Fraude en ligne : RSA revient sur l'attaque 'Rock Phish'

Dans les faits, les membres de « Rock Phish », essayent de diriger les internautes vers une fausse page de YouTube à travers un e-mail.

Les utilisateurs ayant la malencontreuse idée de cliquer sur le lien figurant dans cet e-mail étaient alors dirigés sur un site pirate imitant la présentation des véritables pages de YouTube – comme pour une attaque de phishing « normale ». Le domaine utilisé pour héberger le « site de mystification » est un domaine Rock Phish.

Ce site est conçu pour infecter le système de l'utilisateur avec un logiciel malveillant (« malware ») à travers un « scénario de mystification » indiquant au visiteur que, pour télécharger la vidéo, il doit préalablement installer un fichier Flash (.exe). Ce dernier est en réalité un « véhicule » pour du code pirate permettant d'installer des logiciels malveillants sur le poste de la victime.

Pour plus de détails sur cette attaque, un rapport de Websense Security Labs est disponible sur ce lien.

En suivant les instructions données par l'e-mail et le site de mystification, les équipes de recherche de RSA FraudAction ont pu obtenir le logiciel en question pour étudier son fonctionnement. À la première analyse, ils ont déterminé que son objectif et sa principale fonctionnalité étaient d'envoyer des spams de phishing pour relayer d'autres attaques de Rock Phish.

Dans son communiqué, RSA indique: *« Nous pensons donc logiquement, que la diffusion par Rock Phish de ce logiciel malveillant a pour objet essentiel d'étendre ou de reconstruire son infrastructure de spam. En effet, le site de mystification n'est pas à proprement parler un site de phishing mais plutôt un vecteur de diffusion et d'installation d'un logiciel susceptible d'aider les fraudeurs lors de prochaines attaques. Le logiciel malveillant propagé par le site est en effet un moteur de collecte d'adresses (ou «spambot») capable d'adresser des e-mails de phishing aux victimes de futures attaques menées par le groupe Rock Phish. En d'autres termes, les systèmes infectés par ce logiciel font aujourd'hui partie des infrastructures de spam de Rock Phish… »*

Les résultats présentés par RSA, sont le fruit de l'analyse préliminaire d'un Cheval de Troie qui doit être étudié plus profondément. *« Sur la base de son comportement et des fichiers qu'il installe, nous avons conclu qu'il s'agit d'une variante d'un Cheval de Troie déjà identifié (Troj/Danmec-W) »* indique le rapport mensuel de RSA. Ce module malveillant permet de subtiliser des adresses et de leur adresser des e-mails.

« Nous avons tracé plusieurs adresses IP liées aux points de communication de ce Cheval de Troie dont nous pensons qu'il les utilise pour recevoir des mises à jour contenant les informations suivantes: corps du message des spams à envoyer ; domaines des attaques Rock Phish associés aux spams ; serveurs d'e-mails à travers lesquels le spam doit être émis. Une fois « nourri » de ces informations, le Cheval de Troie crée un fichier crypté contenant les corps des e-mails (de phishing) ainsi que les domaines des attaques Rock Phish (c'est-à-dire les domaines vers lesquels les victimes des futures attaques seront dirigées) » précise l'éditeur.