

### **Phishing : Vecteur d'attaque privilégié : PDF, Word ou ZIP ?**

#### **Sécurité**

Posté par : JerryG

Publié le : 15/9/2014 13:30:00

Comme vous le savez, la malveillance informatique utilise toujours des tactiques de pointe pour optimiser les résultats de chaque campagne lancée. Au cours des derniers mois, nous avons suivi un lanceur de menace particulier dont l'arme favorite était les documents PDF exploitant la faille CVE-2013-2729.

La campagne a débuté par de grandes vagues d'e-mails contenant des PDF au contenu nuisible. Néanmoins, au fil des mois, nous avons observé une diversification des tactiques employées. Au lieu d'utiliser un seul vecteur d'attaque pour distribuer ses logiciels malveillants, le pirate a multiplié les approches.

#### **Par exemple, nous avons observé l'envoi d'e-mails contenant les combinaisons d'attaques suivantes :**

• URL vers un PDF au contenu nuisible + URL vers un logiciel malveillant • l'intéressé reçoit un fichier ZIP

• PDF en pièce jointe + URL vers un logiciel malveillant • l'intéressé reçoit un fichier ZIP

• PDF en pièce jointe + URL vers un document Word au contenu nuisible (CVE-2012-0158)

• Fichier ZIP en pièce jointe contenant le logiciel malveillant

Lors d'une campagne de ce type, nous avons observé que les documents au contenu nuisible et les fichiers ZIP contenaient trois types de logiciels malveillants, chacun ayant plusieurs variantes. Et, comme d'habitude, la plupart des exécutables n'étaient quasiment jamais détectés par les moteurs d'antivirus !

Ces campagnes soulignent combien les pirates tentent systématiquement de nouvelles approches pour infecter les utilisateurs. Et même si les campagnes de grande ampleur à base de kits d'exploits subies l'année dernière sont moins nombreuses aujourd'hui, celles reposant sur les pièces jointes semblent être en augmentation.

À l'origine, les documents à contenu nuisible n'étaient utilisés que par des lanceurs d'APT de très haut niveau. D'ordinaire, il semble qu'un certain nombre de cybercriminels sont entrés dans la danse. C'est un bon exemple de la manière dont les pirates repoussent sans cesse les limites pour installer des logiciels malveillants. Et cela montre à quel point le paysage des menaces informatiques est en perpétuelle évolution, conclut Ismet Geri, Directeur de Proofpoint France et Europe du Sud.