RSA dévoile les nouvelles techniques d'attaques informatiques

Le RSA Anti-Fraud Command Center (AFCC) est le « quartier général » de lutte contre la fraude de RSA, la division sécurité d'EMC. Il surveille et analyse l'activité de la fraude en ligne chaque mois et développe une intelligence sur la fraude unique sur le marché.

Le RSA anti-Fraud Command Center a édité récemment deux rapports de fraude mettant en avant des nouvelles techniques d'attaques informatiques :

En août, RSA nous alertait sur une sur une technique d'attaque informatique inédite qui combine messagerie instantanée et Trojan.

- Habituellement, les Trojan servent à créer un accès sur un ordinateur afin qu'un pirate puisse en prendre le contrôle à distance pour voler des données (identifiants, codes…).
- Le Trojan « Zeus » identifié par RSA ce mois-ci fonctionne différemment. Il ne se contente pas d'ouvrir un accès sur un ordinateur infecté, il récolte des données et les copie sur un « serveur de dépôt ».
- Le fraudeur utilise alors sa messagerie instantanée pour être alerté en temps réel si des données sont disponibles sur ce serveur.

En septembre, RSA identifiait que les fraudeurs détournent les tchats des supports techniques des institutions financières.

- Une fausse page du site bancaire est crée par le pirate. La victime est invitée à se connecter pour pouvoir accéder à ses comptes. Il s'agit d'une attaque de phishing classique. Le fraudeur récupère alors les identifiants de la victime lors de sa connexion au site factice.
- Puis alors qu'habituellement la victime est redirigée vers le véritable site. Cette fois-ci une fenêtre apparaît à l'écran et l'invite à démarrer un tchat avec le support technique.
- De l'autre coté, le fraudeur se fait passer pour un représentant de la banque sous prétexte de lui assurer un maximum de sécurité lui soutire un maximum d'informations critiques. E-mail, téléphone, date de naissance…autant d'informations précieuses et monnayables.