

Redes sociales utilizadas para propagar malware



Autor: Cristian Borghello, Technical & Educational Manager de ESET para Latinoamérica

Fecha: Lunes 28 de enero del 2008

Introducción

Cuando se habla de redes sociales [1] o comunidades virtuales [2], se suele tener una vaga idea de lo que se está mencionando; pero en resumen, se puede decir que una red de este tipo se caracteriza por tener actores (usuarios) y relaciones entre ellos que se generan en un mundo virtual como Internet.

Actualmente, existe una infinidad de estas comunidades y cada una de ellas, en forma más o menos original, persigue el mismo fin: lograr relacionar a los usuarios y que los mismos interactúen en esta comunidad. Algunas de estas redes son:

- **Photolog o Fotolog:** comunidad creada para compartir fotos e ideas asociadas a las mismas
- **Orkut:** tiene la posibilidad de desarrollar perfiles personales y relacionarse con otros participantes de la comunidad
- **MySpace:** perfiles personales con información, fotos, blog y redes de amigos
- **FaceBook:** una red social nacida en un ambiente universitario y abierta al público. Es uno de los sitios más visitados en Internet y su principal fortaleza es que permite el desarrollo de aplicaciones a terceros
- **Twitter:** red para enviar micro-mensajes (hasta 140 caracteres como si se tratase de un SMS)
- **Flickr y Picassa:** servicios adquiridos por Yahoo! y Google respectivamente, para compartir fotos
- **LinkedIn:** una red social orientada a contactos de negocios. Se puede encontrar personas del mismo interés académico o laboral
- **Second Life:** podría ser la evolución de las anteriores, ya que no sólo permite interactuar con las personas sino que ya es un mundo virtual completo en 3D, inspirado en novelas de ciencia ficción

Existen otros cientos de ejemplos de redes sociales, tales como Live Spaces, Xing, y muchos más, pero que en su mayoría son similares a las anteriores descritas.

Potenciales amenazas y daños

Cuando se habla de usuarios interactuando, debe sumarse a las amenazas ya conocidas en Internet, una nueva y potencial fuente de daños: el riesgo de comprometer la confidencialidad, privacidad, anonimato e intimidad del usuario.

Esto que puede sonar a película extraída de Hollywood, cobra vital importancia si se tiene en cuenta que cada usuario dispone de un perfil en la red, el cual podría ser parte de un ataque hacia su persona o hacia personas relacionadas.

A grandes rasgos, y en un sentido práctico, se podría dividir a los usuarios de estas redes en dos grupos, en términos de seguridad:

- Usuarios reales que crean perfiles reales
- Usuarios dañinos que crean perfiles falsos

En esta “simulación”, los primeros serán potenciales víctimas y los segundos quienes se aprovechen de estas víctimas. Esta división imaginaria es la que lamentablemente se da en muchas redes sociales y de la que se debe estar atento cuando se decide ingresar a dichas comunidades.

Ahora bien, ¿Qué significa lo anterior y cómo repercute en la seguridad de los usuarios?

Al igual que cualquier otra “revolución” en la web, las comunidades virtuales han significado gran cantidad de usuarios (millones) y por supuesto, esto significa gran cantidad de información y dinero que circula en estos sitios, debido a que los perfiles creados por los usuarios y sus relaciones son información útil que puede ser obtenida por los delincuentes, para ser comercializada o explotada con cualquier fin.

Las redes de delincuentes que utilizan al malware como herramienta no son ajenas a estas revoluciones y al momento los creadores del malware han comprendido el valor que tienen estos usuarios como posibles víctimas de sus infecciones (y de sus estafas).

En la práctica

Son innumerables los casos de utilización de códigos maliciosos en redes sociales, desde ataques a los perfiles de los usuarios para robar sus datos, malware propagados en cualquiera de ellas, engaño a los usuarios [3], utilización de reproductores de videos vulnerables en perfiles de usuarios, phishing de cuentas bancarias, la utilización de scripts para descargar archivos dañinos en los equipos de los usuarios; hasta robo de dinero y objetos (físicos) en mundos virtuales.

Para exponer lo anterior desde un sentido práctico que baje a la realidad y actualidad a las posibles consecuencias del abuso de las comunidades virtuales, a continuación se describe un caso que ha sido publicado en el Blog del Laboratorio de ESET Latinoamérica en enero del 2008 [4].

Este caso trata de la creación de sitios web falsos y procedentes de China en donde se simula ser el sitio web del perfil de un usuario de MySpace para lograr que otro usuario inocente ingrese al mismo y

descargue, en forma automática y sin su intervención, un troyano *downloader* que luego descargará otros malware en el equipo ya infectado.

El funcionamiento es el siguiente:

- A través de la posibilidad de ver los perfiles de ciertos usuarios de MySpace se simula ser uno de estos usuarios
- La URL creada por el atacante es similar a las verdaderas de los perfiles de usuarios de Myspace, pero el dominio apunta (en este caso) a sitios chinos creados para alojar malware



Imagen 1 – Sitio falso simulando ser un perfil de MySpace

- El usuario engañado, creyendo que verá el perfil de otro usuario, ingresa (haciendo clic) a la dirección falsa
- Este sitio contiene un script ofuscado que se ejecuta en el equipo del usuario y descarga un archivo dañino que también se ejecuta automáticamente infectando el sistema

```
<SCRIPT Language="JavaScript">
eval(unescape("%66%75%6E%63%74%...%3D%6E%65%77%20%41%7
</SCRIPT>
↓
http://...net/session/file.php?action=download&mode=abc
```

Imagen 2 – Script ofuscado

Esta descarga y ejecución automática se logran a través de la explotación de fallos en el navegador o aplicaciones que el usuario no ha parcheado. En este caso, los troyanos descargados son detectados por el motor ThreatSense® de Heurística Avanzada de los productos de ESET, logrando la protección del usuario desde incluso antes que este vector de ataque sea conocido.

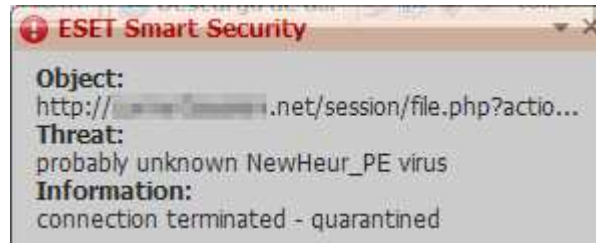


Imagen 3 – Detección de ESET Smart Security

La falta de prevención y educación por parte del usuario tiene, en este caso, diferentes facetas tales como:

1. No verificar la "calidad" de los contactos que agrega a su red virtual, ya que puede hacer que agregue usuarios que persiguen fines delictivos.
2. No verificar una dirección web puede hacer que ingrese a un sitio falso.
3. No actualizar las aplicaciones puede generar la descarga de archivos dañinos automáticamente a su sistema sin su intervención.
4. No utilizar un antivirus con capacidades proactivas puede hacer que se infecte.

Como puede verse, el funcionamiento es relativamente sencillo y se basa en la interacción que mantienen los usuarios dentro de la red: si un usuario puede interactuar con otro, podrá engañarlo. Sin ir más lejos, es la misma interrelación dañina que se genera en la vida real y ya existía anteriormente con el correo electrónico, el chat y otros medios de comunicación en Internet.

Conclusiones

El caso descrito sólo es uno de los cientos que pueden encontrarse al navegar y que demuestra lo fácil que resulta utilizar las nuevas herramientas para engañar al usuario e infectar sus sistemas.

Cuando surgió Internet, todos los usuarios se volcaron a ella sin tener un claro concepto de su potencial y de las posibles amenazas que podían existir. Mucha agua ha corrido bajo el puente y ya son incontables los tipos de ataques que actualmente puede sufrir un usuario al conectarse.

Las comunidades virtuales están significando un cambio global en la forma de pensar el mundo y también significan nuevas oportunidades personales, académicas, comerciales, laborales y... nuevos usuarios que podrían ser infectados por el malware.

Lo expuesto no debe considerarse en desmedro de las comunidades virtuales, sino todo lo contrario: es una simple exposición de sucesos reales y de las consecuencias, potenciales que pueden darse si no tiene los conocimientos necesarios acerca de esta nueva herramienta que brinda Internet.

Más Información:

[1] Red social

http://es.wikipedia.org/wiki/Red_social

[2] Comunidad virtual

http://es.wikipedia.org/wiki/Comunidad_virtual

[3] Troyano que simula ser una actualización

<http://blogs.eset-la.com/laboratorio/2008/01/14/troyano-myspace-simula-actualizacion-microsoft/>

[4] Blog del Laboratorio de ESET Latinoamérica

<http://blogs.eset-la.com/laboratorio/>