Les équipements réseau menacés par le malware Linux/Moose

Le malware **Linux/Moose** fait l'objet d'un article détaillé sur le blog sécurité **d'ESET**. Les experts de la société ont mis en lumière cette nouvelle menace, qui infecte les équipements réseau fonctionnant sous Linux.

Moose ne s'appuie par sur une faille de sécurité de Linux, mais sur les identifiants d'accès prévisibles de certains outils réseau. Ainsi, **nombre de boxes ADSL utilisent 'admin'** comme mot de passe administrateur. Ce n'est pas une faille en soi, l'interface du routeur n'étant pas accessible depuis la Toile. Sauf si l'ennemi vient de l'intérieur, via un PC infecté par exemple.

Avant de s'installer, Moose s'assure que les ressources nécessaires sont disponibles sur le routeur. Une fois en place, il se charge **de trouver d'autres victimes à infecter**. De par sa nature même (qui consiste à ne s'insinuer que sur des produits mal protégés), il ne menace en général que les routeurs.

Fraude aux réseaux sociaux

Moose capte à la volée **les cookies de connexion** des utilisateurs du foyer. Il les utilise essentiellement pour **générer des likes** sur les pages de certains comptes de réseaux sociaux. Certains pirates sont visiblement tellement en mal de reconnaissance qu'ils en viennent à demander à des routeurs de les aimer !

La parade pour contrer ce malware est simple : **redémarrez votre passerelle réseau** et changez son mot de passe administrateur aussi rapidement que possible. Actuellement, Moose ne modifie en effet pas le *firmware* des équipements réseau. Il ne survivra donc pas à un *reboot*.

À lire aussi :
Pertes de données pour Linux 4.0 sur les systèmes Raid
Une faille d'un client WiFi expose Android, Linux et BSD
Linux 4.0 inaugure la mise à jour à chaud du noyau

Crédit photo : © ESET