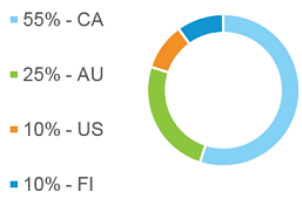
Le cheval de Troie Ramnit refait surface

Le cheval de Troie Ramnit refait surface

Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle Une première pour un botnet bancaire selon IBM



En février dernier, suite à une opération menée par plusieurs États ainsi que des acteurs privés (parmi lesquels Microsoft, Symantec et AnubisNetworks) qui a été coordonnée par le centre de lutte contre la cybercriminalité d'Europol, un réseau de serveurs de contrôle du botnet Ramnit a été démantelé. Trois cents domaines internet exploités par les pirates ont également été redirigés.
Détecté pour la première fois en 2010, le cheval de Troie Ramnit permettrait de gagner un accès distant aux ordinateurs Windows infectés et de subtiliser par la suite des données sensibles, comme des informations bancaires. Wil van Gemert, le directeur des opérations d'Europol, a salué le succès de l'opération : « cette opération réussie illustre l'importance pour les forces de l'ordre internationales de travailler de concert avec l'industrie privée afin de lutter contre la menace globale du cybercrime ».
Seulement, les chercheurs d'IBM ont mis la main sur une variante du cheval de Troie qui se base sur une infrastructure C&C différente de son prédécesseur et emploie un fichier de configuration plus court ainsi qu'un schéma d'injection web différent pour infecter les victimes. Plus de la moitié des infections a été observée au Canada. En seconde position sur la liste des pays les plus affectés viennent l'Australie qui compte à elle seule une infection sur quatre, puis les États-Unis.
Selon les chercheurs de la X-Force d'IBM, il semblerait que ce soit la première fois qu'un botnet de fraude bancaire refasse surface, ce qui a aiguisé leur curiosité puisque, jusqu'à présent, c'étaient plutôt les botnets de spams qui étaient souvent ramenés en circulation, les cybercriminels derrière les botnets de fraude bancaire préférant se contenter de l'argent déjà collecté et du fait qu'ils n'aient pas été arrêtés.
Les experts expliquent que « le cheval de Troie arborait un fichier de configuration lourd avec des déclencheurs d'URL qui lui indiquaient vers quelle banque, quelle transaction et quels sites de réseau social se tourner pour collecter des informations d'identification ». La configuration de Ramnit est orientée pour tenir les victimes éloignées d'une liste exhaustive d'outils de scans en ligne, de sites web d'antivirus, des sites d'information sur le cybercrime, mais également des blogs de sécurité. « Dans son ancienne configuration, la seule utilisation des mots « cybercriminalité » ou « police » de la part des victimes suffisait à déclencher un effet de redirection ».
Une autre trace laissée par les anciennes configurations est la liste relativement importante de sites de recrutements récoltant les informations d'identification, afin de viser ceux qui sont à la recherche d'un emploi et de les recruter. « Pour les victimes, cela pouvait être une lame à double tranchant étant donné que les opérateurs Ramnit pouvaient également obtenir toutes les informations qu'elles ont mises sur leur CV professionnel ».
La X-Force Threat Intelligence d'IBM n'a pas eu vent du fait que le code source de Ramnit ait été vendu ouvertement, partagé avec d'autres groupes de cybercriminels ou sur les forums dans le marché noir. Aussi, ils pensent qu'il y a de fortes chances qu'il s'agisse là du même groupe d'individus qui a remis cette nouvelle version en activité.

Réagissez à cet article

Source : *Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle, une première pour un botnet bancaire selon IBM*