Vie et mort d'une signature Antivirus

La Haye. -Tout démarre facilement, un peu trop aisément d'ailleurs. Un *hacker*du côté de l'attaque qui contrôle un voire plusieurs serveurs. Ces serveurs ont sous leur pouvoir des *Botnets*, plusieurs **ordinateurs zombies** (infectés à l'insu de leur propriétaire) qui vont alors formuler des **attaques sous forme de *phishing* (hameçonnage) ou DOS***(deny of service)*

C'est là un type d'attaque aux « vertus » multiples qui vont alors pouvoir chercher des informations telles que des données sensibles pour une société ou un particulier. Bien souvent il s'agit de saisir des **informations bancaires** ou des identifiants de compte. Candid Wüest explique qu'outre la démarche, la **différence de législations joue en faveur des pirates** : « *Le problème est que dans certains Etats, faire tourner ou observer des données bancaires n'est pas à proprement parler légal mais n'est* ***pas illégal non plus*****«** .

Dès lors, le chercheur intervient pour trouver la nature du document infecté. Partant d'un fichier en .gif, il va le renommer puis l'ouvrir avec différents programmes et logiciels. Le spécialiste va même tenter de le dézipper et là… c'est le drame. On se rend alors compte qu'en décompressant le fichier, d'autres **programmes*a priori* invisibles vont s'introduire dans la machine**. « *On plonge alors plus profondément dans le cod*e » confie Candid Wüest « *et on peut trouver comment préparer une* ***contre-mesure*****«** .

En tout, il ne faudra que **15 minutes**, entre la prise de connaissance d'un *malware* jusqu'à l'émission d'une nouvelle signature. Après l'édition de cette signature, elle est intégrée à la base de données de l'éditeur.

A en croire le spécialiste, après cela tout va bien dans un monde presque parfait. Sauf que surgissent parfois des failles dans certains programmes comme Adobe , ce qui provoquent bien des déboires de la part de *malwares* déjà existants et dont les spécialistes pensaient avoir trouver la parade. Baptisé « **Neosploit**« , le kit d'outil pour pirates avait attiré l'attention des chercheurs de l'**US CERT** (*US Computer Emergency Response Team*) et de Secure Computing. Un kit capable de faire tomber les sécurités des fichiers pdf.

Bref, la guerre anti-malware a donc bien lieu. Elle est loin d'être finie.