Incroyable technique pour analyser les agissements des cybercriminels

Incroyable technique pour analyser les agissements des cybercriminels

Depuis 2007, Zeus empoisonne la vie de millions d'internautes. Ce #logiciel malveillant s'installe sournoisement dans les ordinateurs afin de voler des informations bancaires. Zeus et ses variantes ont ainsi réussi à infecter les serveurs de grandes sociétés comme la NASA, Amazon et Facebook. Selon Mourad Debbabi, professeur et titulaire de la Chaire de recherche en sécurité des systèmes d'information à l'Université Concordia, la Toile est un véritable champ de bataille. Les attaques lancées par les pirates informatiques font des victimes chaque jour, mais les chercheurs ont ces cyberfraudeurs à l'œil : ils les observent pour mieux défendre les internautes, prévenir les fraudes et contre-attaquer !

L'équipe de Mourad Debbabi surveille notamment les « botnets » (contraction de *robot* et de *network*), des réseaux de machines infectées appelées « zombies » qui exécutent les directives des cybercriminels. Les gens installent des maliciels comme Zeus en cliquant sur une pièce jointe ou sur un lien compromis par un code nuisible. L'ordinateur contaminé envoie ensuite des courriels indésirables pour attirer d'autres victimes qui feront partie du *botnet*. Cet ensemble de machines infectées communique avec un ou des serveurs de commande et contrôle qui gèrent diverses attaques.
Pour déjouer ces *botnets* et d'autres menaces, le professeur Debbabi et ses collaborateurs des paliers universitaire, gouvernemental et industriel canadiens ont développé une plateforme de cyber-renseignements. Il s'agit d'un réseau d'ordinateurs peu sécurisés qui « attirent » les cyberattaques, permettant aux chercheurs d'analyser en temps quasi réel une multitude de données (pourriels, virus, etc.) nécessaires pour contrecarrer les escrocs du Web. Cette cyberinformation sert à protéger le parc informatique et les renseignements privés des entreprises et des organisations : mise en quarantaine des ordinateurs infectés, pare-feu renforcé, logiciels de détection… Tel est pris qui croyait prendre !

Réagissez à cet article

Original de l’article mis en page : Cyberguerre : la science contrattaque | Scientifique en chef