Gusanos que dañan el Sistema Operativo

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

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

En la actualidad, los códigos maliciosos poseen, en su mayoría, una clara intención por parte de sus creadores: ***obtener dinero****. Es así que gran parte del software dañino suele ser desarrollado con los objetivos de robar información o crear/ampliar redes botnets. Sin embargo, aún existen códigos maliciosos que poseen fines meramente dañinos, es decir, cuyo único fin es comprometer el buen funcionamiento y rendimiento del equipo afectado.*

Win32/VB: el gusano

Los códigos maliciosos detectados por ESET NOD32 como *Win32/VB.[variante] gusano*, refieren a una familia de malware desarrollada en el lenguaje de programación Visual Basic. Tal es el caso del gusano *Win32/VB.NJU*. Ésta y otras variantes de la familia -como *Win32/VB.NSF* y *Win32/VB.OIY*, son una serie de gusanos que modifican los archivos del sistema, reemplazando archivos benignos por el archivo dañino -que utiliza el mismo nombre- y ocultando los archivos originales.

Estas variantes poseen la capacidad de evitar que el usuario encuentre sus archivos originales, lo cual repercute directamente sobre el tiempo de uso del equipo para concretar una acción determinada. Por ejemplo, luego de la infección con la variante *Win32/VB.NJU*, un usuario observará su unidad C: como se presenta en la siguiente imagen:

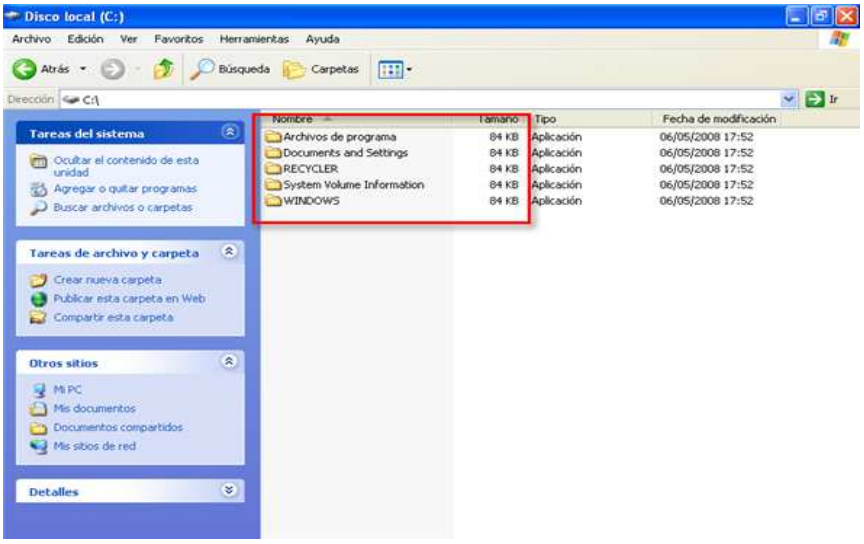

Imagen 1 – Sistema infectado con Win32/VB.NJU

Al acceder a la unidad C: el usuario verá carpetas que simulan ser las originales cuando en realidad éstas se encuentran ocultas. De este modo, aquellas que parecen ser las carpetas originales, son en realidad copias del gusano. En este sentido, resulta de interés dar cuenta de que todas las carpetas tienen el mismo peso (84 KB), lo cual debería llamar la atención del usuario.

Aclaración: existen casos similares con otras variantes, en tanto éstas realizan los mismos cambios pero, en lugar de hacerlo con carpetas, modifican, por ejemplo, todos los archivos de Word del sistema operativo o todos los archivos de "Mis Documentos", entre otros.

Luego de ocultar los archivos originales y crear copias del malware, el gusano modifica las siguientes entradas del registro:

- No mostrar archivos ocultos:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
- Ocultar las extensiones de los archivos:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt

Aclaración: el registro es una base de datos que poseen todos los sistemas operativos de Microsoft Windows, donde se almacena la configuración general del sistema y las aplicaciones instaladas. Desde el editor de registro (una interfaz gráfica), se lo puede manipular y realizar diversas configuraciones del sistema operativo.

Una vez que se han realizado estos cambios en el sistema, el usuario observará las carpetas que contienen la amenaza, como si fuesen las originales, previas al momento de infección del equipo. Si se modifican las entradas del registro antes mencionadas, volviendo a la versión original, se verá con claridad cuáles fueron las acciones de ataque realizadas al sistema:

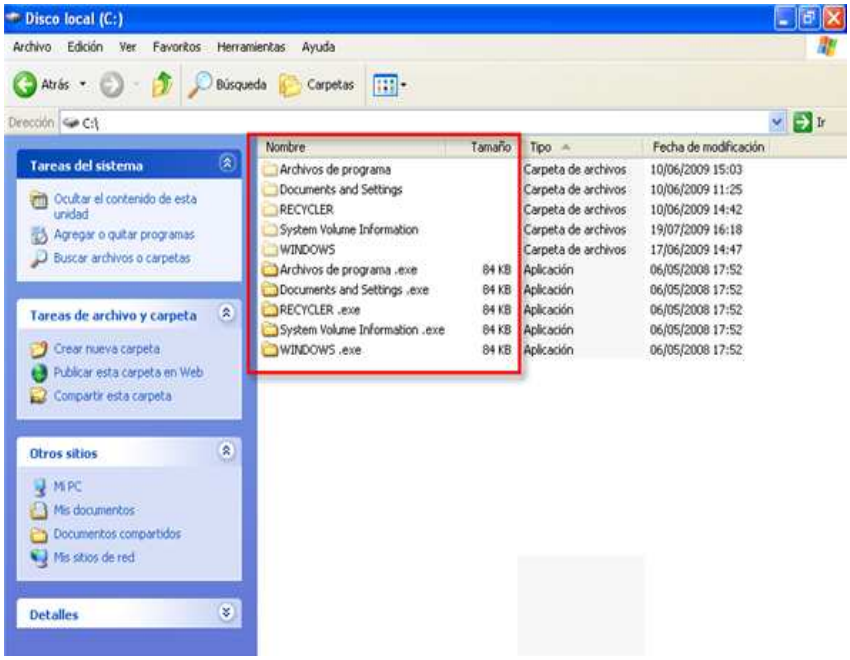

Imagen 2 - Sistema infectado con Win32/VB.NJU

En la imagen, se observa que las carpetas originales fueron ocultadas y se colocaron archivos de extensión EXE con el mismo nombre.

Sin embargo, como ya se mencionó, para visualizar estos cambios es necesario modificar el registro. Al respecto, es importante aclarar que un usuario que se infecta con una variante de esta familia no podrá, en caso de que lo desee, modificar el registro a través de su interfaz gráfica.

Esto se debe a que, además de los cambios mencionados, se realizan gran cantidad de modificaciones en el sistema operativo con el objetivo de dificultar la tarea de recuperación en los sistemas infectados. Este tipo de acciones son frecuentes en diversos códigos maliciosos. A continuación se enlistan los cambios más significativos que afectan al usuario en el sistema infectado.

Modificaciones al sistema

Tras realizar las acciones maliciosas principales (ocultar archivos o carpetas y crear copias del gusano), este código malicioso modifica el sistema para evitar la recuperación de los archivos originales. A continuación, se explica este proceso a partir de imágenes incluyéndose además, el detalle de la clave de registro que ha sido modificada para concretar esta acción:

1. Elimina la posibilidad de ver las opciones de configuración de las carpetas en el menú Herramientas. La recuperación de los archivos que se han ocultado se dificulta en este caso, debido a que posibilita la modificación, en forma gráfica, de las configuraciones de archivos ocultos y extensiones de archivos:

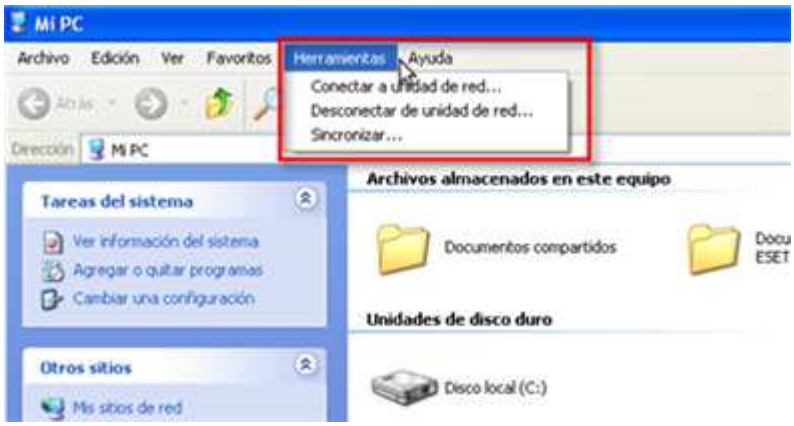

Imagen 3 – Eliminación de opciones de herramientas

La clave modificada fue:
KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\explorer\NoFolderOptions

2. Deshabilita el acceso a la administración gráfica del registro. Este paso es fundamental ya que dificulta la restauración del resto de las modificaciones para aquellos usuarios sin conocimientos de otras vías de editar el registro.

Imagen 4 – Bloqueo de edición del registro

La clave modificada fue:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools

3. Deshabilita el administrador de tareas. Esto impide visualizar los procesos en ejecución y también dificulta la detección del gusano.

Imagen 5 – Bloqueo del Administrador de Tareas

La clave modificada fue:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskmgr

4. Deshabilita la opción “Restaurar el sistema”. De esta forma, el usuario no podrá volver a un estado anterior del sistema sin infectar.

Imagen 6 – Bloqueo de Restaurar Sistema

La clave modificada fue:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\DisableSR

5. Deshabilita la línea de comandos (*cmd.exe*). Algunos usuarios más experimentados, podrán modificar el registro desde esta aplicación, ejecutando ciertos comandos y sin necesidad de ingresar a la interfaz gráfica de edición del registro. Para estos usuarios, también se impide la restauración del registro.

Imagen 7 – Bloqueo de linea de comandos

La clave modificada fue:
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\DisableCMD

6. Deshabilita la administración de usuario en el Panel de Control. De esta forma, el usuario no podrá crear otra cuenta administrativa en el sistema.

Imagen 8 – Bloqueo de Cuentas de Usuario en Panel de Control

La clave modificada fue:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowCpl

Conclusión

Como se puede observar, esta familia de gusanos es realmente dañina, debido a que recupera una funcionalidad que se encuentra en disminución en el malware actual: la capacidad de realizar acciones destructivas del sistema. Así entonces, los códigos maliciosos como los de la familia *Win32/VB* resultan de alto impacto en la usabilidad y rendimiento diario del sistema, afectando directa y automáticamente la disponibilidad de archivos o carpetas de uso cotidiano.

Ante la aparición de este tipo de archivos dañinos, queda claro que, aunque en disminución, todavía existen desarrolladores de códigos maliciosos con intenciones meramente dañinas.

Frente a este panorama, **la prevención** es fundamental y, en este sentido, la mejor herramienta para la protección contra diversos ataques informáticos es combinar una efectiva solución de seguridad con capacidades proactivas, como ESET NOD32 Antivirus o ESET Smart Security, junto con información y capacitaciones para los usuarios sobre las últimas tendencias en seguridad informática.

***Importante**: la manipulación del registro de Windows debe ser realizada por usuarios con conocimientos del mismo, ya que su incorrecta modificación puede afectar la funcionalidad del sistema operativo.*

Más información

ESET Latinoamérica
http://www.eset-la.com
Plataforma Educativa de ESET Latinoamérica
http://edu.eset-la.com
Blog de Laboratorio de ESET Latinoamérica
http://blogs.eset-la.com/laboratorio