Octave Klaba, OVH : « la capacité à filtrer des DDoS de 5 à 6 Tbit/s »

Silicon.fr : Après l'attaque de 1,2 Gbit/s que vous avez subie fin 2016, où en êtes-vous de votre réflexion sur la protection contre les DDoS ?

Octave Klaba : Cela fait environ 18 mois à 2 ans que nous avons pris l'initiative de créer une équipe interne travaillant sur les solutions logicielles et matérielles de nettoyage. Au départ, nous avions intégré une technologie du marché qui nous a permis d'arriver à un premier niveau de filtrage, notamment sur des attaques assez simples de type amplification DNS. C'est ce qu'on a appelé le VAC v1. Mais, nous savions alors que nous aurions à déployer de nouveaux datacenters, une dizaine environ. Pour éviter d'avoir à multiplier les achats de technologies externes, nous avons donc développé notre propre solution, en embauchant des compétences dédiées. C'est ce qui a donné naissance au VAC v2, mis en place à Gravelines, Varsovie, Singapour et Sydney et qui permet d'encaisser plus de 300 Gbit/s. Cette version a été peu déployée in fine, car nous avons commencé à travailler sur la version 3, basée sur des cartes 100 Gbit/s. Soit, sur ces cartes, une capacité de 80 à 90 millions de paquets par seconde. Notre solution comportant 6 cartes, cela amène la capacité totale à 600 Gbit/s par VAC. Comme nous allons aligner 12 datacenters, on va agréger une connectivité de 5 à 6 Tbit/s. C'est ce que nous sommes en train de déployer actuellement ; la version 3 est actuellement en test à Roubaix et sera prochainement mise en production. En parallèle, on termine l'interconnexion de tous les datacenters afin que tous les VAC fonctionnent de concert. Ce qui est assez complexe.

Pourquoi ?

O.K. : Cela nécessite en particulier des mises à jour du réseau, et des configurations assez pointues, car on veut filtrer les éventuelles DDoS au plus près de l'émission. Par exemple, si le flux arrive de Seattle, c'est notre datacenter sur la côte ouest des Etats-Unis qui va le réceptionner et filtrer les éventuelles attaques DDoS. Ce qui permet d'utiliser l'ensemble des capacités des datacenters et d'orchestrer les opérations de nettoyage. Après l'interconnexion, on remplacera les VAC de génération 1 et 2 par la dernière version. L'ensemble du dispositif devrait être prêt en mars prochain.

En même temps, OVH arrive en Asie où les capacités réseau coûtent très cher et où chaque opérateur est maître chez lui. Tout l'enjeu pour nous consiste à nettoyer le trafic pour nos clients sur place sans subir de surcoûts en bande passante. Faire participer nos systèmes anti-DDoS européen et américain à cette protection masque donc aussi un enjeu économique. Cette protection globale, dont le coût sera bien inférieur à celle offerte par les acteurs locaux, devrait nous permettre de faire la différence commercialement.

Echangez-vous avec d'autres acteurs sur la protection anti-DDoS ?

O.K. : Non, même si cela aurait été souhaitable. Les informations sur les attaques DDoS sont généralement très confidentielles. Nous avons choisi de sortir du bois parce que nous avons identifié des phénomènes intéressants, comme l'arrivée des DDoS basés sur des objets connectés.

Mais, pour beaucoup, cela signifie qu'OVH s'est fait hacker ou a été attaqué, alors que nous avons simplement protégé un de nos clients.

Le blogueur spécialisé en cybersécurité Brian Krebs explique que l'auteur de Mirai (le malware employé pour constituer des botnets d'objets connectés) vendrait également des services de protection contre les DDoS. Avez-vous une réaction ?

O.K : En 2012-2013, on subissait des attaques DDoS qui provenait d'un de nos concurrents ciblant certains de nos clients avec des DDoS pour tenter de les récupérer…

Au-delà des DDoS, OVH se sent-il concerné par la menace des attaques étatiques ?

O.K. : Forcément. D'abord, dans nos métiers, seuls les paranos survivent. Ensuite, nous hébergeons les données de nos clients, leur confiance est la base de notre métier. Notre propre sécurité interne est la clef du contrat commercial et moral avec nos clients. Nous travaillons comme si les hackers étaient déjà à l'intérieur d'OVH ; ce sont des mesures que nous avons prises après des attaques subies voici 5 ou 6 ans. Même si c'est un coût et que cela ajoute des contraintes dans nos modes de fonctionnement. Tous les administrateurs sont par exemple sous la norme PCI-DSS. On teste aussi régulièrement l'ensemble des salariés pour voir comment ils réagissent à des menaces, comme du phishing.

A lire aussi :

DDoS : la menace de moins en moins fantôme

FPGA : l'arme secrète d'OVH pour parer les attaques DDoS