Amateurs de bons plans : attention aux chevaux de Troie
Une nouvelle vague de spam est actuellement en cours et cible cette fois les amateurs de bons plans avec la supposée liquidation du site marchant MOOO.COM et des rabais jusqu'à 95%.

Un faux site marchand
En réalité, le site MOOO.COM n'est pas un site marchand, mais un service DNS, avec des sous-domaines configurés pour des actions ciblées. Ralf Benzmüller, directeur du laboratoire de sécurité de G Data précise que « jusqu'à présent, les scripts de transfert ont été utilisés pour mener les internautes vers des sites spécifiques. L'utilisation d'un service DNS pour le transfert n'avait pas été exploitée jusqu'à présent par les pirates. A nouveau on constate que les cybercriminels s'appuient sur une approche ciblée basée sur l'ingénierie sociale pour toucher leurs victimes ».

Une offre alléchante, du spam et un cheval de Troie Buzus
Au cœur du dispositif ; une offre alléchante annonçant -95% pour cause de liquidation soutenue par une campagne de spam. Dans les e mails spam, les pirates y ont glissé un lien vers le fichier « ausverkauf.exe », qui contient une version du cheval de Troie Buzus. Pour les internautes, il s'agit d'un lien pour accéder aux produits soldés.

Les conséquences
Les chevaux de Troie de la famille Buzus analysent les systèmes de leurs victimes et transfèrent aux pirates les données personnelles (cartes bancaires, banque en ligne, e-mail et accès FTP). Le malware tente ensuite de diminuer les paramètres de sécurité de l'ordinateur pour le rendre plus vulnérable et plus accessible.

Les conseils G Data :
- Ne jamais ouvrir les emails dont le destinataire est inconnu ou « unrequested ».
- Ne pas accepter le téléchargement qui se lance via un lien dans un e-mail.
- Utiliser un scanner de virus avec un filtre http comme celui proposé par G Data qui bloque les contenus Web nuisibles, avant qu'ils n'atteignent le navigateur Internet et protège contre les conséquences fâcheuses.