Attaque DDoS en Europe : record de trafic battu

Les infrastructures européennes ont subi, **lundi 10 février**, la plus grosse attaque DDoS (Distributed Denial of Service) de son histoire, rapportent nos confrères de *TechWeekEurope* sur la base d'un rapport de CloudFlare. Selon le prestataire CDN (content delivery networks) américain, **l'attaque a frôlé les 400 Gbit de données envoyées par seconde** sur les réseaux du Vieux Continent. Détenu par l'attaque contre l'éditeur anti-spam Spamhaus en mars 2013, le précédent record de 300 Gbit/s vient donc de tomber.

Les détails de l'attaque ne sont pas connus. CloudFlare laisse entendre qu'un client en particulier a été visé, mais le prestataire n'en révèle pas le nom. Mais, contrairement à l'affaire Spamhaus, la récente offensive n'aurait **pas eu d'impact sur les infrastructures**. Celles-ci *« disposaient de capacités supplémentaires*, assure **Matthew Prince**, le dirigeant de CloudFlare. *Globalement, le réseau n'a pas été affecté »*.

Faille du protocole NTP

OVH a également reporté une attaque massive. *« En ce moment, les DDoS, que notre réseau reçoit, **dépassent largement 350 Gbit/s**… durant des heures »*, a signalé **Octave Klaba**, fondateur et dirigeant de l'hébergeur français, dans un tweet du 11 février. Malgré la concordance calendaire des attaques (qui auraient commencé dimanche soir dernier), rien n'indique qu'il s'agit assurément de la même offensive. Akamai, concurrent direct de CloudFlare, n'a évoqué aucune trace de surcharge réseau de son côté.

La méthode utilisée par les attaquants n'est pas tout à fait nouvelle. Ils se sont servis d'une faille du protocole Network Time (NTP) de synchronisation des horloges systèmes qui **permet de lancer des requêtes d'information sur les clients connectés** et leur trafic en cours (la requête monlist ou MON_GETLIST en l'occurrence). Envoyées en nombre, ces requêtes peuvent générer un trafic massif à même de faire tomber le réseau comme n'importe quelle attaque DDoS.

Quelqu'un dispose d'un nouveau gros canon

Ce qui est relativement innovant, en revanche, c'est l'usurpation d'adresse IP qui **donne l'apparence au système que ces requêtes proviennent de la victime**. Le serveur NTP renvoie alors, en toute confiance, une liste des 600 dernières adresses IP connectées, amplifiant d'autant le trafic. En d'autres termes, une petite requête suffit désormais à provoquer un gros trafic.

*« Quelqu'un dispose d'un gros et nouveau canon. **De vilaines choses sont à prévoir** »*, a commenté, sur Twitter, Matthew Prince, CEO de CloudFlare. Et d'ajouter que *« ces attaques par amplification NTP deviennent vraiment problématiques »*. Si CloudFlare se dit en mesure de contrer les attaques DDoS NTP, l'entreprise recommande de **modifier la configuration des serveurs NTP et des pare-feu**. *« Cela rend le web plus sûr pour tout le monde »*, assure le prestataire.

Lire également

Les attaques DDoS de plus en plus puissantes