Découverte d’un malware sous Linux derrière un important botnet | Le Net Expert Informatique

Découverte d’un malware sous Linux derrière un important botnet

Réputé plus sûr que Windows, Linux connaît aussi son lot d’attaques, et en connaîtra de plus en plus avec l’augmentation des objets connectés reposant sur une distribution Linux. En témoigne un nouveau malware découvert principalement en Asie, qui forme un botnet capable d’orchestrer des attaques DDOS très puissantes, jusqu’à plus de 150 Gbps.

La firme Akamai a révélé lundi la découverte d’un botnet qui serait capable d’organiser une attaque DDoS de plus de 150 Gbps, formé grâce à un malware qui cible les ordinateurs et serveurs sous Linux. Baptisé XOR DDoS, l’armée de zombies rassemblés par des chevaux de Troie se compose également de nombreux appareils connectés dont la couche logicielle repose souvent sur des systèmes Linux non mis à jour, soit que le service après-vente n’est pas assuré, soit que les utilisateurs n’aient pas le réflexe de mettre à jour le firmware d’un appareil qui semble fonctionner correctement.

Selon Akamai, le malware d’origine asiatique se répandrait grâce aux services SSH d’appareils mal sécurisés tels que de routeurs, qui peuvent être attaqués par force brute (tenter des milliers de mots de passe jusqu’à tomber sur le bon). Chaque accès gagné sur une machine permet de gagner un nouveau relais vers de nouveaux serveurs, et ainsi de suite.

Le botnet XOR DDoS aurait déjà été utilisé de très nombreuses fois (une vingtaine d’attaques par jour dont 90 % vers l’Asie), avec des degrés divers de puissance, allant de flots de données de 2 Gbps à plus de 150 Gbps. Les cibles prioritaires seraient le secteur du jeu d’argent, suivi par les institutions éducatives. Une orientation qui peut être le fait des créateurs du botnet, ou des clients qui louent ses services pour attaquer une URL ou une adresse IP en payant à l’heure et à la puissance d’attaque voulue.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.numerama.com/magazine/34342-decouverte-d-un-malware-sous-linux-derriere-un-important-botnet.html
par Guillaume Champeau