

Un virus porno es utilizado para extorsionar a los internautas, advierte Trend Micro

- Denominado Kenzero, este troyano japonés se instala en los equipos que usan el popular servicio de intercambio de archivos Winni, utilizado por más de 200 millones de personas, y exige el pago de una cantidad económica para solucionar una supuesta violación de la ley de derechos de autor.

Bogotá, 19 de abril de 2010 – Trend Micro, líder global en seguridad de contenidos en Internet y para centros de datos dinámicos, alerta de la aparición de un **nuevo troyano** que ha comenzado a circular en Japón. Este malware ha sido **creado para realizar un chantaje económico a sus víctimas**.

A continuación se explica cómo funciona:

Según explica **Rik Ferguson, Asesor de seguridad de Trend Micro**, las víctimas son captadas cuando deciden descargar de redes para compartir archivos lo que creen que van a ser copias ilegales de juegos. En la mayoría de los casos el malware está disfrazado bajo copias ilegales para menores de 18 años de juegos de temática *hentai*, un cómic japonés de carácter pornográfico.



Figura 1: ejemplo de juego japonés legal

Una vez instalado el malware en el equipo del usuario, éste debe cumplimentar un formulario con sus datos personales, incluyendo su nombre completo, fecha de nacimiento, password del juego, dirección de email, dirección postal, sexo, ingresos anuales, nombre de la compañía y teléfono, entre otros datos, justificando que éstos son para realizar un mejor seguimiento.

Mientras el usuario está cumplimentando esta información, el malware está recopilando automáticamente otros detalles sobre el equipo de la víctima, como son la cuenta de usuario, el dominio, el nombre del equipo, información sobre la versión del sistema operativo, contenidos de la memoria, historial del uso de archivos y los favoritos de Internet Explorer. Asimismo, también captura pantallas de las páginas visitadas.

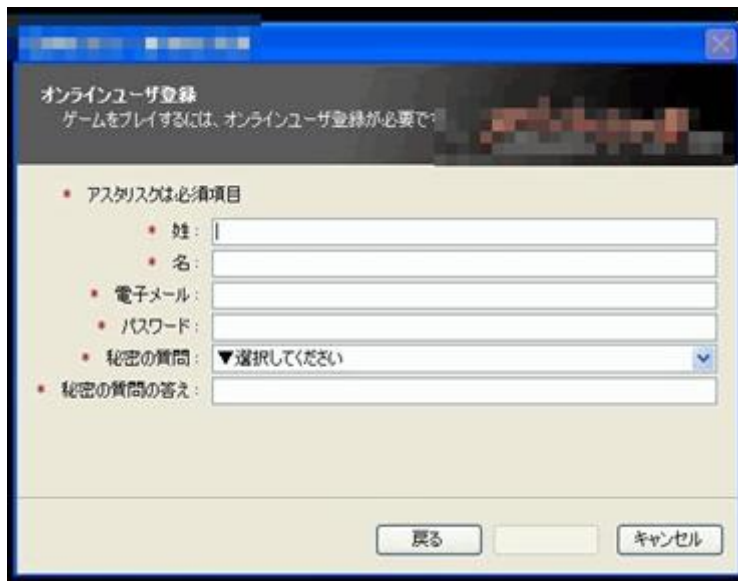


Figura 2: información que solicita el troyano

Toda esta información lo que hace es que, además de infectar los ordenadores que comparten archivos en red, también publica el historial de algunas páginas visitadas en un sitio de Internet para, posteriormente, chantajear al usuario que desee retirar su nombre de éste.

El troyano japonés se instala en los equipos que usan el popular servicio de intercambio de archivos conocido como Winni, que es utilizado por hasta **200 millones de personas**. Denominado **Kenzero**, el malware ya está siendo monitorizado y controlado por Trend Micro.

Lo que hace este troyano es publicar online algunas imágenes de las páginas visitadas con el nombre del usuario, para luego enviarle un email exigiendo un pago con tarjeta de crédito con el fin de “resolver así la violación de la ley de derechos de autor”, tal y como aclara **Ferguson**, y proceder a retirar la página.

El email procede de una compañía llamada “Romancing Inc” (que casualmente también poseen el dominio donde la información robada ha sido publicada) y que alertan de la complicada situación al usuarios ofreciéndose a resolver la infracción de los derechos de autor mediante el pago de una cantidad. La compañía está registrada bajo el pseudónimo de Shoen Overns.

*“Anteriormente hemos visto ese nombre asociado a los virus troyanos Zeuz y Koobface. Se trata de una banda criminal establecida que sigue involucrada en este tipo de actividad”, apunta **Ferguson**, que añade que “Kensero es una modalidad de ransomeware (malware*

para extorsionar) que infecta el ordenador y codifica los documentos, imágenes y música almacenadas, antes de exigir un pago para proporcionar una clave que los descodifique”.

“Sin embargo, en lugar de coger el dinero, la organización vende los detalles de la tarjeta de crédito”, tal y como explica **Ferguson**, que aconseja “ignorar el chantaje y utilizar un programa online gratuito para escanear y detectar los programas maliciosos, pues siempre es mejor descargar contenido de sitios de confianza”.

Es muy probable que los atacantes tengan guardado un as bajo la manga en forma de trampa, pues el instalador también coloca algún archivo mp3 en el equipo de la víctima con nombres como Back Duck, Chukar y Quail. Estos archivos mp3 se encuentran a la venta en una web a un elevado precio (58 millones de yenes, lo que equivale a unas 402.000 libras esterlinas).

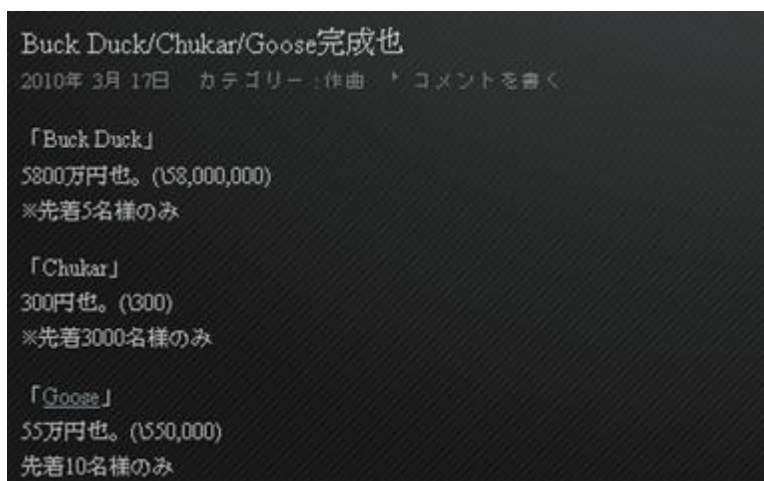


Figura 3: música a la venta....

Ferguson señala que hay una variante que está afectando a usuarios en Europa.

¿Podría ocurrir que una vez que el usuario haya sido víctima de una extorsión sea de nuevo extorsionado con otra notificación de Romancing Inc sobre “violación de los derechos de autor”? La ley japonesa sobre copyright ha sido reforzada en gran parte para abordar el problema de las descargas ilegales.