

Des spammeurs utiliseraient des messages 'subliminaux'

Sophos, éditeur spécialisé de la sécurité des réseaux, vient d'identifier un nouveau message intrusif ou 'spam' de manipulation d'actions boursières qui contient une animation graphique dispensant un message caché, insidieux dit 'subliminal' visant des internautes susceptibles de vouloir placer de l'argent.

Ces images, au format GIF, sont constituées d'une série de cadres montrés en succession. Ce procédé est fréquemment utilisé dans l'animation de sites Web, mais il vient d'être adopté par des spammeurs qui tentent vraisemblablement de tromper la détection par les filtres 'antispams'.

Dans le cas de la campagne repérée par les analystes de SophosLabs, le document texte, présenté sous forme d'image, vise faire monter artificiellement le prix des actions d'une entreprise appelée Trimax.

Mais, contrairement à la plupart des courriels similaires, celui-ci affiche brièvement, toutes les 15 secondes environ, le message 'BUY !!!'.

Ce 'BUY !!!' est comparable aux messages subliminaux parfois utilisés dans les publicités télévisées de certains pays, afin d'influencer le subconscient des téléspectateurs.

« Les spammeurs envoient souvent leurs messages sous forme d'images animées dans l'espoir d'empêcher les filtres antispam de les identifier par une reconnaissance optique des caractères », souligne Annie Gay, vice-présidente de Sophos Europe Continentale, Moyen-Orient et Afrique.

« Celui-ci tente d'être 'subliminal', mais on peut douter qu'il parvienne vraiment à pousser subconsciemment les investisseurs à acheter des actions. Par ailleurs, les solutions antispams sophistiquées, telles que celles développées par Sophos sont parfaitement capables de protéger les utilisateurs contre ce type d'astuce. »

Les campagnes de spams boursiers, dites 'pump-and-dump', fonctionnent ainsi : les spammeurs achètent à bas prix des actions d'une compagnie, puis font monter leur valeur en incitant d'autres acheteurs à en faire autant (souvent en diffusant massivement de 'bonnes nouvelles' sur l'entreprise). Ils se hâtent ensuite de les revendre en tirant profit de la hausse. Les experts de Sophos estiment que ce type de campagne constitue environ 15 % de l'ensemble du spam diffusé, contre seulement 0,8% en janvier 2005.

Plus généralement, 2006 a également connu une forte augmentation du nombre de messages de spams contenant des images, qui sont passés de 18,2% du total en janvier à plus de 35% aujourd'hui. Cette méthode est censée éviter d'être détectés par certains filtres antispam reposant sur l'analyse du contenu textuel des courriels.

« Ce type de messages en images circule dans le monde entier, non seulement en anglais, mais aussi par exemple en russe et en italien », poursuit Annie Gay.

« Il est probable que les spammeurs vont utiliser cette technique de plus en plus fréquemment, pour

contourner les systèmes de filtrage. »