita / Shutterstock