

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

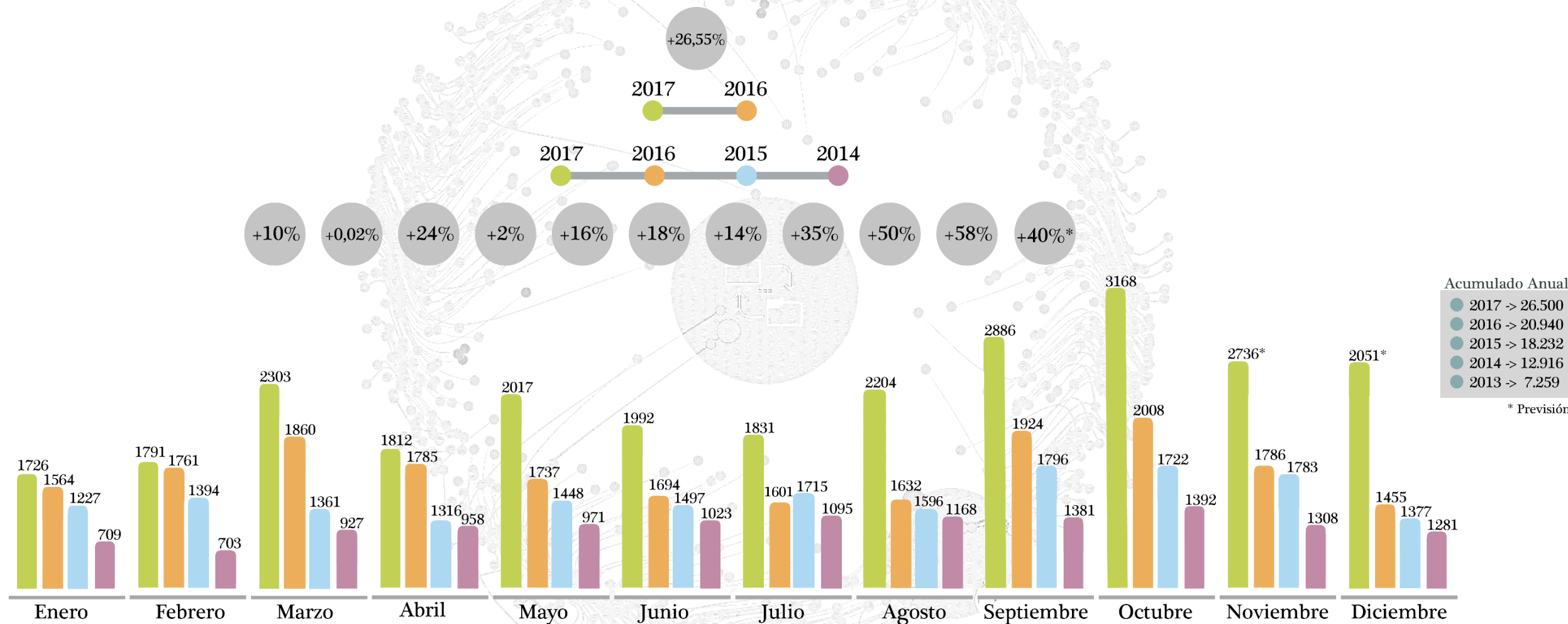
UN AÑO DE ATAQUES



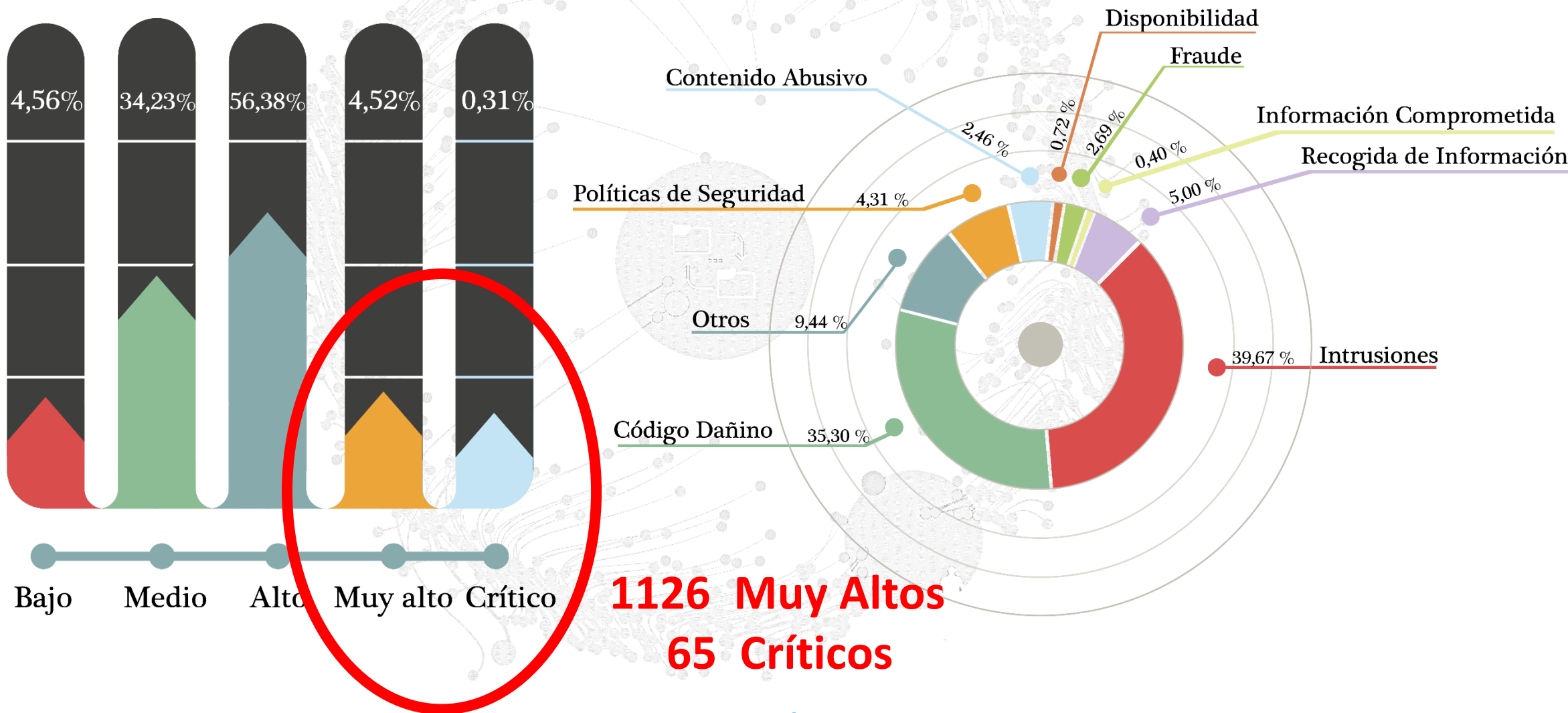
- Equipo Respuesta a Incidentes
- CCN-CERT
- incidentes@ccn-cert.cni.es

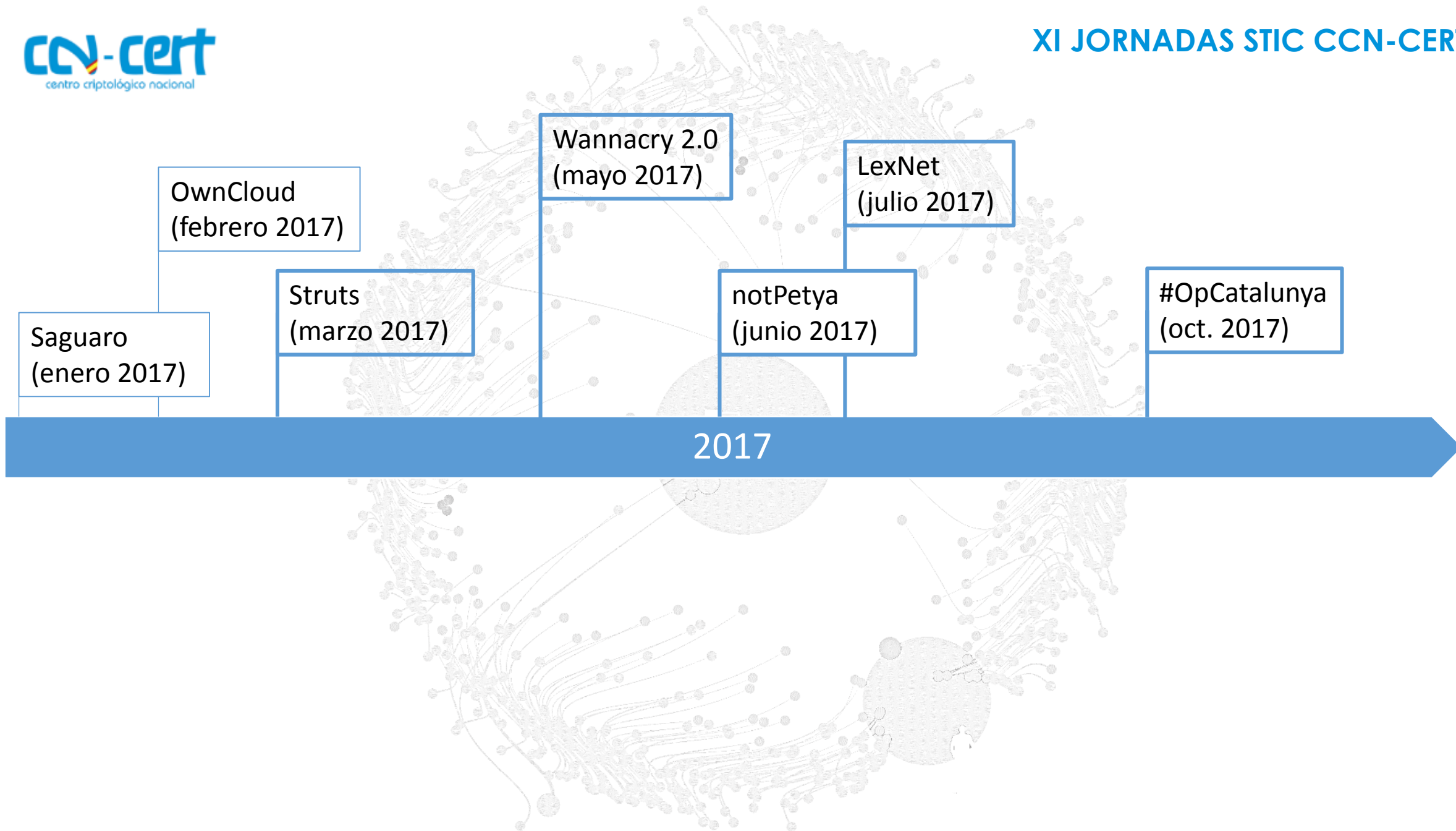


Incidentes Gestionados



Incidentes Gestionados - Peligrosidad - Tipología



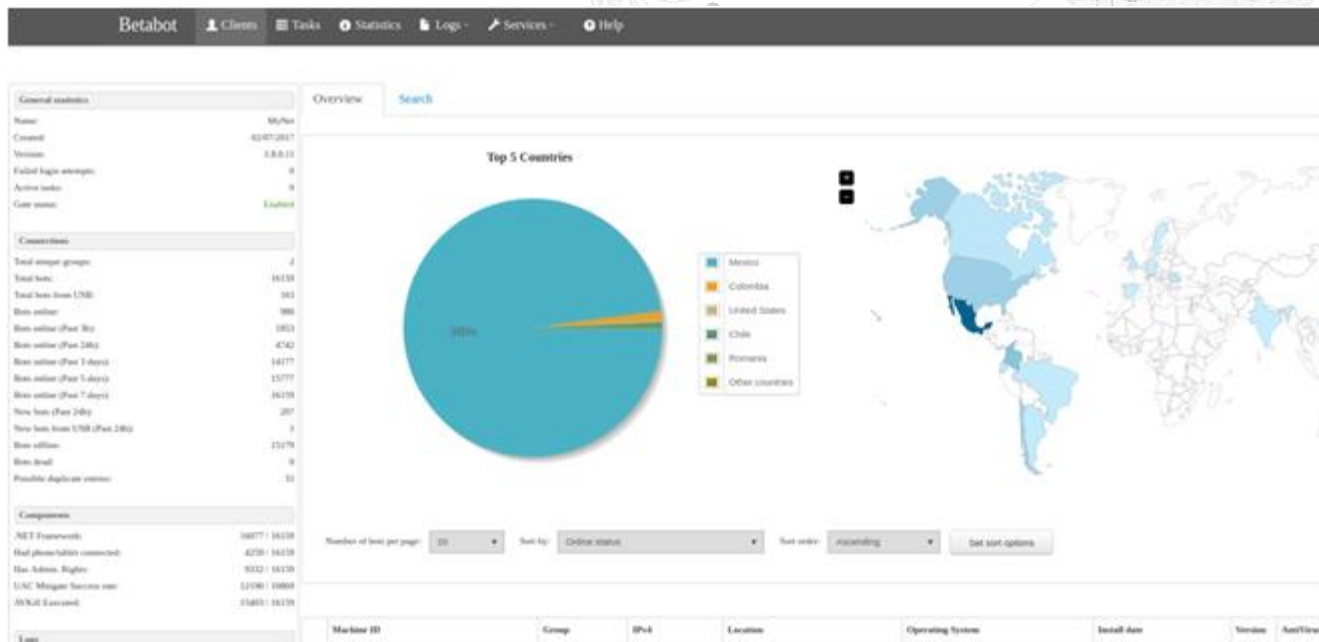


Saguaro
(enero 2017)

- › Actor mexicano con intereses económicos y enfocado en el **robo de credenciales**
- › Uso de múltiples troyanos para crear botnets
- › Varios servidores C2 habían sido registrados en España. Se hizo un *DNS sinkholing* sobre dichos dominios



2017



- › **~17.000 bots**
- › **> 60.000 IPs** diferentes afectadas
- › **> 36 países** afectados

OwnCloud
(febrero 2017)

- Suite que permite tener un servidor en una nube privada para compartir archivos, gestionar tareas, reproducir archivos online...
- Explotación de **varias vulnerabilidades**, acceso a archivos y ejecución de código...
- **10 entidades afectadas**. Algunas de ellas, siguen siendo vulnerables.

2017



Nextcloud Security Scan

➤ <https://scan.nextcloud.com>



Check the security of your private cloud server

Privacy does not exist without security. To help you keep your data yours, this scan analyzes the security of your server and gives you an overview of what to improve.

<https://vulnerable.net>

Running ownCloud 8.0.0.7

✗ NOT on latest patch level

Vulnerabilities

Your instance has known vulnerabilities, below you can see a list of them. Learn more about [our security efforts](#).

High

Local file inclusion on MS Windows Platform

Command injection when using external SMB storage

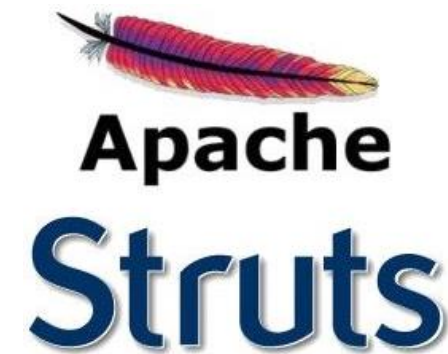
PHP arbitrary class instantiation in "files_external"

Struts
(marzo 2017)

- › Vulnerabilidad **que afecta a millones de servidores web conectados a Internet** empleados por grandes empresas e instituciones en todo mundo
- › En España, **75 organismos afectados. 6 de ellos con impacto crítico.**
- › **4 equipos desplazados.** Trabajo en fin de semana.

2017

- › Herramienta de soporte para el desarrollo de aplicaciones Web.
- › El 29 de enero de 2017, se hizo pública una vulnerabilidad con código **CVE-2017-5638**, que permitiría a un atacante ejecutar órdenes remotas sobre un servidor a través de un contenido subido al componente de análisis Jakarta Multipart.
- › El 16 de agosto de 2017 se hizo pública una **nueva vulnerabilidad CVE-2017-9805**, que afecta a este software, que de la misma forma que la anterior vulnerabilidad, permitiría a un atacante ejecutar órdenes remotas sobre un servidor.



Wannacry 2.0
(mayo 2017)

2017

- 12.05.2017 se tiene constancia de ciberataque tipo **ransomware** (WannaCry)
- 12.05.2017 CERTs nacionales difunden primeras alertas. Primera versión **vacuna WannaCry Prevention**. Investigación del modo de proceder del código dañino.
- 13.05.2017 CCN desarrolla **vacuna NoMoreCry v0.1**. Más de 50.000 descargas.
- 14.05.2017 se publica **informe de código dañino** (CCN-CERT ID 17/17 Ransom.WannaCry) Se actualiza NoMoreCry para WINDOWS XP / 2000.
- 15/16.05.2015 **Vigilancia y coordinación con organismos**. Se remiten +90 alertas de conexión a servidores. Se sigue actualizando la herramienta.

Ataque masivo de ransomware que afecta a un elevado número de organizaciones españolas

Publicado el: 12/05/2017

El ciberataque, efectuado con el uso de una red de bots, afecta a un elevado número de organizaciones españolas.

Ataque de ransomware que afecta a sistemas Windows

Publicado el: 12/05/2017

El ciberataque, efectuado con el uso de una red de bots, afecta a un elevado número de organizaciones españolas.

Medidas de mitigación contra el ataque masivo de ransomware

Publicado el: 12/05/2017

El ciberataque, efectuado con el uso de una red de bots, afecta a un elevado número de organizaciones españolas.

CCN-CERT NoMoreCry Tool V.0.3, actualizada la vacuna frente a WannaCry

Publicado el: 15/05/2017

Fecha alerta

El CCN-CERT ha actualizado a una versión 3 su herramienta para prevenir la infección por el malware **WannaCry 2.0**. Se trata de **NoMoreCry-v0.3** (para Windows XP y superiores) y **NoMoreCry2000-v0.3** (para Windows 2000). En ambos casos se crea en el equipo los objetos de exclusión mutua que impiden la ejecución del código dañino. Esta nueva versión de la herramienta consta también de un fichero de texto (**NoMoreCry_mutek**) que obligatoriamente debe acompañar al ejecutable en la misma ruta. Dentro de este fichero se encuentran los nombres de los objetos de exclusión mutua que la herramienta creará.

Microsoft Security Bulletin MS17-010 - Critical

Security Update for Microsoft Windows SMB Server (KB433885)

Published March 13, 2017

Version: 1.0

Executive Summary

The security update resolves vulnerabilities in Microsoft Windows. The most serious of the vulnerabilities could allow remote code execution in the affected systems. Security updates are available for Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016.

Lost in Translation

ShadowBrokers leak

WIKI... Just want ShadowBrokers to be trying to help people. This week ShadowBrokers has been helping people. Not other people like having more problems? So this week is being about money. ShadowBrokers always give people ShadowBrokers money to be using. Sometimes people are being target audience. Follow the link for more details. Windows, Linux, Android, etc. you thought that was it? Some of you people is sending money to ShadowBrokers.

WannaCry 2.0 ransomware outbreak started appearing in the wild.

WannaCry 2.0 ransomware outbreak started appearing in the wild.

Microsoft Security Bulletin MS17-010 - Critical

ShadowBrokers leak

WannaCry 2.0 ransomware outbreak started appearing in the wild.



- Robo de credenciales.
- ETERNALBLUE para propagación.
- ¿Demostración de fuerza?

NotPetya
(junio 2017)

2017

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

8UeiNr-ngRtrs-NFx836-CyWwqF-wmKmf3-dsWL7g-PLtmUm-qgEoWa-ubECnf-NAEyfT

If you already purchased your key, please enter it below.

Key:

- Ataque a la cadena de suministro en Ucrania.
- Propagación desde sedes ucranianas.
- Destructivo, no *ransomware*.
- Imposible descifrar los ficheros aunque se pague.

- Campaña contra AAPP y empresas #OpCatalunya (4 fases).
- **Más de 70 páginas web** atacadas.
- Ataques de DDoS.
- Data Dumps (30 objetivos).
- Uso de redes sociales e IRC para visibilidad y coordinación.
- Sin impacto grave (caída breve del servicio web).

#OpCatalunya
(oct. 2017)



➤ Ataques:

- **TCP Flood**
- **UDP Flood**
- **HTTP/S Flood**
- **Slow Loris**

```
[17:48] -- WE ARE LEGION.
[17:48] -- *****
[17:48] -- WELCOME TO ANONPLUS.
[17:48] -- WebChat: webchat.anonplus.org
[17:48] -- *****
[17:48] -- IRC
[17:48] -- #network
[17:48] -- #IRC1: irc.anonplus.org <--> ports: 9999/21441 for SSL, 6661/21331 for plaintext
[17:48] -- USEFUL CHANNELS:
[17:48] -- #anonplus [get help and info about op/services]
[17:48] -- #vhost [to change your vhost]
[17:48] -- #italy [supporto in lingua italiana]
[17:48] -- #help [help about IRC]
[17:48] -- End of /MODE command.
[17:48] -- Usermode change: +sxx
[18:09] -- Channel Users Name
[18:09] -- #TangoDown 1 [+nt]
[18:09] -- #catalunya 1 [+nt]
[18:09] -- #jail 2 [+ntr]
[18:09] -- #help 2 [+ntr]
[18:09] -- #press.it 8 [+ntr]
[18:09] -- #italy 4 [+ntr] AnonPlus - Italian channel
[18:09] -- #opers 3 [+ntrO]
[18:09] -- #vhost 1
[18:09] -- #anonplus 15 [+ntr] AnonPlus
[18:09] -- #opisla 1 [+nt]
[18:09] -- #opocatalunya 12 [+ntr] Regional Government of Andalusia #DataLeak https://ghostbin.com/paste/7uytvc
[18:09] -- #phantom 2 [+ntr]
[18:09] -- #FreeCatalonia 1 [+nt]
[18:09] -- End of /LIST
```

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

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

➤ Síguenos en

