2007 : une année record pour les 'malwares'

En 2007, les solutions Eset ont balayé plus de quatre milliards de messages. Bilan des courses parmi ceux-ci, Eset affirme que près de **34 millions** contenaient des fichiers malicieux, *« un record dans le monde des malwares »* précise le communiqué du groupe.

« L'année 2007 nous a appris que le monde en ligne fourmille de logiciels malicieux et que les attaquants sont loin d'être en manque d'inspiration. Les vecteurs d'attaque sont très variés, mais utilisent souvent la faiblesse humaine pour pénétrer les systèmes », déclare Pierre Marc Bureau, chercheur en malwares pour Eset.

La menace Mac

« À l'automne 2007, nous avons observé une des premières attaques visant autant les PCs utilisant Windows de Microsoft que les ordinateurs Apple qui utilisent le système d'exploitation OS X. Le vecteur d'infection de cette attaque est d'inciter une victime à télécharger et à installer un faux codec » commente Bureau.

Le malware s'attaquant à OS X a un comportement semblable à celui de Win32/Zlob mais est beaucoup plus rudimentaire en comparaison des menaces avancées qui s'attaquent à Windows. Si un utilisateur exécute ce fichier malicieux, il doit entrer son mot de passe administrateur pour que le malware puisse effectuer ses opérations malicieuses.

La charge active du malware est de modifier la configuration de serveur de noms (DNS) de la victime, pour que toutes les requêtes DNS faites par un ordinateur infecté soient dirigées vers un serveur appartenant aux attaquants. Ce serveur peut ensuite être utilisé pour rediriger les visiteurs de sites bancaires vers des sites frauduleux utilisés pour voler ces informations sensibles.

Faux codecs

Un des vecteurs d'infection les plus populaires en 2007 a été l'installation de faux codecs. Des pirates ont enregistré une multitude de sites Web et les ont annoncés sur les sites de recherche comme Google et Yahoo. Les utilisateurs cherchant un "codec", c'est-à-dire un logiciel d'encodage et de décodage de flux vidéo, étaient dirigés vers ces sites malicieux.

Les utilisateurs qui acceptent de télécharger et d'exécuter les fichiers exécutables se trouvant sur ces sites infectent leurs ordinateurs avec une multitude de malware.

La famille de malware Zlob est connue pour utiliser fréquemment cette technique d'ingénierie sociale comme vecteur d'infection.

Nuwar (Storm Worm)

Son nom (Storm Worm), provient de la première grande campagne de spam qui a été menée pour le distribuer au mois de janvier en référence à la tempête Kyrill.

Premièrement, cette menace est l'une des premières à utiliser un réseau P2P pour sa communication de commande et contrôle. Enfin, le fait que Nuwar utilise un réseau décentralisé

pour communiquer fait en sorte qu'il est très difficile pour la communauté de chercheurs d'évaluer le nombre de systèmes infectés.