LinkedIn victime du malware Zeus

Victime de son succès, le réseau social à caractère professionnel **LinkedIn** est de plus en plus utilisé par les cybercriminels pour identifier des cibles potentielles d'utilisateurs. Selon l'entreprise de sécurité Trusteer, **des spams ressemblant fortement aux messages de notifications ont envahi le site communautaire**.

Lorsque l'utilisateur clique dessus il est alors renvoyé vers un serveur basé en Russie qui permet aux hackers d'installer frauduleusement un malware, et notamment **le cheval de Troie Zeus 2**. Une fois sur l'ordinateur, Zeus transmet les données sur un serveur à Zhejiang en Chine.

Cette technique classique de phishing (hameçonnage) est souvent utilisée pour les fraudes bancaires. Mais dans le cas d'une attaque sur LinkedIn, **elle sert surtout à accéder aux informations confidentielles d'une entreprise** stockées sur un ordinateur mais également sur son réseau.

68% des entreprises sont d'ailleurs susceptibles de cliquer sur ce type de message rapporte Trusteer. **Mickey Boodaei**, le P-dg, ajoute que «*c'est extrêmement dangereux car beaucoup d'utilisateurs cliquent presque automatiquement sur ces liens sans essayer de vérifier leur authenticité*». LinkedIn envoie pourtant régulièrement des avertissements pour signaler de se rendre sur le site de la personne en question avant d'approuver sa demande d'ajout.

Mais il est de plus en plus difficile d'identifier ce type de phishing et de *malware*. Trusteer conseille donc de **ne jamais ouvrir les e-mails provenant des réseaux sociaux** et encore moins de cliquer sur les liens qu'ils contiennent. Efficace mais radical. *«Il faut directement passer par le réseau social*», conseille Mickey Boodaei. Tout simplement.