Bitdefender : Une augmentation de faux services de paiement en ligne
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 16/5/2013 14:00:00

Bitdefender, Ã©diteur de solutions de sÃ©curitÃ©, publie une Ã©tude sur **les arnaques de services de paiement en ligne**, pour la vente de particulier Ã particulier, dont le nombre et lâ□□ampleur augmentent avant les vacances.

Les achats en ligne de voitures, motos et produits Ã©lectroniques sont les plus risquÃ©s pour les acheteurs, comme pour les vendeurs !

Ces arnaques concernent de faux sites de paiement en ligne, crÃ©Ã©s par des pirates se prÃ©sentant comme des tiers de confiance, censÃ©s assurer une transaction sÃ©curisÃ©e entre vendeur et acquÃ©reur et ainsi leur Ã©viter les dÃ©convenues dâ□□une transaction en direct (non-rÃ©ception de la marchandise ou non paiement).

Bitdefender prÃ©voit une augmentation de ce type dâ□□arnaque au mois de juin, avant le dÃ©but des vacances dâ□□Ã©tÃ©, particuliÃ¨rement pour la vente de voitures, de motos et de produits Ã©lectroniques.

AprÃ¨s 10 mois de recherche, cette Ã©tude rÃ©vÃ¨le que 16.8 % des arnaques de ce type, enregistrÃ©es ces 12 derniers mois, ont Ã©tÃ© crÃ©Ã©es au mois de juin. Les scammeurs sont, en effet, plutÃ´t actifs dans la crÃ©ation de faux sites de paiement en ligne avant les pÃ©riodes de vacances. AprÃ¨s une diminution stable de juillet Ã octobre, le nombre de ces faux sites commence ainsi Ã augmenter avant les vacances dâ□□hiver, et plus particuliÃ¨rement en dÃ©cembre. Une recrudescence est ensuite notÃ©e en fÃ©vrier, avec un pic Ã plus de 17% des arnaques dÃ©tectÃ©es.

Cette Ã©tude de Bitdefender, rÃ©alisÃ©e sur plus de 2 000 faux sites Web de paiement en ligne, montre aussi que les voitures, les motos et les produits Ã©lectroniques sont en tÃªte de liste des articles utilisÃ©s par les scammeurs pour escroquer les clients en ligne. Les scammeurs se font gÃ©nÃ©ralement passer pour des vendeurs lÃ©gitimes, sur de vrais sites de vente en ligne, et redirigent ensuite les acheteurs sur le faux site de paiement qu'ils contrÃ´lent. Les scammeurs

rÃ©cupÃ¨rent ainsi l'argent et ne livrent bien entendu jamais les marchandises.

Top 5 des articles utilisÃ©s dans les arnaques de faux paiements en ligne :

1. Les voitures

2. Les motos

3. Les produits Ã©lectroniques

4. Les articles de valeur

5. Les vÃ©los

Parmi les services Ã©galement pris en charge par les scammeurs, via de fausses transactions, Bitdefender dÃ©nombre : les dÃ©pÃ´ts bancaires (versements), le transfert de dossiers mÃ©dicaux ou encore dâ□□Ã©chantillons liÃ©s Ã des analyses mÃ©dicales.

Â« *Les scammeurs peuvent Ãªtre tout Ã fait convaincants - c'est prÃ©cisÃ©ment comme cela quâ□□ils gagnent de lâ□□argent* Â» dÃ©clare Catalin Cosoi, Responsable des stratÃ©gies de sÃ©curitÃ© chez Bitdefender. Â« *Ils se donnent beaucoup de mal pour donner l'impression d'Ãªtre lÃ©gitimes, au point mÃªme de conseiller Ã leurs cibles de se protÃ©ger contre la fraude Ã la carte bancaire. Afin de rassurer leurs victimes, lâ□□usage classique est quâ□□ils ne demandent jamais dâ□□informations bancaires, ce qui au final ne change rien dans le cas de cette arnaque, puisque les escrocs reÃ§oivent directement un transfert dâ□□argent.* Â»

Bitdefender conseille vivement aux utilisateurs de vÃ©rifier les informations WHOIS (enregistrement de domaine, hÃ©bergement, activitÃ© en ligne) avant tout paiement en ligne ou utilisation dâ□□un service de transfert dâ□□argent, censÃ© sÃ©curiser la transaction. En effet, contrairement aux vrais sites, plus de 90% des faux sites de paiement en ligne sont enregistrÃ©s seulement pour un an et utilisent des adresses email comme contact@privacyprotect.org pour conserver leur anonymat.

De plus, les vrais sites de paiement en ligne utilisent des serveurs de connexions sÃ©curisÃ©es (SSL) pour protÃ©ger les clients. Ces derniers doivent donc voir apparaÃ®tre une adresse commenÃ§ant par Â« https:// Â» dans la barre de leur navigateur. MalgrÃ© tout, les sites frauduleux peuvent Â« emprunter Â» le logo des services de vÃ©rification SSL, les utilisateurs sont donc invitÃ©s Ã vÃ©rifier que le site est bien identifiÃ© par la sociÃ©tÃ© dâ□□authentification et Ã effectuer quelques vÃ©rifications en ligne concernant ce tiers de confiance. Bien souvent, une simple recherche Web permet dâ□□Ã©venter le piÃ¨ge en tombant par exemple sur des tÃ©moignages dâ□□utilisateurs, victimes de ce type dâ□□arnaque.

Pour retrouver Bitdefender en ligne