Après les PDF, les spams XLS font leur apparition

Point clé de ce type d'attaques, l'utilisation de la pièce jointe pour aguicher leur cible. Cet élément est indéniablement la nouveauté marquante parmi les pratiques utilisées par les spammeurs pour déjouer les filtres anti-spam.

À peine moins de quinze jours après les spams PDF (*lire notre article*), les spams XLS se diffusent partout. Il s'agit d'un courrier contenant une pièce jointe au format Microsoft Excel dans laquelle on trouve des informations incitant le lecteur à acheter des actions en bourse ou des substances dopant la sexualité.

La particularité d'un spam embarqué dans un tableur est que le spammeur peut jouer avec le contenu, la position, la fusion et l?alignement des cellules dans le but de brouiller les pistes face aux barrières anti-spam. Cette pratique n'est pas nouvelle, elle était déjà employée avec les tables dans les messages HTML.

Dans l'exemple ci-dessus, nous lisons clairement le mot VIAGRA. Seulement si l'on analyse le contenu, il n'y a quasiment qu'une lettre par cellule. Les cellules C5 et C6 ont été fusionnées, même chose pour les cellules E1-E2-E3-E4 et E5.

La colonne F est vide et a été diminuée en taille pour ne plus qu'elle soit visible à l'?il. Tout cela est fait dans le but de tromper les moteurs de filtrage reposant sur l'analyse littérale du contenu des cellules.

Mathieu Tarnus, directeur marketing de GoTo Software explique: « *Chez GoTo Software nous avons anticipé l'évolution de cette pratique dans le développement de la technologie Vade Retro. Nous nous appuyons aujourd'hui sur de nombreuses autres méthodes pour identifier la nature du message. Certaines techniques nous permettent même d'isoler de grandes vagues de spams avant qu'elles ne se propagent. Notre technologie est aujourd'hui distribuée en Russie et au Japon. Etant donnée l'hétérogénéité des langages, il est inconcevable que nous nous basions sur l'analyse sémantique du message pour en déterminer la nature*. »

Le message, détecté par le laboratoire de la technologie de filtrage Vade Retro dans la nuit de samedi 21 à dimanche 22 juillet ressemble à cela: