XOR DDoS : une attaque massive générée par un botnet… Linux

Jusqu'à présent relativement épargné, l'environnement Linux est de plus en plus prisé des cybercriminels. Un réseau botnet de machines Linux infectées est aujourd'hui capable de générer une attaque par déni de service distribué (DDoS) dont les capacités peuvent paralyser un réseau d'entreprise. Akamai a ainsi constaté que le botnet pouvait générer des **attaques DDoS de plus de 150 Gbit/s** de bande passante.

Baptisé XOR DDoS, le malware qui structure ce botnet a été découvert en septembre 2014. Il s'installe sur tous types de plates-formes Linux, dont des routeurs ou des NAS. Les attaquants s'introduisent en obtenant les identifiants de connexion par force brute. Une fois dans la place, ils téléchargent et installent XOR avec des commandes basées sur des techniques de rootkit pour masquer leur passage, indiquait l'éditeur Avast dès janvier dernier.

20 attaques par jour

XOR DDoS lance actuellement jusqu'à 20 attaques par jour, indique le fournisseur de CDN (content delivery networks), par voie de blog. Les cibles des attaquants se concentrent principalement sur les secteurs du jeu et de l'éducation. Elles se déroulent pour 90% d'entres elles sur la région Asie. Pour le moment.

Akamai insiste sur le fait que XOR DDoS n'exploite pas une vulnérabilité Linux (comme celles touchant glibc, Bash ou OpenSSL ces derniers temps) mais bien les services SSH (Secure Shell) exposés à des attaques par force brute, qui permettent de déceler les mots de passe trop simples à deviner.

Linux de plus en plus ciblé par les attaques

Même si la faute en revient en partie aux utilisateurs et administrateurs (qui utilisent des mots de passe faibles ou ne changent tout simplement pas les codes par défaut des routeurs), il n'en reste pas moins que XOR DDoS montre la montée en puissance de Linux parmi les plates-formes ciblées par les cybercriminels. *« XOR DDoS illustre la stratégie d'attaquants qui changent de méthodes et construisent des réseaux de zombies en utilisant des systèmes Linux compromis pour lancer des attaques DDoS*, commente Stuart Scholly, vice-président responsable de la division sécurité chez Akamai. *Cela se produit beaucoup plus fréquemment que par le passé, lorsque les machines Windows étaient les principales cibles des malwares pour les attaques DDoS. »* La triste rançon du succès en quelque sorte pour l'OS Open Source.

Lire également
Recrudescence d'attaques DDoS depuis de «vieux» routeurs
Les protocoles Internet de plus en plus exploités par les attaques DDoS

Une faille BIND ouvre la voie aux attaques DDoS des serveurs DNS

crédit photo © Duc Dao – shutterstock