El ID-01/16 y el ID-02/16 están disponibles en la parte pública de su portal web

Elex y Gozi, los dos nuevos códigos dañinos analizados por el CCN-CERT

- **El CERT Gubernamental Nacional publica ambos informes con sus reglas SNORT, YARA e IOCs correspondientes**

Madrid, 10 de febrero de 2016.- El CCN-CERT ha publicado en la parte pública del portal dos nuevos Informes de Código Dañino:

- **CCN-CERT ID-01/16 Elex**: recoge el análisis de una variante del código dañino "Elex", cuya principal característica es la de redirigir la URL de la página de inicio de los navegadores de Internet a otra que está incrustada en el propio código. Además, lleva a cabo la instalación en el sistema del servicio "*SFFK*", que será el encargado de ejecutar el binario que hace esta redirección y de permanecer a la escucha del servidor de mando y control (C&C) a la espera de recibir la orden para realizar descargas adicionales y ejecutarlas en el sistema.
  "Elex" es un tipo de "Adware" capaz de mostrar al usuario publicidad mientras éste navega por páginas de Internet.
- **CCN-CERT ID-02/16 "Gozi":** recoge el análisis de la familia de troyanos identificada como "Win32.Gozi", que ha sido diseñada para la obtención de información del equipo infectado y su envío a un servidor de Mando y Control (C2) controlado por los atacantes.
  El código dañino tiene embebida una librería DLL que se encuentra ofuscada en el interior de la aplicación, siendo esta librería la que contiene realmente la carga dañina y la aplicación ejecutable.

Los informes recogen las siguientes secciones:

Características del código dañino
Detalles generales
Procedimiento de infección
Características técnicas
Persistencia en el sistema
Conexiones de red
Archivos relacionados
Detección
Desinfección
Información del atacante

10 de febrero de 2016

Además, se incluyen diversos Anexos con regla SNORT, Indicadores de Compromiso (IOC) y Regla Yara.

Pueden acceder a los informes en la sección de Informes Públicos del portal del CCN-CERT.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/
@CCNCERT

http://youtu.be/5XxS9mZZfKs