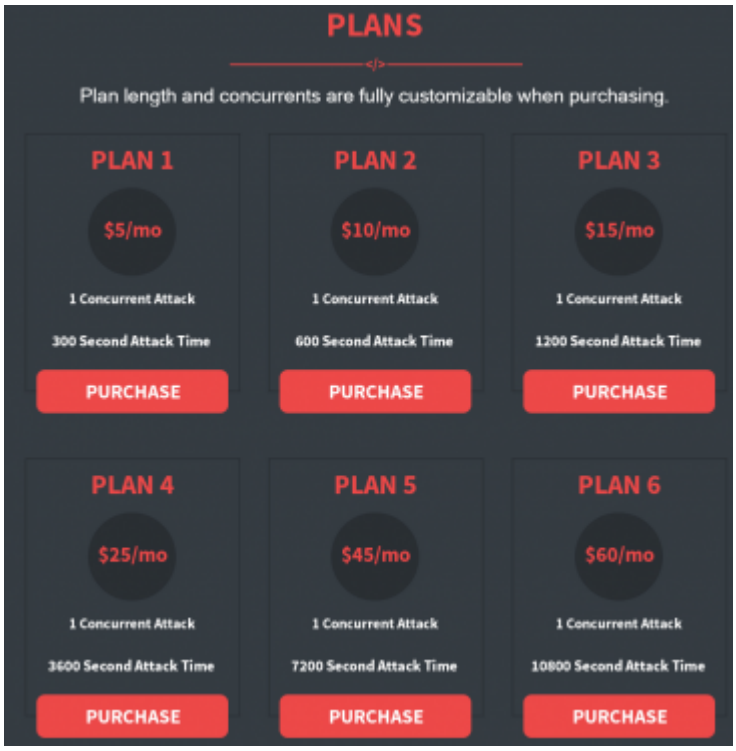
# Les attaques DDoS, l'autre machine à cash des cybercriminels

Les ransomwares sont devenus le gagne-pain des cybercriminels. Les attaques DDoS sont en train de suivre la voie tracée par son coreligionnaire. Kaspersky Lab s'est penché sur le coût et la rentabilité des attaques par déni de service disponibles en mode SaaS sur les places de marché du Dark Web. Et les surprises sont au rendez-vous.

## A partir de 5 dollars pour 5 minutes d'attaque

En moyenne, « *une attaque DDoS coûte 25 dollars de l'heure. En utilisant un botnet d'environ 1000 PC, le prix baisse à 7 dollars de l'heure* », peut-on lire dans le récit de Kaspersky Lab. Mieux des sites proposent des services DDoS low cost sur des durées limitées, « *5 dollars pour une campagne de 300 secondes avec une puissance de 125 Gb/s* ». Et cela peut monter jusqu'à « *400 dollars pour une attaque durant 24 heures* ».




Pour autant, les coûts varient selon plusieurs facteurs. Par exemple, si le service utilise des botnets issus d'objets connectés (de type Mirai), la facture finale sera moins chère qu'en se servant d'un botnet basé sur des serveurs. « *Un botnet de 1000 caméras de surveillance sera moins onéreux en terme d'organisation qu'un botnet de 100 serveurs, car les terminaux IoT sont plus insécurisés et en général oubliés par leurs propriétaires* », souligne les équipes de Kaspersly Lab.

## Des facteurs différenciant

Autre élément impactant le coût, le type de cible et le pays où elle se trouve. En effet, les prix fluctuent en fonction de la protection de la cible face aux attaques par saturation. « *Si la cible se protège avec du filtrage de trafic, les cybercriminels devront mettre en place des mécanismes pour contourner ces protections. Avec au passage une augmentation du prix* », constate l'éditeur.

De même, quand la cible est un site web gouvernemental, le prix d'une attaque est plus élevé. A titre d'exemple, une offensive sur un site web non protégé peut varier de 50 à 100 dollars, alors que sur un site protégé, l'opération peut coûter plus de 400 dollars. La localisation de la cible peut jouer un rôle sur le coût. « *Une attaque DDoS aux Etats-Unis coûtera plus cher qu'une attaque similaire en Russie* », analyse Kaspersky Lab.

## Rentabilité en hausse

Côté rentabilité, l'étude montre que le cybercriminels combine la demande d'une rançon (plusieurs milliers de dollars en bitcoin) et la menace d'une attaque DDoS. « *Ces DDoS ransomware se transforment en une entreprise à marge élevée : la rentabilité d'une attaque peut dépasser les 95%* », indique l'étude. Et d'ajouter : « *Les propriétaires de sites préfèrent payer sans vérifier que la menace est réelle.* » Au final, l'étude de Kaspersky Lab conclut que le coût des attaques DDoS devrait baisser à l'avenir, mais que leur fréquence va augmenter.

**A lire aussi :**

Comment le ransomware est devenu le gagne-pain des cybercriminels

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

**Photo credit: Jason A. Samfield via VisualHunt / CC BY-NC-SA**