Le FBI et Microsoft font trembler le botnet DorkboOscar Barthe

Le FBI et Microsoft font trembler le botnet Dorkbot

En partenariat avec les forces de l'ordre de plusieurs pays comme le FBI et Interpol ainsi que d'autres acteurs IT et télécoms comme Eset, Microsoft a mené une attaque contre les infrastructures du botnet Dorkbot. Le but de l'attaque était, à défaut de l'éradiquer, de perturber son fonctionnement.

Le botnet Dorkbot permet à ses utilisateurs de récupérer les identifiants de connexion de différents services comme Gmail, Facebook, Twitter ou encore Steam.
En partenariat avec les forces de l'ordre de plusieurs pays comme le FBI et Interpol ainsi que d'autres acteurs IT et télécoms comme Eset, Microsoft a mené une attaque contre les infrastructures du botnet Dorkbot. Le but de l'attaque était, à défaut de l'éradiquer, de perturber son fonctionnement.
Microsoft a fait sa bonne action. La firme de Redmond a déclaré jeudi avoir collaboré avec les autorités de plusieurs régions pour perturber le fonctionnement du botnet Dorkbot.
Découvert il y a quatre ans, ce dernier a infecté aujourd'hui plus d'un millions de machine. Il est utilisée pour récupérer les identifiants de connexion de différents services comme Gmail, Facebook, Netflix, PayPal, Steam ou encore eBay. La firme de Redmond ne s'est toutefois pas lancée seule dans l'attaque contre Dorkbot, et a travaillé ainsi avec le fournisseur de solution de sécurité Eset, le Cert polonais Polska, la commission canadienne de Radio-télévision et de télécommunications, l'agence de sûreté américaine, le FBI, Interpol, Europol et la police montée du Canada.
Les utilisateurs sont pour la majeure partie d'entre eux infectés lors de leur navigation sur internet sur des sites pas forcément bien protégés. Dorkbot exploite la moindre faille logicielle via un exploit kit ou les spam. Il peut aussi utiliser un système de ver pour se diffuser à travers les réseaux sociaux, les services de messagerie ou les clés USB.

Une attaque efficace mais pas durable
Microsoft n'a toutefois pas détaillé comment il s'y était pris pour perturber les infrastructures de Dorkbot. Ce n'est d'ailleurs pas la première fois que la firme collabore avec les autorités dans ce genre de situation. Les actions coordonnées visant à déconnecter les serveurs hébergeant les botnet ont souvent un impact immédiat mais les bénéfices ne durent pas. Souvent, les cybercriminels remettent rapidement sur pied une nouvelle infrastructure et s'attaque à la reconstruction du botnet en infectant d'autres ordinateurs.
La situation autour de Dorkbot devenait critique. Ses créateurs ont diffusé un kit permettant d'utiliser le botnet comme base pour en construire d'autres, plus puissants. Baptisé NgrBot, il était en vente sur le deep web.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-le-fbi-et-microsoft-font-trembler-le-botnet-dorkbot-63185.html
Par Oscar Barthe