Waledac, el troyano enamorado

Autor: Sebastián Bortnik, Analista de Seguridad de ESET para Latinoamérica
Fecha: Viernes 27 de Marzo del 2009

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

Índice

Los eventos especiales son frecuentemente utilizados por los atacantes como excusa para realizar ataques a través de Ingeniería Social y atraer al usuario. Por lo tanto, en fechas como el Día de San Valentín (o Día de los Enamorados), se espera que se aproveche el acontecimiento con fines maliciosos.

En años anteriores ya se habían presentado amenazas que se tomaban ventaja de los "más enamorados" para infectar su sistema. Este año, la distribución del troyano Waledac *ha tenido características peculiares, sujetas a un interesante análisis sobre el trabajo constante de los atacantes por modificar (¿y perfeccionar?) los métodos y técnicas de infección.*

Descripción general

Waledac es un troyano que se distribuyó masivamente en diciembre del 2008 y enero y febrero del 2009, aprovechando un acontecimiento celebrado en muchos países del mundo como el "Día de San Valentín". Se caracteriza por la utilización de métodos de Ingeniería Social [1] para propagarse.

El principal objetivo de Waledac es formar una Botnet [2] y para eso convierte al equipo infectado en *zombie* de modo que los creadores de la red puedan realizar las acciones que deseen con éste. Algunas de las funciones de la Botnet ya detectadas son:

- Captura de direcciones de correo electrónico
- Envío de spam
- Robo de información del sistema
- Descarga de otras amenazas y capacidad de auto-actualización
- Alojamiento web en sistemas previamente infectados
- Uso y explotación de la técnica de Fast-Flux

La primera aparición de este código dañino fue detectada en diciembre del 2008. Desde entonces, la amenaza fue reactivada en varias ocasiones, aumentando en cada una de ellas el número de equipos integrantes de la Botnet. El ataque alcanzó su masividad en febrero, mediante el envío de correos de spam con contenidos relacionados a San Valentín (específicamente, postales virtuales).

Muchas de las características de Waledac (objetivos, técnicas de propagación, etc.) son similares a *Nuwar* (también conocido como *Gusano Storm o Gusano de la Tormenta*), una de las Botnets de mayor tamaño y difusión en el 2008, también explotada vía correo electrónico en el Día de San Valentín del 2008 [3].

Método de infección

Al ser un troyano, Waledac no posee métodos propios de reproducción y propagación. Su principal vía de acceso a los sistemas es el engaño a través de técnicas de Ingeniería Social y el envío de correos masivos para continuar su propagación.

El correo que recibe el usuario contiene una invitación para ver un contenido exclusivo, como una postal de San Valentín y, en todos los casos, un enlace a un sitio web:

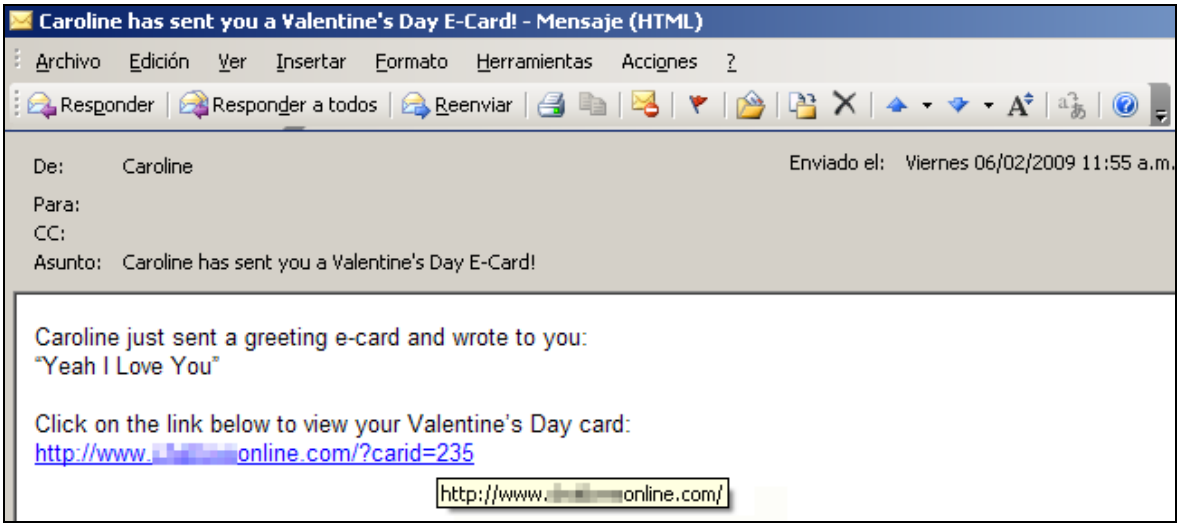

Imagen 1 - Correo electrónico recibido

Si el usuario accede al sitio web podrá observar diferentes interfaces gráficas que se caracterizan por poseer escaso contenido de texto, pocas (e impactantes) imágenes y mensajes directos invitándolo nuevamente a ver la postal.

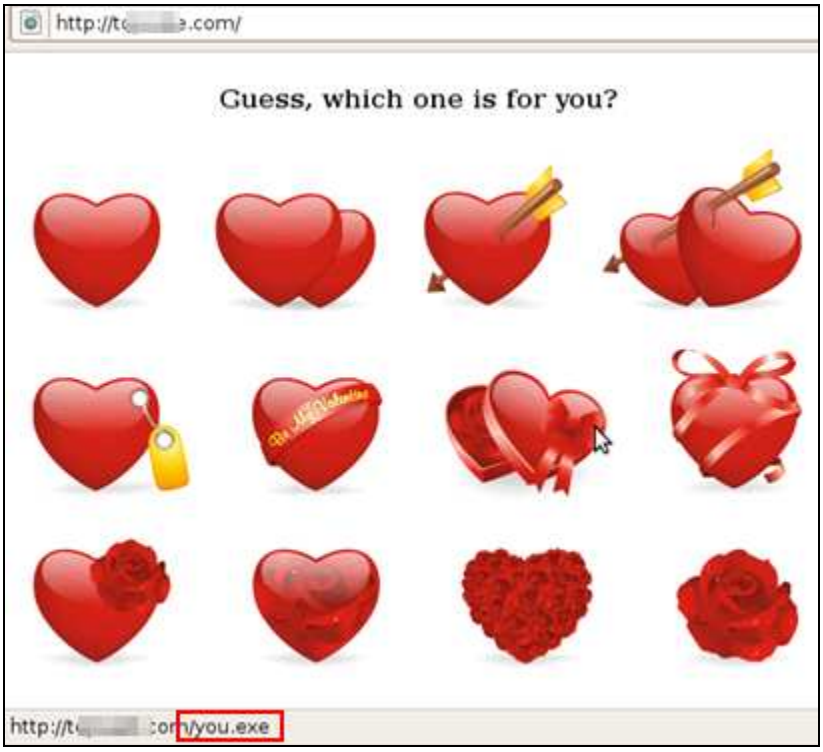

Imagen 2 - Sitio Web

Como se presenta en la imagen, al hacer clic sobre el sitio web, en lugar de ver una postal, se descarga un archivo de extensión EXE que, al ejecutarse, infecta al equipo.

Asimismo, el sitio web está configurado para llevar a cabo un método de infección doble. Además del archivo ejecutable que el usuario descarga, los atacantes combinan esta técnica con la de Drive-by-Download [4] para, de tener éxito, infectar al usuario con dos tipos de amenazas distintas.

Si se observa el código HTML, se puede observar un *iframe* oculto que accede a otro sitio web, en segundo plano, mientras el usuario visita el sitio web principal. Finalmente, de forma transparente, se descargan otras aplicaciones maliciosas de sitios de juegos online, por lo general del tipo adware.

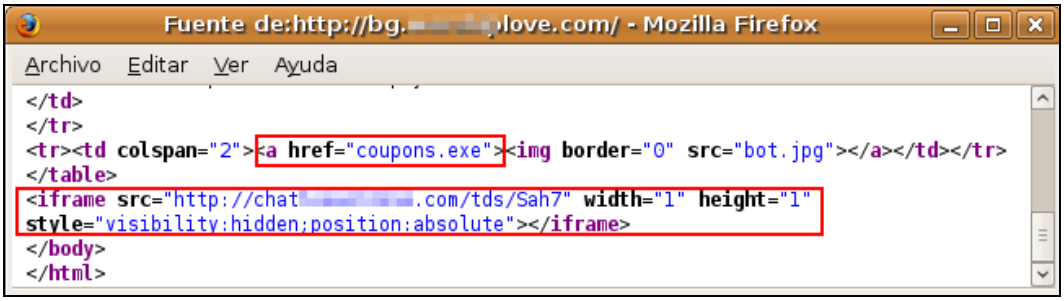

Imagen 3 – Frame para explotar la técnica de Drive-by-Download

Con estas técnicas, los atacantes tienen doble chance de infectar al usuario con dos amenazas diferentes. Cabe destacar que la técnica de Ingeniería Social (que culmina con la descarga de un archivo EXE por parte del usuario) puede ser explotada en cualquier navegador, no así la técnica de Drive-by-Download que podrá ser aprovechada solo si el usuario posee en el navegador alguna vulnerabilidad que pueda ser explotada por la amenaza.

Funcionamiento

Modificaciones realizadas en el sistema

Si el usuario descarga el archivo EXE y luego lo ejecuta, se da inicio al proceso de modificaciones del sistema y a la ejecución de actividades maliciosas. A partir de ese momento, el equipo ya está infectado.

Primero, el troyano agrega una línea en la siguiente clave de registro con el fin de ejecutarse en el próximo inicio de sesión:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Introduce una entrada del tipo "cadena" cuyo contenido es la misma ruta del archivo descargado, ya que el troyano no se copia a ninguna carpeta del sistema.

El archivo malicioso contiene predeterminadamente las rutinas necesarias para iniciar el envío de spam, en su mayoría con contenidos farmacéuticos (como venta de viagra, cialis o relacionados).

Una vez abierto, el archivo no puede ser eliminado por el usuario dado que se encuentra en ejecución. Sin embargo, puede ser encontrado en el Administrador de Tareas y finalizado por el usuario, a diferencia de otros archivos maliciosos que utilizan técnicas de ocultamiento más complejas.

Botnet

Como mencionamos anteriormente, el principal objetivo de Waledac es la creación de una Botnet. De esta forma, independientemente de las acciones que realice el archivo malicioso, se ejecutan de modo automático en el equipo las rutinas necesarias para que los dueños de esta red puedan enviarle comandos y realizar las acciones que deseen con cualquier terminal infectada.

Una vez que el sistema pasa a formar parte de la botnet, éste se convierte en un equipo *zombie*, como se denomina a las computadoras que conforman la red. Una de las funciones principales para las que es utilizado el equipo infectado es para el alojamiento web. Utilizando el servidor web Nginx[1], en los equipos se hospedan sitios que luego son utilizados para propagar la amenaza.

Asimismo, la Botnet es conformada en una red del tipo Fast-Flux. Estas, son "redes avanzadas de ataque y con capacidad de modificación, lo que dificulta los procedimientos de seguimiento e inhabilitación de las mismas" [5]. El objetivo de las redes Fast-Flux es ocultar las direcciones IP de los servidores centrales de las actividades maliciosas, haciendo uso de los equipos infectados como puentes para la comunicación con el resto de los usuarios. De esta forma, los dominios afectados contienen variadas direcciones IP en su resolución, todas ellas correspondientes a los equipos infectados y son éstos quienes realizan la comunicación con los servidores que alojan los contenidos.

,De este modo, tanto la comunicación con el centro de Comando y Control de la Botnet (*C&C*) como el alojamiento de los sitios web maliciosos son distribuidos a lo largo de toda la red y modificados constantemente para dificultar el rastreo de los servidores y administradores de la misma.

[1] Más información: http://nginx.net/

Cada vez que un usuario se conecta con un sitio web cuyo dominio fue registrado por los creadores del malware, lo está haciendo a un dirección IP (equipo) diferente, todos ellos sistemas *zombies* integrantes de la Botnet.

En la siguiente imagen puede observarse cómo, al realizar un ping[2] a un dominio afectado, varía la respuesta al finalizar e iniciar nuevamente la consulta. Esta modificación de la resolución de la dirección IP del dominio indica que ha cambiado el sistema desde donde se descarga la amenaza:

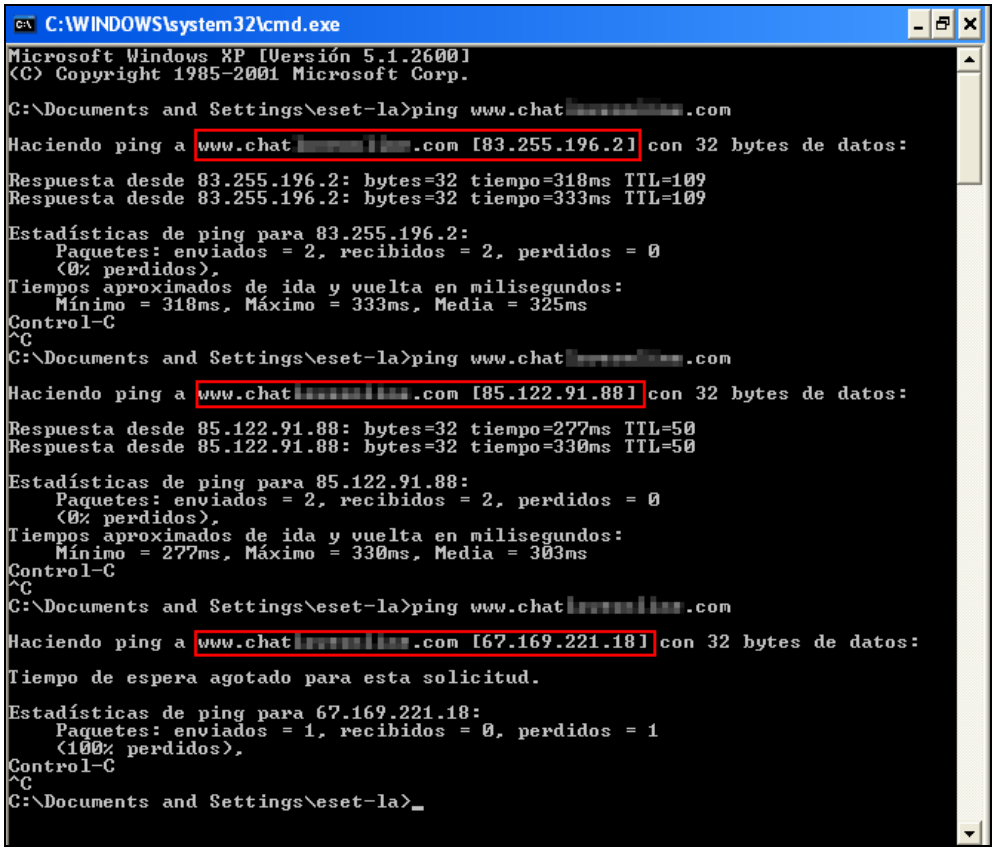

Imagen 4 - Consulta ping al dominio

[2] Ping es un comando para verificar conectividad con un extremo – en este caso, el dominio. La respuesta del comando muestra, entre otras cosas, la resolución del dominio y el tiempo de respuesta, de haberlo. Más información: http://es.wikipedia.org/wiki/Ping

Una consulta dig[3] al dominio comprueba que la IP que resuelve el sitio web es asignada con un tiempo de vida de cero segundos. Por lo tanto, al realizar una nueva consulta, la dirección IP es consultada nuevamente, obteniendo una nueva respuesta:

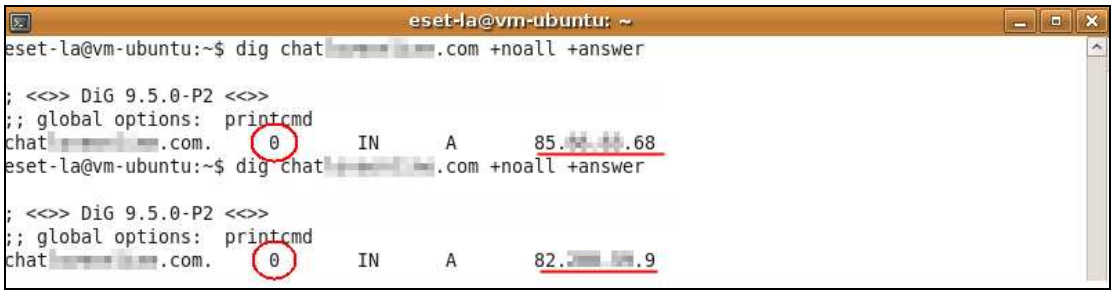

Imagen 5 - Consulta dig al dominio

La segunda característica notable de la Botnet es que las comunicaciones son realizadas vía protocolo HTTP, lo que dificulta el seguimiento de las tareas llevadas a cabo por la misma ya que la información transmitida dentro de la red se encuentra cifrada.

En la siguiente imagen se puede observar cómo son visualizadas las comunicaciones HTTP con una aplicación de análisis de tráfico de red:

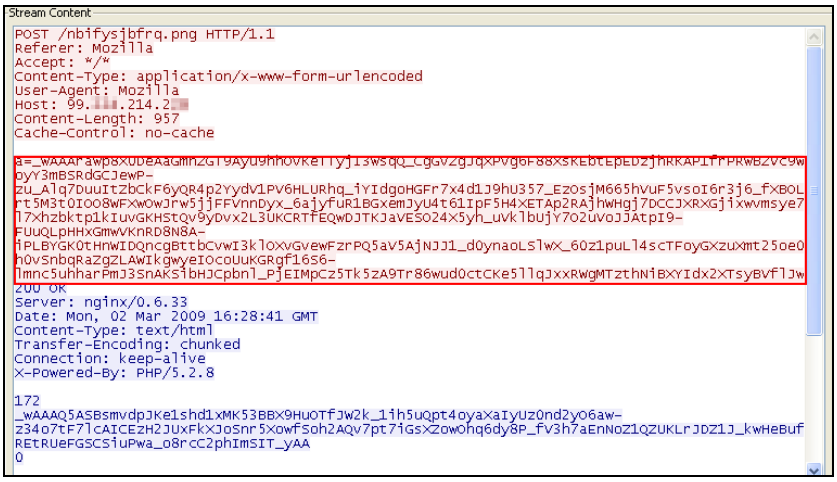

Imagen 6 – Tráfico cifrado

[3] **Dig** es una herramienta para realizar consultas a servidores de nombre DNS. Más información: http://en.wikipedia.org/wiki/Domain_Information_Groper

Rotación de binarios

Además de las características ya explicadas para dificultar su seguimiento y análisis, los autores de Waledac han trabajado diariamente para evitar la detección de la amenaza por parte de los productos de seguridad.

Para ello, han recurrido a un esquema de rotación de binarios que consiste en realizar pequeñas variaciones a los archivos maliciosos de forma tal que las técnicas estáticas de detección interpreten a todos ellos como diferentes archivos, siendo en realidad iguales las acciones realizadas por cada uno.

El sitio sudosecure.net [6], que ha hecho un detallado seguimiento de Waledac, ha detectado (a fines de febrero de 2009) casi 3.000 binarios diferentes, analizando más de 100 dominios afectados. De este modo, por ejemplo, con el nombre *loveyou.exe* se han detectado 20 binarios diferentes.

Ante estas técnicas, la detección de amenazas por bases de firmas es insuficiente y sólo un antivirus con capacidades de detección proactiva puede prevenir la descarga y ejecución de los binarios que han sido modificados recientemente, a través de técnicas de heurística.

Métodos de prevención

Frente a todo ataque que contenga un componente de Ingeniería Social, la primera barrera de prevención es el usuario. En el caso de Waledac, es importante recordar las siguientes precauciones:

- No visitar enlaces de correos electrónicos no solicitados
- No descargar (ni ejecutar) archivos descargados desde sitios web desconocidos

Los diferentes archivos maliciosos utilizados por Waledac son detectados por ESET NOD32 Antivirus, según la versión del archivo descargado, como:

- *Win32/*Waledac.*XX* (siendo XX la versión detectada)
- Una variante de *Win32/*Waledac.*XX* (detección heurística de nuevas versiones)
- Una variante de Win32/Kryptic.XX (detección heurística de nuevas versiones)

Además, cuando la amenaza comenzó su propagación masiva en febrero, los principales dominios asociados a la amenaza fueron bloqueados por ESET, sin permitir siquiera la navegación por dichos sitios, siempre y cuando el usuario tuviera activada la protección de tráfico HTTP (que viene configurada por defecto, de este modo por defecto).

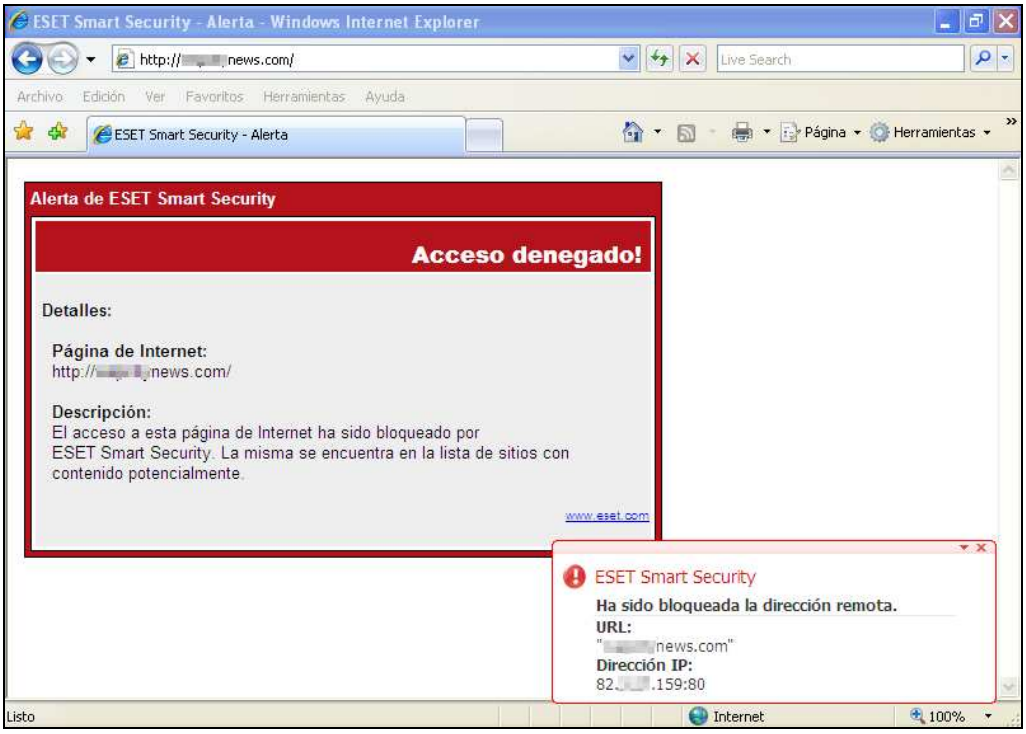

Imagen 7 - Bloqueo HTTP de Waledac

Además, el usuario debe recordar mantener su sistema operativo y navegador actualizados a la fecha, a fin de evitar la explotación de técnicas que permitan la instalación de malware (exploits, Drive-by-Download [4], etc.)

Waledac en el tiempo

Una de las principales características que presenta este troyano es el constante trabajo por parte de sus creadores para rediseñar las técnicas de propagación e infección.

De esta forma, los atacantes engañan a los usuarios a través de técnicas de Ingeniería Social acordes a sus necesidades de acuerdo a la época del año, lo cual demuestra la persistencia de sus autores para mantener la amenaza activa.

Etapa 1: Surgimiento

Waledac fue detectado por primera vez el 20 de Diciembre del 2008 a través del envío de correos con postales para las fiestas navideñas.

La tasa de infección detectada en esta primera etapa fue baja, dada la poca probabilidad de que un usuario ejecute un archivo EXE adjunto a un correo electrónico, forma de distribución utilizada en ese entonces.

Como se mencionaba anteriormente, los creadores del troyano basaron gran parte de su éxito en la continua actualización de las técnicas de Ingeniería Social para infectar al usuario. Su estrategia: llegar al público con el "mensaje del momento".

El siguiente gráfico de Google Trends[4] muestra cómo, en el mes en que el ataque se propagaba con sitios web sobre Obama (enero de 2009), crecían las búsquedas por el nombre del nuevo presidente de los Estados Unidos, debido a su asunción el 20 de enero:

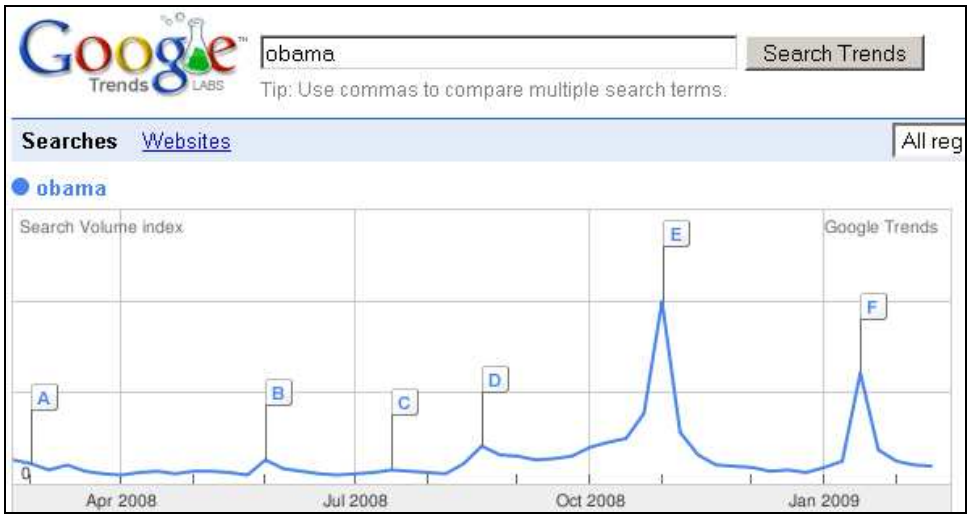

Imagen 8 - Google Trends "Obama", últimos 12 meses a febrero del 2009

[4] http://www.google.es/trends

Etapa 2: Masificación

Al igual que lo ocurrido con el gusano Nuwar, la gran oportunidad para masificar Waledac fue el día de San Valentín, que se festeja en todo el mundo el 14 de febrero. El gráfico de Google Trends corrobora nuevamente el por qué de la elección del tema en febrero:

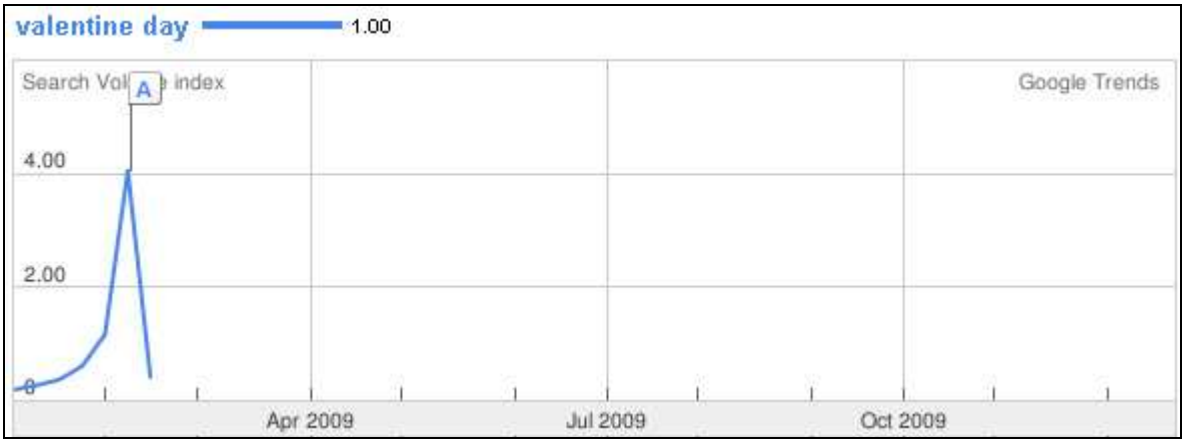

Imagen 9 - Google Trends "Valentine Day", enero y febrero del 2009

Durante la primera quincena de marzo del 2009 se registró el mayor crecimiento de correos no deseados con enlaces a los sitios web afectados que propagaban el troyano.

Fue recién en esta etapa en que Waledac logró popularizarse y afirmar el poder de la Botnet, pudiendo ser la de mayor crecimiento en lo que va del año.

De este modo, el día de San Valentín fue la ocasión elegida por los creadores del troyano para masificar el ataque y aprovecharse de los deseos de los usuarios para estas fechas.

Etapa 3: Seguir con vida

Pasado el 14 de febrero y comenzada la última semana de dicho mes, los creadores de Waledac actuaron nuevamente en función de los intereses de los usuarios: el día de San Valentín ya no era del interés del público (ver imagen 8).

Ante este hecho, todos los dominios afectados por Waledac dejaron de mostrar las imágenes referentes al día de los enamorados (corazones, flores, peluches, etc.) para utilizar una nueva metodología: ahora los usuarios, en lugar de descargar postales de San Valentín, podrían descargar cupones de descuento "*en más de 100.000 tiendas*" [7].

Obviamente, estos descuentos no eran tales, sino que se trataba del mismo troyano que era distribuido los días previos como una postal para los enamorados. También fueron modificados los nombres de los archivos que se descargaban, a fin de estar relacionados a la nueva temática utilizada. Los creadores del troyano no se tomaron respiro y rápidamente adaptaron las técnicas para continuar con su propagación y desarrollo.

Un mes después, luego de aumentar el número de víctimas con los cupones de descuento, se modificaron nuevamente los sitios webs y fueron enviados correos electrónicos no solicitados para la propagación. En esta ocasión, los correos daban anuncio de un ataque terrorista y, manteniendo la línea de correos breves con poco texto, se incluía un enlace a un sitio web malicioso. Si el usuario accedía al sitio, se simulaba una página de una agencia de noticias muy conocida. La noticia en cuestión detallaba sobre un ataque terrorista y se incluía un video. Al intentar iniciar el video, siempre se indicaba la necesidad de instalar un *codec* que es el malware. La principal característica de esta modificación, fue que el ataque terrorista era anunciado en la ciudad donde se localizaba la dirección IP pública del usuario [8]. De esta forma, en la mayoría de los casos la noticia será de mayor impacto para la víctima.

Con esta última modificación, se confirma la tendencia de Waledac de realizar cambios periódicos en sus sitios web y código fuente. Además, la geolocalización de la dirección IP indica la gran capacidad de sus creadores para mejorar sus técnicas ante cada cambio.

Tabla comparativa[5]

	Etapa 1	Etapa 2	Etapa 3
Fecha	**diciembre 2008 – enero 2009**	**Hasta el 24 de febrero del 2009**	**Desde el 24 de Febrero del 2009**
Ingeniería Social	**Postales por navidad** **Noticias sobre Obama**	**Postales de San Valentín**	**Cupones de descuento**
Nombres de los archivos infectados	• *barack.exe* • *baracknews.exe* • *baracknews.exe* • *blog.exe* • *doc.exe* • *ecard.exe* • *news.exe* • *obamasblog.exe* • *obamaspeech.exe* • *president.exe* • *statement.exe* • *usa.exe*	• *card.exe* • *kit.exe* • *love.exe* • *loveexe.exe* • *loveu.exe* • *loveyou.exe* • *meandyou.exe* • *mylove.exe* • *onlyyou.exe* • *postcard.exe* • *run.exe* • *save.exe* • *youandme.exe*	• *couponlist.exe* • *coupons.exe* • *disc.exe* • *discounts.exe* • *list.exe* • *nocrisis.exe* • *print.exe* • *run.exe* • *sale.exe* • *sales.exe* • *saleslist.exe* • *save.exe* • *stopcrisis.exe*

Tasa de infección

Según el Servicio Estadístico de Alerta Temprana de ESET, ThreatSense.Net [9], este troyano ha alcanzado un porcentaje de propagación mundial de menos del 1% entre los usuarios de las soluciones de ESET. Las claves de esta reducida tasa de infección entre los usuarios de ESET NOD32 Antivirus y ESET Smart

[5] La tabla, incluida a modo grafico, es sólo un resumen de algunos de los nombres de archivos más utilizados en cada etapa.

Security son los altos índices de detección del producto ante la amenaza y la rápida respuesta para el bloqueo de dominios afectados.

Según sudosecure.net, son más de 25 mil equipos los infectados, casi 2 mil de ellos en América Latina. El mismo portal detectó, a fines de febrero, un crecimiento de esta tasa a razón de más de **200 nuevos equipos infectados por día**.

Aunque los valores reportados por sudosecure.net son mayores que los detectados en usuarios de las soluciones de ESET, los números continúan siendo bajos comparados con los logrados por el gusano Nuwar, con el cual la comunidad de seguridad ha comparado la amenaza de Waledac.

Galería de imágenes

La variación en las imágenes utilizadas como Ingeniería Social fue una de las características distintivas de esta amenaza, demostrando el trabajo continuo de los creadores y diferenciándose de lo ocurrido años anteriores, donde la distribución se realizaba con una única imagen o un número limitado de ellas.

La siguiente imagen muestra la cantidad de interfaces diferentes utilizadas durante febrero del 2009 para propagar el troyano a través de postales para el día de los enamorados. Tal variedad permite atraer a diferentes usuarios y dificultar la asociación de una imagen con la amenaza y, por ende, el reporte de la misma.

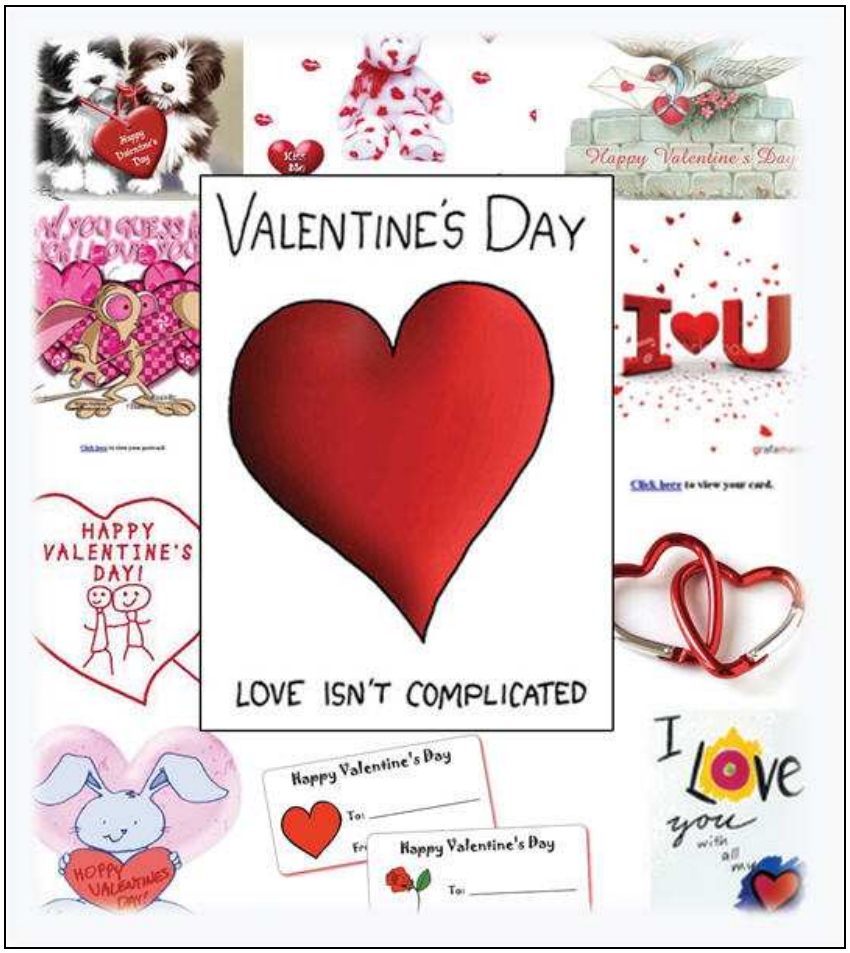

Imagen 10 – Galería de imágenes Waledac

Conclusión

Waledac ha sido la amenaza que mejor aprovechó el día de San Valentín para propagarse y se ha distribuido vía correo electrónico con altos índices durante febrero del 2009.

Dado el constante trabajo de sus creadores por modificar las técnicas de infección, es de esperar que el troyano continúe propagándose a través de la actualización periódica de sus técnicas de infección, con el objetivo de conformar una gran Botnet a lo largo del 2009.

Cabe destacar que, a pesar de utilizar técnicas avanzadas para su propagación y organización, las tasas de infección no han sido altas ni se ha ubicado entre los códigos maliciosos con mayor tasa de infección. ¿A qué se debe esta dualidad entre éxito y fracaso?

Independientemente de las novedosas y trabajosas técnicas de propagación y utilización de las redes Fast-Flux, el archivo malicioso recurre también a algunas bastante primitivas respecto a otros troyanos:

- No se copia a sí mismo en el sistema
- Modifica una única entrada del registro
- El proceso no está oculto al usuario final

Es por ello que es simple para el usuario, aún habiéndose infectado, finalizar el proceso y eliminar el archivo malicioso del sistema, liberando a su equipo de la Botnet.

De todas formas, Waledac es una gran amenaza a considerar durante el 2009, dadas sus exitosas técnicas de propagación y la avanzada tecnología de funcionamiento. Manteniendo las técnicas de infección y modificando las características del archivo malicioso, puede convertirse en una de las Botnets de mayor crecimiento para este año.

Referencias

[1] http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social

[2] http://www.eset-la.com/threat-center/1573-botnets-redes-organizadas-crimen

[3] http://www.eset-la.com/company/1727-eset-informa-propagacion-amenazas-san-valentin

[4] http://www.eset-la.com/threat-center/1792-drive-by-download-infeccion-web

[5] http://blogs.eset-la.com/laboratorio/2008/06/03/redes-fast-flux/

[6] http://www.sudosecure.net/Waledac/

[7] http://blogs.eset-la.com/laboratorio/2009/02/25/Waledac-ya-no-esta-enamorado/

[8] http://blogs.eset-la.com/laboratorio/2009/03/16/otra-vez-waledac/

[9] http://www.eset-la.com/threatsense.net