Revista SiC

El CCN libera para las empresas adheridas al SAT la herramienta REYES al tiempo que certifica el DNI-e 3.0 y publica un nuevo informe sobre ransomware

Realizar una investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes es el principal objetivo de REYES, la herramienta desarrollada por el **CCN-CERT** que ya está disponible, en su última versión, para las organizaciones adscritas al Sistema de Alerta Temprana, SAT -https://reyes.ccn-cert.cni.es-

Esta plataforma se ha creado para agilizar la labor de análisis de incidentes al obtener información contextualizada y correlada con las principales fuentes de información existentes, tanto públicas como privadas. En concreto, dichas compañías podrán acceder a todo tipo de listas negras relacionadas con incidentes –como APT, *botnets*, software malicioso, *ransomware, spam* o la red TOR–; entrar en otras herramientas como MISP (*Malware Information Sharing Platform),* a su vez federada con otras organizaciones como OTAN, FIRST, EGC y otros CERTs; MARTA; o el propio SAT.

DNI-e versión 3.0

Asimismo, el Organismo de Certificación del CCN, al igual que en las versiones 1.0 y 2.0, ha finalizado el proceso de evaluación y certificación del DNIe-DSCF -Dispositivo Seguro de Creación de Firma- en su versión 3.0, desarrollado por la **Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda**, a solicitud de la **Dirección General de la Policía**. La evaluación se ha realizado siguiendo la metodología Common Criteria -ISO 15408- para el nivel de garantía EAL4+ (AVA_VAN.5) y conforme a los estándares europeos para dispositivos cualificados de creación de firma.

La funcionalidad de seguridad certificada del DNI-e 3.0 incluye, entre otras, la capacidad de generar internamente y de manera robusta parejas de claves (pública-privada) para la creación de certificados electrónicos, generación de firmas electrónicas y autenticación del firmante mediante contraseña y biometría.

Buenas prácticas frente el *ransomware*

De forma paralela, el Centro también ha publicado un informe de buenas prácticas frente al *ransomware*. Un tipo de ataque del que el CCN-CERT gestionó un total de 2.030 incidentes relacionados en 2016, un 375% más que el año anterior.

El documento, titulado "CCN-CERT BP-04/16. Buenas Prácticas. Ransomware" pretende facilitar información, herramientas y procedimientos que permitan, en la medida de lo posible, evitar la infección, recuperar los ficheros si hubiera fallado lo anterior y, en cualquier caso, crear un entorno suficientemente seguro para evitar futuras infecciones o minimizar los daños ocasionados por las mismas.