El documento ID-09/16 Ransom.Locky está disponible en el portal del CCN-CERT

Informe sobre Locky, el ransomware que más está afectando a la Administración y empresas estratégicas españolas

- **En tan sólo dos meses desde su aparición, este código dañino ha sido detectado por el Sistema de Alerta Temprana de Internet (SAT-INET) en 231 ocasiones (el 42% del Ransomware localizado en lo que llevamos de año).**

- **El malware se instala principalmente a través de documentos de Word enviados por correo electrónico o visitando una página web comprometida desde un navegador no actualizado.**

Madrid, 26 de abril de 2016.- El CCN-CERT ha publicado en la parte pública de su portal el Informe de Código Dañino: **CCN-CERT ID-09/16 Ransom.Locky,** un malware cuya primera aparición conocida data del 16 de febrero de este año y que se ha ido modificando en tres ocasiones. Este código dañino, que ha sido detectado en 231 ocasiones a través del Sistema de Alerta Temprana del CCN-CERT (en las administraciones públicas y en empresas españolas de interés estratégico), también está siendo especialmente peligroso en hospitales estadounidenses.

El informe recoge el análisis de este Ransomware que se distribuye mayoritariamente mediante documentos Word con macros dañinas, visitando una página web comprometida con un "Exploit Kit" desde un navegador no actualizado o ejecutando el código dañino si se realiza una descarga por una red P2P.

Como es habitual en este tipo de Informes, el CERT Gubernamental Nacional incluye las siguientes secciones:

- Características del código dañino
- Detalles generales
- Procedimiento de infección
- Características técnicas
- Cifrado y ofuscación
- Persistencia en el sistema
- Conexiones de red
- Archivos relacionados
- Detección
- Desinfección
- Información del atacante
- Reglas de detección (Indicador de Compromiso y Yara)

26 de abril de 2016

Pueden acceder a los informes en la sección de Informes de Código Dañino 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