‘Phishing’ deux hackers russes dérobent près de 500,000$

La méthode utilisée par les deux cybercriminels originaires de Russie a été franchement efficace.

Nos deux arnaqueurs ont réussi à voler 508,000 dollars par l’intermédiaire de 260 transferts d’argent de banque turcs. Ils ont pour cela utilisé un cheval de Troie contrôlable à distance. Ce piratage phénoménal a duré pendant près de deux ans.

Selon les informations données par l’agence de presse russe, *RIA Novosti*, les deux auteurs présumés de la fraude sont des adolescents originaires de la ville de Togliatti, située sur les bords du plus grand fleuve européen, la Volga, auraient utilisé un serveur dédié avec accès distant depuis un ordinateur de bureau localisé dans un data center américain.

L’argent volé était ensuite transféré vers les comptes de complices turcs, puis réexpédié sur un compte de la Western Union de Togliatti.

Une fois la main prise sur ce serveur et cet ordinateur, ils ont utilisé un système personnalisé RAT (Remote Administration Trojan). Une application discrète permettant de gérer le trojan à distance.

Puis ils ont procédé à l’infection des ordinateurs de plusieurs centaines de clients des banques turques de façon à récupérer des identifiant, des codes d’accès et des numéros de comptes.

Selon les informations données par la presse russe spécialisée dans la sécurité informatique, l’un des adolescents a été arrêté au mois de juin 2007 tandis que l’autre est actuellement recherché par la police.

Herman Zampariolo, le patron de WSLabi [Wabisabilabi, site permettant la vente aux enchères de vulnérabilités], explique *: « Il s’agit d’un des piratages les plus longs de l’histoire de la sécurité informatique et cette affaire montre une fois de plus la puissance des ‘trojans’ et l’incapacité des banques à en contrôler la prolifération. »*

« D’après le peu d’informations dont on dispose pour le moment, il semble que le ministère de l’Intérieur russe cherche ces deux hommes depuis longtemps, mais cela n’explique pas comment ils ont réussi à être invisibles si longtemps. «