.Seguridad
Cultura de prevención para TI
Publicado en *Revista .Seguridad* (http://revista.seguridad.unam.mx)

Ghost: Honeypot para malware que se propaga a través de dispositivos USB - Parte I

Por *Jonathan Banfi Vázquez*

- numero-26 [1]
- USB [2]
- ghost [3]
- honeypot [4]
- malware [5]

Se mostrará la captura de malware que se propaga a través de dispositivos de almacenamiento USB con el honeypot Ghost en un entorno virtual controlado. Esta primera entrega se enfoca en conocer e implementar Ghost en los sistemas operativos Windows para los que fue diseñado.

En la actualidad existen varios métodos de propagación e infección por software malicioso en los diversos sistemas operativos, por lo que es de vital importancia su detección y análisis para desarrollar contramedidas. Uno de los métodos más utilizados en los sistemas Windows, por su rapidez y por llegar incluso a equipos de cómputo críticos que no están conectados a alguna red [6], es mediante dispositivos de almacenamiento USB.

La propagación inicia cuando el usuario introduce un dispositivo en la computadora infectada, el software malicioso que se está ejecutando en esa máquina detecta que se ha conectado una unidad extraíble y realiza una copia de sí mismo, cambia los atributos de todos los archivos a *ocultos* y *del sistema*, mostrando al usuario únicamente los accesos directos a su información. La infección se lleva a cabo cuando ese dispositivo de almacenamiento es conectado en otra computadora y el usuario intenta acceder a sus archivos a través de los accesos directos diseñados para abrir tanto el archivo o carpeta como el software malicioso, en ese momento el equipo queda comprometido y listo para seguir infectando los dispositivos de almacenamiento que se conecten.

A continuación se describen las tres formas de propagación más comunes registradas por UNAM-CERT:

- **Modificación del archivo Autorun.inf** [7]**:** si no existe el archivo de configuración en el dispositivo USB, el software malicioso que reside en la computadora infectada puede generar uno nuevo con la ruta donde se replicó; dicho archivo contiene la instrucción para ejecutar el *malware* en cuanto el usuario conecte el dispositivo extraíble a otro equipo de cómputo que tenga habilitada la función de "Reproducción automática".
- **Creación de varios accesos directos** [8]**:** se ocultan todos los archivos y carpetas en su ubicación predeterminada para después generar accesos directos que apuntan hacia cada archivo o carpeta (pueden generarse únicamente en la raíz del dispositivo o de manera recursiva en las subcarpetas) y también hacia el software malicioso que se copió a sí mismo, una vez que el usuario da doble clic sobre cualquier acceso directo malicioso. De esta forma, además de abrir el archivo o carpeta, se ejecuta el *malware* y se infecta la computadora.
- **Creación de un sólo acceso directo:** el software malicioso crea una carpeta oculta (a la cual mueve todo el contenido) cuyo nombre es el valor hexadecimal "0A", que corresponde al salto de línea ("\n"), por lo que gráficamente pareciera que el directorio no tiene nombre. El acceso directo contiene la sentencia para abrir la carpeta oculta y ejecutar la supuesta réplica del *malware*, es decir, es una DLL que cambia el nombre de la función interna y parte de su estructura cada vez que se propaga.

El objetivo de este artículo es mostrar, precisamente, la captura de este tipo de *malware* con el *honeypot* Ghost en un entorno virtual controlado, ya que la mayoría de los *honeypots* existentes se enfocan en la detección y captura de amenazas que se propagan a través de la red [9]. A lo largo de dos publicaciones se describirá todo lo necesario para instalar y configurar Ghost de manera que nos permita implementarlo en nuestro laboratorio de análisis de *malware*, de esta forma se podrán detectar las amenazas que se propagan a través de unidades extraíbles y recolectar los archivos de configuración y réplicas que se generen para su posterior análisis; se obtendrá un mejor entendimiento del *malware* y datos que permitan crear inteligencia sobre nuevos vectores de infección y propagación.

Esta primera entrega se enfoca en conocer e implementar Ghost en los sistemas operativos Windows para los que fue diseñado. En la siguiente edición se abordará la configuración de la herramienta, la captura y el análisis del *malware* que se propaga a través de dispositivos USB.

Requerimientos de software

Máquinas virtuales	***Honeypots***
Windows 7 y XP	Ghost [10]

Ghost

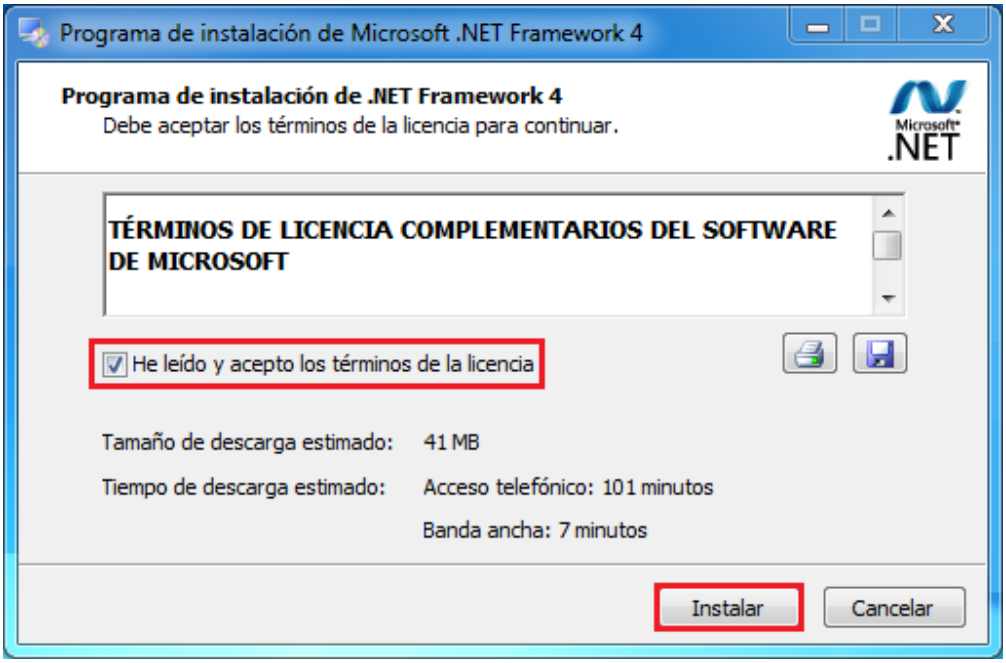
Es un *honeypot* que emula uno o varios dispositivos USB y fue diseñado para detectar, en análisis dinámico, software malicioso que se propaga a través de estos medios de almacenamiento, siempre y cuando el *malware* no realice una detección minuciosa en las características de software y hardware del laboratorio de análisis (y así identifique el dispositivo falso). Fue desarrollado en un principio por Sebastian Poeplau [11] para una tesis de licenciatura en la Universidad Bonn en Alemania, en la actualidad se continúa el desarrollo dentro del Proyecto Honeynet [12].

Implementación

Ghost [13]es compatible con los sistemas operativos Windows XP y Windows 7 de 32 bits, lo cual es conveniente debido a que muchas *sandbox* utilizan estos sistemas operativos como clientes para automatizar los análisis de *malware*. A continuación se mostrará una forma de instalar el *honeypot* en Windows 7 haciendo las respectivas observaciones en los pasos adicionales que se requieren para Windows XP:

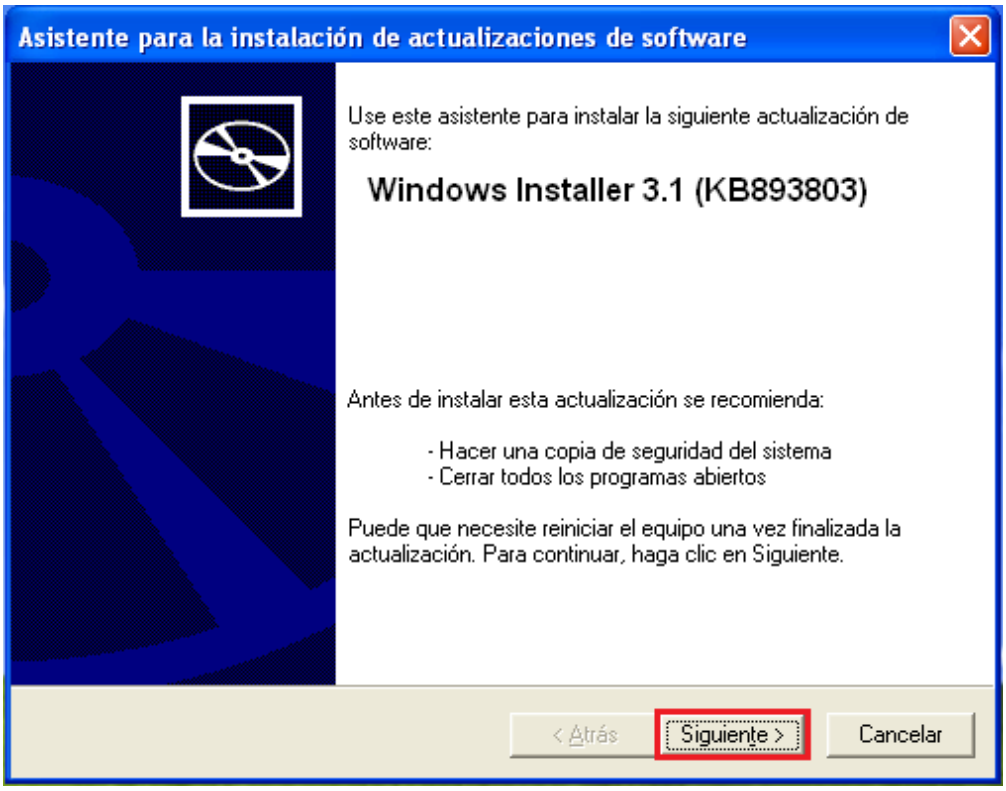
1) Instalar .NET Framework 4

Se requiere esta versión de *framework* [14] o superior en caso de utilizar Ghost desde la interfaz gráfica.

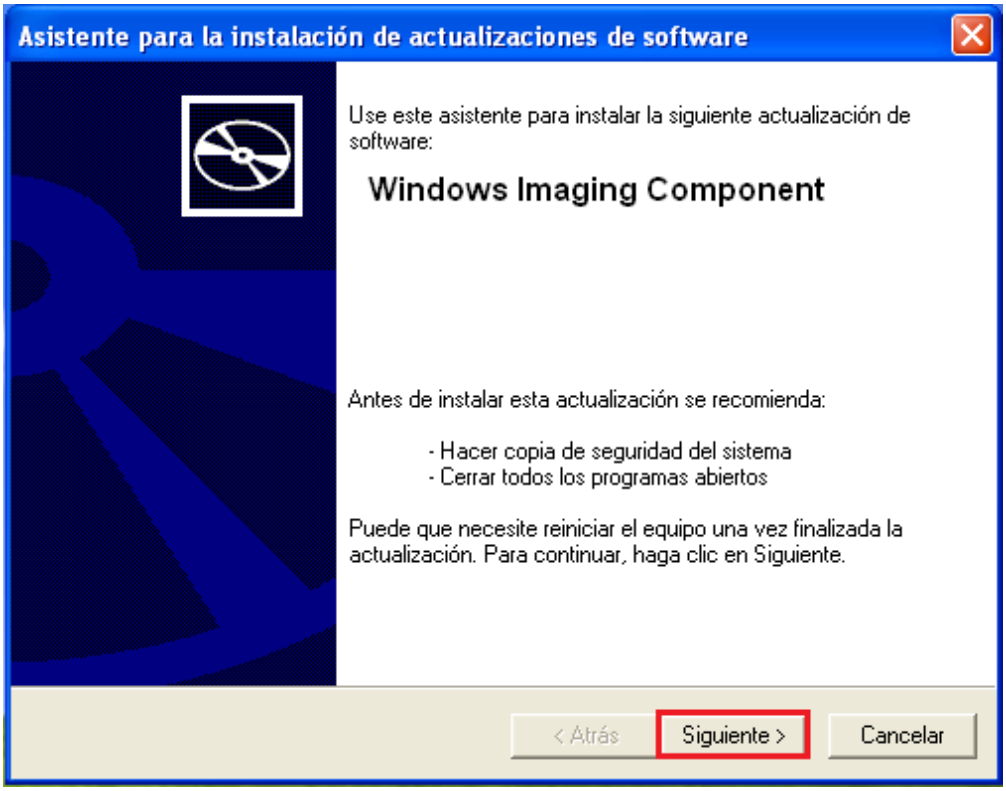


- En Windows XP, antes de instalar el *framework* se requiere:

a) Windows Installer 3.1 [15]



b) Windows Imaging Component [16]

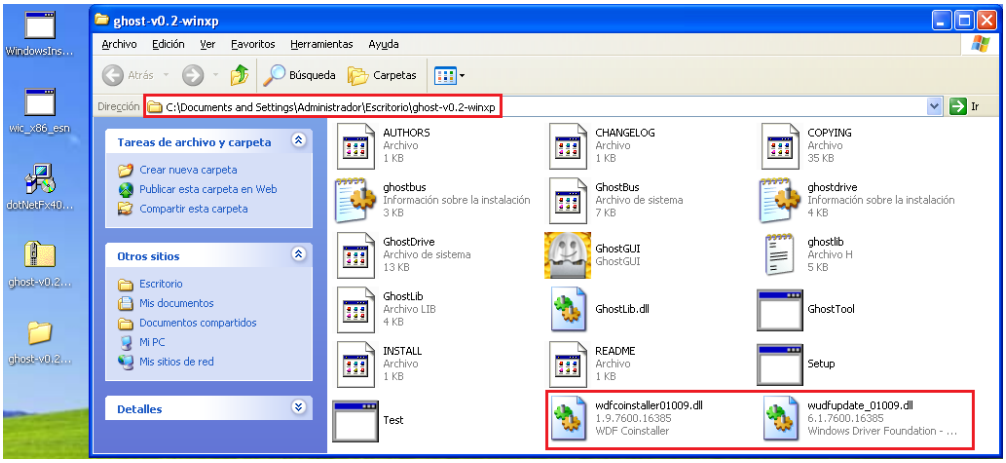


c) Colocar las siguientes dos DLL en la carpeta principal de ghost-v0.2-winxp.zip:

- wdfcoinstaller01009.dll (sha1: b0ba0de22ade0ee5324eaa82e179f41d2c67b63e) [17]

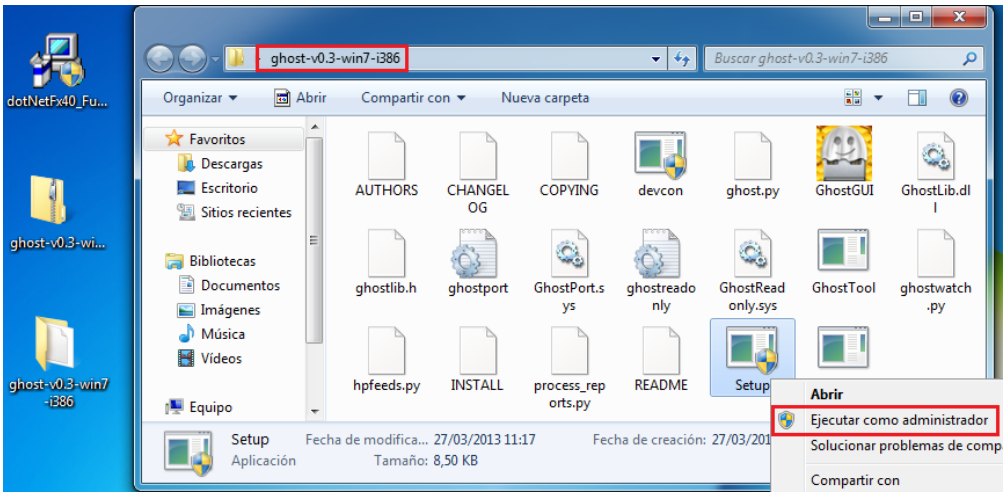
- wudfupdate_01009.dll (sha1: d9688d1849a86dd209732529375c6ada272ff8fd) [18]

La configuración anterior se requiere porque Ghost necesita Windows Drive Framework (WDF [19]), en Windows 7 no es necesario este paso ya que incluye la versión 1.9 [20].

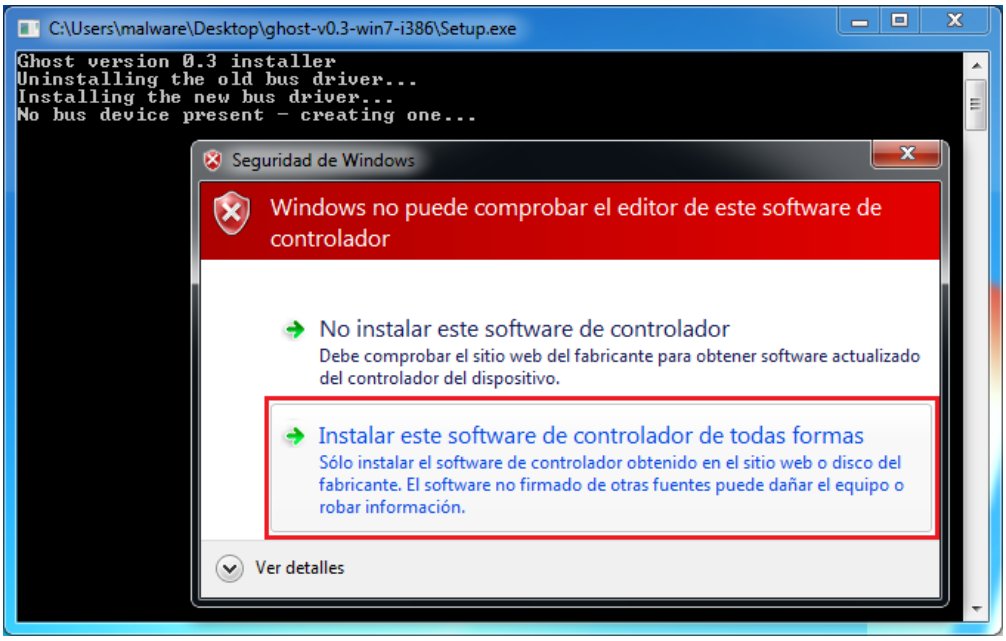


2) Instalar Ghost

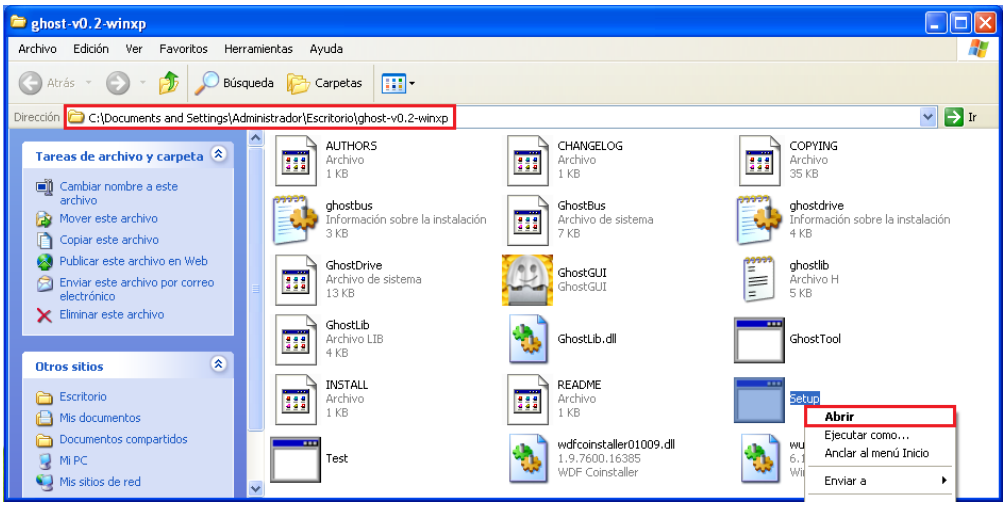
Descargar y descomprimir el archivo "ghost-v0.3-win7-i386.zip" [Archivo .zip [21]], posteriormente ejecutar "Setup.exe".



El sistema operativo preguntará si realmente se quieren instalar los controladores no firmados de Ghost debido a que Microsoft no puede comprobar el software del controlador, hacemos caso omiso y continuamos con la instalación.



- Para Windows XP se usa el archivo "ghost-v0.2-winxp.zip" [Archivo .zip [22]]

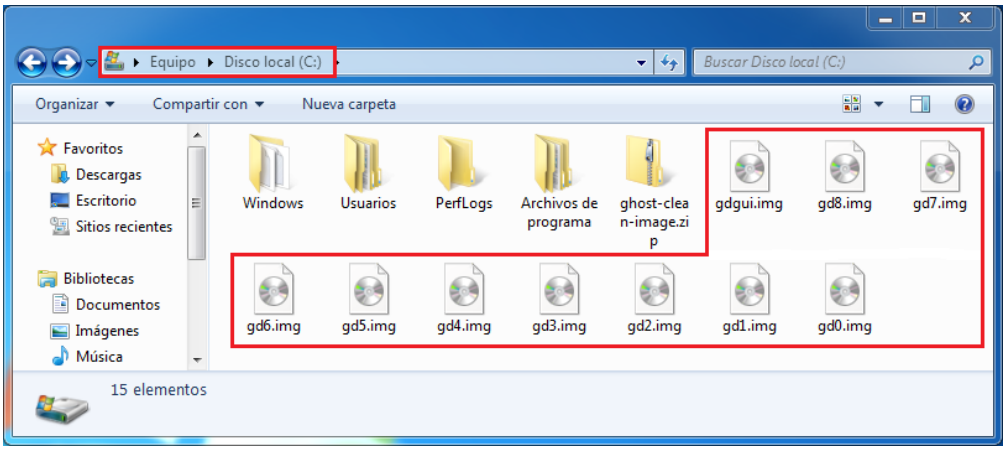


3) Colocar los archivos imagen en la unidad C:

Los dispositivos USB que emulará Ghost requieren archivos de imágenes limpias y con formato para que s e puedan almacenar tanto archivos legítimos (si es que se requieren) como aquellos generados por el *malware* . Las imágenes deben colocarse en la ruta predeterminada "C:\", ya sea que se generen de forma manual o se utilice el archivo "ghost-clean-image.zip" [Archivo .zip [23]] perteneciente al desarrollo de Ghost.

Una vez extraído el archivo "gdgui.img", se debe copiar tantas veces como dispositivos se requieran y deben renombrarse de la siguiente manera, dependiendo cómo se van a montar en el equipo:

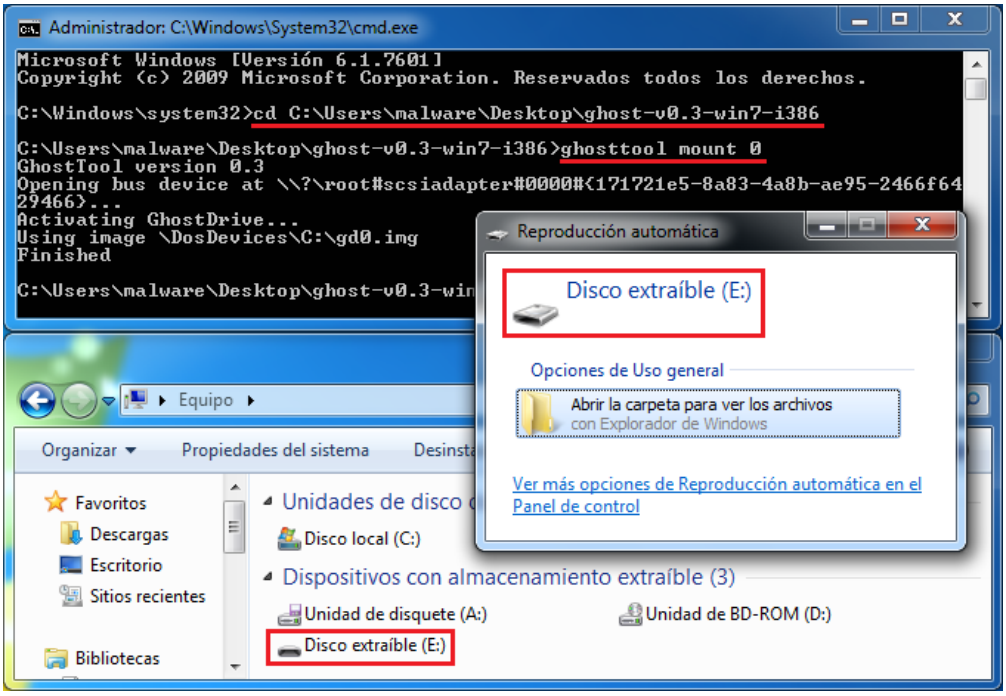
- Desde la interfaz de línea de comandos: "gd0.img" hasta "gd8.img"
- Desde la interfaz gráfica de usuario: "gdgui.img"



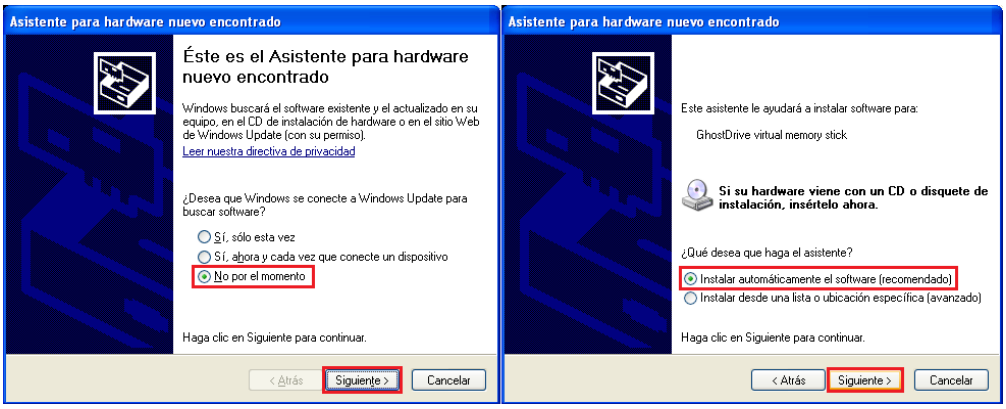
4) Configurar dispositivos desde la interfaz de línea de comandos

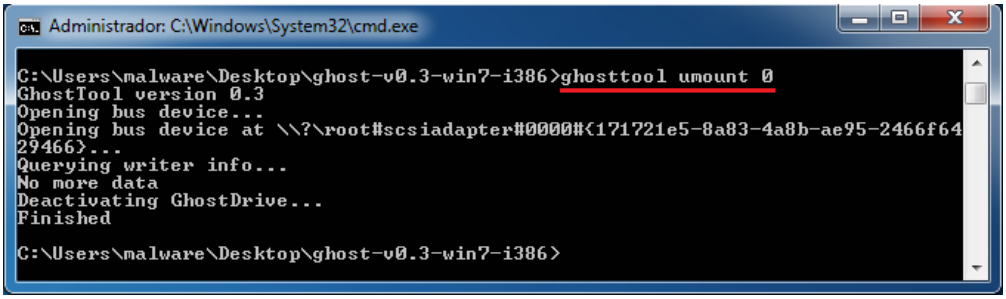
Abrir el "cmd.exe" con permisos de administrador, montar cada uno de los dispositivos "gd[0-8].img" para probar su correcto funcionamiento y finalmente desmontarlos. A continuación se muestran los comandos para el dispositivo "dg0.img":

- ghosttool mount 0
- ghosttool unmount 0



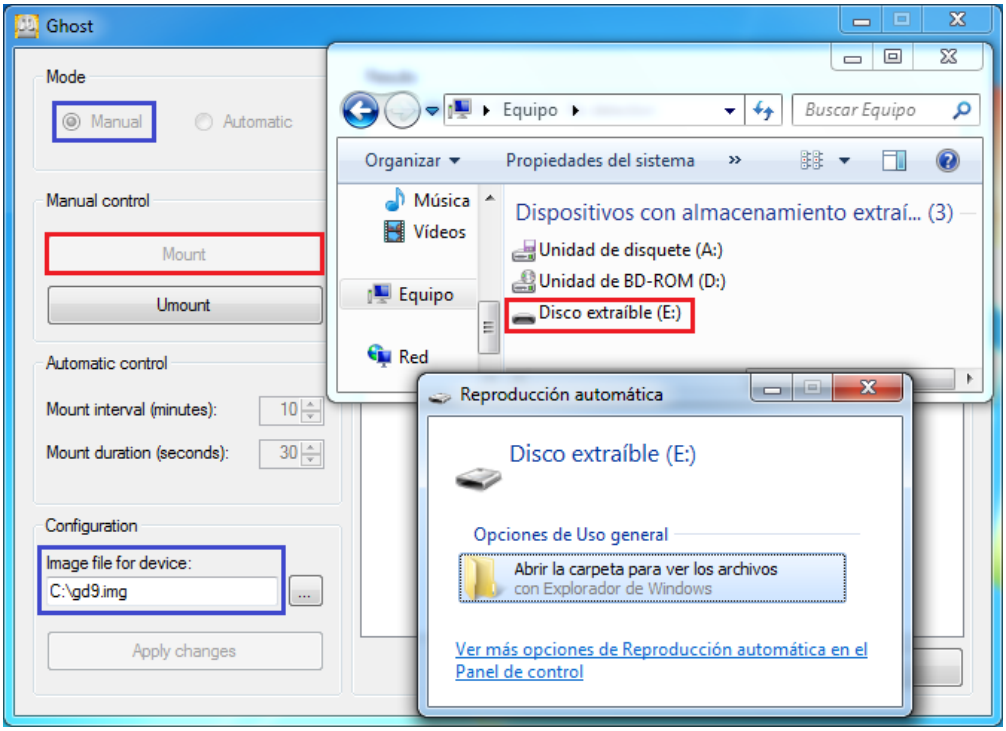
Nota: En Windows XP se abrirá automáticamente el "Asistente para hardware nuevo encontrado", se debe seleccionar la opción "Instalar automáticamente el software (recomendado)". Este procedimiento se realizará para todos los dispositivos que hayamos creado.



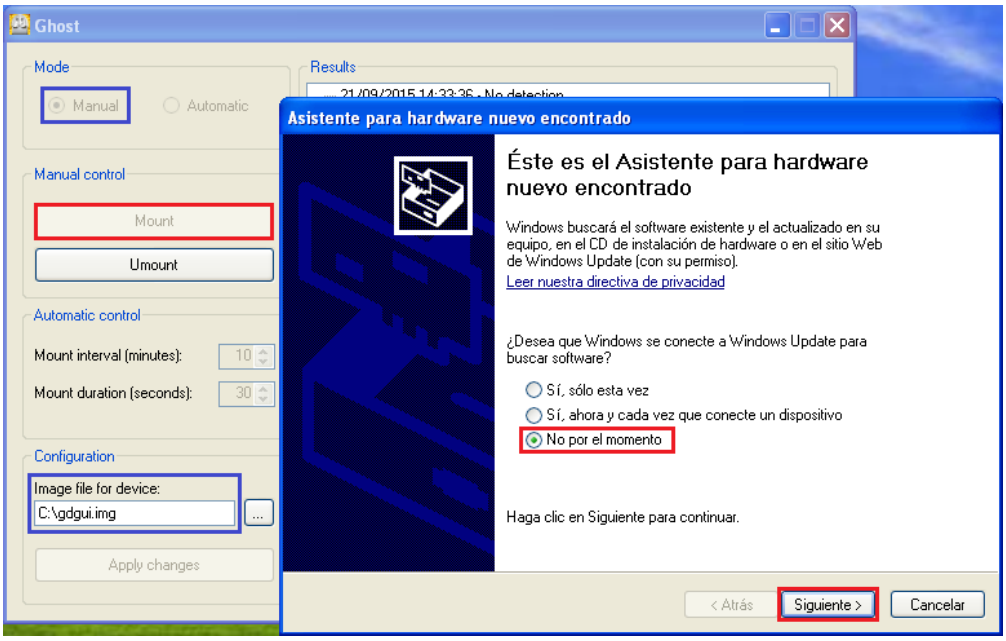


5) Configurar el dispositivo desde la interfaz gráfica de usuario

Abrir "GhostGUI.exe" con permisos de administrador, montar el dispositivo "gd9.img" para probar su correcto funcionamiento y finalmente desmontarlo. A continuación se muestra el modo manual:



Nota: En Windows XP se abrirá automáticamente el "Asistente para hardware nuevo encontrado" y debemos seleccionar la opción "Instalar automáticamente el software (recomendado)".



Finalmente, una vez que los dispositivos son emulados correctamente en el sistema operativo, se observarán como unidades de almacenamiento extraíble con capacidad de 100 MB aproximadamente.

Hasta este momento se mostró una forma de instalar Ghost en los sistemas operativos Windows XP y Windows 7, que son para los que se tiene soporte al día de hoy. Además, se habló de la importancia en la detecci ón oportuna por firmas antivirus de nuevas amenazas que no se propagan por red o que además utiliza n unidades de almacenamiento extraíble.

En la siguiente entrega se hablará del proceso de detección y del análisis de las muestras capturadas.

Si quieres saber más consulta:

- A Honeypot for Arbitrary Malware on USB Storage Devices: https://net.cs.uni-bonn.de/fileadmin/user_upload/gassen/USB_honeypot.pdf [24]
- Interview with Project Leader Sebastian Poeplau: http://resources.infosecinstitute.com/ghost-usb-honeypot/ [25]
- Countering the removable device threat with USB honeypots: https://www.youtube.com/watch?v=9G9oo3b9qR4 [26]

Jonathan Banfi Vázquez [27]

- numero-26
- USB
- ghost
- honeypot
- malware

SSI / UNAMCERT

URL del envío: http://revista.seguridad.unam.mx/numero26/ghost-honeypot-para-malware-que-se-propaga-trav-s-de-dispositivos-usb-parte-i

Enlaces:
[1] http://revista.seguridad.unam.mx/category/revistas/numero26
[2] http://revista.seguridad.unam.mx/category/tipo-de-articulo/usb
[3] http://revista.seguridad.unam.mx/category/tipo-de-articulo/ghost
[4] http://revista.seguridad.unam.mx/category/tipo-de-articulo/honeypot
[5] http://revista.seguridad.unam.mx/category/tipo-de-articulo/malware
[6] http://revista.seguridad.unam.mx/numero-19/sistemas-scada-algunas-recomendaciones-de-seguridad-parte-ii
[7] http://malware.unam.mx/node/54
[8] http://malware.unam.mx/es/content/c%C3%B3digo-malicioso-en-vbscript-se-propaga-por-medio-de-dispositivos-usb
[9] http://revista.seguridad.unam.mx/numero24/poc-captura-de-malware-con-el-honeypot-dionaea-ii
[10] https://github.com/honeynet/ghost-usb-honeypot
[11] https://twitter.com/poeplau
[12] https://honeynet.org/
[13] https://code.google.com/p/ghost-usb-honeypot/downloads/list
[14] http://www.microsoft.com/es-mx/download/details.aspx?id=17851
[15] https://www.microsoft.com/es-mx/download/details.aspx?id=25
[16] https://www.microsoft.com/es-mx/download/details.aspx?id=32
[17] http://www.opendll.com/index.php?file-download=wdfcoinstaller01009.dll&arch=32bit&version=1.9.7600.16385
[18] http://es.originaldll.com/file/wudfupdate_01009.dll/7818.html
[19] https://msdn.microsoft.com/en-us/Library/Windows/Hardware/ff557565(v=vs.85).aspx
[20] https://msdn.microsoft.com/en-us/library/windows/hardware/ff544309(v=vs.85).aspx
[21] https://ghost-usb-honeypot.googlecode.com/files/ghost-v0.3-win7-i386.zip
[22] https://ghost-usb-honeypot.googlecode.com/files/ghost-v0.2-winxp.zip
[23] https://ghost-usb-honeypot.googlecode.com/files/ghost-clean-image.zip
[24] https://net.cs.uni-bonn.de/fileadmin/user_upload/gassen/USB_honeypot.pdf

[25] http://resources.infosecinstitute.com/ghost-usb-honeypot/
[26] https://www.youtube.com/watch?v=9G9oo3b9qR4
[27] http://revista.seguridad.unam.mx/autores/jonathan-banfi-v-zquez