Des Box pourraient être piratées pour mener des attaques DDOS ?

Des Box pourraient être piratées pour mener des attaques DDOS ?

Eset a signalé l'activité d'un ver exploitant une faiblesse du protocole de gestion réseau distant Telnet implémenté dans les routeurs domestiques sous Linux. Des pirates peuvent s'en servir pour construire un botnet et lancer des attaques DDoS.

Construire des botnets à partir de routeurs, modems, points d'accès sans fil et autres terminaux réseaux ne nécessite pas d'exploits très sophistiqués. C'est le cas par exemple de Remaiten, un nouveau ver exploitant les routeurs domestiques sous Linux en tirant partie d'une faiblesse liée aux mots de passe du service de gestion réseau distant Telnet.

Remaiten n'est autre que la dernière incarnation de bots Linux distribués spécialement conçus pour lancer des attaques par déni de service (DDoS). Lorsqu'il scanne des points d'entrée, Remaiten tente de se connecter à des adresses IP aléatoires sur le port 23 (Telnet) et, en cas de connexion fructueuse, il tente de s'authentifier en utilisant une combinaison de nom d'utilisateur et mot de passe en provenance d'une liste d'authentifiants communs, ont indiqué dans un billet de blog les chercheurs de l'éditeur en solutions de sécurité Eset. Ce n'est pas la première fois que les routeurs domestiques sont exposés à du piratage. On se souvient que l'année dernière 700 000 avaient été exposés à cause d'une faille NetUSB et plus récemment, des failles avaient été trouvées dans de nombreux routeurs WiFi Netgear et D-Link.

Scan de ports et fermeture du service Telnet pour se protéger

En cas de succès, le bot exécute plusieurs commandes pour déterminer l'architecture système avant de transférer un petit programme compilé pour permettre de télécharger l'ensemble des commandes de contrôle du botnet. Le ver dispose de versions pour jeux d'instructions mips, mipsel, armeabi et armebeabi. Une fois installé, il se connecte à un canal IRC et attend les commandes d'un pirate distant. Ce bot supporte une variété de commandes pour lancer différentes attaques DDoS et peut même scanner d'autres bots DDoS afin de les désinstaller.

Il est surprenant que de nombreux terminaux réseau utilisent encore Telnet pour la gestion réseau à distance plutôt que le protocole plus sécurisé SSH. Il est encore plus malheureux que de nombreux terminaux soient livrés avec le service Telnet ouvert par défaut. Afin de se protéger, il est recommandé d'utiliser un outil de scan de port en ligne et, dans le cas où le port 23 est ouvert, de fermer le service Telnet depuis la console d'administration web. Une possibilité qui n'est malheureusement pas offerte par tous les fournisseurs d'accès à leurs clients… [Lire la suite]

Réagissez à cet article