

La historia sin fin: Virus Bagle

Autor: Lic. Cristian Borghello, Technical & Educational de Eset para
Latinoamérica

Fecha: Lunes 19 de junio del 2006



Historia

El 18 de enero de 2004 el mundo se vio azotado por una nueva epidemia de virus. En ese momento todo hacía pensar que este era otro gusano común y corriente a los que estamos tan acostumbrados, pero la historia demostró que esta vez era distinto y de hecho el Bagle o Beagle ha demostrado ser el virus más persistente e "inteligente" desde la existencia de Internet. Incluso, algunos autores atribuyen una "estrategia empresarial" detrás del mismo.

A través de los años, los autores del Bagle han demostrado una gran habilidad para lograr cambios técnicos y de distribución en el código del *malware*. El Bagle ha evolucionado incorporando nuevas técnicas de infección, de reproducción y de ingeniería social, lo cual siempre repercute en una gran efectividad en su reproducción y cantidad de infecciones, así como seguramente en el beneficio económico (incalculable) para sus autor/es.

Los autores de estos gusanos han sabido utilizar su código para instalarse alrededor del mundo y posteriormente utilizar esas instalaciones como punto de ataque para nuevos códigos actualizados y con nuevas "funcionalidades".

Cada una de las distintas versiones que han aparecido, es capaz de cosechar distintos tipos de información. El Bagle puede verse como una "inversión a largo plazo" de sus autores, que ha resultado en un negocio rentable. Es decir, que este virus se ha sabido posicionar como un excelente producto que permite a sus creadores distintos tipos de beneficios.

Las diferentes versiones del gusano han sido lanzadas en distintos períodos claves como puede ser importantes encuentros, concursos de gran repercusión o el actual mundial de fútbol. Esto permite asegurar a los autores la mayor difusión, pero también les permite una alta tasa de efectividad posterior a las fechas de difusión, ya que es fácil asumir que gran cantidad de máquinas seguirán infectadas. Es decir que luego de la infección existe un período de "aprovechamiento" de los beneficios a la vez que los medios de información y los expertos "olvidan" el problema.

En el período inicial de Bagle (18-01-2004 a 30-04-2004), sus autores establecieron las funcionalidades básicas: asegurar su reproducción y evitar ser detectado.

El siguiente período (aproximadamente 6 meses) se focalizó en detalles como la forma de distribución y la apariencia de los correos electrónicos que explotan la ingeniería social.

El período actual se ha centrado en las distintas piezas del *malware* para asegurar el beneficio posterior a la infección.

A continuación se realiza un compendio de las principales versiones aparecidas hasta la fecha:

- 18 de enero de 2004. Aparece la primera versión (Bagle.A). El asunto del mail era “hi” y abría la calculadora de Windows.
- 28 de febrero al 4 de marzo 2004. Aparecen las versiones C a K del gusano, marcando lo que posteriormente sería una costumbre: lanzamiento de más de una versión para evitar la detección de los antivirus. Desde la versión J comienza la batalla de insultos con el virus Netsky y el intento de desinstalarlo.
- 18 y 19 de marzo de 2004. Aparecen las versiones P a T que no utilizan adjuntos para reproducirse, sino que aprovechan vulnerabilidades de Windows ya corregidas para propagarse.
- 7 de abril de 2004. Aparece la versión W capaz de deshabilitar gran cantidad de software de seguridad y antivirus, y de aprovecharse de otros troyanos para realizar su función de reproducción.
- 9 de agosto de 2005. Aparece la versión BI que logró una alta tasa de infección en pocas horas y que descargaba gran cantidad de componentes de Internet. La cantidad de versiones publicadas en esta ocasión provocó confusión de las casas antivirus para nombrarlo.
- 21 de septiembre de 2005. Aparecen las versiones CK a CY logrando desactivar casi cualquier Antivirus o Firewall existente.
- 16 de diciembre de 2005. Aparece la versión DR logrando una gran reproducción y mostrando imágenes de Windows.
- 15 de febrero de 2006. Aparece la versión FF aprovechando los juegos de invierno de Torino.
- 16 de junio de 2006. Aparece la versión GK aprovechando el mundial de fútbol y logrando reproducción masiva en apenas una hora.

Descripción

Bagle es un gusano escrito en distintos lenguajes de programación (según la versión puede ser C o Assembler), comprimido y/o encriptado con distintas herramientas, residente en memoria, y que se propaga a través del correo electrónico y redes P2P. Si llega por mail, tiene un asunto que varía con cada versión, su remitente siempre es falso y contiene adjuntos. Este gusano es capaz de actualizarse desde diferentes sitios de Internet y de desactivar cualquier programa de seguridad instalado.

Si bien durante sus cientos de versiones el mismo ha ido cambiando la forma de beneficiarse, sus funcionalidades pueden resumirse en:

- Envío de SPAM: su principal medio de distribución.
- Robo de direcciones de correo electrónico: le permite realizar ataques de Phishing y favorecer el SPAM, así como la venta, por parte de sus autores de las direcciones obtenidas.
- Robo de información confidencial: su principal beneficio.
- Instalación de *Backdoors*: le permite establecer futuros puntos bases de ataques.

La información que las distintas versiones recolectan a través de sus componentes es:

- IP, NAT, Nombre de la computadora infectada y su dominio
- Nombres de usuario y contraseña de POP3/IMAP
- Usuario grabados por el navegador
- Configuración de cuentas FTP, navegadores web y clientes de correo.
- Contraseñas de administradores de passwords.
- Usuario y contraseña de mensajeros instantáneos
- Usuario y contraseñas de dispositivos RAS
- Usuario y contraseñas de sitios de Home-Banking

- Hashing de contraseñas

Gracias a sus múltiples funcionalidades es capaz de realizar las siguientes tareas:

- Instalación de trojanos y *backdoors* que permiten el control remoto de las maquinas infectadas y la creación de redes de bots (zombies).
- Manipulación de DNS y archivos de host del sistema.
- Auto-actualización y descarga de otros *malware* como el trojano Mitglieder.
- Inyección de distintas funcionalidades del sistema operativo.
- Finalización de procesos y servicios de aplicaciones de seguridad (Antivirus, Firewalls, IDS) y del sistema operativo.
- Residencia en memoria.
- Cambio de íconos de sus adjuntos para pasar desapercibido. A continuación se muestran algunos ejemplos:



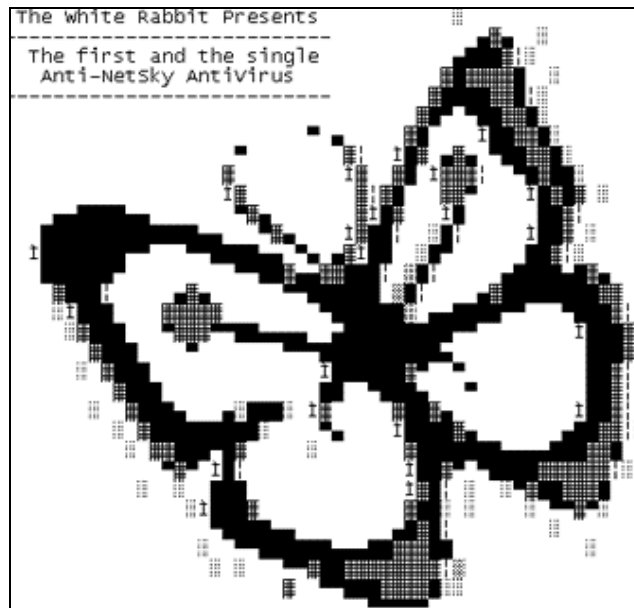
- Utilización de ingeniería social en el cuerpo y asunto del mensaje.
- Generación de nombres de archivos aleatorios (o conocidos por el usuario) para facilitar el engaño.
- Generación de ID para cada computadora infectada.
- Catalogación de equipos infectados.
- Rápida modificación de su código que obliga a los Antivirus a su actualización excepto a aquellos que lo detectan con capacidades proactivas.
- Explotación de vulnerabilidades solucionadas o sin solución así como 0-days.
- Capturas y envío de pantallas.

- Capturas de teclas.
- Auto-caducidad luego de un período de tiempo.
- Recolección y robo de contraseñas para muchas aplicaciones.
- Falsear direcciones de mails de origen.
- Motor propio de envío de correo (SMTP).
- Conexión de sitios remotos para la realización de distintas acciones.
- Encriptación y compresión de distintas partes de su código mediante diferentes técnicas.
- Aprovechamiento de las *botnets* creadas mediante su componente de *backdoor*.
- Evita actualizaciones de programas de seguridad.
- Evita el envío de correos electrónicos a empresas de seguridad.
- Prevención contra ataques de otros *malware* como NetSky.

Este último punto, también es original en nuestra historia, ya que en el año 2004 se desató una guerra entre los creadores de varias versiones de los gusanos Netsky, Bagle y MyDoom exacerbando aún más sus devastadores efectos. En esa época era común encontrar en el código fuente mensajes cruzados, en los que se podían leer insultos, amenazas y descalificaciones mutuas.

Esta guerra fue curiosa, porque si un usuario estaba infectado con Bagle, Mydoom, Deadhat o Nachi (autores que se presume relacionados), y luego era infectado con una versión particular de Netsky, este gusano se encargaba de "desinstalar" los primeros.

A continuación se muestra un texto que permanece encriptado en una de sus versiones (puede leerse el mensaje Anti-NetSky):



Esta batalla finalizó con el arresto del alemán Sven Jaschen, el supuesto "Robin Hood de los virus" y creador de al menos 30 versiones de NetSky y 4 de Sasser.

La Familia

Como ya se mencionó, Bagle se vale de diferentes componentes para realizar sus tareas. Los programas (en su mayoría otros *malware*) de los que se vale para realizar sus funciones son:

Gusano Bagle propiamente dicho: es el encargado de instalar los otros componentes, llevar registro de lo realizado, eliminar "competidores", controlar las redes de bots y mantenerse actualizado desde distintos sitios de Internet.

Mitglieder/Beagoz: troyano encargado de realizar el envío masivo de mail, vulnerar todo el software de seguridad, robar datos y actualizarse. Más información puede ser encontrada en: <http://www.encyclopediavirus.com/virus/vervirus.php?id=2174>

Tooso/Tango: troyano que vulnera y desactiva los componentes de seguridad del sistema y detiene procesos y servicios de actualización de software. Ambos son detectados como variantes de Bagle.

Lodear/Lodeight: troyanos desarrollados para buscar, obtener y actualizar distintos miembros de la familia desde Internet. Son detectados como variantes de Bagle.

Monikey: gusano desarrollado para facilitar la propagación mediante el envío masivo de correo y la utilización de redes P2P. También es detectado como variante de Bagle.

LDPinch, Tarno y Vipgsm: permiten el robo de contraseñas de distintos programas. Más información puede ser obtenida en <http://www.nod32-la.com/about/press.php?id=96>

Formglieder: utilizado para obtener información confidencial como datos bancarios y financieros. Es detectado como variante de Bagle.

Esta familia ha permanecido muy unida a través de las distintas versiones de Bagle, permitiendo que uno de ellos actualice otros y estos a su vez descarguen nuevas versiones.

Por ejemplo Bagle.BK descarga Tooso.E y Tooso.F y este último a su vez actualiza Bagle a su nueva versión Bagle.BN

Descripción

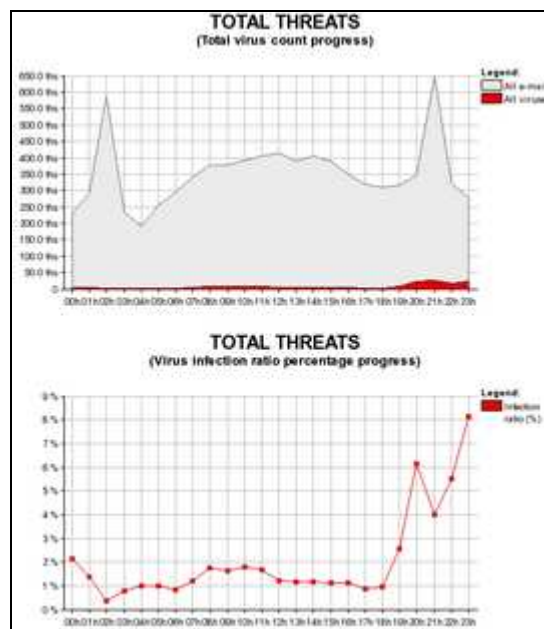
A continuación se detalla la forma de funcionamiento del mismo, teniendo en cuenta que pueden variar según la versión del gusano.

- Arriba un mail haciendo uso de alguna técnica de ingeniería social y generalmente tratando un tema de gran repercusión o interés; o bien el usuario descarga un archivo infectado por redes P2P
- El usuario descarga el mail y ejecuta su adjunto
- El troyano descarga otros componentes del gusano y se instala en el sistema mediante diferentes técnicas según la versión (por ejemplo en carpetas compartidas o recursos de P2P)
- Se ejecuta el segundo programa descargado

- Se recolecta información sensible del sistema infectado
- Se auto-envía a cualquier dirección de mail que haya recolectado

Para este análisis se ha tomado la última versión (Bagle.GK) detectada el 16 de junio de 2006 en donde puede verse la siguiente incidencia en los reportes de VirusRadar.

Cantidad de infecciones detectadas el viernes a las 0 hs. y a las 20 hs.



Cantidad de infecciones detectadas el viernes 16 a las 20 hs.

2006-06-16 17:00	0	0 %	
2006-06-16 18:00	301	0.098 %	1/ 1.0 ths
2006-06-16 19:00	5 848	1.842 %	1/ 54.3
2006-06-16 20:00	19 122	5.494 %	1/ 18.2
2006-06-16 21:00	19 304	2.971 %	1/ 33.7

Time interval: Day Week Month Year

Total infection ratio in the last 24 hours

TOTAL THREATS
(Virus infection ratio percentage progress)

[More information...](#)

Top threats in the last 24 hours

Virus	Count
1. a variant of Win32/B...	44 575
2. Win32/Netsky.Q worm	27 554
3. Win32/Bagle.GK a variant of Win32/Bagle worm	26 345
4. probably unknown New...	14 426
5. Win32/Zafi.B worm	4 161

Top virus in the last 24 hours

Info: a variant of Win32/Bagle worm

Risk: Elevated

Date first captured: 2005-11-01 17:39

Date last captured: 2006-06-16 21:50

Total stopped to date: 111 986

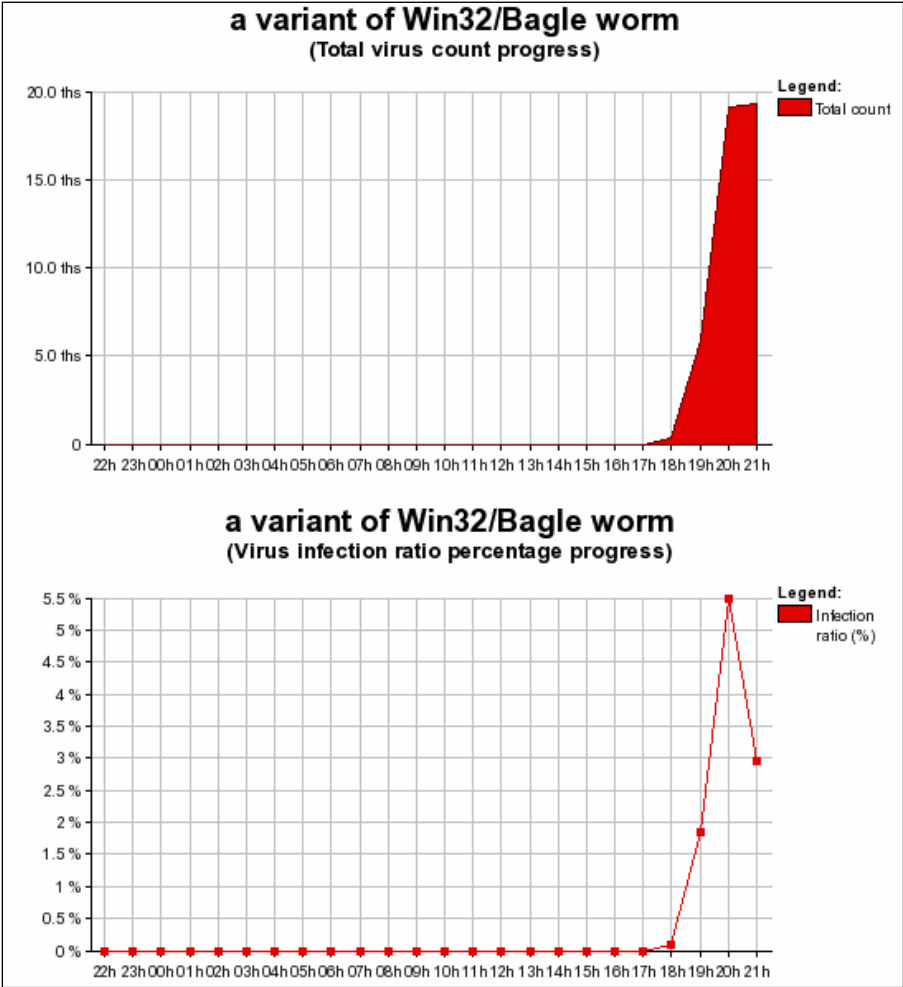
Most active month: 2006-06

Most active date: 2006-06-16

Infection ratio (2006-06-16): 0.566 %

[Virus Encyclopedia NOD32...](#)

[More information...](#)



Como ya se ha mencionado el gusano comienza su distribución y llega por correo electrónico aprovechando alguna fecha especial como el actual mundial de fútbol.

A continuación puede verse el correo electrónico que podemos recibir en nuestra casilla:

```

Received: from terra.com (89.Red-80-32-55.staticIP.rima-tde.net [80.32.55.89]) by tarzan.ophiropt.co.il
(Content Technologies SMTPRS 4.3.17) with SMTP id <T78e5b332730a00000b448@tarzan.ophiropt.co.il> for <efs@ophiropt.co.il>;
Thu, 15 Jun 2006 20:03:21 +0200
Date: Thu, 15 Jun 2006 19:21:25 +0100
To: "Efs" <efs@ophiropt.co.il>
From: "Efs" <efs@ofir.dk>
Subject: Jeffrye
Message-ID: <eopdkrsrswjtystninx@ophiropt.co.il>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="-----zcoognkvxjnszszlikid"
-----zcoognkvxjnszszlikid
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit

<html><body>
Robert<br>
</body></html>

-----zcoognkvxjnszszlikid
Content-Type: application/octet-stream; name="Margrett.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Margrett.zip"

UESDBBQAAAAIACEc0DQue+3KfSEAA08pAAA0AAAAMTUtMDYtMjAwNi5leGxtenVULF2799CI
xNCIoDQ80gdwIh2CdEtKSKo0CFICA0MMnVISOPLS3Q2ChIh0SrfEnBn1ed7nfV/PWedb33e+
v85vMfe19++69rWv2Kx7Zt23sj4AgAIAAFARHzgcAHgE+Ik/5X8FpI2qDACghIL2T/wCAB/L
NgoG7t7faP8FAX4Q/lzJfDnpui/9H/KveVfwfwlgD9t/5J/IT83A7Ag5XsAgArr32N0Q+hx

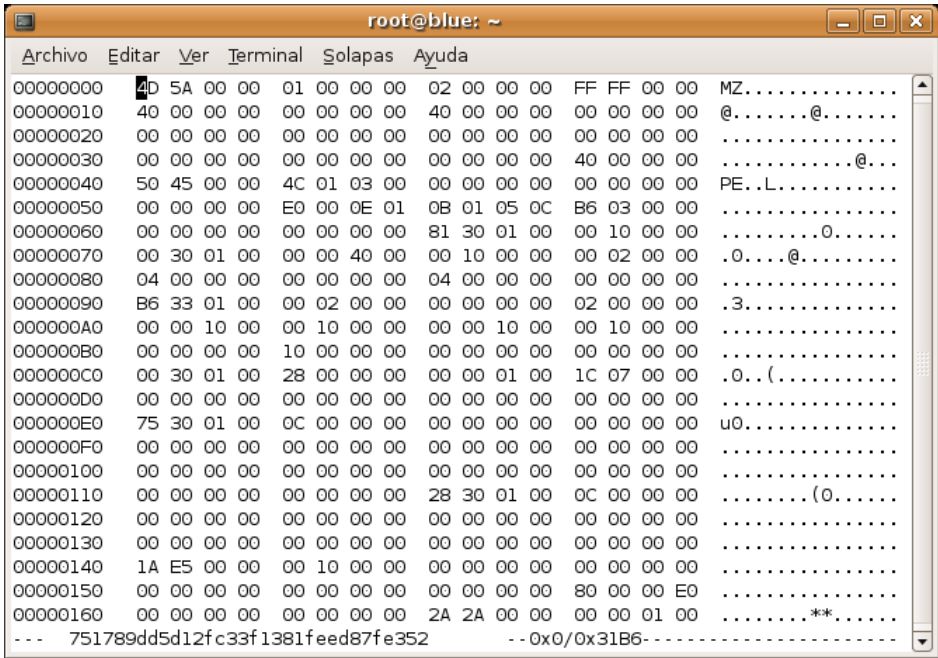
```

Como puede apreciarse, el cuerpo del mensaje contiene "Robert" y a continuación puede verse que el archivo adjunto se llama "Margrett.zip". En la parte inferior de la imagen se aprecia el comienzo del archivo ZIP codificado en BASE64.

Posteriormente podemos ver el contenido del archivo: un ejecutable, la última instancia para comenzar a realizar las acciones ya mencionadas.



Por último vemos el archivo EXE en un editor hexadecimal.



Este archivo es el gusano propiamente dicho detectado como Bagle.GK y podemos comprobar esto fácilmente teniendo un antivirus actualizado e intentando abrirlo:



Conclusiones

Como es fácil apreciar, este gusano hace uso de una amplia variedad de herramientas para llevar a cabo sus fines, que son continuar su supremacía en cuanto a reproducción y robo de información que puede ser aprovechada por sus creadores para la realización de otras acciones delictivas.

En los dos años y medio que lleva en el “mercado”, ha sabido hacerse de una merecida reputación por lo que es fundamental permanecer informados sobre su evolución, ya que siempre se ha valido de nuevas técnicas y de fechas importantes para lograr sus objetivos.

En lo que refiere a sus autor/es, los mismos han sabido permanecer en el anonimato el tiempo necesario como para hacer pensar que podrían seguir así a menos que un ataque sea considerado excesivo por algún cuerpo de delito informático y los mismos consideren seriamente la posibilidad de terminar con esta amenaza.

Mientras esto no suceda todo se deberá considerar la posibilidad de que seguirán apareciendo más versiones de Bagle que seguirán evolucionando y aprovechando el descuido de los usuarios, así como fechas y vulnerabilidades determinadas para su propagación masiva.

Más información:

<http://www.segu-info.com.ar/articulos/articulos.htm>

<http://www.encyclopediavirus.com/virus/vervirus.php?id=3173>

<http://www.hispasec.com/unaaldia/2383>

<http://www.ee.ualberta.ca/~kaut/files/BeagleLessons.pdf>

<http://www.infectionvectors.com/vectorspaces.htm#beagle5>

http://www.virusradar.com/index_esn.html