Conficker, Sality et Dorkbot principaux botnets DDoS au début 2016

Si 2015 a marqué une nouvelle année record en matière d'attaques DDoS (Distributed Denial of Service), notamment avec des pointes à 500 Gbit/s de trafic, 2016 s'annonce plus meurtrière encore. Check Point rapporte ainsi avoir identifié plus de 1 500 familles différentes de malwares pour le seul mois de janvier, *« accentuant la tendance croissante que nous avons constaté à la fin de l'année dernière »*. En décembre 2015, l'éditeur de sécurité dénombrait une hausse de 25% des agents malveillants actifs sur le réseau.

Conficker et Sality arrivent en tête des malwares les plus couramment utilisés pour mener des attaques par dénis de service distribués. *« Ce n'est pas une surprise alors que Conficker et Sality ont occupé le haut du classement des logiciels malveillants au cours des derniers mois »*, indique Check Point. Le premier, que l'on retrouve dans 24% des attaques identifiées, met les machines infectées au service des botnets, et désactive les fonctions de sécurité. Le second, Sality, est un virus persistant qui autorise des opérations à distance, notamment l'installation d'autres malwares.

Les attaques DDoS toujours plus efficaces

Si Conficker et Sality sont des vieux de la vielle, la troisième place du classement est occupée par un (relativement) nouveau venu, Dorkbot, à hauteur de 5% des attaques de janvier. Ce malware malmené en décembre dernier par les équipes de Microsoft est à la base un ver IRC programmé pour voler des données sensibles (dont les mots de passe). Il a ensuite été utilisé pour lancer des attaques DDoS. Et, comme il se doit, permettre l'exécution d'opération à distance sur la machine infectée et y installer d'autres bestioles infectieuses. *« La montée croissante de Dorkbot montre que les pirates utilisent de plus en plus le modèle DDoS pour faire tomber les [sites des] entreprises, ce qui prouve l'efficacité de cette méthode d'attaque populaire »*, commente l'éditeur.

Et cela pourrait être bien pire. Surtout si les attaquants exploitent les failles des protocoles réseau pour amplifier leurs attaques par phénomène de réflexion. Lequel consiste à envoyer une requête volontairement mal formulée avec la référence du site visé par l'attaque pour générer une réponse souvent plus lourde que la demande initiale. L'envoi massivement répété de ce type de réponse peut faire tomber le site web de la cible, du moins si ses services sont mal configurés (ce qui est souvent le cas tant que les entreprises n'ont pas subi une première attaque).

Lire également
Les attaques DDoS atteignent des sommets en 2015
12% des attaques DDoS menées par des concurrents
Quand les attaques DDoS servent à leurrer les équipes IT

crédit photo © Duc Dao – shutterstock