Plus de la moitié des attaques SSH viennent de Chine

Petit exercice pratique, avec un épluchage en règle des tentatives d'accès opérées sur un serveur web de test. De nombreuses attaques par dictionnaire tentent de pénétrer chaque jour sur les serveurs présents sur la Toile via le protocole **SSH** (Secure Shell).

Sur les quinze serveurs les plus actifs détectés, ceux situés en **Chine** sont très présents : **53 %** du total (8 serveurs). Toutes les machines incriminées sont hébergées dans les *datacenters* de **China Telecom**, qui s'avère ici être un bien mauvais élève en matière de lutte antipiratage . À noter également, la présence d'un serveur pirate à Hong-Kong.

Les pays de l'Est (et probablement la Russie) sont l'autre grand vivier de serveurs pirates, avec **20 %** des sources d'attaques opérées sur notre serveur de test. Leur répartition est toutefois plus variée, avec un serveur en **Ukraine** et deux en **Azerbaïdjan**.

Enfin, d'autres serveurs isolés ont été détectés : un au Brésil, un autre en Inde et un troisième aux Pays-Bas. Probablement des machines passées sous la coupe de pirates.

Protéger SSH

Il est donc plus que jamais nécessaire de bien protéger son serveur web. Tout d'abord en installant toutes les mises à jour de l'OS (Linux en général), mais également en appliquant quelques règles de bon sens, comme l'interdiction de se connecter en root via SSH ou encore la mise en place d'un outil comme **fail2ban**, qui freinera très fortement les tentatives d'attaques.

À lire aussi :
La Chine va installer des boîtes noires sur son réseau Internet
TV5 Monde victime d'une attaque de pirates de Daesh
Les sites pirates bloquent Windows 10

Crédit photo : © Karen Roach – Shutterstock