L’attaque DDoS sur PSN et Xbox Live s’est appuyée sur… des routeurs domestiques

L’attaque DDoS sur PSN et Xbox Live s’est appuyée sur… des routeurs domestiques

Pour réaliser leurs attaques, les pirates de Lizard Squad ont créé un botnet qui s’appuie en majorité sur des modem-routeurs hackés. Leur malware a exploité une faille dans la configuration du système d’exploitation Linux.

Fin décembre dernier, les pirates de Lizard Squad ont mis en ligne un service DDoS payant appelé « Lizard Stresser ». Disponible à partir de 5,99 dollars/mois, cet « outil » avait fait ses preuves quelques jours auparavant, en mettant à genoux les réseaux de Playstation Network et Xbox Live. Mais où ces pirates ont-ils trouvé leur puissance de feu ? Principalement dans les petits routeurs domestiques, révèle ainsi KrebsOnSecurity.com.
Avec l’aide de quelques chercheurs en sécurité, le site spécialisé a réussi à mettre la main sur le malware qui a permis de construire le botnet de « Lizard Stresser ». Le logiciel malveillant exploite ainsi une faille de sécurité dans Linux pour prendre le contrôle d’objets connectés, et se diffuse de proche en proche comme un ver.
Après analyse, il s’avère que les routeurs domestiques sont très largement surreprésentés dans ce botnet, sans doute en raison de leur nombre et de leur faible niveau de protection. En effet, l’un des vecteurs d’infection du malware est d’utiliser les identifiants par défauts de ces équipements grand public, tels que « admin/admin » ou « root/12345 » !

Lizard Squad a également piraté le cloud de Google

Cette découverte montre – une fois de plus – qu’il est important de bien configurer et protéger tous ses équipements informatiques, et pas uniquement ses ordinateurs. Selon une récente analyse de l’éditeur Avast, plus de la moitié des modem-routeurs en France ont conservé leur configuration d’origine, et sont donc potentiellement vulnérables. D’ailleurs, se retrouver avec un modem-routeur zombie fait encore partie des choses les moins désagréables. D’autres pirates utilisent des équipements pour réaliser des attaques par détournement DNS, ce qui permet de quantité de données sensibles : mots de passe, informations bancaires, etc.
Mais Lizard Squad ne s’attaque pas seulement aux pauvres particuliers, mais visent également les géants du web. Selon KrebsOnSecurity, les pirates reptiliens ont utilisés des numéros de carte bancaire volés pour créer, fin décembre dernier, des milliers de serveurs virtuels sur le cloud de Google (« Google Compute Engine »). Cette fois, en revanche, le but n’était pas de faire des attaques DDoS, mais de créer des relais Tor. Ce qui a beaucoup énervé les développeurs de ce service d’anonymisation, car cet ajout massif avait pour effet de le fragiliser. Heureusement, Google a rapidement remarqué le subterfuge.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.01net.com/editorial/640591/l-attaque-ddos-sur-psn-et-xbox-live-s-est-appuyee-sur-des-routeurs-domestiques/
Par Gilbert Kallenborn