Alerte : des hackers russes exploitent la faille PDF

L'éditeur de sécurité Symantec vient de lancer une alerte concernant une attaque en cours exploitant la vulnérabilité découverte il y a un mois par le chercheur Petkov D.Petkov.

Heureusement, Adobe a finalement publié un correctif et de nouvelles versions des deux logiciels concernés, en l'occurrence : Acrobat et Reader. Ces patchs sont disponibles au téléchargement sur ce lien.

Grâce à cette publication, le risque est donc limité, mais l'éditeur de sécurité s'inquiète tout de même de la forte activité d'un gang de hackers russe qui essaye d'exploiter la faille sur les postes qui n'ont pas encore été vaccinés.

Ces malfaiteurs de la Toile procèdent d'une façon très simple. Il essaye de contaminer le poste cible avec un trojan rootkit, pour cela ils envoient à la cible des documents PDF malformés, et si ce dernier a le malheur de l'ouvrir il risque de se faire voler des données confidentielles.

Les pourriels utilisés portent différents intitulés. D'après Symantec les principaux sont : BILL.pdf, YOUR_BILL.pdf, INVOICE.pdf et STATEMET.pdf. Des titres qui font bien évidemment référence à un sujet personnel, comme le paiement d'une facture.

En ouvrant le PDF, l'utilisateur procède sans le savoir à l'installation d'un maudit cheval de Troie qui se comporte comme un Rootkit, c'est-à-dire qu'il cherche à se dissimuler au cœur du système en maquillant les traces de son activité.

Ce trojan baptisé « Pidief.a » est également capable de fermer le pare-feu afin de se mettre à jour en dialoguant avec les serveurs de la RBN Russian Business Network (ndlr : hébergeur russe suspecté de travailler étroitement avec des cybercriminels), une fois cette action terminée, il télécharge deux nouveaux Rootkit…

D'après *Computer World*, ce gang s'est déjà fait connaître en septembre 2006, en utilisant une approche très similaire. Les hackers russes exploitaient alors une vulnérabilité zero-day dans le langage XML : VML (Vector Markup Language).

Pour conclure, rappelons que seuls les utilisateurs de Internet Explorer 7 et Windows XP et Windows Server sont vulnérables.

Pour en savoir plus sur la RBN suivre sur ce lien.