EN INTERNET

*Eduardo Fainé Celis **

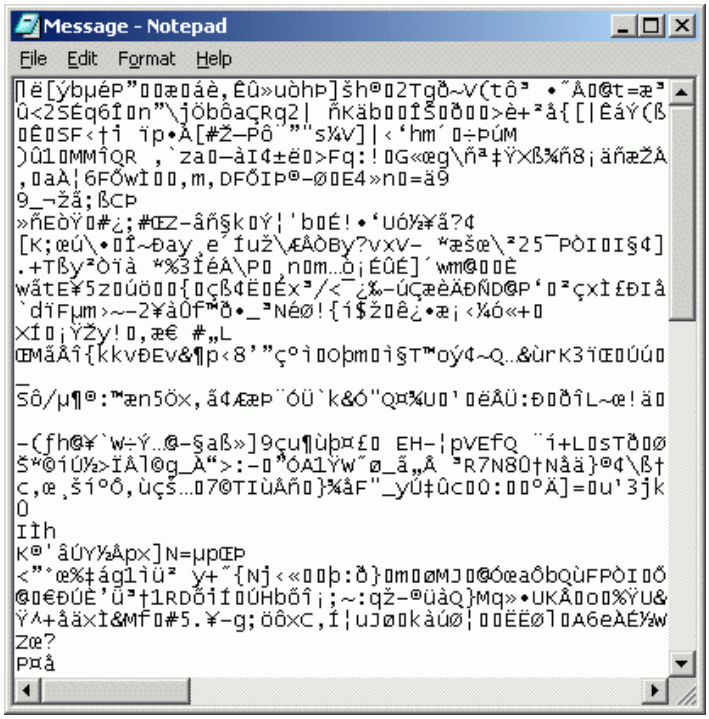
Ataque de virus.

Debo decir que los anuncios de virus son tan rutinarios que a veces me cuesta tomarlos en cuenta, más aún si poseo un buen antivirus que en otras ocasiones ha impedido el ingreso de estos dañinos programas en mi computador. Por lo mismo, cuando hace unas semanas, se informó a través de diversos medios de comunicación, acerca de un nuevo virus llamado Mydoom que estaba difundiéndose a través de Internet, mantuve las actualizaciones al día sin mayor preocupación hasta que de un día al siguiente, mi PC dejó de comportarse como una máquina obediente hasta que me fue imposible lograr que realizara operaciones tan sencillas como abrir programas del Office.

En esta ocasión se trataba de Mydoom, una nueva variante de MIMAIL que se propaga masivamente a través del correo electrónico y la red P2P KaZaa desde las últimas horas del 26 de enero de 2004.

El día anterior, recibí un correo electrónico originado por un supuesto administrador de correo con el siguiente asunto: Undeliverable: Mail Delivery System.

Como había enviado varios mensajes anteriormente ese día, creí que se trataba de alguno que no había llegado a su destinatario, por lo que abrí este correo, encontrando un archivo de texto que era el supuesto contenido de mi mensaje y, al abrirlo, se presentó esta pantalla:



Inmediatamente cerré el archivo, el mensaje, la conexión a Internet y ejecuté el antivirus, sin indicios de ataques, de modo que apagué el PC esperando que todo estuviera en orden, hasta que al encender al otro día comenzaron los problemas. El resultado final fue un disco duro formateado y mi computador casi nuevo desprestigiado por mal rendimiento hasta que fue evidente que ello se debía al virus ya mencionado.

La historia anterior demuestra que ni siquiera un antivirus al día es suficiente precaución cuando se recibe el ataque y que la mejor defensa es desconfiar de todo mensaje cuya procedencia no sea verificable.

¿Cómo opera?

Este gusano creado para atacar computadores que trabajen con cualquiera de las versiones de Windows, utiliza asuntos, textos y nombres de adjuntos variables en los correos a través de los que se envía, por lo que no es posible identificarlo o filtrarlo fácilmente. Además, utiliza como ícono el de un archivo de texto para aparentar inocuidad. Se esparce también copiándose a sí mismo a la carpeta compartida de KaZaa, con los siguientes nombres:

activation_crack.bat
activation_crack.pif
activation_crack.scr
icq2004-final.bat
icq2004-final.pif
icq2004-final.scr
nuke2004.bat
nuke2004.pif
nuke2004.scr
office_crack.bat
office_crack.pif
office_crack.scr
rootkitXP.bat
rootkitXP.pif
rootkitXP.scr
strip-girl-2.0bdcom_patches.bat
strip-girl-2.0bdcom_patches.pif
strip-girl-2.0bdcom_patches.scr
winamp5.bat
winamp5.pif
winamp5.scr

De esta forma otros usuarios de KaZaa pueden descargar el virus.

Tiene la capacidad de abrir puertas traseras que permitirían a un usuario remoto controlar el computador atacado, dependiendo de la configuración de la red y del sistema operativo que emplee. La versión original del virus fue programada para realizar ataques de denegación de servicio contra www.sco.com entre el 1 al 12 de febrero. A partir de esta fecha terminó su actividad con la excepción del troyano que abre la puerta trasera para el acceso remoto al computador; sin embargo, nuevas versiones de virus continúan apareciendo, por lo que no es posible bajar la guardia, debiendo suponer que habrá nuevos ataques bajo formas parecidas. De hecho, una versión posterior fue destinada a saturar el acceso al sitio de Microsoft, razón por la cual esa empresa llegó a ofrecer US$ 250.000 por delatar a los creadores del gusano.

Dado que la fecha de cese no garantiza el fin de los ataques, hay que considerar los siguientes parámetros que permiten desconfiar de los mensajes recibidos:

Se autoenvía por correo electrónico en un mensaje con las siguientes características:

Asunto:
[caracteres sin sentido o vacío]
Delivery Notification: Delivery has failed
Error
hello
Hello
HELLO
hi
HI
Mail Delivery System
Mail Transaction Failed
Nicakhtwewby
Returned mail: User unknown
Server Report Status
test
Test

Undeliverable: Mail Delivery System
Undelivered Mail Returned to Sender

Adjuntos:
[caracteres sin sentido]
body
data
doc
document
file
message
readme
test
text
Las posibles extensiones del archivo **adjunto** son:
.pif
.scr
.zip

El cuerpo del mensaje puede ser alguno de los siguientes:
Mail Transaction Failed. Partial message is available.
The message contains Unicode characters and has been sent as a binary attachment.
The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

Consecuentemente, debería desconfiarse de aquellos mensajes que caigan dentro de estas clases. La mejor herramienta para evitar la entrada en los computadores de programas indeseables sigue siendo la prudencia al conectarse a Internet y abrir los mensajes recibidos. Ante una duda, es preferible perder unos minutos llamando al originador del mensaje que lamentar la pérdida de información valiosa para el usuario.

BIBLIOGRAFÍA

- http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100983
- http://www.enciclopediavirus.com/virus/vervirus.php?id=714&alerta=1

* * *

---

* Capitán de Corbeta. Oficial de Estado Mayor. Aviador Naval. Máster en Diseño y Comunicación Multimedia.