Boletines PandaLabs:

Redes Sociales en el punto de mira

wwwpandasecurity.com/homeusers/security_info | www.pandalabs.com

Índice

1.- Introducción

Una red social se define como un servicio basado en Internet que permite a los individuos construir un perfil público o semi-público dentro de un sistema delimitado, articular una lista de otros usuarios con los que comparten una conexión, y ver y recorrer su lista de las conexiones y de las hechas por otros dentro del sistema. La naturaleza y la nomenclatura de estas conexiones pueden variar de un sitio a otro [1].

Vivimos en un mundo cada vez más globalizado y en el que contamos con diversos mecanismos que permiten salvar las barreras geográficas. El concepto de comunicación tal y como lo conocíamos ha cambiado y las redes sociales se han convertido en una herramienta de gran utilidad en ese nuevo concepto de relación entre las personas: una comunicación global.

Se han creado auténticos mundos virtuales gracias a las redes sociales, en los que millones de personas se comunican y comparten sus conocimientos, aficiones, inquietudes, emociones...

El número de usuarios de este tipo de redes sociales ha aumentado considerablemente en los últimos años. Existe una amplia variedad de redes sociales que se diferencian por su temática, funcionalidades, estética, etc., pero el concepto es el mismo: poner a disposición del usuario una herramienta que le permita comunicarse con otros usuarios.

Sin embargo, desde hace unos años, la popularidad y la confianza que ofrecen las redes sociales está siendo aprovechada por los ciberdelincuentes, que han encontrado una nueva vía de explotación de sus actividades fraudulentas.

En este artículo nos acercaremos al origen y cronología de estas redes, analizaremos las razones de la enorme popularidad de la que gozan, y lo acompañaremos de cifras y datos que así lo corroboran. Por último, nos centraremos en algunos ejemplos de los ataques que han sufrido estas redes sociales y sus consecuencias.

2.- Un poco de historia

El origen de las redes sociales se remonta a 1995 cuando Randy Conrads creó la web *classmates.com* con el objetivo de que las personas pudieran recuperar o mantener el contacto con antiguos compañeros del colegio, instituto o universidad.

Dos años más tarde, en 1997, se creó *SixDegrees.com*, que fue la primera red social en la que se permitía crear perfiles y listas de amigos. Surgió como una herramienta para ayudar a las personas a conectarse y enviar mensajes a otras. A pesar del éxito, en el año 2000 se cerró este servicio.

En 2002, comienzan a aparecer páginas web que promocionan las redes de círculos de amigos online, como *Friendster* y *Fotolog*, y es en 2003 cuando se popularizaron con la llegada de sitios web como *MySpace*, *Hi5* o *LinkedIn*, entre otros.

Incluso algunos de los buscadores online más importantes también crearon sus propias redes sociales, como es el caso de Google, que en 2004 lanzó *Orkut*, y Yahoo!, que en 2005 creó *Yahoo! 360º*.

Facebook fue creado originalmente para estudiantes de la Universidad de Harvard en el año 2004 y fue en el 2006 cuando se abrió a todos los usuarios de Internet.

En 2005, la compañía AOL creó la red social *Bebo*, que también se encuentra entre las más populares.

En 2006 se lanzó la red social *Twitter* y también *Tuenti*, red social española que algunos han calificado como el "*Facebook* español".

1995	1997	2002	2003	2004	2005	2006
Classmates	SixDegrees	Friendster	MySpace	Orkut	Yahoo! 360º	Facebook
		Fotolog	LinkedIn		Bebo	Twitter
			Hi5			Tuenti

Cronología de las principales redes sociales

3.- Origen

Las redes sociales se basan en la Teoría de los Seis Grados de Separación, según la cual cualquier persona puede estar conectada a cualquier otra en el mundo a través de una cadena de conocidos que no tiene más de cinco intermediarios, conectando a ambas personas con solo seis enlaces.

La teoría fue inicialmente propuesta en 1929 por Frigyes Karinthy[1]. El concepto está basado en la idea de que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera.

Cada persona conoce de media, entre amigos, familiares y compañeros de trabajo o colegio, a unas 100 personas. Si cada uno de esos amigos o conocidos cercanos se relaciona con otras 100 personas, cualquier individuo puede pasar un recado a 10.000 personas más, tan solo pidiendo a un amigo que pase el mensaje.

Si esos 10.000 conocen a otros 100, la red ya se ampliaría a 1.000.000 de personas conectadas en un tercer nivel, a 100.000.000 en un cuarto nivel, a 10.000.000.000 en un quinto nivel y a 1.000.000.000.000 en un sexto nivel. En seis pasos, y con las tecnologías disponibles, se podría enviar un mensaje a cualquier individuo del planeta.

[1] El escritor húngaro Frigyes Karinthy (1887 – 1938) fue el primero que propuso el concepto de la teoría de los seis grados de separación en una historia corta llamada *Chains* o *Chain-Links*, incluida dentro de su obra *Everything is Different*.

4.- Funcionamiento

A pesar de la diversidad de redes sociales que existen actualmente, el funcionamiento es similar en todas ellas. Para formar parte de las redes sociales los usuarios deben registrarse, casi siempre de manera gratuita, y después rellenar una serie de formularios con sus datos personales, aficiones, foto personal, etc. Con esta información básica se crea el perfil del usuario, que podrá ampliar con los datos que desee para aumentar las posibilidades de encontrar personas afines.

Una vez registrado, el usuario se centra en ampliar su red social invitando a “amigos”. Para ello, estos sitios web ofrecen una serie de aplicaciones, búsquedas filtradas, mensajes, foros, comunidades, *chats*, etc. Algunos están claramente dirigidos a temáticas concretas, como encontrar pareja o compañeros de estudios, compartir música y fotos entre otros. Otros dejan en manos de los usuarios el propósito para formar parte de las redes: hacer amigos, buscar socios o dinero para negocios, encontrar trabajo, comprar o vender, buscar piso, en resumen, ofrecen un sinfín de posibilidades.

Por otra parte, las redes sociales ofrecen características como la actualización automática de la libreta de direcciones, perfiles visibles, la capacidad de crear enlaces favoritos de cada usuario y otras maneras de conexión social online.

Además, en dichas comunidades se desarrollan diferentes herramientas informáticas para potenciar la eficacia de las redes sociales online ('software social'), que operan en tres ámbitos, "las 3Cs", de forma cruzada:

- Comunicación: nos ayudan a poner en común conocimientos.
- Comunidad: nos ayudan a encontrar e integrar comunidades.
- Cooperación: nos ayudan a hacer cosas juntos.

5.- Popularidad de las Redes Sociales

Desde la aparición de las primeras redes sociales, el número de usuarios de las mismas ha ido creciendo exponencialmente. Actualmente, las redes sociales gozan de una gran popularidad en Internet. Cabe destacar que, según los datos proporcionados por Alexa de los 500 sitios web más visitados a nivel mundial[2], entre los 50 primeros puestos hay 7 redes sociales.

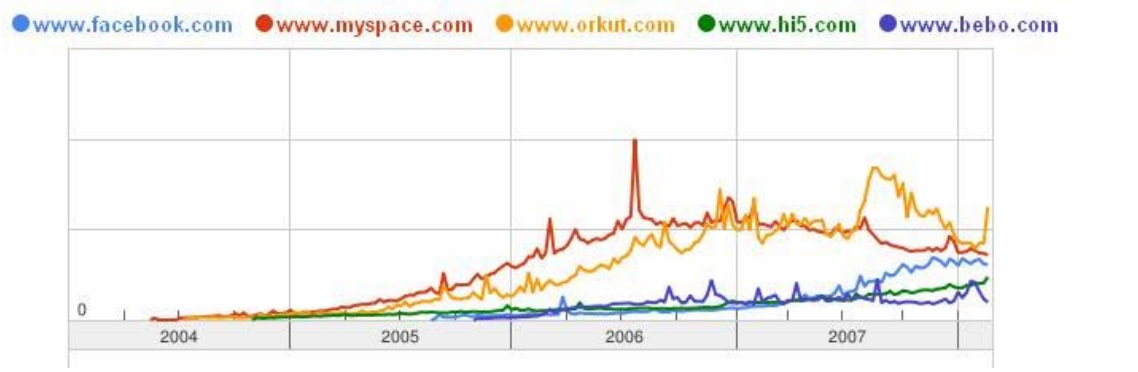
La primera es *Myspace*, que ocupa el sexto lugar, en octavo puesto *Facebook*, le sigue en el puesto 11 *Orkut* y en el 19 *Hi5*. Posteriormente, en los puestos 39, 40 y 41 están *Flickr*, *Friendster* y *Skyrock* respectivamente.

[2] Datos correspondientes al 29/07/2008 y extraídos de la página web: http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

Red Social	Puesto	URL
Myspace	**6**	www.myspace.com
Facebook	**8**	www.facebook.com
Orkut	**11**	www.orkut.com
Hi5	**19**	www.hi5.com
Flickr	**39**	www.flickr.com
Friendster	**40**	www.friendster.com
Skyrock	**41**	www.skyrock.com

Ranking de redes sociales [2]

Por otra parte, la siguiente gráfica de Google Trend representa el volumen de búsquedas realizadas por los internautas de una palabra o frase concreta correspondiente a algunas de las redes sociales más extendidas:



Volumen de búsquedas de las principales redes sociales

El éxito de las redes sociales se puede resumir en los siguientes puntos:

- El ser humano es una criatura social. Necesita comunicarse con otras personas y ampliar estas relaciones.
- No existen barreras. Las redes sociales permiten salvar las limitaciones que presenta la comunicación tradicional, como las barreras geográficas e incluso económicas.
- Fuente de información y conocimientos. Los usuarios que conforman las redes sociales comparten información y conocimientos entre ellos.
- Identidad online. No todo el mundo puede disponer de su propia página web, sin embargo, las redes sociales ofrecen a los usuarios la posibilidad de tener un espacio web propia y personalizarla a su gusto.
- Naturaleza viral. La necesidad de expandir la red de contactos hace que los usuarios inviten a sus amigos y esos amigos a su vez inviten a sus amigos, y así sucesivamente.

6.- Ataques a Redes Sociales

La popularidad y el gran número de usuarios de este tipo de sitios web no ha pasado desapercibido para los ciberdelincuentes, que desde hace algunos años utilizan las redes sociales como un vector de ataque para llevar a cabo sus actividades fraudulentas. Y es que las redes sociales reúnen unos requisitos muy apetecibles para los ciberdelincuentes:

- Cuentan con un gran número de usuarios, lo que permite una distribución rápida del malware. Si se infecta un usuario, cualquier usuario que acceda a dicho perfil, quedaría automáticamente infectado.

- Almacenan muchos datos personales sobre los usuarios, ya que es necesario crear un perfil personal para acceder a ellas. La información va desde nombre o dirección de correo electrónico hasta aficiones, edad, etc.
  Toda esta información puede ser fácilmente accesible para los ciberdelincuentes y se puede utilizar para realizar, por ejemplo, suplantaciones de identidad, ataques dirigidos, o incluso vender los datos obtenidos.

- Los usuarios de las redes sociales confían en sus contactos. Los ciberdelincuentes pueden suplantar la identidad de un miembro de esa red con relativa facilidad y hacerse pasar por él para no levantar ninguna sospecha.

Los ataques a redes sociales no son algo novedoso, ya que el primer ataque se produjo en 2005. Sin embargo, sí se puede apreciar un aumento y una diversificación de estos ataques a medida que el número de usuarios de las redes sociales ha aumentado. A través de ellas no solo se distribuye malware, sino que también se realizan ataques de phishing y suplantación de identidad o incluso se distribuye spam.

Casos más destacados

La mayoría de los ataques se han producido contra las redes sociales más populares, como *MySpace*, *Orkut* o *Facebook*. Esto no quiere decir que sean menos seguras que otras, sino que cuentan con un mayor número de usuarios, lo que aumenta las probabilidades de beneficio de un ataque.

Vamos a hacer un repaso de los ataques más significativos que han sufrido estas redes sociales:

MySpace, la más atacada

MySpace, una de las redes sociales más populares, ha sufrido numerosos ataques y de hecho fue víctima del primero. Se trataba del gusano detectado como MySpace.A creado por un usuario de *MySpace* y que le permitió añadir un millón de usuarios a su lista de contactos.

A finales de 2006, se distribuyó por esta red social un gusano que aprovechaba los perfiles de los usuarios de esa red para propagarse, infectando a todos los usuarios que visitaran un perfil infectado.

Por esas mismas fechas, un banner publicitario en la misma red aprovechó una vulnerabilidad en Windows Metafile para infectar a más de un millón de usuarios con spyware. Apenas unos días después se descubría, también en esa red, un gusano que incrustaba un código Java script en los perfiles de usuario. Cuando alguien intentaba visitar uno de esos perfiles, era redirigido a una web que culpaba al gobierno de Estados Unidos de los ataques del 11-S.

Pero el caso más grave tuvo lugar a principios del 2007. Esta vez se aprovechó de una característica del reproductor QuickTime de Apple para propagar un gusano. Los ciberdelincuentes asociaron varias películas subidas con este reproductor a distintos perfiles. Dicha película tenía un código malicioso, permitiendo a los hackers modificar el perfil de cualquier usuario que visitase el perfil infectado que ellos habían creado.

Además, este gusano presentaba la funcionalidad de enviar spam a todos los contactos de los usuarios infectados. Estos mensajes contenían un supuesta película. Cuando el usuario intentaba verla, era conducido a una página web pornográfica desde la que se descargaba un adware de la familia Zango, diseñado para mostrar publicidad personalizada.

Facebook y sus problemas de seguridad

Desde su creación, *Facebook* se ha convertido en una de las redes sociales con más éxito de Internet, lo que la convierte en un objetivo para los ciberdelincuentes.

A principios del año 2007 un hombre de Illinois, Estados Unidos, se hizo pasar por un adolescente para atraer a menores e intercambiar fotos con ellos. El hombre fue detenido y varios medios y asociaciones comenzaron a criticar la forma en que *Facebook* protegía a los menores.

A mediados del mes de julio, *Facebook* tuvo que enfrentarse a un nuevo problema de seguridad. En este caso se trató de un problema de programación que provocó que cuando un usuario introducía su clave, en vez de a su cuenta, era dirigido a la bandeja de correo de otro usuario, de modo que la información confidencial de unos usuarios quedó a la vista de otros.

Aunque, sin duda, el caso más grave ocurrió a mediados del mes de diciembre, cuando una compañía canadiense de pornografía fue denunciada por *Facebook* como responsable de haber “hackeado” la cuenta de 200.000 usuarios, logrando acceso a datos como su nombre de usuario, su contraseña o su dirección de correo.

También, a comienzos de este año, más de 50.000 usuarios de *Facebook* se vieron afectados por la instalación de un adware, que estaba camuflado como si de una aplicación adicional de la red social se tratara.

Las víctimas recibían una invitación indicando que tenían una invitación “Secret Crush”. Sin embargo, para saber de quién se trataba, debían invitar a 5 personas más a instalar dicha aplicación.

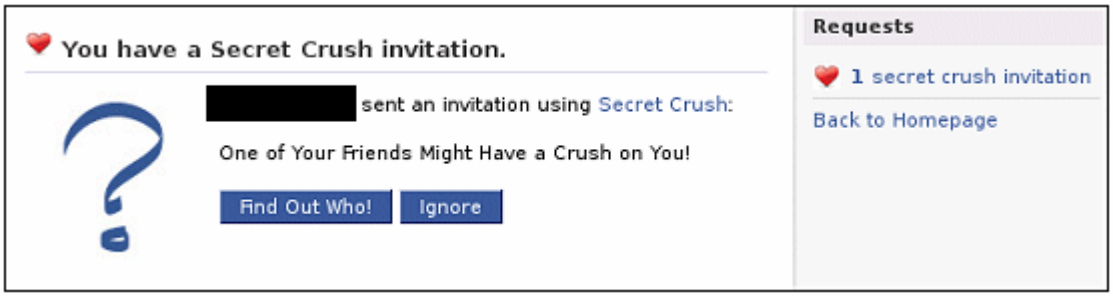


Imagen de la invitación "Secret Crush"

Una vez realizadas estas 5 invitaciones, en lugar de saber quién era el admirador secreto, se les indicaba que debían instalar otra aplicación adicional llamada Crush Calculator, que contenía finalmente el adware.

Por otra parte, en febrero de este año, salió a la luz un caso de suplantación de identidad en *Facebook* un tanto curioso. Un informático de 26 años fue condenado a tres años de cárcel por suplantar la identidad de Moulay Rachid, hermano menor del rey de Marruecos.

También en este año, pero en marzo, fue cuando un grupo de hackers lanzó un ataque contra *MySpace* y *Facebook*. Este ataque aprovechaba un exploit en el control activex que permite a los usuarios subir imágenes a sus perfiles. La vulnerabilidad les permitía saturar el búfer de dicho control para que interpretara las instrucciones que los ciberdelincuentes desearan darle, en lugar de aquellas para las que originalmente estaba diseñado.

Troyano en *Orkut*

A finales de febrero de este año, un troyano detectado como Orkut.AT utilizaba la red social *Orkut* para distribuirse. El procedimiento seguido era el siguiente:

En primer lugar aparecía un perfil en el "scrapbook" (libro de notas) del usuario que contenía una imagen de un vídeo de YouTube de Giselle, una participante del "reality show" Gran Hermano en Brasil. Esto pone de manifiesto que la ingeniería social sigue siendo una de las técnicas más utilizadas por los ciberdelincuentes para atraer la atención de los usuarios y así poder distribuir sus creaciones.

En segundo lugar, cuando el usuario pinchaba sobre el enlace, se le mostraba un mensaje diciendo que no puede ver el vídeo porque no tiene el códec correspondiente y se le ofrecía la posibilidad de descargarlo. Sin embargo, lo que se descargaba era una copia del troyano. Para evitar sospechas, mientras el troyano era descargado, el usuario era redirigido a una página en la que se le mostraba el vídeo prometido.

Una vez infectado el equipo, el troyano publicaba su mensaje malicioso en los "scrapbooks" de todos los contactos de Orkut de su nueva víctima.

Spam en *Twitter*

Como hemos mencionado anteriormente, el spam también ha llegado a las redes sociales y a finales de mayo se detectaron mensajes de spam en *Twitter*.

Mensajes de spam en Twitter

Los usuarios de *Twitter* recibieron oleadas de correos electrónicos del sistema interno de *Twitter*, avisando de la existencia de nuevos followers (usuarios registrados). El problema está en que los perfiles de estos nuevos followers contienen anuncios publicitarios de tipo spam. De esta manera, cuando un usuario intentara saber quién es el follower, visualizaría el spam.

7.- Consejos para navegar por las Redes Sociales

- Instalar en el equipo una solución de seguridad que cuente con tecnologías proactivas: De esta manera, los usuarios estarán protegidos contra los códigos maliciosos que se propagan por estas redes, incluso si estos no han atacado con anterioridad.

- Mantener actualizado el equipo: hay que conocer y resolver todas las vulnerabilidades que afecten a los programas tenemos instalados en el equipo.

- No compartir información confidencial: Si se accede a foros o chats para intercambiar información, conversar, etc., hay que recordar que no se debe dar información confidencial (direcciones de correo, claves, etc.).

- Enseñar a los menores: En el caso de los menores, estos deben saber qué información pueden compartir y cuál no. Para ello, los padres deben conocer las redes sociales a las que acceden y enseñarles la forma correcta y segura de navegar por las mismas.

- No dar más información de la necesaria en los perfiles: A la hora de realizar perfiles de usuario, no hay que dar más información de la necesaria. En caso de que sea obligatorio proporcionar datos privados como la dirección de correo, se debe seleccionar la opción de "no visible para el resto de usuarios" o similar, de tal modo que nadie salvo el propio usuario y los administradores puedan tener acceso a esos datos.

- Denunciar los delitos: Si se observa alguna conducta inapropiada o delictiva (intento de contacto con menores, fotos inadecuadas, perfiles modificados, etc.) hay que hacérselo saber a los administradores de la red social.

8.- Referencias

[1] Definición extraída de un estudio sobre los sitios de redes sociales.
boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), article 11.
http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[2] Páginas web más visitadas a nivel mundial según los indicadores de Alexa:

http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

Anexo

Información general sobre las redes sociales y la teoría de los seis grados de separación respectivamente:
http://es.wikipedia.org/wiki/Red_social

http://en.wikipedia.org/wiki/Six_degrees_of_separation

Enlaces a noticias

Illinois menores
http://www.theregister.co.uk/2007/02/08/facebook_security/

Pornografía Facebook
http://www.pcpro.co.uk/news/148908/facebook-hacked-by-porn-site.html

Secret Crush
http://www.theregister.co.uk/2008/01/04/facebook_adware/

Gusano de Orkut
http://www.theregister.co.uk/2008/02/29/orkut_worm_reloaded/

Ataques a Myspace
http://www.pandasecurity.com/spain/enterprise/media/press-releases/viewnews?noticia=8686&ver=18&pagina=7&numprod=&entorno