Microsoft propose une parade au ver Koobface

Après avoir fait quelques ravages sur les postes de certains utilisateurs peu méfiants, le ver **Koobface** pourrait perdre du terrain. Dans un post sur le blog du **MSRT** (*Malicious Software Removal Tool)*, les équipes de Microsoft ont expliqué qu'elles avaient pu **intégré la parade au ver dans leur utilitaire anti-malware.**

Pourtant Kooface a connu plusieurs moutures qui l'ont conduit à**infecter de nombreux utilisateurs**. Il faut croire que le ver et ses nouvelles variantes a pu se diffuser sur tous les réseaux. **MySpace**, Bebo ou encore Hi5 auraient été aussi sujets à la menace. A la loupe, la technique peut fonctionner sur tous ces sites. **Le ver se connecte à l'une de ces adresses légitimes via les identifiants récupérés** dans les cookies d'un utilisateur. Il cherche ensuite à i **nfecter un nouvel ami auquel est envoyé un message**. Simple et efficace.

Les responsables de Microsoft dévoilent en détail les **caractéristiques du malware**. Dans son commentaire, Scott Molenkamp, chercheur au MSRT indique que « *cette famille de virus n'est pas seulement de la catégorie des vers mais plutôt un **amas de composants différents.** Chacun d'entre eux peut alors agir pour des tâches différentes les unes des autres. Elle peut ainsi coupler le **téléchargement**, **l'hébergement de pages Web**, le **vol de mots de passe** ou encore l'envoi d'identifiants vers des contacts de différents sites de réseaux sociaux***« .**

A la pelle, les sites désormais « protégés » par Microsoft sont, selon l'éditeur : Bebo.com, **Facebook**, Friendster, Fubar.com, hi5.com, LiveJournal, MySpace, myYearbook, Netlog et Tagged. Des cibles du ver Koobface dont beaucoup sont utilisés aux Etats-Unis. **Nulle mention de Twitter et LinkedIn, pourtant touchés par Koobface.**

L'intégration de la parade dans le *Malicious Software Removal Tool*va permettre de nettoyer les postes infectés et permettre d'y voir un peu plus clair quant au nombre d'infections de rang mondial.

Pour autant la vigilance ne doit pas être relâchée dans le sens où les méthodes de piratage de réseaux sociaux ont déjà évolué vers des techniques bien plus fines. Des **faux messages sont désormais envoyés proposés par certains de vos (vrais-faux) amis** contenant des vidéos sur des sites piégés. Là encore, toute prudence est requise.