OutlawCountry : la CIA détourne le trafic des PC et serveurs Linux

Le lot Vault 7 n'en finit pas de livrer ses secrets. Wikileaks vient de publier une documentation d'un malware de la CIA connu sous le nom OutlawCountry. Il vise spécifiquement les systèmes d'exploitation Linux. La documentation date du 4 juin 2015 et détaille un module Kernel pour Linux 2.6 qui donne à la CIA la capacité de réorienter le trafic d'une machine Linux vers une autre destination choisie.

L'accès au shell et les privilèges administrateurs sont nécessaires pour installer OutlawCountry, ce qui signifie que les agents de la CIA doivent compromettre les PC par d'autres moyens avant de déployer le malware.

Une fois installé, OutlawCountry utilise des outils de filtrage de paquets intégrés dans Linux, comme netfilter et iptables. Concrètement, le module se charge de créer une nouvelle table netfilter avec un nom quelconque. Cette table permet de créer des règles à l'aide de la commande iptables. Ces règles ont priorité sur celles existantes et ne sont visibles que pour un administrateur si le nom de la table est connu. Quand l'opérateur supprime le module du Kernel, cette nouvelle table est également supprimée.

Utilisable sur des serveurs ou des PC Linux

OutlawCountry v1.0 contient un module Kernel pour CentOS/RHEL (Red Hat Enterprise Linux) 6.x en 64 bits. La documentation précise que ce module fonctionne qu'avec des kernel par défaut. De plus, le malware supporte uniquement l'ajout de règles DNAT (traduction d'adresse réseau de destination) à la chaîne PREROUTING.

OutlawCountry peut être utilisé pour les serveurs et les PC en autorisant un agent de la CIA à rediriger le trafic de la cible vers des serveurs proxy sous le contrôle de l'agence de renseignement. Cela lui permet de connaître les habitudes de l'utilisateur ou de mener d'autres attaques. Installé sur un serveur, un opérateur de la CIA peut intercepter le trafic de plusieurs utilisateurs à la fois.

Dans la documentation, il est indiqué un hashage MD5 pour un des modules kernel (nf_table_6_64.ko): 2CB8954A3E683477AA5A084964D4665D. Le nom par défaut de la table netfilter cachée est : dpxvke8h18

A lire aussi :

Comment la CIA suit les PC à la trace à l'aide du Wifi

Brutal Kangaroo : quand la CIA cible les réseaux les plus sensibles

Crédit photo : GlebStock / Shutterstock