Un ver informatique cible les routeurs Linksys

Le SANS Institute (SysAdmin, Audit, Network, Security), une organisation regroupant 165 000 professionnels de la sécurité visant à mutualiser l'information sur ces sujets, signale l'existence d'un ver informatique exploitant une **vulnérabilité du système d'authentification** de certains routeurs Linksys. Ce malware, baptisé **TheMoon**, se sert d'une **faiblesse d'un script CGI utilisé dans l'interface d'administration** de nombreux modèles de routeurs Linksys de la série E. Dans un post, le responsable technologique du SANS Internet Storm Center (ISC) signale que la faille peut toucher les modèles suivants : E4200, E3200, E3000, E2500, E2100L, E2000, E1550, E1500, E1200, E1000 et E900.

La construction d'un botnet ?

Dans son alerte sur le réseau SANS publiée la semaine dernière, un administrateur d'un FAI du Wyoming signale que plusieurs de ses clients ont vu leurs routeurs Linksys compromis ces derniers jours. Une fois infectés, les matériels concernés se mettent à **scanner les ports 80 et 8080 saturant la bande passante**. Pour l'instant, les motivations des assaillants restent inconnues, même si le code source du ver suggère l'existence de serveurs de contrôle et commande, qui pourraient utiliser les routeurs infectés pour bâtir un botnet.

Linksys indique travailler à un patch. En attendant, le constructeur a publié un billet afin d'inciter les utilisateurs à **ajuster la configuration des routeurs** pour diminuer le risque d'infection (par exemple en interdisant l'administration à distance).

Le mécanisme d'infection de ce ver, qui bypasse le mécanisme d'authentification, rappelle une autre faiblesse des routeurs Linksys, découverte en janvier par l'ingénieur en sécurité français Eloi Vanderbeken**.** Celle-ci résidait dans l'emploi d'un port exotique (le 32764) pour commander à distance le matériel.

Mise à jour à 14h40 : selon un membre du site communautaire Reddit, ce n'est pas un mais quatre scripts CGI qui sont susceptibles de présenter des vulnérabilités, dont deux ont donné naissance à un exploit signé d'un auteur se présentant sous le pseudonyme de Rew. Au passage, la liste des matériels concernés s'est agrandie, incluant désormais des modèles de la série Wireless-N.

En complément :

– Toute l'actualité de la sécurité IT sur Silicon.fr