Trend Micro alerte sur les attaques Ã la fraude bancaire !
Internet
PostÃ© par : JPilo
PubliÃ©e le : 3/7/2012 11:30:00

Trend Micro, un des leaders mondial de la sÃ©curitÃ© des contenus Internet, annonce la publication dâ□□un nouveau rapport de recherche sur les menaces Ã la fraude bancaire.

Ce document porte sur un systÃ¨me de transfert automatique (ATS - Automatic Transfer System), permettant aux cybercriminels de dÃ©jouer les mesures les plus rÃ©centes en matiÃ¨re de sÃ©curitÃ© bancaire, dans lâ□□objectif de â□□viderâ□□ le compte bancaire des victimes sans laisser de traces dâ□□une activitÃ© criminelle.

Ce rapport, rÃ©digÃ© par **Loucif Kharouni**, chercheur chez Trend Micro, Ã©value comment lâ□□outil ATS est utilisÃ© en association avec des variantes des virus SpyEye et ZeuS pour crÃ©er une attaque â□□Man in the Browser (MitB)â□□. On parle dâ□□une attaque MitB car la cible exÃ©cute un module au sein du navigateur de lâ□□utilisateur qui est programmÃ© pour opÃ©rer automatiquement des transferts de fonds. Ce module Â« connaÃ®t Â» le fonctionnement du site web et permet de modifier Ã la volÃ©e les donnÃ©es transmises et reÃ§ues par la victime.

Cette attaque, qui ne nÃ©cessite pas que le cybercriminel soit en ligne pendant la session web de sa victime, initie un transfert bancaire en utilisant les identifiants de la victime, sans que cette derniÃ¨re ne soit alertÃ©e. (en modifiant la vue du solde du client par exemple).

Le rapport Automatic Transfer System, a New Cybercrime Tool dresse le panorama des attaques qui ont ciblÃ© des banques pourtant utilisatrices de mesures de sÃ©curitÃ© Ã©voluÃ©e : seuils plafonds en matiÃ¨re de transfert, authentification Ã deux facteurs avec notifications via SMS, etc. Les banques en Allemagne, au Royaume-Uni et en Italie ont Ã©tÃ© les principales cibles.

â□□*Ces exactions sont particuliÃ¨rement inquiÃ©tantes, car elles contournent des mesures de sÃ©curitÃ© trÃ¨s strictes* Â», explique **Tom Kellermann**, Vice-prÃ©sident en charge de la cyber sÃ©curitÃ© chez **Trend Micro**. â□□*Cet outil ATS utilise des mÃ©thodes furtives pour modifier certains fichiers, et il devient plus que jamais impÃ©ratif dâ□□utiliser des solutions de protection capables de prÃ©venir le dÃ©clenchement dâ□□une infection, ou de juguler la menace aprÃ¨s infection. Les utilisateurs doivent Ã©galement mettre Ã jour leurs outils de sÃ©curitÃ© pour postes clients, pour mettre toutes les chances de leur cÃ´tÃ© face Ã ces attaques.* â□□

Ã ce jour, lâ□□outil ATS ne cible que les accÃ¨s aux comptes bancaires via un PC sous Windows. Contrairement aux prÃ©cÃ©dents outils criminels qui interagissent avec SpyEye et ZeuS, lâ□□outil ATS nâ□□affiche pas de pop-up et exÃ©cute diffÃ©rentes tÃ¢ches automatiquement : vÃ©rification du solde bancaire, rÃ©alisation de transferts bancaires et modification des transactions bancaires pour dissimuler toute trace dâ□□exaction.

Comment les utilisateurs peuvent se protÃ©ger de ce type dâ□□attaque ?

Câ□□est lors de la premiÃ¨re phase que les utilisateurs doivent se protÃ©ger, car câ□□est Ã ce moment que le malware qui contient le Â« MitB Â» est installÃ© sur le poste client. Afin dâ□□Ã©viter son installation, il convient de rappeler un certain nombre de bonnes pratiques :

1.Garder son PC Ã jour : Les compromissions sont souvent rÃ©alisÃ©es via des vulnÃ©rabilitÃ©s connues qui sont corrigÃ©es par un patch ou une mise Ã jour. Garder son systÃ¨me Ã jour permet de limiter les risques aux vulnÃ©rabilitÃ©s non patchÃ©es. Notons que des solutions permettant de faire du virtual patching permettent de diminuer les risques et peuvent combler les lacunes des systÃ¨mes difficiles Ã patcher :Deep Security - OfficeScan

2. Par dÃ©faut, bloquer lâ□□exÃ©cution de scripts sur son navigateur : Lâ□□activation des scripts sur le navigateur devrait se faire au cas par cas. Toutefois, la gestion des pages autorisÃ©es Ã exÃ©cuter des scripts peut Ãªtre trÃ¨s fastidieuse. NoScript est un module de Firefox qui permet de rÃ©pondre Ã ces attentes de sÃ©curitÃ© sans trop gÃªner lâ□□utilisateur.

3. Utiliser un antimalware efficace: Les solutions classiques fortement basÃ©es sur les signatures sont moins bien adaptÃ©es pour rÃ©pondre aux problÃ©matiques de sÃ©curitÃ© actuelles oÃ¹ un trÃ¨s grand nombre de menaces sont dÃ©couvertes dans un temps trÃ¨s court. Lâ□□utilisation de solutions basÃ©es sur la rÃ©putation doit Ãªtre prÃ©fÃ©rÃ©e : OfficeScan - Titanium