Recrudescence d'attaques DDoS depuis de «vieux» routeurs

Le risque est classé comme moyen. Mais il pourrait prendre de l'ampleur. Les ingénieurs de Prolexic, le bouclier anti-DDoS racheté par Akamai en 2013, ont constaté la recrudescence d'une forme d'attaque par déni de services que l'on pensait abandonnée à ce jour. *« Ce vecteur d'attaque, qui implique l'utilisation du protocole de routage désuet RIPv1, a ressurgi de nouveau le 16 mai après avoir été en sommeil pendant plus d'un an*, indique Bill Brenner du PLXsert, l'équipe du centre de recherches de Prolexis. *Les dernières attaques observées [...] font apparemment usage d'un petit nombre de d'appareils disponibles exploitant RIPv1. »*

RIPv1 est la première version du protocole de routage (*Routing Information Protocol*) écrite en 1988 (dans la RFC1058) et remplacée par sa version 2 en 1996 (RFC1923). Son usage est aujourd'hui déconseillé car s'il permet de partager rapidement et facilement les informations de routage entre les différents routeurs, le protocole est de type «classfull» et ne prend pas en charge les sous-réseaux. De plus, il ne permet pas de gérer l'authentification des sources des mises à jour de routage. *« Pour tirer parti du comportement de RIPv1 dans le cadre d'attaque DDoS par réflexion, une personne malveillante peut fabriquer une demande de requête normale et usurper la source d'adresse IP pour atteindre la cible*, explique l'expert. *La destination correspond une adresse IP issue de la liste des routeurs RIPv1 identifiés sur Internet. Selon les attaques récentes, les attaquants préfèrent les routeurs qui semblent avoir une grande quantité de chemins dans leur table de routage RIPv1. »*

Des pics d'attaque à 12,8 Gbit/s

Conséquence, le PLXsert a constaté des attaques DDoS atteignant des pics de 12,8 Gbit/s à travers 500 routeurs affectés. Un volume qui pourrait s'élever à *« 53 693 sources possibles »* de levier d'attaques, précise le rapport détaillé d'Akamai. Les cyber-criminels peuvent également amplifier les attaques en élargissant la longueur des paquets de réponse jusqu'à 504 octets. *« Nous avons identifié 24 212 appareils sur Internet qui offrent au moins un taux d'amplification de 83% »*, notent les auteurs du rapport.

Bill Brenner invite donc les administrateurs concernés à prendre des mesures défensives. Comment? En basculant leurs routeurs en RIPv2, ou, si ce n'est pas possible, éviter d'exposer le RIP dans l'interface du réseau WAN. Ou encore d'utiliser ACL (access control lists) pour limiter l'usage du port 520 UDP (porte d'entrée de l'attaque) depuis Internet. Et si l'attaque est trop importante, le recours à un prestataire anti-DDoS (comme, au hasard, Akamai) peut devenir incontournable. Selon le fournisseur CDN, les routeurs Netopia fournis ou utilisés par AT&T sont les principaux appareils vecteurs de l'attaque RIPv1 et se concentrent aux Etats-Unis.

Lire également
Attaque DDoS en Europe: record de trafic battu
En 10 ans, les attaques DDoS se sont fortement amplifiées

Une vulnérabilité enrôle massivement pour amplifier les attaques DDoS

crédit photo © Duc Dao – shutterstock