Le code source d’un puissant programme d’attaques informatiques rendu public

The blackforums post that includes links to the Mirai source code.

Le code source d’un puissant programme d’attaques informatiques rendu public

Jeudi 22 septembre, le blog d'un célèbre spécialiste en sécurité informatique, Brian Krebs, était victime d'une des attaques informatiques les plus puissantes jamais recensées. Samedi 1er octobre, celui-ci a annoncé que le code source du programme ayant permis cette attaque avait été publié en ligne. « Ce qui garantit quasiment qu'Internet sera bientôt inondé d'attaques », prévient-il sur son site.

L'attaque en question était de type DDoS, ou « déni de service ». Elle consiste à saturer un serveur de requêtes afin que celui-ci ne soit plus en mesure de répondre. Celle subie en septembre par Brian Krebs était exceptionnelle par son ampleur : le volume de trafic envoyé vers son site a été estimé à environ 620 gigabits par seconde, alors que les attaques les plus violentes de ces dernières années culminaient à 300 Gbits/s.

Pour parvenir à un tel résultat, les auteurs de l'attaque ont utilisé un « botnet », un réseau de machines ne leur appartenant pas qu'ils ont piratées afin de les faire agir à leur guise. Une méthode classique, mais celle-ci a une particularité : les machines en question n'étaient pas, comme souvent, des ordinateurs, mais des objets connectés, comme des caméras de surveillance. Une cible relativement facile pour les pirates puisque ces objets, connectés en permanence, sont souvent mal sécurisés.

i m a g e :
http://s2.lemde.fr/image/2016/10/03/534x0/5007349_6_8042_2016-10-03-6ab49ca-14116-wlu2v0_5182276b854a344ebf95edab19e0b1b8.png

De nouvelles attaques à prévoir

Le code source du programme ayant permis de constituer et de piloter ce botnet a été divulgué vendredi 30 septembre sur un forum fréquenté par des hackeurs, par un utilisateur se faisant appeler *« Anna-Senpai »*, affirme Brian Krebs. *« Quand je me suis lancé dans le DDoS, je n'avais pas l'intention d'y rester longtemps*, écrit cet utilisateur dans le message accompagnant son geste. *J'ai fait de l'argent, de nombreux regards se tournent désormais vers l'Internet des objets, il est donc temps de GTFO »* (*« Get The Fuck Out »*, à savoir : partir)…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le code source d'un puissant programme d'attaques informatiques rendu public