XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

Robando al banco ACME: Ciberasalto

CCN-CERT
centro criptológico nacional

Teniente Coronel
Juan Antonio
Rodriguez Alvarez De Sotomayor

Jefe del Departamento de Delitos Telemáticos.

Unidad Central Operativa (UCO)

GUARDIA CIVIL

jsotomayor@guardiacivil.es

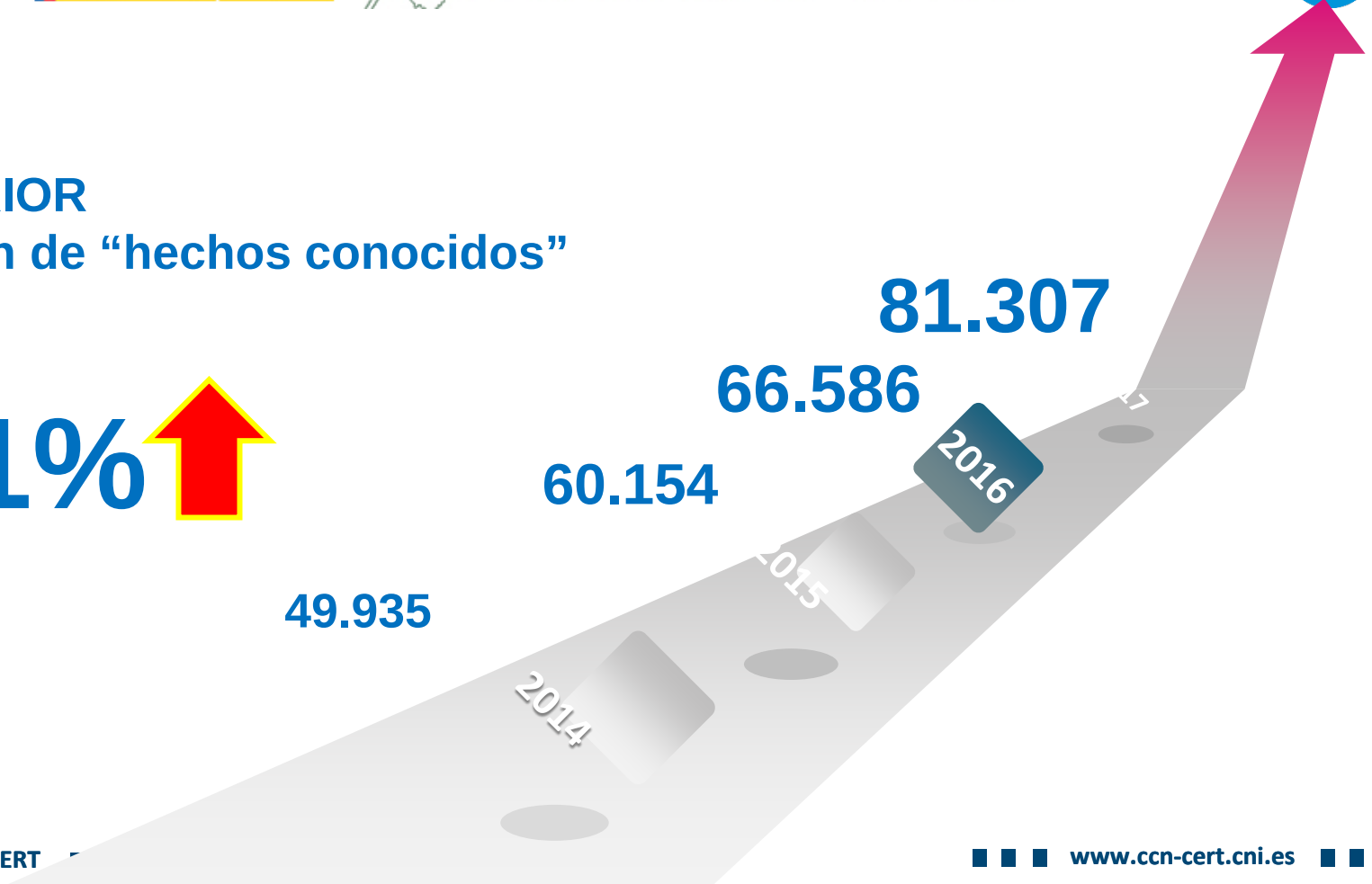
Índice

La gravedad del CIBERCRIMEN

Cibercrimen

Mº INTERIOR
Evolución de “hechos conocidos”

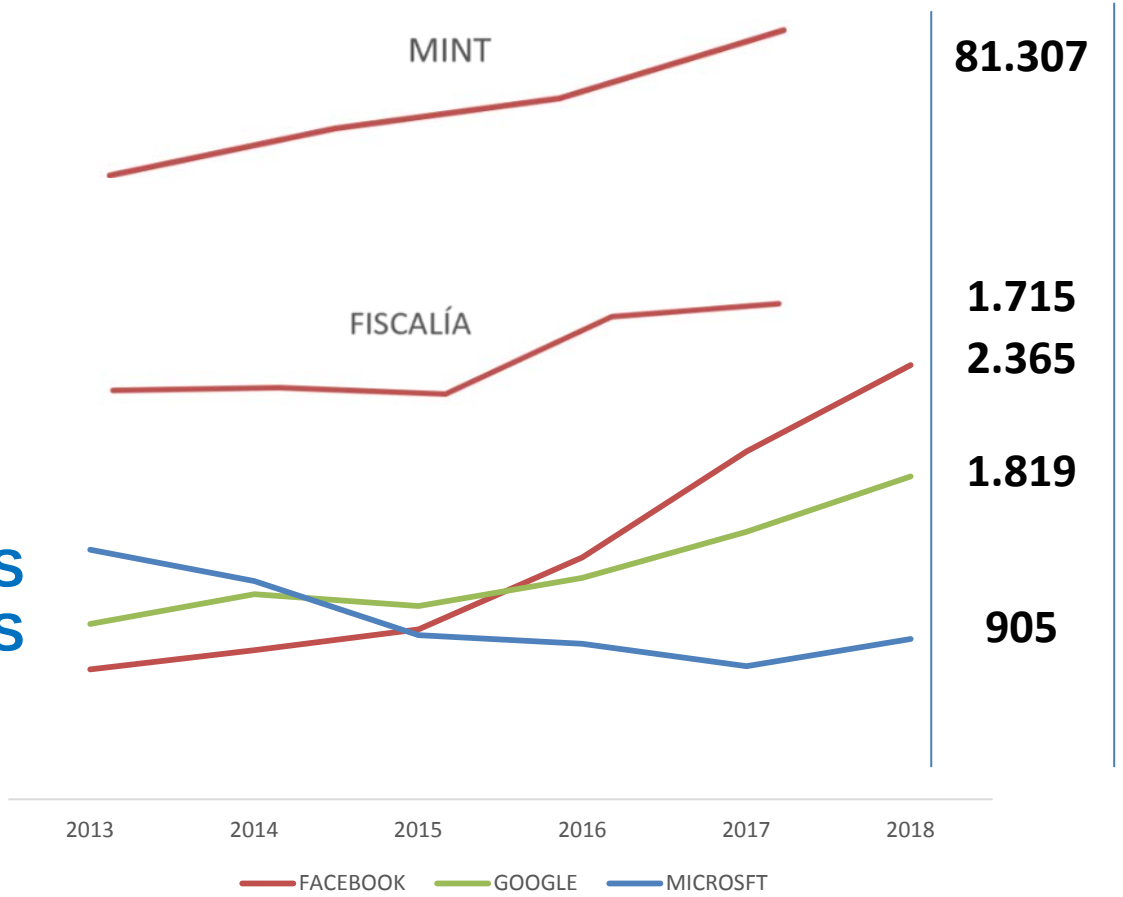
22,1%



DELITOS

ACUSACIONES

REQUERIMIENTOS GUBERNAMENTALES



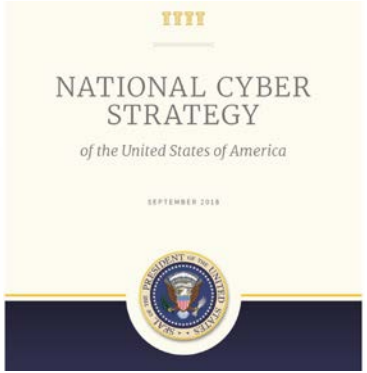
USA NATIONAL CYBER STRATEGY

Pillar I: Protect the American People, the Homeland, and the American Way of Life

Secure Federal Networks and Information

Secure Critical Infrastructure

Combat Cybercrime and Improve Incident Reporting



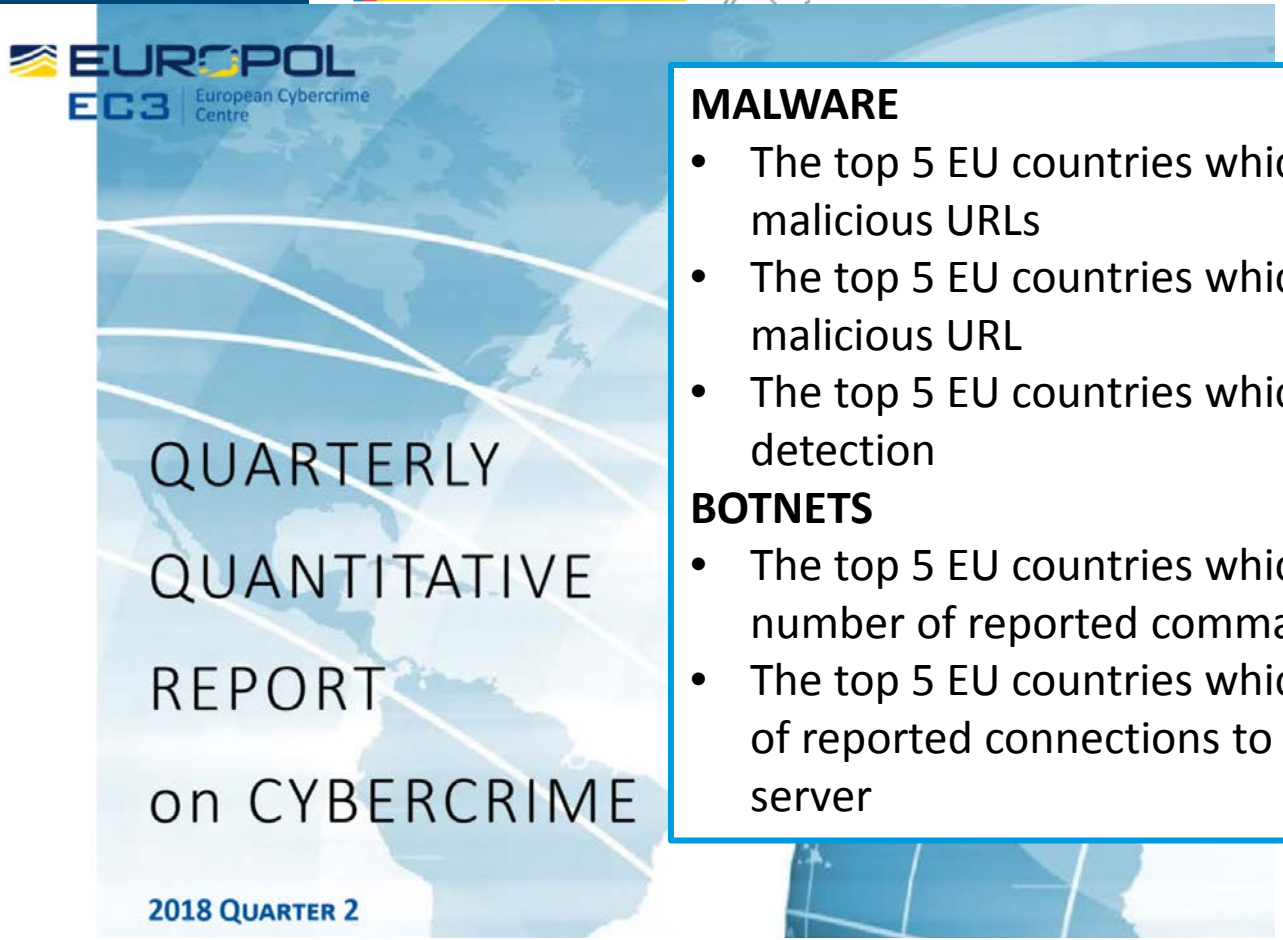
- Mejorar la notificación de incidentes y respuesta
- Actualizar las leyes penales y procesales (interceptación).
- Reducir las amenazas de las organizaciones criminales transnacionales en el Ciberespacio
- Mejorar la detención de criminales en el exterior
- Fortalecer las capacidades de investigación policial en el Ciberespacio de naciones amigas

ORGANISED CRIME GROUPS

STRUCTURE

IOCTA 2018

INTERNET ORGANISED CRIME THREAT ASSESSMENT



MALWARE

- The top 5 EU countries which hosted the most malicious URLs
- The top 5 EU countries which clicked on the most malicious URL
- The top 5 EU countries which had the most malware detection

BOTNETS

- The top 5 EU countries which hosted the highest number of reported command and control servers
- The top 5 EU countries which had the highest number of reported connections to command and control server

El Caso

Una Historia de Phishing

Los ataques de phishing pueden parecer superados tecnológicamente, sin embargo, se están demostrando como un medio potente de hacer dinero fácil.

Podemos identificar 3 roles fundamentalmente:

- La coordinación la operación.
- La disposición de medios técnicos.
- La estructura de medios de blanqueo.

Pueden ser la misma persona….

Diseñando la operación

Persona con amplia experiencia en el diseño de operaciones de phishing y blanqueo.

Lo llamaremos “John”.

Residente en un país del norte de Europa.

Conexiones con grupos organizados dedicados al blanqueo.

Lleva tiempo pensando en realizar un phishing para obtener un importante beneficio económico a corto plazo…

Y lo hace …

¿Qué necesita?

- Un objetivo
  - Se selecciona el Banco ACME, sito en UK
  - Es un buen banco, con muchos clientes.
  - Tiene un contacto dentro que puede proporcionar información.
- Personal especializado en lo técnico
  - Un grupo de personas del “mundillo” con capacidades técnicas.
  - Que tengan acceso a infraestructura informática (para envío de sms), programación, etc.
- Personal especializado en blanqueo de capitales

El Objetivo

El objetivo (I)

Banco muy popular en el mundo anglosajón.

Facturación: 50 mil millones de euros (más o menos)

John tiene una fuente dentro: un director de una de las sucursales de ACME, su amigo Jim.

Ambos se conocen porque Jim ha ayudado en operaciones de blanqueo a John, en otros negocios.

El objetivo (II)

Jim proporciona un listado de teléfonos de clientes de ACME a John.

Además, le dice que no hay problema en realizar las transacciones monetarias una vez realizado el phishing, con los datos de la gente que ha picado.

Jim cobrará un 60% de todo lo recaudado por todo esto, ¿precio de amigos?

Medios Técnicos

El Grupo de Medios Técnicos (I)

Ahora John necesita la infraestructura (grupo de personas) que puedan estudiar al banco ACME y realizar el phishing.

Para ello, en foros ilegales se dirige a varios contactos anteriores con vinculaciones en el “mundillo underground”, y le presentan a Jorge, una persona que trabaja en seguridad informática, con un sueldo escaso, y que ha realizado otro tipo de trabajos para él.

El Grupo de Medios Técnicos (II)

Jorge solo se comunica a través de PGP con John, mediante correos de mail.ru. De hecho, a John la parece fascinante la forma en que Jorge le avisa que hay un nuevo email

Jorge envía una foto de un gatito a John, y eso significa que éste tiene que acceder a su mail.ru dado que tiene un mensaje relacionado con la operación

Comunicación …

El gatito advierte a John que acceda a su mail.ru ….

El Vector de Ataque

Jorge analiza la tecnología de ACME y concluye lo siguiente:

Envío de SMS a clientes del banco ACME, personalizados (gracias a listado proporcionado por Jim), link a web falsa a través de la APP, donde se solicita las palabras clave.

NOTA

- Este banco usa palabras clave en vez de tarjeta de coordenadas.
- Hay seis palabras clave.
- La idea es hacerse con cinco de ellas de cada cliente.

El Vector de Ataque (II)

Datos de clientes

- Listado de un millón de clientes
- Nombre y apellidos
- Obtenidos de hackeos a hospitales, colegios y centros cívicos.

Ataque

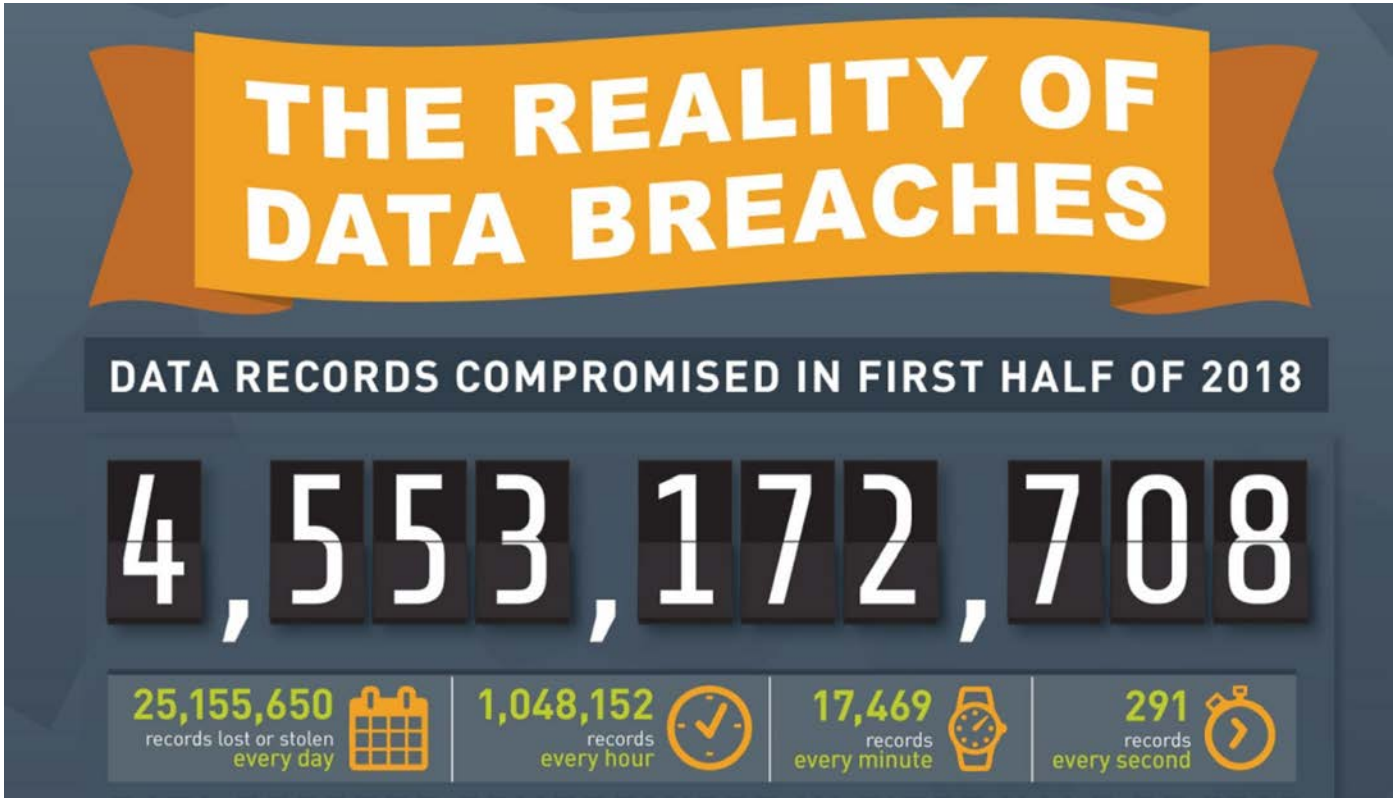
- Envío de SMS, con nombre y apellido
- Se envía a página web falsa, que simula la apariencia de la aplicación móvil.

Obtención credenciales

- Se piden tres palabras clave
- El usuario introduce tres
- La web le indica que hay un error
- Le solicita dos códigos más

Ataque

- En un archivo txt, que posteriormente se envía a John


THE REALITY OF DATA BREACHES
DATA RECORDS COMPROMISED IN FIRST HALF OF 2018
4,553,172,708
25,155,650 records lost or stolen every day
1,048,152 records every hour
17,469 records every minute
291 records every second

Recursos técnicos necesarios

Infraestructura	Qué	Donde
Servicios SMS	Pack 1 millón	Adquirido en país africano
Dominio	Imitando al nombre ACME	Adquirido en Islandia
Hosting	Pagado en criptomoneda	Adquirido en Islandia
Emails	Mail.ru	Russia

La reunión

Cita en un sitio “neutral”

John tiene todo preparado, pero necesita una reunión presencial.

“Hay cosas que no se pueden hablar por teléfono”

“Hay cosas que no se pueden comentar por escrito”

Pero eso sí, mandamos un gatito cuando queremos comunicarnos..

El sitio elegido es un peñón del Mediterráneo, temas a tratar:

- Conocerse personalmente (la importancia del “body language”)
- Tiempo para realizar el phishing
- Infraestructura y medidas de seguridad
- Reparto de beneficios

Blanqueo de dinero

El Blanqueo

John cuenta con Jim para realizar las siguientes acciones

Acceso a las credenciales obtenidas

Envío de archivo TXT

Acceso a las cuentas donde coincidan las palabras clave

Tres de seis

Realización de transferencias, a 3 o 4 conocidas por Jim

En general personas fallecidas

Envío desde esas 3 o 4 CC finales

estructura de blanqueo en China

El Blanqueo (II)

Jim ha logrado acceder a las credenciales, y que ha hecho transferencias por valor de 5.2 millones de euros.

Ha logrado mandar el dinero a la estructura de blanqueo localizada en China. Jim conoce esta estructura de blanqueo porque un bufete de abogados de la City comentó su existencia.

La estructura de blanqueo se queda con un % de cada transferencia realizada.

John necesita: Obtener su dinero // Pagar a Jorge y su equipo, y a Jim

El Reparto

Tras unos días, Jim aparece con tres tarjetas de crédito sin nombre, como adelanto.

Una tarjeta es para John, que se queda con el 30% del total sustraído.

Otra tarjeta es para Jorge, con 10% del total.

El resto, aproximadamente un 60%, es para Jim y los gastos que ha tenido.

Lecciones aprendidas

¿Y el Threat Intelligence?

Nadie se enteró de nada, no hubo Alerta Temprana.

Problemas:

- Círculo cerrado
- Profesionalización de los actores /"Cybercrime as a Service"
- Uso de ataques simples pero efectivos

Threat Intelligence

- Solo se alimentan de datos técnicos
- No existe proactividad, son reactivos

Respuesta

Denuncia / Respuesta

REDES 24/7
Art 29 Convenio de Budapest
Red Interpol
Red G7 – Dpto Justicia USA
RETENCIÓN / PRESERVACIÓN

EUCTF/JCAT/JEFES CIBER LATINOAMERICA
INTERPOL/CEPOL/SINGAPUR
CSIRT-LEA

EUROPOL/ INTERPOL
Colaboración Policial Internacional

INTEGRIDAD Y CUSTODIA DE LAS PRIMERAS EVIDENCIAS

"ORDEN EUROPEA INVESTIGACIÓN"

MEDIDAS ESPECÍFICAS

1. Medidas que implican la obtención de pruebas en tiempo real (art. 28)
2. Investigaciones encubiertas (art. 29)
3. Intervención de telecomunicaciones (art. 30 y 31)
4. Medidas cautelares (art. 32)

PROPUESTA REGLAMENTO UE sobre acceso transfronterizo a la prueba electrónica en materia penal (e-evidence)

Conclusiones

Conclusiones

La gravedad del CIBERCRIMEN.

La importancia de DENUNCIAR/NOTIFICAR.

Ejercer el derecho por una Red más segura

Que permita proteger nuestro tejido industrial y social tecnológico

¡Muchas gracias por su atención!

delitostelemáticos@guardiacivil.es
www.gdt.guardiacivil.es

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional