

Guía básica para limpieza de malware de pharming

Este documento es una guía muy gráfica y sencilla con pasos fáciles para detectar y reparar infecciones por troyanos bancarios que realizan el ataque de pharming. Cada día surgen nuevos métodos para realizar este tipo de ataques por lo que es imposible estar 100% seguro.

PASOS:

1. Revisar archivo de HOSTS

Abrimos con notepad o cualquier editor de textos el archivo:

C:\WINDOWS\System32\Drivers\etc\hosts



En este caso el dominio está siendo redirigido a la dirección IP de un portal falso.

Las entradas que contenga referentes a bancos deberán ser borradas.

Es recomendable poner protección de escritura al archivo dando click derecho en el icono de hosts, seleccionando propiedades, marcando la casilla de solo lectura y seleccionando Aceptar.



Seleccionamos la casilla de Solo lectura.

2. Revisar direcciones IP del Banco

Por lo general los bancos no cambian las direcciones de sus servidores, al día de hoy 12/12/2007:

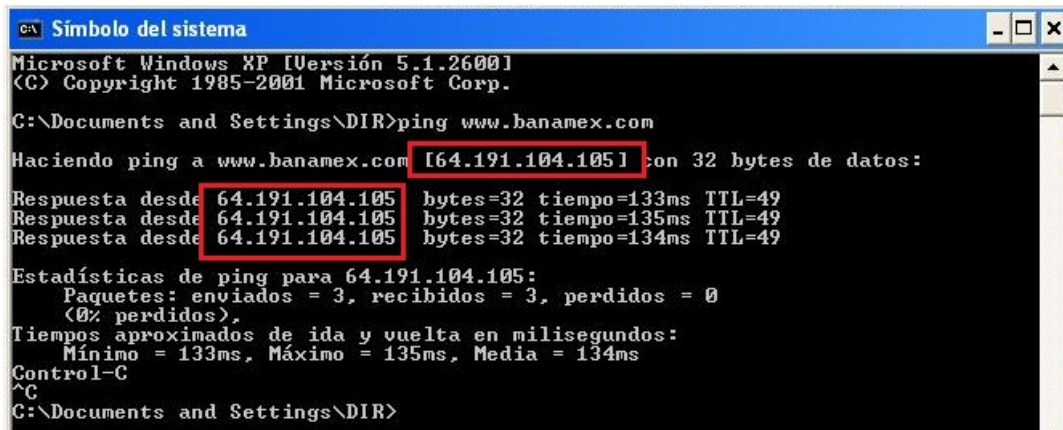
DOMINIO	IP	DESCRIPCION
www.banamex.com	192.193.230.100	Portal Banamex
bóveda.banamex.com.mx	192.193.229.115	Banamex Personas
www.bancanetempresarial.banamex.com.mx	192.193.205.100	Banamex Empresas
www.santander.com.mx	201.134.220.2	Portal Santander
enlace.santander-serfin.com	200.36.161.81	Enlace Santander
www.bancomer.com.mx	148.244.43.5	Portal Bancomer

Para verificar que nos estamos conectando a las direcciones reales, abrimos una ventana de CMD (Inicio, Ejecutar, escribimos cmd y seleccionamos Aceptar) y ejecutamos el siguiente comando:

C:\> ping www.banamex.com

Pinging www.banamex.com [192.193.230.100] with 32 bytes of data:

Las direcciones IP deben de ser las mencionadas anteriormente.



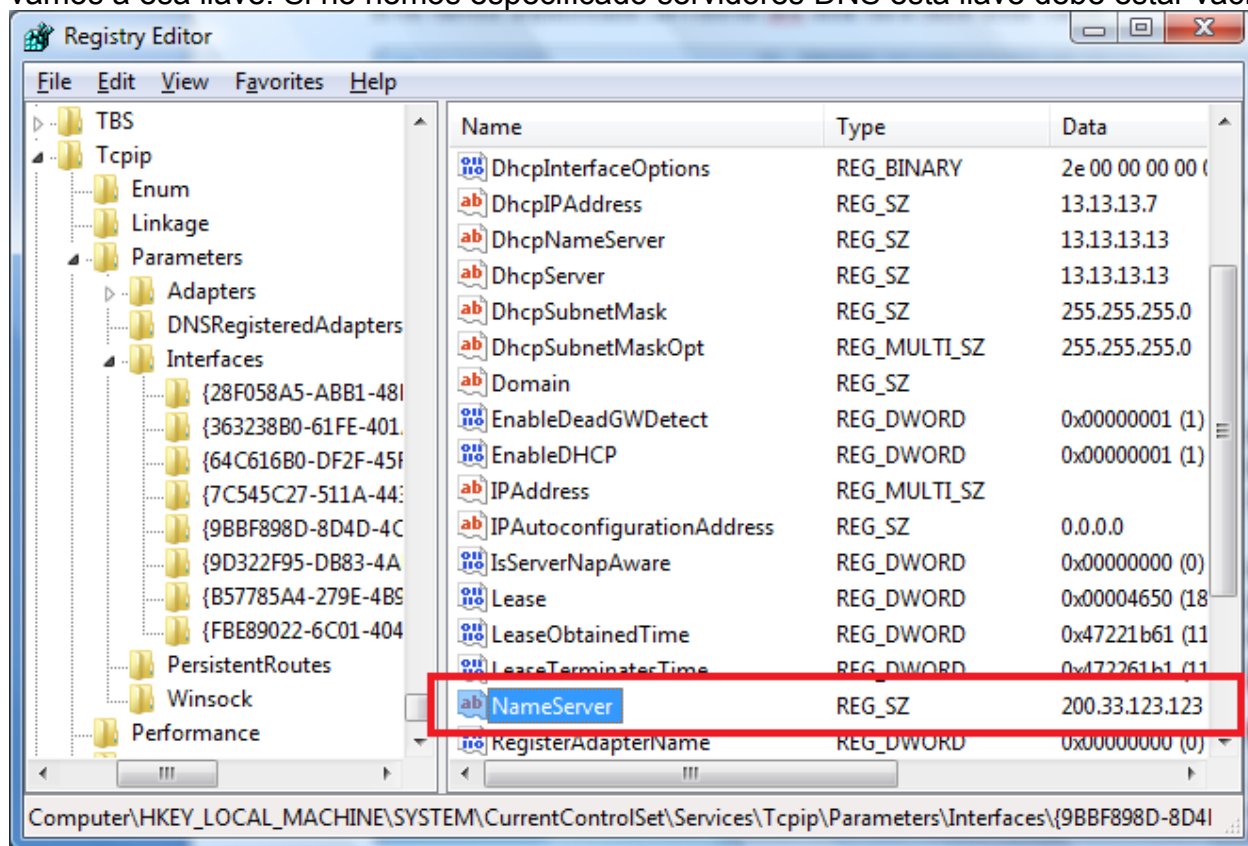
En esta imagen se muestra un ejemplo de un dominio apuntando a una dirección falsa.

3. Revisar servidores DNS de Windows

Existen llaves del registro donde se almacena la dirección de los servidores DNS como:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

Para revisar abrimos regedit (Inicio, Ejecutar, escribimos regedit y seleccionamos Aceptar) y vamos a esa llave. Si no hemos especificado servidores DNS esta llave debe estar vacía.



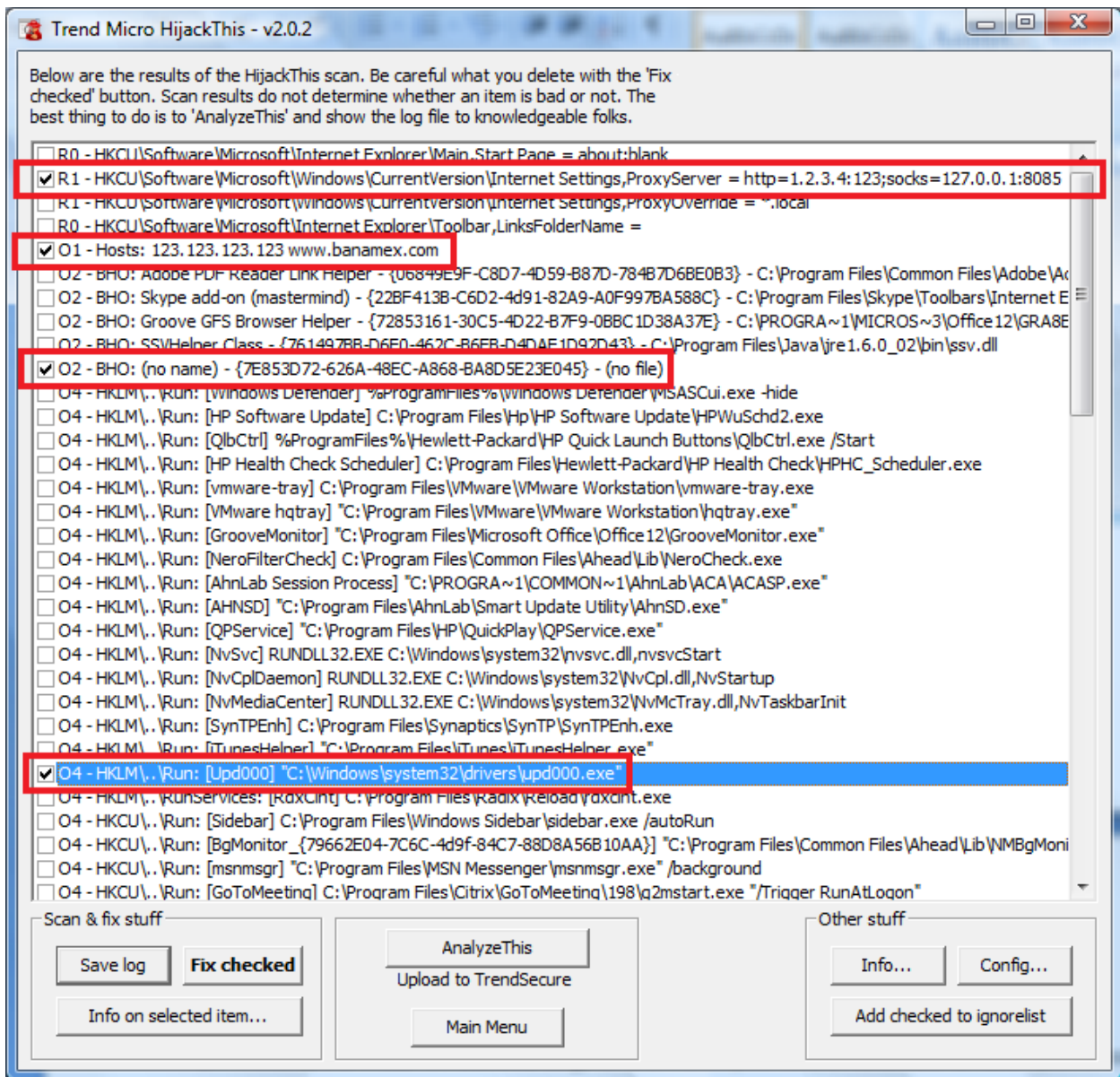
En este caso se está apuntando a un servidor DNS falso

Debemos borrar el contenido de esta llave y revisar las demás interfaces.{3632...}

Y otras llaves donde se almacena el Proxy del Internet Explorer:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Para verificar las llaves del registro y otras configuraciones que puedan estar redirigiendo a servidores falsos se puede usar el programa HiJackThis <http://www.trendsecure.com/portal/en-US/download/HiJackThis.exe>



- R1 – Indica que se está usando un servidor proxy en Internet Explorer
- O1 – Indica que existe una entrada falsa en el archivo HOSTS
- O2– Indica un plugin del navegador sospechoso
- O4– Indica que al iniciar Windows se carga un archivo sospechoso, en este caso llamado upd000.exe
- O17– Indica que hay un NameServer especificado en el registro.

Después de seleccionar las entradas a eliminar se da click en **Fix checked**

4. Revisar servidores DNS del ruteador

Un ataque reciente permite cambiar configuraciones de los ruteadores de Prodigy aunque tengan contraseña de sistema, para revisar el posible envenenamiento del DNS del ruteador es necesario acceder a la página de configuración del DNS:

<http://192.168.2.254/xslt?PAGE=J38>

<http://gateway.2wire.net/xslt?PAGE=J38>

<http://home/xslt?PAGE=J38>

Si pide contraseña y no se la hemos asignado nosotros es probable que sea **admin**.

Nombre DNS	Dirección IP	Tipo de entrada
www.banamex.com	123.123.123.123	Agregada por el usuario

En esta imagen se muestra un registro en la tabla de DNS del ruteador.

Si existen registros debemos eliminarlos todos.

Lo que se puede hacer para no usar el DNS del ruteador es usar los servidores DNS de prodigy, para conseguir las direcciones de los DNS de tu localidad, puedes marcar al número de soporte y preguntar 01-800-1232222.

Para asignar los DNS a la conexión de Windows es necesario dar click derecho sobre el icono de la conexión, abrir las propiedades de la conexión, seleccionar TCP/IP y el botón de propiedades, y en esa ventana poner los DNS.

Propiedades de Protocolo Internet (TCP/IP)

General Configuración alternativa

Puede hacer que la configuración IP se asigne automáticamente si su red es compatible con este recurso. De lo contrario, necesita consultar con el administrador de la red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:

Máscara de subred:

Puerta de enlace predeterminada:

Obtener la dirección del servidor DNS automáticamente

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:

Servidor DNS alternativo:

Opciones avanzadas...

Aceptar Cancelar

En esta imagen se muestra donde se configura las direcciones de los servidores DNS