GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA

centro nacional de inteligencia
centro criptológico nacional

CCN-CERT
centro criptológico nacional

El CCN-CERT publica un nuevo *Informe IA-01/16* contra uno de los ataques más comunes de los últimos años

Medidas de seguridad contra el *Ransomware*

- **El informe, accesible desde la parte pública del portal, actualiza las medidas preventivas y reactivas frente a este tipo de código dañino, así como la restauración de ficheros y su descifrado.**

- **En el año 2015, el Sistema de Alerta Temprana en Internet (SAT-INET) del CCN-CERT gestionó 500 incidentes relacionados con este tipo de ataque, un 150% más que en el ejercicio anterior**

Madrid, 2 de febrero de 2016.- El CCN-CERT ha hecho público un nuevo Informe de Amenazas **IA-01/16 Medidas de seguridad contra Ransomware**, en el que da a conocer determinadas pautas y recomendaciones de seguridad para ayudar a prevenir y gestionar los incidentes de este tipo, cada día más numerosos y agresivos. De hecho, sólo en 2015, el Sistema de Alerta Temprana en Internet (SAT-INET) del CERT Nacional Gubernamental gestionó 500 incidentes relacionados con este tipo de ataques (frente a los 200 de 2014).

Tal y como recoge el informe, en los últimos años, las acciones dañinas de este tipo de malware han ido evolucionando dando lugar a una nueva generación de ransomware denominados "*file encryptors*", cuyo principal objetivo es cifrar la gran mayoría de documentos del equipo. En este caso, la principal herramienta de extorsión será el pago de cierta cantidad de dinero a cambio de la clave que permitirá recuperar (descifrar) los ficheros originales. Las acciones ofensivas de ciertos tipos de ransomware pueden resultar muy dañinas y en un entorno corporativo pueden ser devastadoras, con consecuencias que pueden agravarse aún más si se cuenta con dispositivos de backup directamente conectados con el equipo infectado, ya que algunos tipos de ransomware comprueban cada una de las unidades montadas así como recursos compartidos de red para cifrar también su contenido.

Las acciones ofensivas de ciertos tipos de ransomware pueden resultar muy dañinas y en un entorno corporativo pueden ser devastadoras

El Informe recoge una pequeña introducción así como un listado de medidas preventivas frente a este tipo de código. Posteriormente, y para el caso de haberse producido una infección, se ofrece una serie de medidas generales, junto con la forma de comunicar el incidente y una valoración de escenarios. La restauración de ficheros y el descifrado del ransomware, son los dos últimos capítulos de este informe.

En esta ocasión, se ha eliminado del documento el apartado de Análisis de Ransomware, dado que se incluirán en posteriores Informes de Código Dañino.

2 de febrero de 2016

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 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del ENS.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, a sistemas 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