Akamai dissèque l'attaque du botnet Mirai contre Krebsonsecurity

A l'occasion de son *State of the Internet Report* pour le 3e trimestre, Akamai est revenu en détails sur l'attaque DDoS de Krebsonsecurity, le site du journaliste spécialisé en sécurité Brian Krebs, en septembre dernier. Une attaque massive et record qui avait poussé le prestataire CDN à ne plus assurer la protection du site du journaliste dont les informations, notamment remontées du darkweb, dérangent à plus d'un titre l'activité des cybercriminels. Rendre son site inaccessible est donc un moyen de faire taire le reporter. Mais ce dernier a trouvé refuge auprès du Project Shield, un programme de Google visant à aider les journalistes à lutter contre la censure en ligne.

Cette analyse détaillée de l'attaque de Krebsonsecurity est exceptionnelle. D'habitude, le rapport d'Akamai ne s'attarde pas de manière personnalisée sur les dénis de services distribués visant ses clients. Il est vrai cependant que Brian Krebs n'est plus client et qu'il l'était à titre gratuit depuis 4 ans ce qui peut laisser penser que le prestataire s'autorise cette liberté qui risque fort bien de rester une exception. Néanmoins, l'optimiseur de contenus web peut d'autant plus se permettre cette indiscrétion que Brian Krebs s'était déjà chargé de décrire l'attaque massive dont il avait été victime le 20 septembre. Akamai rapporte donc sa version de l'événement, avec l'autorisation de l'intéressé.

Un botnet Mirai de 24 000 objets

Akamai confirme donc que l'attaque DDoS de Krebsonsecurity a été menée en partie à partir d'un botnet de 24□000 objets connectés piratés par le malware Mirai, essentiellement des caméras de surveillance et leurs enregistreurs numériques. Cette opération a généré une charge de 623 Gbit/s. « *L'attaque la plus élevée jamais atténuée par Akamai* », déclare le prestataire. Et un nouveau record de persécution d'un client du CDN jusqu'alors établi à 555 Mbit/s… le 22 septembre, lors d'une autre attaque visant le média de Brian Krebs.

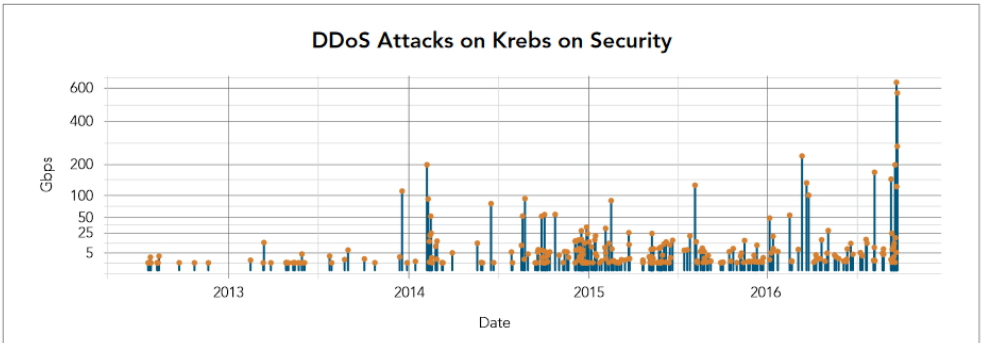

Figure 2-6: All attacks mitigated for krebsonsecurity.com while on the routed platform

« *Cette attaque de 623 Gbit/s s'est traduite par des débordements (floods) de GRE (Generic Routing Encapsulation, NDLR), de SYN (demande de synchronisation, NDLR), et ACK (accusé de réception, NDLR) au niveau réseau, et de PUSH et GET sur la couche applicative*, indique Akamai. *Aucun de ces protocoles n'est*

difficile à atténuer individuellement, mais le volume de cette attaque était impressionnant. Le trafic GRE un vecteur inhabituel, seulement observé à travers une poignée d'attaques chaque année, et ce fût la seule attaque contre le site à utiliser ce protocole. »

Des serveurs C&C très distribués

Akamai a par ailleurs découvert que les serveurs de commande & contrôle (C2 ou C&C) de Mirai étaient suffisamment distribués. Au moment du pique de l'attaque, un botnet était par exemple sous contrôle de 30 adresses IP C2. Par ailleurs, si le botnet apparaît comme segmenté, ses composants peuvent travailler de concert. Et envoyer, dans la majorité des cas, des attaques issues de petites portions du réseau d'objets compromis, comme, plus rarement, des attaques de l'ensemble du botnet. Au final, ce réseau zombie est capable de générer dix types d'attaques différents (2 débordements UDP, 2 type de GRE, deux autres de ACK, un SYN, un DNS, une attaque Valve Engine et même HTTP). Une onzième méthode a été détectée dans les commentaires de l'échantillon examiné par Akamai mais pas exploitée.

Si les flux de charge sont venus d'un peu partout dans le monde (avec pas moins de 210□000 adresses IP recensées à travers les 4 dernières attaques contre Krebsonsecurity analysées), la Colombie s'est révélée être une source majeure de l'attaque. Le pays a contribué à hauteur de près de 15% de l'ensemble des sources d'attaques alors qu'il ne compte «□que□» 5% du trafic généré par Mirai. Akamai n'explique pas ce fait et s'étonne de l'absence des Etats-Unis dans le top 10 des pays attaquants. Probablement grâce au faible nombre de système compromis.

269 attaques en 4 ans

Le rapport nous apprend également que, en 4 ans, le site du journaliste a subi 269 attaques. Dont une douzaine qui ont dépassé les 100 Gbit/s. Des attaques dont l'envergure s'est accélérée en 2016, notamment en mars et août avec 4 «□méga-attaques□», et qui a explosé en septembre avec 5 charges entre 123 Gbit/s et 623 Gbit/s. Celle qui a poussé Akamai à jeter l'éponge et qui confirme, s'il en était besoin, le sérieux du travail de Brian Krebs. La rançon du succès, en quelque sorte.

Lire également
Botnet Mirai : Un gamer mécontent derrière l'attaque DDoS contre Dyn
Le botnet IoT Mirai s'essouffle victime de son succès
DDoS : le code du botnet IoT Mirai mis en libre-service