

Facebook – Otra brecha en el muro

George Lucian Petre

Al ser la red social más importante del momento, con un crecimiento espectacular en el último año, Facebook se ha situado en el punto de mira de importantes ataques cibernéticos que incluyen campañas de spam y distribución masiva de malware. Este estudio presenta el estado del phishing, el spam y otras amenazas que afectan a los usuarios de Facebook. Además, se explica cómo los datos privados de los usuarios están expuestos como resultado de los juegos en las redes sociales. En la última parte del estudio, mostramos a través de un experimento algunas fallas de seguridad que ocurren en estas redes sociales.

Palabras Clave - Facebook, Phishing, Spam, Ingeniería Social, Malware, Amenazas

I. INTRODUCCIÓN

De acuerdo con estadísticas dadas en su propia web [1], Facebook tiene más de 350 millones de usuarios en todo el mundo, cifra superior a la población de los Estados Unidos y que representa el 5,14% de la población mundial y el 20,18% de los usuarios de Internet en todo el mundo [2]. A esto hay que sumarle que más de 700.000 empresas tienen una página en Facebook. Con tales cifras, sin duda podemos decir que Facebook es el lugar ideal para que un usuario malintencionado ponga en marcha un plan de ingeniería social. Nuestro informe realizado para la conferencia de 2008 sobre spam [2] se centró en las amenazas asociadas con el análisis de redes sociales en un momento en que era difícil identificar ataques peligrosos en las redes sociales como Facebook e incluso encontrar muestras de ataques simples. Hoy en día podemos fácilmente identificar campañas de spam, con múltiples variantes de malware dirigidas contra usuarios de Facebook (Koobface), campañas de phishing destinadas a robar cuentas de Facebook o donaciones falsas para desastres como el terremoto de Haití, etc.

II. JUEGOS SOCIALES, UNA PUERTA HACIA EL USUARIO

Una cantidad considerable de nuevos juegos sociales como Farmville, Mafia Wars, Castel Age y otros aparecieron en la segunda parte de 2009. Para lograr un mejor resultado en estos juegos, los usuarios necesitan tantos amigos como sea posible. Por eso, como se muestra en la Fig. n^o. 1 nos encontramos con que muchos de los grupos están diseñados para obtener al instante un gran número de amigos.

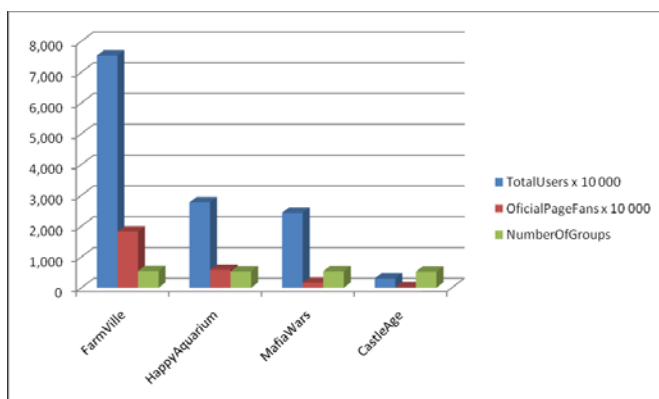


Figura. 1 - Un gráfico comparativo que muestra algunos de los juegos más populares en Facebook, incluyendo el número de usuarios, número de fans en la página principal y grupos dedicados a ellos

Estos grupos son el mejor lugar para que los spammers se cuelen en la lista de amigos de los usuarios. Para comprender mejor cómo estos spammers trabajan, nos unimos a algunos de estos grupos mediante un perfil "honeypot" de Facebook. Elegimos Farmville porque este es el juego más popular en Facebook. Nos unimos a varios grupos y añadimos nuestro perfil a varias listas de amigos. En el nuestro incluimos una foto, que publicamos en el muro del grupo junto con un mensaje que decía "add me as your neighbour" (añádeme como vecino). Tras añadir nuestro perfil al grupo, recibimos un mensaje de bienvenida, al cual contestamos. Después, recibimos un link a una web de video chat. Aunque este escenario es familiar para campañas de correo electrónico de spam, esta situación particular presenta algunas características distintivas:

- El usuario añade el spammer a su perfil, y no a la inversa, como ocurre en los mensajes de spam tradicionales. Esta es la razón por la que la acción de los spammers no constituye un abuso, por lo que su cuenta no puede ser suspendida.
- El spammer primero envía un mensaje de bienvenida. Esta es una estrategia para ganarse la confianza del usuario.
- Por último, después de la respuesta del usuario, el enlace a la página web de videochat se envía a través de un servicio de acortamiento de URLs, que no permite a los usuarios conocer el destino final de la página hasta que hace clic en el vínculo.
- El incluir fotos y otros detalles en el perfil del spammer hacen a éste parecer más humano

III. BROMAS Y FRAUDES

Los viejos hoaxes o engaños- como los que dicen "Si no reenvías este email, Yahoo eliminará tu cuenta- tienen ahora un enfoque más amigable: "NO, YO NO pagaré £ 3.99 al mes por USAR FACEBOOK desde el 9 de julio de 2010!" Este último título no es inventado. Es un grupo que cuenta con más de 888.594 miembros. Más de 500 grupos han clonado la idea y discuten acerca de las tarifas y las diferentes fechas en la que Facebook podría volverse de pago. Debido a la gran escala de este fenómeno, Facebook se vio obligado a negar estos rumores en un importante periódico [4]. Si los engaños tienden a ser más graciosos que peligrosos, hay, sin embargo, una gran cantidad de fraudes potencialmente peligrosos que aprovechan los llamamientos de organizaciones benéficas.

El terremoto en Haití provocó un flujo global de simpatía que se tradujo en considerables donaciones a través de varios canales en todo el mundo. Como resultado de esto, una gran cantidad de ataques de "phishing" se pusieron en marcha, y una cantidad considerable de aplicaciones o páginas de Facebook comenzaron a utilizar la idea de las donaciones a Haití como cebo.

Uno de los casos más interesantes trata sobre un grupo de Facebook que decía que donaría \$ 00,01 por cada usuario de Facebook que se convirtiera en fan de esa página. En sólo 5 días la página alcanzó la asombrosa cifra de 2.000.000 de fans. Poco después, se comenzaron a distribuir enlaces de spam a los usuarios a través de esta página. Después de alcanzar cerca de 2 millones de aficionados, la página fue cerrada por dicho abuso.

IV. PHISHING DE CUENTAS DE FACEBOOK.

A finales de octubre de 2009, nuestros honeypots de correo electrónico fueron el blanco de un ataque masivo de phishing diseñado para recoger las credenciales de los usuarios de Facebook. El ataque fue aún más vistoso porque, junto con el phishing, enviaba también una versión de Zbot [5]. Había dos métodos de entrega:

- Como un archivo adjunto de e-mail
- Como una aplicación enviada después de que el usuario se conectase a un sitio que simula ser Facebook.

Este tipo de ataques de phishing se conciben como un doble golpe: uno es el robot de spam que distribuye el malware y el phishing a través de e-mail y el otro es el robo de credenciales de la cuenta de Facebook que, como se desprende de nuestro experimento, comienza con la publicación de enlaces de malware y spam en los perfiles de los usuarios.

V. MALWARE EN FACEBOOK

Una considerable cantidad de gusanos se distribuyó masivamente a través de los muros de Facebook. El método era sencillo pero efectivo. Usando algunas cuentas robadas de facebook, los atacantes publicaron un enlace de malware asociado a una imagen provocativa y un mensaje atractivo. Algunos ejemplos son: Wanna C Somthin' HOT!?? (¿Quieres ver algo caliente?)|| My Ex-Girlfriend Cheated on me. Here is my revenge! (Mi exnovia me engañó. ¡Ésta es mi venganza) ||. Mientras que algunos de estos gusanos fueron sólo publicados dando lugar a entradas embarazosas en los muros de los usuarios, algunos de ellos distribuyeron malware a través de este método.

Puede sonar muy poco sofisticado, pero la confianza que uno tiene en los vínculos de sus amigos provoca que muchos terminen pinchando en esos vínculos, algo que no harían si el link llegase por correo electrónico.

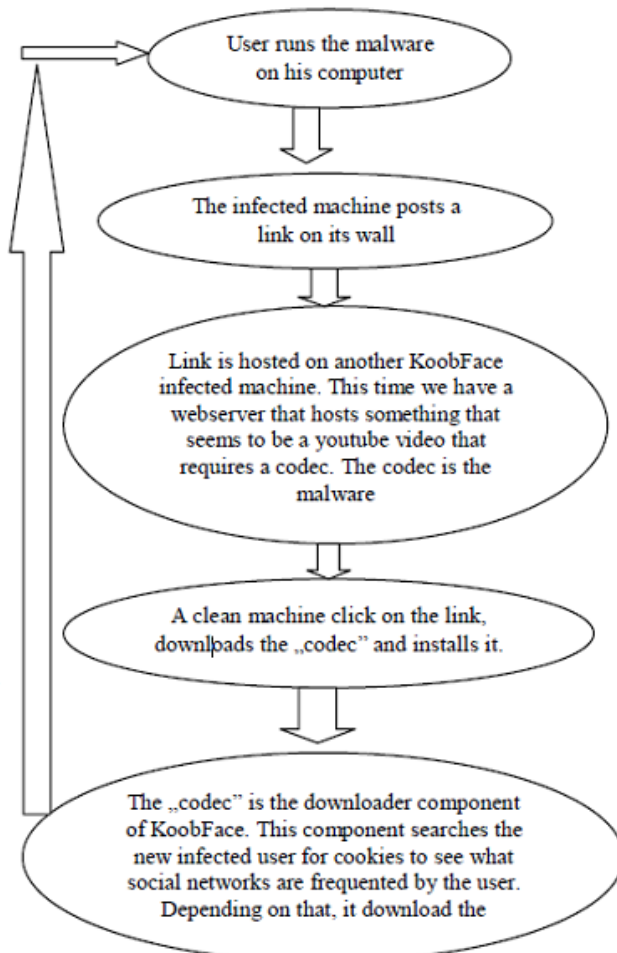


Fig 2: Proceso de KoobFace

VI. KOOFACE – UN EJEMPLAR DE MALWARE REVOLUCIONARIO

Koobface es el primer ejemplar de malware distribuido masivamente y diseñado especialmente para redes sociales. Koobface tiene muchos módulos, siendo uno de ellos el dedicado a la difusión por redes sociales. La clave del éxito de Koobface es el robo de reputación. Un usuario infectado comienza a publicar enlaces a un link de youtube falso. El link apunta, en realidad, a otra máquina infectada con koobface, que ejecuta otro componente de malware Koobface, llamado "Downloader" (el descargador). Una tabla con el esquema que sigue Koobface se puede ver en la figura. 2 El Usuario ejecuta el malware en su ordenador.

La máquina infectada postea un link malicioso en su muro de Facebook. El link está almacenado en otra máquina infectada. Y el proceso se vuelve a repetir.

En otro ejemplo tenemos un servidor web que aloja lo que parece ser un video de youtube que requiere un códec. El codec es en si el malware. Un equipo limpio, hace clic en el enlace, descarga el codec y lo instala. El codec es el componente que descarga Koobface. Este componente busca en el ordenador del nuevo usuario infectado "cookies" para ver qué redes sociales frecuenta el usuario. En función de eso, descarga los componentes más adecuados a su red social.

VII. EXPERIMENTO SOBRE LA ACEPTACIÓN DE LOS USUARIOS

Una de las razones principales para que un sistema de ingeniería social tenga tanto éxito en las redes sociales es que los atacantes pueden fácilmente entrar en el círculo de amigos de confianza de los usuarios. Se realizó un experimento para observar y analizar con qué facilidad los usuarios de Facebook pueden ser engañados para agregar personas desconocidas como amigos.

Hemos creado los siguientes tipos de cuentas: un perfil sin foto y que contiene tan pocos detalles como es posible (perfil 1), un perfil con una foto y algunos detalles (perfil 2) y otro perfil con una gran cantidad de detalles e imágenes (perfil 3). Con cada perfil nos unimos a algunos grupos de interés general para hacer unos cuantos amigos: —Bitch Please. I'm from New York||, —BMW||,

—ADDICTED TO FAMILY GUY||, —Chocolate = Love ♥ !!!||.

Nuestro primer intento de socializar no supuso bastante esfuerzo. Apenas una hora después de empezar a agregar personas a cada perfil, logramos 23 conexiones con el perfil 1, de 47 con el perfil 2 y 53 con el perfil 3.

Posteriormente, nos unimos a grupos relacionados con juegos sociales, y comenzó a añadir amigos. En este caso, tuvimos aún más éxito. Como resultado, después de 24 horas de seguimiento de todos los perfiles, las estadísticas muestran: 85 amigos para el perfil 1, 108 para el 2 y 111 para el perfil 3.

El paso 3 consistió en agregar a amigos mutuos de aquellos que ya eran nuestros amigos. El éxito fue de nuevo muy grande porque más del 50% de amigos en común aceptaron una relación con nuestro perfil.

La última parte del experimento se centró en la publicación de una url desde bit.ly sin texto en cada uno de los 3 perfiles y observar cómo muchas personas lo siguieron. El experimento mostró que alrededor del 24% del total de los amigos de los perfiles siguieron el enlace, aunque no sabían de qué trataba el enlace ni a dónde iba.

VIII. CONCLUSIONES

Este estudio de las amenazas que enfrentan los usuarios de Facebook reveló que a partir de 2008 los ataques son mucho más complejos que antes.

Como se muestra en el experimento de la aceptación, los usuarios están más dispuestos a aceptar a los spammers en su lista de amigos cuando se encuentran en una red social que en cualquier otro entorno en línea de comunicación. Esto provoca que el spam y los sistemas de ingeniería sean más efectivos con estos usuarios que con otros que reciben las amenazas por correo electrónico, por ejemplo.

Por otra parte, hemos visto que en las redes sociales, los usuarios pueden ser engañados para agregar a su perfil de los spammers.

Para concluir, podemos decir que Facebook es la red social más popular en este momento, pero también es, por ello, la red social más expuesta a este tipo de ataques.

REFERENCIAS

1. Facebook Statistics. [clic aquí](#)
2. Internet World Stats [clic aquí](#)
3. Cosoi C. , Petre G. – Spam 2.0 (Workshop) – MIT Spam Conference 2008,Cambridge, MA, USA
4. Telegraph [clic aquí](#)
5. ZBot Trojan Explained [clic aquí](#)
6. The real face of Koobface – J. Baltazar, J. Costoya, R. Flores, Trend Micro Threat Research
7. Is Britney Spears Spam? - A. Zinman, J. Donath - CEAS 2007 – Fourth Conference on Email and Anti-Spam, August 2-3, 2007, Mountain View, California USA
8. Brazen Black Hats: How we fight online fraud in a socially networked world – V. Sharma- VB 2009, Geneva, Switzerland
9. Socialnetworkkeering: or, the friend of my friend is my enemy – A. Lee - VB 2009, Geneva, Switzerland
10. <http://fitzgerald.blog.avg.com/2009/11/new-facebook-worm-dont-click-da-button-baby.html>
11. <http://mashable.com/2010/01/29/facebook-revenge-worm>