CONTACTS PRESSE :
Fabien Rouillon
Eskenzi
+33 1 83 62 88 10
fabien@eskenzipr.com

Bertrand de Labrouhe
Imperva
bertrand.delabrouhe@imperva.com
+33 1 70 15 07 99

Rapport sur le paysage mondial des menaces DDoS pour le 1er trimestre 2016

Chaque attaque DDoS neutralisée est une invitation pour ses auteurs à intensifier leur assaut. C'est là la réalité du secteur de la protection DDoS et l'explication de bon nombre des tendances que nous observons aujourd'hui dans le paysage des menaces DDoS.

Nous publions ces informations dans le cadre de la dernière édition en date de notre rapport sur le paysage mondial des menaces DDoS, où nous analysons des données concrètes relatives à des milliers d'attaques contre nos clients.

Le rapport aborde les tendances les plus récentes en matière d'attaques au niveau des couches réseau et application, ainsi que l'évolution de l'activité des botnets DDoS.

>> Lire le rapport complet (aucune inscription requise)

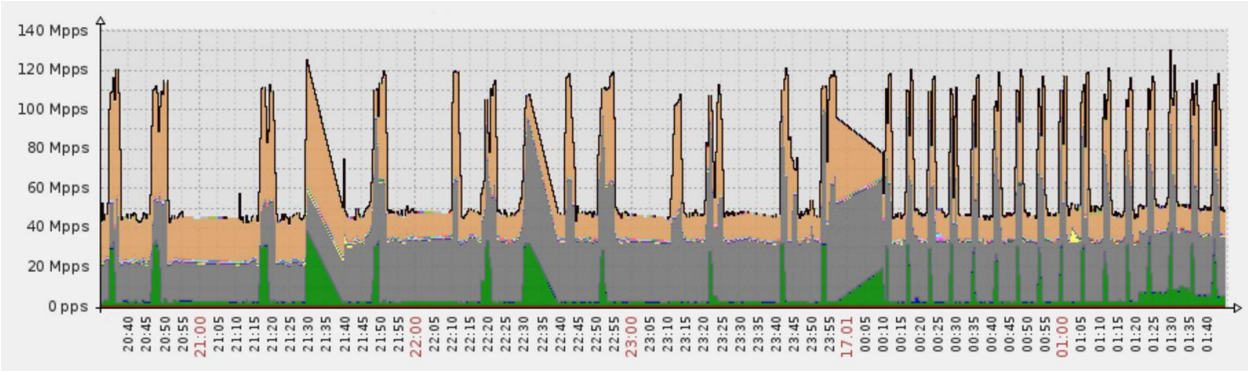
Couche réseau : attaques multivecteurs à très haut débit (Mpps ou Gbit/s)

Dans notre précédent rapport, nous attirions l'attention sur un nombre croissant d'attaques DDoS de type « flood » à très haut débit lancées contre nos clients au niveau de la couche réseau. Dans ce type d'attaques, des paquets de données de petite taille, ne dépassant généralement pas 100 octets, sont émis à un rythme extrêmement élevé de façon à saturer la capacité des commutateurs réseau, ce qui aboutit à un déni de service pour les utilisateurs légitimes.

La vitesse d'émission des paquets est mesurée en Mpps (millions de paquets par seconde). Au 1er trimestre 2016, la fréquence de ces attaques présentant un nombre élevé de Mpps a été sans précédent. En moyenne, nous avons neutralisé une attaque de plus de 50 Mpps tous le quatre jours et une de plus de 80 Mpps tous les huit jours. Plusieurs de ces attaques ont franchi le cap des 100 Mpps, la plus intense culminant à plus de 120 Mpps.

Nous pensons que ces attaques à très haut débit sont une tentative pour mettre en échec les solutions de neutralisation DDoS de la génération actuelle.

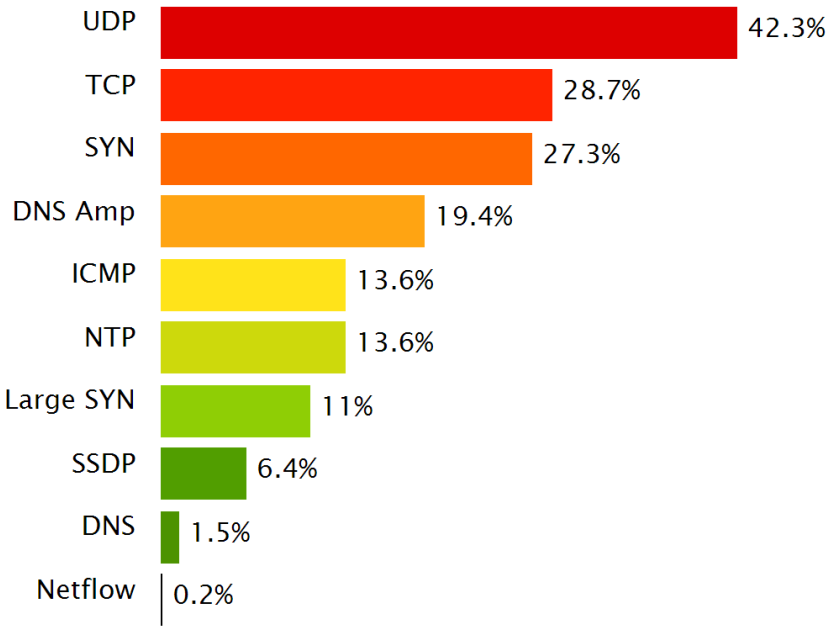
A l'heure actuelle, la majorité des services et appliances de neutralisation sont d'une grande efficacité face aux assauts présentant un nombre élevé de Gbit/s. Cependant, comme les auteurs des attaques s'en rendent compte, bon nombre de ces mêmes solutions n'offrent pas une capacité identique contre les très hauts débits de paquets, car elles n'ont pas été conçues pour en traiter un volume aussi important.



Attaque à très haut débit de paquets sur la couche réseau, culminant à plus de 120 Mpps

Fait intéressant, nous avons également observé l'emploi fréquent d'une combinaison de différents vecteurs pour constituer des assauts plus complexes, avec un débit élevé à la fois en Mpps et en Gbit/s.

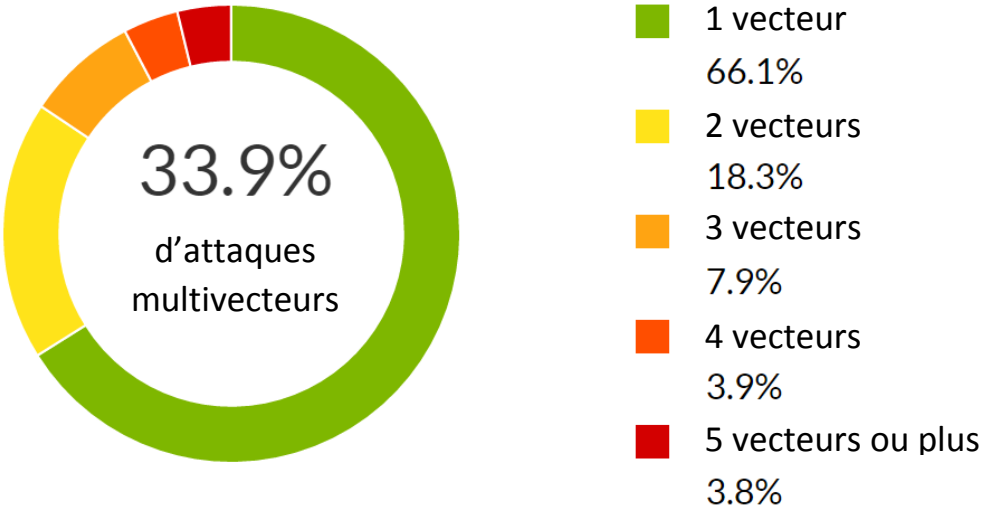
Le scénario le plus courant ici est la combinaison d'une attaque de type UDP Flood à très haut débit et d'une attaque par amplification DNS, grosse consommatrice de bande passante. En conséquence, au 1er trimestre 2016, la fréquence des attaques par amplification DNS a augmenté de 6,3 % par rapport au trimestre précédent.



Répartition des vecteurs d'attaque DDoS par fréquence

En outre, nous avons également constaté un accroissement notable du nombre d'attaques multivecteurs.

Globalement, celles-ci ont représenté 33,9 % de l'ensemble des assauts sur la couche réseau, soit une hausse de 9,5 % par rapport au trimestre précédent. En termes absolus, le nombre d'attaques multivecteurs est passé de 1326 au 4ème trimestre 2015 à 1785 au 1er trimestre 2016.



Répartition des attaques DDoS sur la couche réseau par nombre de vecteurs d'attaque employés

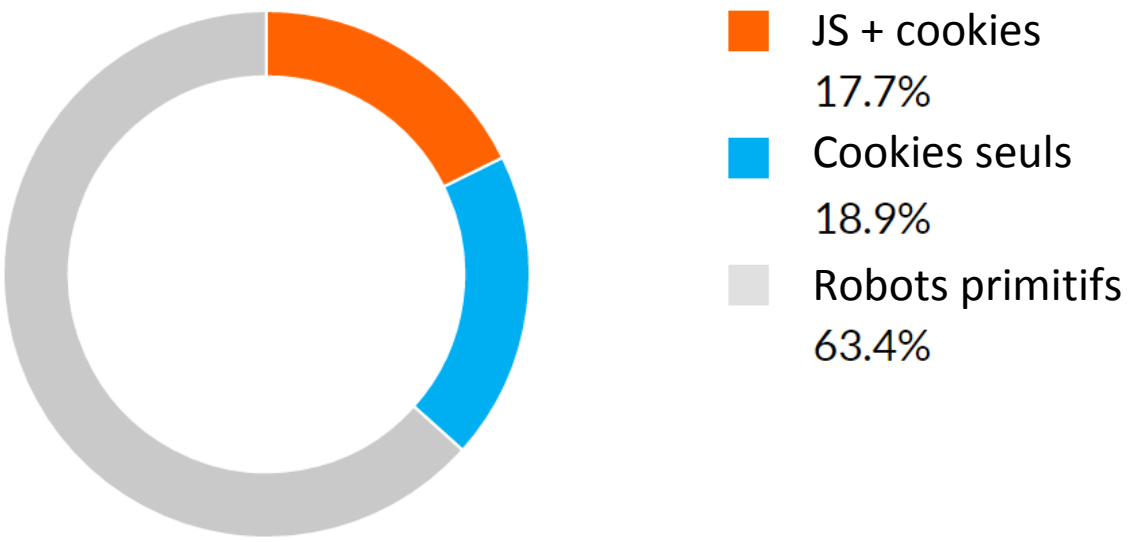
>> Lire le rapport complet (aucune inscription requise)

Couche application : des robots DDoS plus malins

A l'instar des attaques DDoS sur la couche réseau, nous avons vu au premier trimestre 2016 les auteurs d'attaques passer à la vitesse supérieure et se concentrer sur des méthodes susceptibles de contourner les mesures de sécurité. La meilleure illustration en est une augmentation du nombre de robots DDoS capables de se glisser au travers des mailles du filet, à savoir les tests couramment utilisés pour filtrer le trafic d'attaque.

Au 1er trimestre 2016, le nombre de ces robots a explosé pour atteindre 36,6 % du trafic total des botnets, contre 6,1 % au trimestre précédent. Dans le détail, 18,9 % étaient capables d'accepter et de conserver des cookies, tandis que les 17,7 % restants pouvaient également interpréter du code JavaScript.

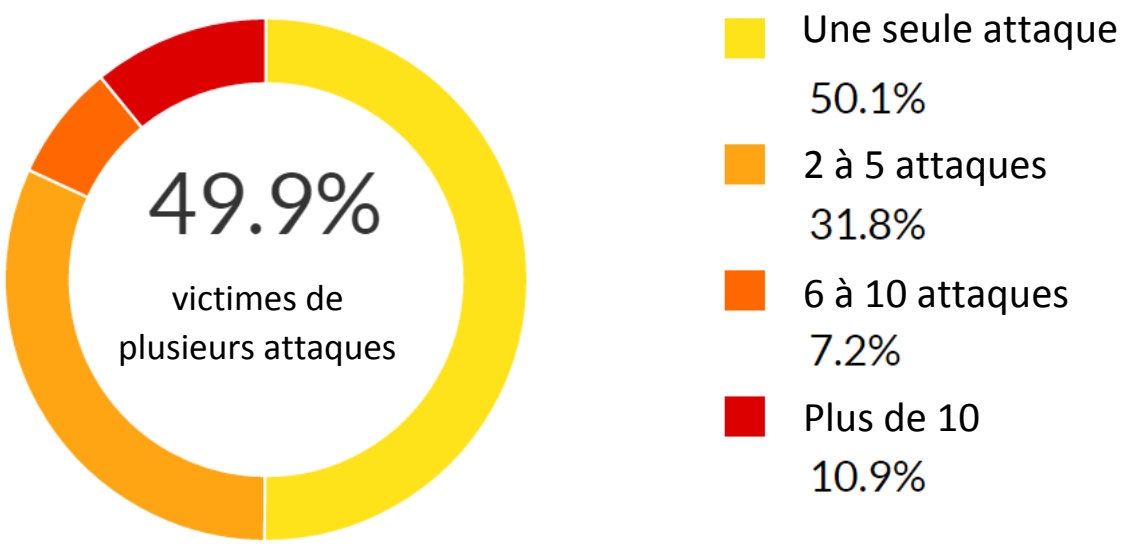
De telles capacités, combinées à une empreinte HTTP d'apparence authentique, rendent les robots malveillants indétectables par la plupart des méthodes.



Répartition des sessions d'attaque sur la couche application en fonction des capacités des robots

En dehors de l'utilisation de robots plus sophistiqués, les assaillants explorent de nouvelles méthodes d'exécution des attaques sur la couche application. Les plus notables d'entre elles sont de type HTTP/S POST flood, employant des requêtes très longues pour tenter de saturer la connexion réseau de la cible.

Enfin, nous avons également observé un accroissement continu de la fréquence des assauts. Au premier trimestre 2016, un site sur deux victime d'une attaque a été ciblé plusieurs fois. Le nombre de sites attaqués entre deux et cinq fois est passé de 26,7 % à 31,8 %.



Répartition par fréquence des attaques contre une cible

>> Lire le rapport complet (aucune inscription requise)

Paysage des botnets : la Corée du Sud en tête des pays à l'origine des attaques

A partir du deuxième trimestre 2015, nous avons enregistré une forte recrudescence de l'activité des botnets DDoS provenant de Corée du Sud, une tendance qui s'est poursuivie ce trimestre. Cette fois, étant à l'origine de 29,5 % de l'ensemble du trafic DDoS sur la couche application, le pays s'est hissé en tête de liste des attaquants.

Pays ciblés		Pays attaquants	
Etats-Unis	50,3 %	Corée du Sud	29,5 %
Royaume-Uni	9,2 %	Russie	10,8 %
Japon	6,7 %	Ukraine	10,1 %
Irlande	5,2 %	Vietnam	7,6 %
Canada	3,2 %	Chine	6,2 %
Allemagne	3,1 %	Etats-Unis	5,7 %
France	2,9 %	Thaïlande	2,0 %
Pays-Bas	2,9 %	République tchèque	1,9 %
Hong Kong	2,4 %	Colombie	1,7 %
Australie	1,5 %	France	1,4 %

Un examen plus approfondi des données révèle que la majorité du trafic d'attaque émanant de Corée du Sud provient de botnets Nitol (52,9 %) et PCRat (38,2 %). Plus de 38,6 % de ces attaques ont été lancées contre des sites web japonais et 30,3 % contre des cibles hébergées aux Etats-Unis.

Il est intéressant de noter, au cours de ce trimestre, une forte augmentation de l'utilisation de Generic!BT bot, un cheval de Troie connu pour infecter les ordinateurs Windows. Celui-ci a été identifié pour la première fois en 2010 et nous voyons aujourd'hui ses variantes employées pour pirater des machines dans le monde entier.

Au 1er trimestre 2016, des variantes de Generic!BT ont ainsi été utilisées dans des attaques DDoS issues de 7756 adresses IP distinctes réparties dans 52 pays, principalement en Europe de l'Est. La majorité de cette activité a été tracée jusqu'en Russie (52,6 %) et en Ukraine (26,6 %).

>> Lire le rapport complet (aucune inscription requise)

Conclusion : des attaques conçues contre les solutions de neutralisation

Les années précédentes, la plupart des attaques observées avaient pour but de causer un maximum de dommages aux infrastructures ciblées. Il s'agissait typiquement d'assauts de force brute, de type « flood », frappant avec une grande capacité et sans faire de détail. Les attaques plus sophistiquées étaient alors rares.

Cependant, au cours des derniers mois, nous avons enregistré un nombre croissant d'attaques orchestrées par rapport aux solutions de neutralisation DDoS. La diversité des méthodes d'attaque ainsi que l'expérimentation de nouveaux vecteurs semblent indiquer un changement de priorité, les assauts étant de plus en plus conçus pour paralyser les solutions de neutralisation, et non plus uniquement la cible.

D'une part, cela dénote l'omniprésence des services et appliances de protection DDoS, qui sont appelés à devenir partie intégrante de la majorité des périmètres de sécurité. D'autre part, cela illustre également le défi auquel le secteur de la neutralisation DDoS va être confronté : des attaques de plus en plus élaborées qui exploitent les points faibles de ses propres technologies.