Alerte : le cheval de Troie Dialer.PZ!tr se diffuse rapidement

Ce maudit canasson a été conçu pour composer des numéros sur-taxés longue distance, d'où son nom de Dialer.

Il l'emporte à nouveau sur W32/Bagle.DY@mm et Netsky.P@mm.

En avril 2007, l'équipe mondiale de recherche en sécurité informatique avait présenté les différents stades du cycle de vie du W32/Dialer.PZ!tr : conception dynamique, production à la chaîne, reporting statistique intelligent, stratégie de déploiement géographique… De quoi sérieusement inquiéter les RSSI !

W32/Dialer.PZ!tr a démarré au mois de juin, exactement au même niveau où il se trouvait fin mai. Son taux de détection est de l'ordre de 14%. Il s'est déployé au grand galop au Mexique et aux États-Unis, sous l'effet d'une campagne de diffusion agressive et continue. La menace a également été détectée dans bien d'autres régions du globe.

« L'approche de l'été, une période de l'année particulièrement propice aux contaminations, semble avoir inspiré les créateurs aguerris de ce logiciel malveillant. », déclare Guillaume Lovet, responsable de l'équipe de recherche des menaces, chez Fortinet.

« Ces derniers ont donc été bien occupés à développer un nouvel ?emballage' pour leurs créations malveillantes qui ? tout du moins l'espèrent-t-ils ? franchiront sans encombre les frontières virtuelles sans être repérées par les dispositifs de sécurité informatique. »

Guillaume Lovet poursuit son explication précisant : *« les auteurs du logiciel malveillant en ont modifié un composant lors du processus de création. Plus précisément, ils ont combiné W32/Dialer.PZ!tr avec une nouvelle variante d'UPX, un compresseur de fichiers très répandu. Le premier spécimen exploitant ce nouveau compresseur a été créé le 21 juin dernier. »*