Boletines PandaLabs:

Waledac e Ingeniería Social

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

Índice

1.- Introducción

Los mensajes de correo electrónico que utilizan la ingeniería social siguen siendo una de las principales vías de entrada de malware en los ordenadores de los usuarios. Habitualmente, el malware llega en un archivo adjunto en los mensajes, haciéndose pasar por cualquier tipo de documento que parezca inofensivo: imágenes, documentos Word, Excel.

Sin embargo, no todas las familias de malware se distribuyen a través de adjuntos en mensajes de correo electrónico. Tal es el caso de la familia Waledac, que ha destacado por su alta actividad durante el primer semestre del año.

Esta familia se caracteriza principalmente por la variedad de temas que utiliza para su distribución y porque se distribuyen en mensajes de correo electrónico que contienen enlaces a páginas web desde las que se descarga el gusano.

En este boletín vamos a analizar la familia de Waledac a fondo. Entre otros temas, hablaremos de las acciones maliciosas que realiza, de datos referentes a su actividad a lo largo del primer semestre de este año, de la temática que ha ido utilizando y consejos para mantenerse protegido.

2.- Storm Worm: el comienzo

El origen del denominado Storm Worm se remonta a enero de 2007, cuando empezaron a circular una serie de correos electrónicos sobre las tormentas que estaban asolando Europa esos días con el objetivo de distribuir malware.

Fue otro método más de ingeniería social, pero sin embargo, a raíz de estos correos electrónicos surgió el fenómeno conocido como Storm Worm, en el que se englobaron diferentes familias de malware que utilizaban esta técnica aunque la temática de los correos fue variando.

Febrero y noviembre fueron los meses con mayor actividad del Storm Worm durante 2007. En concreto debido a diferentes variantes del gusano Nurech, una de las familias englobadas dentro del Storm Worm.

Después de un 2008 tranquilo, a finales de año volvió a iniciarse el fenómeno del Storm Worm a través de una familia de gusanos denominada Waledac.

Como novedades que incorpora esta familia respecto a lo que habíamos visto antes, podemos destacar que no utilizan archivos adjuntos sino enlaces desde los que se descarga el malware cuando el usuario accede al mismo.

Los creadores de este tipo de malware utilizan esta técnica con el fin de dificultar la detección de los mismos por parte de las compañías de antivirus. Antes bastaba con detectar el archivo adjunto para bloquear fácilmente el Storm Worm, ya que era el mismo en todos los casos.

Sin embargo, actualmente es necesario monitorizar y hacer un estudio exhaustivo de los enlaces, puesto que van variando el malware que alojan en función de distintos parámetros al acceder, como por ejemplo la hora, el navegador que se utiliza, la procedencia, etc.

Los ciber-delincuentes se han dado cuenta de que intentar propagar una única muestra no es un método muy efectivo y han optado por esta técnica bastante más eficaz.

3.- Principales efectos

Además, de propagarse a través de correo electrónico mediante enlaces, tienen otras funcionalidades como la de enviar spam, la de obtener información personal del equipo afectado y la de descargar otras familias de malware.

Una vez ejecutado e instalado en el ordenador, realiza las siguientes acciones:

- Modifica entradas del registro del sistema, permitiendo su ejecución tras efectuarse el próximo reinicio del sistema.
- Busca todas las direcciones de correo almacenadas en el equipo con el fin de utilizarlas para propagarse y para enviar spam.
- Encripta la información correspondiente a las direcciones de correo, las almacena en un archivo de nombre aleatorio y las remite a diferentes direcciones preparadas para la recogida de dicha información.
- Su componente backdoor abre un puerto TCP de comunicación que permite a usuarios remotos conectarse y ejecutar comandos arbitrarios en los sistemas infectados, actuando como una red de bots.

Hemos constatado alrededor de 170 dominios pertenecientes a esta familia. Algunos de ellos son los siguientes:

hxxp://terrorismfree.com
hxxp://antiterroris.com
hxxp://fearalert.com
hxxp://easyworldnews.com
hxxp://bestjournalguide.com
hxxp://worldtracknews.com
hxxp://virtualesms.com
hxxp://smspianeta.com
hxxp://freeservesms.com
hxxp://codecouponsite.com
hxxp://thecoupondiscount.com
hxxp://bestcouponfree.com
hxxp://funnyvalentinessite.com
hxxp://thevalentinelovers.com
hxxp://yourvalentineday.com
hxxp://greatbarackguide.com
hxxp://bestbaracksite.com
hxxp://superobamaonline.com
hxxp://newyearcardfree.com
hxxp://bestchristmascard.com
hxxp://freechristmassite.com

Como se puede observar por los nombres de las páginas web, los enlaces están relacionados con el asunto del que tratan los mensajes con el objetivo de engañar a los usuarios y que no desconfíen de la página web a la que han sido redirigidos. Así, en el caso de Barack Obama hay dominios como *hxxp://superobamaonline.com*, para San Valentín *hxxp://yourvalentineday*.

Esta familia lleva activa desde finales de 2008. Los primeros ejemplares se empezaron a detectar en diciembre de ese año y desde entonces han aparecido numerosas variantes (un total de 68) y su distribución ha sido constante en lo que llevamos de año.

La siguiente gráfica representa el volumen de detecciones correspondientes a variantes de la familia Waledac que han sido detectadas por nuestros productos, con lo que nos podemos hacer una idea de la cantidad de muestras de Waledac que ha habido en circulación y que han afectado a los usuarios durante estos meses:

Fig. 1 Detecciones de Waledac reportadas por nuestros productos (Enero-Julio 2009)

Como se puede observar, durante los cinco primeros meses del año la actividad de esta familia ha sido más o menos constante, con un ligero repunte en el mes de abril. Sin embargo, en los dos últimos meses, el de junio y julio, se aprecia un notable aumento de la actividad respecto a los meses anteriores.

4.- En la variedad está el Waledac

La ingeniería social sigue siendo una de las técnicas más empleadas por el malware, y también por el Waledac, para distribuirse. Se puede definir como "una colección de técnicas que se emplean con objeto de manipular a los usuarios para que realicen determinadas acciones, como el envío de información personal, la descarga de archivos, etc."

Si por algo se caracteriza la familia de los Waledac es por la diversidad de temas que han utilizado para distribuirse. La elección de los temas no ha sido casual, sino que han sido cuidadosamente seleccionados en función de:

- Acontecimientos importantes en fechas señaladas, como navidades o San Valentín.
- Noticias falsas, como la renuncia de Barack Obama a la presidencia de EEUU o explosiones en ciertas ciudades.
- Asuntos llamativos, como vales descuento o la posibilidad de espiar los mensajes de cierto número de teléfono.

Los primeros ejemplares aparecieron en navidades del año 2008 y utilizaban felicitaciones navideñas como cebo para engañar a los usuarios y distribuirse.

Renuncia de Barack Obama

En enero de 2009, comenzaron a distribuirse mensajes de correo electrónico sobre la supuesta renuncia de Barack Obama a la presidencia de Estados Unidos. Estos mensajes incluían un enlace a una página web en la que se podía consultar la impactante noticia:

Fig. 2 Mensaje de correo sobre la renuncia de Obama

Si se pulsaba el enlace del mensaje, el usuario era redirigido a una página web que imitaba a la original y en la que se podía leer la supuesta noticia, entre otras, como se puede ver en la siguiente imagen:

Fig. 3 Supuesta página web oficial de Obama

Cuando el usuario pulsaba alguno de los enlaces incluidos en la noticia, se procedía a la descarga del archivo malicioso.

San Valentín

Después de las navidades, San Valentín es la fecha más próxima que los creadores de malware aprovecharon para distribuir sus creaciones. Sin embargo, mucho antes del 14 de febrero, esta familia ya estaba distribuyendo mensajes de correo sobre el día de los enamorados.

De hecho, el 26 de enero de este año publicábamos un post en el blog de PandaLabs advirtiendo de la aparición de una oleada de Waledacs que utilizaba la temática de San Valentín para distribuirse.

En esta ocasión, llegaba en un mensaje de correo que contenía un enlace a una página en la que se mostraban unos corazones y el usuario tenía que seleccionar uno. Si el usuario pulsaba sobre cualquiera de ellos, se procedía a la descarga de un archivo bajo la previa confirmación del usuario.

Este archivo, en realidad, era una copia del gusano.

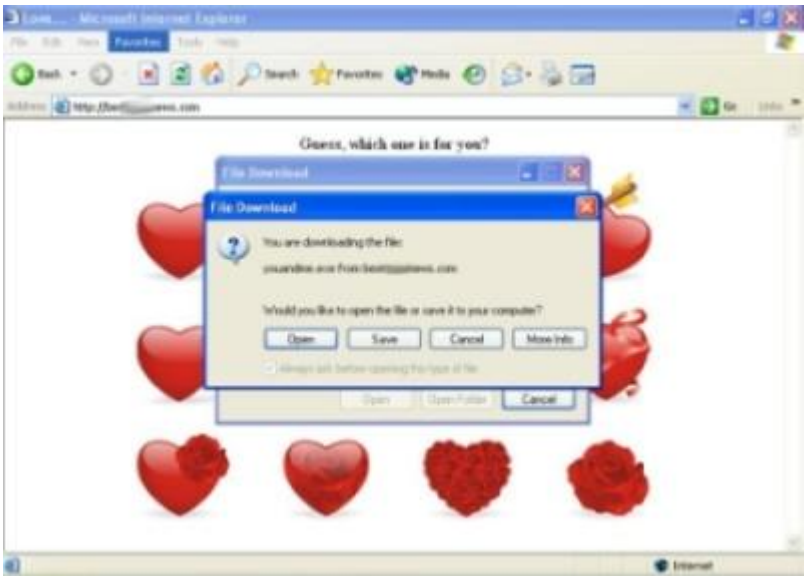

Fig. 4 Página web desde la que se descarga el Waledac

Unos días antes de San Valentín, se volvieron a distribuir mensajes de correo relacionados nuevamente con el día de los enamorados. Estos mensajes contenían un enlace a una página maliciosa que constaba de una imagen romántica y un texto en el que se ofrecía una herramienta para diseñar tarjetas para San Valentín.

Fig. 5 Página web para diseñar tarjetas románticas

El mensaje incluía varios enlaces que en teoría apuntaban a la web de descarga de dicha herramienta. Sin embargo, lo que realmente se descargaba no era una aplicación sino una variante de la familia Waledac.

Vales descuento en tiempos de crisis

Los ciber-delincuentes también han querido aportar su granito de arena para ayudar a los usuarios a sobrellevar mejor la crisis económica. En este caso, los mensajes contenían enlaces que llevaban a una página web en la que se ofrecían vales descuento para numerosos establecimientos.

Fig. 6 Página web desde la que se podían descargar los supuestos vales

Si el usuario decide descargar estos vales descuento y pulsa alguno de los enlaces del mensaje, se estará descargando un archivo con nombres como *couponlist.exe*, *coupons.exe*, *list.exe* o *print.exe*. En principio, un archivo con alguno de esos nombres podría corresponder perfectamente a un listado de vales. Sin embargo, todos estos archivos ejecutables corresponden a una copia del gusano.

Explosiones

Unas semanas después, una nueva temática estaba siendo utilizada para distribuir nuevos ejemplares de Waledac. En esta ocasión, los mensajes trataban sobre una supuesta explosión y contenían un enlace a la noticia.

Si el usuario pulsaba el enlace, era redirigido a una página web en la que podía leer la noticia y además se mostraba un vídeo sobre el suceso. Para no levantar las sospechas de los usuarios, se utilizó la imagen de la agencia Reuters.

Sin embargo, para visualizar el video, se requiere que el usuario descargue una actualización del Flash Player, que no es otra cosa que la copia del gusano.

Espía de sms

La siguiente temática destacada utilizada por el Waledac ha sido hacerse pasar por una aplicación para espiar los sms de otros teléfonos móviles.

Esta técnica consiste en ofrecer un servicio que permite a los usuarios leer los sms recibidos en un teléfono movil. Con el pretexto de poner a prueba a tu pareja o por simple curiosidad, ofrecen un programa que permite acceder a información privada sin que la víctima se percate de ello.

Fig. 7 Página de descarga programa espía

Sin embargo, detrás de este mensaje no hay ningún programa espía, sino un código malicioso de la familia Waledac.

Si el usuario decide descargar y ejecutar el supuesto programa, el ordenador quedará afectado por este gusano.

Independence Day

La última temática de la que se ha aprovechado esta familia para distribuirse está relacionada con el Día de la Independencia de Estados Unidos, el 4 de julio. Los mensajes de correo electrónico de este tipo comenzaron a distribuirse unos días antes de la fecha.

En este caso, los mensajes contienen un enlace a un supuesto video sobre las celebraciones de dicha festividad:

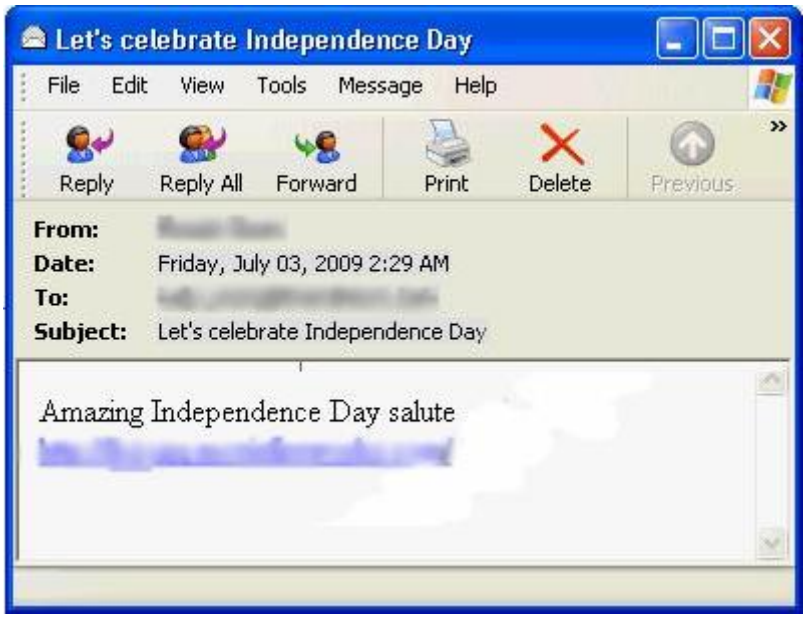

Fig. 8 Mensaje sobre el Día de la Independencia

Si el usuario pulsa el enlace, se abre una página web que imita a la de YouTube, en la que se puede leer una noticia sobre este evento y ver un video de un espectáculo pirotécnico.

Para poder ver el video solicita la instalación de un archivo, supuestamente necesario para su visualización. Sin embargo, en realidad se trata de una copia del gusano.

Fig. 9 Página web desde la que se descarga

Los nombres de archivo que utiliza son *fireworks.exe*, *install.exe*, *patch.exe*, *run.exe*, *setup.exe* y *video.exe*.

5.- Recomendaciones

La ingeniería social sigue siendo el talón de Aquiles de los usuarios, que motivados por su curiosidad, en la mayoría de los casos, no desconfían de mensajes de correo electrónico como los que hemos mencionado en el apartado anterior. Mensajes en los que se distribuyen los códigos maliciosos de esta familia.

Una de las características de los Waledac es que utilizan enlaces a páginas web para distribuirse. Para ello, crean páginas web maliciosas que imitan a las legítimas para no levantar las sospechas de los usuarios. Tal es el caso de la página de YouTube, que con el pretexto de mostrar un supuesto video, ha sido utilizada por los ciber-delincuentes para crear páginas web similares y en apariencia inofensivas.

Cuando sea redirigido a una página web que parece ser una página legítima, como puede ser la de YouTube, asegúrese de que la URL que aparece en la barra de direcciones sea la oficial y no otra.

Sin embargo, si desconoce cuál es la página oficial de ese sitio, puede buscar este dato en cualquiera de los buscadores que utilice habitualmente. Por normal general, el primer resultado se corresponde con la página oficial.

Para evitar realizar estas comprobaciones de forma manual, puede utilizar un software de seguridad que se encargaría de realizar esta tarea. Tal es el caso de *Identity Protect*, un módulo incluido en las últimas soluciones de seguridad de Panda. Este programa se encargaría de bloquear URLs sospechosas o maliciosas y mostraría un mensaje de alerta informando al usuario del riesgo de acceder a ellas.

Si no dispone de ninguna solución que le proporcione este servicio y no se ha percatado de si la página web a la que ha accedido es sospechosa, aún está a tiempo de evitar que su ordenador quede infectado. Para que el archivo malicioso se descargue e instale en el ordenador, es necesaria la confirmación del usuario.

Antes de ejecutar cualquier archivo, es aconsejable analizarlo con una solución de seguridad.

6.- Referencias

Blog PandaLabs

http://pandalabs.pandasecurity.com/archive/New-Alanchun.aspx

http://pandalabs.pandasecurity.com/archive/Nurech.A.worm-Alert.aspx

http://pandalabs.pandasecurity.com/archive/Nurech.A.worm-Alert-II.aspx

http://pandalabs.pandasecurity.com/archive/Malware-Campaign-Impersonates-Barack-Obama_2700_s-Website.aspx

http://pandalabs.pandasecurity.com/archive/Waledac-Storm-worm_2E002E002E00_-New-Target_3A00_-Valentine_1920_s-day.aspx

http://pandalabs.pandasecurity.com/archive/San-Valentine_B400_s-day-is-close.aspx

http://pandalabs.pandasecurity.com/archive/New-waledac_2700_s-campaign.aspx

http://pandalabs.pandasecurity.com/archive/New-Storm-Worm_3A00_-Waledacs.aspx

Enciclopedia de malware

http://www.pandasecurity.com/spain/homeusers/security-info/

Notas de prensa

http://www.pandasecurity.com/spain/enterprise/media/press-releases/viewnews?noticia=9529