Alerte : ‘Storm trojan’ refait surface

D’après les chercheurs en sécurité du laboratoire de Postini :*« Cet email est envoyé massivement dans les boîtes de réception du monde entier. Il s’agit du spam le plus virulent de ces douze derniers mois. »*

Ironie de l’histoire ce pourriel met en garde contre une attaque puisque qu’il porte l’un de ces intitulés : *« Worm Alert!, Worm Detected, Spyware Detected!, Virus Activity Detected! »*.

En réalité, ce spam dissimule un fichier .ZIP qui se présente comme étant un patch de sécurité nécessaire pour se protéger contre une attaque en préparation.

Ce message alarmant à un rôle précis. En l’occurrence, inciter l’internaute à cliquer sur un lien de téléchargement contenant un fichier malveillant. Pour ajouter à la vraisemblance du message d’alerte les pirates ont ajouté un mot de passe au fichier .ZIP.

En réalité, le fichier est une variante du ver Storm Trojan. Ce dernier installe un rootkit qui va se dissimuler dans le système, éteindre l’ensemble des applications de sécurité installées, et dérober des informations confidentielles.

Le pirate ajoute ensuite cette nouvelle victime à son réseau de PC zombies.

Postini a identifié **5 millions de copies de ce pourriel** dans les dernières 24 heures. À ce rythme, certains experts estiment qu’il pourrait passer la barre des 60 millions de mails rapidement.

Notamment parce qu’il a la capacité de se reproduire et de se propager à l’ensemble de la liste de contacts de sa première victime. Ce Storm Trojan semble se mettre à jour et communiquer avec son « maître » par l’intermédiaire d’un réseau P2P.

Le Centre Security Response de Symantec, confirme le phénomène et donne un peu plus de détails, en particulier le nom du fichier qui s’exécute, **wincom32.sys**, plus connu sous le nom de **Trojan.Peacomm.** Un correctif est disponible sur le site de l’éditeur.