Netsky, un viaje en el tiempo

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

Fecha: Lunes 30 de abril del 2007

ESET, LLC 1172 Orange Ave., Coronado, California 92118, USA
phone: (619) 437 – 7037, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

Introducción

En julio del 2005, el adolescente Sven Jaschan recibió una condena de un año y nueve meses, luego de admitir haber creado los gusanos Sasser y Netsky. Al ser juzgado como menor de edad y tras cumplir pocas horas de servicios sociales en su ciudad natal de Verdeen, al norte de Alemania, Sven siguió su vida. Hoy, un año y nueve meses después de este hecho, Netsky también sigue su vida.

Hablar de malware y de creación de nuevas amenazas, generalmente es hablar de innovación.

En este artículo se hablará de la excepción a la regla: Netsky, un gusano que tres años después de su creación, permanece como uno de los más detectados por las firmas antivirus.

Particularmente se analizará la versión Q (o P según la casa antivirus), que resulta ser la más propagada de todas las existentes.

Analizar cuáles pueden ser las causas de este hecho es complicado e incluso es posible que ninguna de las opiniones al respecto coincida. Ante todo, se plantearán algunas preguntas que pueden resultar interesantes:

- ¿Existen nuevas variantes de este gusano? No, no se registran nuevas apariciones desde el año 2004, cuando el equipo en donde el gusano había sido desarrollado fue confiscado por las autoridades que detuvieron a su autor.

- ¿Es detectado por los antivirus? Sí, actualmente todas las variantes son detectadas como lo demuestra la siguiente imagen:

Antivirus	Version	Actualización	Resultado
AhnLab-V3	2007.4.25.0	24.04.2007	Win32/Netsky.worm.29568
AntiVir	7.4.0.14	24.04.2007	Worm/NetSky.P
Authentium	4.93.8	23.04.2007	W32/Netsky.P@mm
Avast	4.7.981.0	23.04.2007	Win32:Netsky-AF
AVG	7.5.0.464	23.04.2007	I-Worm/Netsky.Q
BitDefender	7.2	24.04.2007	Win32.Netsky.P@mm
CAT-QuickHeal	9.00	23.04.2007	W32.NetSky.P
ClamAV	devel-20070416	24.04.2007	Worm.SomeFool.P
DrWeb	4.33	24.04.2007	Win32.HLLM.Netsky.35328
eSafe	7.0.15.0	23.04.2007	Win32.Netsky.q
eTrust-Vet	30.7.3592	24.04.2007	Win32/Netsky.P
Ewido	4.0	24.04.2007	Worm.NetSky.q
FileAdvisor	1	24.04.2007	Low threat detected
Fortinet	2.85.0.0	24.04.2007	W32/Netsky.P@mm
F-Prot	4.3.2.48	24.04.2007	W32/Netsky.P@mm
F-Secure	6.70.13030.0	24.04.2007	Email-Worm.Win32.NetSky.q
Ikarus	T3.1.1.5	24.04.2007	Email-Worm.Win32.NetSky.q
Kaspersky	4.0.2.24	24.04.2007	Email-Worm.Win32.NetSky.q
McAfee	5015	23.04.2007	W32/Netsky.p@MM
Microsoft	1.2405	24.04.2007	Worm:Win32/Netsky.P@mm
NOD32v2	2215	24.04.2007	Win32/Netsky.Q
Norman	5.80.02	24.04.2007	Netsky.P@mm
Panda	9.0.0.4	23.04.2007	W32/Netsky.P.worm
Prevx1	V2	24.04.2007	Malware:NetSky.P
Sophos	4.16.0	23.04.2007	W32/Netsky-P
Sunbelt	2.2.907.0	19.04.2007	Email-Worm.Win32.NetSky.q
Symantec	10	24.04.2007	W32.Netsky.P@mm
TheHacker	6.1.6.095	15.04.2007	W32/Netsky(2).gen@MM
VBA32	3.11.4	23.04.2007	Worm.Win32.Netsky.Q
VirusBuster	4.3.7:9	24.04.2007	I-Worm.Netsky.Q1
Webwasher-Gateway	6.0.1	24.04.2007	Worm.NetSky.P

Imagen 1 - Detección de NetSky.Q

- ¿Utiliza métodos de infección originales? No, sus métodos son el "antiguo" uso del correo electrónico y las redes P2P como medios de propagación masiva.

- ¿Puede influir los nombres de los archivos utilizados que contienen al malware para propagarse? Efectivamente, es posible que esto influya.

- ¿Todos los usuarios y administradores actualizan su software periódicamente? No, y esta puede ser la punta del iceberg.

- ¿Todos los usuarios se capacitan en temas básicos sobre cómo proteger su sistema? No, generalmente al usuario estos temas lo tienen sin cuidado.

- ¿Todos los usuarios utilizan antivirus y firewall? No, y esto puede ser la parte sumergida del iceberg.

- ¿Por qué se sigue propagando? Es lo que se intentará dilucidar.

Desde el momento de su aparición en el 2004 hasta la actualidad, el Netsky.Q siempre estuvo entre los malware de mayor propagación en las estadísticas mensuales, y en muchos casos, alcanzó la cima de los rankings.

En las estadísticas de marzo del 2007, esta variante de la familia únicamente fue superada por la detección heurística de ESET NOD32, la cual engloba la suma de todo tipo de malware desconocido.

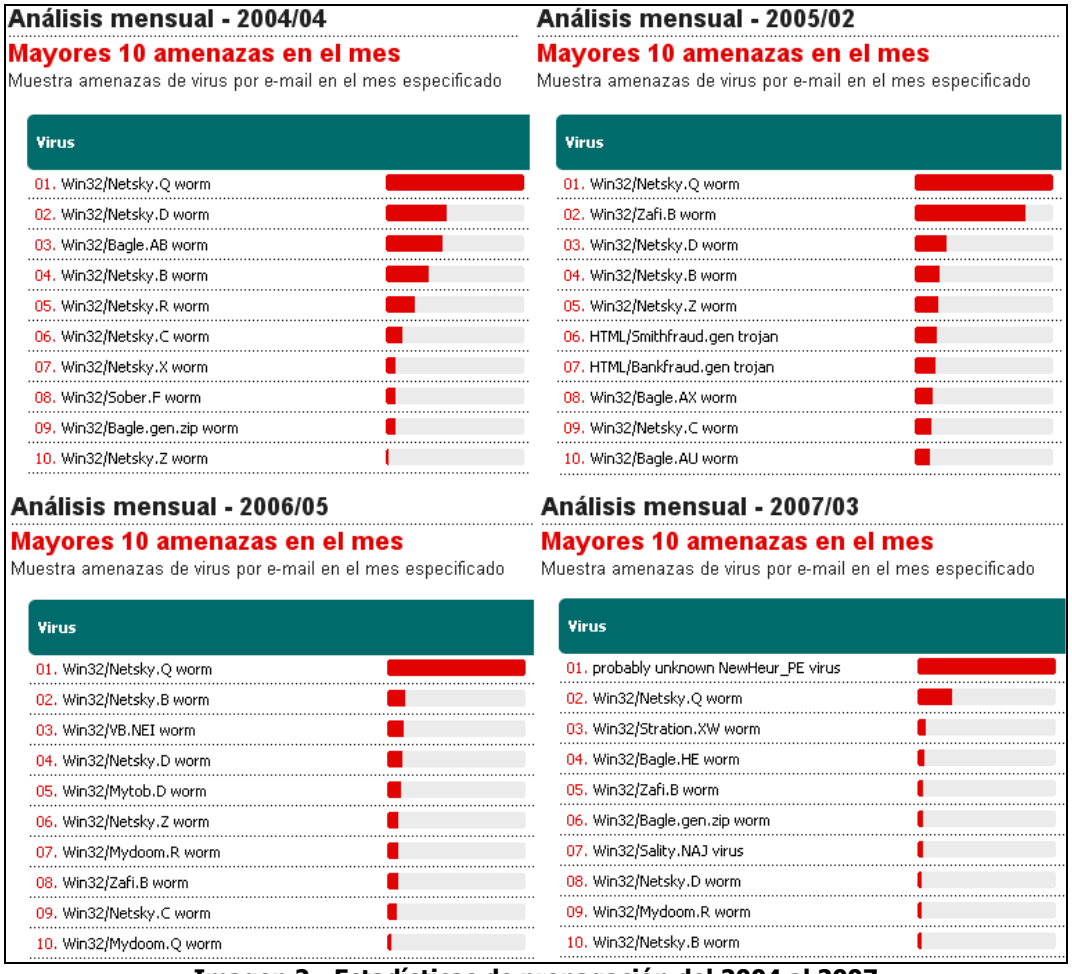

Imagen 2 - Estadísticas de propagación del 2004 al 2007

Arribo

El gusano puede llegar al sistema del usuario por correo o bien ser descargado de redes P2P como Kazaa, eMule, eDonkey, etc.

En el primer caso, la propagación se realiza mediante el envío de correo masivo a direcciones que son obtenidas mediante técnicas que luego serán evaluadas. El usuario recibe un correo electrónico en inglés con un archivo ejecutable o bien con un archivo comprimido (formato zip) conteniendo el ejecutable. El cuerpo del correo varía, pero siempre es un mensaje que intenta engañar al usuario para que descargue el adjunto.

En la siguiente imagen se puede apreciar el formato típico de un mensaje con Netsky:

Imagen 3 - Archivo adjunto al recibir un correo

Como puede verse, se utiliza la Ingeniería Social intentando convencer al usuario de que el correo es inofensivo para que este descargue el adjunto y lo ejecute.

En el caso de las redes P2P, el usuario descarga un archivo ejecutable, engañado al creer que en realidad descarga los archivos en los que está interesado. Esta etapa de la infección se analizará con detalle, más adelante en este documento.

En los casos en que el sistema no se encuentre actualizado, el gusano puede utilizar una antigua vulnerabilidad del año 2001 [1] de Internet Explorer en versiones anteriores a la 6.0, que permite la ejecución del archivo adjunto con sólo leer el mensaje o visualizarlo en el panel de vista previa (sin acción del usuario).Como es evidente, esta última forma de propagación podrá afectar sólo a usuarios que hace más de 6 años no cambian o actualizan su sistema.

Una vez que el archivo comprimido ha sido descargado, el usuario deberá descomprimirlo para luego ejecutarlo.

En lo que respecta al archivo ejecutable en sí, el autor del gusano utilizó una técnica muy antigua y conocida para engañar al usuario: la doble extensión. En la siguiente imagen puede apreciarse que el archivo descargado simula tener extensión ".txt" pero en realidad puede verse que es un archivo ".exe".

Imagen 4 - Doble extensión de archivos

El ejecutable es el gusano propiamente dicho, un archivo de 29.568 bytes empaquetado con la aplicación FSG.

Si se presta atención puede verse que el supuesto "document.txt" es en realidad un archivo del tipo "Aplicación" y no un archivo de texto como simula ser. Además, extendiendo la columna de nombre del archivo puede verse la extensión real.

Es muy normal cometer este error debido a que la configuración por defecto de Windows no muestra las extensiones de los archivos. Para hacerlo, debe cambiarse esta configuración desde Herramientas → Opciones de Carpeta → Ver, y desmarcar la opción "Ocultar las extensiones de archivos conocidos".

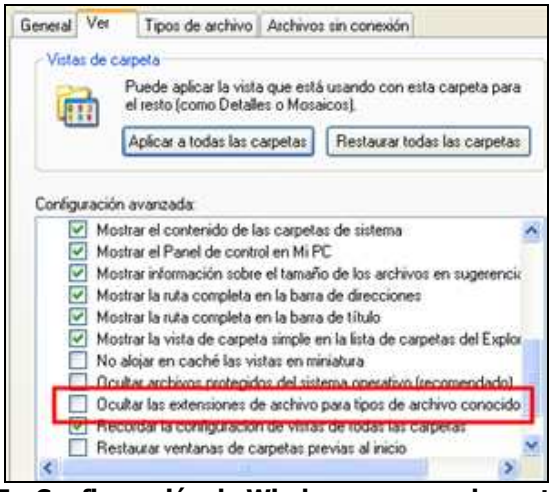

Imagen 5 - Configuración de Windows para ver las extensiones

Si el usuario hace doble clic sobre el archivo mencionado en la imagen número 4 habrá instalado el malware en su computadora y comenzará a formar parte de una extensa red de usuarios infectados que se encargan de propagar más correo basura (spam) con copias del mismo malware.

Luego de la ejecución, el gusano crea un mutex [2] para evitar ejecutarse más de una vez en el mismo sistema y el primer síntoma de infección no se hace esperar. El usuario comenzará a sufrir de inmediato una ralentización notable en las comunicaciones debido al ancho de banda ocupado por el gusano al enviar spam.

Además, al observar los procesos activos se ve que el gusano se encuentra en funcionamiento. Es suficiente terminar este proceso para que el gusano deje de actuar. Como puede verse, las técnicas utilizadas son tan sencillas como el modo de revertir las formas de ataques.

Imagen 6 - Proceso de NetSky ejecutándose

Para asegurar su permanencia en el sistema del usuario, el gusano crea una clave en el registro:

Clave: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Valor: Norton Antivirus AV → X:\WINDOWS\FVProtect.exe (donde X: es la unidad donde se encuentra instalado el sistema operativo).

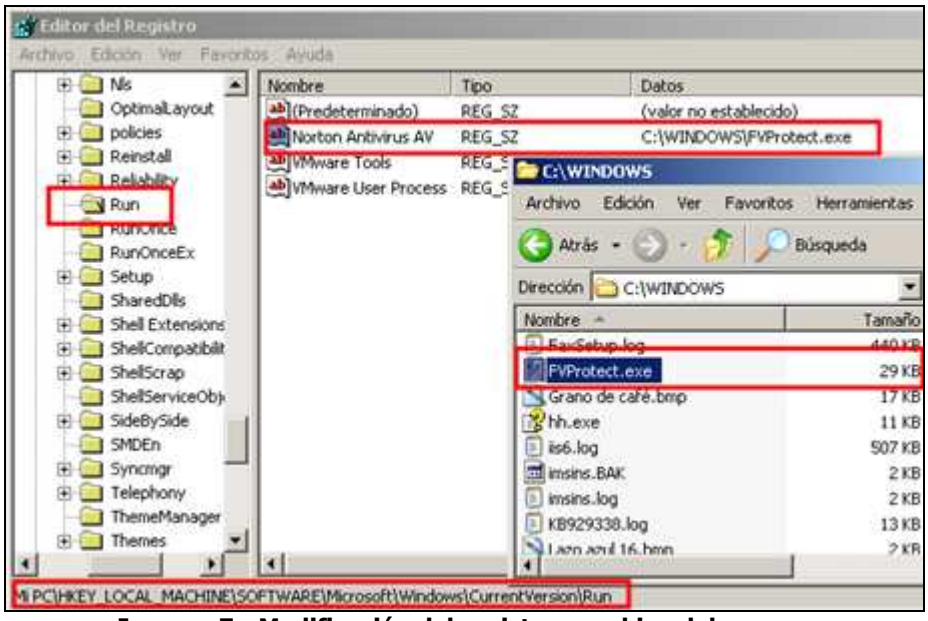

Imagen 7 - Modificación del registro y archivo del gusano

Así también, elimina otras claves del registro, la mayoría de ellas relacionadas con su "rival": el Gusano Bagle [3]. Resulta curioso que, en su código fuente puede encontrarse el siguiente mensaje haciendo referencia a Bagle:

```
"Bagle do not delete SkyNet. You fucked bitch! Wanna go into a prison?
We are the only AntiVirus, not Bagle, shut up and take your butterfly!
        Message from SkyNet AV Team Lets join an all bagle!"
```

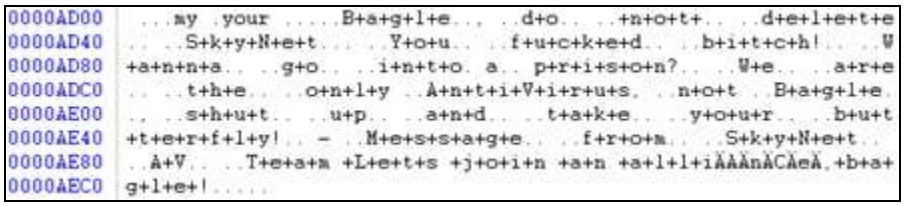

Imagen 8 - Mensaje de Netsky a Bagle

Además de "FVProtect.exe" crea otros archivos en el directorio del Windows para luego utilizarlos en su propagación vía correo electrónico. Ellos son:

- base64.tmp: versión codificada en formato UUEncoded del archivo ejecutable (40.520 bytes)
- zip1.tmp: versión codificada, en formato MIME, del gusano en archivo ZIP (40.882 bytes)
- zip2.tmp: versión codificada, en formato MIME, del gusano en archivo ZIP (40.894 bytes)
- zip3.tmp: versión codificada, en formato MIME, del gusano en archivo ZIP (40.886 bytes)
- zipped.tmp: el gusano en archivo ZIP (29.834 bytes)

Estos archivos se encuentran codificados en Base64 [4] (MIME o UUEnconde) y listos para ser utilizados por cada envío del gusano. Si se convierte este texto a ASCII se podrá apreciar que en realidad se trata de archivos ejecutables o comprimidos.

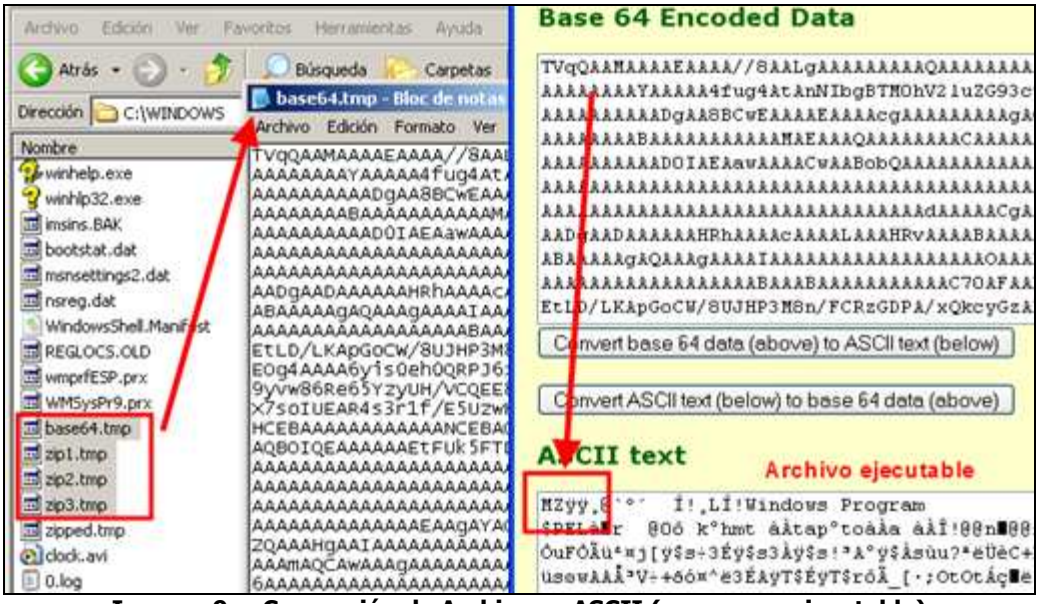

Imagen 9 - -Conversión de Archivos a ASCII (genera un ejecutable)

Propagación

Más allá del efecto mencionado en las comunicaciones, también puede observarse una ralentización en las tareas normales del sistema. Esto se debe a que, al ejecutarse, el gusano crea copias de sí mismo en las carpetas que pueden ser utilizadas en redes P2P. Para ello, busca las siguientes carpetas:

shared files, kazaa, mule, donkey, morpheus, lime, bear, icq, shar, upload, http, htdocs, ftp, download, my shared folder

Y se copia, como se ve a continuación, con distintos nombres que puedan llamar la atención al usuario:

Imagen 10 - Archivos creados por el gusano

Cualquier usuario que busque archivos similares en las redes P2P mencionadas podría descargar una copia del gusano.

Luego de la creación de estos archivos, comienza su otra tarea fundamental: el envío masivo de mensajes. El gusano rastrea todas las unidades del sistema en busca de direcciones de correo que obtiene de archivos del siguiente tipo:

.adb, .asp, .cgi, .dbx, .dhtm, .doc, .eml, .htm, .html, .jsp, .msg, .oft, .php, .pl, .rtf, .sht, .shtm, .tbb, .txt, .uin, .vbs, .wab, .wsh, .xml

El gusano se enviará a todas las direcciones recolectadas en el equipo infectado. El remitente del mensaje es falsificado (spoofing) para engañar al destinatario.

Por otro lado, para evitar que lo reciban las casas antivirus, también evita enviarse a cada uno de los siguientes dominios:

@microsof - @antivi - @symantec - @spam - @avp - @f-secur - @bitdefender @norman - @mcafee - @kaspersky - @f-pro @norton - @fbi - abuse@ @messagel -@skynet @pandasof - @freeav @sophos – ntivir - @viruslis - noreply@ - spam@ - reports@

El asunto del mensaje, es seleccionado aleatoriamente desde una lista que se encuentra en el código fuente del gusano:

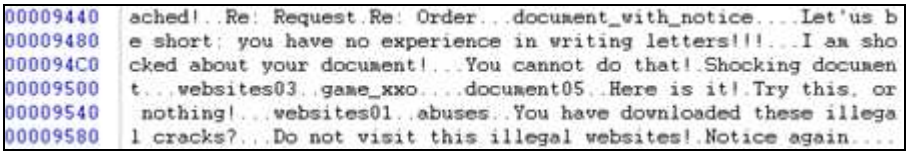

Imagen 11 - Lista de posibles "Asuntos" del mensaje

De la misma forma es creado el cuerpo del mensaje y la firma del mismo:

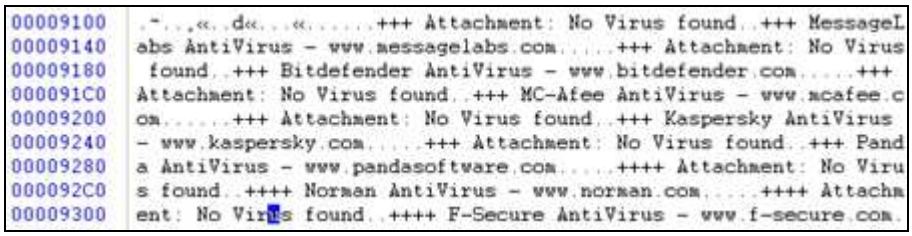

Imagen 12 - Lista de posibles "Cuerpo" del mensaje

Asimismo, también se crean los nombres de los archivos adjuntos al mensaje mediante la nomenclatura: [1] . [2] [Espacios] . [3]

- Donde [1] puede ser alguno de los siguientes nombres:
  document05 - websites03 - game_xxo - your_document
- [2] puede ser una de las siguientes extensiones:
  txt - doc
- Y [3] puede ser una de las siguientes extensiones:
  exe - pif - scr - zip

Un ejemplo podría ser: document05.txt [Espacios] .exe

Si la extensión seleccionada es cualquiera de las tres primeras expuestas en el último punto, el anexo será una copia de las ya mencionadas para el gusano. En caso de que la extensión sea .zip, el anexo será el archivo comprimido que contiene el ejecutable, y el nombre de este último variará entre: "document.txt", "data.rtf" o "details.txt".

Para finalizar, y al igual que la mayoría de los gusanos, Netsky utiliza su propio motor SMTP para enviarse a sí mismo a todas las direcciones de correo recolectadas anteriormente.

Para ello, al instalarse, copia en el directorio del sistema una librería dinámica (archivo DLL) con el nombre "userconfig9x.dll" de 26.624 bytes de tamaño y empaquetado con una versión modificada de UPX.

Esta librería es la que se encarga, entre otras cosas, del envío masivo de correo. Analizando el tráfico de red, se puede ver que se conecta a distintos servidores y ejecuta los comandos necesarios para el envío de correo.

Estas acciones se pueden reproducir, con los mismos resultados, mediante un sencillo comando telnet en DOS:

```
PUSH 1.1000DD28                    ASCII "HELO %s♪◙"
PUSH EAX
PUSH DWORD PTR SS:[EBP+10]
LEA EAX,DWORD PTR SS:[EBP-100]
PUSH 1.1000DD14                    ASCII "MAIL FROM:<%s>♪◙"
PUSH DWORD PTR SS:[EBP+14]
LEA EAX,DWORD PTR SS:[EBP-100]
PUSH 1.1000DD04                    ASCII "RCPT TO:<%s>♪◙"
PUSH EAX
LEA EAX,DWORD PTR SS:[EBP-100]
PUSH 1.1000DCFC                    ASCII "DATA♪◙"
```

Imagen 13 - Comandos enviados por el motor SMTP

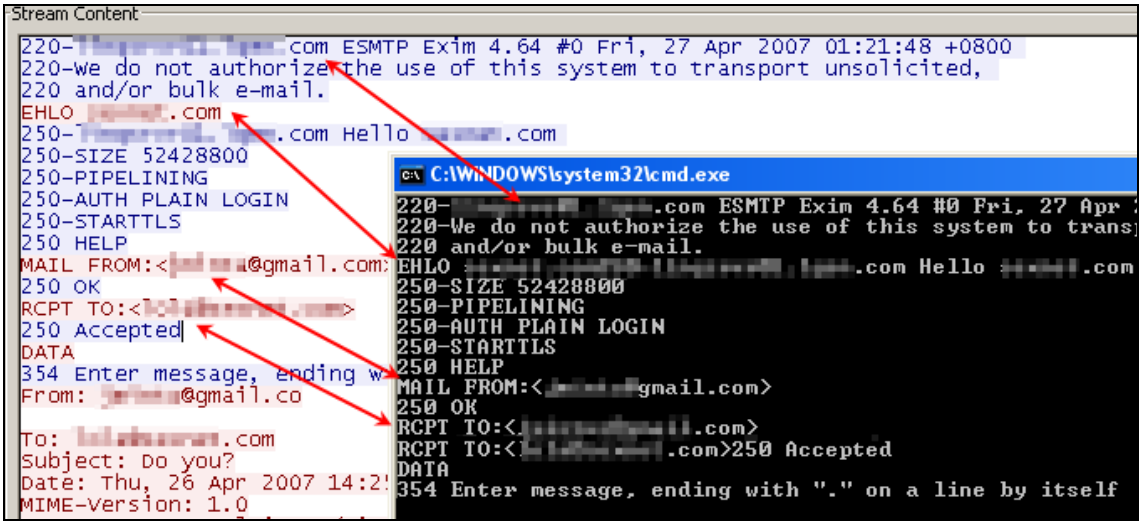

Imagen 14 – Resultado de los comandos enviados y acción reproducida con telnet

Estas conexiones son realizadas por el gusano en forma masiva cuando el mismo se activa, produciendo una degradación notable en el sistema y en las conexiones.

Conclusiones

Como puede verse el funcionamiento de este gusano no es complejo; sin embargo, el hecho de no controlar el funcionamiento del sistema y de las conexiones puede llevar a que el mismo logre tasas de infecciones como las mencionadas al comienzo del presente.

Ampliando las respuestas planteadas al inicio del documento, se puede lograr un acercamiento al porqué Netsky sigue siendo uno de los efectivos gusanos, luego de 4 años de su creación, detección y abandono del desarrollo original.

- Todos los usuarios y administradores actualizan su software periódicamente?

Como se mencionó Netsky explota una vulnerabilidad corregida en el año 2001. Lamentablemente muchos usuarios no actualizan sus sistemas (operativo, aplicaciones, navegador, etc.) produciendo que el mismo se encuentre vulnerable, aún cuando los agujeros de seguridad hayan sido solucionados hace años. Muchas veces se culpa al fabricante del software, pero también hay que ser conciente que la seguridad del sistema recae sobre el usuario.

- ¿Todos los usuarios utilizan antivirus y firewall?

La sencilla instalación de cualquiera de estas aplicaciones soluciona casi por completo los problemas de este gusano. Como se mencionó, todos los antivirus detectan a Netsky y además la instalación de un firewall asegura que ningún programa extraño intente conectarse desde y hacia el sistema para realizar envíos no deseados, sin autorización del usuario.

- ¿Todos los usuarios se capacitan en temas básicos para proteger su sistema?

Este es otro tema que es importante remarcar. No conocer los puntos básicos para la protección del sistema puede llevar a situaciones lamentables que, con un mínimo de interés podrían haberse evitado. Pensando en esta situación, ESET desarrolló su Plataforma Educativa [5] en la que el usuario encontrará valiosa información sobre cómo protegerse de las amenazas actuales.

- ¿Por qué se sigue propagando Netsky?

Por la combinación de los puntos anteriores y por la técnica de engañar a los usuarios curiosos mediante Ingeniería Social [6]. La cantidad de usuarios en Internet crece a un ritmo acelerado, se renuevan y así

siempre hay nuevos blancos ideales de este tipo de malware. Nunca faltarán usuarios y, lamentablemente, nunca faltarán nuevos "Netskys" para infectarlos.

A esto se debe sumarle que las redes de intercambio de archivo son una técnica eficaz para lograr que usuarios incautos descarguen este tipo de código malicioso bajo la creencia que descargan archivos útiles para sus fines. Cabe aclarar que muchas de estas aplicaciones suelen ser material pirateado, warez, cracks, etc.

En el ranking de este mes, Netsky se encuentra en la décima posición debido a un fuerte incremento de nuevas amenazas. Sin embargo, está situación se ya vivió durante los 4 años de vida del Netsky y dicho gusano volvió a escalar a las principales posiciones.

Es curioso que una antigua amenaza como la familia Netsky se mantenga vigente con el correr del tiempo, aún cuando es detectado por todos los antivirus existentes en el mercado actual. En casos como este, se puede observar cómo la educación toma fundamental relevancia, ya que un usuario capacitado siempre tendrá menos chances de ser infectado por cualquier tipo de malware actual y futuro.

Para más información:

[1] MIME Header Vulnerability
http://www.microsoft.com/technet/security/bulletin/MS01-020.mspx

[2] Mutex
http://es.wikipedia.org/wiki/Exclusi%C3%B3n_mutua_(inform%C3%A1tica)

[3] Bagle
http://www.eset-la.com/link.php?i=113

[4] Sistema de numeración Base64
http://es.wikipedia.org/wiki/Base64

[5] Plataforma Educativa de ESET
http://edu.eset-la.com

[6] El arna infalible: la Ingeniería Social
http://www.eset-la.com/threat-center/1515--arma-infalible:-ingenieria-social