Operaciones día a día en un CERT nacional

Alberto Hernández Moreno
Director de Operaciones

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

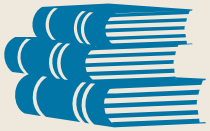
TRABAJANDO POR LA CONFIANZA DIGITAL

Punto de partida: instrumentos estratégicos de ciberseguridad

El marco de referencia de la ciberseguridad nacional

Directrices

ECSN
PNCS y
Planes Derivados



- ✓ Estructura del sistema
- ✓ Principales actores
- ✓ Hola de Ruta

CERTS Nacionales

(*) Aprobado por el Consejo de Seguridad Nacional Julio/2015

- ✓ CERT de los Ejércitos y Armada
- ✓ Centro de operaciones de SI del Ministerio de Defensa

- ✓ **CERT de ciudadanos empresas, IICC, RedIris**

certsi_
CERT DE SEGURIDAD E INDUSTRIA

- ✓ CERT de la AGE, CCAA, Admón. Local y Entidades Públicas

CCN-CERT
centro criptológico nacional

CERT de Seguridad e Industria (CERTSI)

Año 2012 → Acuerdo Marco de Colaboración:

Secretaría de Estado de Seguridad	+	Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información	=	CERTSI
CNPIC		**INCIBE**		Apoyo tecnológico FCSE

Servicios






Detección

Análisis

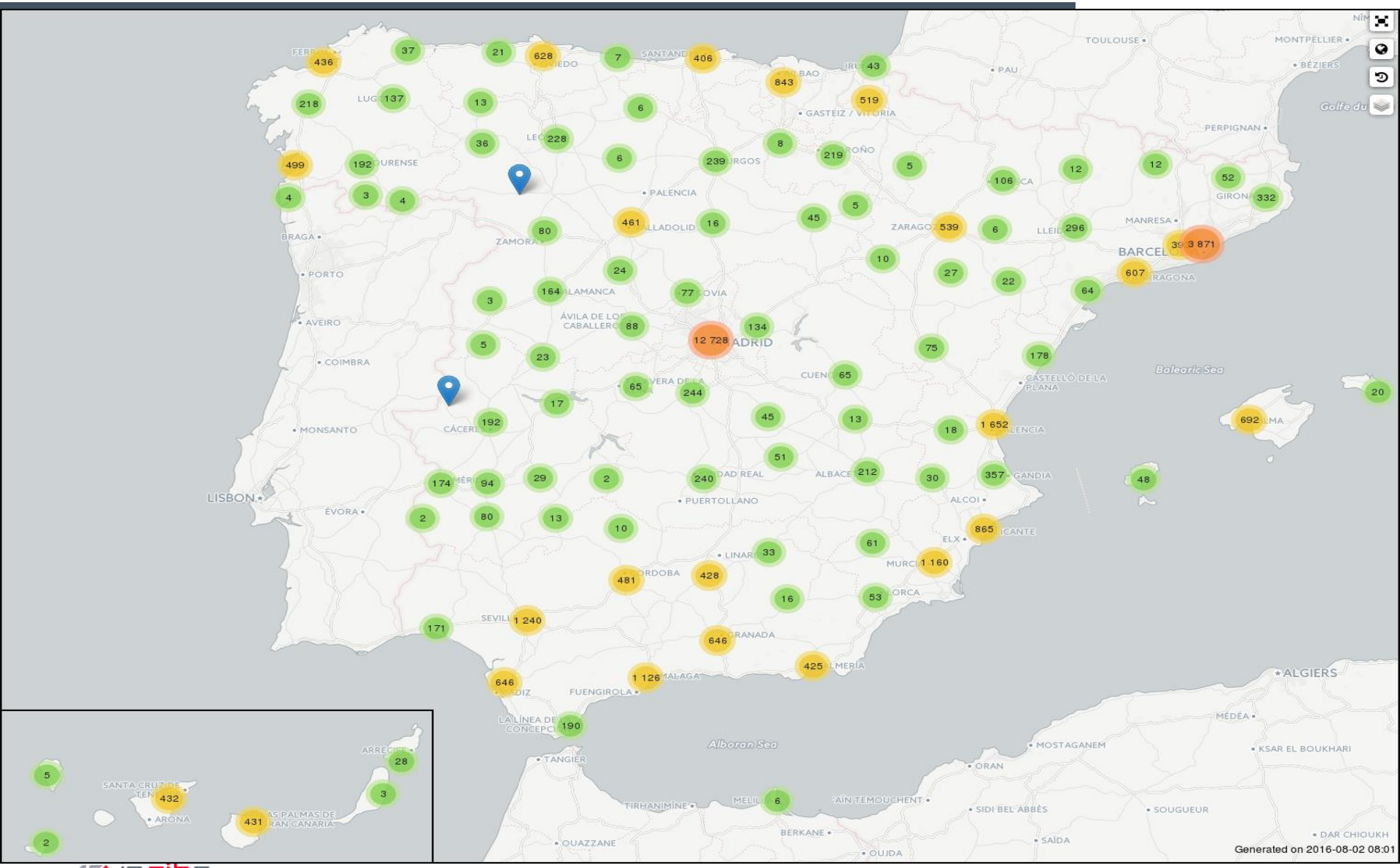
Notificación

Apoyo a la respuesta

Intercambio de información, CyberEx e Indicadores

Lecciones aprendidas

¿Qué pasa en España?



Incidentes gestionados desde CERTSI

2015

49.976

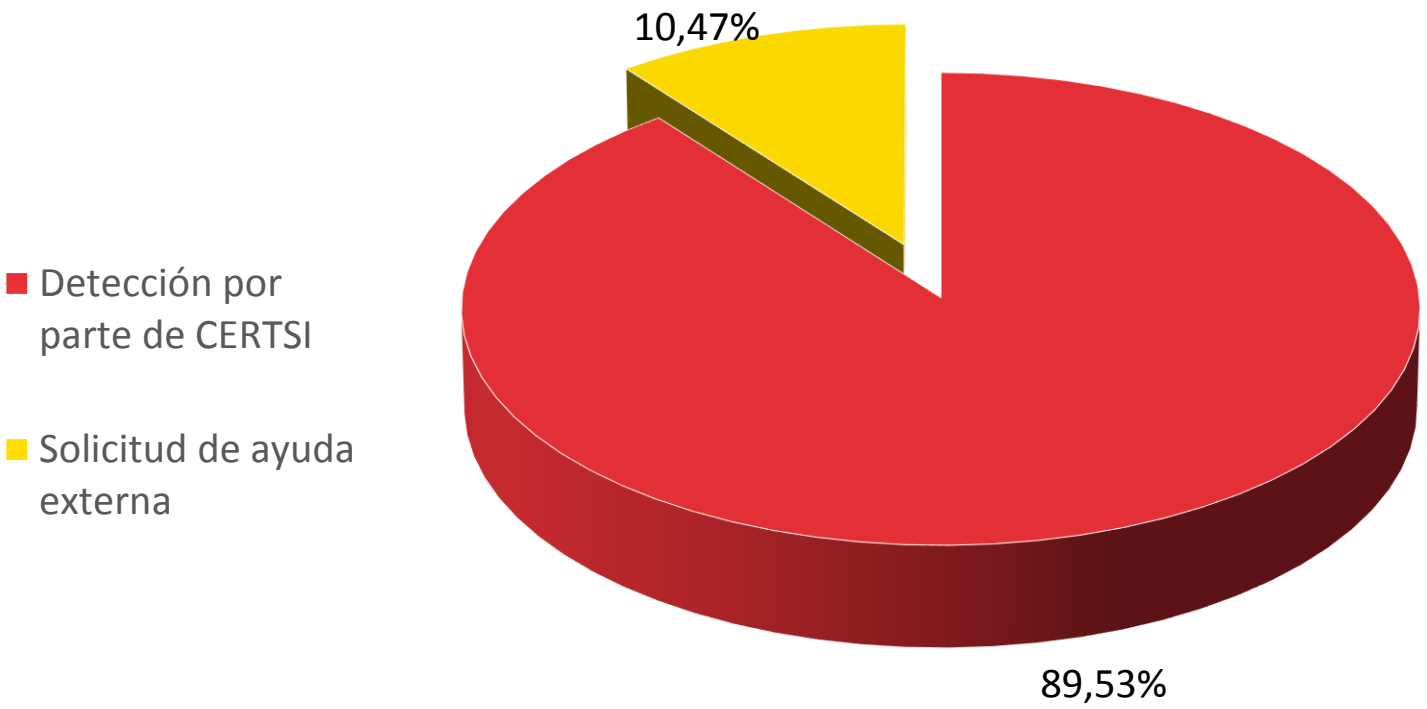
Incidentes gestionados	Ciudadanos y empresas	Red Académica (RedIRIS)	Infraestructuras críticas
	45.689	4.153	134

2016

Incidentes gestionados	Ciudadanos y empresas	Red Académica (RedIRIS)	Infraestructuras críticas
	22.311	3.205	280

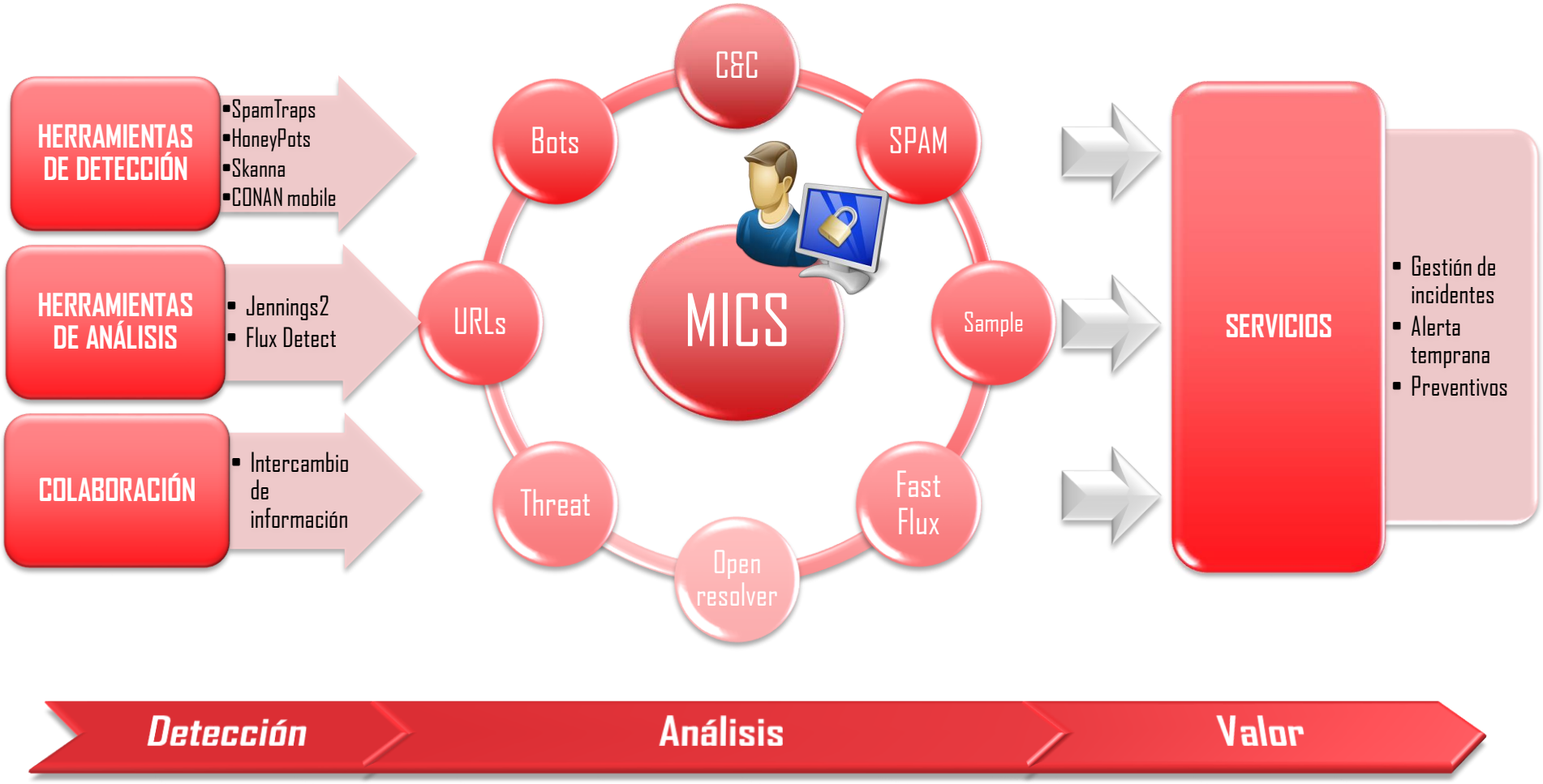
25.596 (31 agosto 016)

Indicadores 2015: Detección interna frente a notificación externa



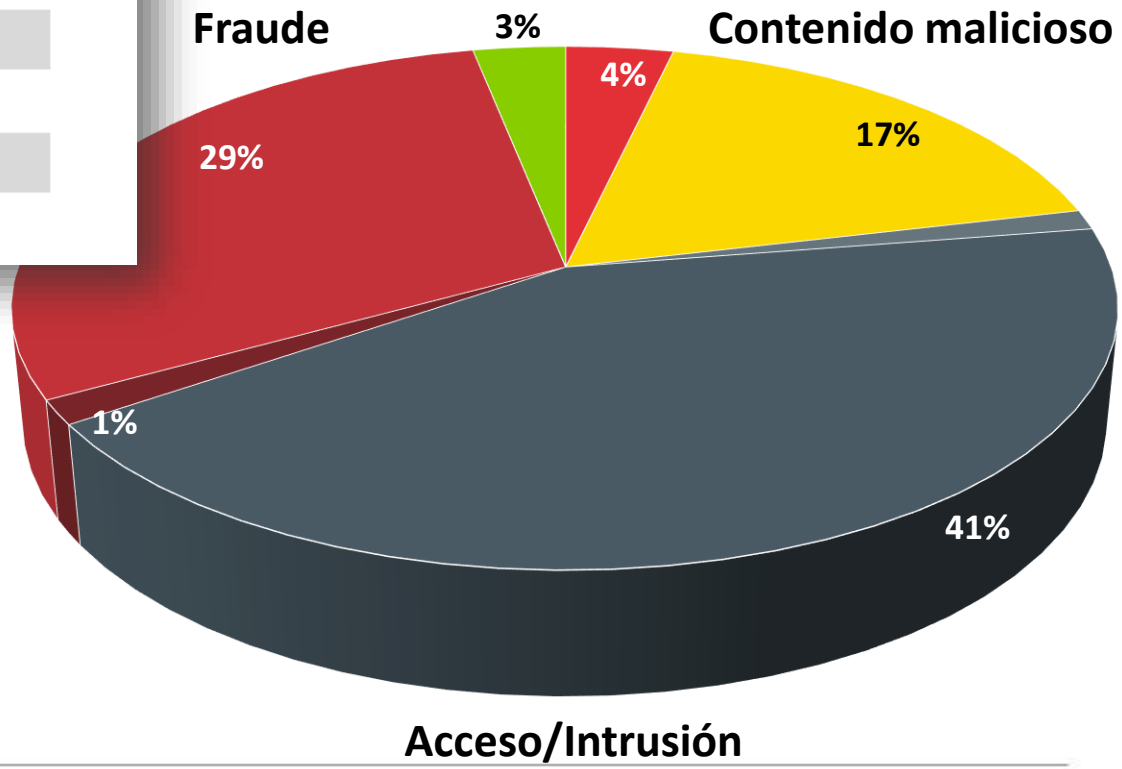
Gráficos extraídos de ICS-CERT Monitor September 2014-February 2015

Detección proactiva

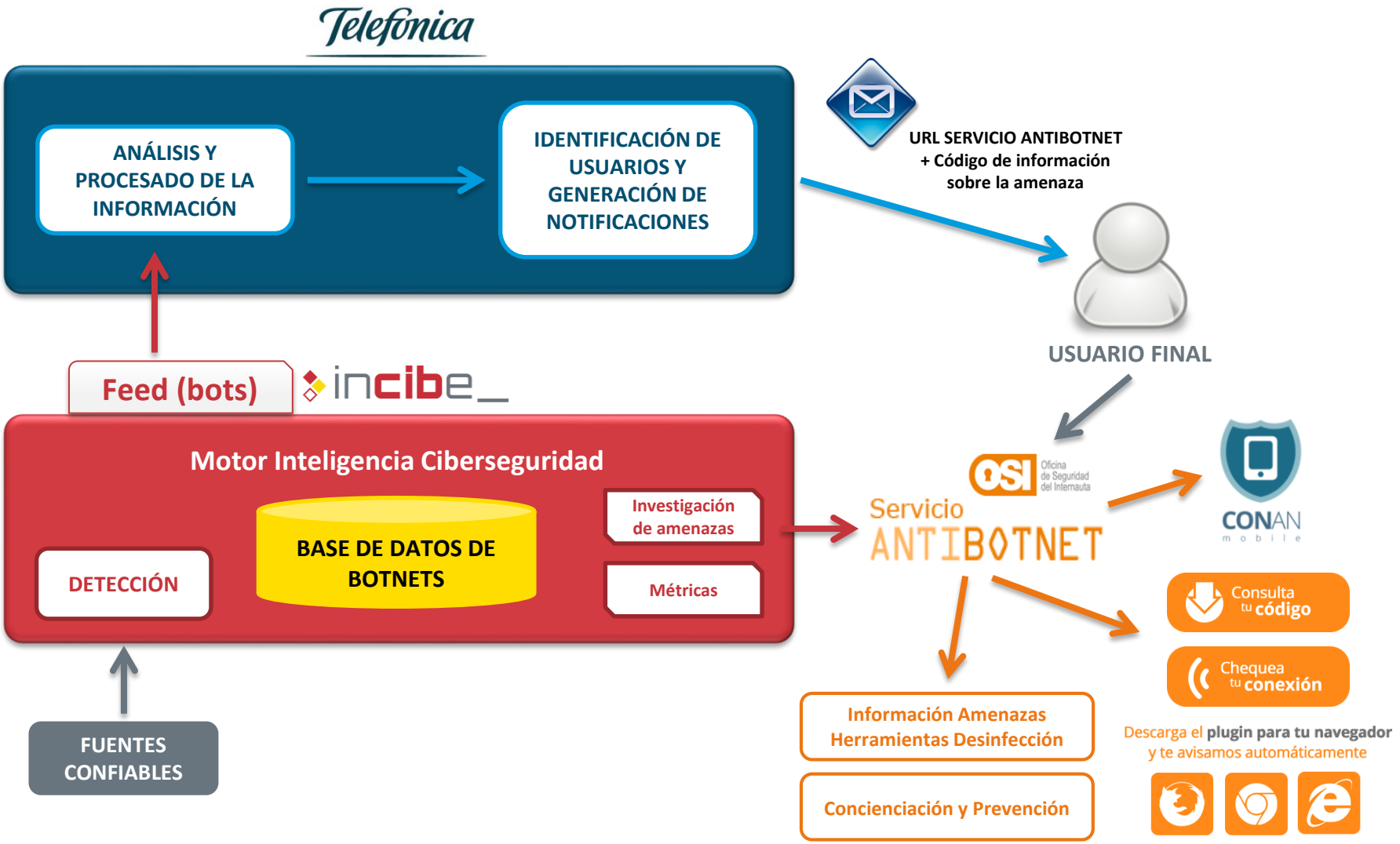


Análisis

Tipo de incidente	Agosto	Acumulado 2016
SPAM	113	940
Virus, troyanos, gusanos, spyware	343	4.556
Escaneos de red	8	316
Acceso no autorizado	835	11.065
Denegación de servicio	21	389
Robo de información	6	23
Fraude	1.337	7.699
Otros	150	808

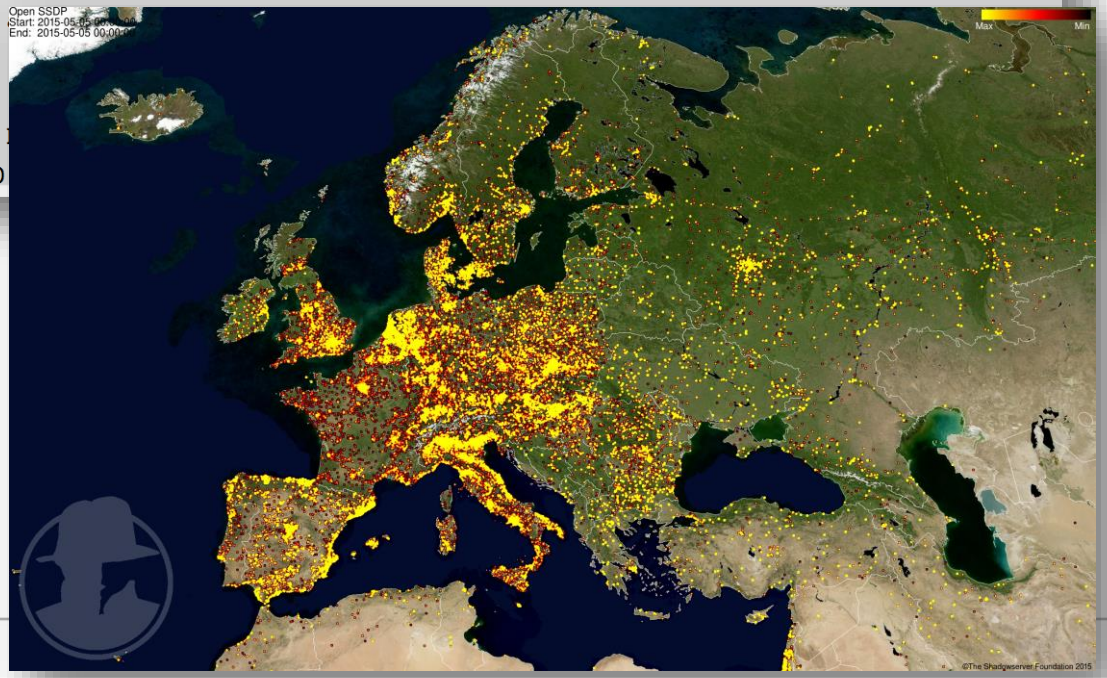


Notificación Servicio ANTIBOTNET



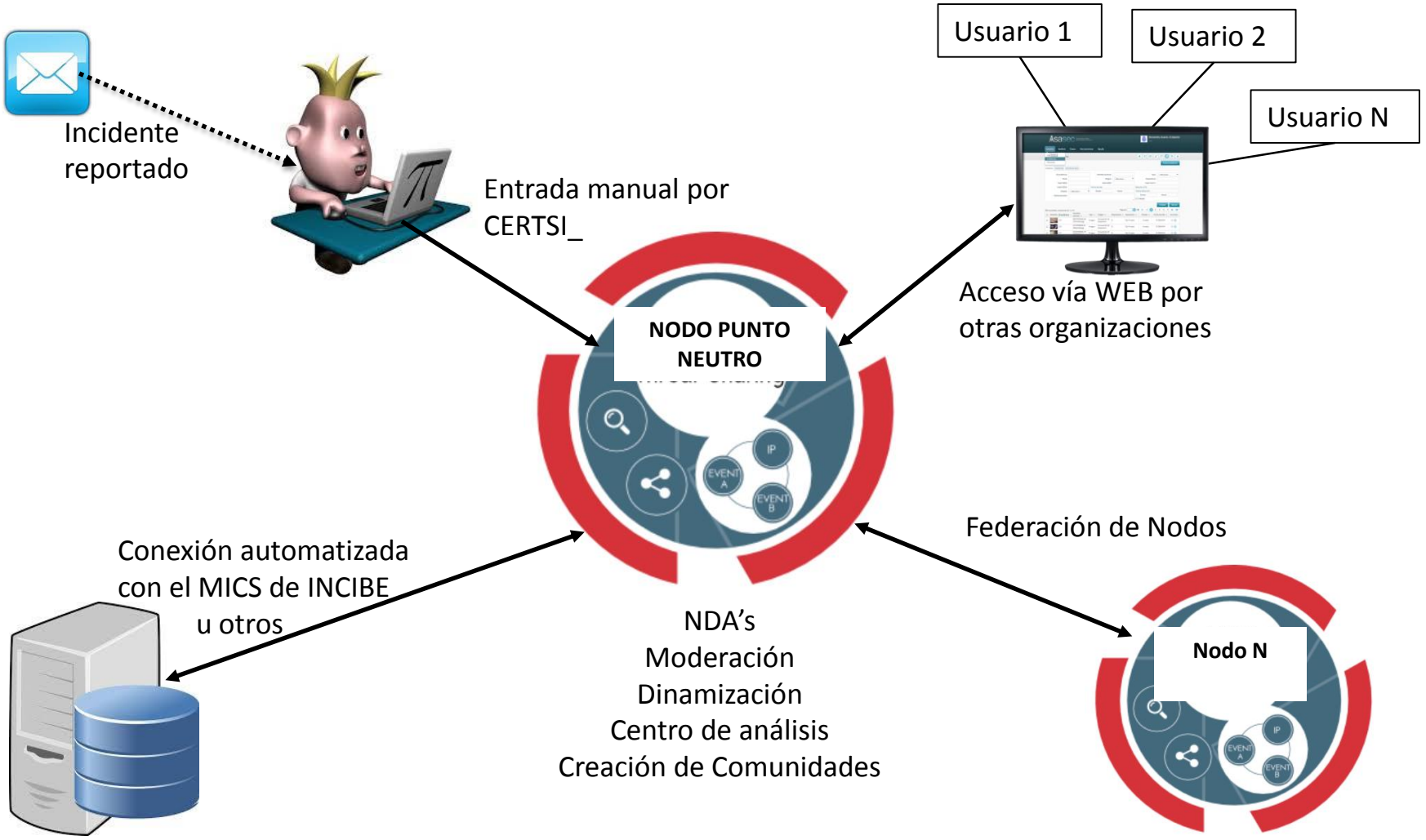
Respuesta: Ciberextorsión: Armada Collective, DD4B, Kadyrovtsy

```
From: "Armada Collective" armadacollective@openmailbox.org
To: abuse@victimdomain; support@victimdomain; info@victimdomain
Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @ XXX

When we say all, we mean all - users will not be able to access sites host with you at
all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It
will not be hard, we will not crash it at the moment to try to minimize eventual damage,
which we want to
your logs!

If you don't pay
and will go up 20
```



Fuente: The Shadowserver Fundation

Intercambio de información: Proyecto ICARO



Alerta temprana de INCIBE 2015 (ciudadanos, empresas, profesionales y SCI)

5.862

Llamadas telefónicas atendidas

280

Avisos técnicos de seguridad para profesionales y sistemas de control industrial

64

Avisos para ciudadanos

23

Avisos para empresas

Follow us!

CONTACT	Con el CERT de Seguridad e Industria **(CERTSI)** **certsi@certsi.es**
SUBSCRIBE	Instituto Nacional de Ciberseguridad **(INCIBE)** **https://www.incibe.es**
LEARN	Sobre la Alerta Temprana de **CERTSI** **https://www.incibe.es/CERT/Alerta_Temprana/**
FOLLOW	Facebook, Twitter, G+, LinkedIn. **@incibe @certsi**
REPORT	incidentes, vulnerabilidades, fraude online, phishing, malware, etc. **incidencias@certsi.es**

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

NATIONAL CYBERSECURITY INSTITUTE OF SPAIN

10 incibe_ 2005-2016

TRABAJANDO POR LA CONFIANZA DIGITAL

GOBIERNO DE ESPAÑA

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO