

Utilizando Redes Sociales para propagar malware



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

Fecha: 23 de Febrero del 2009

Utilizando Redes Sociales para propagar malware

Los beneficios de las redes sociales son innumerables, tanto para usuarios como para los atacantes que han encontrado en ellas múltiples formas de aprovecharlas para engañar a los usuarios y propagar nuevas amenazas, como sucede con el caso del gusano Koobface que, en diciembre del 2008, logró una repercusión importante por afectar a las principales redes sociales [1].

Introducción

El gusano Koobface logró una alta tasa de promoción en los medios informativos en diciembre pasado debido a la original técnica de propagación utilizada, si bien la tasa de infección del mismo no alcanzó a ser importante por la rápida acción de las redes sociales y las empresas de seguridad para bloquearlo.

El origen de Koobface se remonta a agosto del 2008 y su nombre es un anagrama de la conocida red social Facebook. El gusano también afecta a otras redes como Myspace, Bebo, Hi5, Friendster, Tagged o Livejournal , y podría hacerlo con cualquier otra, ya que la metodología utilizada puede ser replicada fácilmente por otros creadores de malware.

Esto se debe a que en realidad el gusano no afecta a la red social en sí misma sino que se aprovecha de algunas de sus funcionalidades para engañar al usuario y continuar su propagación.

Para visualizar completamente las acciones del gusano Koobface, ESET Latinoamérica también ha desarrollado un Video Educativo sobre lo que tendría que haber hecho el usuario para evitar infectarse y propagar la amenaza [2].

Metodología

La forma de actuar del gusano es la misma utilizada en otros medios de comunicación virtual (chat, redes P2P, foros, etc.) y lo único "original" del mismo es que al utilizar una red social como plataforma de ataque, la propagación del mismo es masiva y podría ser capaz de alcanzar altos niveles de infección en muy poco tiempo.

1. Engañando al usuario e infectándolo

Como primer paso, el usuario recibe un mensaje en su perfil de la red social desde un contacto ya infectado previamente, haciendo referencia a algún tema curioso o que pueda llamarle la atención (videos, imágenes con contenido sexual o no, cracks o warez, noticias de catástrofes o escándalos, etc.). Esta es una técnica de Ingeniería Social [3] ampliamente difundida y que en muchos casos, dependiendo del nivel de conocimiento del usuario, termina dando resultado.

En esta ocasión, y para aumentar el nivel de engaño, se inserta un mensaje llamativo que incluye un enlace a un perfil creado en Geocities que, al ser un servicio gratuito, es utilizado entre muchos otros por los atacantes para crear perfiles masivamente con este objetivo:



Imagen 1 - Mensaje recibido en Facebook

Si el usuario cae en el engaño e ingresa al sitio, será redirigido de forma transparente a un sitio dañino, mediante un *script*, como puede verse a continuación:



Imagen 2 - Redirección a sitio dañino

En este sitio se simula la ejecución de un video, para lo cual se debe descargar un plugin, que en realidad termina siendo un archivo ejecutable dañino, detectado por [ESET NOD32](#) como *Koobface*.



Imagen 3 - Supuesto video que descarga una amenaza

Nota: para futura referencia debe notarse que el archivo es descargado desde una dirección IP que puede parecer aleatoria, y utiliza el puerto 7777 para realizar la conexión.

En este punto, si el usuario aceptó y descargó el archivo, su sistema estará infectado y en él figurará un nuevo proceso llamado *bolivar[número].exe* (número dependerá de la versión del gusano analizada) el cual es almacenado en `X:\Windows` (siendo X la unidad del sistema).

Si se analiza el sistema con [ESET SysInspector](#) [4] puede observarse que también se encuentra activo otro proceso llamado *webserv.exe* encargado de mantener activo un servidor web, en el puerto 7777. Es por ello que anteriormente figuraba una dirección IP como proveedora del archivo dañino, ya que cada usuario está sirviendo estos archivos al resto de la comunidad.



Imagen 4 – Procesos activos del malware

2. Formando parte de una Botnet

A partir de este momento el sistema infectado forma parte de una Botnet [5] orientada a obtener información del usuario y de sus contactos, además de vulnerar ("crackear") [CAPTCHA \(Completely Automated Public Turing test to tell Computers and Humans Apart\)](#), las imágenes que se presentan al usuario al momento de registrarse en un servicio determinado.

Cuando el sistema acaba de infectarse, el gusano busca en él las cookies que almacenan la información perteneciente a los perfiles del usuario en las redes sociales mencionadas. En estos pequeños archivos se encuentran los datos que permiten al usuario (y ahora al gusano) efectuar acciones sobre la red social, como ver su perfil, enviar mensajes, ver los contactos, etc.

La información recolectada es enviada al centro de Comando y Control (C&C – Command & Control) de la Botnet en donde se procederá a procesarla para futuros usos.

El C&C responderá al sistema infectado con una serie de comandos entre los cuales se destacan (dependiendo de la versión del gusano analizado):

- Envío de mensajes desde el perfil del usuario a sus contactos, punto fundamental en la propagación del gusano (ver punto 1)
- Envío de información de los datos del usuario
- Envío de información de los contactos del usuario en la red social
- Descarga y ejecución de otros troyanos al equipo del usuario, para romper CAPTCHAs
- Descarga de imágenes del tipo CAPTCHA
- Auto-actualización del gusano a una nueva versión
- Descarga de URL (direcciones web), los textos de los asuntos y los mensajes que serán enviados posteriormente a los contactos

3. Enviando mensajes

El usuario, al desconocer que su sistema se encuentra infectado y formando parte de una Botnet, hace uso de sus recursos en forma normal y, en algún momento, ingresará a su perfil de la red social. El gusano, que verifica las ventanas y aplicaciones abiertas, al detectar el login del usuario, procede a rastrear sus contactos y a enviar un mensaje a cada uno de ellos.

El asunto del mensaje y el texto del mismo dependerá de los parámetros recibidos por el C&C. Luego, a cada mensaje se le adjunta la URL (en este caso de Geocities).

Cada contacto del usuario recibirá un mensaje con esa información y, ante la confianza de recibir el mensaje de una persona conocida, la propagación del gusano continúa (el ciclo comienza nuevamente desde el punto 1 del presente).

Como podemos apreciar, el motivo de la gran cantidad de infecciones se debe a la confianza que cada usuario deposita en su red de contactos y a que cada una de estas personas no sospecha que un amigo pueda tener infectado su equipo.

Este mismo principio se cumple en otros medios de comunicación como el chat, el correo electrónico y la mensajería instantánea, en donde los creadores de malware aprovechan la confianza del usuario como medio para propagar sus amenazas.

En este caso, Koobface no tuvo una alta tasa de infección debido a que las redes sociales bloquearon los mensajes que tenían URL de Geocities y que guardaban un formato similar a las utilizadas por el gusano. De todos modos, esto no significa que no puedan aparecer nuevas versiones que aprovechen la Ingeniería Social y la confianza del usuario para infectar su sistema.

4. Rompiendo CAPTCHA

Las CAPTCHAS son una prueba desafío-respuesta utilizada para determinar cuándo el usuario es o no humano y típicamente son utilizadas en casi cualquier servicio web para verificar que quien está intentando registrarse es un usuario y no un proceso automático (robot) que intenta hacerlo masivamente.

En el caso de Koobface, el C&C descarga al equipo del usuario un nuevo archivo *captcha[número].dll* encargado de realizar el proceso por el cual se puede violar la imagen del CAPTCHA. Estos archivos son detectados por ESET NOD32 como *Win32/Agent.OLA*.

Este proceso es agregado al registro de Windows, para que sea ejecutado cada vez que el equipo se inicia. Con ESET SysInspector puede verse esta modificación en la clave RUN del registro:

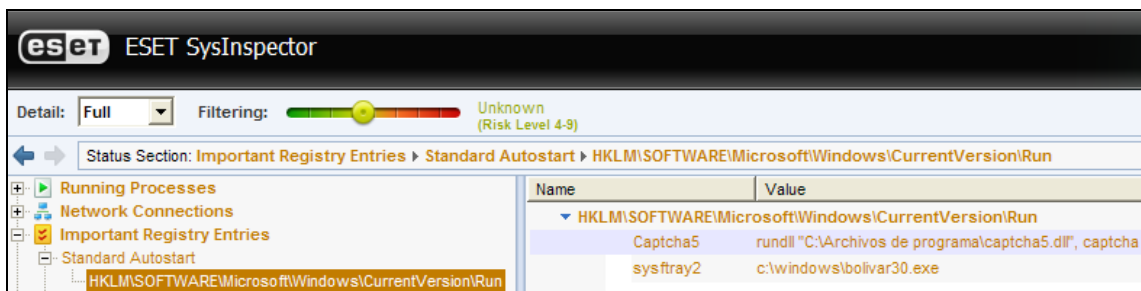


Imagen 5 – Clave RUN del registro con los trojanos de Koobface

A partir de este momento, cuando el usuario arranque su sistema, se le presentará una ventana informando que debe ingresar un código para terminar el proceso:



Imagen 6 – CAPTCHA presentado al usuario

Como puede verse, en realidad lo que se le presenta es una imagen del tipo CAPTCHA que ha sido previamente enviada por el C&C. La información ingresada por el usuario, sea correcta o incorrecta ya que no se puede verificar la veracidad de la misma, es enviada al C&C, identificada con una ID única y almacenada en una base de datos:

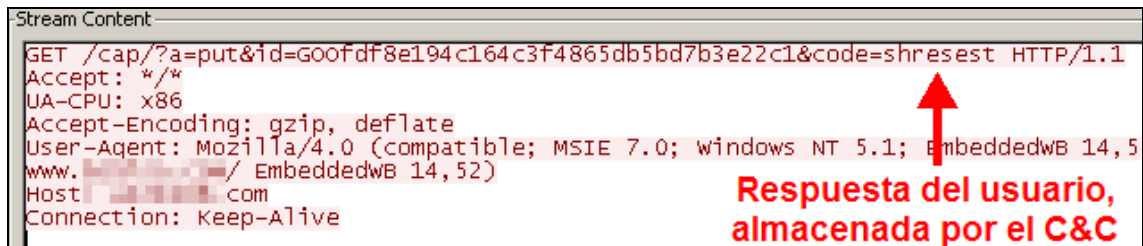


Imagen 7 - Respuesta enviada por el usuario

Posteriormente, estos datos son utilizados para el registro automático en distintos servicios ya que si se presenta esta imagen, el proceso automático de registro sabrá qué responder, debido a que el desafío ya fue resuelto previamente... por un usuario.

Sin extenderse y sin dar detalles técnicos, es fácil darse cuenta que se utiliza al usuario para resolver el CAPTCHA, almacenando la respuesta del mismo.

Conclusiones

El engaño a los usuarios es el medio por el cual los creadores de malware, spammers y otras personas relacionadas a estas actividades se ganan la vida indebidamente.

La utilización de las redes sociales como metodología de propagación de estos engaños sólo es un nuevo medio que se suma a los ya existentes. A esto, debemos agregar que se utiliza a los usuarios como herramientas para romper un medio de seguridad como las CAPTCHAS, permitiendo la generación de mayor cantidad de amenazas futuras.

Una vez más, la forma de evitar ser utilizados por los delincuentes es estar informado sobre estos engaños y peligros, y utilizar programas de seguridad de última generación que permitan detectar amenazas conocidas y desconocidas.

Más Información:

[1] ¿Qué es Koobface?

<http://blogs.eset-la.com/laboratorio/2008/12/08/que-es-koobface/>

[2] Video Educativo "Infección a través de Redes Sociales"

<http://www.eset-la.com/threat-center/videos-educativos>

[3] El arma infalible: la Ingeniería Social

<http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social>

[4] ESET SysInspector

<http://www.eset-la.com/sysinspector>

[5] Botnets, redes organizadas para el crimen

<http://www.eset-la.com/threat-center/1573-botnets-redes-organizadas-crimen>

Plataforma educativa de ESET Latinoamérica

<http://edu.eset-la.com/>