Asunto: Ciudadanos infectados con el “virus de la Policía”

Información Pública

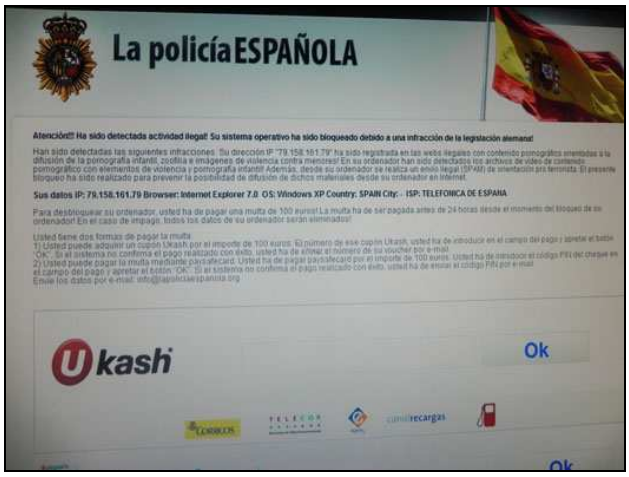
Introducción

La presente nota informativa recoge como actuar en el caso de que se detecte que un ciudadano ha sido infectado con el denominado comúnmente como “virus de la policía”.

Análisis

Existe un tipo de malware que está afectando a multitud de ciudadanos españoles con ordenadores **Windows**. Dicho malware **bloquea el equipo** a los usuarios con mensajes falsos en nombre de **“La policía Española”** y solicita el **pago de una multa** de 100€ para desbloquearlo.

Al ejecutarse dicho malware aparece en pantalla un mensaje en el que se muestra la dirección IP del equipo infectado indicando que desde ese equipo se ha descargado material pedófilo y que por tanto tiene que pagar una multa, añadiendo también las instrucciones para el pago de la misma a través de **Ukash** o **PaySafeCard** y una casilla para meter el PIN. A continuación una captura de pantalla de un equipo infectado:

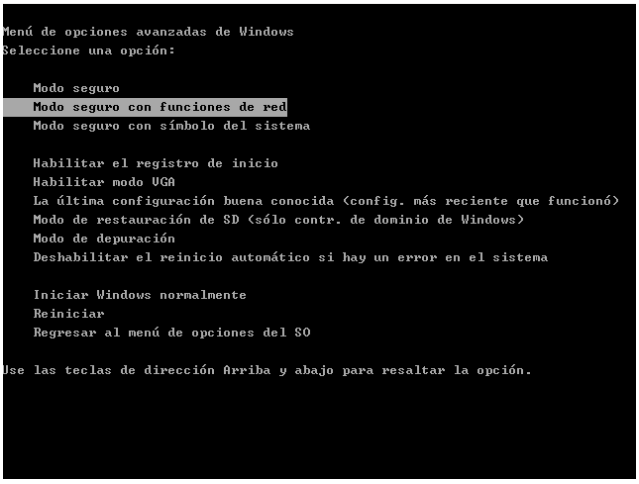


Desinfección

Los **pasos** a seguir para desinfectar un equipo infectado son los siguientes (basados en los publicados por la **Oficina de Seguridad del Internauta** http://www.osi.es/es/actualidad/avisos/2012/01/virus-muestra-un-falso-mensaje-del-cuerpo-nacional-de-policia):

1. **Reiniciar** el equipo (Ir a **Inicio**->**Apagar**->Seleccionar **Reiniciar**).

2. Justo cuando se está reiniciando el equipo presionar repetidamente la **tecla F8** antes de que vuelva a cargarse de nuevo la pantalla de inicio de Windows hasta entrar en el **Menú de opciones avanzadas de Windows.** Con las teclas de dirección Arriba y Abajo (flechas) nos situamos en la opción **Modo seguro con funciones de red,** pulsamos la **tecla Enter** y comenzará el arranque del sistema.



3. Una vez arrancado de nuevo el equipo realizamos una **Restauración del sistema a un punto temporal anterior** cuando el equipo aún no estuviera bloqueado y funcionara correctamente. En la **Oficina de Seguridad del Internauta** nos indican como proceder para hacer una restauración de nuestro sistema (para sistemas Windows 7,Windows Vista y Windows XP) http://www.osi.es/es/protegete/protege-tu-ordenador/restauracion-del-sistema/

4. Si **NO es posible** realizar una restauración del sistema a un punto temporal anterior o aún habiéndolo hecho nuestro equipo continua infectado procederemos a utilizar un programa antimalware, por ejemplo el programa **Malwarebytes Anti-Malware.** Volvemos a iniciar en **Modo seguro con funciones de red,** nos dirigimos a la página de **Malwarebytes Anti-Malware y lo descargamos** desde este enlace http://www.malwarebytes.org/mbam-download.php (la versión gratuita por ejemplo). A continuación, ejecutamos el archivo .exe descargado para instalarnos el programa. Fijarnos en que en el paso donde nos indica **Finalizar** estén marcadas las dos siguientes casillas:

Una vez iniciado este programa, nos dirigimos a la pestaña **Escaner** y seleccionamos la opción de **Realizar un análisis completo**, seleccionamos todas las unidades del equipo y pulsamos **Analizar**:

Al finalizar dicho análisis nos habilitará la opción de **Mostrar Resultados**, pincharemos y podremos ver si en nuestro tenemos algún archivo infectado.

Seleccionamos todos y pinchamos en la opción de "**Eliminar todo**". Probablemente sea necesario reiniciar el equipo. Una vez hecho esto el equipo debería funcionar con normalidad.

NOTA PARA USUARIOS TÉCNICOS: Un análisis técnico del troyano (http://www.hispasec.com/laboratorio/Troyano_policia.pdf) indica que existen dos formas posibles de eliminar el troyano. Una forma sería introducir el PIN: **1029384756** en el cuadro de texto indicado para ello y pulsar OK. Otra forma seria crear un fichero de texto vacío de nombre **pinok.txt** en el mismo directorio donde está el malware y la imagen que suele ser **C:\Documents and Settings\nombre_usuario\Datos de programa\kodak** en Windows XP y **C:\Usuarios\nombre_usuario\Datos de programa\kodak** en Windows 7 y Vista. Ante la persistencia del mismo se recomienda seguir los pasos anteriores.

ACTUALIZACIÓN A FECHA 12 ABRIL 2012: Desde la **BIT** se informa de una nueva herramienta creada por **Hispasec** para "*prevenir (en lo posible) que el malware se ejecute de nuevo al inicio del sistema*", pudiendo así tener un control de las aplicaciones que intentarían cambiar el registro de Windows para ejecutarse al inicio. Mas información y descarga de esta herramienta gratuita en http://unaaldia.hispasec.com/2012/04/hispasec-presenta-winlockless.html

Ayuda

Ante cualquier duda al respecto puede dirigirse a **CSIRT-cv** a través de nuestro formulario de contacto en http://www.csirtcv.gva.es/es/formulario/contacto-y-suscripciones.html o través de las redes sociales en las que estamos presentes: https://www.facebook.com/Csirtcv y https://twitter.com/csirtcv

La **Oficina de Seguridad del Internauta** pone también a la disposición de los ciudadanos un teléfono para consultas, 901 111 121 y un chat http://www.osi.es/te-

ayudamos/soporte-por-chat.

Denuncia

Si un ciudadano desea poner en manos de la policía éste u otro tipo de delito telemático puede dirigirse a la **Brigada de Investigaciones Tecnológicas de la Policía Nacional (BIT)** http://www.policia.es/colabora.php (Apartado de **Delitos Tecnológicos**) o bien al **Grupo de Delitos Telemáticos de la Guardia Civil** https://www.gdt.guardiacivil.es/webgdt/pinformar.php

Referencias

- Sección de alertas de la BIT http://www.policia.es/org_central/judicial/udef/alertas_1.html
- Oficina de Seguridad del Internauta http://www.osi.es/
- Hispasec Sistemas http://unaaldia.hispasec.com/2012/03/whitepaper-estudio-tecnico-del-troyano.html