Glosario

AWK. Es un lenguaje de programación diseñado para procesar datos basados en texto, ya sean archivos o flujos de datos.

Bash. Es un intérprete de órdenes de Unix para el proyecto GNU. También puede ser utilizado como un lenguaje de programación, ya que se compone de todas las sentencias básicas de un leguaje estructurado común.

Batch. En DOS, OS/2 y Microsoft Windows, un archivo de batch es un archivo de texto que contiene una serie de comandos para ser ejecutados desde el intérprete de comandos.

Botnets. Son redes mundiales conformadas por equipos infectados, los cuales son conocidos como "Zombis". Estos equipos son llamados actualmente "Bots" y están a la espera de una orden enviada por una computadora central conocida como Comando y Control (Command and Control, C&C); hoy en día existen variaciones en la infraestructura que permiten la existencia de múltiples computadoras centrales e incluso con capacidades de convertir a un simple "bot" en computadora central. Son utilizadas para causar negaciones de servicio distribuidas (DDoS). A menudo los atacantes dueños de estas redes hacen millonarias sumas de dinero rentándolas para propósitos maliciosos.

Bots. Se trata de un programa robot, el cual se encarga de realizar funciones rutinarias. Pero que también pueden ser usados para crear cuentas en sitios que otorgan cuentas de correo gratuitas, para con esas cuentas realizar daños. También llegan a ser programas que a través de órdenes enviadas desde una computadora central controlan el equipo personal de la víctima, es decir, la convierten en un "Zombi".

Caballo de Troya (Trojan horse). Se disfraza él mismo como un programa funcional mientras encubre propósitos maliciosos y ocultos. Setiri y Hydan son buenos ejemplos.

Combinación de códigos maliciosos. Combina varias técnicas, las cuales ya fueron descritas, para incrementar la efectividad. Se ejemplifican con Lion y Bgbear.B.

Dirección IP. Es un código numérico que identifica a un equipo de cómputo en una red. Se forma de 32 bits, o bien, cuatro octetos en su versión 4.

Dirección MAC. Significa Media Access **C**ontrol (MAC) y es un identificador único y físico de cada interfaz de red, ya sea cableada o inalámbrica. Es asignada por el fabricante de acuerdo con la regulación de la IEEE. Se conforma de seis bytes y siempre es representada en sistema hexadecimal.

DNS. Significa Domain Name System que en español se puede nombrar como Sistema de Nombres de Dominio. Su función es proveer el mecanismo para el nombramiento de recursos y una manera en que los nombres son usables en diferentes equipos, redes, familias de protocolos, redes internas y organizaciones administrativas.

Exbibyte. Es una unidad de almacenamiento de información. Corresponde a 20^{60} bytes, es decir 1,152,921,504,606,846,976 bytes. Se representa con el símbolo EiB. El empleo del prefijo "exbi" (exa binario) se debe a que es la potencia de 2 que más se aproxima a "exa", prefijo cuyo valor es 10^{18}, es decir, 1,000,000,000,000,000,000.

Exploit. Es aquel código que ataca una vulnerabilidad en particular de un sistema operativo o aplicación. Los exploits no son necesariamente maliciosos, ya que gran cantidad de ellos son creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Sin embargo, existen ocasiones en que son componentes comunes de los programas maliciosos como los gusanos informáticos.

FTP. Es el File Transfer Protocol, o Protocolo de Transferencia de Archivos. Tiene la intención promover la compartición de archivos, incentivar el uso remoto de computadoras de manera indirecta o implícita, proteger un usuario de variaciones en los sistemas de almacenamiento de archivos entre equipos, y transmitir la información confiable y eficientemente.

GPL. Su significao es General Public License, o bien, Licencia Pública General; es una licencia creada por la Free software Foundation en 1989 y es usada principalmente para proteger la libre distribución, modificación y uso del software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan las libertades anteriores a los usuarios.

Gusano (Worm). Se propaga a través de la red. Se auto-replica. Usualmente no requiere de interacción humana para propagarse. Algunos ejemplos son Morris Worm, Code Red y SQL Slammer.

HTTP. El Hypertext Transfer Protocol es un protocolo a nivel de aplicación para sistemas de información transaccionales, colaborativos y distribuidos. Es un protocolo genérico y sin patria definida, el cual puede ser usado para muchas otras tareas además de uso para hiper texto. Ha estado en uso por la iniciativa global de información World-Wide-Web desde 1990.

Inundadores (Flooders). Los usuarios maliciosos utilizan los inundadores para atacar sistemas de redes de cómputo con una carga extra de tráfico de red para llevar a cabo una negación de servicio (DoS). Y cuando la negación de servicio es ejecutada simultáneamente por muchos sistemas comprometidos (también llamados zombis), el ataque es conocido como negación de servicio distribuida (DDoS).

Keyloggers. Son programas espías que toman el control de los equipos, para espiar y robar información. Monitorean el sistema y registran las pulsaciones del teclado para robar las claves tanto de páginas financieras y correos electrónicos, así como cualquier información introducida por teclado que el equipo utiliza para conocer lo que la víctima ha realizado; como conversaciones, ubicaciones visitadas, ejecuciones, movimientos, etcétera.

Mailers y Mass-Mailers. Son un especial tipo de gusanos de computadoras, los cuales se envían ellos mismos en correos electrónicos. Los Mass-Mailers se enviarán a múltiples correos incluyendo una copia de ellos mismos una vez que el código fue invocado. Programas como Happy99 o calificado como W32/SKA.A@m envían una copia de sí mismo cada vez que el usuario envía un nuevo mensaje.

MD5. Es un algoritmo de reducción criptográfico diseñado por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad. La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal. Cualquier información a la que se le aplique el algoritmo tendrá un correspondiente hash de salida que en teoría es único, es decir, que no puede producirse con alguna otra combinación.

Modelo de interconexión TCP/IP. Son las siglas de Transmission Control Protocol/Internet Protocol, es la arquitectura que rige todas las comunicaciones entre todas las computadoras en Internet. Es un conjunto de instrucciones que dictan cómo se han de enviar paquetes de información por distintas redes. También tiene una función de verificación de errores para asegurarse que los paquetes llegan a su destino final en el orden apropiado.

Perl. Es un lenguaje de programación interpretado y diseñado por Larry Wall en 1987. Toma características del lenguaje C, del lenguaje interpretado shell, AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

Pharming. Es un software maligno que suplanta el servicio DNS mediante el archivo hosts local para así conducir a la víctima a una página Web falsa. El efecto se aprecia al intentar entrar a un determinado nombre de dominio en nuestro navegador redirecciona a la víctima al sitio que el atacante ha cambiado. Por ejemplo, la página de un banco puede ser www.banco.com (213.132.253.4) y el DNS resuelve la dirección 123.234.134.60, entonces no es fácil percatarse de que se está visitando una página falsa perteneciente al atacante.

Phishings. Del inglés "fishing" (pescando). Este término se utiliza para identificar la acción fraudulenta de conseguir información confidencial, vía correo electrónico o página web, con el propósito de que los usuarios de cuentas bancarias lo contesten, o entren a páginas aparentemente iguales a la del banco o de los portales con ingreso por contraseña.

Programas generadores de correo spam. Estos programas son usados para enviar mensajes no solicitados a grupos de mensajería instantánea, grupos de noticias, o cualquier otro tipo de dispositivos móviles en forma de correo electrónico o mensajes SMS por telefonía celular.

Usualmente los spammers lo hacen para ganar dinero al inundar las redes con tráfico que contiene cierta publicidad.

Protocolo DHCP. Significa Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red.

Protocolo IRC. El Internet Relay Chat es para uso de conferencia con base texto. Ha sido desarrollado desde 1989, año cuando fue originalmente implementado para establecer conversaciones entre un grupo de personas.

Puerta trasera (Backdoor). Lleva a cabo un desvío de los controles normales de seguridad para dar al atacante acceso. Han sido muy útiles para los usuarios maliciosos las siguientes aplicaciones: Netcat, Virtual Network Computing (VNC), subseven y back Orifice. Sin embargo, los dos primeros pueden ser utilizados legítimamente como herramientas de administración remota, e ilegítimamente como herramientas de ataque.

Puertos. Son los puntos finales de una comunicación. Son interfaces, por las cuales, diferentes tipos de datos pueden ser enviados y recibidos. Se cuenta con 65535 interfaces de software en cada dispositivo.

Red de datos. Es un conjunto de equipos de cómputo interconectados entre sí, de tal forma que pueden intercambiar información.

RootKit a nivel de núcleo. Manipula la parte central del sistema operativo, el núcleo, para ocultar y crear puertas traseras. Algunos ejemplos: Adore y Kernel Instrusion System.

RootKit a nivel usuario. Reemplaza y modifica programas ejecutables usados por administradores y usuarios del sistema. Pueden aplicar la familia de Linux RootKit (LRK), Universal RootKit y FakeGINA.

Script Kidie. Es alguien que busca una presa fácil. No busca información específica o una víctima en concreto. Su objetivo es ganar de la forma más sencilla posible privilegios. Hace esto centrando su actividad en la búsqueda de una vulnerabilidad por toda Internet, que les permita explotar el sistema. Tarde o temprano encontraran a alguien vulnerable. Algunos de ellos son usuarios avanzados que desarrollan sus propias herramientas y garantizan su futuro acceso mediante puertas traseras. Otros no saben lo que hacen y solo saben ejecutan herramientas. Independientemente de su nivel de conocimientos, comparten una estrategia común, una búsqueda aleatoria de cualquier vulnerabilidad, para a continuación aprovecharse de ella.

Sed. Es un editor de flujo, una potente herramienta de tratamiento de texto para el sistema operativo Unix que acepta como entrada un archivo, lo lee y modifica línea a línea mostrando el resultado en la salida estándar.

Sendmail. Es un popular "Agente de Transporte de Correo" (MTA, Mail Transport Agent) en Internet, cuya tarea consiste en encaminar los mensajes o correos de forma que estos lleguen a su destino.

Servicio simulado. AAAEs un servicio de red que simula a un servicio legítimo, maneja algunas órdenes del este, sin embargo no llega más lejos y su función básica capturar los datos que iban dirigidos al servicio en cuestión.

SHA1. Es el segundo de los algoritmos de la familia SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) desarrollado por la NSA (Agencia de seguridad Nacional de los Estados Unidos) y publicado en el NIST (National Institute of Standards and Technology). Produce una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 2^{64} bits. Esta basado en principios usados por Ronald L. Rivest, diseñador de MD4 y MD5.

Virus. Infecta un archivo del sistema víctima (p.e. ejecutable, documento de procesador de palabras, etcétera). Él mismo se replica. Normalmente requiere de la interacción humana para su activación (abriendo un archivo, leyendo un correo electrónico, arrancando el sistema o ejecutando un programa infectado). Algunos ejemplos son Michelangelo y CIH.

WMIC. El Windows Management Instrumentation Command-line revela una gran cantidad de información sobre Windows Server 2003 y hardware subyacente, mediante el uso de Windows Management Instrumentation (WMI). El primer propósito de WMIC es facilitar administración de tareas automáticas y de script. Sin embargo, también es útil para la resolución de problemas ya que sus reportes con información del sistema no están disponibles con otras herramientas.

Apéndices

Preparación de la infraestructura

Para el correcto funcionamiento de la herramienta TRUMAN es necesaria la utilización de equipos de cómputo con ciertas características en específico. En la infraestructura básica se debe contar con lo siguiente:

- Un servidor de arranque por red y servicios de red. Instalado con un sistema operativo GNU/Linux.
- Un equipo con Windows XP, puede ser en cualquiera de sus versiones.

Las siguientes consideraciones deben hacerse al instalar la herramienta:

- El servidor de GNU/Linux almacena dos imágenes del cliente Windows XP. Una de ellas es una imagen limpia, es decir, sin infecciones; la segunda es una imagen contaminada como producto de la ejecución de un código malicioso, ésta última se genera cada vez que se ejecuta un programa malicioso para su análisis.
- Los estados de antes y después de la infección son ampliamente comparados para la obtención de la información relevante.
- El sistema operativo del equipo cliente será restaurado por el servidor mediante la utilización de la imagen no contaminada. Esto permitirá dejar listo al cliente para un nuevo análisis.

Antes de instalar el desarrollo de la herramienta TRUMAN en el servidor, será necesaria la instalación de una serie de utilidades que complementan al desarrollo y le permiten desempeñar todas sus funcionalidades. A continuación un listado de dichos complementos.

- Servidor DHCP (dhcpd)
- Servidor Apache 2 con soporte Perl (httpd y mod_perl)
- Servidor TFTP

- Sendmail
- Snort
- Tcpflow
- Tcpdump
- Comando “dd”
- Entre otras.

Por último queda mencionar las características físicas y lógicas tanto del servidor como del cliente de la herramienta. En el caso del servidor se debe instalar en un equipo con al menos 1 Gb de memoria RAM, por lo menos 10 Gb en disco duro, un procesador de mínimo 1.6 Ghz y dos interfaces de red 10/100 Mbps; debe tener instalado un sistema operativo GNU/Linux de manera básica, es decir, sin interfaz gráfica, ya que no es necesaria; para el desarrollo de este proyecto he utilizado la distribución de GNU/Linux Debian 4.0 Etch, la cual resulta sencilla de instalar, utilizar y administrar. Para el caso del cliente en realidad puede tratarse de un equipo no muy potente, pues sólo llevará a cabo la tarea de ser cliente; se recomienda que tenga 256 Mb de memoria, 2 Gb en disco duro y una interfaz de red 10/100 Mbps; debe contar con un Windows XP instalado en una partición de 2 Gb y se recomienda que no más, aunque sí puede ser menos. Creo que no es necesario mencionar que ambos equipos deben contar con los medios de entrada suficientes para realizar la instalación de sus respectivos sistemas operativos como unidades de CD y DVD, según sea el caso. También se requiere un cable cruzado para su interconexión. Para este proyecto la implementación se realizó en equipos virtuales, pero una instalación en equipos físicos es cien por ciento viable, en realidad en el DSC/UNAM-CERT se cuenta con una implementación física de prueba.

Instalación de la herramienta TRUMAN ampliada

Conociendo el apéndice anterior se puede proceder a la instalación de la infraestructura y la herramienta en su total funcionalidad. Antes de comenzar se deben interconectar ambos equipos mediante el cable cruzado y la segunda interfaz de red del servidor a la red interna que le proporcione salida a Internet. Por último encender el servidor e iniciar sesión como “root” para comenzar.

Instalación del Servidor

Paso 1. Se procede a instalar el servidor de SSH para la administración remota del equipo, mediante la ejecución de los siguientes comandos (el primero para actualizar la lista de paquetes disponibles y el segundo para la instalación del servicio SSH).

```
# apt-get update
# apt-get install openssh-server
```

Paso 2. A continuación se instalan algunas utilerías necesarias con el comando de abajo. (Fig. A.1)

```
#apt-get install perl tftpd-hpa dhcp3-server xinetd tcpdump tcpflow
psmisc binutils gcc make libperl-dev libc6-dev libwww-perl sendmail
libpcap0.8 libpcap0.8-dev libpcre3 libpcre3-dev
```

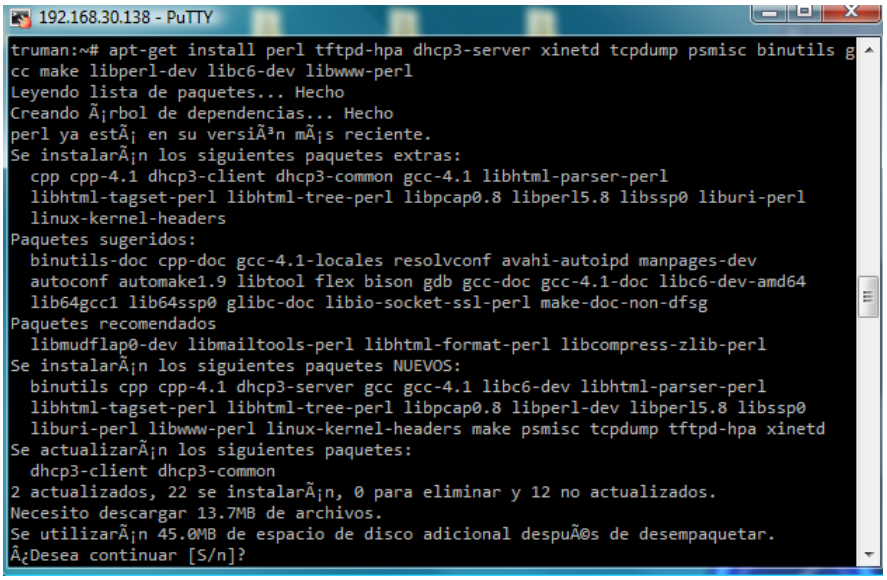

Fig. A.1. Comando para la instalación de utilerías.

Paso 3. Modificar la configuración de la segunda tarjeta de red con una dirección estática (en este caso se usó 4.5.6.1/24). Utilizar el siguiente comando y editar el archivo como se muestra en la figura. (Fig. A.2, página siguiente)

```
# vim /etc/network/interfaces
```

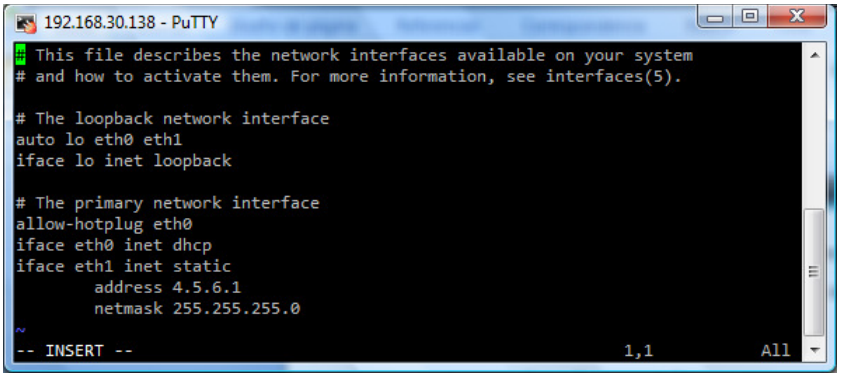

Fig. A.2. Configuración de la interfaz de red.

Enseguida reiniciar los servicios de red con el siguiente comando para que surtan efecto las configuraciones.

```
# /etc/init.d/networking restart
```

Es importante mencionar que TRUMAN permite configurar cualquier segmento de red, por esta ocasión se usó la red 4.5.6.0/24 que es la que está configurada por defecto en el empaquetado original de TRUMAN.

Paso 4. Ahora se debe realizar la instalación del servidor apache 2 desde el código fuente. Para ello seguir la siguiente bitácora de comandos. (Fig. A.3)

```
# wget http://www.eu.apache.org/dist/httpd/httpd-2.2.14.tar.gz
# wget http://www.eu.apache.org/dist/httpd/httpd-2.2.14.tar.gz.md5
# md5sum httpd-2.2.14.tar.gz
# tar -zxvf httpd-2.2.14.tar.gz
# cd httpd-2.2.14
# ./configure --enable-so
# make && make install
# /usr/local/apache2/bin/apachectl start
# ls -l /usr/local/apache2/
```

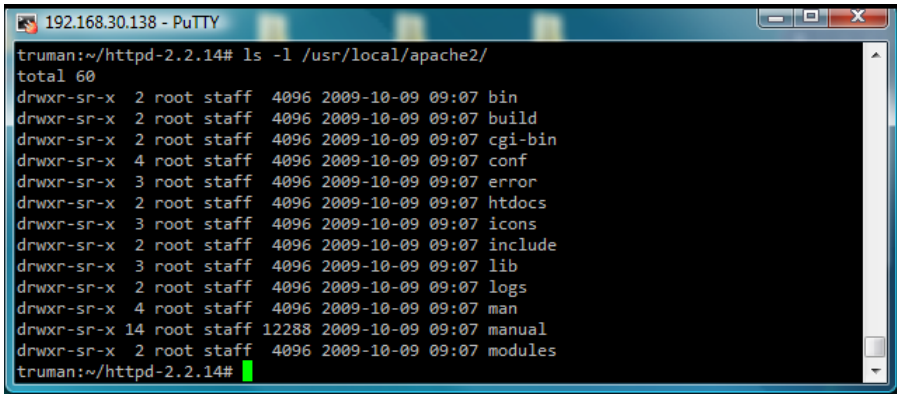

Fig. A.3. Instalación de Apache 2.

Paso 5. Instalación de mod_perl para Apache 2. Los siguientes comandos ayudarán a resolver este paso. (Fig. A.4)

```
# wget http://perl.apache.org/dist/mod_perl-2.0-current.tar.gz
# tar xzvf mod_perl-2.0-current.tar.gz
# ln -s /usr/lib/libgdbm.so.3 /usr/lib/libgdbm.so
# cd mod_perl-2.0.4/
# perl Makefile.PL MP_APXS=/usr/local/apache2/bin/apxs
# make && make test
```

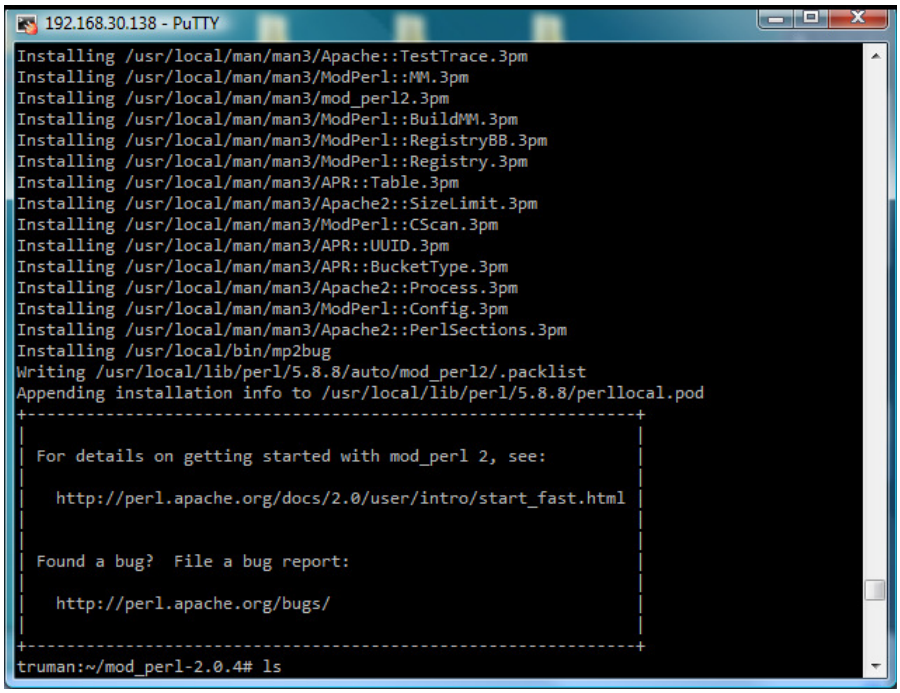

Fig. A.4. Instalación de mod_perl para Apache 2.

Paso 6. Editar y agregar en el archivo /usr/local/apache2/conf/httpd.conf la línea: LoadModule perl_module modules/mod_perl.so. En la sección correspondiente para Dynamic Shared Object Support (Soporte de Objetos Compartidos y Dinámicos). Posteriormente se debe reiniciar el servicio de Apache 2. Los siguientes dos comandos servirán para el propósito. (Fig. A.5)

```
# vim /usr/local/apache2/conf/httpd.conf
# /usr/local/apache2/bin/apachectl restart
```

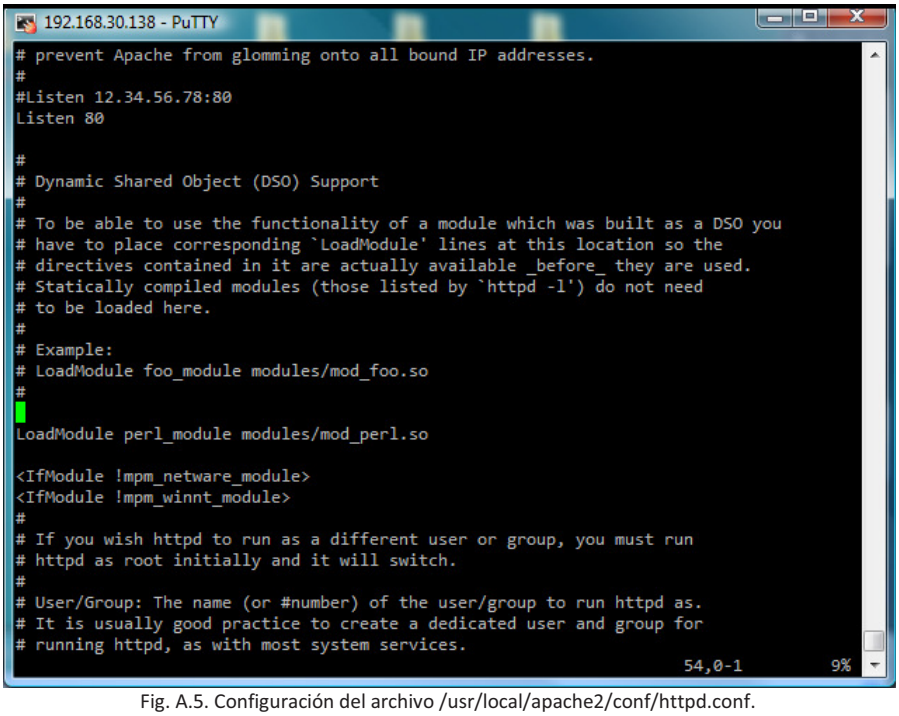

Fig. A.5. Configuración del archivo /usr/local/apache2/conf/httpd.conf.

Paso 7. Editar el archivo /etc/default/tftpd-hpa y cambiar RUN_DAEMON a "yes", cambiar "/var/lib/tftpboot" por "/tftpboot". Se debe iniciar el servicio, solo que antes se sugiere eliminar del arranque del envoltorio de "tftp" y matar el proceso correspondiente a "inetd". (Fig. A.6)

```
# vim /etc/default/tftpd-hpa
# mv /etc/rc2.d/S20openbsd-inetd /etc/rc2.d/K20openbsd-inetd
# /etc/init.d/tftpd-hpa start
# chmod +x /etc/init.d/apache2.sh
```

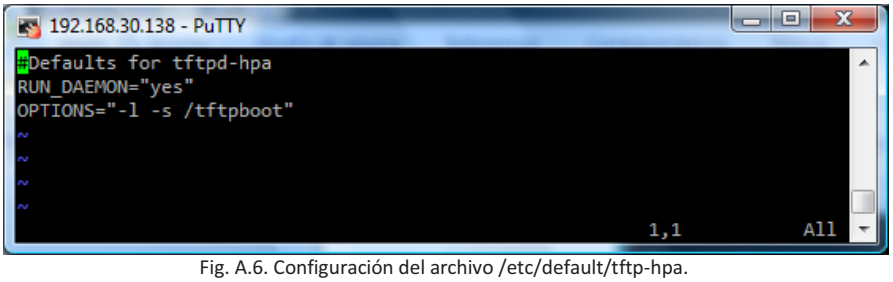

Fig. A.6. Configuración del archivo /etc/default/tftp-hpa.

Para este punto se sugiere editar el archivo /etc/init.d/apache2.sh, al igual configurarlo para que se ejecute en cada reinicio del sistema. Para lo cual serán útiles los comandos siguientes.

```
# echo '#!/bin/bash' > /etc/init.d/apache2.sh
# echo '/usr/local/apache2/bin/apachectl start' >> /etc/init.d/apache2.sh
# echo '/etc/init.d/tftpd-hpa restart' >> /etc/init.d/apache2.sh
```

```
# ln -s /etc/init.d/apache2.sh /etc/rc2.d/S21apache2
```

Paso 8. Para que la herramienta de comparación de sistemas de archivos de la herramienta ampliada funcione correctamente se debe instalar un módulo de perl, el cual es "Digest-MD5-File". Para lograrlo seguir las siguientes líneas de comandos.

```
# wget  http://search.cpan.org/CPAN/authors/id/D/DM/DMUEY/Digest-MD5-
File-0.07.tar.gz
# tar xzvf Digest-MD5-File-0.07.tar.gz
# cd Digest-MD5-File-0.07
# perl Makefile.PL
# make
# make install
```

Paso 9. Ahora bien comencemos con la instalación de la herramienta TRUMAN. He construido un paquete llamado truman-0-2_DSC.tar.gz, el cual contiene todos los programas que componen a esta versión mejorada. A través de colocar cada archivo en su ubicación específica quedará la herramienta instalada. La lista de comandos a continuación será útil para este propósito.

```
# tar xzvpf truman-0.2_DSC.tar.gz
# cd truman-0.2_DSC
# cp -r forensics/ /
# cp -r images/ /
# cp -r results/ /
# cp -r tftpboot/ / && ln -s /tftpboot /var/lib/tftpboot
# cp -r mnt/ /
# cp  etc/dhcp3/dhcpd.conf /etc/dhcp3/dhcpd.conf
# cp etc/init.d/* /etc/init.d/
# ln -s /etc/init.d/services.sh /etc/rc2.d/S99services
# cp etc/xinetd.d/* /etc/xinetd.d/ && /etc/init.d/xinetd restart
# cp usr/bin/dumphive /usr/bin/
# cp usr/local/apache2/cgi-bin/truman.cgi /usr/local/apache2/cgi-bin/
```

Paso 10. Editar el archivo /etc/dhcp3/dhcpd.conf en la parte de "host client7" donde se deberá poner la dirección MAC del cliente Windows a utilizar. (Fig. A.7, página siguiente)

```
# vim /etc/dhcp3/dhcpd.conf
```

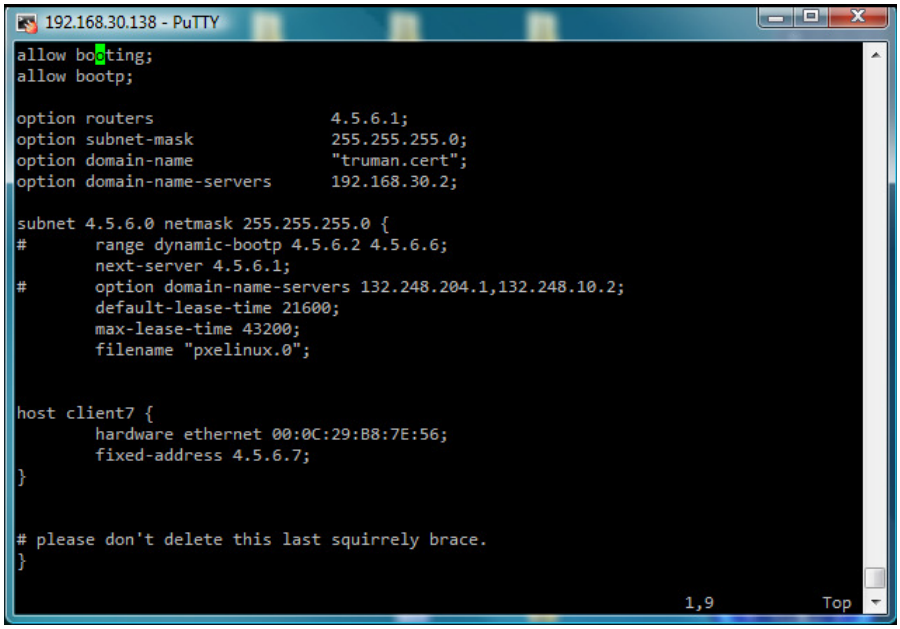

Fig. A.7. Configuración del archivo /etc/dhcp3/dhcpd.conf.

Paso 11. Modificar el archivo /etc/services agregándole dos líneas al final con las siguientes instrucciones.

```
# echo -e '# Truman Services' >> /etc/services
# echo -e 'ddsave\t\t45611/tcp\t\t\t# Truman save requests' >>
/etc/services
# echo -e 'ddrestore\t45612/tcp\t\t\t# Truman restore requests' >>
/etc/services
```

Paso 12. Creación de la utilidad /bin/ddquiet. Fácilmente con las siguientes órdenes de Shell.

```
# echo '#!/bin/bash' > /bin/ddquiet
# echo '/bin/dd $* 2>/dev/null' >> /bin/ddquiet
# chmod 755 /bin/ddquiet
```

Paso 13. Para que el funcionamiento de TRUMAN sea normal se deben asignar una serie de permisos y cambio en dueños y grupos. Seguir la lista de órdenes a continuación.

```
# chgrp daemon /forensics/queue/ /forensics/exes/
# chmod g+rwx /forensics/queue/ /forensics/exes/
# chown -R daemon:daemon /tftpboot/pxelinux.cfg/
# chmod g+rwx /tftpboot/pxelinux.cfg/
# chmod g+rw /tftpboot/pxelinux.cfg/*
# chmod o+x,g+x,u+x /usr/local/apache2/cgi-bin/truman.cgi
# chmod o+w /fauxservers/start.flag
```

Paso 14. Ahora se procede con la instalación de Snort. Poner atención a la bitácora.

```
# wget http://dl.snort.org/snort-current/snort-2.8.4.1.tar.gz
# tar xzvf snort-2.8.4.1.tar.gz
# cd snort-2.8.4.1
# ./configure
# make
# make install
```

Paso 15. Para asegurar el levantamiento de todos los servicios se recomienda reiniciar el servidor en este momento. A continuación una vista de cómo debe lucir el comando “netstat -natup". (Fig. A.8)

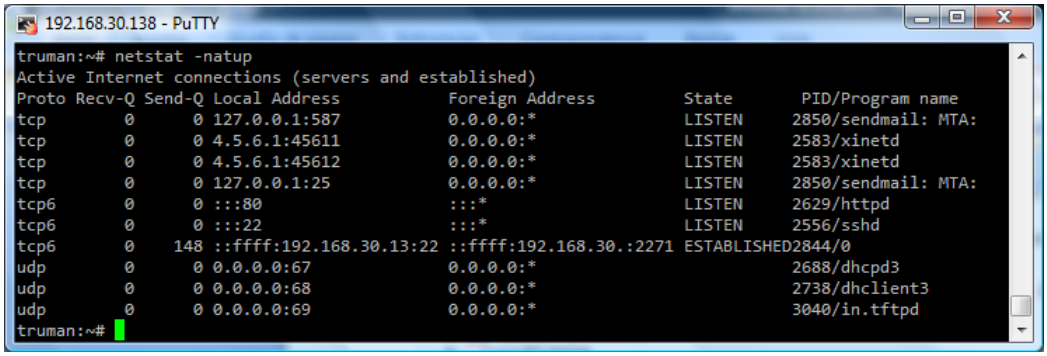

Fig. A.8. Salida del comando “netstat -natup”.

Instalación del Cliente

Paso 1. Se debe configurar en el BIOS del equipo el arranque vía red. La mayoría de los equipos recientes soportan esta funcionalidad. (Fig. A.9)

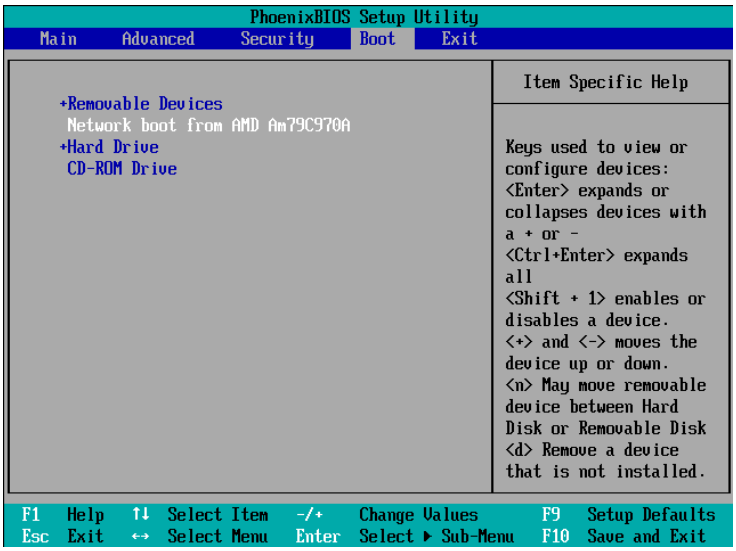

Fig. A.9. Configuración del BIOS.

Paso 2. Antes se debe crear una cuenta con privilegios de administración para ser configurada con inicio de sesión automático en este cliente. Para lograr éste último propósito se deben seguir las siguientes instrucciones:

a) Hacer clic en el menú de **Inicio** y en **Ejecutar**, escribir "regedit" y hacer clic en **Aceptar**. (Fig. A.10)

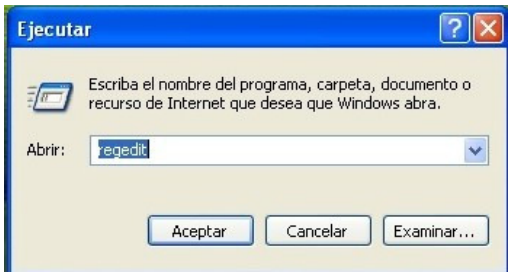

Fig. A.10. Ejecutando "regedit".

b) Buscar la siguiente clave de Registro. (Fig. A.11)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

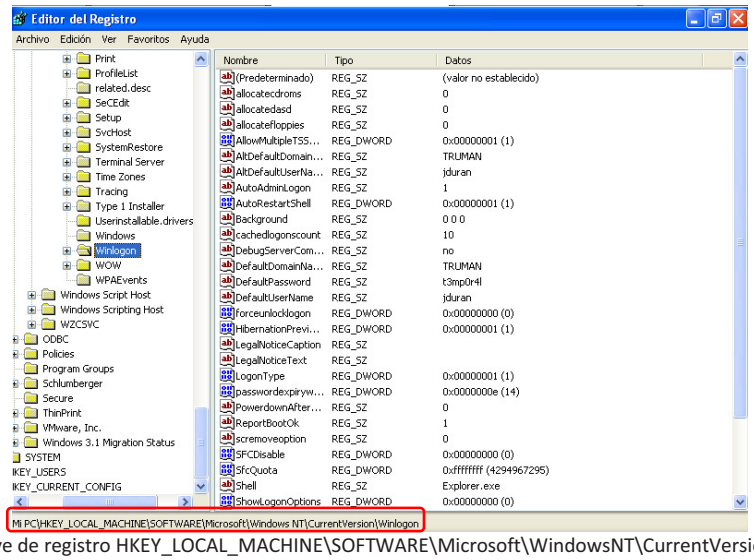

Fig. A.11. Llave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon.

c) Utilizando los datos de la cuenta que se quiera configurar (nombre de usuario y contraseña), hacer doble clic en la entrada **DefaultUserName**, escribir el nombre de usuario y hacer clic en **Aceptar**. (Fig. A.12)

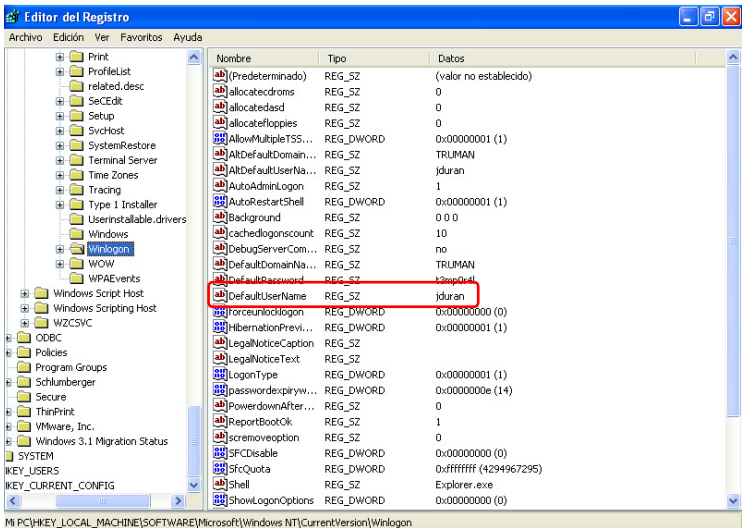

Fig. A.12. Señalamiento del valor a modificar.

d) Hacer doble clic en la entrada **DefaultPassword**, escribir la contraseña en el cuadro de información del valor y, a continuación, hacer clic en **Aceptar**. (Fig. A.13)

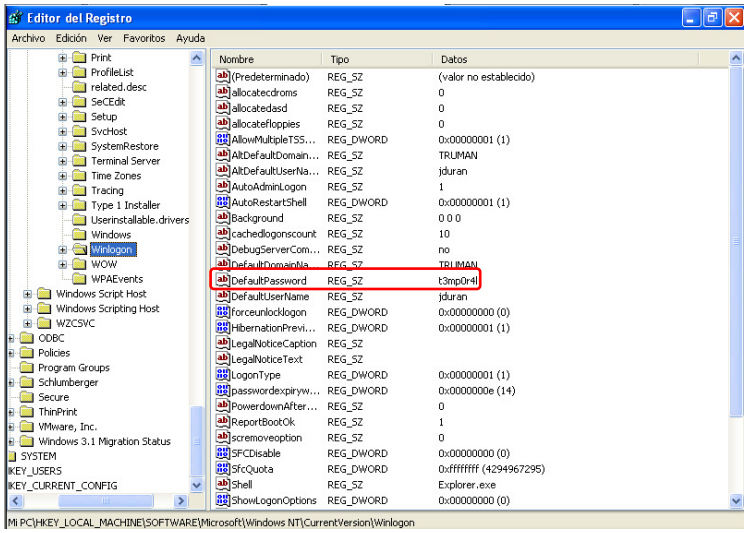

Fig. A.13. Señalamiento del valor a modificar.

e) Hacer doble clic en la entrada **AutoAdminLogon**, escribir 1 en el cuadro de información del valor y hacer clic en aceptar. (Fig. A.14)

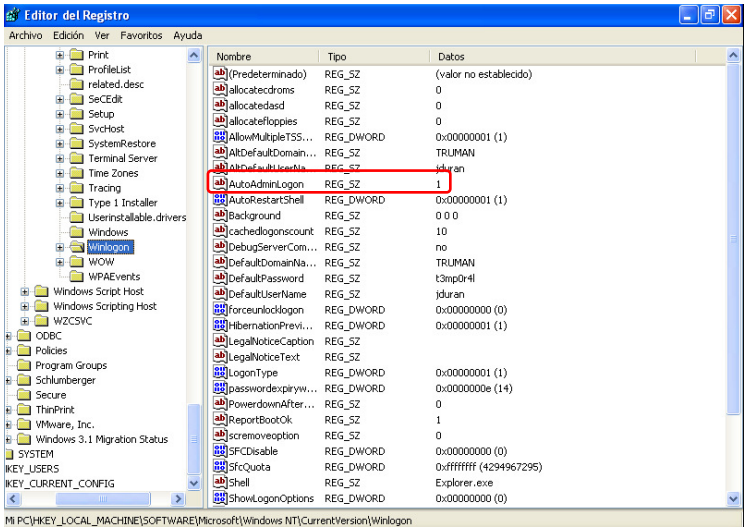

Fig. A.14. Señalamiento del valor a modificar.

f) Por último salir del editor del registro. Hacer clic en **Inicio**, después en **Apagar equipo**, luego en **Reiniciar**, para verificar el inicio automático que se acaba de configurar. (Fig. A.15)

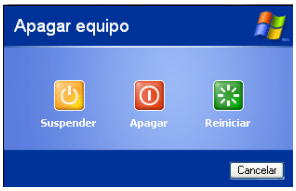

Fig. A.15. Pantalla de apagado y reinicio del sistema.

Nota. Si no hay ningún valor denominado **DefaultUserName, DefaultPassword y/o AutoAdminLogon**, se deberá crearlos. Para ello, seguir estos pasos:

En el Editor del Registro, hacer clic en **Edición**, en **Nuevo** y, a continuación en **Valor alfanumérico**.

a) Escribir “DefaultUserName”, “DefaultPassword” o “AutoAdminLogon” como nombre del valor y, a continuación, presionar ENTRAR.
b) Hacer doble clic en cada una de las claves que se acaban de crear y escribir el nombre de usuario y contraseña en el cuadro **Información del valor**, respectivamente.
c) Si no se especifica ninguna cadena en **DefaultPassword,** Windows XP cambia automáticamente el valor de la clave **AutoAdminLogon** de **1** (verdadero) a **0** (falso), con lo que deshabilitará la característica de inicio de sesión automático.

Paso 3. El siguiente paso es desactivar el firewall, servicio de antivirus, de actualizaciones y las alertas.

Para desactivarlos dar clic en **Inicio** y después en **Panel de Control**. Después de haber entrado en el Panel de control acceder al **Centro de seguridad** y desactivar las alertas. Ésto es, una vez en la ventana y en la parte de la izquierda hay una columna llamada "Recursos". Dirigirse a "Cambiar la forma en que el Centro de seguridad me alerta". Es como se muestra a continuación. (Fig. A.16)

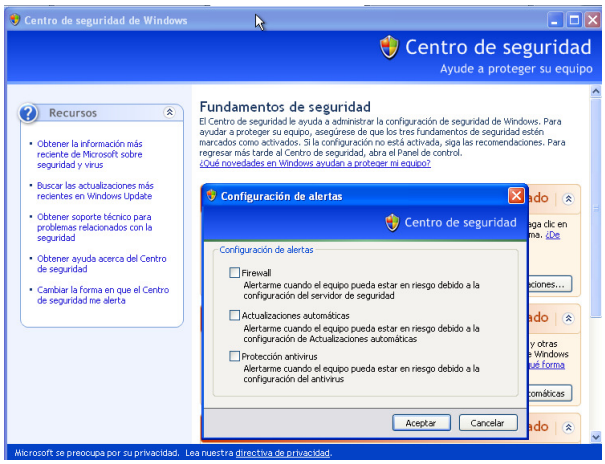

Fig. A.16. Configuración de las alertas de seguridad de Windows.

Ahora bastará con desactivar las tres casillas de selección, después dar clic en **Aceptar**.

A partir de la ventana anterior también se pueden desactivar cada uno de los rubros comprendidos en el **Centro de Seguridad** (firewall y actualizaciones). El resultado debe ser el siguiente. (Fig. A.17)

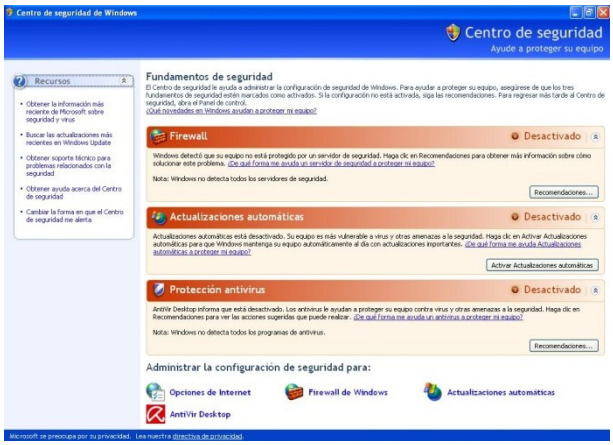

Fig. A.17. Características de seguridad desactivadas.

Paso 4. Ahora es necesario desactivar la funcionalidad de restauración automática.

Para desactivarla dar clic en **Inicio** y después en **Panel de Control**. Después de haber entrado en el Panel de control acceder a Rendimiento y mantenimiento para después dirigirse a **Sistema**. Y colocado en la pestaña de **Restaurar sistema** habilitar la casilla para desactivar la restauración del sistema. (Fig. A.18)

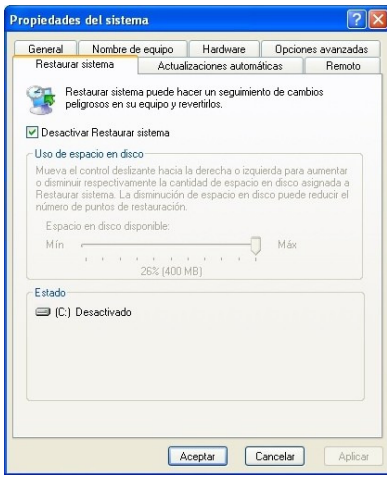

Fig. A.18. Restauración del sistema desactivado.

Paso 5. Ahora sólo resta instalar la parte de la herramienta TRUMAN correspondiente a Windows XP. Para ello se debe acomodar el contenido de la carpeta win32 en el sistema de archivos de Windows, considerando que win32 es la raíz de dicho sistema de archivos. (Fig. A.19)

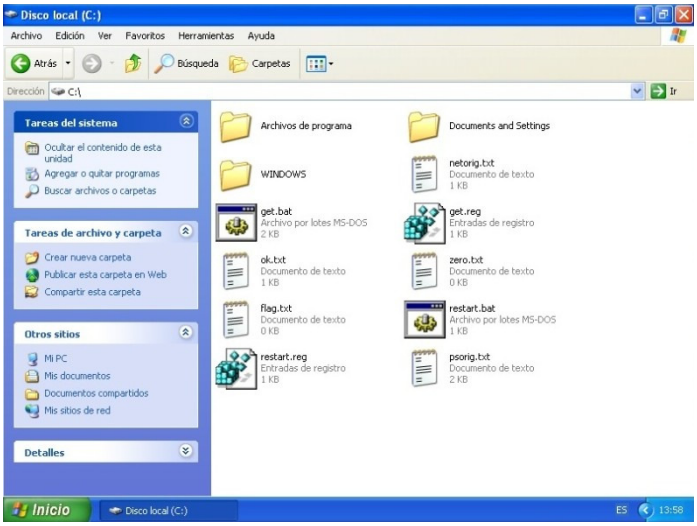

Fig. A.19. Instalación de TRUMAN en Windows.

Paso 6. En este paso se tiene que registrar el arranque de las aplicaciones de TRUMAN en Windows. Esto se realiza mediante la ejecución de los archivos get.reg y restart.reg, los cuales están en C:\. Así como también ejecutar los comandos de abajo para procesos y conexiones iniciales e instalar la herramienta wmic .

```
C:\>tasklist > "C:\psorig.txt"
C:\>netstat -na > "C:\netorig.txt"
C:\>wmic
```

La imagen de abajo es como se verá la pantalla de inicio. (Fig. A.20)

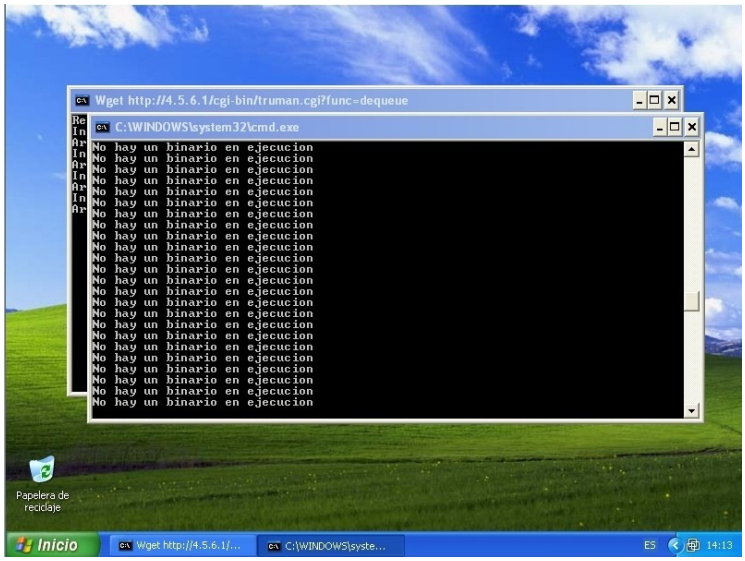

Fig. A.20. Pantalla de inicio de TRUMAN en Windows.

Ajustes generales

Antes de comenzar el análisis de códigos maliciosos es necesario obtener la imagen limpia del sistema cliente, con la que se va a restaurar una vez que se contamine. Para ello reiniciar el sistema cliente y elegir la opción tres en el menú de arranque de TRUMAN (fig. A.21). Se realizará la imagen, al terminar de ejecutar los comandos de abajo para guardar la imagen y obtener la información de la imagen limpia. De forma autómatica el cliente se reiniciará y se colocará en el modo de espera para el análisis de malware.

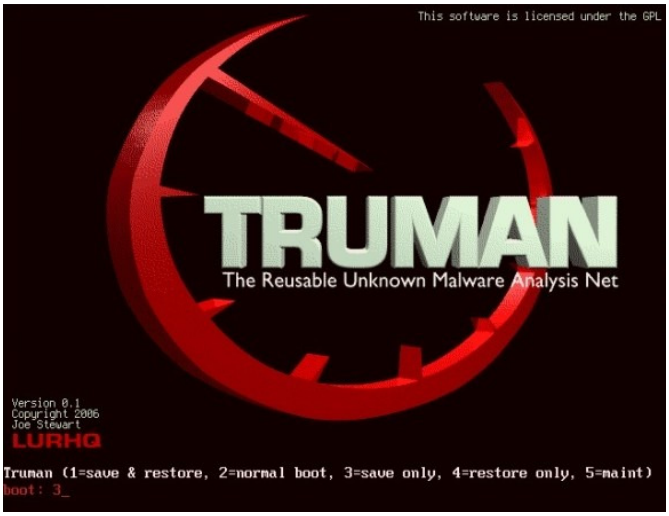

Fig. A.21. Menú de arranque de TRUMAN en Windows.

```
# mv /images/ddsave.img /images/ddrestore.img
# /forensics/getorig.sh
```

Únicamente resta colocar muestras de códigos maliciosos en el directorio /forensics/queue para que comience a analizarlos automáticamente.

Anexos

Anexo 1. Archivo C:\get.bat

```
@ECHO OFF
set SERVER_IP=4.5.6.1
set REPORT_CGI=truman.cgi

rem echo Reporting successful boot to boot server...
echo Reportando arranque exitoso al servidor de arranque...

rem con esta linea manda ejecuta el script cgi del servidor para poner el arranque de truman en 1, ver
truman
.cgi
wget -q -O C:\ok.txt http://%SERVER_IP%/cgi-bin/%REPORT_CGI%?res=booted > nul


:retr
rem echo Attempting to retrieve next file in queue...
echo Intentando recuperar el siguiente archivo en cola...

rem activa el envio de malware contenido en la carpeta /forensics/queue del servidor,lo hace uno a la vez
rem y lo coloca en la ruta C:\WINDOWS\system32\sandnet.exe. Si la dicho directorio estuviera vacio
enviara un
 archivo de 0 bytes
wget -q -O C:\WINDOWS\system32\sandnet.exe http://%SERVER_IP%/cgi-bin/%REPORT_CGI%?func=dequeue > nul


rem verifica si el archivo es de 0 bytes comparandola binariamente con otro archivo que tambien es de 0
bytes

fc /b C:\WINDOWS\system32\sandnet.exe C:\zero.txt | find "FC: no se han encontrado diferencias" > nul

rem error 2 si el comando falla
if errorlevel==2 echo El comando fc fallo

rem error 1 y error no es 2 se dirige a la etiqueta filefound
if errorlevel==1 if not errorlevel==2 goto filefound

rem echo File not found, sleeping 60 seconds...
echo Archivo no encontrado, durmiendo 60 segundos...
sleep 60
goto retr

:filefound
copy C:\WINDOWS\system32\sandnet.exe C:\
rem echo Executing malware sample...
echo Ejecutando muestra de malware...
echo 1 > C:\flag.txt
```

Anexo 2. Archivo C:\restart.bat

```
@ECHO OFF

:retr
fc /b C:\flag.txt C:\zero.txt | find "FC: no se han encontrado diferencias" > nul

rem error 2 si el comando falla
if errorlevel==2 echo El comando fc fallo

rem error 1 y error no es 2 se dirige a la etiqueta filefound
if errorlevel==1 if not errorlevel==2 goto binaryexe

echo No hay un binario en ejecucion
```

```
sleep 1
goto retr

:binaryexe
echo Durmiendo 300 segundos (5 min)...
sleep 300
tasklist > C:\psnew.txt
rem pslist > C:\psnew.txt
netstat -na > C:\netnew.txt
rem echo Volcando memoria fisica...
rem dd.exe if=\\.\PhysicalMemory of=c:\memdump.img bs=4096 conv=noerror
echo Rebooting...
rem shutdown -r
wmic os where primary=true Call Reboot
```

Anexo 3. Archivo /forensics/compare.pl

```
#!/usr/bin/perl -w
#Este script hace una comparacion del sistema de archivos entre el orig y el new,
#es decir, la imagen limpia y la contaminada
use Digest::MD5::File qw(dir_md5_hex file_md5 file_md5_hex url_md5_hex);
#########################################################
#####    VALIDAR Y CARGAR LOS ARGUMENTOS             #####
#########################################################
if (@ARGV == 0)
{
        print "Modo de Uso \n$0 -i Ruta_Imagen\n$0 -x Ruta_Imagen\n";
        exit 1;
}

#cambiar imagen para obtener valores del original
$IMAGEN=$ARGV[1];
$ORIGINAL="/forensics/orig/orig.md5";
$NUEVO="/forensics/new/new.md5";

if ($ARGV[0] eq "-i" && @ARGV == 2) {
        #print "\n######## Entrando al modo INICIAL ########";
        inicial($ORIGINAL);
        exit 0;
}
elsif ($ARGV[0] eq "-x" && @ARGV == 2)
{
        #print "\n####### Entrando al modo COMPARACION ########";
        comparacion();
        exit 0;
}
else
{
        print "\nModo de Uso \n$0 -i,-x Ruta_Imagen\n";
        exit 1;
}


#########################################################
#####                     FUNCIONES                 #####
#########################################################


### Funcion para encontrar los archivos y/o registros dentro del archivo
### encontrar(CadenaArchivo,ArchivoInfo)
sub encontrar{
        my $file;
        my $archivo;
        $file=shift;
        #print "Cadena: $file";
        #$file=~ s/\\/\\\\/g;
        $archivo=shift;
        open(AI,$archivo);
        while (<AI>) {
                if (/^\Q$file\E/) {
                        chomp($_);
                        return split(/\|/,$_);
                }
        }
        return ();
}

### Funcion para leer los directorios
## leerDir (RutaAbsolutaDirectorio [ArchivoGuardar])
```

```
sub leerDir
{
#       print "\nLeyendo Directorio $_[0]";
#        if (!defined($guardar)) {$guardar='orig.md5'; }

        if (defined($_[1])) {$guardar=$_[1];}

        my $d;
        my @dir;
        $d=$_[0];
        chomp($d);
        #if ($d=~/\"$/) {chop($d);}
#       print "\nDirectorio: '$d'";
        opendir(DH,$d) || die "No se pudo abrir directorio: '$d'";
        @dir=readdir DH;
#       print "@dir";
        foreach (@dir) {
#               print "$_\n";
                if (-d $d."/".$_) {
                 if (/(^.$)|(^..$)/) {
                         next;
                 }
                        #print "\nDirectorio:'$d\\$_'";
                        leerDir($d."/".$_,$guardar);
                        next;
                }
                if (-f $d."/".$_) {
                         open(SV,">>$guardar") or die "Error al abrir archivo para guardar";
                 print SV "\n$d/$_|".file_md5_hex($d."/".$_);
                 close(SV);
                 next;
                }
        }
}

#### Se le pasa como argumento el archivo de salida a guardar
sub inicial
{
        #print "\nFUNCION INICIAL: \nArchivo de Salida $_[0]";
        open(SV,">$_[0]") or die "Error al BORRAR archivo para guardar";
        close(SV);
        leerDir($IMAGEN,$_[0]);
}

sub comparacion
{
        my @reg;
        #print "\nFuncion de comparacion";
        inicial($NUEVO);
        `sed 's/\\/mnt\\/new/C:/g' $NUEVO > $NUEVO.res`;
        `rm $NUEVO`;
        `mv $NUEVO.res $NUEVO`;

        #OJO ajuste previo para probar con los siguientes comandos
        #Las siguientes cuatro lineas efectivas son para una optimizacion en la clasificacion de los
archivos
        #print $ORIGINAL.$NUEVO."\n";
        `diff --text $ORIGINAL $NUEVO | grep "^<" | grep -v -f /forensics/patternsfs.txt | sed -e
's/<\\s//g' > /forensics/.orig.md5.diff`;
        `diff --text $ORIGINAL $NUEVO | grep "^>" | grep -v -f /forensics/patternsfs.txt | sed -e
's/>\\s//g' > /forensics/.new.md5.diff`;
        $ORIGINAL="/forensics/.orig.md5.diff";
        $NUEVO="/forensics/.new.md5.diff";

        print "\nArchivos creados:";
        open(TMP,$NUEVO);
        while (<TMP>)
        {
                undef @dato;
                chomp $_;
                @reg=split(/\|/,$_);
                @dato=encontrar($reg[0],$ORIGINAL);
                if (@dato == 0)
                {
                        print "\n$reg[0]";
                }
        }
        close(TMP);

        print "\n\nArhivos modificados:";
        open(TMP,$NUEVO);
```

```
        while (<TMP>)
        {
                undef @dato;
                chomp $_;
                @reg=split(/\|/,$_);
                @dato=encontrar($reg[0],$ORIGINAL);
                if (@dato == 0)
                {
                        next;
                }
                elsif ($dato[1] ne $reg[1])
                {
                        print "\n$dato[0]";
                }
        }
        close(TMP);

        print "\n\nArchivos borrados:";
        open(SAL,$ORIGINAL);
        while (<SAL>)
        {
                undef @dato;
                chomp $_;
                @reg=split(/\|/,$_);
                @dato=encontrar($reg[0],$NUEVO);
                if (@dato == 0)
                {
                        print "\n$reg[0]";
                }
        }
        close(SAL);
        `rm $NUEVO`;
        `rm $ORIGINAL`;
}
```

Anexo 4. Archivo /forensics/ajustar.sh

```
#!/bin/bash
#Este script sirve para ajustar la salida del respaldo del registro de windows para hacerlo mas
trabajable
#$1 es el archivo a ajustar p.e. default.reg

if [ $# -eq 1 ]; then
        cp $1 $1.bkp #haciendo una copia del archivo original para convervarlo en el formato original
        sed -i 's/^\s$/#####/' $1 #sustutiyendo lineas en blanco con un espacio por #####
        sed -i 's/\]\r/\]####/' $1 #sustituyendo "]\r" por "]####"
        sed -i 's/\r//' $1 #eliminando todos los "\r" que en vi se ven como ^M
        perl -ne 's/,\\\n/,/g; print' < $1 > $1.tmp; mv $1.tmp $1 #eliminando saltos de linea de los
registros con valores hex, para que sean de una sola linea
        sed -i 's/,\s\s/,/g' $1 #juntar esos valores sustituyendo ",[espacio][espacio]" por ","
        sed -i '/REGEDIT4/d' $1 #eliminando la linea que contiene el patron REGEDIT4, que es la primera
        perl -ne 's/\n/\|\|/g; print' < $1 > $1.tmp; mv $1.tmp $1 #sustituyendo todos los saltos de
linea "\n" por ||, resulta en texto completamente junto
        perl -ne 's/#####\|\|/\n/g; print' < $1 > $1.tmp; mv $1.tmp $1 #sustituyendo el patron "#####||"
por salto de linea "\n"
        sed -i 's/####||/###/' $1 #sustituyendo el patron "####||" por "###"
        sed -i '/^$/d' $1 #eliminando lineas en blanco
else
        echo -e "Modo de Uso \n$0 Ruta_Dump_Registro\n"
        exit -1
fi
```

Anexo 5. Archivo /forensics/comparer.pl

```
#!/usr/bin/perl -w
#Este script hace la comparacion del registro de Windows entre orig y new, limpio y contaminado
#@ARGV[0] es el archivo original, p.e. /forensics/orig/default.reg
#@ARGV[1] es el archivo nuevo, p.e. /forensics/new/default.reg


######################################################
######   VALIDAR Y CARGAR LOS ARGUMENTOS          #####
######################################################
if (@ARGV != 2)
{
        print "Modo de Uso \n$0 Ruta_Archivo_Reg Ruta_Archivo_Reg\n";
        exit 1;
```

```
}

$ORIGINAL=$ARGV[0];
$NUEVO=$ARGV[1];

if ( -e $ORIGINAL && -e $NUEVO)
{
        comparacion();
        exit 0;
}
else
{
       print "Alguno de los archivos no existe\n";
       exit 1;
}

### Funcion para encontrar los registros dentro del archivo
sub encontrar
{
        my $file;
        my $archivo;
        $file=shift;
        $archivo=shift;
        open(AI,$archivo);
        while (<AI>)
        {
                if (/^\Q$file\E/)
                {
                        chomp($_);
                        return split(/###/,$_);
                }
        }
        return ();
}

sub encontrar_reg
{
        my $file;
        my $archivo;
        $file=shift;
        $archivo=shift;
        open(AI,$archivo);
        while (<AI>)
        {
                if (/\Q$file\E/)
                {
                        chomp($_);
                        return($_);
                }
        }
        return ('');
}

sub comparacion
{
        my @reg;
        #print "\nLlaves creadas y registros:";
        $imprime = 0;
        open(TMP,$NUEVO);
        while (<TMP>)
        {
                undef @dato;
                chomp $_;
                @reg=split(/###/,$_);
                @dato=encontrar($reg[0],$ORIGINAL);
                if (@dato == 0)
                {
                        if ( $imprime == 0 && $imprime != 1)
                        {
                                print "\nLlaves creadas y registros:";
                                $imprime = 1;
                        }
                        print "\n$reg[0]\n";
                        @registros=split(/\|\|/,$reg[1]);
                        foreach $r (@registros)
                        {
                                if ( $r ne '' )
                                {
                                        $r =~ s/\\\\/\\/g;
                                        print "\t$r\n";
                                }
```

```
                        }
                }
        }
        close(TMP);

        #print "\n\nLlaves modificadas y registros:";
        $imprime = 0;
        open(TMP,$NUEVO);
        while (<TMP>)
        {
                undef @dato;
                chomp $_;
                @reg=split(/###/,$_);
                @dato=encontrar($reg[0],$ORIGINAL);
                if (@dato == 0)
                {
                        next;
                }
                elsif ($dato[1] ne $reg[1])
                {
                        if ( $imprime == 0 && $imprime != 1)
                        {
                                print "\nLlaves modificadas y registros:";
                                $imprime = 1;
                        }
                        print "\n$dato[0]\n";
                        @registros_orig=split(/\|\|/,$dato[1]);
                        @registros_new=split(/\|\|/,$reg[1]);
                        open(ORIG,">/tmp/.orig_reg") or die "Error al BORRAR archivo temporal";
                        foreach $r (@registros_orig)
                        {
                                if ( $r ne '' )
                                {
                                        $r =~ s/\\\\/\\/g;
                                        print ORIG "$r\n";
                                }
                        }
                        close(ORIG);
                        open(NEW,">/tmp/.new_reg") or die "Error al BORRAR archivo temporal";
                        foreach $r (@registros_new)
                        {
                                if ( $r ne '' )
                                {
                                        $r =~ s/\\\\/\\/g;
                                        print NEW "$r\n";
                                }
                        }
                        close(NEW);
                        comparacion_reg("/tmp/.orig_reg","/tmp/.new_reg");
                }
        }
        close(TMP);
}

sub comparacion_reg
{
        my $original = shift;
        my $new = shift;
        my $dato;

        #print "\n\n\tRegistros creados:";
        $i = 0;
        undef @creados;
        open(TEMP,$new);
        @file = <TEMP>;
        foreach $f (@file)
        {
                undef $dato;
                chomp $f;
                $dato=encontrar_reg($f,$original);
                if ($dato eq '')
                {
                        #print "\n\t$f";
                        $creados[$i] = $f;
                        $i++;
                }
        }
        close(TEMP);
        if (@creados != 0)
        {
                print "\n\tRegistros creados:\n";
```

```
                foreach $r (@creados)
                {
                        print "\t$r\n";
                }
        }

        #print "\n\n\tRegistros modificados:";
        $i = 0;
        undef @modificados;
        open(TEMP,$new);
        @file = <TEMP>;
        foreach $f (@file)
        {
                undef $dato;
                chomp $f;
                $dato=encontrar_reg($f,$original);
                if ($dato eq '')
                {
                        next;
                }
                elsif ($dato ne $f)
               {
                        #print "\n\t$dato";
                        $modificados[$i] = $dato;
                        $i++;
                }
        }
        close(TEMP);
        if (@modificados != 0)
        {
                print "\n\tRegistros modificados:\n";
                foreach $r (@modificados)
                {
                        print "\t$r\n";
                }
        }

        #print "\n\n\tRegistros borrados:";
        $i = 0;
        undef @borrados;
        open(SAL,$original);
        @file = <SAL>;
        foreach $f (@file)
        {
                undef $dato;
                chomp $f;
                $dato=encontrar_reg($f,$new);
                if ($dato eq '')
                {
                        #print "\n\t$f";
                        $borrados[$i]=$f;
                        $i++;
                }
        }
       close(SAL);
        if (@borrados != 0)
        {
                print "\n\tRegistros borrados:\n";
                foreach $r (@borrados)
                {
                        print "\t$r\n";
                }
        }
}
```

Anexo 6. Archivo /forensics/forensics.sh

```
#!/bin/sh

#$1 imagen a cargar, p.e. ddsave.img
#$2 punto de montaje y subdirectorio de salida en /forecsics, p.e. new

HIVEPATH=/mnt/new/WINDOWS/system32/config

if [ -e /tmp/go.txt ]; then
        /fauxservers/stop.sh 2> /dev/null
        /usr/local/apache2/bin/apachectl stop
        FILENAME=`cat /tmp/go.txt`
       FPATH=/results/${FILENAME}-files
        rm -f /tmp/go.txt
```

```
        rm /tmp/*.bin 2> /dev/null
        rm /forensics/new/* 2> /dev/null
        mount -o loop -r -t ntfs /images/ddsave.img /mnt/new
        mkdir -p $FPATH
        echo -e "================================= Reporte TRUMAN ====================================="
> $FPATH/Reporte_${FILENAME}.txt
        echo >> $FPATH/Reporte_${FILENAME}.txt
        echo "Binario: $FILENAME" >> $FPATH/Reporte_${FILENAME}.txt
        echo Firma MD5: `md5sum /forensics/exes/$FILENAME | awk '{print $1}'` >>
$FPATH/Reporte_${FILENAME}.txt
        echo Firma SHA1: `sha1sum /forensics/exes/$FILENAME | awk '{print $1}'` >>
$FPATH/Reporte_${FILENAME}.txt
        #cd /mnt/new
        #sed 's/\/mnt\/orig/C:/g' -e 's/\//\\/g' /forensics/orig/orig.md5 > /forensics/orig/orig.md5.res
        #rm /forensics/orig/orig.md5
        #mv /forensics/orig/orig.md5.res /forensics/orig/orig.md5

        echo -e "\n--------------------------------------------------------------------------------------
-" >> $FPATH/Reporte_${FILENAME}.txt

        #Realizando la comparacion del sistema de archivos y de acuerdo a los archivos diferenciados
        perl /forensics/compare.pl -x /mnt/new | sed 's/\//\\/g' | grep -v -f /forensics/patternsfs.txt
> /forensics/new/.reporte.tmp
        sleep 5
        cat /forensics/new/.reporte.tmp >> $FPATH/Reporte_${FILENAME}.txt
        rm /forensics/new/.reporte.tmp
        #Realizando el volcado del registro de windows
        dumphive $HIVEPATH/default /forensics/new/default.reg
        dumphive $HIVEPATH/software /forensics/new/software.reg
        dumphive $HIVEPATH/system /forensics/new/system.reg

        #Ajustando los volcados para dejarlos de la forma: Llave###Valores
        /forensics/ajustar.sh /forensics/new/default.reg
        /forensics/ajustar.sh /forensics/new/software.reg
        /forensics/ajustar.sh /forensics/new/system.reg

        #Extrayendo archivos de procesos y puertos en escucha
        cp /mnt/new/psnew.txt /forensics/new/psnew.txt.bkp
        cp /mnt/new/netnew.txt /forensics/new/netnew.txt.bkp

        #para pslist
        #sed -e '/^\s$/d' -e '/Process\sinformation/d' -e '/CPU\sTime/d' /mnt/new/psnew.txt | awk
'{print $1}' | egrep -v "(cmd|pslist|sleep)" > /forensics/new/psnew.txt

        #para tasklist
        sed -e '/^\s$/d' -e '/Nombre\sde\simagen/d' -e '/=========/d' -e 's/\sI/I/g' -e 's/\sP/P/g'
/mnt/new/psnew.txt | awk '{print $1}' | egrep -v "(cmd\.exe|tasklist\.exe|sleep\.exe|wuauclt\.exe)" >
/forensics/new/psnew.txt

        #sed -e '/^\s$/d' -e '/Conexiones\sactivas/d' -e '/Proto/d' /mnt/new/netnew.txt | awk '{print
$1,"|",$2,"|",$3,"|",$4}' | sed 's/\s//g' > /forensics/new/netnew.txt
        sed -e '/^\s$/d' -e '/Conexiones\sactivas/d' -e '/Proto/d' /mnt/new/netnew.txt | grep -v
"127\.0\.0\.1" | sed 's/^\s\s//g' > /forensics/new/netnew.txt

        diff /forensics/orig/psorig.txt /forensics/new/psnew.txt | grep "> " | sed 's/>\s//g' >
/tmp/process.txt
        perl /forensics/finder.pl /forensics/orig/psorig.txt /tmp/process.txt > /tmp/process.txt.bkp
        if test -s /tmp/process.txt.bkp
        then
                echo -e "\n--------------------------------------------------------------------------------
---------" >> $FPATH/Reporte_${FILENAME}.txt
                echo -e "\nProcesos levantados:\n" >> $FPATH/Reporte_${FILENAME}.txt
                cat /tmp/process.txt.bkp | grep -v "logon\.scr" >> $FPATH/Reporte_${FILENAME}.txt
        fi
        rm /tmp/process.txt /tmp/process.txt.bkp

        diff /forensics/orig/netorig.txt /forensics/new/netnew.txt | grep "> " | sed 's/>\s//g' >
/tmp/network.txt
        perl /forensics/finder.pl /forensics/orig/netorig.txt /tmp/network.txt > /tmp/network.txt.bkp
        if test -s /tmp/network.txt.bkp
        then
                echo -e "\n--------------------------------------------------------------------------------
---------" >> $FPATH/Reporte_${FILENAME}.txt
                echo -e "\nConexiones activas:\n" >> $FPATH/Reporte_${FILENAME}.txt
                echo -e "Proto  Direccion Local        Direccion Remota       Estado\n" >>
$FPATH/Reporte_${FILENAME}.txt
                cat /tmp/network.txt.bkp >> $FPATH/Reporte_${FILENAME}.txt
        fi
        rm /tmp/network.txt /tmp/network.txt.bkp

        #Comparando las direfencias entre los volcados de registro
```

```
        echo -e "\n--------------------------------------------------------------------------------------------
" >> $FPATH/Reporte_${FILENAME}.txt
        echo -e "\nInforme de Registros en \\HKEY_LOCAL_MACHINE\\DEFAULT :" >>
$FPATH/Reporte_${FILENAME}.txt
        #diff /forensics/orig/default.reg /forensics/new/default.reg | grep "> " | sed 's/>\s//g' | grep
-v -f /forensics/patternsrg.txt > /forensics/new/.default.reg.temp
        #perl /forensics/comparer.pl /forensics/orig/default.reg /forensics/new/.default.reg.temp >>
$FPATH/Reporte_${FILENAME}.txt
        #rm /forensics/new/.default.reg.temp
        diff --text /forensics/orig/default.reg /forensics/new/default.reg | grep "< " | sed 's/<\s//g'
| grep -v -f /forensics/patternsrg.txt > /tmp/orig.default.reg
        diff --text /forensics/orig/default.reg /forensics/new/default.reg | grep "> " | sed 's/>\s//g'
| grep -v -f /forensics/patternsrg.txt > /tmp/new.default.reg
        perl /forensics/comparer.pl /tmp/orig.default.reg /tmp/new.default.reg > /tmp/default.rep
        if [ -s /tmp/default.rep ]; then
                cat /tmp/default.rep >> $FPATH/Reporte_${FILENAME}.txt
        else
                echo -e "\nNo se detectaron diferencias" >> $FPATH/Reporte_${FILENAME}.txt
        fi
        rm /tmp/orig.default.reg /tmp/new.default.reg /tmp/default.rep

        echo -e "\n--------------------------------------------------------------------------------------------
" >> $FPATH/Reporte_${FILENAME}.txt
        echo -e "\nInforme de Registros en \\HKEY_LOCAL_MACHINE\\SOFTWARE :" >>
$FPATH/Reporte_${FILENAME}.txt
        #diff /forensics/orig/software.reg /forensics/new/software.reg | grep "> " | sed 's/>\s//g' |
grep -v -f /forensics/patternsrg.txt > /forensics/new/.software.reg.temp
        #perl /forensics/comparer.pl /forensics/orig/software.reg /forensics/new/.software.reg.temp >>
$FPATH/Reporte_${FILENAME}.txt
        #rm /forensics/new/.software.reg.temp
        diff --text /forensics/orig/software.reg /forensics/new/software.reg | grep "< " | sed 's/<\s//g'
| grep -v -f /forensics/patternsrg.txt > /tmp/orig.software.reg
        diff --text /forensics/orig/software.reg /forensics/new/software.reg | grep "> " | sed
's/>\s//g' | grep -v -f /forensics/patternsrg.txt > /tmp/new.software.reg
        perl /forensics/comparer.pl /tmp/orig.software.reg /tmp/new.software.reg > /tmp/software.rep
        if [ -s /tmp/software.rep ]; then
                cat /tmp/software.rep >> $FPATH/Reporte_${FILENAME}.txt
        else
                echo -e "\nNo se detectaron diferencias" >> $FPATH/Reporte_${FILENAME}.txt
        fi
        rm /tmp/orig.software.reg /tmp/new.software.reg /tmp/software.rep

        echo -e "\n--------------------------------------------------------------------------------------------
" >> $FPATH/Reporte_${FILENAME}.txt
        echo -e "\nInforme de Registros en \\HKEY_LOCAL_MACHINE\\SYSTEM :" >>
$FPATH/Reporte_${FILENAME}.txt
        #diff /forensics/orig/system.reg /forensics/new/system.reg | grep "> " | sed 's/>\s//g' | grep -
v -f /forensics/patternsrg.txt | grep -i "system\\\controlset002\\\services" >
/forensics/new/.system.reg.temp
        #perl /forensics/comparer.pl /forensics/orig/system.reg /forensics/new/.system.reg.temp >>
$FPATH/Reporte_${FILENAME}.txt
        #rm /forensics/new/.system.reg.temp
        diff --text /forensics/orig/system.reg /forensics/new/system.reg | grep "< " | sed 's/<\s//g' |
grep -v -f /forensics/patternsrg.txt | grep -i "system\\\controlset002\\\services" > /tmp/orig.system.reg
        diff --text /forensics/orig/system.reg /forensics/new/system.reg | grep "> " | sed 's/>\s//g' |
grep -v -f /forensics/patternsrg.txt | grep -i "system\\\controlset002\\\services" > /tmp/new.system.reg
        perl /forensics/comparer.pl /tmp/orig.system.reg /tmp/new.system.reg > /tmp/system.rep
        if [ -s /tmp/system.rep ]; then
                cat /tmp/system.rep >> $FPATH/Reporte_${FILENAME}.txt
        else
                echo -e "\nNo se detectaron diferencias" >> $FPATH/Reporte_${FILENAME}.txt
        fi
        rm /tmp/orig.system.reg /tmp/new.system.reg /tmp/system.rep

        #echo -e "\n" >> $FPATH/Reporte_${FILENAME}.txt

        #script para el analisis de trafico
        /forensics/traffic.sh /tmp/sandnet.pcap

        echo -e "\n--------------------------------------------------------------------------------------------
-" >> $FPATH/Reporte_${FILENAME}.txt
        echo -e "\nAnalisis de trafico\n" >> $FPATH/Reporte_${FILENAME}.txt

        if [ -s /tmp/.report_traffic ]; then
                cat /tmp/.report_traffic >> $FPATH/Reporte_${FILENAME}.txt
        else
        echo -e "\nEl analisis de trafico no arrojo resultados" >> $FPATH/Reporte_${FILENAME}.txt
        fi

        echo -e "\n" >> $FPATH/Reporte_${FILENAME}.txt
```

```
        umount /mnt/new;
        #/fauxservers/stop.sh 2> /dev/null
        cp /tmp/sandnet.pcap /results/capturas/${FILENAME}.pcap 2> /dev/null

        perl /forensics/mailreport.pl "$FILENAME" "$FPATH/Reporte_${FILENAME}.txt"

        scp -r -q $FPATH/ malware-unam@quimera.seguridad.unam.mx:/home/malware-unam/TRUMAN/Reportes/

        /usr/local/apache2/bin/apachectl start

fi
```

Anexo 7. Archivo /forensics/traffic.sh

```
#!/bin/bash
#Toma un archivo (arg[1]), o todos los pcap en un directorio
#Genera reporte
#Requiere Snort 2.8.4.1 o superior

#----------------------VARIABLES---------------------------
#Localizacion de snort:
snort_loc=/usr/local/bin/snort

#Archivo de configuracion de snort
snort_conf=/etc/snort/snort.conf
#----------------------------------------------------------

#Revision de integridad de argumentos
if [[ $# -ge 2 || $# -eq 0 || $1 == "--help" ]]; then
        echo "Uso: ./traffic captura.pcap"
        exit 1
        fi

        #inicializacion del archivo de reporte
        echo -ne "" > /tmp/.report_traffic

        #Si tenemos argumento valido:
        #Snort sobre el archivo de captura, genera alert
        echo "Snort procesando..."
        $snort_loc -r $1 -l /tmp/ -c $snort_conf -b &> /dev/null
        #$snort_loc -r $1 -l /tmp/ -c $snort_conf -b
        echo "Listo. 1"

        #Voy a limpiar el alert porque esta lleno de repetidos


        #Busca IP, la imprime con el numero de conexiones
        grep -E "([0-9]{1,3}\.){3}[0-9]{1,3}:80" /tmp/alert | awk 'gsub(":80","",$4) {print $4}' | uniq
-c > /tmp/.http
        grep -E "([0-9]{1,3}\.){3}[0-9]{1,3}:21" /tmp/alert | awk 'gsub(":21","",$4) {print $4}' | uniq
-c > /tmp/.ftp
        awk '/^\[\*\*\].*IRC/{getline; getline; print}' /tmp/alert | awk 'gsub(":","\t",$4)
gsub(":","\t",$2) {print $2"\t"$4}' | uniq -c > /tmp/.ircs
        awk '/Otro puerto/{getline; getline; print}' /tmp/alert | awk 'gsub(":","\t",$4)
gsub(":","\t",$2) {print $2"\t"$4}' | uniq -c > /tmp/.otros

        #Generando reporte
        echo "Generando Reporte"
        #echo -ne "Servidores http contactados:\n\n" > /tmp/.report_traffic
        while read http
        do
                serv=`echo $http | awk '{print $2}'`
                dom=`nslookup $serv | grep -w name | awk '{print $4}' | sed 's/\.$//' | awk '{print $0"
"}'`
                echo -ne "\t$dom($serv)\n" >> /tmp/.https
        done < /tmp/.http
        sort /tmp/.https | grep -v "4\.5\.6\." | uniq >> /tmp/.httpss
        if test -s /tmp/.httpss
        then
                echo -ne "Servidores http contactados:\n\n" > /tmp/.report_traffic
                cat /tmp/.httpss >> /tmp/.report_traffic
                echo -ne "\n" >> /tmp/.report_traffic
        fi

        #echo -ne "Servidores ftp contactados:\n\n" >> /tmp/.report_traffic
        while read ftp
        do
                serv=`echo $ftp | awk '{print $2}'`
                dom=`nslookup $serv | grep -w name | awk '{print $4}' | sed 's/\.$//' | awk '{print $0"
"}'`
                echo -ne "\t$dom($serv)\n" >> /tmp/.ftps
```

```
        done < /tmp/.ftp
if test -s /tmp/.ftps ; then sort /tmp/.ftps | uniq >> /tmp/.ftpss ; fi
if test -s /tmp/.ftpss
then
        echo -ne "Servidores ftp contactados:\n\n" >> /tmp/.report_traffic
        cat /tmp/.ftpss >> /tmp/.report_traffic
        echo -ne "\n" >> /tmp/.report_traffic
fi

#echo -ne "Servidores IRC contactados:\n\n" >> /tmp/.report_traffic
while read irc
do
        serv=`echo $irc | awk '{print $4}'`
        data=`echo $irc | awk '{print "puerto origen: "$3"; puerto destino: "$5}'`
        dom=`nslookup $serv | grep -w name | awk '{print $4}' | sed 's/\.$//' | awk '{print $0" "}'`
        echo -ne "$dom($serv) con $data\n" >> /tmp/.ircss

done < /tmp/.ircs
if test -s /tmp/.ircss ; then sort /tmp/.ircss | uniq >> /tmp/.ircsss ; fi
if test -s /tmp/.ircsss
then
        echo -ne "Servidores IRC contactados:\n\n" >> /tmp/.report_traffic
        cat /tmp/.ircss | awk '{print "\t" $0}' >> /tmp/.report_traffic
        echo -ne "\n" >> /tmp/.report_traffic
fi

echo "Listo. 2"


#Proceso para sacar flujos - en gran parte para saber los nombres de archivo...
#echo -ne "Informacion de Conexiones IRC\n\n" >> /tmp/.report_traffic
ct=1
while read pareja
do

        tcpflow -r $1 "(src host `echo $pareja | awk '{print $2}'` and src port `echo $pareja | awk
'{print $3}'` and dst host `echo $pareja | awk '{print $4}'` and dst port `echo $pareja | awk '{print
$5}'`) or (src host `echo $pareja | awk '{print $4}'` and src port `echo $pareja | awk '{print $5}'` and
dst host `echo $pareja | awk '{print $2}'` and dst port `echo $pareja | awk '{print $3}'`)"

        tcpflow -c -r $1 "(src host `echo $pareja | awk '{print $2}'` and src port `echo $pareja | awk
'{print $3}'` and dst host `echo $pareja | awk '{print $4}'` and dst port `echo $pareja | awk '{print
$5}'`) or (src host `echo $pareja | awk '{print $4}'` and src port `echo $pareja | awk '{print $5}'` and
dst host `echo $pareja | awk '{print $2}'` and dst port `echo $pareja | awk '{print $3}'`)" >
/tmp/.tcpflow

        echo $pareja | awk '{print $2}' | awk -F . '{print $1"\n"$2"\n"$3"\n"$4}' > /tmp/.ip_clt
        ip=""
        while read oct
        do
                if [ `echo $oct | wc -c` == 2 ]; then
                        ip="${ip}00${oct}."
                elif [ `echo $oct | wc -c` == 3 ]; then
                        ip="${ip}0${oct}."
                else
                        ip="${ip}${oct}."
                fi
        done < /tmp/.ip_clt
        ip=`echo $ip | sed 's/\.$//g'`
        ls -l $ip* | awk '{print $8}' > /tmp/.flujos
        while read flujo
        do
                srv=`echo $flujo | awk -F "-" '{print $2}'`
                clt=`echo $flujo | awk -F "-" '{print $1}'`
                echo -ne "\tConexion $ct: \n\n" >> /tmp/.irc_connections
                #echo -ne "\t" >> /tmp/.irc_connections
                cat $clt-$srv >> /tmp/.irc_connections
                echo -ne "\n" >> /tmp/.irc_connections
                cat $clt-$srv >> /tmp/.irc_connections
                echo -ne "\n" >> /tmp/.irc_connections
                #cat $srv-$clt | awk '{print "\t\t" $0}' >> /tmp/.irc_connections
                #cat $srv-$clt | awk '{print "\t\t" $0}' >> /tmp/.irc_connections
                rm $clt-$srv $srv-$clt
        done < /tmp/.flujos
        ct=`expr $ct + 1`
done < /tmp/.ircs
if test -s /tmp/.irc_connections
then
        echo -ne "Informacion de Conexiones IRC\n\n" >> /tmp/.report_traffic
        cat /tmp/.irc_connections >> /tmp/.report_traffic
        echo -ne "\n\n" >> /tmp/.report_traffic
```

```
fi

echo "Listo. 3"

#echo -ne "Otras conexiones:\n\n" >> /tmp/.report_traffic
cat /tmp/.otros | awk '{print $2" "$3" "$4" "$5}' > /tmp/.otross
cat /tmp/.ircs | awk '{print $2" "$3" "$4" "$5}' > /tmp/.ircss
grep -v -f /tmp/.ircss /tmp/.otross > /tmp/.otrosss
while read otro
do
        if [[ `echo $otro | awk '{print $3}'` != `echo $ip | sed -r -e 's/^0+//' -e 's/.0+/./g'` &&
`echo $otro | awk '{print $3}'` != "4.5.6.7" ]]; then
                echo "A `echo $otro | awk '{print $3}' | nslookup | grep -w name | awk '{print $4}' |
sed 's/\.$//'` (IP `echo $otro | awk '{print $3}'`, puerto `echo $otro | awk '{print $2}'`) desde el
puerto `echo $otro | awk '{print $4}'`" >> /tmp/.otrosssss
        fi
done < /tmp/.otrosss
if test -s /tmp/.otrosssss
then
        echo -ne "Otras conexiones:\n\n" >> /tmp/.report_traffic
        cat /tmp/.otrosssss >> /tmp/.report_traffic
#       echo -ne "\n\n" >> /tmp/.report_traffic
fi
rm /tmp/alert /tmp/.http /tmp/.https /tmp/.httpss /tmp/.ftp /tmp/.ftps /tmp/.ftpss /tmp/.ircs /tmp/.ircss
/tmp/.ircsss /tmp/.irc_connections /tmp/.flujos /tmp/.otros /tmp/.otross /tmp/.otrosss /tmp/.otrosssss
/tmp/.ip_clt /tmp/snort* 2> /dev/null
```

Anexo 8. Archivos varios

Archivo /etc/init.d/services.sh.

```
#!/bin/bash

while [ 1 ]
do

        state=`cat /fauxservers/start.flag`;

        if [ "${state}" == "10" ];
        then
                /fauxservers/start.sh > /dev/null 2> /dev/null;
                echo "00" > /fauxservers/start.flag;
                # echo "$state";
        fi
        if [ "${state}" == "11" ];
        then
                /fauxservers/stop.sh > /dev/null 2> /dev/null
                /forensics/forensics.sh > /dev/null 2> /dev/null
                echo "00" > /fauxservers/start.flag;
                # echo "$state";
        fi
done
```

Archivo /fauxservers/start.sh

```
#!/bin/sh

tcpdump -c 10000 -n -l -i eth1 -s 1514 -w /tmp/sandnet.pcap not port 45612 and not port 45611 &
/etc/init.d/nat up
```

Archivo /fauxservers/stop.sh

```
#!/bin/sh

tcpdump -c 10000 -n -l -i eth1 -s 1514 -w /tmp/sandnet.pcap not port 45612 and not port 45611 &
/etc/init.d/nat up
```

Archivo /usr/local/apache2/cgi-bin/truman.cgi

```
#!/usr/bin/perl

## truman.cgi
```

```
##
## (c)2006 Joe Stewart <jstewart@lurhq.com>
##
## Handles cycling of the Truman boot parameters and script control

use CGI;
use strict;

$| = 1;
my $queue = "/forensics/queue";
my $postqueue = "/forensics/exes/";

my $q = new CGI;
my $res = $q->param('res');
my $func = $q->param('func');

if ($func eq "dequeue")
{
        opendir(DIR, $queue) or die "can't opendir $queue : $!\n";
        my $file;
        my $size;
        while ( defined ($file = readdir(DIR)) )
        {
            next if $file =~ /^\.\.?$/;
            $size = (stat("$queue/$file"))[7];
            if ($size)
            {
                print "Content-Length: $size\n";
                print "Content-Type: application/x-executable\n\n";
                open(IN,"$queue/$file") or die "Can't open $file : $!\n";
                my $buf;
                system("/bin/echo \"10\" > /fauxservers/start.flag");
                system("/bin/cp /tftpboot/pxelinux.cfg/truman /tftpboot/pxelinux.cfg/default > /dev/null
2> /dev/null");
                while(!eof(IN))
                {
                        read(IN,$buf,1024);
                        print $buf;
                }
            close IN;
            system("mv $queue/$file $postqueue");
            open(OUT,">/tmp/current.txt");
            print OUT $file;
            close OUT;
            closedir(DIR);
            exit;
            }
        }
        # nothing in queue, send a 0-byte response
        closedir(DIR);
        print "Content-Length: 0\n";
        print "Content-Type: application/x-executable\n\n";
        exit;
}
if ($res eq "restoresuccess")
{
        # make normal boot the default
        system("/bin/cp /tftpboot/pxelinux.cfg/normalboot /tftpboot/pxelinux.cfg/default");
}
elsif ($res eq "savesuccess")
{
        # give forensic scripts the go-ahead
        system("/bin/mv /tmp/current.txt /tmp/go.txt");
        system("/bin/echo \"11\" > /fauxservers/start.flag");
        system("/bin/cp /tftpboot/pxelinux.cfg/normalboot /tftpboot/pxelinux.cfg/default");
}
elsif ($res eq "booted")
{
        # make truman boot the default
        system("/bin/cp /tftpboot/pxelinux.cfg/truman /tftpboot/pxelinux.cfg/default");
}
print "Content-type: text/html\n\n";
print "Ok\n";
```

Archivo /etc/init.d/nat

```
#!/bin/sh

IPTABLES="/sbin/iptables"
```

```
case $1 in

  up )
        #para habilitar la repeticion y el cliente pueda realizar consultas a internet
        /bin/echo 1 > /proc/sys/net/ipv4/ip_forward

        #para borar todas las reglas previas
        $IPTABLES -F
        $IPTABLES -X
        $IPTABLES -Z
        $IPTABLES -t nat -F

        #Estableciendo politica por defecto
        $IPTABLES -P INPUT ACCEPT
        $IPTABLES -P OUTPUT ACCEPT
        $IPTABLES -P FORWARD ACCEPT
        $IPTABLES -t nat -P PREROUTING ACCEPT
        $IPTABLES -t nat -P POSTROUTING ACCEPT

        # Habilita el NAT
        $IPTABLES -t nat -A POSTROUTING -s 4.5.6.0/24 -d 0.0.0.0/0 -j MASQUERADE
        # Deja pasar los paquetes ICMP
        $IPTABLES -A INPUT -i eth0 -p ICMP -j ACCEPT
        # Permite conexiones al puerto 80 (HTTP)
        $IPTABLES -A INPUT -i eth0 -p TCP --dport 80 -m state --state NEW -j ACCEPT
        # Permite conexiones al puerto 22 (SSH)
        $IPTABLES -A INPUT -i eth0 -p TCP --dport 22 -m state --state NEW -j ACCEPT
        # Acepta comsultas a DSN
        $IPTABLES -A OUTPUT -o eth0 -p UDP --dport 53 -j ACCEPT
        # Acepta paquetes de conexiones ya establecidas
        $IPTABLES -A INPUT -i eth0 -p TCP -m state --state RELATED -j ACCEPT
        # Rechaza paquetes de conexiones nuevas
        $IPTABLES -A INPUT -i eth0 -m state --state NEW,INVALID -j DROP
        # Rechazamos paquetes de forwarding de conexiones no establecidas
        $IPTABLES -A FORWARD -i eth0 -m state --state NEW,INVALID -j DROP

        #Bloquea trafico de salida hacia IPs privadas o locales
        $IPTABLES -A OUTPUT -o eth0 -p TCP -m state --state NEW,INVALID -d 10.0.0.0/8 -j DROP
        $IPTABLES -A OUTPUT -o eth0 -p UDP -d 10.0.0.0/8 -j DROP
        $IPTABLES -A OUTPUT -o eth0 -p TCP -m state --state NEW,INVALID -d 172.16.0.0/16 -j DROP
        $IPTABLES -A OUTPUT -o eth0 -p UDP -d 172.16.0.0/16 -j DROP
        $IPTABLES -A OUTPUT -o eth0 -p TCP -m state --state NEW,INVALID -d 192.168.0.0/16 -j DROP
        $IPTABLES -A OUTPUT -o eth0 -p UDP -d 192.168.0.0/16 -j DROP
        ;;

  down )
        #para deshabilitar la repeticion y el cliente pueda realizar consultas a internet
        /bin/echo 0 > /proc/sys/net/ipv4/ip_forward

        #para borar todas las reglas previas
        $IPTABLES -F
        $IPTABLES -X
        $IPTABLES -Z
        $IPTABLES -t nat -F
        ;;

  * )
        echo "Opcion no existente"
        ;;

esac
```

Anexo 9. Archivo /forensics/mailreport.pl

```
#!/usr/bin/perl

open (MAIL,"|/usr/lib/sendmail -t");
print MAIL "To: jduran\@seguridad.unam.mx\n";
print MAIL "From: truman_unam-cert\n";

print MAIL "Subject: Analisis del Malware @ARGV[0], TRUMAN UNAM-CERT\n\n";

$reporte=`cat @ARGV[1]`;

print MAIL $reporte;

close MAIL;
```

Anexo 10. Tutorial relaciones de confianza con SSH.

Si se está constantemente administrando servidores de manera remota, le parecerá molesto estar tecleando las extensas contraseñas que se seleccionan con el fin de lograr una alta seguridad. Sin embargo, es posible crear confianza entre dos equipos de manera que no se tenga que volver a teclear nunca más la contraseña y sin perder seguridad.

Para crear confianza entre dos equipos es necesario crear una llave pública y agregarla al archivo *authorized_keys* del equipo remoto. Por ejemplo, imaginar que el usuario "manuel" está en una WorkStation NetBSD cuyo hostname es "andromeda" y desea conectarse al equipo "mononeurona.org" usando la cuenta de usuario "httpuser". Los pasos serían los siguientes. Se crea la llave pública con el comando keygen-ssh (cuando le pregunte la frase sólo de *enter*):

```
$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/manuel/.ssh/id_dsa):
Created directory '/home/manuel/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/manuel/.ssh/id_dsa.
Your public key has been saved in /home/manuel/.ssh/id_dsa.pub.
The key fingerprint is:
ca:6d:4e:6c:f5:fd:10:3b:59:7b:11:80:59:7d:8b:54 manuel@andromeda
```

Ahora se copia la llave pública al equipo remoto:

```
$ scp .ssh/id_dsa.pub
httpuser@mononeurona.org:/home/httpuser/.ssh/andromeda_id_dsa.pub
```

Se ingresa al otro equipo, tecleando la contraseña por última vez.

```
$ ssh httpuser@mononeurona.org
```

Una vez adentro, se inserta el archivo con nuestra llave pública al archivo "*authorized_keys*".

```
$ cat .ssh/andromeda_id_dsa.pub >> .ssh/authorized_keys
```

Se realiza la comprobación de los permisos. El directorio ".ssh" debe tener permisos de ejecución y lectura pero no de escritura.

```
$ chmod 555 .ssh && chmod 644 .ssh/authorized_keys
```

Nos salimos del servidor remoto con *exit* y volvemos a teclear.

```
$ ssh httpuser@mononeurona.org
```

Por último se tendrá la capacidad de entrar automáticamente sin teclear nada.

Anexo 10. Muestra de un reporte generado por la herramienta.

========== Reporte TRUMAN ==========

Binario: urdvxc.exe
Firma MD5: 10e0bcf74ff73f508c2aa6e8640dff99
Firma SHA1: f603b19309adc848141f1482f73600a49495be24

Archivos creados:
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\clbvvlrs.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\clxlczxq.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\ejthwsbr.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\esjkbccv.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\lbexzkbk.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\lzjvxjel.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\njwrczcc.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\nsekrlvz.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\ntwwcbnq.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\sbwrkxcs.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\stttklte.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\ttkklzcs.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\xclsclbs.exe
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\xtxvnrex.exe
C:\Archivos de programa\Archivos comunes\System\ado\scjejqze.exe
C:\Archivos de programa\NetMeeting\xksjxljj.exe
C:\Archivos de programa\VMware\VMware Tools\Guest
SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\cnrstqbb.exe
C:\Archivos de programa\VMware\VMware Tools\Guest
SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\htvtlchz.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\eznnthwj.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\hjkbllwk.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\jllslbnb.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\jnkwrxnr.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\knhbwsnv.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\krhwtjeh.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\lhvclnlt.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\rvjbkxtl.exe
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\zhqvnthb.exe
C:\WINDOWS\system32\oobe\actsetup\blvccbsx.exe
C:\WINDOWS\system32\oobe\actsetup\brvecwcs.exe
C:\WINDOWS\system32\oobe\actsetup\btesnnel.exe
C:\WINDOWS\system32\oobe\actsetup\btqkxenz.exe
C:\WINDOWS\system32\oobe\actsetup\cwbbnetr.exe
C:\WINDOWS\system32\oobe\actsetup\hlrrerkq.exe
C:\WINDOWS\system32\oobe\actsetup\knkskthw.exe
C:\WINDOWS\system32\oobe\actsetup\lrlzztll.exe
C:\WINDOWS\system32\oobe\actsetup\nzzwhebn.exe
C:\WINDOWS\system32\oobe\actsetup\rkjenssc.exe
C:\WINDOWS\system32\oobe\actsetup\rrthsntk.exe
C:\WINDOWS\system32\oobe\actsetup\tchekrqt.exe
C:\WINDOWS\system32\oobe\actsetup\vrrkkhbn.exe
C:\WINDOWS\system32\oobe\actsetup\zvswnlev.exe
C:\WINDOWS\system32\oobe\cthsnblj.exe
C:\WINDOWS\system32\oobe\error\ektltnch.exe
C:\WINDOWS\system32\oobe\error\erettxjr.exe
C:\WINDOWS\system32\oobe\error\jkhehnjn.exe
C:\WINDOWS\system32\oobe\error\kbwnhlkk.exe
C:\WINDOWS\system32\oobe\error\lktkttrb.exe
C:\WINDOWS\system32\oobe\error\neehnzxl.exe
C:\WINDOWS\system32\oobe\error\sswzlttc.exe
C:\WINDOWS\system32\oobe\error\xenjnbqe.exe
C:\WINDOWS\system32\oobe\html\dslmain\nevttblh.exe
C:\WINDOWS\system32\oobe\html\dslmain\qxztllwj.exe
C:\WINDOWS\system32\oobe\html\dslmain\slhcezwb.exe
C:\WINDOWS\system32\oobe\html\iconnect\jsnsljzh.exe
C:\WINDOWS\system32\oobe\html\iconnect\shrtrsbs.exe
C:\WINDOWS\system32\oobe\html\isptype\lnvlnzbq.exe
C:\WINDOWS\system32\oobe\html\mouse\bccxejnc.exe
C:\WINDOWS\system32\oobe\html\mouse\bzrbbsrn.exe
C:\WINDOWS\system32\oobe\html\mouse\cjxsjlbr.exe
C:\WINDOWS\system32\oobe\html\mouse\hcvxrtwz.exe
C:\WINDOWS\system32\oobe\html\mouse\jjlhknhh.exe
C:\WINDOWS\system32\oobe\html\mouse\jlkshlvl.exe
C:\WINDOWS\system32\oobe\html\mouse\khkvhhsb.exe
C:\WINDOWS\system32\oobe\html\mouse\klkhkrts.exe
C:\WINDOWS\system32\oobe\html\mouse\lbzcxver.exe
C:\WINDOWS\system32\oobe\html\mouse\nrlcnzsh.exe
C:\WINDOWS\system32\oobe\html\mouse\qetvqlnw.exe
C:\WINDOWS\system32\oobe\html\mouse\rbnrnnxt.exe
C:\WINDOWS\system32\oobe\html\sconnect\jkhjlhbb.exe
C:\WINDOWS\system32\oobe\html\sconnect\vznnebet.exe
C:\WINDOWS\system32\oobe\icserror\vcejlxkt.exe
C:\WINDOWS\system32\oobe\isperror\hkenntsl.exe
C:\WINDOWS\system32\oobe\isperror\jjtrkbnj.exe
C:\WINDOWS\system32\oobe\isperror\knkbrnbn.exe
C:\WINDOWS\system32\oobe\isperror\ktkbeknl.exe
C:\WINDOWS\system32\oobe\isperror\rkeetqew.exe
C:\WINDOWS\system32\oobe\isperror\skqbvxsq.exe
C:\WINDOWS\system32\oobe\isperror\tsjhshcj.exe
C:\WINDOWS\system32\oobe\isperror\ztceskls.exe
C:\WINDOWS\system32\oobe\krcxzncj.exe
C:\WINDOWS\system32\oobe\qjeejeej.exe
C:\WINDOWS\system32\oobe\regerror\cetrjwtt.exe
C:\WINDOWS\system32\oobe\regerror\ehxzeshx.exe
C:\WINDOWS\system32\oobe\regerror\etnwxxnv.exe
C:\WINDOWS\system32\oobe\regerror\kjtzrlbb.exe
C:\WINDOWS\system32\oobe\regerror\rcwnttzv.exe
C:\WINDOWS\system32\oobe\regerror\wlkbbnrq.exe
C:\WINDOWS\system32\oobe\regerror\wtkkxrlr.exe

C:\WINDOWS\system32\oobe\regerror\xcjnkske.exe
C:\WINDOWS\system32\oobe\setup\bknkjheh.exe
C:\WINDOWS\system32\oobe\setup\bvqncler.exe
C:\WINDOWS\system32\oobe\setup\crjrhltv.exe
C:\WINDOWS\system32\oobe\setup\elrbjlrn.exe
C:\WINDOWS\system32\oobe\setup\enbsjwre.exe
C:\WINDOWS\system32\oobe\setup\esjhxblq.exe
C:\WINDOWS\system32\oobe\setup\eskcxkhr.exe
C:\WINDOWS\system32\oobe\setup\hlqstwxz.exe
C:\WINDOWS\system32\oobe\setup\hnhkkene.exe
C:\WINDOWS\system32\oobe\setup\hwncrnhh.exe
C:\WINDOWS\system32\oobe\setup\hxckwnzl.exe
C:\WINDOWS\system32\oobe\setup\hxxttskn.exe
C:\WINDOWS\system32\oobe\setup\jejrhnvh.exe
C:\WINDOWS\system32\oobe\setup\jtxsbxwn.exe
C:\WINDOWS\system32\oobe\setup\kjqkxtnz.exe
C:\WINDOWS\system32\oobe\setup\kksksesr.exe
C:\WINDOWS\system32\oobe\setup\knkhrczb.exe
C:\WINDOWS\system32\oobe\setup\lhkhbjzl.exe
C:\WINDOWS\system32\oobe\setup\lkjtrhks.exe
C:\WINDOWS\system32\oobe\setup\lnestrnt.exe
C:\WINDOWS\system32\oobe\setup\nkhlvlzt.exe
C:\WINDOWS\system32\oobe\setup\nleevxqj.exe
C:\WINDOWS\system32\oobe\setup\nstnnnkk.exe
C:\WINDOWS\system32\oobe\setup\ntwbjnxv.exe
C:\WINDOWS\system32\oobe\setup\nvbbshss.exe
C:\WINDOWS\system32\oobe\setup\nwqjkkhn.exe
C:\WINDOWS\system32\oobe\setup\rresnsct.exe
C:\WINDOWS\system32\oobe\setup\rserkten.exe
C:\WINDOWS\system32\oobe\setup\sejkhevn.exe
C:\WINDOWS\system32\oobe\setup\seqtjbee.exe
C:\WINDOWS\system32\oobe\setup\shbqjhcl.exe
C:\WINDOWS\system32\oobe\setup\tnqsbljb.exe
C:\WINDOWS\system32\oobe\setup\tqkbrhnx.exe
C:\WINDOWS\system32\oobe\setup\tthzxntk.exe
C:\WINDOWS\system32\oobe\setup\vjbssbhj.exe
C:\WINDOWS\system32\oobe\setup\vkckxhbn.exe
C:\WINDOWS\system32\oobe\setup\wnklretl.exe
C:\WINDOWS\system32\oobe\setup\wrbbnjss.exe
C:\WINDOWS\system32\oobe\setup\wtenslnj.exe
C:\WINDOWS\system32\oobe\setup\zeblsxxw.exe
C:\WINDOWS\system32\oobe\setup\zhhrrltb.exe
C:\WINDOWS\system32\oobe\setup\zhzsnhje.exe
C:\WINDOWS\system32\oobe\setup\znnhhhtk.exe
C:\WINDOWS\system32\oobe\tttnwshl.exe
C:\WINDOWS\system32\urdvxc.exe
C:\WINDOWS\Help\bzehxvnz.exe
C:\WINDOWS\Help\hwexrtne.exe
C:\WINDOWS\Help\jbnshhqj.exe
C:\WINDOWS\Help\jjlenkbt.exe
C:\WINDOWS\Help\Tours\htmlTour\klbvejnk.exe
C:\WINDOWS\Help\Tours\htmlTour\kzerbzks.exe
C:\WINDOWS\Help\Tours\htmlTour\kzkzkjkb.exe
C:\WINDOWS\Help\Tours\htmlTour\qejnhetj.exe
C:\WINDOWS\Help\Tours\htmlTour\rbnesqvr.exe
C:\WINDOWS\Help\Tours\htmlTour\rqkjqjqb.exe
C:\WINDOWS\Help\Tours\WindowsMediaPlayer\Audio\llknblj.exe
C:\WINDOWS\Help\Tours\WindowsMediaPlayer\Cnt\tjnbzhbh.exe
C:\WINDOWS\Help\tsbjbtvn.exe
C:\WINDOWS\Web\wcxnjhhj.exe

Arhivos modificados:
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Glaciar.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Ataque radial.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Bebida de limón.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Dulces.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Día luminoso.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\En blanco.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Fiesta.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Girasol.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Gráficos circulares.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Hiedra.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Hojas.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Maíz.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Naturaleza.htm
C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\Técnico.htm
C:\Archivos de programa\Archivos comunes\System\ado\MDACReadme.htm
C:\Archivos de programa\NetMeeting\netmeet.htm
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\allclasses-frame.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\allclasses-noframe.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\package-frame.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\package-summary.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\package-tree.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\VMGuestLibErrorException.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\VMGuestLibHandle.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\VMGuestLibInterface.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\constant-values.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\help-doc.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\index-all.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\index.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\overview-summary.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\overview-tree.html
C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\serialized-form.html
C:\WINDOWS\system32\oobe\actsetup\actconn.htm
C:\WINDOWS\system32\oobe\actsetup\actdone.htm

C:\WINDOWS\system32\oobe\actsetup\activ.htm
C:\WINDOWS\system32\oobe\actsetup\activerr.htm
C:\WINDOWS\system32\oobe\actsetup\activsvc.htm
C:\WINDOWS\system32\oobe\actsetup\actlan.htm
C:\WINDOWS\system32\oobe\actsetup\adeskerr.htm
C:\WINDOWS\system32\oobe\actsetup\adrdyreg.htm
C:\WINDOWS\system32\oobe\actsetup\apolicy.htm
C:\WINDOWS\system32\oobe\actsetup\aprvcyms.htm
C:\WINDOWS\system32\oobe\actsetup\areg1.htm
C:\WINDOWS\system32\oobe\actsetup\aregdial.htm
C:\WINDOWS\system32\oobe\actsetup\aregdone.htm
C:\WINDOWS\system32\oobe\actsetup\ausrinfo.htm
C:\WINDOWS\system32\oobe\actshell.htm
C:\WINDOWS\system32\oobe\dtsgnup.htm
C:\WINDOWS\system32\oobe\error\cnncterr.htm
C:\WINDOWS\system32\oobe\error\dialtone.htm
C:\WINDOWS\system32\oobe\error\hndshake.htm
C:\WINDOWS\system32\oobe\error\isp2busy.htm
C:\WINDOWS\system32\oobe\error\noanswer.htm
C:\WINDOWS\system32\oobe\error\pberr.htm
C:\WINDOWS\system32\oobe\error\pulse.htm
C:\WINDOWS\system32\oobe\error\toobusy.htm
C:\WINDOWS\system32\oobe\html\dslmain\dslmain.htm
C:\WINDOWS\system32\oobe\html\dslmain\dsl_a.htm
C:\WINDOWS\system32\oobe\html\dslmain\dsl_b.htm
C:\WINDOWS\system32\oobe\html\iconnect\icntlast.htm
C:\WINDOWS\system32\oobe\html\iconnect\iconnect.htm
C:\WINDOWS\system32\oobe\html\isptype\isptype.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_a.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_b.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_c.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_d.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_e.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_f.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_g.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_h.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_i.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_j.htm
C:\WINDOWS\system32\oobe\html\mouse\mouse_k.htm
C:\WINDOWS\system32\oobe\html\sconnect\scntlast.htm
C:\WINDOWS\system32\oobe\html\sconnect\sconnect.htm
C:\WINDOWS\system32\oobe\icserror\icsdc.htm
C:\WINDOWS\system32\oobe\isperror\ispcnerr.htm
C:\WINDOWS\system32\oobe\isperror\ispdtone.htm
C:\WINDOWS\system32\oobe\isperror\isphdshk.htm
C:\WINDOWS\system32\oobe\isperror\ispins.htm
C:\WINDOWS\system32\oobe\isperror\ispnoanw.htm
C:\WINDOWS\system32\oobe\isperror\isppberr.htm
C:\WINDOWS\system32\oobe\isperror\ispphbsy.htm
C:\WINDOWS\system32\oobe\isperror\ispsbusy.htm
C:\WINDOWS\system32\oobe\msobshel.htm
C:\WINDOWS\system32\oobe\regerror\rcnterr.htm
C:\WINDOWS\system32\oobe\regerror\rdtone.htm
C:\WINDOWS\system32\oobe\regerror\rhndshk.htm
C:\WINDOWS\system32\oobe\regerror\rnoansw.htm
C:\WINDOWS\system32\oobe\regerror\rnomdm.htm
C:\WINDOWS\system32\oobe\regerror\rpberr.htm
C:\WINDOWS\system32\oobe\regerror\rpulse.htm
C:\WINDOWS\system32\oobe\regerror\rtoobusy.htm
C:\WINDOWS\system32\oobe\setup\ident1.htm
C:\WINDOWS\system32\oobe\setup\oempriv.htm
C:\WINDOWS\system32\oobe\setup\acterror.htm
C:\WINDOWS\system32\oobe\setup\activate.htm
C:\WINDOWS\system32\oobe\setup\act_plcy.htm
C:\WINDOWS\system32\oobe\setup\autoupdt.htm
C:\WINDOWS\system32\oobe\setup\au_plcy.htm
C:\WINDOWS\system32\oobe\setup\badeula.htm
C:\WINDOWS\system32\oobe\setup\badpkey.htm
C:\WINDOWS\system32\oobe\setup\compname.htm
C:\WINDOWS\system32\oobe\setup\dialup.htm
C:\WINDOWS\system32\oobe\setup\drdyisp.htm
C:\WINDOWS\system32\oobe\setup\drdymig.htm
C:\WINDOWS\system32\oobe\setup\drdyoem.htm
C:\WINDOWS\system32\oobe\setup\drdyref.htm
C:\WINDOWS\system32\oobe\setup\dtiwait.htm
C:\WINDOWS\system32\oobe\setup\fini.htm
C:\WINDOWS\system32\oobe\setup\hnwprmpt.htm
C:\WINDOWS\system32\oobe\setup\iconn.htm
C:\WINDOWS\system32\oobe\setup\ics.htm
C:\WINDOWS\system32\oobe\setup\ident2.htm
C:\WINDOWS\system32\oobe\setup\isp.htm
C:\WINDOWS\system32\oobe\setup\ispwait.htm
C:\WINDOWS\system32\oobe\setup\jndomain.htm
C:\WINDOWS\system32\oobe\setup\jndom_a.htm
C:\WINDOWS\system32\oobe\setup\keybd.htm
C:\WINDOWS\system32\oobe\setup\keybdcmt.htm
C:\WINDOWS\system32\oobe\setup\migdial.htm
C:\WINDOWS\system32\oobe\setup\miglist.htm
C:\WINDOWS\system32\oobe\setup\migpage.htm
C:\WINDOWS\system32\oobe\setup\neweula.htm
C:\WINDOWS\system32\oobe\setup\neweula2.htm
C:\WINDOWS\system32\oobe\setup\Oobedisc.htm
C:\WINDOWS\system32\oobe\setup\prodkey.htm
C:\WINDOWS\system32\oobe\setup\prvcyms.htm
C:\WINDOWS\system32\oobe\setup\refdial.htm
C:\WINDOWS\system32\oobe\setup\reg1.htm
C:\WINDOWS\system32\oobe\setup\reg3.htm
C:\WINDOWS\system32\oobe\setup\regdial.htm
C:\WINDOWS\system32\oobe\setup\security.htm
C:\WINDOWS\system32\oobe\setup\timezone.htm
C:\WINDOWS\system32\oobe\setup\username.htm

C:\WINDOWS\system32\oobe\setup\welcome.htm
C:\WINDOWS\system32\oobe\updshell.htm
C:\WINDOWS\Help\ciadmin.htm
C:\WINDOWS\Help\ciquery.htm
C:\WINDOWS\Help\ixqlang.htm
C:\WINDOWS\Help\migwiz.htm
C:\WINDOWS\Help\migwiz2.htm
C:\WINDOWS\Help\Tours\htmlTour\best_fr.htm
C:\WINDOWS\Help\Tours\htmlTour\footer.htm
C:\WINDOWS\Help\Tours\htmlTour\safe_fr.htm
C:\WINDOWS\Help\Tours\htmlTour\start_fr.htm
C:\WINDOWS\Help\Tours\htmlTour\connected_fr.htm
C:\WINDOWS\Help\Tours\htmlTour\unlock_fr.htm
C:\WINDOWS\Help\Tours\WindowsMediaPlayer\Audio\snd.htm
C:\WINDOWS\Help\Tours\WindowsMediaPlayer\Cnt\contents.htm
C:\WINDOWS\Web\tip.htm

Archivos borrados:

Procesos levantados:

urdvxc.exe

Conexiones activas:

Proto	Direccion Local	Direccion Remota	Estado
TCP	4.5.6.7:1404	61.1.46.14:139	SYN_SENT
TCP	4.5.6.7:1405	61.1.121.9:139	SYN_SENT
TCP	4.5.6.7:1407	61.1.235.69:139	SYN_SENT
TCP	4.5.6.7:1408	61.1.166.6:139	SYN_SENT

Informe de Registros en \HKEY_LOCAL_MACHINE\DEFAULT :

No se detectaron diferencias

Informe de Registros en \HKEY_LOCAL_MACHINE\SOFTWARE :

Llaves creadas y registros:

[software\Classes\CLSID\{0026A548-2A19-E8A0-B03E-B8692A75086E}]
@="bklzwtkhbsrcrxje"

[software\Classes\CLSID\{0026A548-2A19-E8A0-B03E-B8692A75086E}\LocalServer32]
@="C:\WINDOWS\Web\wcxnjhhj.exe"

[software\Classes\CLSID\{007196C5-0DD4-0764-F61E-200F74EEE57C}]
@="zkebjblzbhnzrrhj"

[software\Classes\CLSID\{007196C5-0DD4-0764-F61E-200F74EEE57C}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\nrlcnzsh.exe"

[software\Classes\CLSID\{00A77F45-682B-8DE9-9E19-E2C9F51D8388}]
@="rentxzenjkbelbhr"

[software\Classes\CLSID\{00A77F45-682B-8DE9-9E19-E2C9F51D8388}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\kksksesr.exe"

[software\Classes\CLSID\{03F7EF8A-104D-1443-9F1B-069899745744}]
@="tbvhhztrhkekrtnw"

[software\Classes\CLSID\{03F7EF8A-104D-1443-9F1B-069899745744}\LocalServer32]
@="C:\WINDOWS\system32\oobe\qjeejeej.exe"

[software\Classes\CLSID\{048BF78C-E618-0789-65EC-7B42EEBABDDC}]
@="zkvrzhrvljzqzxjl"

[software\Classes\CLSID\{048BF78C-E618-0789-65EC-7B42EEBABDDC}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\sysinfo\jrtqcssx.exe"

[software\Classes\CLSID\{06F57557-AB6C-8A55-4922-73547511B8D2}]
@="kehlzctbeczstjnl"

[software\Classes\CLSID\{06F57557-AB6C-8A55-4922-73547511B8D2}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\iconnect\jsnsljzh.exe"

[software\Classes\CLSID\{0737E842-2BBE-EE74-78D8-D848BDF721C1}]
@="bwbbtrcbnrrbkbkk"

[software\Classes\CLSID\{0737E842-2BBE-EE74-78D8-D848BDF721C1}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\btqkxenz.exe"

[software\Classes\CLSID\{0A0F1486-35D6-89D7-D882-CA1A59862B6E}]
@="renwknhtkkrecbjs"

[software\Classes\CLSID\{0A0F1486-35D6-89D7-D882-CA1A59862B6E}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\CompatCtr\jbnxjtkn.exe"

[software\Classes\CLSID\{0A82E0CD-C707-C66F-56D8-BFEEEC72B3FF}]
@="rlhqnvnessnhkbvt"

[software\Classes\CLSID\{0A82E0CD-C707-C66F-56D8-BFEEEC72B3FF}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\zhzsnhje.exe"

[software\Classes\CLSID\{0B44EB36-CB81-9FE3-EB6F-ED253BC824C5}]
@="tnnltenwtnlxzjnk"

[software\Classes\CLSID\{0B44EB36-CB81-9FE3-EB6F-ED253BC824C5}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\Vendors\CN=Microsoft Corporation,L=Redmond,S=Washington,C=US\kkrtrbns.exe"

[software\Classes\CLSID\{0CB9093C-C0DA-0F8E-EE4A-9320FEEE77D5}]
@="sklnzsljwbhkttnh"

[software\Classes\CLSID\{0CB9093C-C0DA-0F8E-EE4A-9320FEEE77D5}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\knhbwsnv.exe"

[software\Classes\CLSID\{101E4C4F-A301-AD71-148E-584F7618A0AC}]
@="bswbsqqtbzwnsteh"

[software\Classes\CLSID\{101E4C4F-A301-AD71-148E-584F7618A0AC}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\rbnrnnxt.exe"

[software\Classes\CLSID\{110F9774-FAAC-0A3E-8A58-182D5A948013}]
@="rrhknbkzhnbskjjk"

[software\Classes\CLSID\{110F9774-FAAC-0A3E-8A58-182D5A948013}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\sysinfo\bjlkjrls.exe"

[software\Classes\CLSID\{118AD934-6512-CF10-DF50-2B2755D07C2F}]
@="lkslnejjlekhlwnt"

[software\Classes\CLSID\{118AD934-6512-CF10-DF50-2B2755D07C2F}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\sysinfo\cntbrbzr.exe"

[software\Classes\CLSID\{1226CFC0-5DF7-E1AE-525D-DDC9F4EE73C7}]
@="vrbltwjtblbhljeb"

[software\Classes\CLSID\{1226CFC0-5DF7-E1AE-525D-DDC9F4EE73C7}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\lhvclnlt.exe"

[software\Classes\CLSID\{12A1AE19-7750-B91F-6F8E-968150CDEFB7}]
@="bhvslsqkkksswrwe"

[software\Classes\CLSID\{12A1AE19-7750-B91F-6F8E-968150CDEFB7}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\htvtlchz.exe"

[software\Classes\CLSID\{1329366B-3CA3-C056-4832-FDA8BAC1351F}]
@="eehbjnbksrhbzjbb"

[software\Classes\CLSID\{1329366B-3CA3-C056-4832-FDA8BAC1351F}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\UpdateCtr\rrbvcsbb.exe"

[software\Classes\CLSID\{14302FB3-F2A5-DB6E-7519-BFCD38B9AFFD}]
@="tsltzrzbjqhsnelv"

[software\Classes\CLSID\{14302FB3-F2A5-DB6E-7519-BFCD38B9AFFD}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\rvjbkxtl.exe"

[software\Classes\CLSID\{18A58AED-3730-309F-8879-665F0274DEA3}]
@="wtcssrwxtbnctvjs"

[software\Classes\CLSID\{18A58AED-3730-309F-8879-665F0274DEA3}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\esjhxblq.exe"

[software\Classes\CLSID\{1C64F2C7-C016-2C06-7A72-AED0431EDCD1}]
@="ejqnhhzrxbevhjkt"

[software\Classes\CLSID\{1C64F2C7-C016-2C06-7A72-AED0431EDCD1}\LocalServer32]
@="C:\WINDOWS\system32\oobe\isperror\rkeetqew.exe"

[software\Classes\CLSID\{1CF024E4-90BE-8922-5971-A43B3A64F18C}]
@="qqxjkjxvnsqjjvjj"

[software\Classes\CLSID\{1CF024E4-90BE-8922-5971-A43B3A64F18C}\LocalServer32]
@="C:\Archivos de programa\NetMeeting\xksjxljj.exe"

[software\Classes\CLSID\{1FCB9023-A1D4-188C-5AE1-F34B8E87832B}]
@="netrrhjcxnkeljjn"

[software\Classes\CLSID\{1FCB9023-A1D4-188C-5AE1-F34B8E87832B}\LocalServer32]
@="C:\WINDOWS\system32\oobe\regerror\wtkkxrlr.exe"

[software\Classes\CLSID\{20D10BF1-3113-E7B7-0A47-A5B469034DB2}]
@="ckxtklbvtwzttttb"

[software\Classes\CLSID\{20D10BF1-3113-E7B7-0A47-A5B469034DB2}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\tnqsbljb.exe"

[software\Classes\CLSID\{2360DC15-1EEF-8DF9-7DB2-18C9E52FDBC3}]
@="ejenrkzwnhtvsbsl"

[software\Classes\CLSID\{2360DC15-1EEF-8DF9-7DB2-18C9E52FDBC3}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\znnhhhtk.exe"

[software\Classes\CLSID\{252D5362-7DB0-49E3-7A16-3B8CFC851C4F}]
@="xbllstvehwntcjhn"

[software\Classes\CLSID\{252D5362-7DB0-49E3-7A16-3B8CFC851C4F}\LocalServer32]

@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\ttkklzcs.exe"

[software\Classes\CLSID\{26A2097D-FE7E-31E3-EB0D-B476CC974DA8}]
@="stqzzlrlbjnlclbn"

[software\Classes\CLSID\{26A2097D-FE7E-31E3-EB0D-B476CC974DA8}\LocalServer32]
@="C:\WINDOWS\system32\oobe\error\ektltnch.exe"

[software\Classes\CLSID\{292B16F1-5F5D-C6FE-83FB-7BD902DB1DB8}]
@="vnbnxjlwjhejwvrt"

[software\Classes\CLSID\{292B16F1-5F5D-C6FE-83FB-7BD902DB1DB8}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\esjkbccv.exe"

[software\Classes\CLSID\{2B74AF48-6A85-7222-6651-EBBAE148C5B3}]
@="xtlbhbtkeetsbltj"

[software\Classes\CLSID\{2B74AF48-6A85-7222-6651-EBBAE148C5B3}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\enbsjwre.exe"

[software\Classes\CLSID\{2BBBB93E-C8E8-C1EE-093F-EA211A62B27B}]
@="rkbnhjnsvjqbjvjh"

[software\Classes\CLSID\{2BBBB93E-C8E8-C1EE-093F-EA211A62B27B}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\wrbbnjss.exe"

[software\Classes\CLSID\{2C7A5774-0575-3C1C-1789-B8C3E1CD9DDE}]
@="ljrxbnzzjlekrljv"

[software\Classes\CLSID\{2C7A5774-0575-3C1C-1789-B8C3E1CD9DDE}\LocalServer32]
@="C:\WINDOWS\system32\oobe\isperror\tsjhshcj.exe"

[software\Classes\CLSID\{2EF89262-692C-51D0-CD84-C415D73F84EB}]
@="rqbqclnchthzrckt"

[software\Classes\CLSID\{2EF89262-692C-51D0-CD84-C415D73F84EB}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\jtxsbxwn.exe"

[software\Classes\CLSID\{308E81ED-7218-8209-0B65-409E8A527503}]
@="lebkhbnhqqlseebs"

[software\Classes\CLSID\{308E81ED-7218-8209-0B65-409E8A527503}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\jejrhnvh.exe"

[software\Classes\CLSID\{3246BB5C-F56C-50CE-9DC1-4568A444BF1F}]
@="vbhbbbzvtserjbtj"

[software\Classes\CLSID\{3246BB5C-F56C-50CE-9DC1-4568A444BF1F}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\vjbssbhj.exe"

[software\Classes\CLSID\{326CE86B-F468-EA85-5628-FD4D0FFDBB85}]
@="telvvbjhbebkeheh"

[software\Classes\CLSID\{326CE86B-F468-EA85-5628-FD4D0FFDBB85}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\sysinfo\rbcjjwqr.exe"

[software\Classes\CLSID\{35349B95-82D3-1178-19ED-0E5D2312F5C0}]
@="nnjbeeqrssrjcbjh"

[software\Classes\CLSID\{35349B95-82D3-1178-19ED-0E5D2312F5C0}\LocalServer32]
@="C:\WINDOWS\system32\urdvxc.exe"

[software\Classes\CLSID\{35400ED6-5CB6-5FB6-F0B9-AF184FD63763}]
@="znjesseklsctnjbq"

[software\Classes\CLSID\{35400ED6-5CB6-5FB6-F0B9-AF184FD63763}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\hlrrerkq.exe"

[software\Classes\CLSID\{363304E6-ADDF-9355-8F4C-D71315751C40}]
@="cvhljnllltcxsksj"

[software\Classes\CLSID\{363304E6-ADDF-9355-8F4C-D71315751C40}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\Vendors\CN=Microsoft Corporation,L=Redmond,S=Washington,C=US\Remote Assistance\vxwqhwzs.exe"

[software\Classes\CLSID\{3676C97E-85F8-4FE1-4FF3-5761EBCB649D}]
@="xvqkktrhqqrqjevz"

[software\Classes\CLSID\{3676C97E-85F8-4FE1-4FF3-5761EBCB649D}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\lhkhbjzl.exe"

[software\Classes\CLSID\{37128C75-4B63-71FC-DD33-D9492FBB2EFB}]
@="blkblsqessbqevet"

[software\Classes\CLSID\{37128C75-4B63-71FC-DD33-D9492FBB2EFB}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Client\wbjbjelb.exe"

[software\Classes\CLSID\{37201920-C149-2EC6-4F1B-17CA78F01B82}]
@="zsxwkzrrkrckrwtb"

[software\Classes\CLSID\{37201920-C149-2EC6-4F1B-17CA78F01B82}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\lnestrnt.exe"

[software\Classes\CLSID\{37FA2744-03C3-5EAA-90C6-D685E5878DB2}]
@="rbtrhbhhwktsxswk"

[software\Classes\CLSID\{37FA2744-03C3-5EAA-90C6-D685E5878DB2}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\nvbbshss.exe"

[software\Classes\CLSID\{38A7613E-68DB-4B91-C168-6B5F071086CB}]
@="lsvewrsltrrrlrth"

[software\Classes\CLSID\{38A7613E-68DB-4B91-C168-6B5F071086CB}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\hjkbllwk.exe"

[software\Classes\CLSID\{3A4B53AC-423A-E7CA-C4DA-B78A959F8C03}]
@="brcjrenqelbtxecz"

[software\Classes\CLSID\{3A4B53AC-423A-E7CA-C4DA-B78A959F8C03}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Server\ccthwjlr.exe"

[software\Classes\CLSID\{3AE1D8CD-A6F7-40FE-B888-56FCBA8BCA46}]
@="swksvshjjvzxhwrl"

[software\Classes\CLSID\{3AE1D8CD-A6F7-40FE-B888-56FCBA8BCA46}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\CompatCtr\tnslrrhk.exe"

[software\Classes\CLSID\{3C0749DE-9D0D-1B9A-52E6-2C347FDD15A9}]
@="hvqencttzrjzrlct"

[software\Classes\CLSID\{3C0749DE-9D0D-1B9A-52E6-2C347FDD15A9}\LocalServer32]
@="C:\WINDOWS\system32\oobe\tttnwshl.exe"

[software\Classes\CLSID\{3C1D709C-0F4D-5DA4-2232-7AFD13C0C23F}]
@="wxxervevljszkztr"

[software\Classes\CLSID\{3C1D709C-0F4D-5DA4-2232-7AFD13C0C23F}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Client\ttzvrbzr.exe"

[software\Classes\CLSID\{4014C362-2DA7-40F3-1C21-53E8844CD087}]
@="rbsxskhteketbnes"

[software\Classes\CLSID\{4014C362-2DA7-40F3-1C21-53E8844CD087}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\nwqjkkhn.exe"

[software\Classes\CLSID\{490CDDA9-7D56-3D09-CC3C-5136306CC8A0}]
@="kejhzqjrsqerkllr"

[software\Classes\CLSID\{490CDDA9-7D56-3D09-CC3C-5136306CC8A0}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\CompatCtr\hrtbebze.exe"

[software\Classes\CLSID\{494FEB7F-6626-1241-41D8-59E22DB24FC2}]
@="sjnvkrevsxwthtvv"

[software\Classes\CLSID\{494FEB7F-6626-1241-41D8-59E22DB24FC2}\LocalServer32]
@="C:\WINDOWS\system32\oobe\isperror\ktkbeknl.exe"

[software\Classes\CLSID\{49BC4B7D-A77B-DCF4-C29B-8F5040D7C9A5}]
@="rjtrnlzhbszcehkk"

[software\Classes\CLSID\{49BC4B7D-A77B-DCF4-C29B-8F5040D7C9A5}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\dslmain\qxztllwj.exe"

[software\Classes\CLSID\{4A167404-9A8F-6684-EF47-19FB5BD943EF}]
@="wleljthntbkzhkse"

[software\Classes\CLSID\{4A167404-9A8F-6684-EF47-19FB5BD943EF}\LocalServer32]
@="C:\WINDOWS\system32\oobe\regerror\rcwnttzv.exe"

[software\Classes\CLSID\{4AA4DEB6-F141-B724-8BCF-4995A82419F6}]
@="ntretwelktbsvvhs"

[software\Classes\CLSID\{4AA4DEB6-F141-B724-8BCF-4995A82419F6}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\lkjtrhks.exe"

[software\Classes\CLSID\{4D9B3AD6-F9C1-0739-3A6E-3D55D45A69E3}]
@="swjhhtjhjhwtbqne"

[software\Classes\CLSID\{4D9B3AD6-F9C1-0739-3A6E-3D55D45A69E3}\LocalServer32]
@="C:\WINDOWS\Help\jjlenkbt.exe"

[software\Classes\CLSID\{4F2D630B-CD4C-1206-EDF4-4ED3900B1398}]
@="wnshlsrkhtwhbskl"

[software\Classes\CLSID\{4F2D630B-CD4C-1206-EDF4-4ED3900B1398}\LocalServer32]
@="C:\WINDOWS\system32\oobe\regerror\ehxzeshx.exe"

[software\Classes\CLSID\{4F82FDE5-2426-891D-5E88-22E06725D2A6}]
@="xbnkkkrewltrnkkt"

[software\Classes\CLSID\{4F82FDE5-2426-891D-5E88-22E06725D2A6}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\UpdateCtr\trkhkjxz.exe"

[software\Classes\CLSID\{5064A943-EF53-7ACA-9C6F-789E5941E345}]
@="enkkvhtbzjvlsrqt"

[software\Classes\CLSID\{5064A943-EF53-7ACA-9C6F-789E5941E345}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\jlkshlvl.exe"

[software\Classes\CLSID\{52287B95-3257-CCF7-3B86-B73978B045A2}]
@="rnxhxjekxnzhvhvc"

[software\Classes\CLSID\{52287B95-3257-CCF7-3B86-B73978B045A2}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\seqtjbee.exe"

[software\Classes\CLSID\{5373C2B2-504D-1A46-08FD-6B79798FD4D0}]
@="wctjeleblbenewhj"

[software\Classes\CLSID\{5373C2B2-504D-1A46-08FD-6B79798FD4D0}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\lzjvxjel.exe"

[software\Classes\CLSID\{54E27EDA-9B99-0E27-7246-DB3CDD577165}]
@="ceebznjelxlwtseq"

[software\Classes\CLSID\{54E27EDA-9B99-0E27-7246-DB3CDD577165}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\hnhkkene.exe"

[software\Classes\CLSID\{555B79E9-DA80-976E-4918-FE9C20D88A6F}]
@="shxettcbbbevnvke"

[software\Classes\CLSID\{555B79E9-DA80-976E-4918-FE9C20D88A6F}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\hxckwnzl.exe"

[software\Classes\CLSID\{56F8EF1A-30C4-77DB-B4A1-F7FB92D83438}]
@="jkshnxnckhxncsnr"

[software\Classes\CLSID\{56F8EF1A-30C4-77DB-B4A1-F7FB92D83438}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\ErrMsg\vlvxqrek.exe"

[software\Classes\CLSID\{575E02AB-D638-2559-43AB-60DF97B0D256}]
@="ntsbvlxxrnlsqblt"

[software\Classes\CLSID\{575E02AB-D638-2559-43AB-60DF97B0D256}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\hlqstwxz.exe"

[software\Classes\CLSID\{5820F447-EF2B-74E0-E561-3A3CA71075CB}]
@="esrechlnhztkxrzt"

[software\Classes\CLSID\{5820F447-EF2B-74E0-E561-3A3CA71075CB}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\klkhkrts.exe"

[software\Classes\CLSID\{5B228E8B-E361-D45F-80A9-90E145C6C2D7}]
@="hebnjwhkeejqrqhe"

[software\Classes\CLSID\{5B228E8B-E361-D45F-80A9-90E145C6C2D7}\LocalServer32]
@="C:\WINDOWS\system32\oobe\error\kbwnhlkk.exe"

[software\Classes\CLSID\{5B974BBE-61BD-D89A-783C-6F06BBE18E40}]
@="elkexjtxkrtwbelk"

[software\Classes\CLSID\{5B974BBE-61BD-D89A-783C-6F06BBE18E40}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\UpdateCtr\lwklbvze.exe"

[software\Classes\CLSID\{5BE00A73-5A3E-77A2-C459-9289E7FFBB15}]
@="rtnrjhkwjheeztte"

[software\Classes\CLSID\{5BE00A73-5A3E-77A2-C459-9289E7FFBB15}\LocalServer32]
@="C:\WINDOWS\system32\oobe\isperror\hkenntsl.exe"

[software\Classes\CLSID\{5D09B84E-B9C6-5014-708E-C73B5555D548}]
@="shtwzjqqjlecjrns"

[software\Classes\CLSID\{5D09B84E-B9C6-5014-708E-C73B5555D548}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\System\ado\scjejqze.exe"

[software\Classes\CLSID\{5DF14F9D-6ED4-DA4A-49A4-40F085A9BB86}]
@="bnkeznntlqxewltk"

[software\Classes\CLSID\{5DF14F9D-6ED4-DA4A-49A4-40F085A9BB86}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\dslmain\slhcezwb.exe"

[software\Classes\CLSID\{5E037685-2221-5D8C-A3FF-E6E39E9DCAA1}]
@="xcnvewljsrnxcjee"

[software\Classes\CLSID\{5E037685-2221-5D8C-A3FF-E6E39E9DCAA1}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\xclsclbs.exe"

[software\Classes\CLSID\{60F07540-55BC-AC34-166A-67B6FA4DD197}]
@="ntrhehrscelxjblk"

[software\Classes\CLSID\{60F07540-55BC-AC34-166A-67B6FA4DD197}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\sconnect\jkhjlhbb.exe"

[software\Classes\CLSID\{616F8160-B381-7FEA-D13A-58E0EF4C12E8}]
@="wbjssqehshnqvhjs"

[software\Classes\CLSID\{616F8160-B381-7FEA-D13A-58E0EF4C12E8}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\wesnhzec.exe"

[software\Classes\CLSID\{62E182EE-072E-85DF-552C-319B98B64E6C}]
@="rkzneschtcshhlbr"

[software\Classes\CLSID\{62E182EE-072E-85DF-552C-319B98B64E6C}\LocalServer32]
@="C:\WINDOWS\system32\oobe\regerror\cetrjwtt.exe"

[software\Classes\CLSID\{6756A72C-5FD9-3E32-6951-6704AEF8DD60}]
@="kjxxbtlxcshjtnrt"

[software\Classes\CLSID\{6756A72C-5FD9-3E32-6951-6704AEF8DD60}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\cwbbnetr.exe"

[software\Classes\CLSID\{68342826-C702-235F-DF6B-EDBD264885AB}]
@="xbwhtxwrbjnkhlks"

[software\Classes\CLSID\{68342826-C702-235F-DF6B-EDBD264885AB}\LocalServer32]
@="C:\WINDOWS\Help\Tours\htmlTour\qejnhetj.exe"

[software\Classes\CLSID\{68905909-F475-DD43-8FE8-914E341AEFD6}]
@="skllekkjhnjbqknh"

[software\Classes\CLSID\{68905909-F475-DD43-8FE8-914E341AEFD6}\LocalServer32]
@="C:\WINDOWS\Help\Tours\htmlTour\kzkzkjkb.exe"

[software\Classes\CLSID\{68B4E7F8-6512-EF00-DF46-2E62C2F0A63F}]
@="qbwjberbjtnlseke"

[software\Classes\CLSID\{68B4E7F8-6512-EF00-DF46-2E62C2F0A63F}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\panels\nntlskwn.exe"

[software\Classes\CLSID\{68BCC440-B815-D682-4315-91A7B7819B77}]
@="bjjresekrrxnlrnn"

[software\Classes\CLSID\{68BCC440-B815-D682-4315-91A7B7819B77}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\sbwrkxcs.exe"

[software\Classes\CLSID\{691C27E5-1C9A-A9C4-98FD-9CD1018A9557}]
@="ljxbcjbqrblnzbth"

[software\Classes\CLSID\{691C27E5-1C9A-A9C4-98FD-9CD1018A9557}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\com\vmware\vmguestlib\cnrstqbb.exe"

[software\Classes\CLSID\{6B4FB954-58B2-E021-8CE4-02B6166FF436}]
@="sqtllnnqerzhlhce"

[software\Classes\CLSID\{6B4FB954-58B2-E021-8CE4-02B6166FF436}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\dslmain\nevttblh.exe"

[software\Classes\CLSID\{6C3EC276-E5AB-B2F5-9FF2-DC2EA9780271}]
@="llvtrzkkszxhhtjc"

[software\Classes\CLSID\{6C3EC276-E5AB-B2F5-9FF2-DC2EA9780271}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\knkskthw.exe"

[software\Classes\CLSID\{6CC6DDD2-220B-8F89-077A-058CE7A629E7}]
@="jqlbkhjlrjblbjrk"

[software\Classes\CLSID\{6CC6DDD2-220B-8F89-077A-058CE7A629E7}\LocalServer32]
@="C:\WINDOWS\system32\oobe\icserror\vcejlxkt.exe"

[software\Classes\CLSID\{6EAF3580-B150-6D5F-D7BB-CC0EC951A6CF}]
@="htvjsnvvcktsrbhv"

[software\Classes\CLSID\{6EAF3580-B150-6D5F-D7BB-CC0EC951A6CF}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\nleevxqj.exe"

[software\Classes\CLSID\{6F03B46B-1AE1-2DB9-BC4A-13EEB848AB0F}]
@="esbrejslcjbrwnbn"

[software\Classes\CLSID\{6F03B46B-1AE1-2DB9-BC4A-13EEB848AB0F}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\njwrczcc.exe"

[software\Classes\CLSID\{717B6B22-F136-7AEB-2A9C-C75BEAAEAF04}]
@="lbljcwehjzhsnekk"

[software\Classes\CLSID\{717B6B22-F136-7AEB-2A9C-C75BEAAEAF04}\LocalServer32]
@="C:\WINDOWS\Help\Tours\WindowsMediaPlayer\Cnt\tjnbzhbh.exe"

[software\Classes\CLSID\{71AD80F1-0996-B6AC-8140-3E7EE8B8E5DD}]
@="ebzzrjjlbkxwqrnt"

[software\Classes\CLSID\{71AD80F1-0996-B6AC-8140-3E7EE8B8E5DD}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\wnklretl.exe"

[software\Classes\CLSID\{75175DF7-EF56-52A0-8766-55465E7173E2}]
@="ksntjzrkwctrekbl"

[software\Classes\CLSID\{75175DF7-EF56-52A0-8766-55465E7173E2}\LocalServer32]
@="C:\WINDOWS\Help\Tours\WindowsMediaPlayer\Audio\lllknblj.exe"

[software\Classes\CLSID\{75E2B229-566A-02B3-1798-BB27E8D05ADD}]
@="xlhqkkbjjwshvskn"

[software\Classes\CLSID\{75E2B229-566A-02B3-1798-BB27E8D05ADD}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\xtxvnrex.exe"

[software\Classes\CLSID\{78138571-F4A5-1948-2DF6-7E7EB47A2658}]
@="lzkjqtkbknjshhlt"

[software\Classes\CLSID\{78138571-F4A5-1948-2DF6-7E7EB47A2658}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\hwncrnhh.exe"

[software\Classes\CLSID\{796977ED-D431-7FF4-F3CB-2ABEBC687630}]
@="btsnzejjtskjnthj"

[software\Classes\CLSID\{796977ED-D431-7FF4-F3CB-2ABEBC687630}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\shbqjhcl.exe"

[software\Classes\CLSID\{79910627-6A00-CDCE-579B-2C3D5BA84B34}]
@="lwkqhsntbjljvvjj"

[software\Classes\CLSID\{79910627-6A00-CDCE-579B-2C3D5BA84B34}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Common\seshhtth.exe"

[software\Classes\CLSID\{7A353246-74DA-B2BB-F2FB-06498428684C}]
@="nzceztecqsnjetqx"

[software\Classes\CLSID\{7A353246-74DA-B2BB-F2FB-06498428684C}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\vrrkkhbn.exe"

[software\Classes\CLSID\{7D2FAF53-4ADD-C43A-4E61-1B61075FC924}]
@="brbbwlwqrbksqwlt"

[software\Classes\CLSID\{7D2FAF53-4ADD-C43A-4E61-1B61075FC924}\LocalServer32]

@="C:\WINDOWS\pchealth\helpctr\System\sysinfo\vkchbbxh.exe"

[software\Classes\CLSID\{7D4B8C8E-CD51-F9C0-4E76-69F5FA0CE599}]
@="qxcxljtqsrnbhbhl"

[software\Classes\CLSID\{7D4B8C8E-CD51-F9C0-4E76-69F5FA0CE599}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\rqxjhbsl.exe"

[software\Classes\CLSID\{7D708FBB-FDAD-D4ED-7B5A-FE8D0FFA7493}]
@="rhvsbjzhhscnvkkn"

[software\Classes\CLSID\{7D708FBB-FDAD-D4ED-7B5A-FE8D0FFA7493}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\knkhrczb.exe"

[software\Classes\CLSID\{80314ACA-04E4-B2F8-6BB3-7D4A764F3C5F}]
@="csbhskjhhxcnervk"

[software\Classes\CLSID\{80314ACA-04E4-B2F8-6BB3-7D4A764F3C5F}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\btesnnel.exe"

[software\Classes\CLSID\{82FC74DE-CCA4-17F1-FA1E-760DC404A317}]
@="lrwwxklvreqnxsjk"

[software\Classes\CLSID\{82FC74DE-CCA4-17F1-FA1E-760DC404A317}\LocalServer32]
@="C:\WINDOWS\system32\oobe\error\xenjnbqe.exe"

[software\Classes\CLSID\{83E68555-BBFE-A215-0174-977FF8FD732A}]
@="cljjzwvnejbjnqen"

[software\Classes\CLSID\{83E68555-BBFE-A215-0174-977FF8FD732A}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Common\shnkjjbh.exe"

[software\Classes\CLSID\{83EA0F26-E3A8-F644-2E66-1BEC818FD94B}]
@="xhekjnkzjxvejhzn"

[software\Classes\CLSID\{83EA0F26-E3A8-F644-2E66-1BEC818FD94B}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\ntwbjnxv.exe"

[software\Classes\CLSID\{83F033B6-3E4F-B858-069E-1DEA757A732D}]
@="zwebxjhczltnqbqs"

[software\Classes\CLSID\{83F033B6-3E4F-B858-069E-1DEA757A732D}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\zeblsxxw.exe"

[software\Classes\CLSID\{84485E16-B0EE-B618-6D56-157A7AFC754C}]
@="hnqbrxhnrwsleklt"

[software\Classes\CLSID\{84485E16-B0EE-B618-6D56-157A7AFC754C}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\wtenslnj.exe"

[software\Classes\CLSID\{8472F7AB-E15F-6E7A-D99B-11C50742533C}]
@="vsrhxtrwkvzncjlx"

[software\Classes\CLSID\{8472F7AB-E15F-6E7A-D99B-11C50742533C}\LocalServer32]
@="C:\WINDOWS\Help\Tours\htmlTour\rbnesqvr.exe"

[software\Classes\CLSID\{86E8AB09-0C84-E4C6-F1DE-EA22EE4A3934}]
@="cssjsrnlshkxvjzn"

[software\Classes\CLSID\{86E8AB09-0C84-E4C6-F1DE-EA22EE4A3934}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\zhqvnthb.exe"

[software\Classes\CLSID\{882762E8-7BC2-4999-5905-7973DF8F5974}]
@="zerlbrwvlrechlsq"

[software\Classes\CLSID\{882762E8-7BC2-4999-5905-7973DF8F5974}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Client\jjennetl.exe"

[software\Classes\CLSID\{8A96C138-FA33-D993-8688-97EC8A607557}]
@="xbbbhejjkekewlqr"

[software\Classes\CLSID\{8A96C138-FA33-D993-8688-97EC8A607557}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\CompatCtr\zlhqrlbx.exe"

[software\Classes\CLSID\{8B661C54-1876-647A-AFA9-232DA309CCC1}]
@="cchrhlrsrqxhrejb"

[software\Classes\CLSID\{8B661C54-1876-647A-AFA9-232DA309CCC1}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\Vendors\CN=Microsoft Corporation,L=Redmond,S=Washington,C=US\vsekkehe.exe"

[software\Classes\CLSID\{8B6B6AF7-467C-32F0-1C1F-CF0AB649D65E}]
@="hsjrbrnexjntzbsr"

[software\Classes\CLSID\{8B6B6AF7-467C-32F0-1C1F-CF0AB649D65E}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\rresnsct.exe"

[software\Classes\CLSID\{8BF6F24D-2C3C-D83A-E9AE-EC1C4F01DAEE}]
@="znerrehzcserqktr"

[software\Classes\CLSID\{8BF6F24D-2C3C-D83A-E9AE-EC1C4F01DAEE}\LocalServer32]
@="C:\WINDOWS\Help\jbnshhqj.exe"

[software\Classes\CLSID\{8CE16525-B646-EEE9-9681-39D46032B080}]
@="zsttbclchknqzskv"

[software\Classes\CLSID\{8CE16525-B646-EEE9-9681-39D46032B080}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\blvccbsx.exe"

[software\Classes\CLSID\{8D58E095-95F5-75C9-1ECD-A1B105812332}]
@="cjeljxsejtbnxjtb"

[software\Classes\CLSID\{8D58E095-95F5-75C9-1ECD-A1B105812332}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\ntwwcbnq.exe"

[software\Classes\CLSID\{8FBE6833-4B81-D3D0-BD98-7B192C046CC5}]
@="trqtslxehhkknleb"

[software\Classes\CLSID\{8FBE6833-4B81-D3D0-BD98-7B192C046CC5}\LocalServer32]
@="C:\WINDOWS\system32\oobe\isperror\jjtrkbnj.exe"

[software\Classes\CLSID\{917C9DB7-A28B-CB00-ADAF-6908C65B70AD}]
@="txkeknhnlcbtvrnv"

[software\Classes\CLSID\{917C9DB7-A28B-CB00-ADAF-6908C65B70AD}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\tthzxntk.exe"

[software\Classes\CLSID\{91FB423F-5099-7870-A17C-A31006B70863}]
@="ssvxbkkxrnjltwqj"

[software\Classes\CLSID\{91FB423F-5099-7870-A17C-A31006B70863}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\nkhlvlzt.exe"

[software\Classes\CLSID\{920D60B8-BB03-71F7-3EDF-E3410301F4E0}]
@="elkrwtcsehtkzekh"

[software\Classes\CLSID\{920D60B8-BB03-71F7-3EDF-E3410301F4E0}\LocalServer32]
@="C:\WINDOWS\system32\oobe\regerror\wlkbbnrq.exe"

[software\Classes\CLSID\{9238D60C-A78B-0639-7E0D-921AA5100090}]
@="bjrtteelswherebq"

[software\Classes\CLSID\{9238D60C-A78B-0639-7E0D-921AA5100090}\LocalServer32]
@="C:\WINDOWS\system32\oobe\krcxzncj.exe"

[software\Classes\CLSID\{924E3D0D-2679-EF9B-71B4-113A38F4B786}]
@="lrsxtvhrsjbskszb"

[software\Classes\CLSID\{924E3D0D-2679-EF9B-71B4-113A38F4B786}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\lrlzztll.exe"

[software\Classes\CLSID\{92C756DF-E46F-0CE9-9FC2-B05BCAC48D54}]
@="nlqktvxllhrvezwt"

[software\Classes\CLSID\{92C756DF-E46F-0CE9-9FC2-B05BCAC48D54}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\brvecwcs.exe"

[software\Classes\CLSID\{9615EF71-014F-8973-B235-6BB870093E0E}]
@="xxjbsrhekqrtnzbs"

[software\Classes\CLSID\{9615EF71-014F-8973-B235-6BB870093E0E}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\isptype\lnvlnzbq.exe"

[software\Classes\CLSID\{96186C85-0E8A-D7D6-B8CE-58925A368A34}]
@="qkrnxhklkteexnrt"

[software\Classes\CLSID\{96186C85-0E8A-D7D6-B8CE-58925A368A34}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\lbzcxver.exe"

[software\Classes\CLSID\{9639A854-6A08-A929-EA74-6658559553E1}]
@="lkwqebnrkbernkbt"

[software\Classes\CLSID\{9639A854-6A08-A929-EA74-6658559553E1}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\qetvqlnw.exe"

[software\Classes\CLSID\{96B5C05D-0A64-92D1-38DC-46A95C6A77B6}]
@="brkhhwtkbzlwqbnj"

[software\Classes\CLSID\{96B5C05D-0A64-92D1-38DC-46A95C6A77B6}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\nstnnnkk.exe"

[software\Classes\CLSID\{99E96E31-813C-416A-B501-37DCD14C1253}]
@="qtnhtkrhlhbnhlxh"

[software\Classes\CLSID\{99E96E31-813C-416A-B501-37DCD14C1253}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\cjxsjlbr.exe"

[software\Classes\CLSID\{9A3AE452-10C1-86E3-ED60-2306FC7C0BAD}]
@="hjsnecjntbjkssev"

[software\Classes\CLSID\{9A3AE452-10C1-86E3-ED60-2306FC7C0BAD}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\rzqstbqq.exe"

[software\Classes\CLSID\{9C8C2A58-0FAD-AF7C-CDB7-4CDC59E8E5A3}]
@="ljnsjjrwshtslzeb"

[software\Classes\CLSID\{9C8C2A58-0FAD-AF7C-CDB7-4CDC59E8E5A3}\LocalServer32]
@="C:\WINDOWS\Help\tsbjbtvn.exe"

[software\Classes\CLSID\{9D1D618E-EFC0-EC73-4721-1F0A6BCD4F10}]
@="ltczkllstbthwljl"

[software\Classes\CLSID\{9D1D618E-EFC0-EC73-4721-1F0A6BCD4F10}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Common\rwcjrqhw.exe"

[software\Classes\CLSID\{9E929E0C-FD56-322E-BE5E-49024FC954A7}]
@="vhhbshentrjkksec"

[software\Classes\CLSID\{9E929E0C-FD56-322E-BE5E-49024FC954A7}\LocalServer32]
@="C:\WINDOWS\Help\bzehxvnz.exe"

[software\Classes\CLSID\{9EEBBEDB-D9B2-5CEA-1B37-C835EE0CA7F2}]
@="kkzhqtqkwkhcjhxk"

[software\Classes\CLSID\{9EEBBEDB-D9B2-5CEA-1B37-C835EE0CA7F2}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\bvqncler.exe"

[software\Classes\CLSID\{A1C155BC-81B7-7E44-B517-235D34BD11E6}]
@="skhhthqjltjhtbkt"

[software\Classes\CLSID\{A1C155BC-81B7-7E44-B517-235D34BD11E6}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\rrthsntk.exe"

[software\Classes\CLSID\{A1EB21B0-93CB-6A56-C7F3-D8BAC1C6D9E4}]
@="nsrljqwkbllknkxn"

[software\Classes\CLSID\{A1EB21B0-93CB-6A56-C7F3-D8BAC1C6D9E4}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\vkckxhbn.exe"

[software\Classes\CLSID\{A2900343-2DAD-D1AA-70C2-563448A32C69}]
@="bhjhjllnkrjnhhje"

[software\Classes\CLSID\{A2900343-2DAD-D1AA-70C2-563448A32C69}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Client\knenvxlj.exe"

[software\Classes\CLSID\{A2F6940D-2E6A-C73B-077D-01A6FDD1A521}]
@="jclltblsbtvsnbrl"

[software\Classes\CLSID\{A2F6940D-2E6A-C73B-077D-01A6FDD1A521}\LocalServer32]
@="C:\WINDOWS\system32\oobe\error\sswzlttc.exe"

[software\Classes\CLSID\{A444DA5E-8020-74A6-F83A-E1D4431F9C12}]
@="eenqhlwknbxwblwj"

[software\Classes\CLSID\{A444DA5E-8020-74A6-F83A-E1D4431F9C12}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\nzzwhebn.exe"

[software\Classes\CLSID\{A56129F2-22A9-26DE-9D0F-9FFE9585F22B}]
@="jshqctbnlqzsrkvl"

[software\Classes\CLSID\{A56129F2-22A9-26DE-9D0F-9FFE9585F22B}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\bknkjheh.exe"

[software\Classes\CLSID\{A61DB195-1958-C95E-495E-DB6B6F0337AC}]
@="wzlxhwsjelkzrqvl"

[software\Classes\CLSID\{A61DB195-1958-C95E-495E-DB6B6F0337AC}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\nsekrlvz.exe"

[software\Classes\CLSID\{A783A33D-30B6-C96D-115C-30BFA0B79CBC}]
@="senesthkkhbnzkrw"

[software\Classes\CLSID\{A783A33D-30B6-C96D-115C-30BFA0B79CBC}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\tqkbrhnx.exe"

[software\Classes\CLSID\{A84B4FB5-E327-043D-C252-040844411FAB}]
@="jbnelcllhnnjkbrs"

[software\Classes\CLSID\{A84B4FB5-E327-043D-C252-040844411FAB}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\Vendors\CN=Microsoft Corporation,L=Redmond,S=Washington,C=US\erwskeqr.exe"

[software\Classes\CLSID\{A931E274-C4C7-A4AA-5AF9-3071CADA2775}]
@="svwtbtbwvjvwxrrs"

[software\Classes\CLSID\{A931E274-C4C7-A4AA-5AF9-3071CADA2775}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\NetDiag\hsjqschn.exe"

[software\Classes\CLSID\{AC753B34-2C88-B44A-21A8-ED22C9AD09AC}]
@="ejebnrntkhjbnrsn"

[software\Classes\CLSID\{AC753B34-2C88-B44A-21A8-ED22C9AD09AC}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\sysinfo\rercrnhh.exe"

[software\Classes\CLSID\{ADDF57D7-6C02-B77D-9604-A850006B4601}]
@="hhbelbtthwcbvtck"

[software\Classes\CLSID\{ADDF57D7-6C02-B77D-9604-A850006B4601}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\sejkhevn.exe"

[software\Classes\CLSID\{AEBD7F25-6306-F72A-2D9A-E5B8AD4399F1}]
@="srltrstwnzqbvsck"

[software\Classes\CLSID\{AEBD7F25-6306-F72A-2D9A-E5B8AD4399F1}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\UpdateCtr\qxshkkqn.exe"

[software\Classes\CLSID\{AF0181CB-B933-41B7-A229-96ACFDF80B12}]
@="zqjktlvrhtkrlswn"

[software\Classes\CLSID\{AF0181CB-B933-41B7-A229-96ACFDF80B12}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\lbexzkbk.exe"

[software\Classes\CLSID\{AFA58B0D-4C3D-E90B-CF64-00CE780BA5BA}]
@="snqvkbrrktkllllhs"

[software\Classes\CLSID\{AFA58B0D-4C3D-E90B-CF64-00CE780BA5BA}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\tchekrqt.exe"

[software\Classes\CLSID\{B2374239-6BE1-CCCA-776C-E5BC5C03EA2C}]
@="xezhlvrchzrsevbw"

[software\Classes\CLSID\{B2374239-6BE1-CCCA-776C-E5BC5C03EA2C}\LocalServer32]

@="C:\sandnet.exe"

[software\Classes\CLSID\{B2C11550-352D-2588-2B00-55B92A5AE1A2}]
@="ehrtlhqhcevlreet"

[software\Classes\CLSID\{B2C11550-352D-2588-2B00-55B92A5AE1A2}\LocalServer32]
@="C:\WINDOWS\system32\oobe\error\lktkttrb.exe"

[software\Classes\CLSID\{B467C6CB-1F46-9988-CCDE-83FD25DE8439}]
@="eksxtteknxvsjzvb"

[software\Classes\CLSID\{B467C6CB-1F46-9988-CCDE-83FD25DE8439}\LocalServer32]
@="C:\WINDOWS\system32\oobe\isperror\knkbrnbn.exe"

[software\Classes\CLSID\{B4E87BDA-9197-7A4A-3DCC-9D820B2648B1}]
@="sshsheklhnlvneth"

[software\Classes\CLSID\{B4E87BDA-9197-7A4A-3DCC-9D820B2648B1}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\sysinfo\rnbrkrlv.exe"

[software\Classes\CLSID\{B9350F7D-7FC0-A2AB-9AFE-9A61A3768F1F}]
@="eejjlnzjzjvrqqtt"

[software\Classes\CLSID\{B9350F7D-7FC0-A2AB-9AFE-9A61A3768F1F}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\clbvvlrs.exe"

[software\Classes\CLSID\{BBAE1B4C-9650-8503-F248-B9783434FFE9}]
@="ssknsxkrwrrzlklb"

[software\Classes\CLSID\{BBAE1B4C-9650-8503-F248-B9783434FFE9}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote
Assistance\Interaction\Server\ezslqrbz.exe"

[software\Classes\CLSID\{C039A8AE-771A-2609-ABE9-6FF57A8E39B3}]
@="ktrsbxwvnvttxkjz"

[software\Classes\CLSID\{C039A8AE-771A-2609-ABE9-6FF57A8E39B3}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\bccxejnc.exe"

[software\Classes\CLSID\{C1C97595-B998-B9A8-EEBA-A15A7B78460F}]
@="ezenrcehetbkkltw"

[software\Classes\CLSID\{C1C97595-B998-B9A8-EEBA-A15A7B78460F}\LocalServer32]
@="C:\WINDOWS\system32\oobe\isperror\ztceskls.exe"

[software\Classes\CLSID\{C4C08C4B-AD9B-37B1-8F3F-AD38323512C3}]
@="teblqlnrlehqzetr"

[software\Classes\CLSID\{C4C08C4B-AD9B-37B1-8F3F-AD38323512C3}\LocalServer32]
@="C:\WINDOWS\system32\oobe\error\erettxjr.exe"

[software\Classes\CLSID\{C57C74A9-ABB0-E9F3-8C85-DDD33CAD0CC8}]
@="ncvltxnhrkbhrbrt"

[software\Classes\CLSID\{C57C74A9-ABB0-E9F3-8C85-DDD33CAD0CC8}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\khkvhhsb.exe"

[software\Classes\CLSID\{C7E60805-E539-09E9-CB93-CD66115CA697}]
@="ckshbtbjsqnsbnjj"

[software\Classes\CLSID\{C7E60805-E539-09E9-CB93-CD66115CA697}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote
Assistance\Interaction\Client\ekjvhbcn.exe"

[software\Classes\CLSID\{C94D7379-F270-70B2-1635-CEF70473F7AC}]
@="hqjtcknhhblejwnh"

[software\Classes\CLSID\{C94D7379-F270-70B2-1635-CEF70473F7AC}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote
Assistance\Interaction\Client\zqwkjbbt.exe"

[software\Classes\CLSID\{C951E857-742D-BCE1-6758-8E4B76563BB9}]
@="bbzhehtnbebbbnee"

[software\Classes\CLSID\{C951E857-742D-BCE1-6758-8E4B76563BB9}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Common\hxrshqsj.exe"

[software\Classes\CLSID\{CA776317-17BB-7877-01FA-D15CFEE0C200}]
@="bkevtnbkbecqcecr"

[software\Classes\CLSID\{CA776317-17BB-7877-01FA-D15CFEE0C200}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\rserkten.exe"

[software\Classes\CLSID\{CC64B45D-D6FC-76B2-D06F-CEF1AD314B4D}]
@="bscnkbrcbqezsvbb"

[software\Classes\CLSID\{CC64B45D-D6FC-76B2-D06F-CEF1AD314B4D}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\bzrbbsrn.exe"

[software\Classes\CLSID\{CD201855-6C54-FCC8-84E8-F1B657D49D38}]
@="kkrvsewtknjlhxqn"

[software\Classes\CLSID\{CD201855-6C54-FCC8-84E8-F1B657D49D38}\LocalServer32]
@="C:\WINDOWS\Help\Tours\htmlTour\kzerbzks.exe"

[software\Classes\CLSID\{CE0EF9DB-3F2A-681E-D781-EB9E924CD2CA}]
@="qenhjjncrewrwxsr"

[software\Classes\CLSID\{CE0EF9DB-3F2A-681E-D781-EB9E924CD2CA}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\stttklte.exe"

[software\Classes\CLSID\{D0ECC340-FF63-8EA0-9298-CBB529B6A295}]

@="lvvcjzsrhhntkbkq"

[software\Classes\CLSID\{D0ECC340-FF63-8EA0-9298-CBB529B6A295}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\jIlslbnb.exe"

[software\Classes\CLSID\{D6189896-AD1C-E3B2-AFE6-4B692E91B20F}]
@="twehenjtetvwbjsk"

[software\Classes\CLSID\{D6189896-AD1C-E3B2-AFE6-4B692E91B20F}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\zhhrrltb.exe"

[software\Classes\CLSID\{D66AACB8-8641-5407-E008-85900D01CED3}]
@="xjsvwrssbswchzlk"

[software\Classes\CLSID\{D66AACB8-8641-5407-E008-85900D01CED3}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\ejthwsbr.exe"

[software\Classes\CLSID\{D72366D6-CA69-61DD-540C-ACA7B20FA09A}]
@="bbnlerevtjbqthlz"

[software\Classes\CLSID\{D72366D6-CA69-61DD-540C-ACA7B20FA09A}\LocalServer32]
@="C:\WINDOWS\system32\oobe\regerror\xcjnkske.exe"

[software\Classes\CLSID\{D8583457-F929-F1B1-F466-B04B4DE7B055}]
@="stlnrnbszkejrjnw"

[software\Classes\CLSID\{D8583457-F929-F1B1-F466-B04B4DE7B055}\LocalServer32]
@="C:\WINDOWS\system32\oobe\regerror\etnwxxnv.exe"

[software\Classes\CLSID\{DD6D709D-20CF-A598-269A-404587CC94A9}]
@="clebchklslkvjebs"

[software\Classes\CLSID\{DD6D709D-20CF-A598-269A-404587CC94A9}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\UpdateCtr\snqesjrk.exe"

[software\Classes\CLSID\{DEDA84E9-967E-0E2E-ADE2-FDBFBD314AAB}]
@="jvtvsnkbnrrblsrt"

[software\Classes\CLSID\{DEDA84E9-967E-0E2E-ADE2-FDBFBD314AAB}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\hcvxrtwz.exe"

[software\Classes\CLSID\{DF03105A-30A9-3197-36B8-BD0941DFE414}]
@="bkwsxqhjjjqsklqn"

[software\Classes\CLSID\{DF03105A-30A9-3197-36B8-BD0941DFE414}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\panels\sncncweb.exe"

[software\Classes\CLSID\{DFE578BA-0D6B-E1F5-CFAA-CBAE2CEEFA62}]
@="jrkwcvebnltzrrlb"

[software\Classes\CLSID\{DFE578BA-0D6B-E1F5-CFAA-CBAE2CEEFA62}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Server\neqvzkeh.exe"

[software\Classes\CLSID\{E07DD403-A919-FBD0-EF84-734B257407BB}]
@="lzqknjhkkrxjevlh"

[software\Classes\CLSID\{E07DD403-A919-FBD0-EF84-734B257407BB}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\DVDUpgrd\shrrtjet.exe"

[software\Classes\CLSID\{E3F90F3D-DE26-194B-80C0-216D5D35B848}]
@="hrvlbksltklstrrj"

[software\Classes\CLSID\{E3F90F3D-DE26-194B-80C0-216D5D35B848}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\errors\jcjjlqnq.exe"

[software\Classes\CLSID\{E3FB3D9B-A958-33C1-23B9-C8414EC3D98D}]
@="hwstnjbvkzkkhvwj"

[software\Classes\CLSID\{E3FB3D9B-A958-33C1-23B9-C8414EC3D98D}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\zvswnlev.exe"

[software\Classes\CLSID\{E52FA195-5A6F-2177-F3BD-B37D3644ACC2}]
@="bxhkncjsshtlnxel"

[software\Classes\CLSID\{E52FA195-5A6F-2177-F3BD-B37D3644ACC2}\LocalServer32]
@="C:\WINDOWS\Help\Tours\htmlTour\rqkjqjqb.exe"

[software\Classes\CLSID\{E6C4D142-ADFB-1690-E3B7-17999EBDA1FA}]
@="stqetlvnnztnwjst"

[software\Classes\CLSID\{E6C4D142-ADFB-1690-E3B7-17999EBDA1FA}\LocalServer32]
@="C:\WINDOWS\Help\Tours\htmlTour\klbvejnk.exe"

[software\Classes\CLSID\{E6DFE252-C79A-1A39-A41E-56906D3E84AA}]
@="ljqnqxnwlhbczqrk"

[software\Classes\CLSID\{E6DFE252-C79A-1A39-A41E-56906D3E84AA}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\NetDiag\xrvxszvs.exe"

[software\Classes\CLSID\{E81E3309-BDD5-BC2F-852A-715DB42797F9}]
@="qxectnwxntxxejkq"

[software\Classes\CLSID\{E81E3309-BDD5-BC2F-852A-715DB42797F9}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\mouse\jjlhknhh.exe"

[software\Classes\CLSID\{E995A142-7914-3FE8-D60B-AD05B1EE5EFC}]
@="heeshhskvkssnreb"

[software\Classes\CLSID\{E995A142-7914-3FE8-D60B-AD05B1EE5EFC}\LocalServer32]
@="C:\WINDOWS\Help\hwexrtne.exe"

[software\Classes\CLSID\{EA871865-08D6-D09D-46FD-1F353EB479FC}]
@="xbsnhbnrewrlksjn"

[software\Classes\CLSID\{EA871865-08D6-D09D-46FD-1F353EB479FC}\LocalServer32]
@="C:\WINDOWS\system32\oobe\regerror\kjtzrlbb.exe"

[software\Classes\CLSID\{EB14F04F-488B-81F4-9203-A1A7C1EAE661}]
@="svktsrlzrxxncbns"

[software\Classes\CLSID\{EB14F04F-488B-81F4-9203-A1A7C1EAE661}\LocalServer32]
@="C:\WINDOWS\system32\oobe\isperror\skqbvxsq.exe"

[software\Classes\CLSID\{EB7935A8-CBBC-2CC9-1FFE-716534693637}]
@="zjjwtqhlhvvevbvb"

[software\Classes\CLSID\{EB7935A8-CBBC-2CC9-1FFE-716534693637}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Server\ctjxljxh.exe"

[software\Classes\CLSID\{EC40C1E2-EE92-6F30-D05F-D15B16DBC97D}]
@="tzrjcecvxewnxvek"

[software\Classes\CLSID\{EC40C1E2-EE92-6F30-D05F-D15B16DBC97D}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\jnkwrxnr.exe"

[software\Classes\CLSID\{EC7E5912-D564-0AAC-21C5-A12A9CB288C8}]
@="ktjezkshwjbkjenx"

[software\Classes\CLSID\{EC7E5912-D564-0AAC-21C5-A12A9CB288C8}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\rc\qbrblthb.exe"

[software\Classes\CLSID\{EE289F35-7DEB-B0AF-20F2-690232F44615}]
@="lrtbslntveeqbrth"

[software\Classes\CLSID\{EE289F35-7DEB-B0AF-20F2-690232F44615}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Common\bbsbrlee.exe"

[software\Classes\CLSID\{EF92C14A-BD41-692A-E27C-367A8FDC52A5}]
@="rjqthhjzvshervhh"

[software\Classes\CLSID\{EF92C14A-BD41-692A-E27C-367A8FDC52A5}\LocalServer32]
@="C:\WINDOWS\system32\oobe\cthsnblj.exe"

[software\Classes\CLSID\{EFFB84CB-2818-00BA-CEF5-914848B920AE}]
@="rbesnwhkkchehejl"

[software\Classes\CLSID\{EFFB84CB-2818-00BA-CEF5-914848B920AE}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\crjrhltv.exe"

[software\Classes\CLSID\{F059511F-ED8F-4E6D-1CA0-71D619AFB174}]
@="hhlttzhlenqvqtec"

[software\Classes\CLSID\{F059511F-ED8F-4E6D-1CA0-71D619AFB174}\LocalServer32]
@="C:\WINDOWS\system32\oobe\error\neehnzxl.exe"

[software\Classes\CLSID\{F06E222D-826A-DEBB-DB42-EAFB0908234E}]
@="wjbhbhqltktltnwe"

[software\Classes\CLSID\{F06E222D-826A-DEBB-DB42-EAFB0908234E}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Common\kbzzlwlr.exe"

[software\Classes\CLSID\{F148A717-4004-F18A-39BF-324236EA4566}]
@="lbjskrsxkjhsxsxh"

[software\Classes\CLSID\{F148A717-4004-F18A-39BF-324236EA4566}\LocalServer32]
@="C:\WINDOWS\system32\oobe\actsetup\rkjenssc.exe"

[software\Classes\CLSID\{F33C7334-AADE-9EF5-6DAC-7026EF6CCC05}]
@="wvnjqjjnenrjtqkw"

[software\Classes\CLSID\{F33C7334-AADE-9EF5-6DAC-7026EF6CCC05}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Server\shrnxshq.exe"

[software\Classes\CLSID\{F47CF54F-845E-6CA5-3C6B-EE10C17D4AD5}]
@="xekctnjtvehjjsek"

[software\Classes\CLSID\{F47CF54F-845E-6CA5-3C6B-EE10C17D4AD5}\LocalServer32]
@="C:\WINDOWS\system32\oobe\error\jkhehnjn.exe"

[software\Classes\CLSID\{F59B9001-7B62-FC18-C39A-959985D05ED7}]
@="lnhkwqksleqlkbne"

[software\Classes\CLSID\{F59B9001-7B62-FC18-C39A-959985D05ED7}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\kjqkxtnz.exe"

[software\Classes\CLSID\{F699592F-1B83-75DA-AFEF-3F2E360FBE28}]
@="jxslkchwevkwltqq"

[software\Classes\CLSID\{F699592F-1B83-75DA-AFEF-3F2E360FBE28}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\eskcxkhr.exe"

[software\Classes\CLSID\{F6BFA9DF-28C3-0887-B82C-D27B0183AFF1}]
@="tzcrtjekhhlnthve"

[software\Classes\CLSID\{F6BFA9DF-28C3-0887-B82C-D27B0183AFF1}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\eznnthwj.exe"

[software\Classes\CLSID\{F6E2CBA6-BEB3-0707-4082-DBDCD6B25DCE}]
@="evssqcbbstrbtnjt"

[software\Classes\CLSID\{F6E2CBA6-BEB3-0707-4082-DBDCD6B25DCE}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\sysinfo\jbrhbztz.exe"

[software\Classes\CLSID\{F6FB7DDA-6804-18EB-FF7D-98A6670DE13C}]
@="ehbrhqvtrrjbrhck"

[software\Classes\CLSID\{F6FB7DDA-6804-18EB-FF7D-98A6670DE13C}\LocalServer32]
@="C:\Archivos de programa\Archivos comunes\Microsoft Shared\Stationery\clxlczxq.exe"

[software\Classes\CLSID\{F78FD0B0-9278-DAC5-18A8-ABCD9B80B615}]
@="jbnbtskkkkrsvxbq"

[software\Classes\CLSID\{F78FD0B0-9278-DAC5-18A8-ABCD9B80B615}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\hxxttskn.exe"

[software\Classes\CLSID\{F83557ED-5FD1-739A-99EC-11BA129BF0CE}]
@="krkrhvnctwezrblx"

[software\Classes\CLSID\{F83557ED-5FD1-739A-99EC-11BA129BF0CE}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\sconnect\vznnebet.exe"

[software\Classes\CLSID\{F9C5784C-C3B6-DD55-1C3F-F4AE48481FE8}]
@="htrtbqhqktnnnsss"

[software\Classes\CLSID\{F9C5784C-C3B6-DD55-1C3F-F4AE48481FE8}\LocalServer32]
@="C:\WINDOWS\system32\oobe\html\iconnect\shrtrsbs.exe"

[software\Classes\CLSID\{FA0A69DC-4FD1-49D3-0E33-64A2A116FC63}]
@="qzrshklzjseznbjr"

[software\Classes\CLSID\{FA0A69DC-4FD1-49D3-0E33-64A2A116FC63}\LocalServer32]
@="C:\WINDOWS\system32\oobe\setup\elrbjlrn.exe"

[software\Classes\CLSID\{FB1C0137-43E6-D54E-816F-E7A416DFACDB}]
@="ltetblsjsvkvbqlt"

[software\Classes\CLSID\{FB1C0137-43E6-D54E-816F-E7A416DFACDB}\LocalServer32]
@="C:\WINDOWS\pchealth\helpctr\System\Remote Assistance\Interaction\Common\rbntkevt.exe"

[software\Classes\CLSID\{FECE81BA-3616-7952-F36C-1B8A9FAED60C}]
@="wzvvqbeshstletsh"

[software\Classes\CLSID\{FECE81BA-3616-7952-F36C-1B8A9FAED60C}\LocalServer32]
@="C:\Archivos de programa\VMware\VMware Tools\Guest SDK\vmGuestLibJava\doc\krhwtjeh.exe"

Informe de Registros en \HKEY_LOCAL_MACHINE\SYSTEM :

No se detectaron diferencias

Analisis de trafico

El analisis de trafico no arrojo resultados