Face aux botnets IoT, les opérateurs vont devoir collaborer, selon Arbor

D'année en année, les attaques DDoS progressent. Comme un métronome, Arbor Networks livre son rapport annuel sur la sécurité des infrastructures (WISR) recensant les différentes campagnes en saturation. La 12ème édition prend une teinte particulière. « *Surtout sur la fin de l'année* », rapporte Eric Michonnet, directeur Europe Centrale, du Sud et Afrique du Nord chez Arbor Network (photo ci-contre). Il fait référence à l'apparition des botnets IoT dont le plus connu, Mirai, détient un palmarès déjà riche avec Brian Krebs, OVH ou le gestionnaire de DNS Dyn aux Etats-Unis.

Jusqu'à 5 Tbps et des vieux protocoles réseaux

Le fait marquant est que la puissance de frappe des attaques en déni de service a explosé. Le rapport évoque une campagne à 800 Gbps, soit une progression de 60% par rapport à 2015. Sur 11 ans, la taille des offensives a cru de de 7900%. Et le futur est plutôt pessimiste. « *L'attaque sur OVH a montré des débits pouvant atteindre 1 Tbps* », constate le dirigeant. Il ajoute qu'Arbor Networks se prépare en 2018 « *à mitiger des attaques pouvant aller jusqu'à 5 Tbps* ».

Les botnets IoT ont clairement changé la donne. « *La surface d'attaque est énorme, la seule limite est le tuyau d'entrée de ces attaques via les objets connectés. Mais il est probable que certains pans de l'Internet vont être submergés* », souligne Eric Michonnet. Pour expliquer ce déferlement, il pointe du doigt l'existence de vieux protocoles réseaux qui font aujourd'hui le régal des cybercriminels. « *A l'amplification DNS et les horloges réseaux, on voit de plus en plus l'usage de protocoles comme SMB, qui fait de la remontée d'informations machines ou le SSDP pour la découverte d'adresse réseau. Ce dernier date de 1982.* » Une remise en question de l'architecture réseau du Web est à mener pour éviter les risques d'attaques distribuées. Outre l'aspect réseau, il souligne également la difficulté à « *nettoyer* » les vecteurs trop divers et diffus de l'IoT. « *Caméras de surveillance, domotique, wearables, sont autant de vecteurs qu'il est difficile de patcher.* » A cela s'ajoute la publication du code source de Mirai, une aubaine pour les cybercriminels.

Une collaboration entre opérateurs nécessaire

Pour résoudre le problème, la balle est aussi dans le camp des grands opérateurs, disposant de backbones et vendant du trafic en gros (wholesale), assure le responsable. « *Avec ce niveau de trafic, la question de la bande passante est cruciale, il faut donc aller au plus près de la source de l'attaque pour résoudre le problème.* » Pour lui, pas de miracles : « *Des opérateurs européens se posent la question d'un*

partage d'informations et d'une interconnexion. Une collaboration des transitaires IP peut s'avérer très utile pour accompagner les attaques de grandes ampleurs. »

Les outils d'atténuation de DDoS vont être obligés aussi de s'améliorer. « *Notamment sur les alertes pour proposer aux clients touchés une vision et une analyse en temps réel* », explique Eric Michonnet qui lève le voile sur la roadmap d'Arbor Networks.

Des solutions pour éviter de perdre de l'argent. Le rapport de la société américaine constate qu'un quart des répondants ont vu le coût d'une attaque DDoS majeure dépasser les 100 000 dollars. 5% des sondés voient ce chiffre aller au-delà du million de dollars. La fréquence des attaques est montée de 41% sur un an pour atteindre 21 par mois pour les ISP. Du côté des entreprises et les administrations, il faut tabler sur 10 attaques par mois, soit une progression de 17%. Si on se penche sur les datacenters, ils sont la cible de plus de 50 attaques par mois.

A lire aussi :

DDoS : la menace de moins en moins fantôme

Leet : un botnet IoT plus effrayant que Mirai arrive

Crédit Photo : Lightspring-Shutterstock