Malware : eBay est victime du ‘troisième homme’

Les utilisateurs du célèbre site de ventes aux enchères eBay, sont ciblés par un trojan très dangereux. Ce dernier, nommé Trojan.Bayrob essaye de mener à terme une attaque de type *« man in the middle »* que l’on peut traduire par *« le troisième homme ».*

Comment cela fonctionne ? Le pirate est positionné entre le client et le site de ventes aux enchères et récupère toutes les informations nécessaires.

Ce système permet de faire dialoguer la victime potentielle avec un site Web légitime à travers une URL frauduleuse créée par le pirate afin de capturer en temps réel des informations personnelles sur sa victime.

Le Trojan.Bayrob implémente un serveur proxy de façon a ce que toutes les informations envoyées sur eBay se retrouvent sur un faux site contrôlé par le Hacker.

Le trafic des paquets est redirigé en changeant les paramètres correspondants à au moins six URL eBays stockés dans les fichiers temporaires de la victime. Bayrob a été conçu pour dérober les données de configuration du poste dont une variété de scripts PHP.

Au moins, un des scripts, Var.php, télécharge des versions frauduleuses d’eBay pour duper la victime et lui faire croire que la page sur laquelle il se trouve est légitime. L’attaquant peut même imiter un vendeur que l’acheteur potentiel connaît ce qui ajoute de l’authenticité à l’arnaque.

Selon EMC, un kit de phishing universel de ce type peut être trouvé sur le Web pour environ 1.000 euros, clé en main.

Dans un communiqué , l’éditeur Symantec s’inquiète de la prolifération de ce type d’attaques. Ce dernier casse-tête sécuritaire en date, est un mauvais coup pour eBay qui est de plus en plus souvent critiqué par ses utilisateurs. Ces derniers estiment que la fraude augmente et que cela est inacceptable.

L’approche *« man-in-the-middle »*est inhabituelle sur eBay, généralement les hackers qui ciblent ce site préfèrent les méthodes traditionnelles comme le phishing ou l’utilisation de keyloggers.

Néanmoins, bien exécuter du code dans le cadre d’une attaque *« man in the middle »* est très difficile, ce qui risque de limiter son utilisation.