

Les utilisateurs de Twitter touchés par l'attaque de phishing 'LOL' **Des milliers de comptes ont été compromis par des pirates cherchant à créer un réseau zombie sur le Web 2.0**

Paris, le 22 février 2010 – Sophos, un des leaders mondiaux de la sécurisation et de la protection des données, avertit les utilisateurs de Twitter que la vaste attaque menée contre eux au cours du week end avait pour objectif de leur dérober leurs mots de passe et d'exploiter ces comptes piratés pour lancer des campagnes de spam.

Toujours en cours, cette campagne a débuté ce samedi, lorsque des utilisateurs de Twitter ont découvert que des membres du réseau de micro-blogging leur avaient posté des messages présentés comme humoristiques, mais en réalité conçus pour récupérer des mots de passe. Ces messages débutent par des phrases telles que « Lol. this is me?? », « lol, this is funny. », « Lol. this you?? » ou « ha ha, u look funny on here », suivies de liens renvoyant l'utilisateur vers une fausse page d'accueil Twitter hébergée par un site Web basé en Chine.

« Les cybercriminels à l'origine de cette attaque cherchent à créer un réseau zombie, un botnet, de comptes piratés qu'ils utilisent ensuite pour envoyer du spam, diffuser du code malveillant ou dérober d'autres coordonnées », commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos Europe du Sud. « Il n'y a rien de drôle dans cette attaque 'LOL'. Si vous avez été piégé par ces liens, ou si vous découvrez dans votre boîte d'envoi des messages que vous n'avez pas écrit, vous devez changer immédiatement votre mot de passe Twitter. »

Les experts de Sophos ont découvert que bien que la majorité des messages infectés ait circulé via des échanges privés entre utilisateurs individuels, des liens dangereux ont également été postés sur des listes publiques. Cela signifie que même des personnes qui ne sont pas officiellement inscrites sur Twitter peuvent en être victimes.

« Ces messages sont partagés d'autant plus largement qu'ils sont relayés par des services tels que GroupTweet, qui étendent la fonctionnalité Twitter standard de messagerie directe (DM) pour permettre des envois vers des destinataires multiples, voire même les rendre publics », poursuit Michel Lanaspèze. « C'est ainsi qu'on a pu voir des comptes Twitter avertir leurs 'suiveurs' de cette campagne de phishing, pour ensuite en être eux-mêmes victimes. »

Selon Sophos, cette campagne porte déjà ses fruits, puisque les pirates ont commencé à distribuer du spam proposant du Viagra à partir des comptes compromis.

« Tant que les utilisateurs de Twitter piratés ne changeront pas leurs mots de passe, les intrus pourront continuer à diffuser du spam via leurs comptes », conclut Michel Lanaspèze. « Les cyber-attaques lancées via les réseaux sociaux deviennent de plus en plus communes. Le rapport sur les menaces publié le mois dernier par Sophos a ainsi montré une augmentation de 70% du nombre d'utilisateurs signalant des attaques de spam et de malware via des sites de réseau social. »

Des informations complémentaires sur cette attaque sont disponibles sur le blog de Graham Cluley, à l'adresse <http://www.sophos.com/blogs/gc/g/2010/02/21/video-twitter-phishing>

A propos de Sophos.

Plus de 100 millions d'utilisateurs dans 150 pays ont retenu Sophos comme la meilleure défense du marché contre les menaces complexes et les risques de pertes de données. Ses solutions intégrées de sécurisation et de protection des informations sont simples à déployer, à administrer et à utiliser, et offrent le coût global de possession le plus avantageux du marché. Elles permettent le chiffrement des données, la protection des systèmes d'extrémité, la sécurisation du Web et de la messagerie et le contrôle d'accès réseau avec le support permanent des SophosLabs, le réseau mondial de centres d'analyse des menaces de Sophos. Avec plus de deux décennies d'expérience, Sophos est reconnu comme un leader de la sécurisation et de la protection des données par les principaux analystes du marché, et ses produits ont reçu de nombreuses récompenses.

<http://www.sophos.fr>