Augmentation de 140% des attaques DDoS à plus de 100 Gbit/s en 2016

Si le volume d'attaques DDoS n'a progressé que de 4% entre les quatrièmes trimestres respectifs de 2015 et 2016, le nombre d'attaques par déni de service distribué à plus de 100 Gbit/s a explosé de 140% en un an. Soit 12 attaques de ce type contre 5 un an plus tôt, constate Akamai dans son rapport sur l'état de la sécurité Internet au quatrième trimestre 2016.

Un nombre certes anecdotique en regard des 3 826 charges DDoS contenues par l'opérateur de CDN (content delivery networks) sur les trois derniers mois de 2016. Mais cette minorité cache une puissance de feu phénoménale. La plus importante d'entre elle a été mesurée à 517 Gbit/s. Et elle ne venait pas d'un réseau perverti d'objets connectés comme ce fut le cas au troisième trimestre 2016 avec Mirai. Ce malware avait notamment orchestré une attaque du site du journaliste spécialisé Brian Krebs à 623 Gbit/s. Un record, selon Akamai.

Spike concurrent de Mirai

Dans le cas plus récent, l'attaque a été lancée à partir de Spike, un botnet « traditionnel » (non-IoT) qui sévit sur le réseau depuis plus deux ans. Néanmoins, 7 des 12 attaques à plus de 100 Gbit/s restent attribuées à Mirai qui profite de la faible sécurité des objets connectés (notamment les caméras de surveillance et enregistreurs numériques) pour alimenter son réseau malveillant.

Un tir de puissance sensiblement affaibli qui peut laisser penser à une amélioration de la situation. D'autant que la tendance se confirme entre les troisième et quatrième trimestres 2016. Le nombre d'attaques DDoS a diminué de 16% et celles supérieures à 100 Gbit/s sont passées de 19 à 12 (-37%). Mais ce ne serait qu'un recul pour mieux sauter. *« Notre analyse du 4e trimestre 2016 montre bien que notre vieil adage « Attendez-vous à l'inattendu » est toujours d'actualité en matière de sécurité Web*, prévient Martin McKeay, Senior Security Advocate et éditeur du rapport d'Akamai. *Les pirates qui maîtrisent Spike, par exemple, peuvent avoir été tentés de relever le défi Mirai afin de devenir plus compétitifs. Dans ce cas, l'industrie doit s'attendre à voir d'autres opérateurs de botnet tester les limites de leurs moteurs d'attaque, générant des attaques d'encore plus grande ampleur. »* Les prochains trimestres confirmeront, ou non, ces craintes.

Lire également
Akamai renforce ses défenses anti bot avec Cyberfend
Akamai dissèque l'attaque du botnet Mirai contre Krebsonsecurity
DDoS : la menace de moins en moins fantôme