Boletines PandaLabs:

La rentabilidad de los falsos antimalware

wwwpandasecurity.com/homeusers/security_info | www.pandalabs.com

Índice

1.- Introducción

En los últimos meses han ganado protagonismo los llamados falsos antimalware también conocidos como rogue antimalware. Este tipo de programas no son novedosos, aunque últimamente están proliferando, ya que reportan un importante beneficio para los ciberdelincuentes.

Últimamente se han detectado numerosos mensajes de spam que distribuyen este tipo de molestos programas. Utilizan la ingeniería social para engañar a los usuarios y los temas más habituales siguen siendo las noticias de actualidad, temas morbosos o los videos de famosos.

Estos programas se caracterizan por mostrar mensajes alarmistas de manera continuada para acabar con la paciencia de los usuarios y que finalmente registren el producto y por tanto desembolsando una cierta cantidad de dinero.

Además, los ciberdelincuentes se aprovechan de que la máxima preocupación de los usuarios en cuanto a los riesgos de Internet es el robo de contraseñas, datos bancarios o información personal del usuario. Por tanto, no hay nada mejor para asustarle que mostrar mensajes alertando que su información personal corre peligro porque su ordenador está infectado con un troyano ladrón de contraseñas.

Para los ciberdelincuentes es relativamente sencillo diseñar estos programas, ya que son muy similares entre ellos y basta con modificar parte de su configuración para obtener un nuevo programa con el que obtener beneficios económicos.

Por lo tanto, es importante que los usuarios puedan reconocer este tipo de programas engañosos y así evitar caer en la trampa. Aunque muchos de estos programas tienen interfaces y funciones muy parecidas a los auténticos antivirus, no son en realidad más que un engaño.

En este artículo explicaremos en qué consisten estos programas, cuáles son las vías de entrada habituales y cómo actuar ante este tipo de amenazas. Asimismo, podrá comprobar a través de una serie de gráficas el notable aumento de este tipo de amenazas que afectan directamente al bolsillo de los usuarios.

2.- Características

En líneas generales, se trata de aplicaciones que informan de una falsa infección en el equipo y que ofrecen una supuesta solución para eliminar dicha infección. Para ello, el usuario debe registrarse y pagar un importe determinado.

A pesar de que en un principio este tipo de herramientas se ofertan como gratuitas, a la hora de registrarse, el usuario finalmente tiene que pagar. Ofrecen análisis online gratuitos, pero los resultados son una farsa. Bien porque alertan sobre amenazas inexistentes o bien porque esas amenazas son instaladas por las propias herramientas. Además, muestran mensajes continuos y molestos de que el ordenador está infectado.

Después de analizar numerosos ejemplares de este tipo de malware, los datos confirman que tienen un comportamiento muy similar, no solo en cuanto al tipo de mensajes que muestran sino también en cuanto a modificaciones en el sistema.

A continuación, enumeramos las características comunes de este tipo de programas:

- Avisos de alertas falsas a través de ventanas emergentes, notificaciones en la barra de tareas y modificación del salvapantallas.
- Diseño y funciones similares a las de los verdaderos antivirus.
- Finalizan el análisis completo del equipo en un tiempo muy reducido.
- Las infecciones que muestran hacen referencia a ficheros inexistentes en el equipo o que han sido descargados por ellos mismos.
- Todos solicitan registrar previamente el producto para poder realizar la desinfección, y este registro siempre conlleva un gasto económico para el usuario.

Respecto a los efectos que producen en el equipo, podemos señalar que realizan numerosas modificaciones en el registro de Windows con el objetivo de hacer creer al usuario que está realmente infectado.

Estas modificaciones tienen las siguientes consecuencias:

- Modifica el fondo de escritorio.
- Establece un salvapantallas diseñado por el propio adware.
- Oculta la pestaña Escritorio y la pestaña Protector de pantalla de las Propiedades de Pantalla. De esta manera, el usuario no puede modificar ni el fondo de escritorio ni el salvapantallas.

Habitualmente, el fondo de escritorio y el salvapantallas que establece el adware contienen mensajes en los que se alerta al usuario de que el ordenador está infectado.

El objetivo que se persigue con estas técnicas es terminar con la paciencia de los usuarios para que acaben registrándose y abonando la cantidad solicitada.

Finalmente, lo que en principio parecía ser gratis, acaba saliendo caro.

Muchos de estos programas se publicitan diciendo detectar más que los demás. La cuestión no es que detecten más que los demás, sino que detectan amenazas inexistentes, o en algunos casos introducidas por ellos mismos en el ordenador.

Se valen de la falsa percepción de que un programa de seguridad que detecta algo que otro no lo hace es mejor, es decir, cuanto más detecte una solución de seguridad, mejor. Pero nada más lejos de la realidad; el hecho de que detecte más no quiere decir que sea mejor, ya que como ocurre en estos casos, muchas veces lo que detecta es falso o inexistente.

El objetivo de este tipo de programas es puramente económico, conseguir que los usuarios adquieran la licencia correspondiente.

3.- Vías de entrada habituales

Uno de los posibles medios de entrada de estos programas en nuestros ordenadores es a través de la visita a ciertas páginas web de dudoso contenido, como páginas web de contenido para adultos, entre otras. Para ello, utilizan la técnica conocida como Drive by download para descargar archivos. Esta técnica permite la descarga automática de un fichero sin conocimiento del usuario aprovechando posibles vulnerabilidades en el ordenador. También se suelen utilizar banners publicitarios que ofrecen descargas gratuitas.

Otro medio de distribución de estos programas es a través de las páginas web de software pirata. Utilizan técnicas de ingeniería social para engañar a los usuarios, ya que renombran los ficheros con nombres atractivos para que los usuarios los descarguen pensando que se tratan de cracks, números de serie...

Sin embargo, los ciberdelincuentes son conscientes de la rentabilidad que supone este negocio y no dudan en poner todos los medios a su alcance para asegurar una buena distribución de estos programas. Así, ya no solo se pueden descargar desde páginas de dudosa reputación, sino también desde páginas web legítimas. En julio publicamos un interesante artículo, Webs legales en jaque, que trata el tema de infección de páginas web legales.

Ahora solo falta conseguir que los usuarios visiten estas páginas web; pero, ¿cómo se consigue esto? A través del spam.

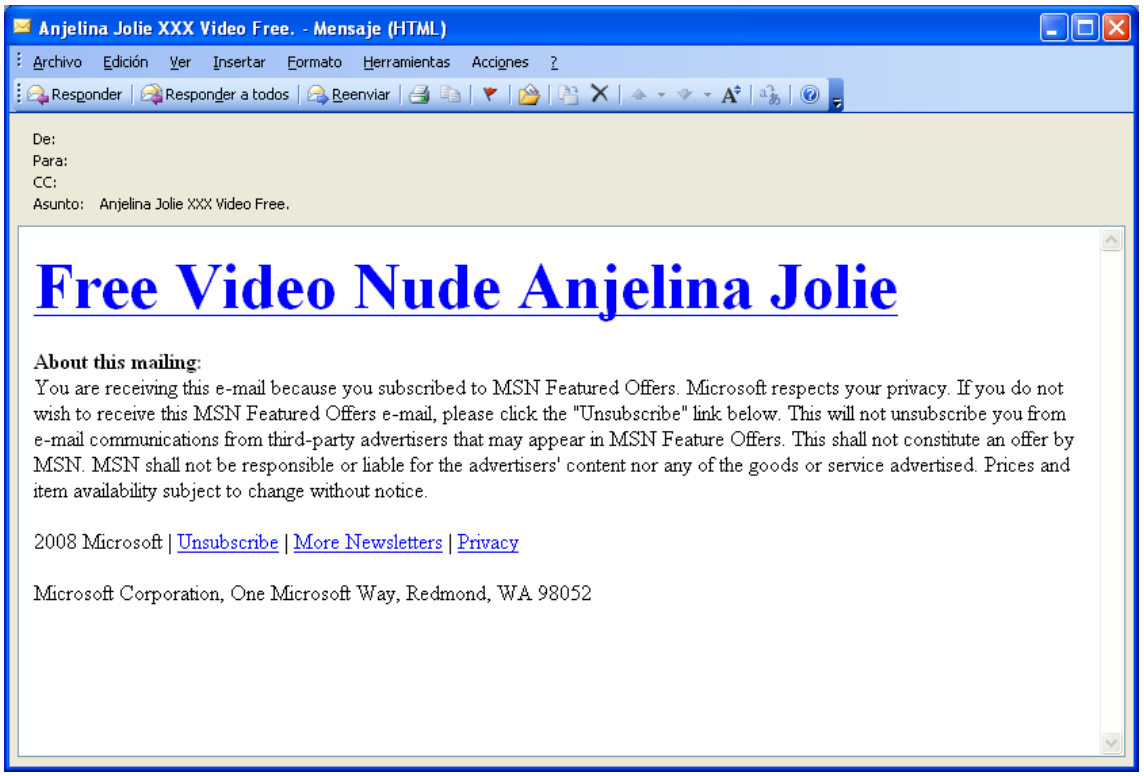
Algunas familias de troyanos como los *Exchanger* y los *Spammer* están diseñados para enviar masivamente mensajes de spam.

Este tipo de mensajes adjuntan el propio adware o incluyen un enlace que apunta a una página web desde donde se descarga el fichero mediante el método Drive by download mencionado previamente.

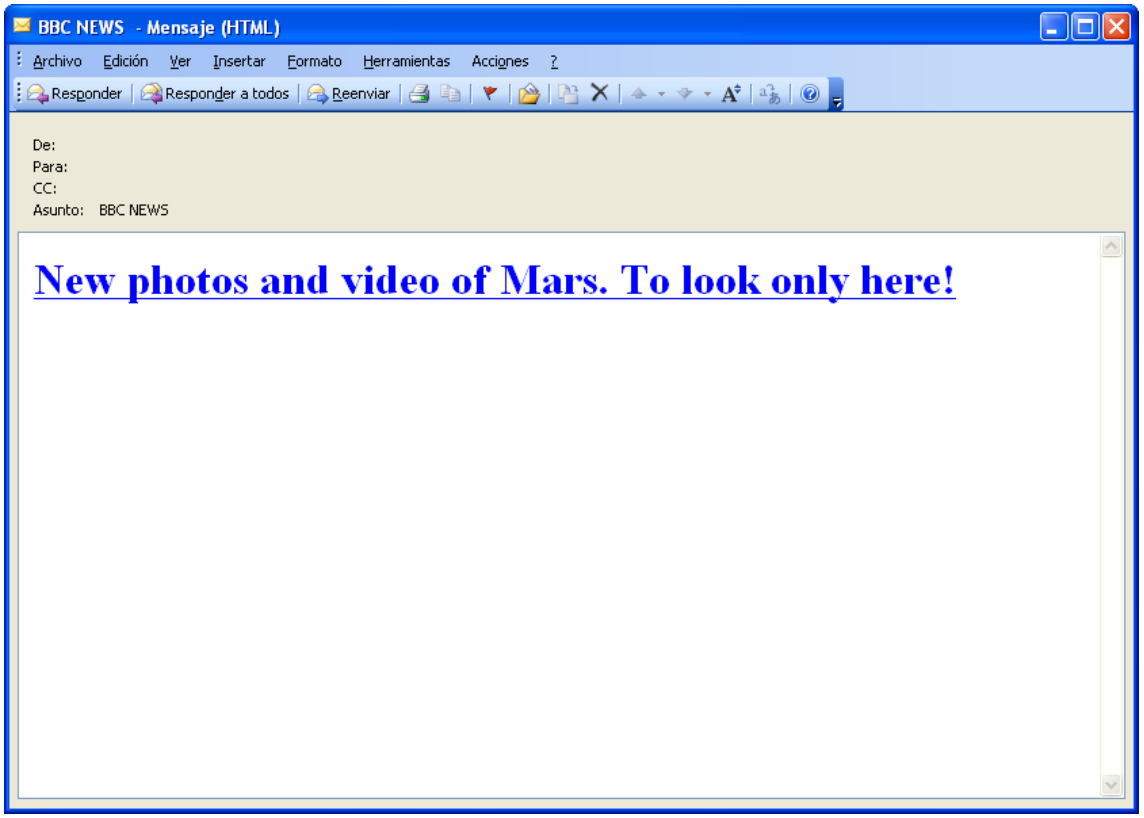
Los mensajes de spam se utilizan para distribuir cualquier tipo de malware, pero hasta ahora lo más habitual era que estos mensajes estuvieran diseñados para distribuir troyanos, sobre todo de tipo ladrón de contraseñas. Sin embargo, en los últimos meses, se ha detectado un cambio en el tipo de malware distribuido a través de spam y ahora son estos falsos antimalware los más utilizados.

Los temas estrella que utilizan para engañar a los usuarios siguen siendo los mismos: noticias de actualidad y videos de famosos.

Las siguientes imágenes corresponden a mensajes de correo electrónico utilizados para distribuir estos programas:



Mensaje sobre un video de una famosa



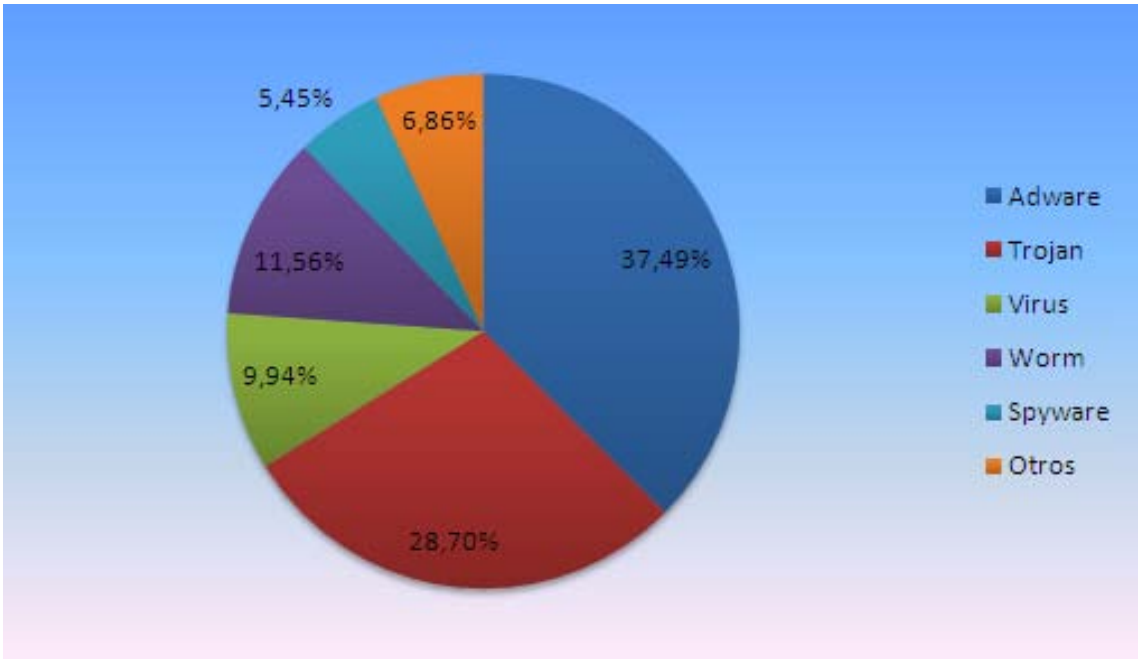
Mensaje de una supuesta noticia de la BBC

Por último, otra vía habitual de entrada de estos programas es a través de malware. Existen ciertas familias de malware que descargan este tipo de programas. Tal es el caso de la familia de los *Nuwar*, o incluso algunas familias de adware que a su vez descargan otros ejemplares de adware, como es el caso de *Adware/Bravesentry*.

4.- Cifras y Datos

En el tercer informe trimestral ya mencionamos el importante incremento que se había producido en la categoría de los adware, debido principalmente a estos programas de falsos antimalware.

Los datos de la siguiente gráfica reflejan que la categoría de adware se sitúa en un 37,49% durante este trimestre (julio-septiembre), mientras que el trimestre pasado el porcentaje era de un 22,03%.

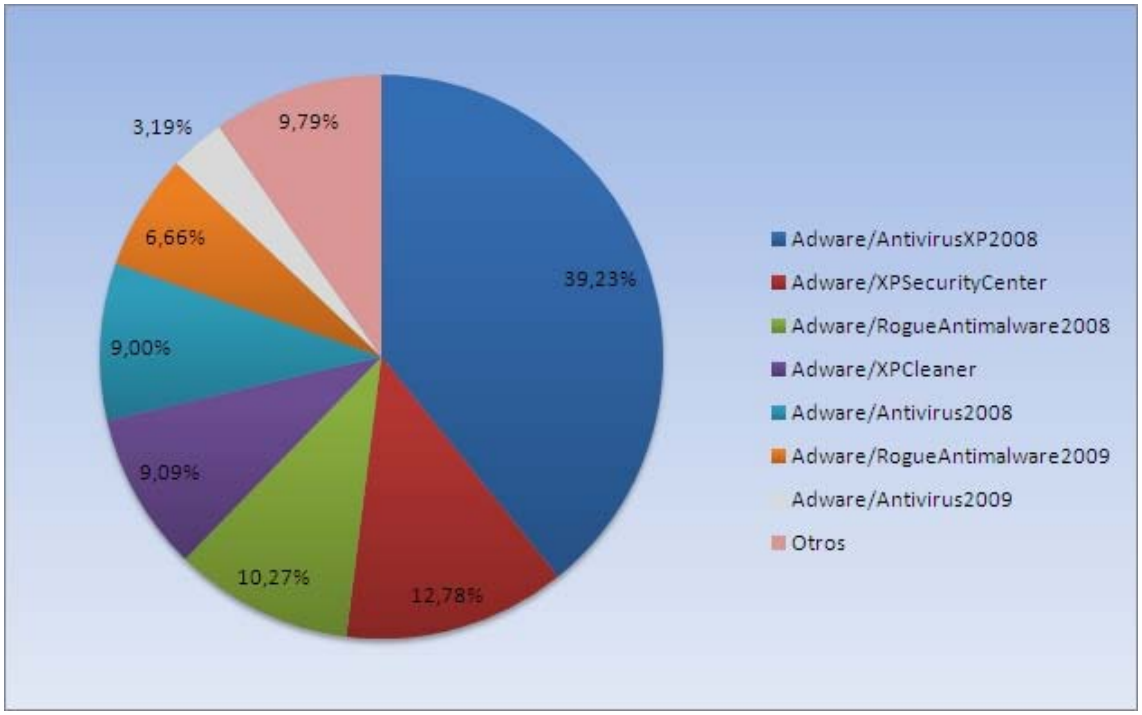


Distribución de malware por categorías

Según los datos recogidos durante el periodo de mayo a agosto, se puede observar que a partir de mayo el número de falsos antispyware ha ido creciendo exponencialmente, alcanzando la cota máxima en julio. A partir de ese mes, parece que la tendencia es a la baja, aunque los niveles siguen siendo muy superiores a los de mayo.

Evolución falso antispyware (mayo agosto)

Respecto a la distribución de los ejemplares más activos, se puede observar en la siguiente gráfica que el adware más activo en los últimos meses ha sido el AntivirusXP2008, con un 39,23% respecto al resto de ejemplares.

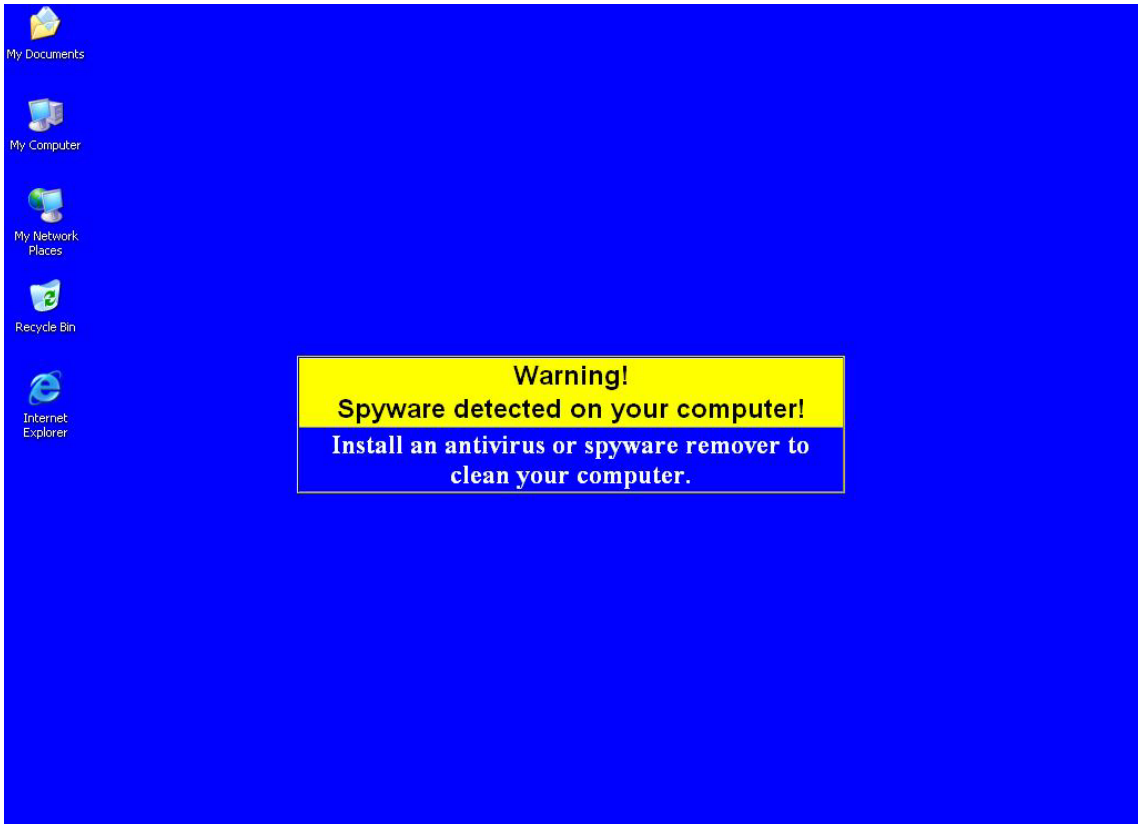


Distribución de ejemplares más activos

Entre los ejemplares que hemos analizado en estos meses, hay uno que no ha destacado por ser el más activo, pero sí por utilizar un salvapantallas un tanto curioso para asustar al usuario: unas cucarachas comiéndose el escritorio.

5.- Análisis a fondo: MalwareProtector2008

Cuando se ejecuta, el adware modifica el fondo de escritorio estableciendo el siguiente:



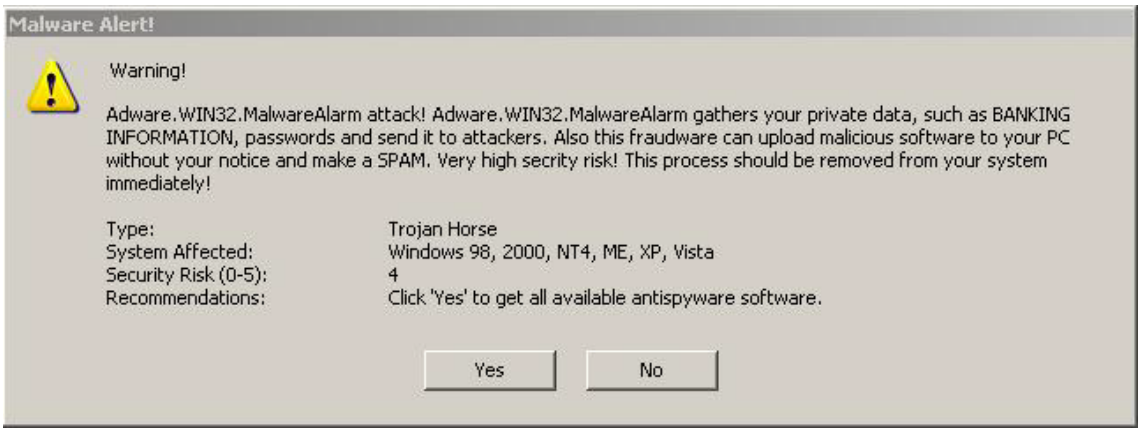
Fondo de escritorio establecido por MalwareProtector2008

En el mensaje se puede leer lo siguiente:

¡Aviso! ¡Spyware detectado en su ordenador! Instale un antivirus o un antispyware para desinfectar su ordenador.

De esta manera tan llamativa, consigue hacer creer al usuario que su ordenador está infectado.

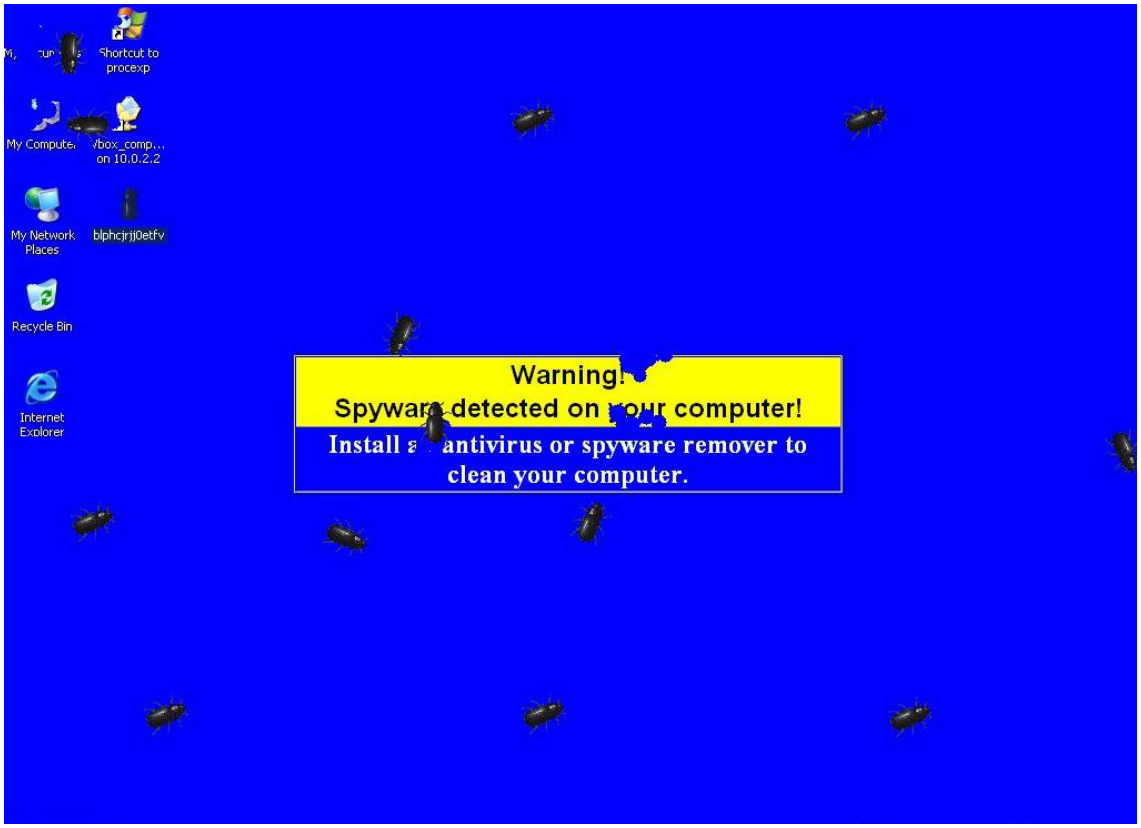
Posteriormente, muestra un mensaje en el que se alerta al usuario de que su ordenador contiene un adware diseñado para robar contraseñas o información bancaria:



Mensaje de alerta mostrado por MalwareProtector2008

Además, se le insta a que elimine dicha amenaza del sistema lo antes posible. Para ello, se le ofrece un software antispyware que desinfectará el ordenador:

En el caso de que no aceptemos el mensaje, se ejecutará cada cierto tiempo un salvapantallas que simula unas cucarachas comiéndose el escritorio:

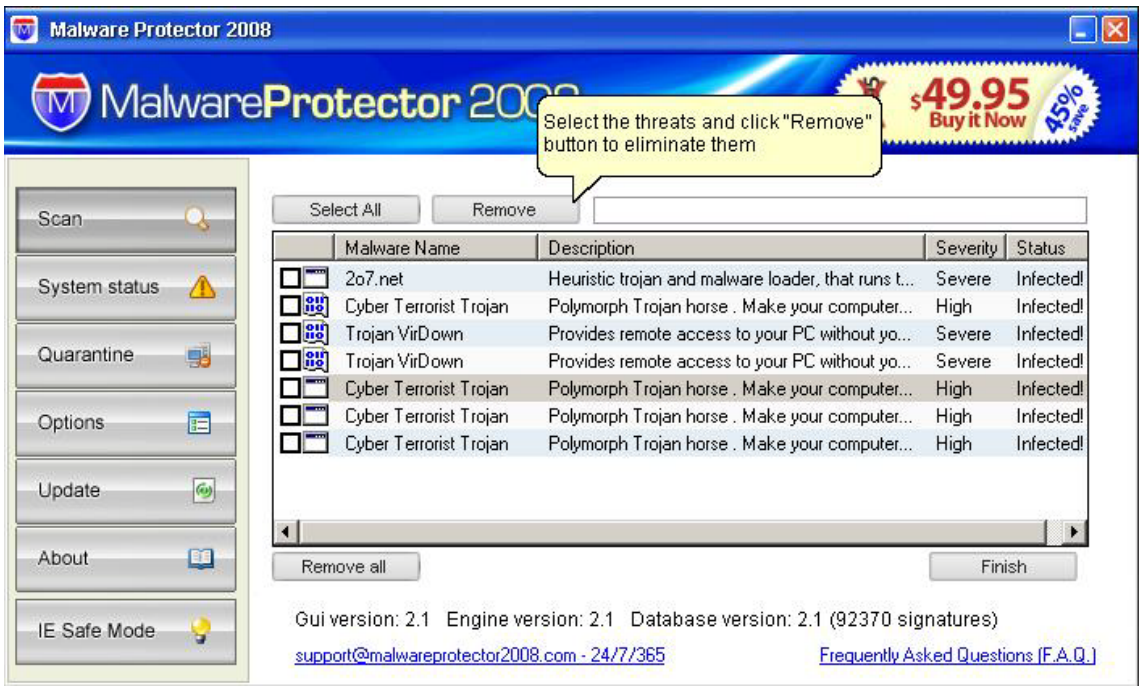


Salvapantallas mostrado por MalwareProtector2008

Esta es otra de las técnicas utilizadas para conseguir que el usuario acabe aceptando el mensaje y descargando un falso programa antivirus.

Si se acepta el mensaje, se procederá a la descarga del falso programa antimalware. Una vez descargado, el programa comenzará a realizar un análisis del ordenador en busca de posible malware.

El resultado del análisis es una farsa y muestra una serie de amenazas que supuestamente han infectado el ordenador:

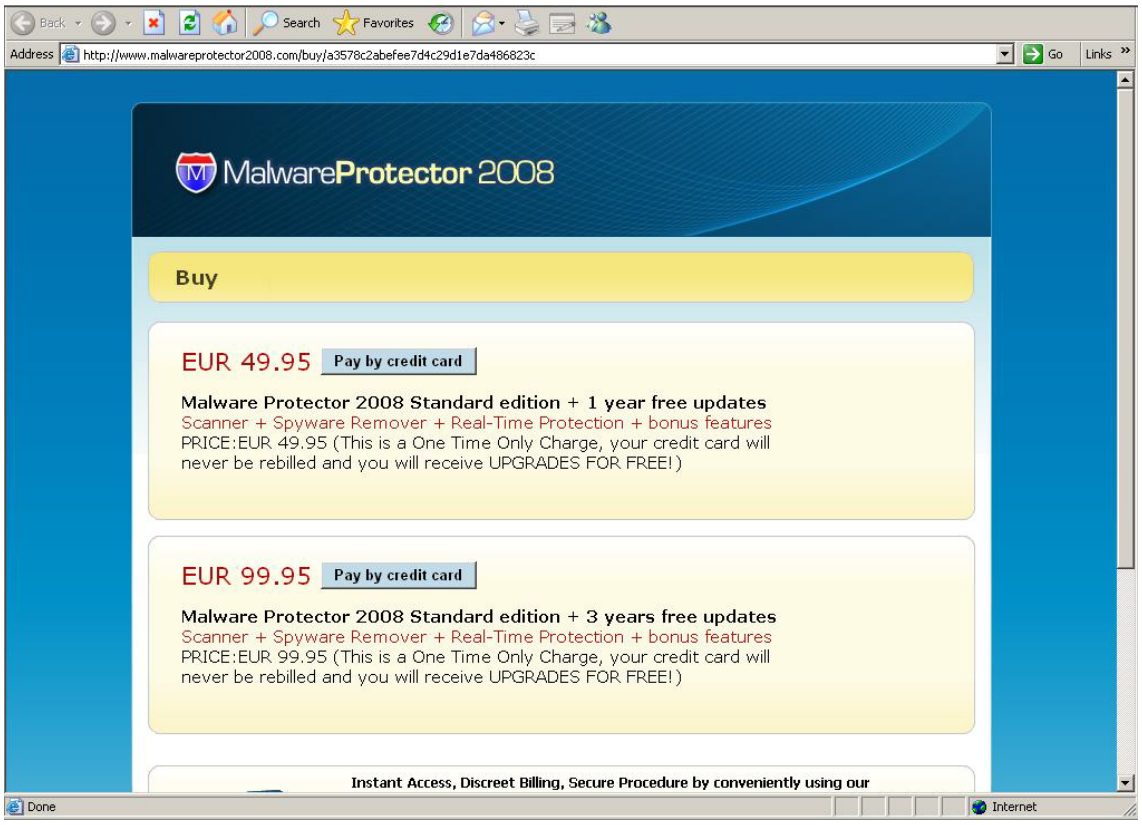


Resultado del análisis realizado por MalwareProtector2008

Si seleccionamos la opción de eliminar el malware, se mostrará una ventana indicando que el ordenador está infectado con adware y spyware y que es aconsejable registrarse para eliminar dichas amenazas y estar protegido:

Interfaz del MalwareProtector2008

Para poder registrarnos, deberemos abonar la cantidad que se indica en la página web a la que se nos redirige al pulsar el botón para obtener el modo completo de la aplicación:



Página web del MalwareProtector2008

Una vez nos hayamos registrado y abonado la correspondiente cantidad, el ordenador continuará desprotegido y vulnerable frente a otro tipo de amenazas.

Las características de este adware son muy similares a las del resto de falsos antimalware: los mensajes de alerta que muestra, la interfaz de la aplicación, el modo de actuación...por lo que este análisis detallado facilitará a los usuarios la identificación de este tipo de programas.

6.- Consejos

El *spam* es el medio habitual utilizado para distribuir este tipo de programas, por lo tanto hay que tener especial precaución con los mensajes de correo electrónico que recibimos con noticias o asuntos llamativos. En estos emails se invita al usuario a seguir un enlace para poder ver el vídeo o las imágenes de esa falsa noticia. Por lo tanto, no debemos hacer click en los enlaces incluidos en este tipo de mensajes, ya que en tal caso podríamos estar descargando en el ordenador uno de estos falsos antimalware.

Desconfía de aquellos programas que no recuerdes haber instalado y que comienzan a mostrar falsas infecciones o ventanas emergentes en los que se te invita a comprar algún tipo de antivirus. Lo más seguro es que en tu equipo se haya instalado alguno de estos programas maliciosos.

Es importante mantener actualizados todos los programas. Un programa no actualizado puede ser un programa vulnerable. Por ello, conviene mantener actualizados todos los programas que se tengan instalados en el equipo, ya que

muchos de estos códigos maliciosos utilizan vulnerabilidades existentes en los ordenadores para introducirse en ellas e infectarlas.

Es conveniente analizar cada cierto tiempo el equipo con un antivirus de confianza, de modo que si alguno de estos ejemplares está residente en el equipo, pueda ser detectado y eliminado.