

# Amenazas para la ciberseguridad en la gestión del software en la empresa

Daniel Fírvida – Coordinador de Servicios  
de Ciberseguridad

[daniel.firvida@incibe.es](mailto:daniel.firvida@incibe.es)

[www.incibe.es](http://www.incibe.es)

INSTITUTO NACIONAL DE  
CIBERSEGURIDAD  
SPANISH NATIONAL  
CYBERSECURITY INSTITUTE



# ¿Qué es INCIBE?

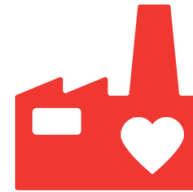
Entidad de referencia para el **desarrollo de la ciberseguridad y de la confianza digital** de:



**Ciudadanos y menores**



**Profesionales** de la ciberseguridad



Empresas, en especial de **sectores estratégicos**



**Red IRIS**

**Red académica** y de investigación española (RedIRIS)

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

Historia



**2006**



**Nace INTECO**

Instituto Nacional de Tecnologías de la Comunicación

**2012**



**INTECO**

Se focaliza en el mundo de la ciberseguridad

**2014**



**Se transforma en INCIBE**

Instituto Nacional de Ciberseguridad de España



Ciudadanos



Operadores de **infraestructuras críticas**



Profesionales

Red **IRIS**

**Red académica** y de investigación española (RedIRIS)



Empresas, en especial de **sectores estratégicos**



FCSE

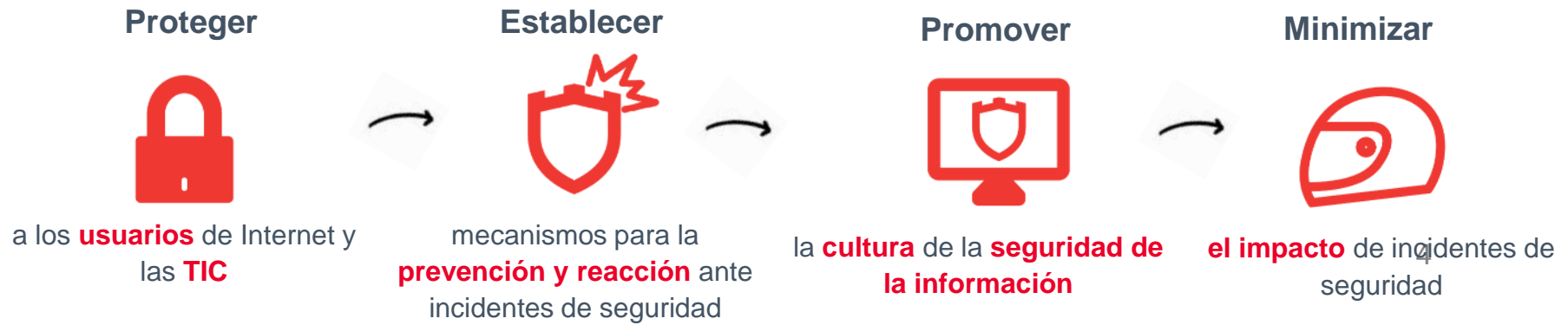
 	GOBIERNO DE ESPAÑA	MINISTERIO DEL INTERIOR
Secretaría de Estado de Seguridad		
<b>CNPIC</b>		

+

 	GOBIERNO DE ESPAÑA	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Secretaría de Estado de Sociedad de la Información y Agenda Digital		
<b>INCIBE</b>		

=


<b>CERTSI</b>



# Incidentes gestionados desde CERTSI

¿Ha sufrido un incidente? Contactenos a través de los siguientes canales

**Ciudadanos y empresas:** [www.osi.es](http://www.osi.es) - Tlf: [901 111 121](tel:90111121) - [incidencias@certsi.es](mailto:incidencias@certsi.es).

Personal perteneciente a la red académica y de investigación (**Red IRIS**): [iris@certsi.es](mailto:iris@certsi.es).

**Operadores estratégicos y de infraestructuras críticas:** [pic@certsi.es](mailto:pic@certsi.es).

Reporte de incidentes

2015



Incidentes  
gestionados

2016

49.976

45.689



Ciudadanos  
y empresas

95.395

4.153

Red IRIS

Red Académica  
(RedIRIS)

3.995

134



Infraestructuras  
críticas

363

99.717 (31 Octubre 2016)

# INCIBE



summer  
bootcamp



FORMACIÓN  
FCSE

FORMACIÓN  
CERTS

10º  
enise  
ENCUENTRO INTERNACIONAL DE SEGURIDAD DE LA INFORMACIÓN  
Trabajando por el desarrollo de la industria nacional de Ciberseguridad  
León, 18 y 19 de octubre de 2016  
Parador Hotel San Marcos de León



Identificar  
talento



Concienciar  
a las familias



Encuentro  
de empresas  
y organizaciones

# Estructura



Situación actual.



Amenazas de seguridad y su evolución.

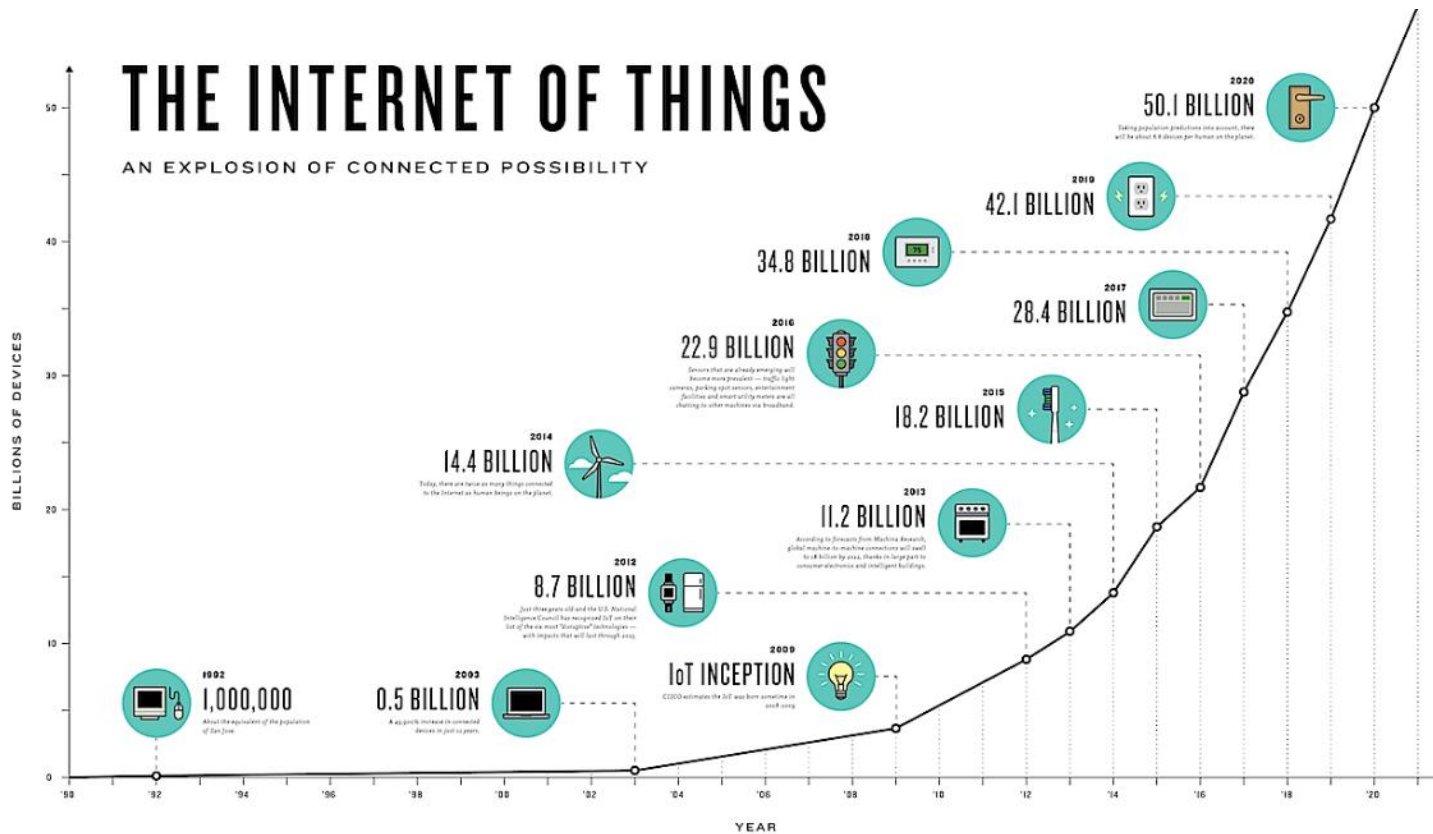


Gestión de la seguridad.



Gestión de software en dispositivos móviles.

# Cualquier dispositivo conectado a internet...



En el año 2.020 se estima que habrá más de **30.000 millones** de dispositivos conectados a la red.

...puede ser atacado





A connected smart collar.



Bluetooth

My SATIS

アプリを立ち上げてSATISと接続

Bluetooth® Connected

SKIP

NEXT

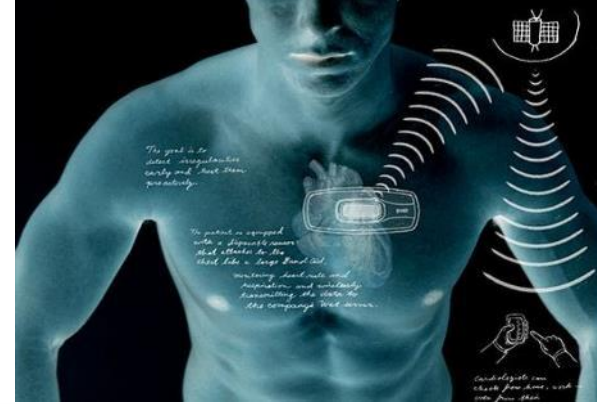
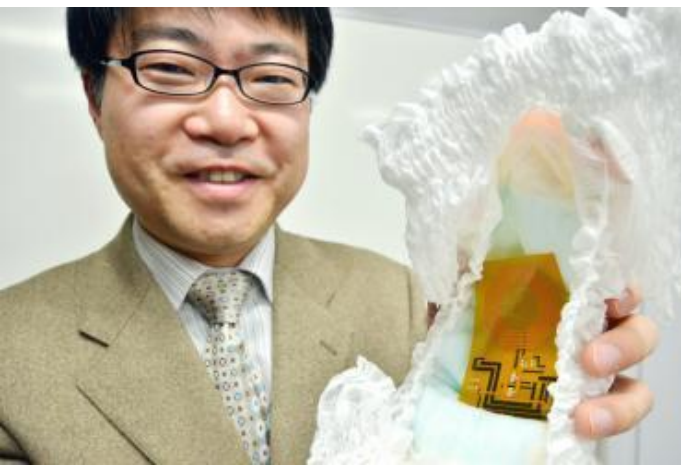
How Do I Do That?

These things are not just smartphones and tablets.

They're every thing.

A Dutch startup, Sparked, is using wireless sensors on cattle.

So that when one is sick or pregnant, it sends a message to the farmer. Each cow transmits 200 mb of data per year.



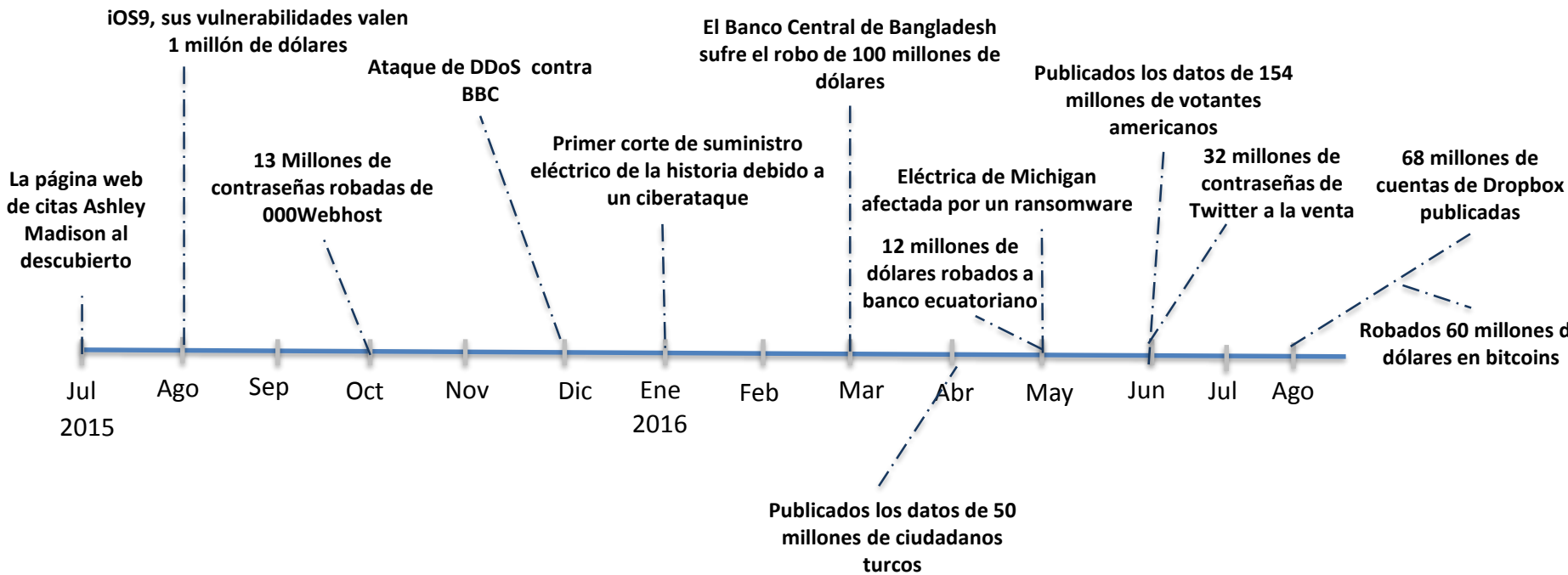


<https://youtu.be/bVp0TNTow9E>





## Bitácora de Incidentes Ciberseguridad



En los últimos 2 años se han producido más de **200 hechos relevantes**



**Se estima que diariamente hay 1,5 millones de personas víctimas del cibercrimen.**

**El cibercrimen representa el 0,8% del PIB mundial,**



**mayor que al tráfico de drogas y de armas.**

Fuente: Intel Security

En 2015 hubo fugas de información que expusieron más de 169 millones de registros personales.



Incluyen nombres, direcciones, números de teléfono, números de cuenta, registros médicos, etc.

Expuestas más de 400 millones de cuentas de Friend Finder Network Inc.

**Adult FriendFinder** Hookup, Find Sex or Meet Someone Hot Now

Username: \_\_\_\_\_ Password: \_\_\_\_\_ [Login](#)  
[Forgot password?](#)

[Join Now!](#) [Home](#) [Browse](#) [Hookup](#) [Dating Forums](#) [Live Chat](#)

**Sign Up Now!**  
Start Hooking Up Tonight!

I am/We are a:

Interested in meeting:  
 Man  Women  
 Couples / Groups  TS/TV/TGs

My birthdate:  
Month  Day  Year

Country:

Zip code:

[Register Now](#)

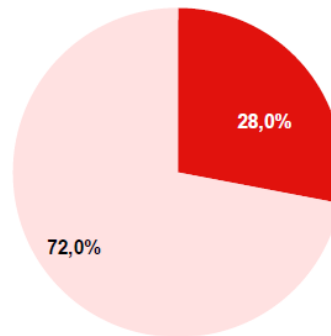
The Hottest  
**Dating, Hookup and Sex  
Community**

ADULT FRIENDFINDER

# Evolución

## 2012

### Malware detectado en el total de la muestra (%)



■ Muestra con malware

■ Muestra sin malware



## 2014

ES Español (España, internacional) GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR COMISIÓN GENERAL DE LA POLICIA Y DE LA GUARDIA CIVIL CUERPO NACIONAL DE POLICIA

**Atención!**

Fue detectado un caso de actividad ilegal. El sistema operativo fue bloqueado por violación de las leyes de España. Fue detectada la siguiente infracción:

Desde su dirección IP bajo el número [redacted] fue efectuado un acceso a páginas de Internet que contienen pornografía, pornografía infantil, zoofilia, asimismo como violencia sobre los menores. En su ordenador, asimismo fueron encontrados archivos de vídeo que contienen pornografía, elementos de violencia y pornografía infantil. Desde el correo electrónico asimismo se realizaba envío de spam con subtexto de terrorismo. El bloqueo del ordenador se realiza para suprimir la posibilidad de acciones ilegales por su parte.

IP: [redacted]

Para quitar el bloqueo del ordenador, usted debe pagar una multa de **100 EURO**.

Usted tiene una forma de pago: Realizar el pago a través de Ukash and Paysafecard. Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introduzcalos uno detrás de otro, y después pulse OK). Si el sistema le genera un error, usted deberá enviar el código al correo electrónico ([deposito@cyber.polico.net](mailto:deposito@cyber.polico.net)).

## 2016

endesa

**RESUMEN DE LA FACTURA**

Fecha factura: 30 de mayo de 2016  
Periodo de facturación: del 28/04/2016 al 29/05/2016  
Factura nº: WYS24 [redacted] 76  
Ref Factura: 52577831 [redacted] 83  
Total Factura: 985,59 €

Datos del Cliente

código personal: 91 [redacted] 34  
Actividad económica (CNAE): [redacted]  
CUPS: [redacted] 3107  
Potencia contratada: 26,3, 26,3 y 26,3 KW  
Tarifa de acceso: 3.0A  
Contrato de acceso: 213 [redacted] 38  
Número de Contador: 003 [redacted] 1

[Consulta tu factura y consumo](#)

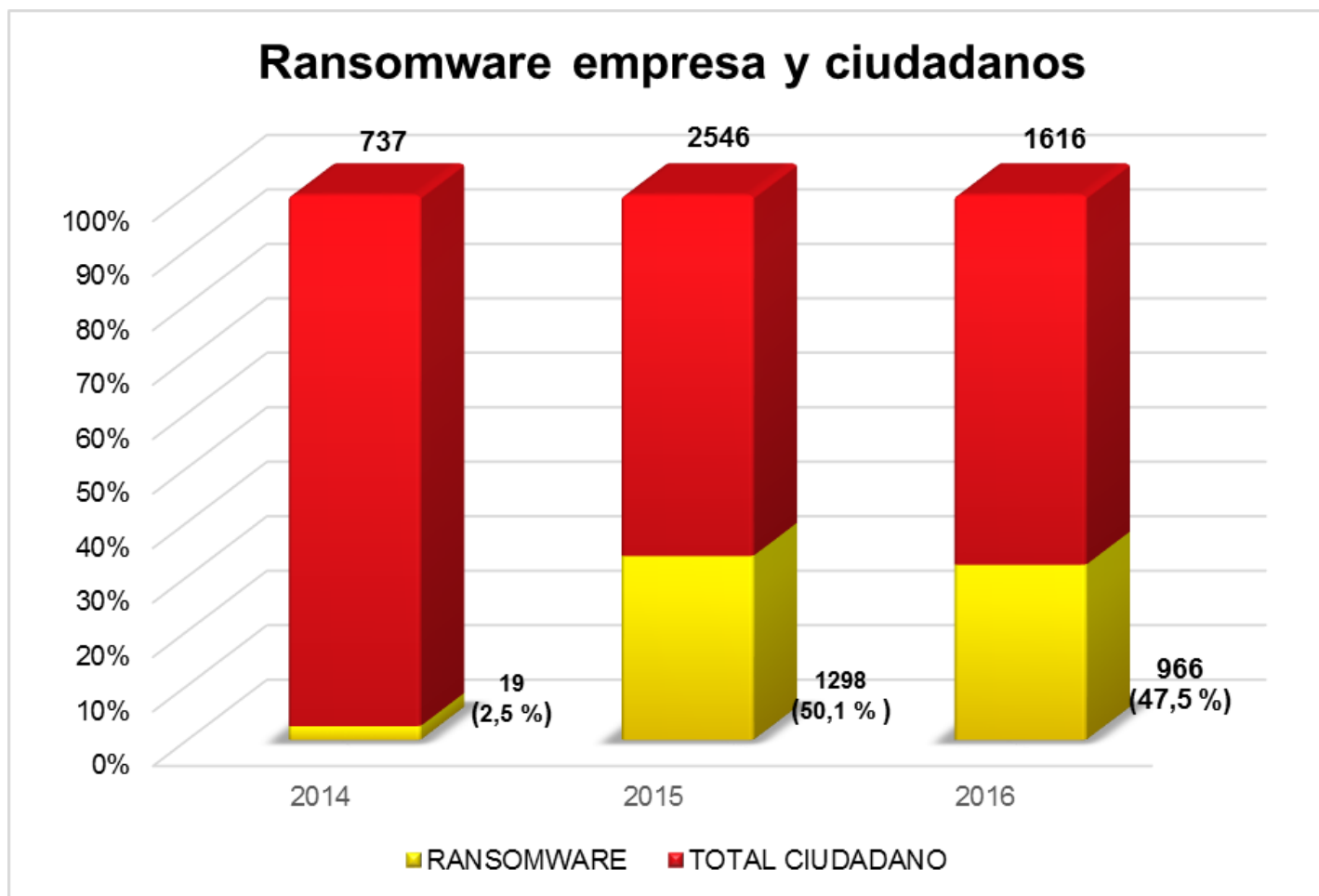
Política de privacidad

La utilización de esta Web le atribuye la condición de Usuario de la misma y expresa su aceptación plena y sin reservas de todas y cada una de las Condiciones Generales publicadas por ENDESA ENERGÍA SA y ENDESA ENERGÍA XXO SL (a partir de ahora "Endesa") en el momento mismo en que Ud. accede a la Web, sin perjuicio de la aceptación de las condiciones particulares que en su caso resulten de aplicación.

Cualquier utilización distinta a la autorizada está expresamente prohibida, quedando Endesa facultada para denegar o retirar el acceso y uso de la Web, en cualquier momento, y sin previo aviso, a aquellos usuarios que incumplan estas condiciones generales o las condiciones particulares que, en su caso, resulten de aplicación.

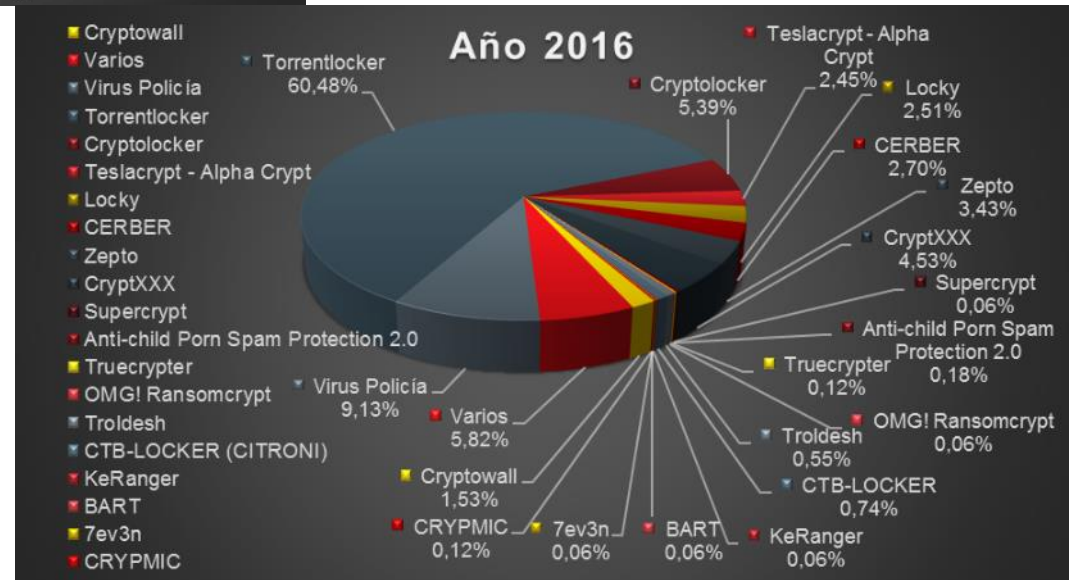
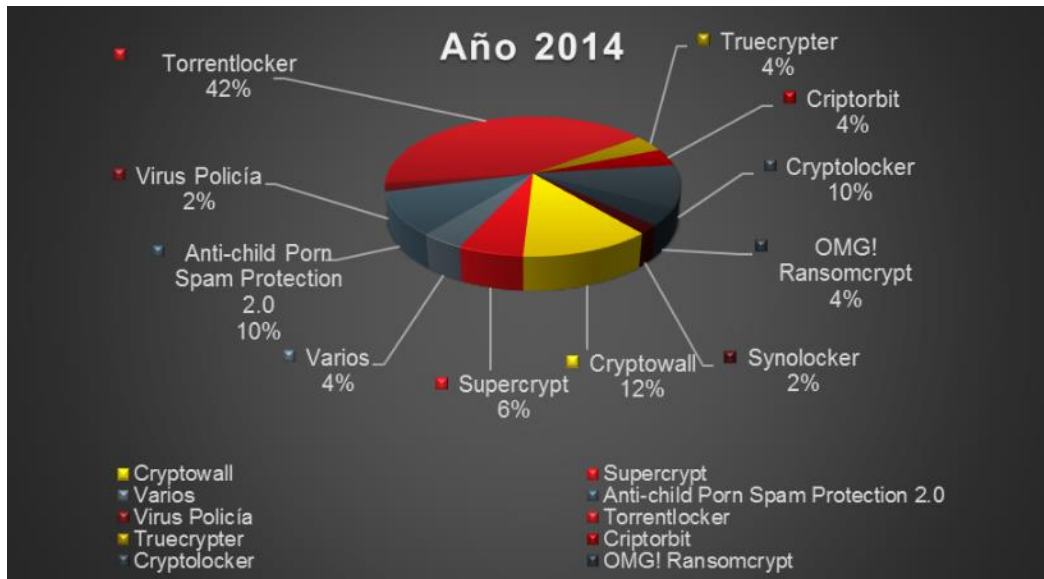
© Endesa S.A. 2016

# Ransomware





# Ransomware



# Ransomware ENDESA



Estimado cliente:

Se ha detectado una campaña fraudulenta simulando avisos de factura de Endesa que invitan a descargarse la factura. Una vez abierto el mail, si haces "clic", enlazas a una página con código malicioso ("virus") que bloquea los archivos personales de los usuarios de ordenadores.

Desde Endesa te recomendamos no hacer clic en los enlaces de ningún eMail de factura que no cumpla que el remitente sea "Endesa Online" [gestiononline@endesaonline.com](mailto:gestiononline@endesaonline.com).

Estamos realizando las acciones pertinentes contra estos ataques informáticos. Te mantendremos informado de cualquier cambio relevante sobre este asunto.

Gracias por confiar en nosotros.

Equipo de Atención al Cliente.

[www.endesaclientes.com](http://www.endesaclientes.com)

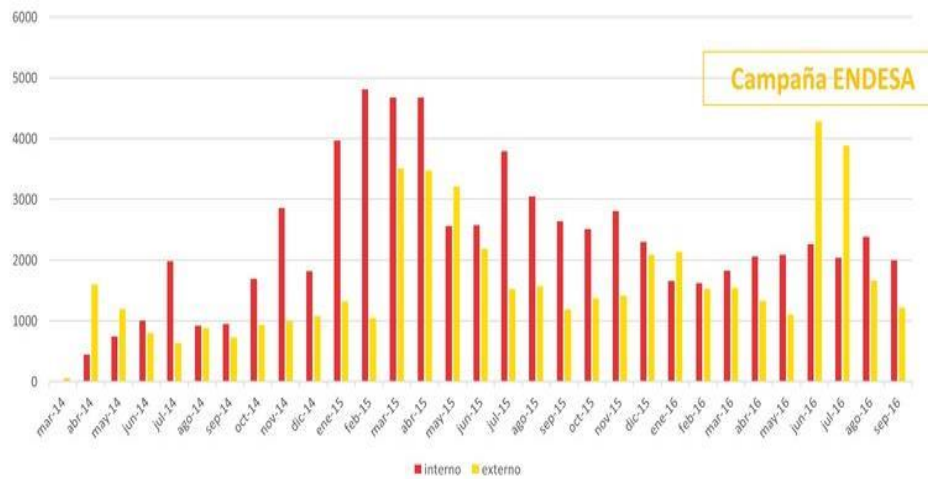


# Ransomware ENDESA



## Ransomware suplantando a Enxesa

Campaña fraudulenta de tipo phishing que suplanta la identidad de la empresa Enxesa con una supuesta factura de la compañía como gancho. A través de un enlace descarga un virus que secuestra la información y solicita dinero para su rescate.



820 casos resueltos del Ransomware de la Campaña Enxesa

# Malware por correo electrónico

Correos españa @bradfordskips.com

Carta Certificada CD 61278791640

**CORREOS**

Su paquete ha llegado a 30 de agosto de 2016. Courier entregará una carta certificada a usted. Imprima la información de envío y mostrárla en la oficina de correos para recibir la carta certificada.

[Descargar información sobre el envío](#)

Si la carta certificada no se recibe dentro de los 30 días siguientes, puede reclamar una indemnización a usted para el mantenimiento de la carta de mantener en la oficina más cercana a usted.

Condiciones y Términos del Servicio de localización de envíos

La consulta del estado detallado para envíos individuales y del estado final de entrega de los envíos de correo certificado que Correos le ofrece para sus envíos remitidos con carácter registrado. Este servicio no se responsabiliza de los errores u omisión de información, por acciones derivadas de la información obtenida por este servicio.

[Haga clic aquí para darse de baja.](#)

@ Copyright 2016 Sociedad Estatal Correos y Telégrafos

Correos

server17.org/b2un2c80.php?id=

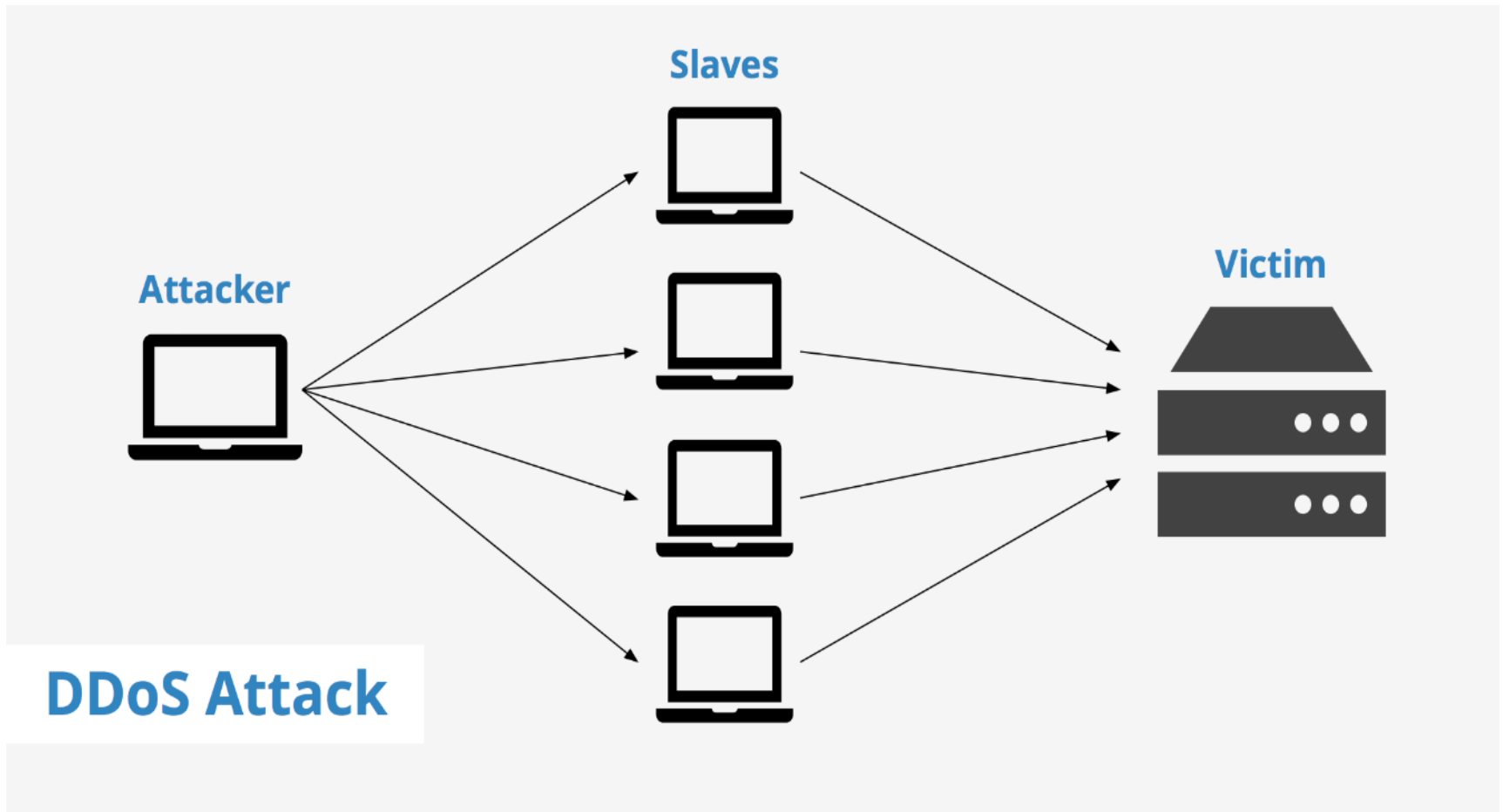
Para acceder rápido a una página, arrástrala a esta barra de marcadores. [Importar marcador](#)

**CORREOS**

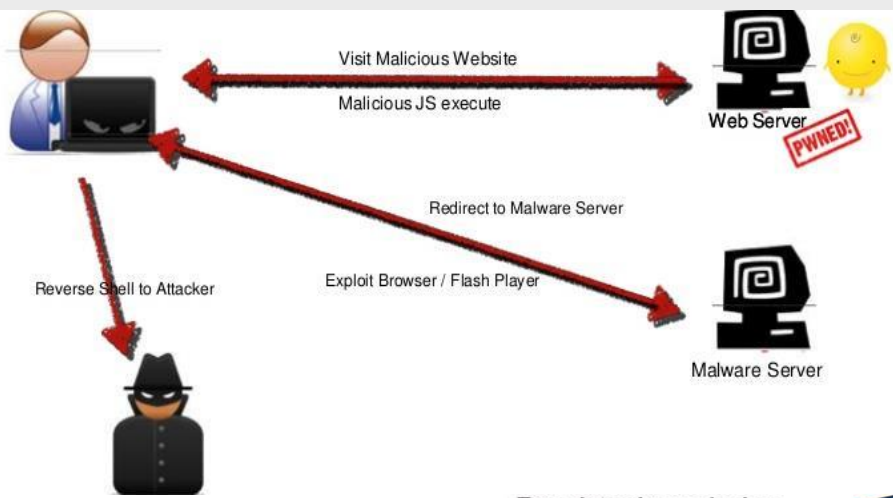
re un momento...

Antivirus	Resultado
AegisLab	Suspar.Gen/c
Avira (no cloud)	HEUR/Suspar.Gen
Cyren	JS/Nemucod.DA!Eldorado
F-Prot	JS/Nemucod.DA!Eldorado
Fortinet	JS/Nemucod.ATA!tr.dldr
K7AntiVirus	Trojan ( 004dfe6d1 )
K7GW	Trojan ( 004dfe6d1 )

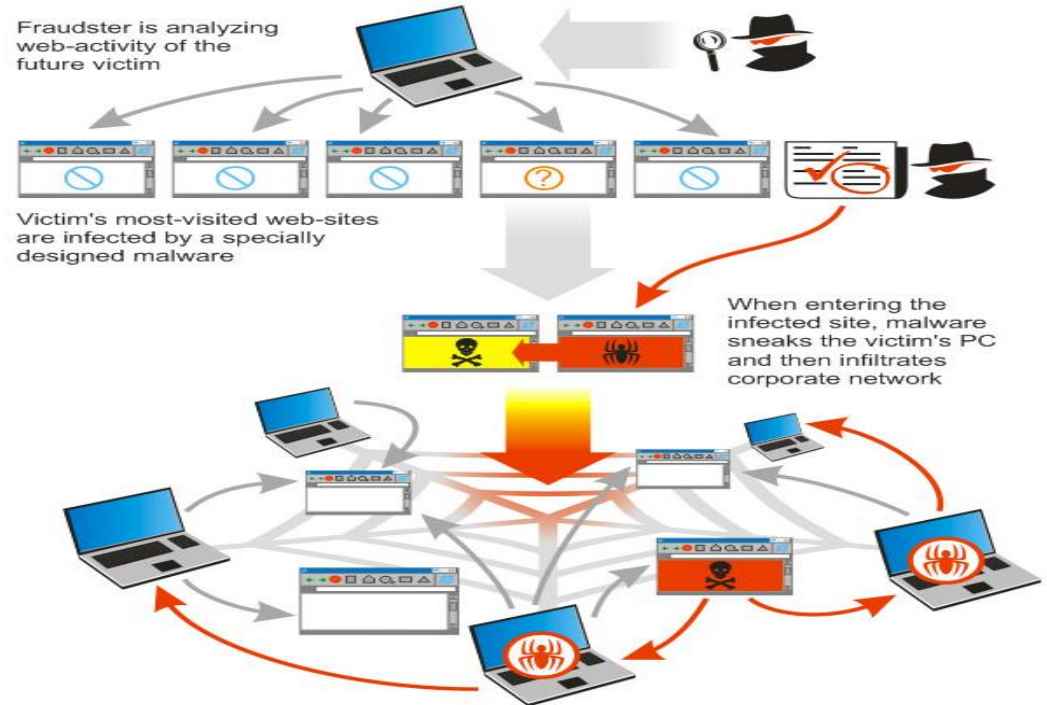
# Denegación de servicio distribuida (DDOS)



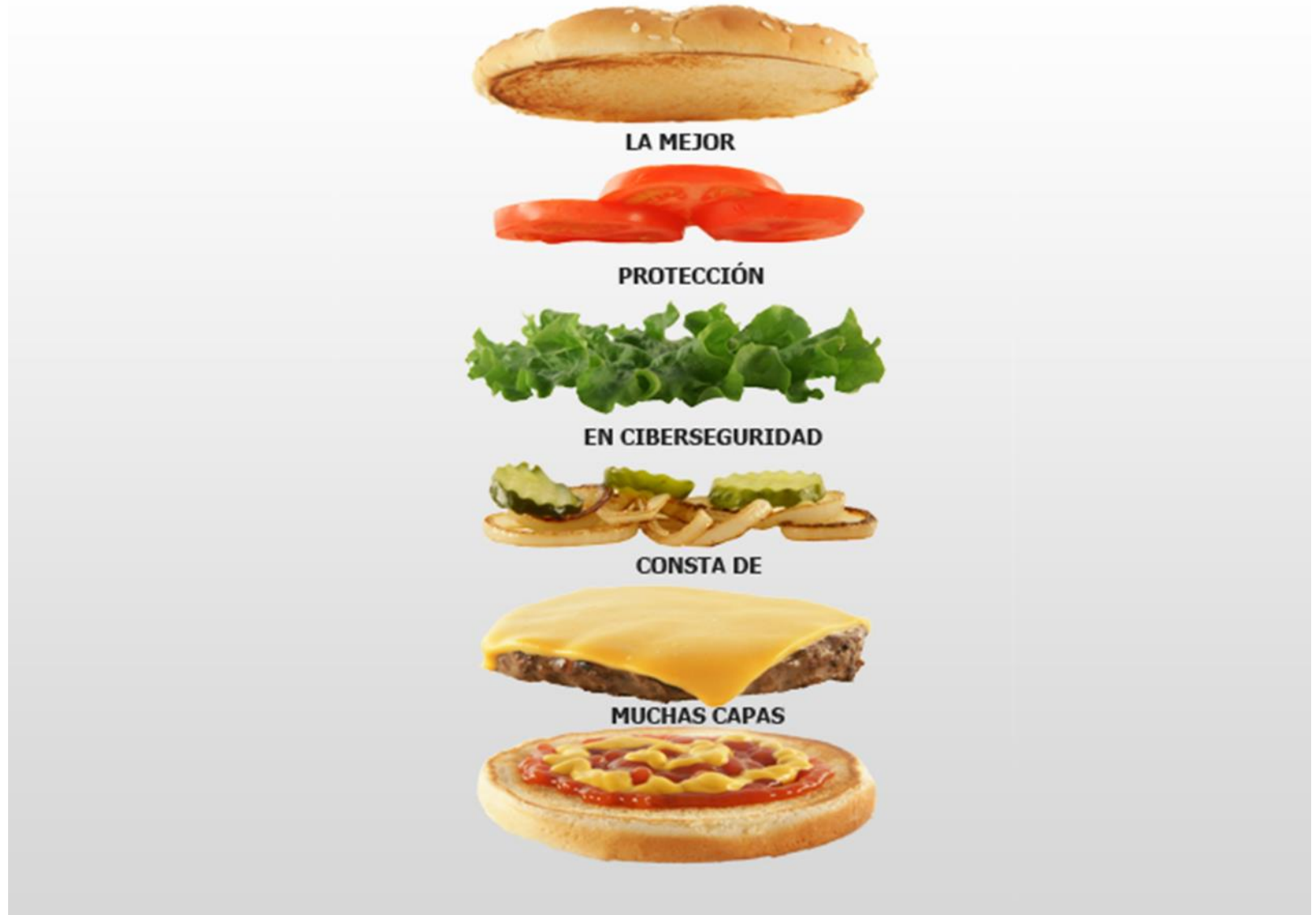
## Drive by download



## Watering hole attack



# Gestión de la seguridad





# Medidas técnicas

- ◆ La importancia de la política de actualizaciones.
- ◆ Gestión de contraseñas y Borrado seguro.
- ◆ Fortificación de configuraciones.
- ◆ Política de control de accesos / (IRM) Information Rights Management -> Gestionar los permisos de los usuarios para reducir la posibilidad de filtraciones de información.
- ◆ Cifrado de información: discos duros, pendrives y móviles.
- ◆ Copias de seguridad periódicas.
- ◆ Blacklisting / Whitelisting.
- ◆ Auditar y Monitorización continua de la red.

# Concienciación a los empleados

- ◆ Uso seguro de redes WiFi.
- ◆ Uso seguro del correo electrónico.
- ◆ Prácticas de navegación segura.
- ◆ Identificación de posible malware.
- ◆ Uso de dispositivos externos.
- ◆ Seguridad en dispositivos móviles.
- ◆ Técnicas de ingeniería social.

La **ciberseguridad** TI  
empieza por TI





# Política de actualizaciones



# SOFTWARE

## Selección de contraseñas



Utiliza siempre **contraseñas robustas**, difíciles de adivinar por otras personas y **nunca las compartas** o las pongas a la vista.

# Política de control de accesos



# SOFTWARE

Monitorización continua de la red



# Lo más importante: SENTIDO COMÚN



Sigue siempre las **recomendaciones** de seguridad, aplica el **sentido común** y si tienes dudas, pregunta a **personal especializado**.





## Malware – Tipos principales

- ♦ **SMS Premium:** Los usuarios se suscriben automáticamente a un servicio de tarificación adicional.
- ♦ **Ransomware:** Cifra multitud de ficheros y solicita un pago a cambio de su devolución.
- ♦ **Botnets:** Realizan multitud de acciones como ataques DDOS, robo de información sensible, monitorización, etc.
- ♦ **Espionaje:** extrae Información como la localización, la lista de contactos, el listado de páginas visitadas, etc.
- ♦ **Robo de credenciales:** es un subtipo del anterior. Busca expresamente Información sensible referente a bancos, redes sociales, etc.

## Vulnerabilidades



### Vulnerabilidades en dispositivos móviles reportadas en 2015

Android	iOS	Windows Phone	Blackberry OS
130	385	1	4

### Vulnerabilidades críticas en dispositivos móviles reportadas en 2015

Android	iOS	Windows Phone	Blackberry OS
50	20	0	1

En 2015 se descubrió una media de 1 vulnerabilidad 0day por semana.

# Un caso real

Escáner desnudo (>50.000 descargas)



**Escáner Desnudo**  
vjjv - 5 de marzo de 2015  
Acción

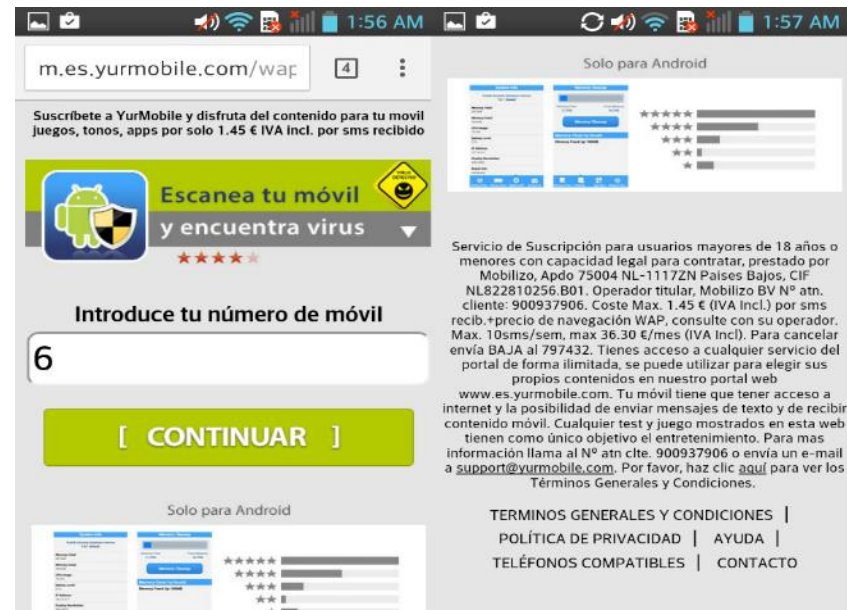
**Instalar**    **Añadir a la lista de deseos**

Esta aplicación es compatible con tu dispositivo.

★★★★☆ (1.070)    **g+1** +462    Recomendar esto en Google

Para abrir la cámara deberás pulsar el botón en la parte inferior y descargar las aplicaciones que ves

Descargar



m.es.yurmobile.com/wap

Suscríbete a YurMobile y disfruta del contenido para tu móvil juegos, tonos, apps por solo 1.45 € IVA Incl. por sms recibido

**Escanea tu móvil y encuentra virus** ★★★★★

Introduce tu número de móvil

6

**[ CONTINUAR ]**

Solo para Android

Servicio de Suscripción para usuarios mayores de 18 años o menores con capacidad legal para contratar, prestado por Mobilizo, Apdo 75004 NL-1117ZN Países Bajos, CIF NL822810256.B01. Operador titular, Mobilizo BV N° atn. cliente: 900937906. Coste Max. 1.45 € (IVA incl.) por sms recib + precio de navegación WAP, consulte con su operador. Max. 10sms/sem, max 36.30 €/mes (IVA Incl.). Para cancelar envía BAJA al 797432. Tienes acceso a cualquier servicio del portal de forma ilimitada, se puede utilizar para elegir sus propios contenidos en nuestro portal web www.es.yurmobile.com. Tu móvil tiene que tener acceso a internet y la posibilidad de enviar mensajes de texto y de recibir contenido móvil. Cualquier test y juego mostrados en esta web tienen como único objetivo el entretenimiento. Para mas información llama al N° atn clte. 900937906 o envía un e-mail a [support@yurmobile.com](mailto:support@yurmobile.com). Por favor, haz clic [aquí](#) para ver los Términos Generales y Condiciones.

TERMINOS GENERALES Y CONDICIONES | POLÍTICA DE PRIVACIDAD | AYUDA | TELÉFONOS COMPATIBLES | CONTACTO

## Un caso real

0 days en iPhone utilizadas contra un defensor de los derecho humanos.

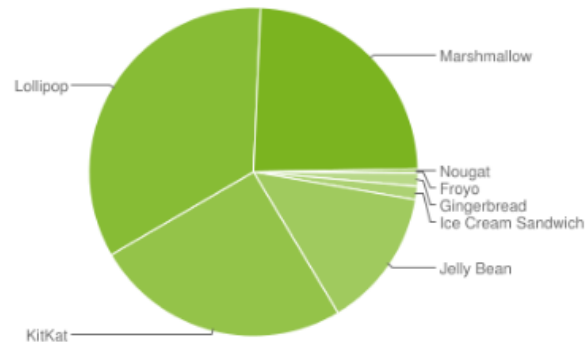


# Fragmentación

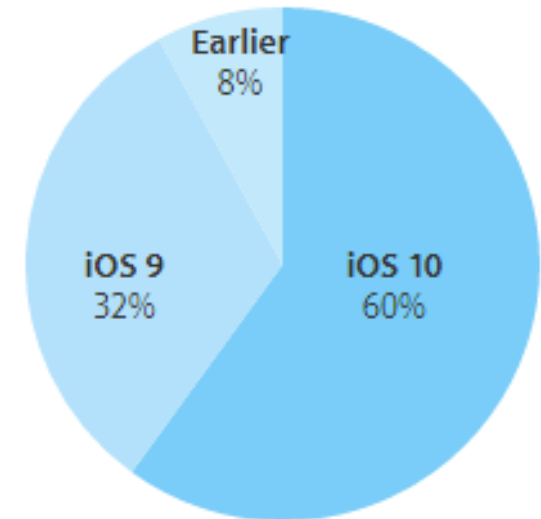
Version	Codename	API	Distribution
2.2	Froyo	8	0.1%
2.3.3 - 2.3.7	Gingerbread	10	1.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.3%
4.1.x	Jelly Bean	16	4.9%
4.2.x		17	6.8%
4.3		18	2.0%
4.4	KitKat	19	25.2%
5.0	Lollipop	21	11.3%
5.1		22	22.8%
6.0	Marshmallow	23	24.0%
7.0	Nougat	24	0.3%

Data collected during a 7-day period ending on November 7, 2016.

Any versions with less than 0.1% distribution are not shown.



60% of devices are using iOS 10.

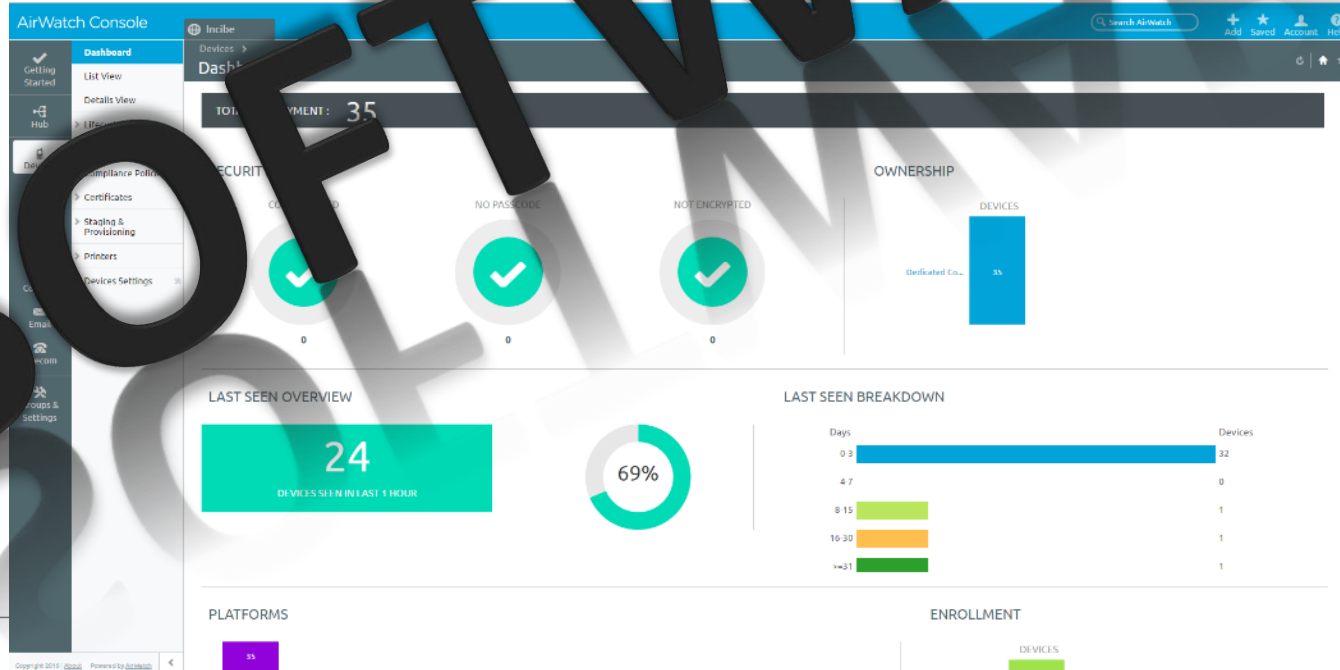


As measured by the App Store on October 25, 2016.



# Soluciones MDM

- Imposibilitar la instalación de cierto tipo de aplicaciones como por ejemplo juegos.
- Imposibilitar el uso de aplicaciones desactualizadas, como por ejemplo el navegador.
- Localización remota de los dispositivos en el caso de que ha sido sustraído o se haya perdido, o incluso el envío de notificaciones.
- Bloqueo de funcionalidades: NFC, cámara, acceso a ciertas configuraciones del terminal, etc.
- Forzar establecer un mecanismo de seguridad: contraseña patrón, etc.
- Instalación de certificados de seguridad.
- Bloqueo remoto del terminal o eliminación del contenido.
- Detección de intentos de root, jailbreak o ploteo.



# ¿Más información?



## Ransomware suplantando a Endesa

Campaña fraudulenta de tipo phishing que suplanta la identidad de la empresa Endesa con una supuesta factura de la compañía como gancho. A través de un enlace descarga un virus que secuestra la información y solicita dinero para su rescate



[Ampliar información](#)

# «Protege tu empresa» en [www.incibe.es](http://www.incibe.es)

### Formación para PYMES



### Kit de Concienciación



### ¿Conoces tus riesgos?



### Avisos de seguridad

- ◆ Filtradas credenciales de Dropbox  
31/08/2016
- ◆ Otra oleada de ransomware suplantando a Correos  
31/08/2016
- ◆ Actualización urgente de seguridad en Apple iOS9  
26/08/2016

### Últimas entradas del Blog



#### Cinco estrategias paralímpicas aplicadas a la empresa cibersegura

Publicado el 07/09/2016

¡Comienzan los Juegos Paralímpicos! Un evento deportivo, que ya va por su decimoquinta edición, en el que participan atletas de todo el mundo con diversidad funcional física, mental o sensorial,...

Gracias por su atención

