Le botnet IoT Mirai cible Windows pour mieux se répandre

Des chercheurs en sécurité ont découvert un trojan Windows utilisé pour la distribution du malware Linux Mirai capable d'infecter des objets connectés et réaliser des attaques DDoS massives.

Mirai a été développé entre la fin 2015 et le début 2016, mais il est monté en puissance à l'automne 2016 en infectant des centaines de milliers de routeurs et de caméras de surveillance. Son auteur, pisté par Brian Krebs, a depuis livré le code source du malware, ouvrant ainsi la porte à de multiples variantes et à des améliorations des techniques d'enrôlement.

Une des variantes de Mirai a été détectée par la société russe de sécurité Dr.Web. Il s'agit d'un trojan Windows élaboré dans le seul but d'aider Mirai à se diffuser sur un plus grand nombre de dispositifs. Habituellement, les versions standards de Mirai fonctionnent en infectant un périphérique, via une adresse IP aléatoire. Le malware essayant de se connecter à travers un port Telnet en utilisant une liste d'identifiants admin. D'autres versions ont permis de lancer cette technique de test via SSH. Mais dans tous les cas, Mirai s'attaquait à des équipements fonctionnant avec des OS Linux.

Une surface de tests plus grande

Ce n'est plus le cas, le trojan découvert par Dr.Web aide les cybercriminels à lancer des attaques de détection d'identifiant depuis des terminaux sous Windows. Et cela même si Mirai (fonctionnant sous Linux) ne peut s'exécuter sous Windows. Concrètement, ce trojan sert d'amplificateur en ciblant les terminaux Windows pour trouver et détecter des équipements sous Linux vulnérables. Il cible plus de ports (cf ci-dessous) :

22 – Telnet
23 – SSH
135 – DCE / RPC
445 – Annuaire Active Directory
1433 – MSSQL
3306 – MySQL
3389 – RDP

Dès que le cheval de Troie réussit à compromettre un nouvel objet, si la plateforme tourne sur Linux, il exécute des séries de commandes pour placer Mirai et l'enrôler. Si la plateforme tourne sous Windows, alors il créé une copie de lui-même pour chercher d'autres périphériques sous Linux.

Dr.Web a récemment découvert cette version Windows de Mirai, mais l'éditeur est incapable de savoir quel impact elle aura sur l'écosystème Mirai.

A lire aussi :

Leet : un botnet IoT plus effrayant que Mirai arrive

A louer : un botnet Mirai de 400 000 objets pour lancer des DDoS

Photo credit: wocintechchat.com via Visualhunt