Une attaque ‘pharming’ sophistiquée a visé 50 organismes financiers

Websence vient de révéler qu’une attaque massive et sophistiquée, exploitant la technique du ‘***pharming***‘, a tenté durant trois jours de tromper les clients d’une cinquantaine d’institutions financières aux Etats-Unis, en Europe et en Asie.

Les mafieux ont exploité une faille ? corrigée depuis longtemps ? sous Windows, forçant un ordinateur non mis à jour à charger un fichier cheval de Troie nommé ‘*iexplorer.exe*‘, qui ensuite lançait le téléchargement de cinq autres fichiers à partir d’un serveur installé en Russie.

Si l’internaute visitait un site bancaire ciblé à partir de son PC infecté, il était orienté vers un faux site imitation – un par banque – sur lequel il était classiquement invité à déposer ses identifiants. Puis dans la foulée réorienté automatiquement et de manière transparente sur le site officiel de la banque où la procédure continuait de se dérouler ‘normalement’.

Seule indication du déroulement de l’attaque, un message d’erreur invitait l’internaute à couper son pare-feu et son antivirus. Sur les PC vérolés était également installé un ‘*bot*‘ permettant à l’attaquant de prendre le contrôle à distance du poste.

Le code vérolé qui exploitait la faille de Microsoft était hébergé par des serveurs situés en Allemagne, en Estonie et en Grande-Bretagne.

L’attaque s’est déroulée durant trois jours, infectant quotidiennement selon Websense environ 1000 machines par jour, essentiellement en Australie et aux Etats-Unis. La fermeture par les fournisseurs d’accès des sites pirates usurpant l’identité des banques, ainsi que des serveurs, a mis fin à l’attaque mardi matin.

Une inconnue demeure, comme dans toutes ces affaires de ‘*phishing*‘, ‘*pharming*‘ ou d’usurpation d’identité : combien d’internautes ont été victimes de l’arnaque ?