Panda lance une alerte au 'malware' SpamtaLoad

PandaLabs a détecté un grand nombre d'emails contenant le cheval de Troie SpamtaLoad.DO. De fait, ce '*malware*' a représenté jusqu'à**40%** des messages infectés reçus par PandaLabs chaque heure.

Ce cheval de Troie atteint les systèmes via des emails à l'objet et au texte variables. Par exemple : ?Error?, ?Good day?, ?hello? ou ?Mail Delivery System?.

Texte de l'email :

-« Mail transaction failed. Partial message is available. »

-« The message contains Unicode characters and has been sent as a binary attachment. »

Le cheval de Troie est contenu dans le fichier exécutable joint au message qui porte un nom variable.

Si l'utilisateur exécute le fichier, SpamtaLoad.DO affiche un faux message d'erreur ou ouvre le Bloc-notes et un texte s'affiche. Le cheval de Troie télécharge alors le ver Spamta.TQ sur le système. Ce ver est conçu pour réexpédier SpamtaLoad.DO à toutes les adresses email trouvées sur l'ordinateur compromis.

« L'infection des ordinateurs par ce type de code malicieux n'est pas le but en soi des pirates. Dans la plupart des cas, ils servent à distraire l'attention des éditeurs de solutions de sécurité. Pendant que ces derniers concentrent leurs efforts pour éliminer ces malwares, les cyber-criminels en profitent pour lancer silencieusement d'autres codes malicieux. Ces autres spécimens sont généralement beaucoup plus dangereux, » explique Luis Corrons, directeur technique de PandaLabs.

Les vers et chevaux de Troie de la famille Spamta ont été très actifs au cours des dernières années. PandaLabs a détecté plusieurs vagues d'infections dues à cette famille de codes malicieux, la dernière datant de novembre dernier.

« Lors de ces vagues d'attaques, de nombreuses variantes de la même famille ont été mises en circulation pendant une période très courte. Les utilisateurs doivent redoubler de prudence, puisque ce cheval de Troie pourrait être le signe annonciateur d'une nouvelle vague d'attaques », indique Luis Corrons.