Les' trojans' envahissent le Web chinois

Le volume des attaques en provenance de Chine est en hausse. C'est une tendance confirmée par l'ensemble des éditeurs de solutions de sécurité.

Et les récentes attaques contre des sites occidentaux ainsi que les tentatives d'intrusion contre des réseaux gouvernementaux américains, français et allemands, ont poussé l'éditeur Finjan à surveiller de plus près l'évolution de l'activité virale en Chine. Bilan des courses, les trojans sont de plus en plus nombreux sur les sites chinois.

Menée par le MCRC (Malicious Code Research Center), le centre de recherche des codes malveillants de Finjan, l'étude met en exergue l'augmentation des attaques en provenance de Chine. Les hackers chinois semblent se construire une armée de PC zombies.

Pour cela, il dissimule des codes malveillants sur des sites Web, et en l'occurrence, il s'agit de chevaux de Troie. Cette technique de diffusion permet aux cybercriminels de l'empire de contourner les mécanismes des technologies de sécurité.

L'utilisation des trojans n'est pas la seule technique des hackers chinois. Ces derniers utilisent également des exploits « zero-day », c'est-à-dire des codes malveillants qui n'ont pas encore été référencés et pour lesquels, il n'existe pas encore de correctifs.

Et d'après Finjan les Hackers de Chine n'ont peur de rien puisque des sites gouvernementaux sont également infectés. Le système très complexe développé par les hackers Chinois est présenté sous la forme d'un schéma sur ce lien. L'on constate, que les attaques sont très bien structurées, par exemple les trojans sont capables de se mettre à jour. D'autres sites sont dédiés au décompte des utilisateurs infectés et permettent aux hackers de réaliser des tableaux statistiques très précis.

Les trojans utilisés par les cybercriminels permettent de collecter des informations sur les utilisateurs infectés, des données qui portent par exemple sur la nature de l'OS utilisé, les applications de sécurité installées, des informations confidentielles…bref suffisamment de détails pour dresser un portrait exact de l'utilisateur ciblé.

*« Le développement rapide de ces activités est très inquiétant pour les gouvernements. »*indique le CTO de Finjan, Yuval Ben-Itzhak. *"Les solutions antivirus et celles de filtrage des URL sont insuffisantes contre ces attaques. Les réseaux des cybercriminels sont très bien structurés et il est difficile de les tracer. »*

Cette publication de l'éditeur, intervient alors que le directeur général du MI5 (les services secrets britanniques) a récemment indiqué que les attaques en provenance de Chine menaçaient les entreprises britanniques. Ultime preuve de la crainte grandissante de certains pays à l'égard du voisin chinois et de ses hackers qui sont parmi les plus actifs au monde.