

Russie : un gang de cybercriminels s'exile vers l'Est

Il ne faut pas crier victoire trop rapidement, mais l'information a le mérite de mettre en exergue les efforts consentis par tous les acteurs de la Toile pour lutter contre les mafieux technophiles.

Pour Raimund Genes, CTO pour la division antivirus de Trend Micro :« *Il semble que les fournisseurs d'accès de RBN ont décidé de les « blacklister », et de couper l'accès au Web.* »

Rappelons que selon des chercheurs de Verisign, la RBN proposait du Bullet proof Hosting (dissimulation de l'IP), fournissait des malwares et travaillait étroitement avec des cybercriminels.

D'après Genes :« *toutes les formes de cybercriminalité étaient présentes chez RBN mais ces derniers temps l'activité devenait trop importante. Ils ont été trop gourmands.* »

Dernièrement, ils ont tout de même infiltré un site gouvernemental d'un grand pays pour y placer des liens redirigeant les internautes vers un site panaméen utilisé par des membres d'un cybergang pour mener des attaques et dérober des informations personnelles.

Des sites brésiliens et également américains ont été piégés par des clients de la RBN. Notamment par le biais d'attaques utilisant des injections SQL. « *Il faut croire que les gouvernements aussi ont été agacés par les agissements de la RBN* » déclare Genes

Trend Micro, indique dans une note que l'hébergeur a probablement déménagé en Asie. Pour preuve depuis quelques jours des sites chinois et taiwanais hébergent des kits de malwares (MPack et IcePack) développés par les membres de la RBN.