INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

FALSOS ANTIVIRUS Y ANTIESPÍAS

Intento de fraude a través de la venta de falsas herramientas de seguridad

INTECO-CERT

Octubre 2008

ÍNDICE

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

En las últimas semanas se ha observado un incremento del fraude basado en falsas soluciones de seguridad, en particular antivirus y antiespías.

Esta técnica, que ya fue documentada desde el 2002, apoyada en la ingeniería social, está siendo actualmente explotada de forma masiva con dos finalidades:

- venta de las falsas soluciones de seguridad
- capturar los datos de tarjetas de crédito de los usuarios.

Los ciberdelincuentes intentan convencer a los internautas de la presencia de software dañino en sus ordenadores, con la finalidad de que estos compren sus falsas herramientas de seguridad.

Para ello, no dudan en utilizar todo tipo de llamativos anuncios y mensajes de error – ventanas emergentes con avisos alarmantes, diferentes mensajes modificando el fondo de escritorio, resultados de falsos análisis similares a los de antivirus legítimos… - que advierten al usuario de la infección del sistema y de que sólo es posible desinfectarlo a través de la solución de seguridad que se oferta comprar.

El usuario víctima utiliza su tarjeta de crédito para adquirir la solución recomendada que, en el mejor de los casos, lo único que hará será dejar de mostrar los mensajes alarmantes, y, en cambio los ciberdelincuentes reciben el dinero y los datos de la tarjeta de crédito proporcionados por el usuario.

Hay que destacar además que la instalación del falso antivirus adquirido, también puede ser aprovechada por los estafadores para instalar otro tipo de código malicioso.

2. MÉTODOS UTILIZADOS PARA EMBAUCAR A LOS USUARIOS

Los métodos utilizados para embaucar a los internautas y hacerles llegar todos estos mensajes alarmistas son varios y muy diversos, y no siempre requieren de una infección previa:

- **Al visitar una página Web fraudulenta.** Páginas de apariencia profesional, donde se muestra información falsa, que advierte de la detección de código malicioso en el sistema. A estas páginas se puede llegar:
    - a través de enlaces en otras Web. Páginas legítimas que han sido comprometidas, enlaces en redes sociales y foros…
    - al pulsar enlaces en aplicaciones de mensajería instantánea. Un ordenador comprometido envía a sus contactos direcciones de la página maliciosa para que el contacto lo pulse y sea redirigido a la página maliciosa.
    - a través de correo no deseado (spam). Publicidad de antivirus gratuitos o actualizaciones de seguridad falsas, que aparenta ser enviados por el fabricante del producto. El fin es que el usuario visite la página fraudulenta.
- **Mediante una infección previa. En ocasiones el código del virus es relativamente inocuo, creado únicamente con la intención de asustar al propietario del sistema para que compre el nuevo y falso antivirus.**

3. UN CASO DE USO: VISITA DE UNA URL FRAUDULENTA

Se recibe una ventana emergente, correo, mensaje por mensajería… donde se indica una URL desde la cual se puede descargar un antivirus.

Al conectarnos a esta Web se obtiene un "supuesto" análisis en línea de nuestra maquina que indica que está infectada por numerosos virus.

Es destacable que el análisis da resultados sin importar el sistema operativo que se tiene, como se puede observar en la siguiente captura realizada desde un ordenador con un sistema operativo GNU/Linux instalado.

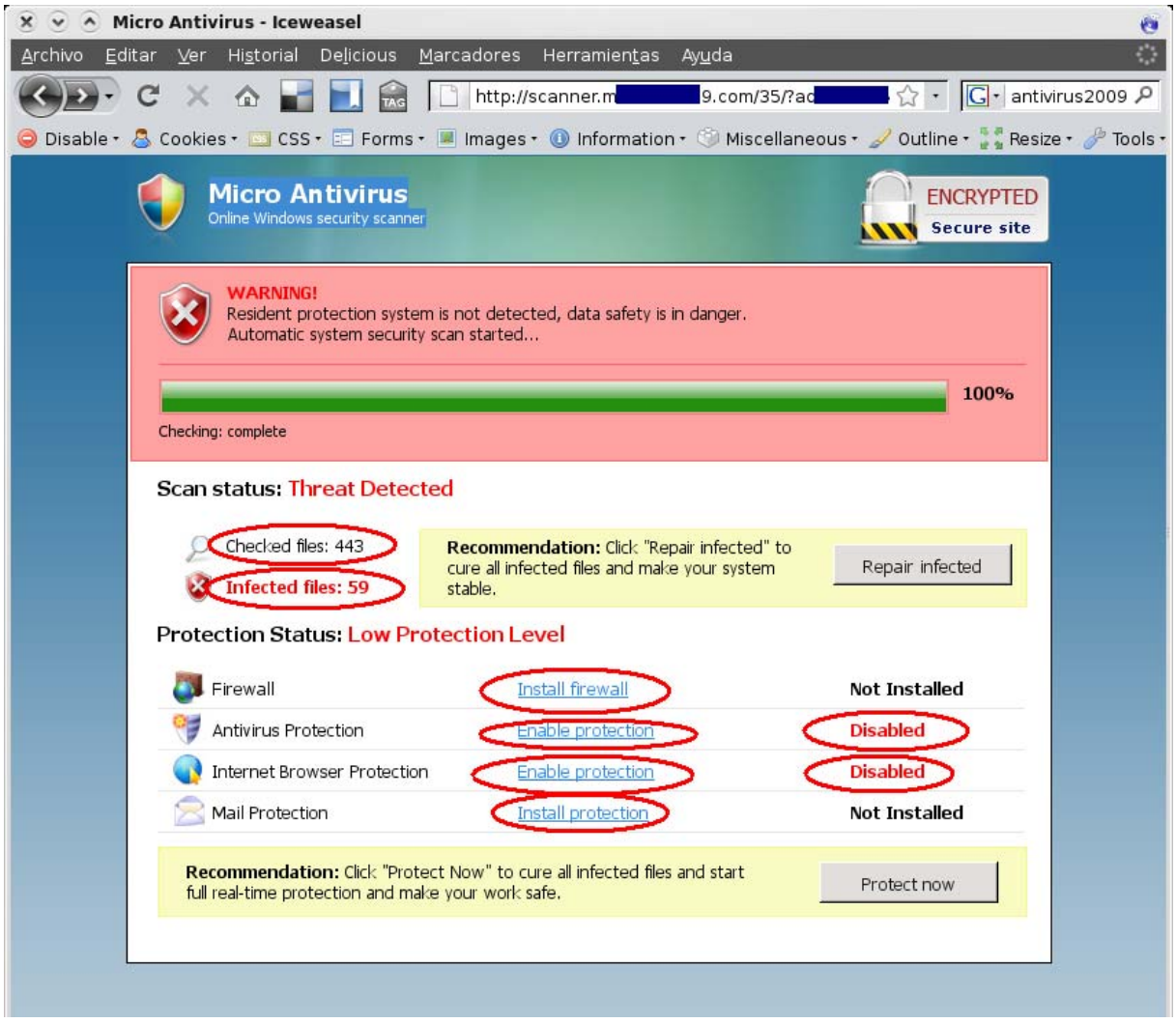

Ilustración 1: Captura del falso análisis en línea mostrado tras visitar la URL fraudulenta.

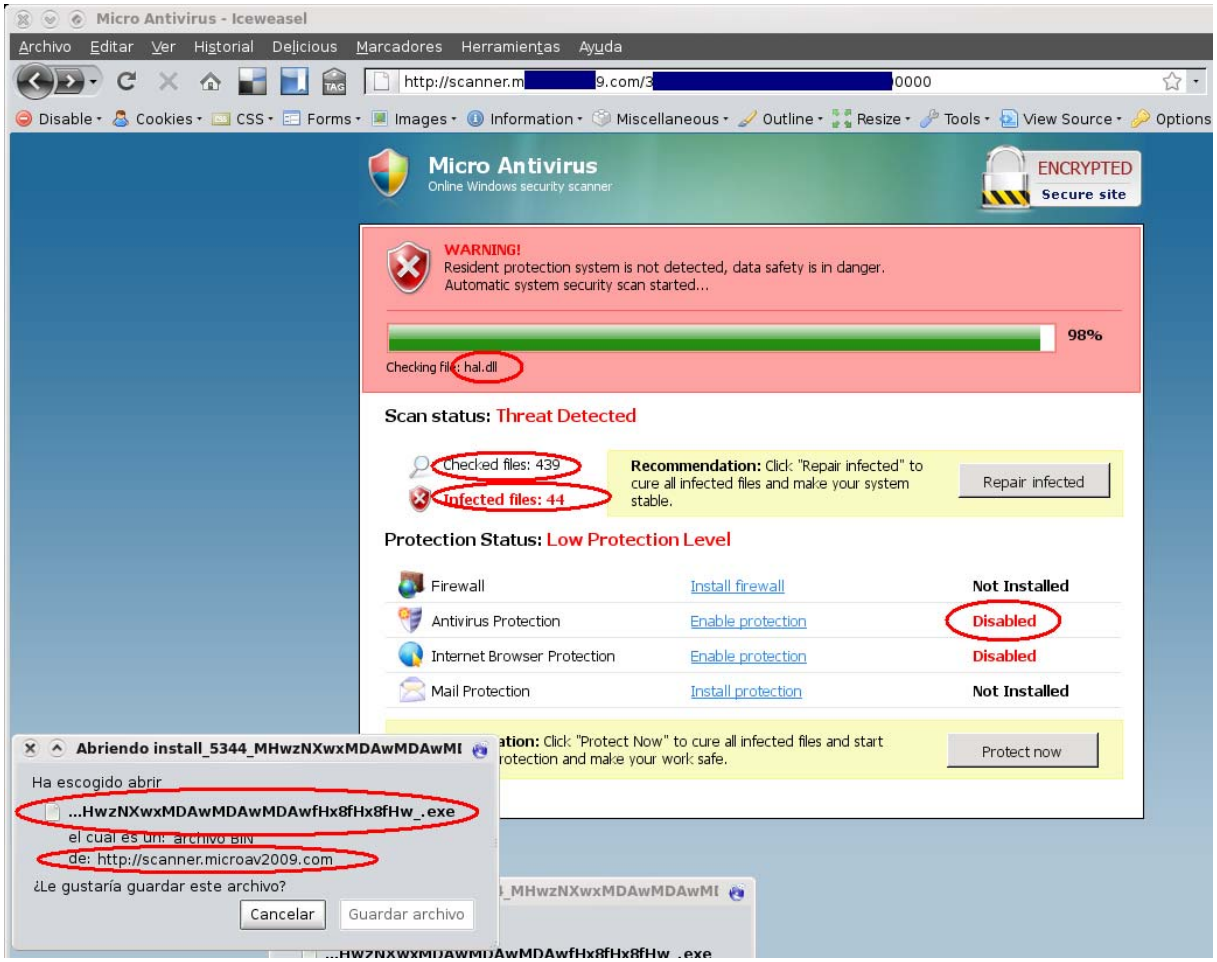

Ilustración 2: Captura de la página maliciosa en el momento de la descarga del falso antivirus.

Una vez instalado el falso antivirus, se solicita su registro, para lo cual, desde la nueva herramienta, se conduce al usuario a una página Web que pregunta la versión que se va a registrar y los datos para el cargo en la cuenta bancaria. Es a partir de este momento cuando datos bancarios confidenciales son entregados al estafador.

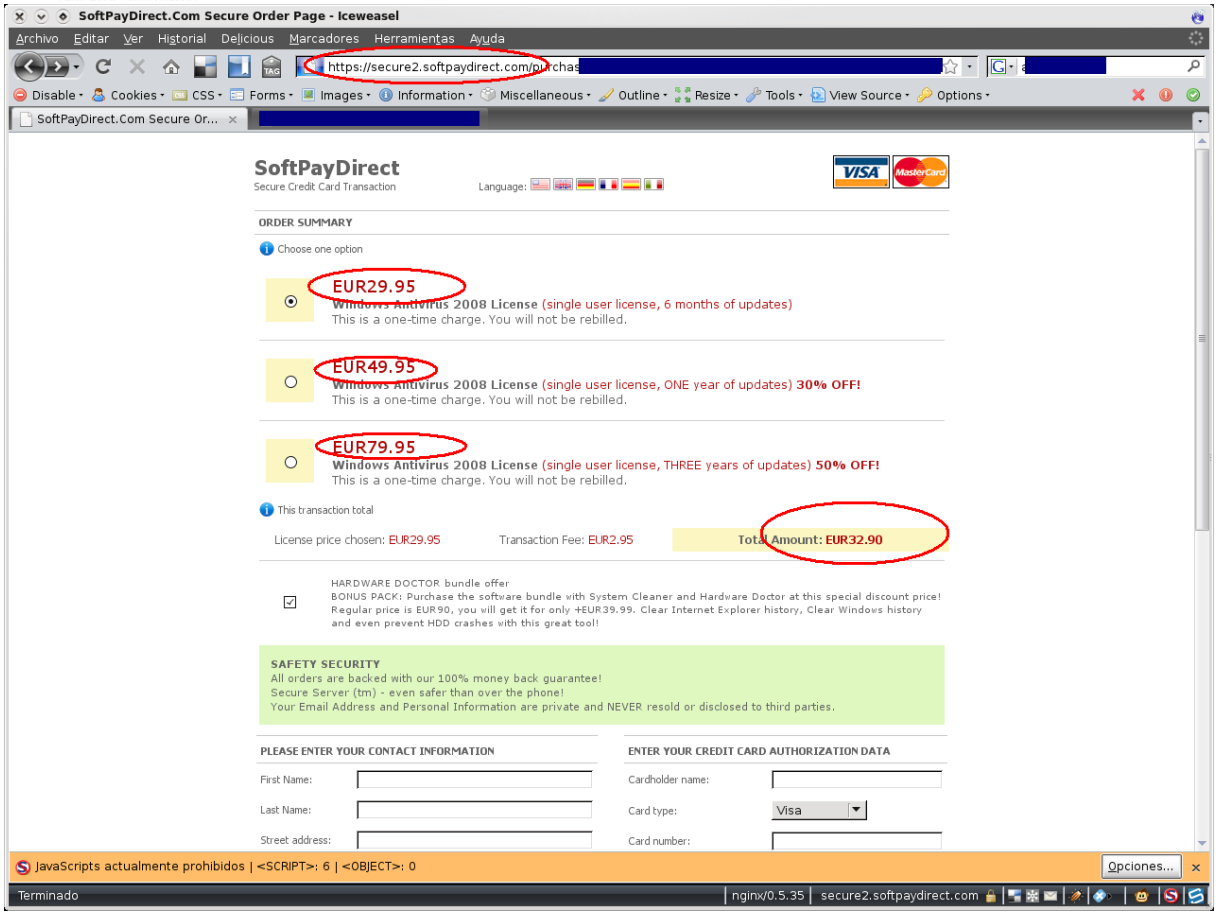

Ilustración 3: Captura del formulario de registro del falso antivirus.

Un detalle que debería despertar la sospecha sobre la existencia de un fraude, es que el formulario solicita el código CVC2, que permitirá al atacante realizar cargos a la tarjeta bancaria sin necesidad de que el usuario infectado apruebe dicha operación.

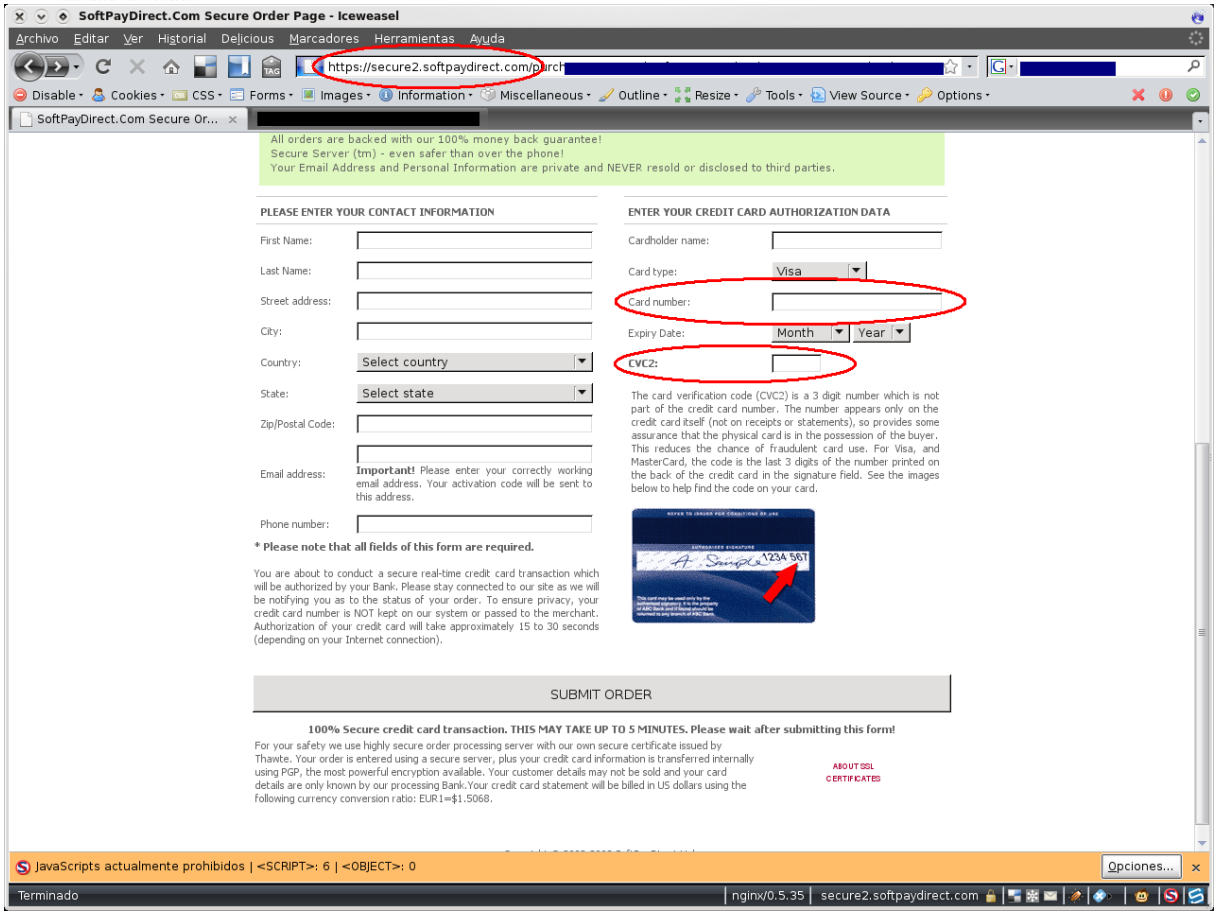

Ilustración 4: Captura del formulario de compra del falso antivirus.

4. CONCLUSIONES

La distribución de supuestos antivirus o antiespías, como el descrito en este documento, proporciona al estafador una vía no sólo para hacer que el usuario pague por algo que no hace nada, si no que además pondrá a disposición del distribuidor de la estafa un acceso al equipo del usuario que podría ser utilizado para infectar el ordenador con un troyano bancario u otro tipo de código malicioso.

Además, a través de este tipo de engaños, los defraudadores disponen de los datos de la tarjeta bancaria del usuario que podrían ser utilizados posteriormente.

Hay que destacar también cómo, una vez más, las técnicas de ingeniería social utilizadas por los estafadores consiguen generar temor en el usuario y convencerle de que realice determinadas acciones. Como siempre, ante este tipo de amenazas, el sentido común es el arma más efectiva.

Este tipo de actividades pueden llegar a dar grandes beneficios a los atacantes. Durante el estudio realizado por INTECO-CERT sobre una página con este propósito, se contabilizaron alrededor de unos 800.000 usuarios infectados que estarían realizando los correspondientes pagos con sus tarjetas de crédito, con lo que el importe defraudado podría ser muy significativo.

5. PREVENCIÓN

Desde INTECO-CERT se proponen las siguientes recomendaciones para evitar ser víctima de este tipo de fraude:

1. **Mantener el antivirus y el antiespías correctamente actualizado**, con las últimas firmas de virus.
2. **No pulsar sobre ningún pop-up** que muestre mensajes publicitarios de soluciones antivirus y antiespías. No hay que confiarse, los falsos antivirus imitan en apariencia a los popularmente conocidos.
3. Ante **mensajes alarmistas** en el ordenador, se recomienda **no interactuar** con ellos, como, por ejemplo, no pulsar el botón desinfección en un mensaje de análisis falso o usar el ratón para cerrar la ventana. Mejor pulsar la combinación de teclas control + alt + supr (o delete en algunos teclados) para ver la lista de programas en ejecución, y eliminar los sospechosos. Se recomienda consultar esos procesos desde otro ordenador para ver su legitimidad.
4. **No descargue antivirus ni antiespías de fuentes no confiables.** Desde la sección de Útiles Gratuitos de INTECO-CERT dispone de una amplia gama de soluciones.
5. **Evite páginas Web de dudosa legitimidad**. En la sección de Útiles Gratuitos – Análisis de URLs hay un listado de herramientas para el análisis de direcciones de páginas Web. Estas herramientas ofrecen un indicador al visitar cada página durante la navegación (y los enlaces que esta contiene) que nos ayudará a determinar si el acceso a dicha URL puede afectar o no a la seguridad de nuestro sistema.
6. **No hacer uso de los enlaces de correo electrónicos** que vengan de fuentes que no sean de confianza.
7. **Mantenerse informado** a través de servicios de seguridad como el de INTECO en www.inteco.es o http://cert.inteco.es