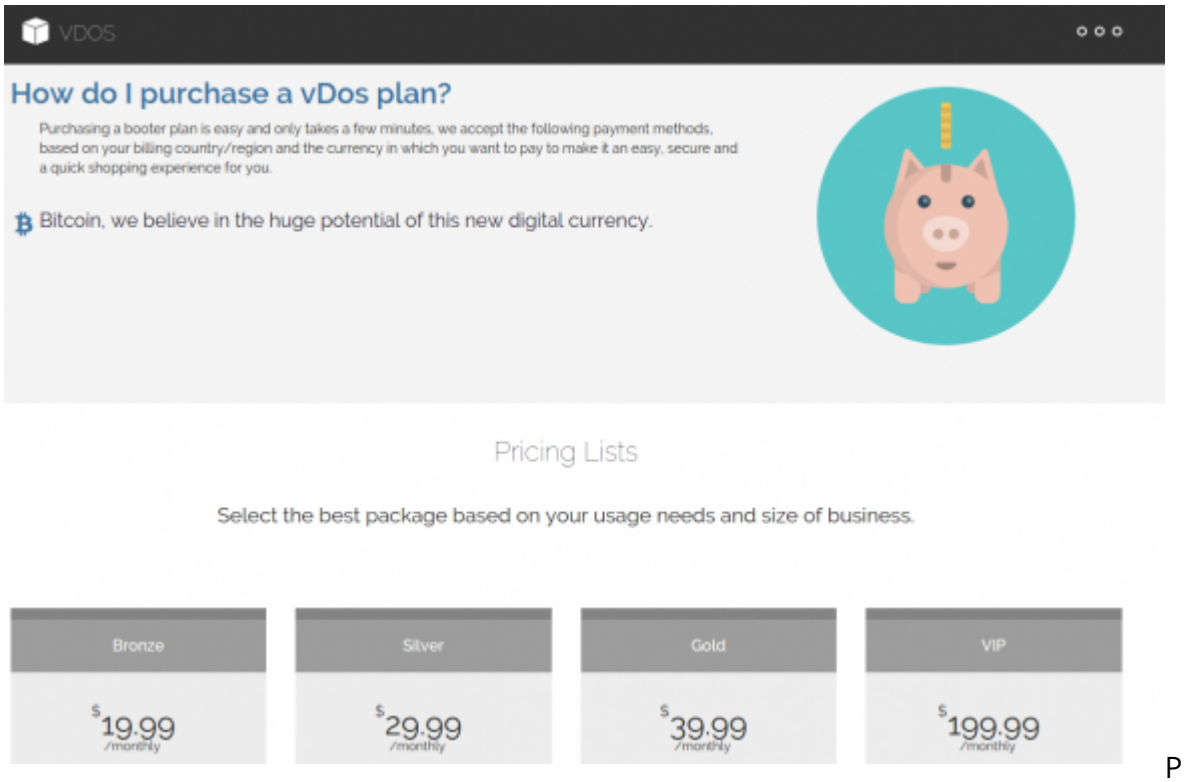
DDoS à vendre : autopsie d'un service de hacking à la demande

Deux jeunes Israéliens de 18 ans ont été arrêtés en fin de semaine dernière, ils sont soupçonnés d'être les organisateurs d'un service appelé vDOS, vendant des attaques par déni de service (DDoS). Les deux hackers ont été relâchés vendredi contre caution, mais doivent éviter toute communication électronique pendant une durée de 30 jours. Cette affaire permet de lever le voile sur le fonctionnement d'un service d'attaque 'as-a-service' comme vDOS. Selon KrebsonSecurity, le blog du journaliste spécialisé Brian Krebs, le service a généré plus de 600 000 $ de chiffre d'affaires en deux ans et a mené quelque 150 000 attaques DDoS visant, dans la plupart des cas, à faire tomber des sites Internet. Le service de hacking était opérationnel depuis septembre 2012.



Promues principalement sur le site spécialisé Hackforums, les offres de vDOS étaient facturées entre 19,99 et 199,99 $ par mois. Les tarifs dépendaient du temps (en secondes) que va durer l'attaque par saturation. Selon Brian Krebs, en quatre mois (de avril à juillet 2016), vDOS a lancé des attaques qui ont totalisé 277 millions de secondes, soit 8,81 ans. Ce qui signifie donc qu'un service comme vDOS était en mesure de lancer plusieurs attaques simultanément.

Le service de hacking hacké

Les secrets de vDOS ont été dévoilés suite à un piratage du service de DDos. Brian Krebs affirme être en possession d'une copie de la base de données, répertoriant les 'clients ' du service ainsi que leurs cibles. Signalons que la société CloudFlare a, de son côté, publié un fichier des logs de vDOS entre avril et juillet 2016 : y figurent le nom de l'utilisateur qui a payé l'attaque, son IP, la nature de son navigateur Internet, l'adresse Internet de la cible, la méthode d'attaque ainsi que sa durée.

vDOS était hébergé sur au moins quatre serveurs loués chez un hébergeur bulgare appelé Verdina.net. Mais reste inaccessible depuis vendredi, le service ayant été ciblé par une attaque BGP (Border Gateway Protocol), une méthode qui permet à un acteur du réseau de capturer l'adresse IP d'un autre. Selon Brian Krebs, c'est la société BackConnect Security qui est à l'origine de ce détournement, une mesure que son Pdg explique par la volonté de stopper une attaque DDoS émanant de vDOS, qui a frappé son entreprise pendant plus de six heures jeudi dernier (avec des débits dépassant les 200 Gbit/s).

Autre 'détail' intéressant : avant d'être mis hors service par l'attaque BGP, vDOS était protégé par CloudFlare, un prestataire offrant aux entreprises… des services de lutte contre les DDoS.

A lire aussi :

L'Internet des objets au service des attaques DDoS

DDoS : 9 attaques sur 10 sont lancées depuis des services à la demande

Bientôt un Bitcoin pour rémunérer les attaques DDoS ?

crédit photo © igor.stevanovic / shutterstock