Congreso Cyberworking

Situación actual de la Ciberseguridad

Ponferrada, 31 de mayo 2018

Juan Delfín Peláez Álvarez
Experto en Ciberseguridad INCIBE
juan.pelaez@incibe.es

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

GOBIERNO DE ESPAÑA

MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

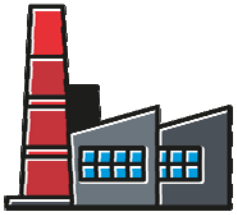
¿Qué es INCIBE?

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Entidad de referencia para el **desarrollo de la ciberseguridad** y de la **confianza digital** de:

Ciudadanos



Empresas**, en especial sectores estratégicos**

Sociedad Mercantil Estatal y Medio Propio dependiente de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital que lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

Servicios de Ciberseguridad: CERTSI

2012 Acuerdo Marco Colaboración

GOBIERNO DE ESPAÑA — MINISTERIO DEL INTERIOR

Secretaría de Estado de Seguridad

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

+

GOBIERNO DE ESPAÑA — MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Secretaría de Estado para la Sociedad de la Información y la Agenda Digital

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

=

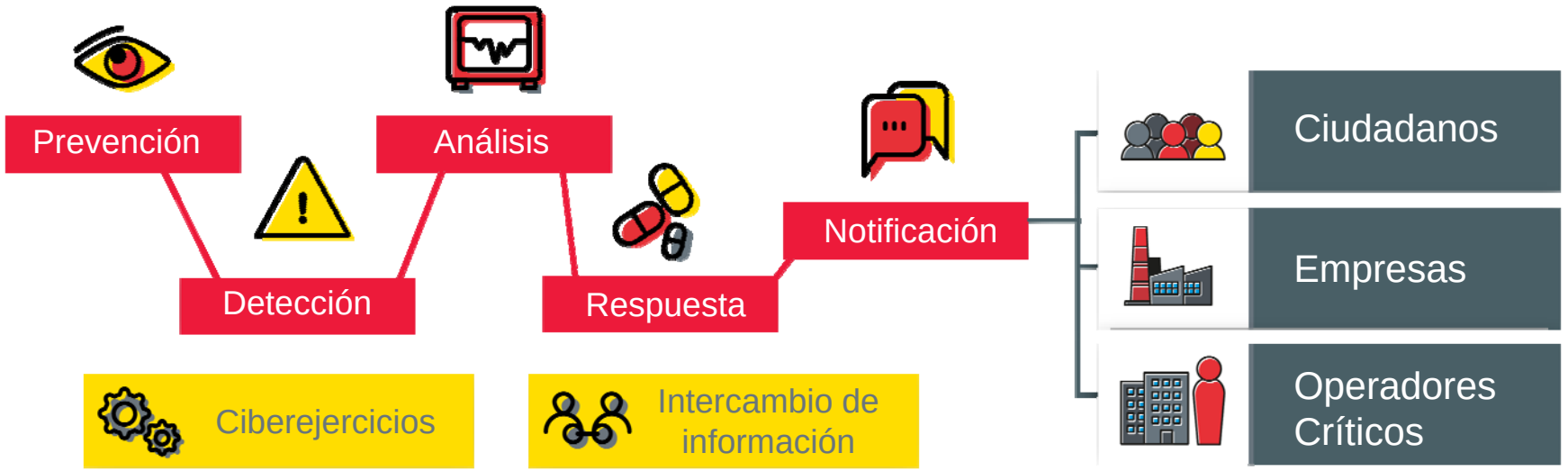
certsi_

Apoyo Tecnológico FCSE

CERT de Seguridad e Industria (CERTSI)

certsi_
CERT DE SEGURIDAD E INDUSTRIA

Referencia para la resolución técnica de incidentes de ciberseguridad que afectan a ciudadanos y empresas



incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Contenidos CERTSI para profesionales de ciberseguridad

certsi_

https://www.certsi.es

- Avisos de ciberseguridad, avisos de Sistemas de Control Industrial
- Blog especializado en contenidos técnicos de ciberseguridad
- Esquema Nacional de Seguridad Industrial (ENSI)
  - Política general
  - Indicadores de ciberresiliencia
  - Análisis de riesgos ligeros de seguridad integral
  - Construcción de capacidades de la Cadena de Valor
- Servicio de información sobre vulnerabilidades
- Guías y estudios
- Bitácora de ciberseguridad con los principales acontecimientos de ciberseguridad que tienen lugar a lo largo del año
- Nivel de alerta en ciberseguridad de INCIBE

certsi_ incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

CERT de Seguridad e Industria (CERTSI)

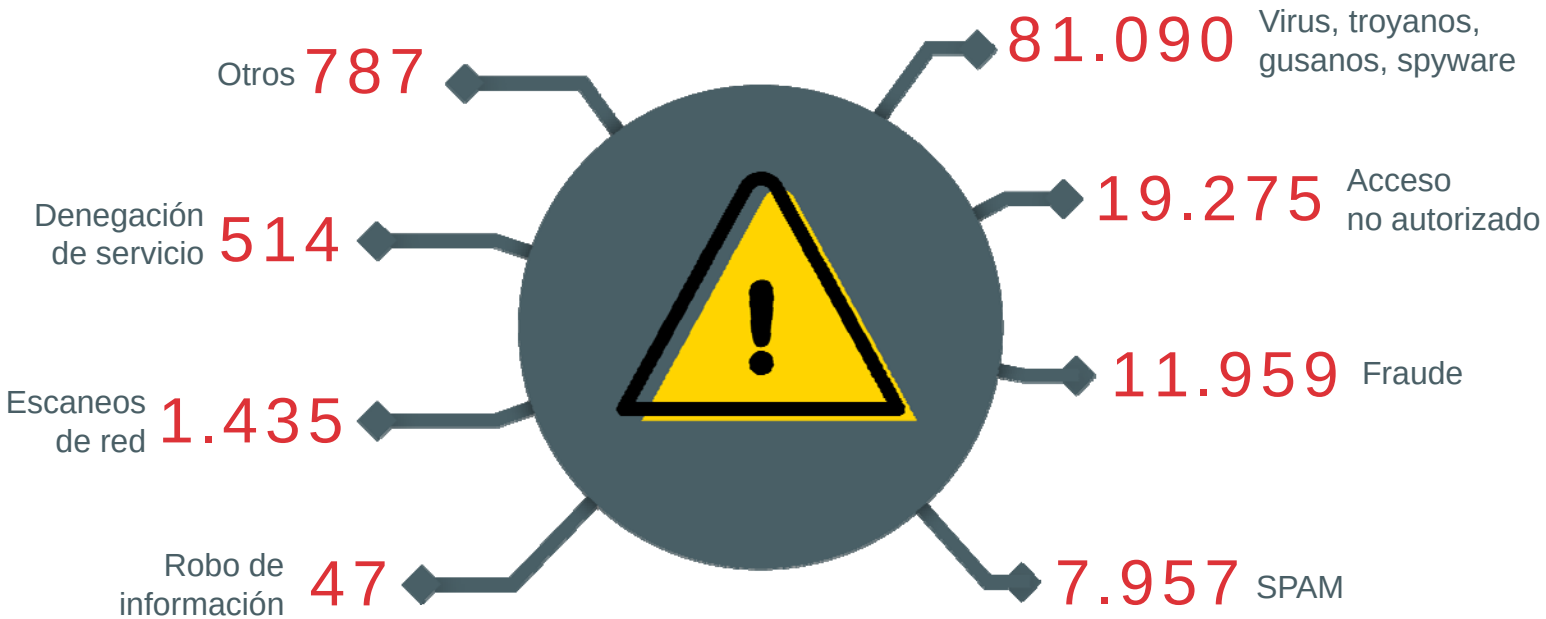
Incidentes gestionados en 2017: **123.064**

+6,77% Respecto 2016

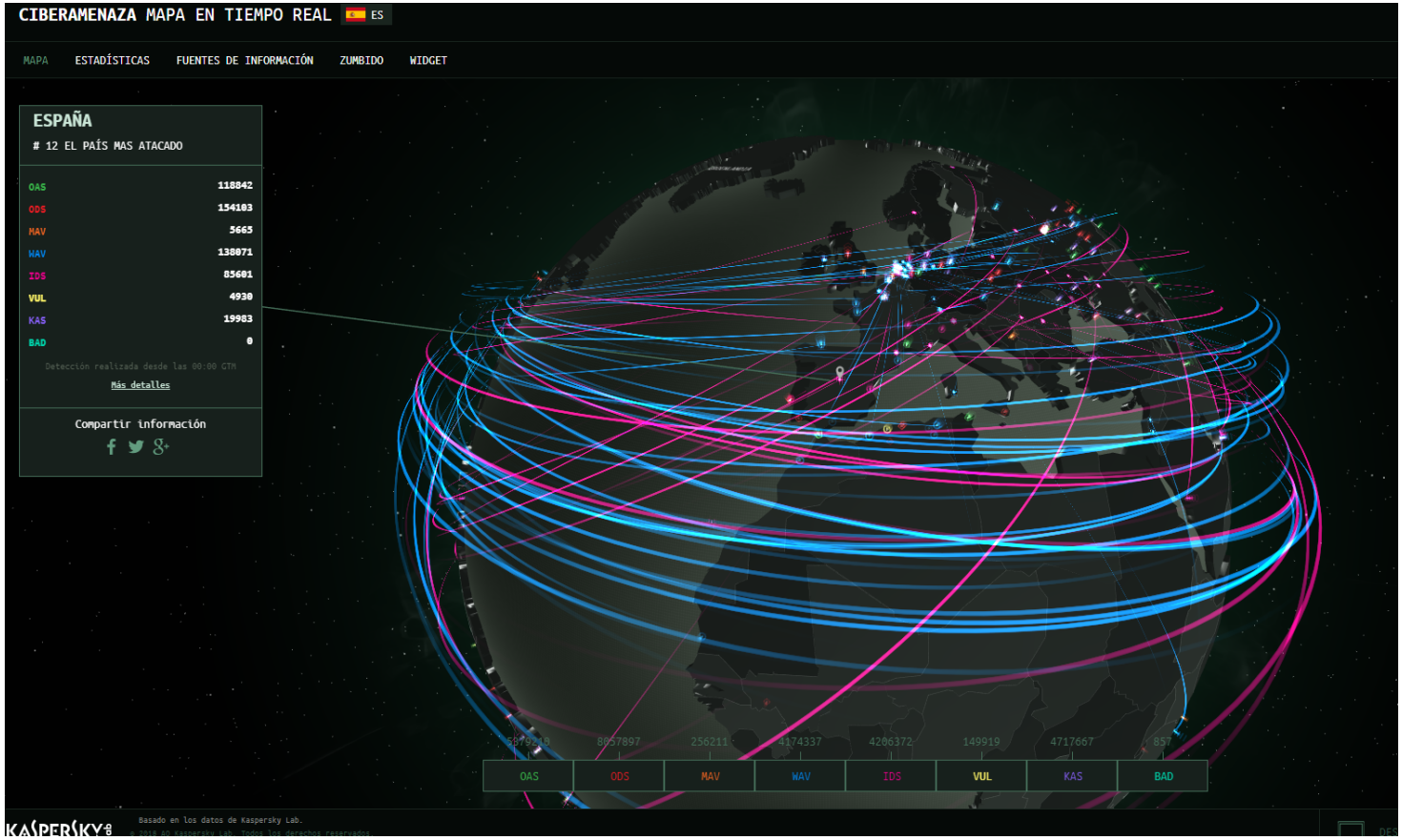
116.642	885	5.537
Ciudadanos y empresas	Operadores Críticos	Red Académica (RedIRIS)

inclbe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Tipos de incidentes 2017



CIBERAMENAZAS EN TIEMPO REAL

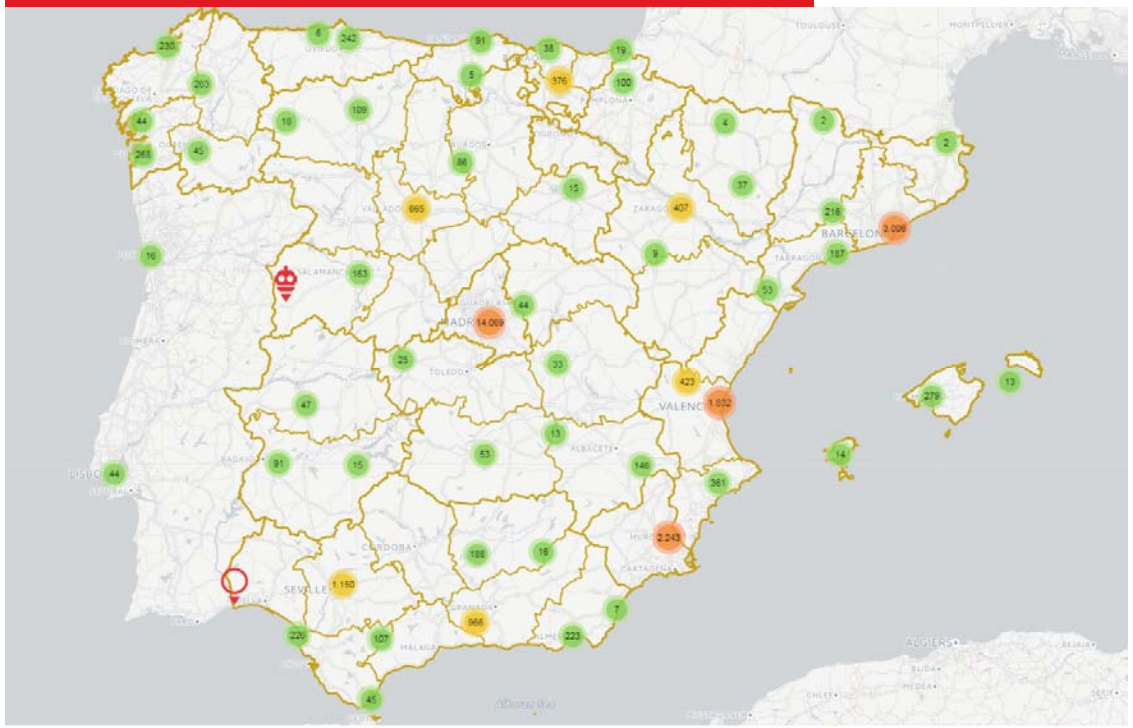


1.	Rusia
2.	Vietnam
3.	Alemania
4.	India
5.	Brasil

Infecciones EN EL ÚLTIMO MES		
1	Trojan.Script.Generic	16.28%
2	DangerousObject.Multi.Generic	15.71%
3	Trojan.Script.Miner.gen	6.59%
4	HackTool.MSIL.KMSAuto.bq	4.74%
5	HackTool.Win32.KMSAuto.m	4.74%
6	Trojan.WinLNK.Agent.qj	2.87%
7	HackTool.Win32.KMSAuto.c	2.33%
8	Trojan.JS.Miner.m	2.13%
9	Net-Worm.Win32.Kido.ir	1.63%
10	HackTool.MSIL.KMSAuto.bl	1.63%

cybermap.kaspersky.com

¿Qué pasa en España?



Datos de 2017

49.924 Usuarios notificados por Incidentes (páginas web, equipos infectados,..).
131.857 Usuarios notificados por botnets. 50% de desinfección
2.425 Incidentes de Ransomware

Tendencias:

- ❑ Minado de Criptomonedas
- ❑ Ransomware
- ❑ Spyware-keylogers

haveibeenpwned.com
cybermap.kaspersky.com

2017 – Incidentes mediáticos

certsi_
CERT DE SEGURIDAD E INDUSTRIA

Caso: WannaCry- mayo 2017

- Ransomware propagado en Mayo 2017
- Solicita +/- 300$ por ordenador
- Afecto a 230.000 equipos en 150 países
- Afecto a Telefónica, NHS, FedEX, etc.
- Un único monedero bitcoin
- “kill switch”
- Vulnerabilidad “EternalBlue” para Windows

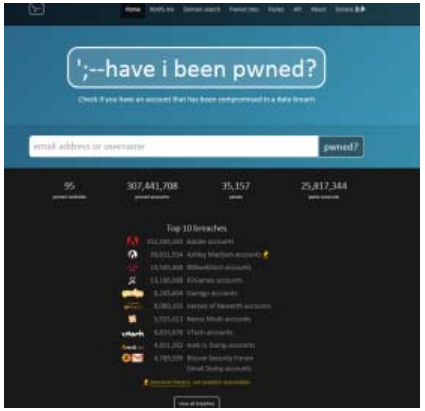
Caso: Petya/NotPetya/Petrwrap – junio 2017

- Variante de un ransomware conocido como Petya
- Actúa en Junio 2017 pero daña e inutiliza el equipo
- Solicita rescate de 300$
- Afecto a Ucrania y empresas que trabajan con su gobierno
- Un único monedero bitcoin
- No hay “kill switch”
- Vulnerabilidad “EternalBlue” + PSExec + passwords
- Vector software M.E.Doc

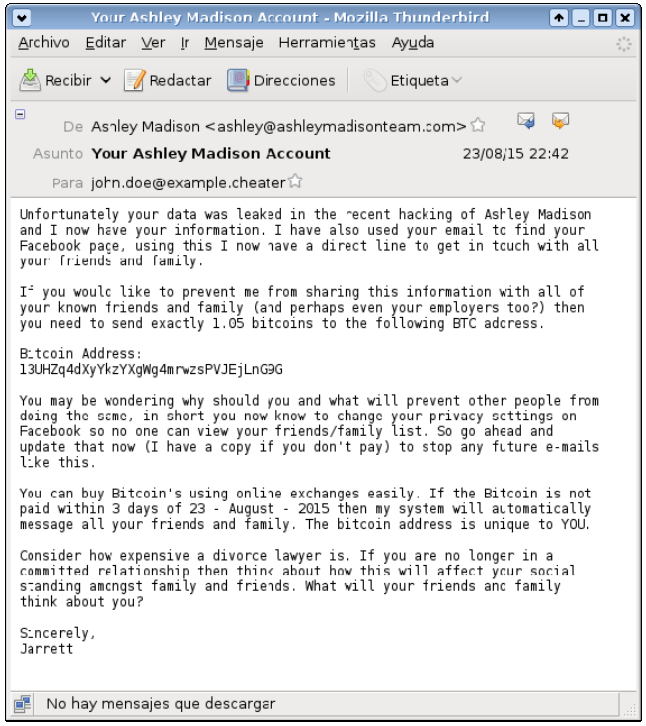
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Caso: Extorsión a usuarios de Ashley Madison - 2015

La lista de usuarios afectados, se hizo pública. ....con correos electrónicos, ips,....Algunos usuarios fueron extorsionados



https://haveibeenpwned.com/



https://btcdirect.eu/es-es

Usar contraseñas seguras: Con letras, Números y caracteres especiales

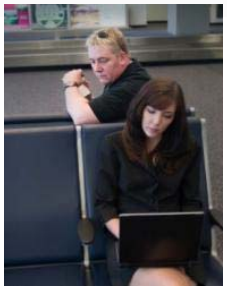
Terrible! Top 30 Worst Ashley Madison Passwords

PASSWORD	NUMBER OF USERS
123456	120511
12345	48452
password	39448
DEFAULT	34275
123456789	26620
qwerty	20778
12345678	14172
abc123	10869
pussy	10683
1234567	9468

PASSWORD	NUMBER OF USERS
696969	8801
ashley	8793
fuckme	7893
football	7872
baseball	7710
fuckyou	7458
111111	7048
1234567890	6572
ashleymadison	6213
password1	5959

PASSWORD	NUMBER OF USERS
madison	5219
asshole	5052
superman	5023
mustang	4865
harley	4815
654321	4729
123123	4612
hello	4425
monkey	4296
000000	4240

Usar contraseñas seguras: Con letras, Números y caracteres especiales

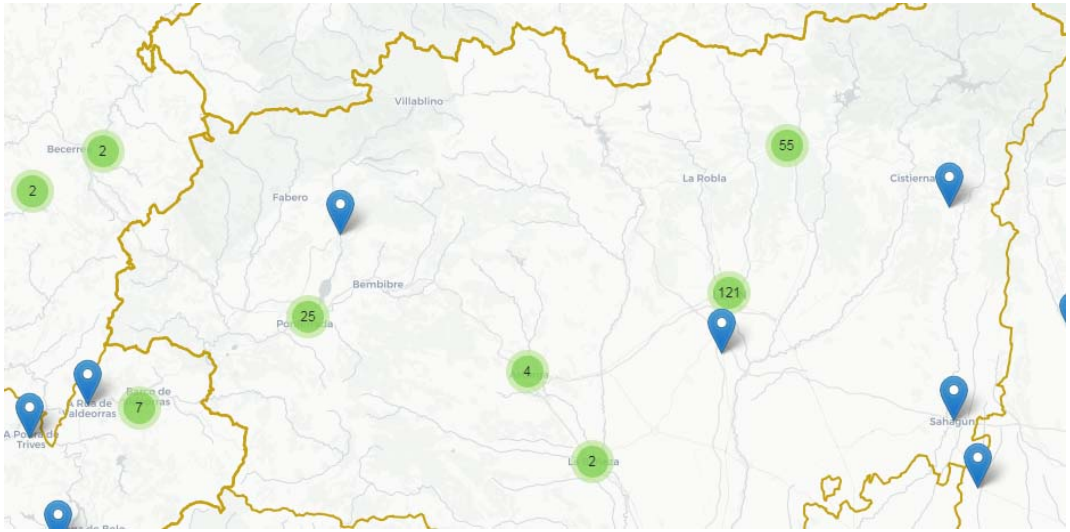


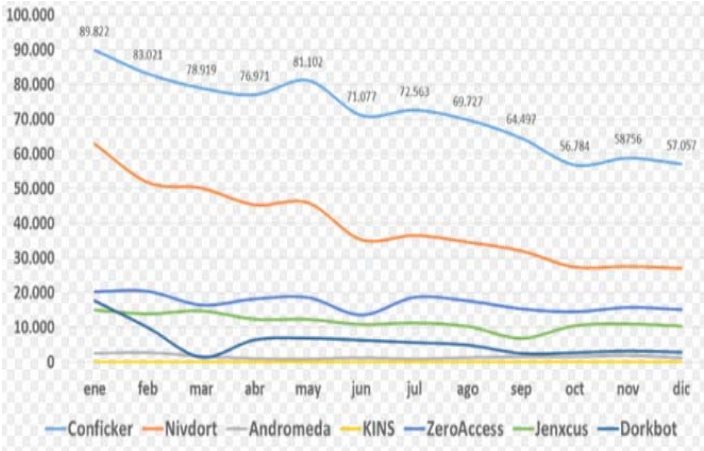
Otros métodos: keyloger, phising, shoulder surfing, fuerza bruta, man in the middle atack,...

Nivel de Alerta en León

Caso: El FBI lanza una alerta Mundial : Hay que reiniciar los routers - mayo-2018

En la provincia de León se detectan diariamente una media de 207 equipos y recursos comprometidos.





Tipos/Objetivos de estos Ataques:

- **Conficker**: Realizar Spam. Robo de contraseñas.
- **Nivdort**: Espiar (Keylogger). Para p.e, recoger información de tarjetas de crédito.
- **ZeroAccess**: Capacidad de procesamiento. Minería de Bitcoins.
- **Andromeda**: controlar equipos. Para p.e, realizar ataques de denegación de servicio DDoS.
- **Mirai**: Equipos IoT. Realizar ataques de denegación de servicio DDoS.
- **Necurs**: Fraude. Distribución de Ransowmare.

Ransomware en España

El 41% de empresas Españolas ha sufrido una infección por Ransomware.

Según un estudio elaborado por **Trend Micro** sobre la base de encuestas a más de 1.000 responsables de Tecnologías de la Información de **grandes organizaciones** en Reino Unido, España, Francia y Alemania.

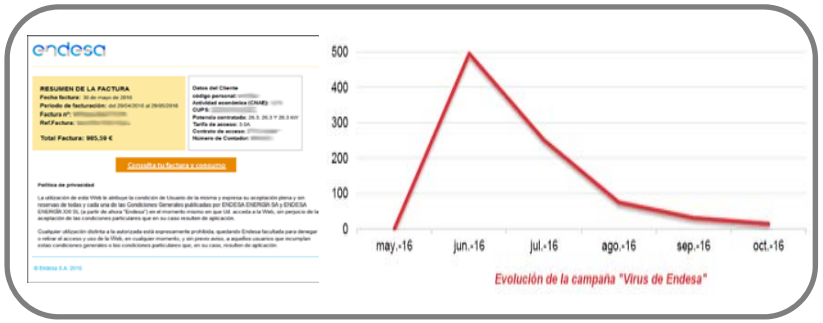
2.425 casos de Ransomware resueltos en 2017 por INCIBE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

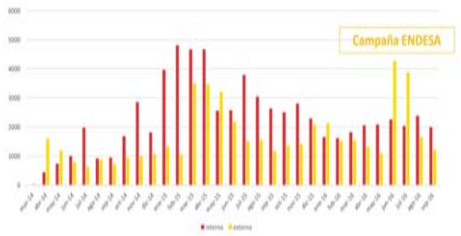
Campañas de Ransomware en España

Evolución de la campaña de Correos

Evolución de la campaña "Virus de la policía"



Evolución de la campaña "Virus de Endesa"



Ransomware de la Campaña Endesa 820 casos resueltos en 2016 por INCIBE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Formación especializada

Curso de ciberseguridad en sistemas de control y automatización industrial

Curso avanzado de ciberseguridad en dispositivos móviles

Curso de ciberseguridad básico para FCSE

Curso de ciberseguridad avanzado para FCSE

Curso para micropymes y autónomos

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Servicios de ciberseguridad: Protege tu empresa

protege tu empresa

https://www.incibe.es/protege -tu-empresa

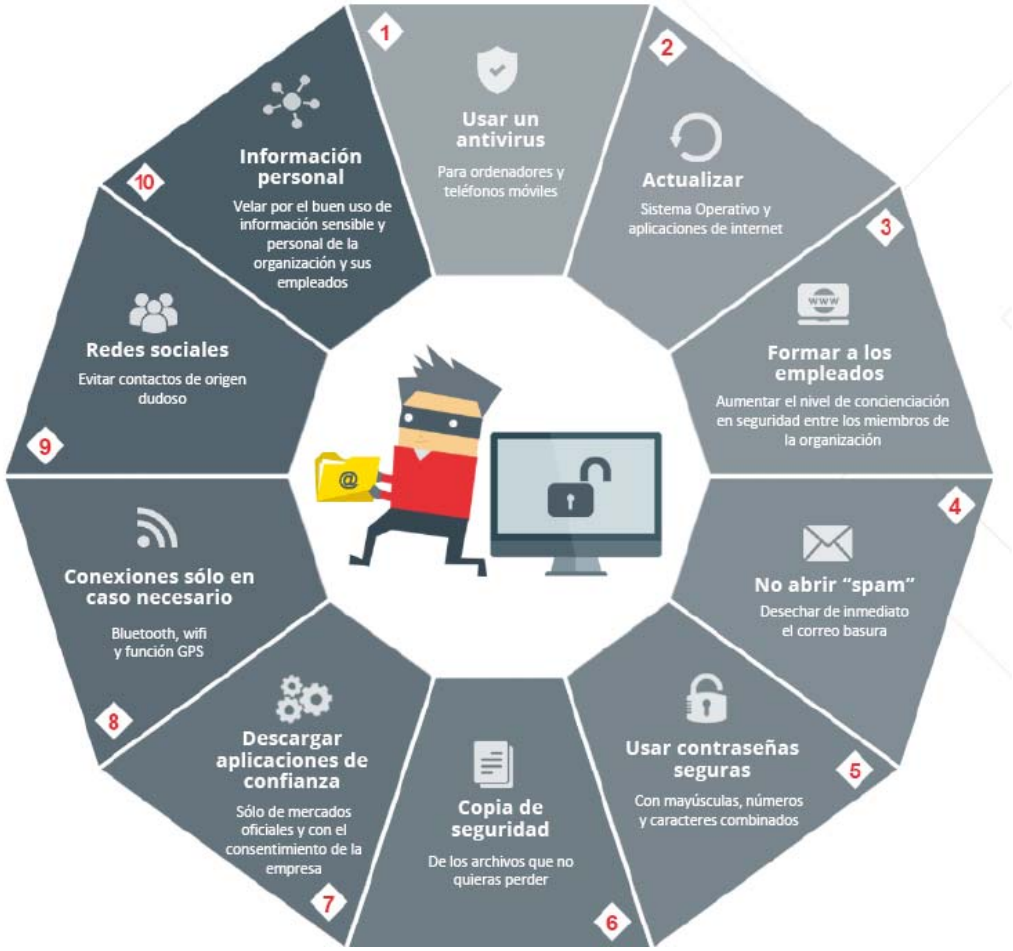
Información	Formación	Herramientas	Atención al internauta
Blog, boletines, ¿qué te interesa?, avisos de seguridad	Antibotnet, antiransomware, juegos de rol, kit de concienciación, respuesta y soporte, catálogo, sellos de confianza, política de seguridad	Hackend, formación sectorial, talleres, guías, cursos para micro-pymes y autónomos	Formulario de contacto y dudas sobre servicios y problemas de ciberseguridad

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

12 ENISE, Encuentro Internacional de Seguridad de la Información

Próxima edición: Octubre 2018, León

Consejos de Ciberseguridad para Pymes



Síguenos en

CONTACTO	Cuidamos **nuestra imagen digital** para reflejar lo que somos, lo que sabemos hacer y lo que hacemos info@incibe.es
VISÍTANOS	Instituto Nacional de Ciberseguridad (INCIBE) info@incibe.es
INFÓRMATE	CERT de Seguridad e Industria (CERTSI) https://www.certsi.es Oficina de Seguridad del Internauta (OSI) https://www .osi.es CyberCamp https://www.cybercamp.es Internet Segura for Kids https://www.is4k.es
SÍGUENOS	Twitter, Youtube, Facebook, LinkedIn, G+. @Incibe @Certsi_ @Osiseguridad @is4k @CyberCampEs @CiberEmprende @protegeempresa
REPÓRTANOS	Incidentes, vulnerabilidades, fraude online, phishing, malware, etc. incidencias@certsi.es, consultas@osi.es y empresas@incibe.es

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD