# Phishing : quand les fraudeurs piègent les fraudeurs!

Un groupe de cybercriminels marocains qui se fait appeler Mr-Brain vient de lancer un site Web qui propose au téléchargement un outil de phishing simple d'utilisation.

Ladite URL propose des outils pour s'attaquer aux cibles suivantes : Bank of America, eBay, PayPal et HSBC.

Ces « phishing tools » proposés par Mr-Brain sont spécialement conçus pour faciliter le travail des autres cybercriminels. Ils peuvent être utilisés pour déployer rapidement des sites de phishing très réalistes.

Il suffit d'avoir des connaissances très basiques pour utiliser ces outils automatisés. Avec ces « phishing kits » la configuration d'une attaque d'hameçonnage n'excède pas cinq minutes.

Mais en réalité, l'intention des membres de Mr-Brain est bien différente. Malins, ils veulent qu'un maximum de personnes utilise ces outils, parce qu'une partie du code du logiciel permet à ce gang de récupérer les données des victimes des utilisateurs de l'outil.

Ils sont donc les réels bénéficiaires des attaques menées par « leurs clients ». Pour faire simple, ils arnaquent les arnaqueurs.

L'adresse mail associée à Mr-Brain est dissimulée dans le script de configuration du soft. Elle est présentée comme un morceau essentiel au bon fonctionnement du logiciel.

Du coup, les fraudeurs amateurs évitent de l'altérer. Qui plus est, elle est cryptée et dissimulée dans un fichier invisible nommé « niarB », ce qui donne Brain, une fois les lettres replacées dans le bon ordre.

Selon Netcraft, à l'origine de cette découverte, tous les phishing kits téléchargés sur le site renvoient, dans le dos des fraudeurs, des informations sur les internautes déjà piégés. Les membres de Mr-Brain utilisent pour cela une adresse Gmail.

Les membres de Mr-Brain seraient à l'origine de plusieurs attaques de phishing. Les sommes générées par ce gang ne sont pas connues, mais Netcraft assure qu'il s'agit d'un groupe très actif.