

Virus, banqueros y ladrones

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

Fecha: Martes 26 de septiembre del 2006



Presentación

Cuando pensamos que podríamos ser robados, lo último que se nos ocurriría es un programa que “vigila” nuestras acciones a la espera que ingresemos nuestros datos confidenciales en alguna institución financiera, comercial y/o bancaria para aprovecharlos en fines delictivos.

Durante el desarrollo del presente se mostrará el accionar de un troyano generalmente denominado “banker”, detectado por Eset NOD32 bajo el nombre de Win32/Bancodor.AB, aunque puede ser llamado con otra denominación por el resto de las casas antivirus. El objetivo es informar sobre los peligros que representan este tipo de programas maliciosos para la privacidad de los usuarios.

Este malware llega por correo electrónico en mensajes de otras personas infectadas o bien en forma de spam. Generalmente invitan al usuario a descargar un archivo mediante diversas técnicas de engaño (Ingeniería Social).

Estos troyanos en particular tienen un objetivo bien definido, que podría suponerse por su nombre: pretenden obtener datos confidenciales de los usuarios para posteriormente enviarlos a personas que se dedican a utilizarlos, causando pérdidas, generalmente económicas, a los dueños de esos datos.

El funcionamiento es sencillo:

1. Se instala un programa (banker) en el sistema de cualquier usuario.
2. El programa monitorea todas las acciones del usuario sin que este se percate de nada extraño.
3. Si el usuario realiza algunas de las acciones previstas por el creador del malware, como puede ser ingresar a su home-banking, la información ingresada por el usuario es almacenada en archivos (texto, imagen o video).
4. Cada cierto tiempo el programa envía la información recolectada a su creador.
5. El delincuente utiliza los datos recibidos ocasionando fraudes, robos o cualquier otro fin delictivo imaginado.

El mensaje engañoso no necesariamente tiene que ver con acciones financieras y puede ser de cualquier tipo. El objetivo del mismo es simplemente engañar al usuario para que el mismo haga clic en el enlace proporcionado, descargando un archivo ejecutable.

Nota importante: para el desarrollo del artículo, y apuntando a las conclusiones que se desean extraer, se trabaja con un antivirus instalado, pero desactualizado que no detecta el ingreso del malware que se está probando. El objetivo es analizar como un sistema ya infectado es difícil de controlar y remarcar la importancia de defensas proactivas y actualizadas.

Etapa 1: El engaño

El usuario recibe un correo con una tarjeta postal, en donde puede verse claramente que el enlace apunta a un archivo ejecutable. Cuando el usuario presiona sobre el enlace, se descarga el archivo. Posteriormente si se desea ver la supuesta tarjeta el archivo será ejecutado en el sistema del usuario.

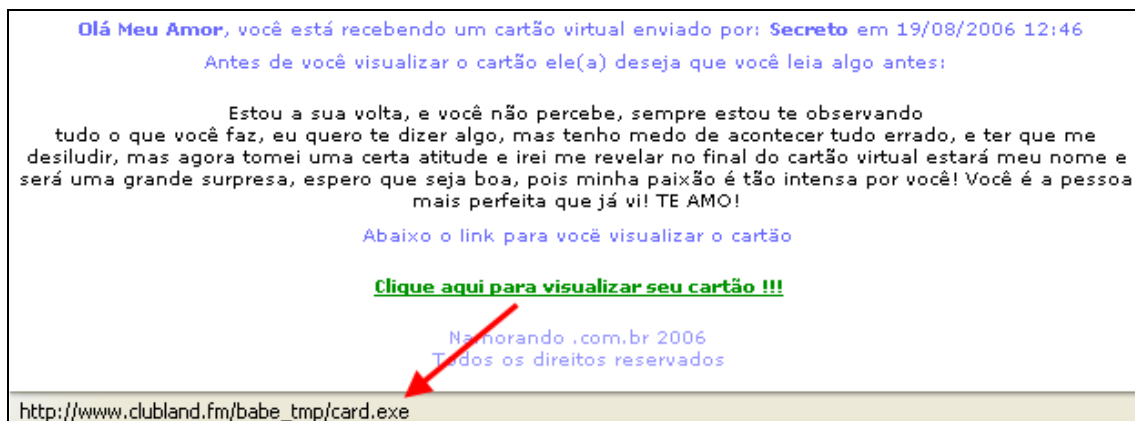


Imagen 1 – Mensaje de Correo para descargar el banker

Para seguir con el procedimiento, aquí se simula que el usuario descarga el archivo y lo almacena en su sistema para su visualización posterior.

Como ya se mencionó, el antivirus instalado permanece desactualizado y no detecta como amenaza el programa descargado.

Etapa 2: La ejecución

Cabe aclarar que el archivo descargado no es un virus, sino un troyano. La diferencia fundamental es que el objetivo del mismo no es propagarse por el sistema infectando otros archivos, sino engañar al usuario pretendiendo ser otro programa (en este caso una tarjeta virtual), permaneciendo oculto y “vigilando” las acciones del usuario.

Luego, se hace doble clic sobre el archivo y por supuesto, la tarjeta no aparece, aunque en algunos casos, y para completar el engaño, podría aparecer.

Aquí las acciones realizadas van a variar según el troyano con el que se esté tratando. En nuestro caso en particular se ven dos efectos visuales inmediatos:

1. Una pantalla negra que se abre y se cierra de inmediato (ejecución de un proceso en DOS).
2. Cierre inesperado de aplicaciones como el navegador FireFox y el Antivirus. Es decir que la poca protección que da el antivirus desactualizado, ahora tampoco existe.

Luego de ello, no se percibe ningún efecto indeseado y para el usuario todo puede pasar como un error temporal, e incluso que la tarjeta virtual no se ve como debería verse.

A continuación, se analizará con profundidad lo ocurrido:

1. El usuario hace doble clic y aparece una pantalla negra.

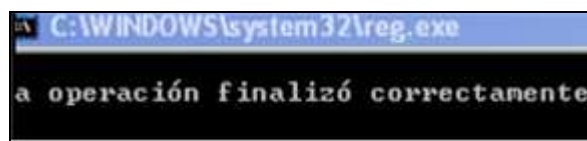


Imagen 2 – Proceso que modifica el registro

Como puede apreciarse en la barra de título, se ha ejecutado un programa llamado “reg.exe”. El mismo es utilizado para modificar el registro de Windows.

Un análisis pormenorizado de las modificaciones realizadas, arroja los siguientes resultados:

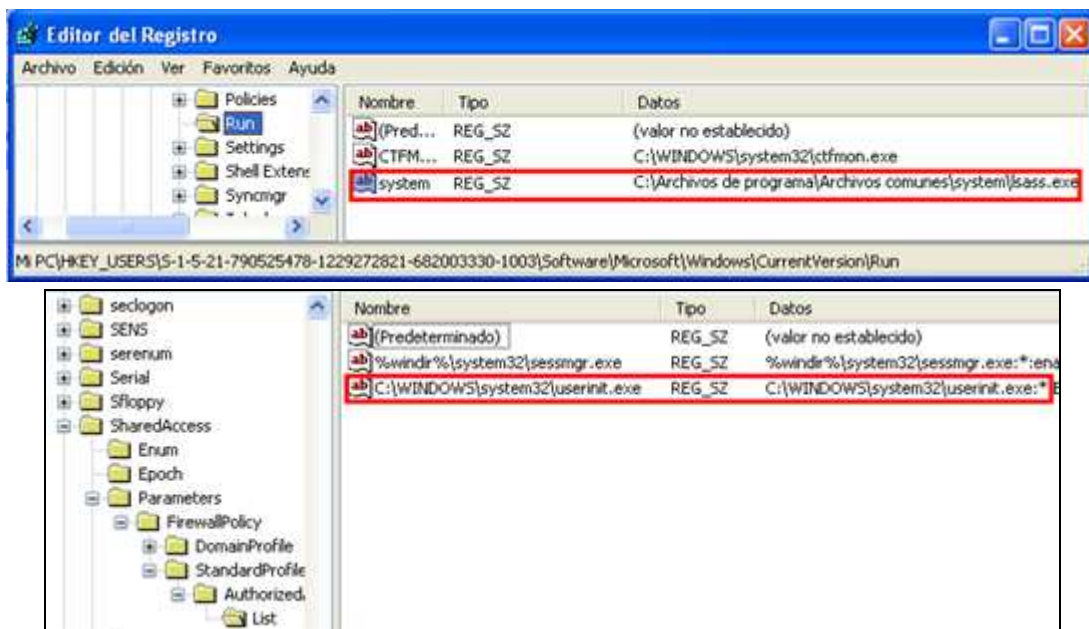


Imagen 3 – Modificaciones en el Registro de Windows

2. Se cierra FireFox y el antivirus instalado, esa vez y cada vez que se intente abrirlos. El objetivo de finalizar estos procesos es dejar Internet Explorer como único recurso de navegación web para el usuario, y que el troyano no sea detectado por programas de seguridad o antivirus.

Para confirmar esto, se puede ver la lista de procesos en funcionamiento antes y después de la ejecución del banker:

Nombre de imagen	N..	C	Uso de ...
VMwareService.exe	S...	0..	1.868 KB
nod32krn.exe	S...	0..	20.068 KB
firefox.exe	C...	0..	23.804 KB
ctfmon.exe	C...	0..	3.060 KB
nod32kui.exe	C...	0..	2.804 KB

Nombre de imagen	N..	C	Uso de ...
VMwareService.exe	S...	0..	1.868 KB
nod32krn.exe	S...	0..	20.068 KB
ctfmon.exe	C...	0..	3.060 KB

Imagen 4 – Lista de procesos

En la imagen se puede apreciar que fueron cerrados dos procesos pero no se observa otro programa extraño en ejecución. Esto es debido a que el troyano examinado oculta sus procesos de forma tal que no pueda ser encontrado fácilmente.

Etapa 3: El robo de información

La ejecución del archivo fue un poco sospechosa, pero todo sigue funcionando sin problemas en el sistema y a menos que se preste mucha atención, nada indicaría que puede estar siendo “observados” por un invitado indeseado.

Para continuar en la banca online se puede verificar que realmente el programa instalado realiza la grabación de los datos que el usuario ingresa, además de tomarse libertades como modificar los sitios webs que desea.

Estas acciones pueden visualizarse detalladamente en el siguiente video:

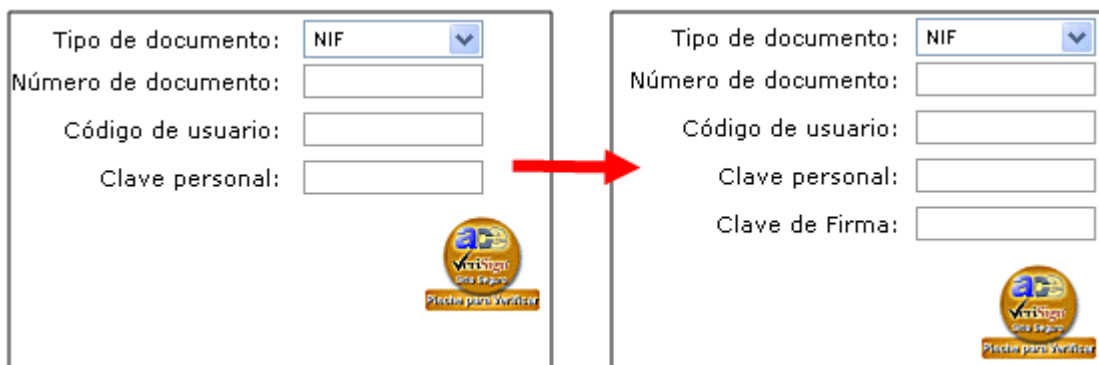
<http://www.nod32-la.com/link.php?i=27>

Es sabido que cualquiera puede ser engañado mediante el phishing, por lo que un usuario responsable con su dinero, seguirá todas las recomendaciones dadas normalmente para evitar este tipo de engaños:

1. No hacer clic en enlaces para ingresar a la banca online. Escribir la URL directamente en el navegador.
2. Verificar el candado en la parte inferior y que la página a la cual se ingresa comienza con https.
3. Verificar el certificado digital luego de ingresar al sitio.

Siguiendo este procedimiento, para esta demostración se toma www.banesto.es debido a que es una de las entidades afectadas por este troyano en particular. De todos modos, cabe aclarar que el banco afectado puede ser cualquiera y de cualquier nacionalidad.

En ambas oportunidades se tipeo la URL (www.banesto.es), se verifico que el home-banking de banesto comenzara con https, el candado y el certificado digital. Todo esto sobre Internet Explorer, ya que el troyano se encarga de cerrar cualquier otro programa de navegación que se intente utilizar.



The image displays two side-by-side screenshots of the Banesto login page. The left screenshot shows the login form with the following fields: 'Tipo de documento:' (dropdown menu set to 'NIF'), 'Número de documento:', 'Código de usuario:', and 'Clave personal:'. The right screenshot shows the same form but with an additional field for 'Clave de Firma:'. A red arrow points from the left screenshot to the right one, indicating the modification.

Imagen 5 – Modificación en el Ingreso de datos en el sitio de Banesto de España

En estas dos imágenes puede apreciarse la misma página web de banesto en un sistema sin infección y en un sistema afectado por el troyano.

Como puede verse en la segunda imagen, se incorpora un dato más. Si el usuario, generalmente apresurado por realizar sus tareas, no presta excesiva atención, sin duda ingresará esta última clave.

Entonces, ¿a qué se debe la diferencia en los sitios web?

Aquí cobra relevancia el dato que el malware cierra cualquier navegador excepto IE. Esto es debido que el troyano es capaz de interceptar las instancia de este navegador y modificar la página que se está mostrando al usuario para solicitar los datos que sean necesarios obtener (la clave en este caso).

Luego que el desprevenido usuario ingresa todos los datos solicitados, los mismos son almacenados por el troyano en un archivo y enviados al autor del mismo cada cierto tiempo.

Actualmente, la información obtenida puede ser grabada en archivos de texto, imágenes (mediante capturas de pantalla cada cierto tiempo) o en videos grabados por el troyano.

En conclusión, el usuario nunca sabrá como fue que sus datos confidenciales fueron obtenidos por el delincuente y como su cuenta bancaria llego a cero.

Etapa 4: Análisis post-mortem

Las pruebas anteriores fueron realizadas en caja negra (black-box) debido a que se realiza una acción sin conocer los resultados que pueden obtenerse. En base a lo que se observa se extraen resultados, algunos de los cuales ya fueron descritos.

A continuación un análisis más técnico nos proporciona información detallada del malware. El troyano analizado tiene las siguientes características:

- Nombre de detección: Win32/Bancodor.AB
- Fecha descubrimiento: abril de 2006
- Sistema operativos: Windows 2000, XP y 2003
- Empaquetador: UPX (Ultimate Packer for eXecutables)
- Tamaño empaquetado: 35 kb
- Tamaño desempaquetado: 120 kb

Para comenzar el análisis se averigua en empaquetado y se procede a desempaquetar el ejecutable.

Recordemos que el empaquetamiento es una acción que se puede realizar a cualquier ejecutable (aunque es mas normal en el malware) para cambiar su apariencia y comprimirlo en tamaño. Esto se realiza para ocultar el programa dañino de los antivirus tradicionales (al cambiar la apariencia) y para facilitar la distribución (al ser más pequeño).

Luego de analizar el código puede verse que el mismo graba los siguientes archivos, que permanecían empaquetados, en diferentes directorios:

- **programas\archivos comunes\system\lsass.exe** → utilizado para asegurarse su arranque. Se agrega al registro como se verá posteriormente.

- **sistema\winaupd.dll** → archivo propio del malware
- **sistema\lxvid.dll** → archivo inyectado en distintos procesos a monitorear
- **sistema\Un.b** → archivo encriptado con parámetros empleados por el troyano

Además, en distintas etapas, guarda archivos temporales que luego son eliminados:

- **c:\bkup.reg** → temporal al ejecutarse el programa
- **sistema\divx.ini** → log de las acciones realizadas e información robada

Nota: “sistema” es el directorio system32 del sistema que puede variar según el sistema operativo (`windows\system32` en Windows XP y 2003 o `winnt\system32` en Windows 2000). “Programas” es el directorio `C:\Archivo de Programas`, que puede variar según el idioma de instalación seleccionado para Windows.

Debido a la utilización de ciertas tecnologías de Rootkit este programa malicioso oculta su presencia ante el sistema y el usuario, como ya pudo verificarse al ver la lista de procesos activos.

Más allá de esto, los archivos mencionados pueden ser encontrados en el directorio del sistema:

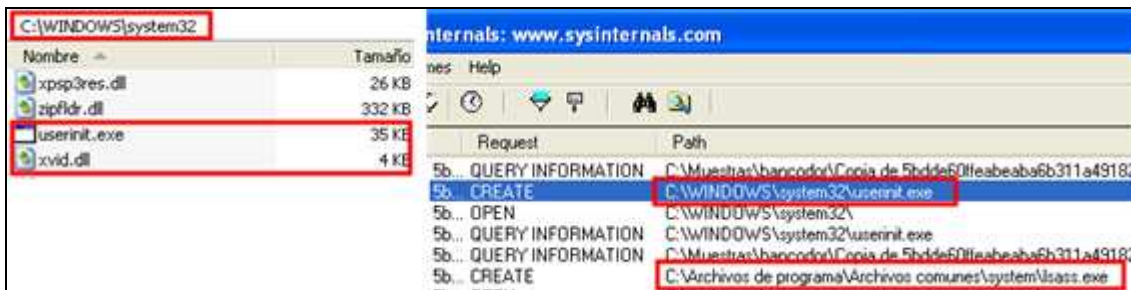


Imagen 6 – Archivos del banker

Con respecto a los archivos donde se registran las acciones y los parámetros se encuentra lo siguiente:

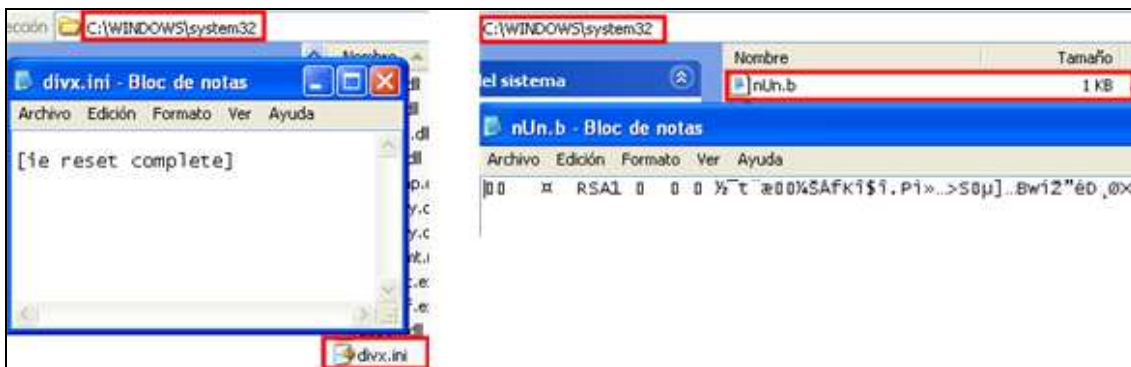


Imagen 7 – Contenidos de los archivos del banker

El primer archivo muestra las acciones realizadas por el troyano y el segundo los parámetros (encriptados) utilizados por el mismo.

Además, se modifican/elimina/agrega claves en el registro para asegurar su permanencia en el sistema y dificultar su hallazgo y remoción.

Algunas de modificaciones pudieron verse en las imágenes anteriores y otras que se agregan son las siguientes:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer]
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Search]
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AboutURLs]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main]
[HKEY_USERS\.Default\Software\Microsoft\Internet Explorer]
[HKEY_USERS\.Default\Software\Microsoft\Internet Explorer\Main]
[HKEY_USERS\.Default\Software\Microsoft\Internet Explorer\Search]
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser]
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\LocalUser\Software\Policies\Microsoft\Internet Explorer\Control Panel]
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
```

Por otro lado, las claves eliminadas son las siguientes:

```
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects]
[-HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs]
[-HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser]
```

Para asegurar su ejecución en el próximo arranque, el troyano modifica la sección del registro que es consultada por Windows al iniciar. Estas claves indican que programas deben ejecutarse al iniciar el sistema operativo.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run → Archivos de programa\Archivos Comunes\system\lsass.exe
```

Es importante remarcar que lsass.exe también es un archivo del sistema que se almacena en otra ubicación. Esta técnica de utilizar el mismo nombre que archivos del sistema es usada a menudo por el malware para confundir al usuario.

Luego de instalarse, el troyano procede a detener los procesos que pueden dificultar su trabajo (como FireFox) o pueden delatar su presencia (como los antivirus).

La lista de procesos es extensa:

WINLDR.AXE - NETSCAPE.EXE - OPERA.EXE - FIREFOX.EXE - MOZILLA.EXE - M00.EXE - WINTBPX.EXE - SWCHOST.EXE - SVOHOST.EXE - SVC.EXE - WINSOCK.EXE - SPOOLS.EXE - KERNELS32.EXE - mwfibpx.exe - nod32kui.exe - mcupdate.exe - mw1hel~1.exe - realsched.exe - tbon.exe - pucxyloo.exe - mouse32a.exe - winupdates.exe - backweb- - qttask.exe - mediagateway.exe - sox1.exe - shstat.exe - SpyAxe.exe - xcommsvr.exe - rwnt.exe - shost.exe - MouseElf.exe - aimexdll.exe - batserv2.exe - Elogerr.exe - sysc.exe - stopads.exe - istsvc.exe - uwx5.exe - dazzler.exe - secure.exe - spoolsv32.exe - ibm00001.exe - kernels64.exe - driver64.exe - paytime.exe - type32.exe - mediapipe.ex - adduz32.exe - itbill.exe - spysheriff.exe - apifl.exe - drsmartloadb.exe - gcasserv.exe - mpp2pl.exe - unspypc.exe - realsched.exe - isstart.exe - logitray.exe - wininstall.exe - statusclient.exe - mpcsvc.exe - backorif.exe - NopeZ.exe - usrprmt.exe - netnw.exe - hpbpsttp.exe - nvarem.exe - apifl.exe - UnSpyPC.exe

En ella se resaltan los siguientes:

- Navegadores: netscape.exe, opera.exe firefox.exe, mozilla.exe
- Programas de seguridad: svc.exe
- Otros malware: secure.exe, spoolsv32.exe, backorif.exe
- Antivirus: nod32kui.exe

Anteriormente se mencionó que el troyano utiliza técnicas de rootkit para ocultar sus procesos. Ejecutando un detector de rootkit puede apreciarse esta “calidad” del programa dañino, ocultarse y simular ser otro archivo del sistema:

Process	Parameters
System Idle	
System	
C:\WINDOWS\system32\cmd.exe	
C:\WINDOWS\System32\smss.exe	
C:\WINDOWS\System32\alg.exe	
C:\WINDOWS\system32\csrss.exe	ObjectDirectory=\Windows SharedSection
C:\WINDOWS\system32\winlogon.exe	
C:\WINDOWS\system32\services.exe	
C:\WINDOWS\system32\lsass.exe	
C:\WINDOWS\system32\svchost.exe	
C:\WINDOWS\system32\svchost.exe	
C:\WINDOWS\system32\svchost.exe	-k netsvcs
C:\Instala\gmer\gmer.exe	
C:\WINDOWS\system32\svchost.exe	-k NetworkService
C:\Archivos de programa\Archivos co...	C:\Muestras\bancoador\58DDE6*1.EXE
C:\WINDOWS\system32\svchost.exe	-k LocalService
C:\WINDOWS\Explorer.EXE	
<hr/>	
Name	S
C:\Archivos de programa\Archivos comunes\system\lsass.exe	0
C:\WINDOWS\system32\ntldr.dll	0
C:\WINDOWS\system32\kernel32.dll	0
C:\WINDOWS\system32\ADVAPI32.dll	0

Imagen 8 – Proceso oculto del banker

El efecto de reemplazo del formulario en la página web es perfectamente visible y puede apreciarse si se observa con atención. Nuevamente, este efecto, puede visualizarse en el segundo video ubicado en el siguiente enlace:

<http://www.nod32-la.com/link.php?i=28>

Una vez que el troyano almacena los datos se conecta cada cierto tiempo a un servidor en Internet y envía los datos obtenidos. El tráfico de red generado por el troyano se ve a continuación:

	Source	Destination	Protocol	Info
26	237.130	237.2	DNS	Standard query A realbrothers.net
39	237.130	237.2	DNS	Standard query A realbrothers.net
36	237.2	237.130	DNS	Standard query response, Server failure
79	237.130	237.2	DNS	Standard query A realbrothers.net, local cache
53	237.2	237.130	DNS	Standard query response
70	237.2	237.130	DNS	Standard query response, Server failure
29	237.2	237.130	DNS	Standard query response, Server failure

Imagen 9 – Conexiones realizadas por el banker

Este servidor actualmente se encuentra dado de baja por lo que las conexiones han fallado.

Conclusiones

El robo de información se ha convertido en el principal objetivo de los creadores de malware como lo demuestra los cientos de adware y espías detectados diariamente uno de cuales ha sido analizado anteriormente. Puede ver el informe del adware HotBar en el siguiente enlace:

<http://www.nod32-la.com/link.php?i=26>

A estos espías se ha unido una forma mas activa de robo como es el uso de los troyanos bancarios. Todo indica que esta tendencia seguirá en ascenso y que sus creadores seguirán perfeccionando sus técnicas de infección y ocultamiento para lograr sus propósitos delictivos.

La reciente aparición de un troyano con todas las características estudiadas y que además graba en video las acciones del usuario en sitios webs confirma esta tendencia de perfeccionamiento con fines maliciosos.

Es importante remarcar que el malware avanza continuamente y que viejos trucos son adecuados y relanzados en nuevas variantes de códigos dañinos por lo que estar protegido con software de detección proactiva que detecte comportamientos, además de por firmas, anómalos es fundamental.