Des hackers dérobent 800.000 euros avec des attaques de phishing

D'après nos confrères de silicon.com, une grande arnaque par hameçonnage, menée par des hackers russes a touché l'institution bancaire Suédoise Nordea.

Les cybercriminels à l'origine de cette arnaque ont utilisé un cheval de Troie sophistiqué pour récupérer les informations personnelles des utilisateurs de la banque et notamment les numéros de compte et les codes personnels.

La première attaque touchant Nordea s'est déroulée au mois d'août 2006 et a été détectée seulement un mois plus tard. D'après la banque, à l'heure actuelle **250** de ses utilisateurs ont été dupés par cette cyberattaque et 800.000 euros dérobés. Selon McAfee, il s'agirait de la plus grande escroquerie en ligne jamais observée.

Pour duper les clients de Nordea, les hackers ont utilisé une feinte plutôt habile. Ils ont envoyé de nombreux mails de téléchargement d'une solution de sécurité gratuite. Seulement en réalité en pièce jointe du mail était dissimulé un puissant outil d'intrusion, le cheval de Troie nommé **'haxdoor.ki'.**

Le logiciel malveillant se met en branle dès que l'internaute contaminé tente de visiter la page Web de sa banque. Une fois sur la page de la banque Nordea un message d'erreur apparaît. Ce dernier propose à l'utilisateur de ressaisir ses codes permettant son identification. Ces détails sont ensuite discrètement renvoyés sur les serveurs de l'attaquant.

La police suédoise est remontée à la source de ces attaques. Selon les premières informations dont nous disposons, elles semblent provenir de Russie et passent par des serveurs hébergés aux États-Unis. La police a déjà arrêté une centaine de complices localisés en Suède.

Un porte-parole de Nordea a expliqué :*« malgré ces arrestations, les attaques sont toujours en cours et le spam se diffuse toujours. Tous nos clients touchés pas ces attaques ont été intégralement remboursées. »*

Il a ajouté : *« ces cyberattaques en provenance de pays étrangers sont un phénomène global particulièrement inquiétant. »*