



Las 35 presentaciones pueden descargarse en el portal www.ccn-cert.cni.es y son fiel reflejo de lo tratado los días 10 y 11 de diciembre en Madrid

Disponibles las ponencias de las VIII Jornadas del CCN-CERT

- El CCN-CERT alaba la magnífica actitud de los expertos al ceder el contenido de sus ponencias y al compartir, de este modo, su experiencia y conocimiento.
- Las ponencias abordan aspectos como el ciberespionaje, los APTs, la persistencia en BIOS, investigaciones digitales de gran escala, cloud computing, comunicaciones móviles, vulnerabilidades en iOS, sistemas de control industrial, o ataques de relay en tarjetas EMV NFC.

Madrid, 19 de diciembre de 2014.- Desde hoy mismo están disponibles en la parte pública del portal del CCN-CERT (<https://www.ccn-cert.cni.es>) las ponencias ofrecidas en las **VIII Jornadas STIC CCN-CERT** los días 10 y 11, en el Colegio de Médicos de Madrid. Son 36 los documentos recogidos y en ellos se plasma a la perfección la altísima calidad de las ponencias y el gran conocimiento de todos los expertos que acudieron como ponentes y que, desinteresadamente, han cedido este material.

En el portal del CERT Gubernamental Nacional pueden encontrarse las siguientes ponencias:

- Inauguración y bienvenida (CCN)
- Novedades CCN-CERT (CCN)
- Gestión de Incidentes en 2014 (CCN)
- Persistencia en BIOS. Estado del Arte (David Barroso, Eleven Paths)
- Homeland - el enemigo puede estar en tu casa (Juan Garrido, Innotec System)
- iOS. Regreso al futuro II (Raúl Siles, DinoSec)

MÓDULO 1: CIBERESPIONAJE/APTs

- China y el ciberespionaje: Sun Tzu, APT1 y los tiempos interesantes. (Antonio Sanz Alcober, S2Grupo)
- El APT de los 26 millones (Vicente Díaz, Kaspersky)
- Ataques avanzados: APT28

18 de diciembre de 2014



- (Ricardo Hernández, FireEye)
- Experiencias y tendencias en investigaciones digitales de gran escala (Carlos Frago, One eSecurity)
- Rootkit, quién te ha visto y quién te ve (Josechu Migoya y Francisco Oca, InnoTec System)
- Cómo defender las comunicaciones personales de ciberataques (Sebastián Rosales –INDRA)
- Caso práctico APT: Cuando las barbas de tu vecino veas pelar... (Antonio Sanz Alcober, S2 Grupo)
- Abuso de la funcionalidad de los sistemas de control industrial. Demo (Joel Sevilla Febre y Óscar Navarro Carrasco, S2Grupo)
- Medidas fundamentales para mitigar el ciberespionaje. La Segmentación (Miguel Sanz y Miguel Ángel Martín, AUTEK)

MÓDULO 2: NUEVAS AMENAZAS, HERRAMIENTAS Y TECNOLOGÍAS

- Ataques de relay en tarjetas EMV NFC con dispositivos Android Demo. (José Vila, Ernst & Young) (Ricardo Rodríguez, Universidad de León)
- Pre-fetching of suspicious mobile apps based on Big Data techniques and correlation (Alfonso Muñoz y Sergio de los Santos - Eleven Paths)
- Ghost in the Shell (Jaime Sánchez, Telefónica)
- Desmitificando el AntiVirus (Abraham Pasamar, INCIDE)
- UEFI Arma de doble filo. Demo (CCN)
- Wearables IT (Jorge Dávila, UPM)
- Desmitificando BAD USB (Josep Albers, ESET)
- Comunicaciones móviles seguras: Selfies y Planes estratégicos. (CCN)
- Sistemas de mitigación DDoS coordinados con la operadora. Experiencia en un entorno universitario. Demo (Alex López, Arbor Networks)

MÓDULO 3: ESTRATEGIA DE CIBERSEGURIDAD. ENS Y CUMPLIMIENTO NORMATIVO

- Seguridad en Cloud Computing. Guía 823 (José A. Mañas, UPM)
- Gestión de Incidentes. Visión del CSIRT-CV (Lourdes Herrero, GVA)
- Adecuación al ENS de la plataforma eAdministración del Gobierno Vasco (Jaime Domínguez-Macaya, Gobierno Vasco)
- Actualización ENS y resultados INES (CCN y Carlos F. Gómez, SEAP-MINHAP)

18 de diciembre de 2014

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es



TALLERES

Taller 1: Herramientas detección APTs

- CARMEN. Detectando lo desconocido...
(CCN y D. de los Reyes- Antonio Villalón de S2Grupo)
- MISP, MARTA Y MARIA
(CCN y Fernando Muñoz y Myriam Sánchez de InnoTec System)

Taller 2: Conociendo al atacante

- Desarrollo de Exploits en Win32
(Ignacio Sorribas WISE Security)

Taller 3: Herramientas cumplimiento normativo

- PILAR. Sendas de Ataque
(José A. Mañas, UPM)
- LUCIA. Demo
(CCN y Joaquín Seco Martínez, CSA)
- CLARA. Demo
(CCN y SIDERTIA)

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, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre 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

#8JornadasCCN_CERT 

18 de diciembre de 2014

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es

