StormWorm : de la tempête à la mer d'huile

Profitant de la conférence Toorcon dédiée à l'univers du hacking -qui se déroule à San Diego- le spécialiste de la sécurité, Brandon Enright, a dressé le bilan de l'évolution de la propagation de ce maudit canasson.

Pour lui, s'il y a effectivement eu une forte augmentation du code malveillant au début de cette année 2007, depuis le mois de juillet la tendance s'est inversée et le phénomène est de nouveau sur le déclin.

Interrogé dans les colonnes de *Vnunet.com*, le chercheur a expliqué que : *« la taille du réseau botnet associé à Zhelatin diminuait rapidement et de façon constante depuis plusieurs mois ».*

Le chercheur américain a notamment souligné l'incroyable tentative de contamination organisée par un gang de hackers au mois de juillet. Ces derniers avaient concocté une attaque utilisant le mail comme point de départ. Suite à cette affaire, l'on estimait que près de 1,5 million de machines avaient été contaminées. Or selon Enright la réalité est bien différente. Selon lui seulement 200.000 machines ont effectivement été touchées.

Depuis cette période, les éditeurs d'antivirus ont presque tous publié des correctifs afin de nettoyer et corriger les erreurs provoquées par le code. Enright a également rappelé que Microsoft avait publié une mise à jour pour de son outil Microsoft Malicious Software Removal Tool, afin de définitivement contrer ce problème.

Ces efforts conjoints des grands éditeurs ont permis de réduire la taille du réseau Storm Worm. Aujourd'hui, il ne compterait plus que 160.000 machines dont 20.000 infectés et accessibles, par les hackers. La recherche menée par Enright a été réalisée avec les données statistiques de l'éditeur moscovite Kaspersky.

« Le mois de septembre a été particulièrement calme » a précisé Kaspersky. Reste que l'on ne sait pas encore si les chiffres de l'éditeur sont authentiques ou bien si les auteurs de Zhelatin ont décidé de faire un « break » en attendant que la publicité autour du réseau StormWorm se calme.

Pour la petite histoire, ce nom « Storm Worm » qui fait référence à une rafale de vent, remonte à l'époque des premières attaques, car au début, les pourriels envoyés par les cybercriminels évoquaient l'arrivée prochaine de violentes bourrasques sur l'Europe.