

INTECO-CERT team update

FIRST TC / TF-CSIRT Las Palmas, January 27th 2015

Javier Berciano



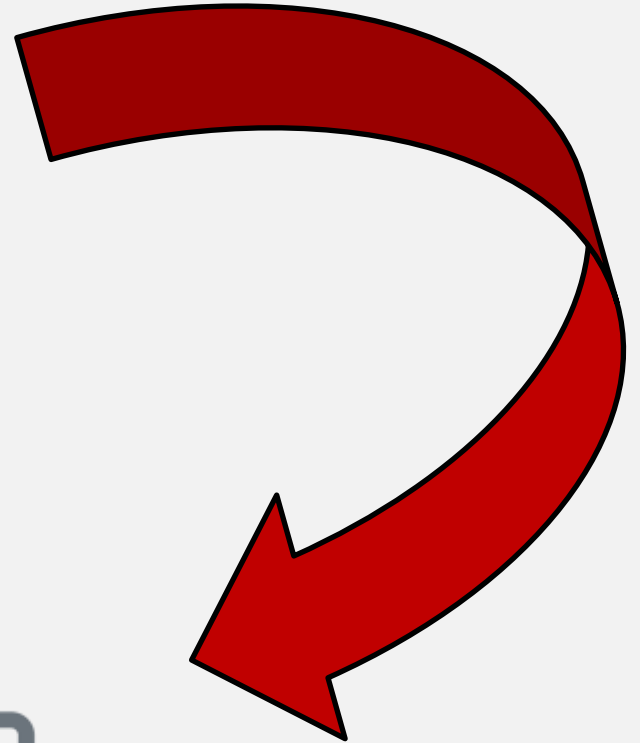
INTECO → INCIBE



inteco



Instituto Nacional
de Tecnologías
de la Comunicación

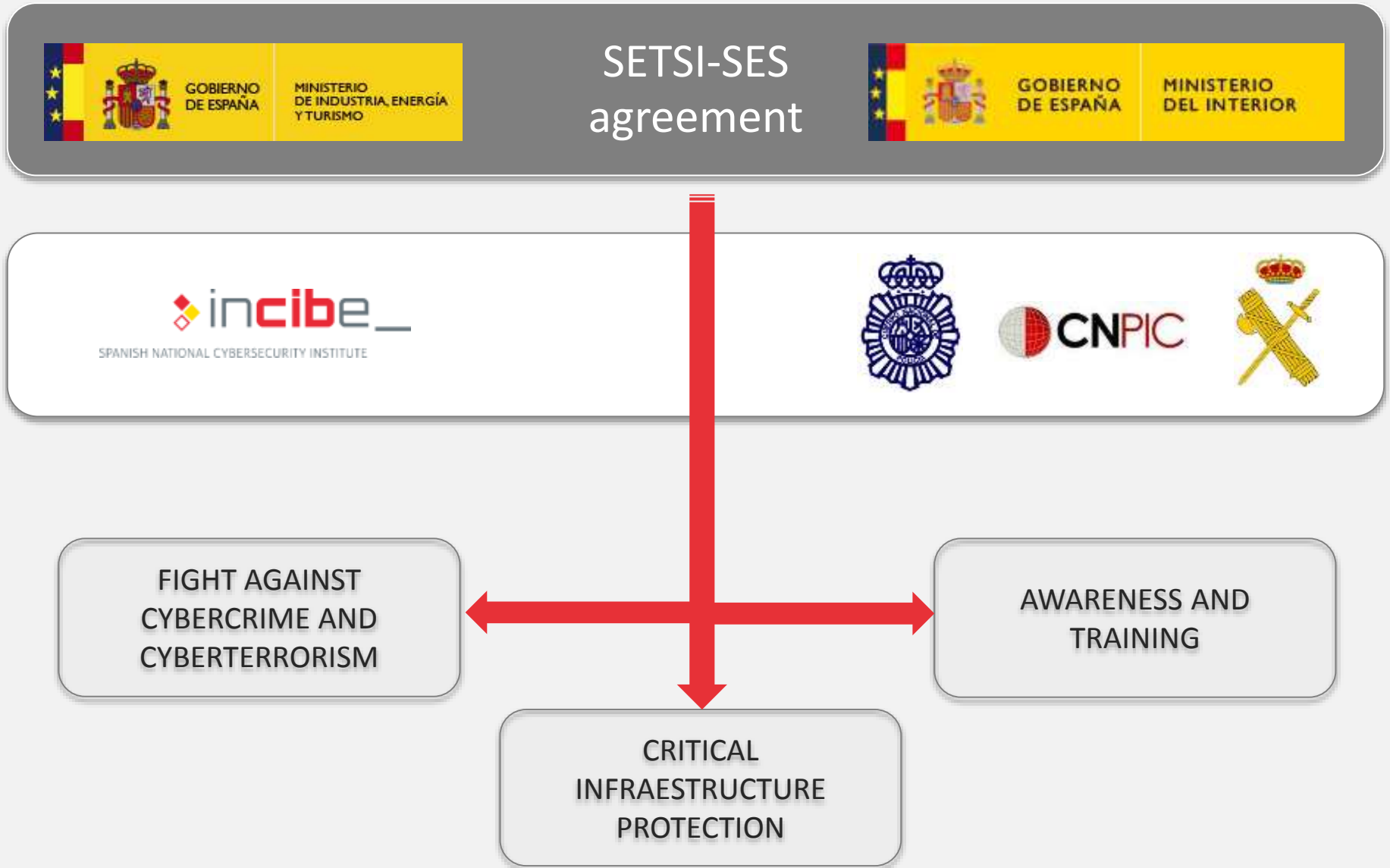


incibe _

SPANISH NATIONAL CYBERSECURITY INSTITUTE



Coordination SETSI-SES





INTECO-CERT → CERTSI

inteco
(cert)



 **certsi**

CERT DE SEGURIDAD E INDUSTRIA

Incident handling	Proactive detection	Early warning	Cyber Exercises	Awareness raising
--------------------------	---------------------	---------------	-----------------	-------------------



Enterprises and citizens
incidencias@certsi.es



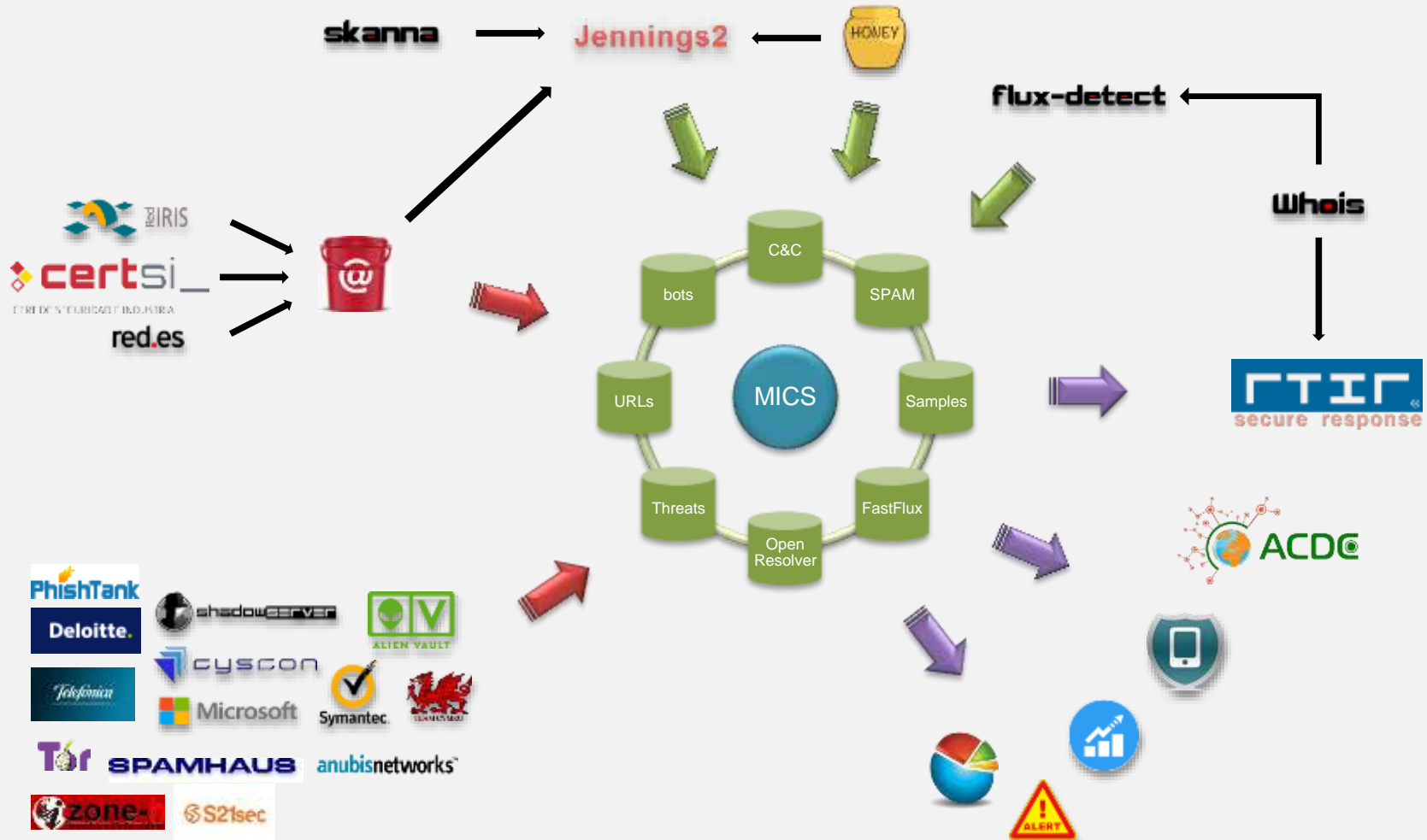
Critical infrastructures
pic@certsi.es



24x7x365



Incident handling	Proactive detection	Early warning	Cyber Exercises	Awareness raising
-------------------	----------------------------	---------------	-----------------	-------------------



Incident
handling

Proactive
detection

Early
warning

Cyber
Exercises

Awareness
raising

0day vulnerabilities reports

General software

SCADA software



Incident
handling

Proactive
detection

Early
warning

**Cyber
Exercises**

Awareness
raising

CYBER-ES

15 critical infrastructures operators involved

Design: APT behaviour scenario with 3 phases

- **Phase 1: Social engineering**
- **Phase 2: Internal pentest**
- **Phase 3: Incident handling scenario**

Incident
handling

Proactive
detection

Early
warning

Cyber
Exercises

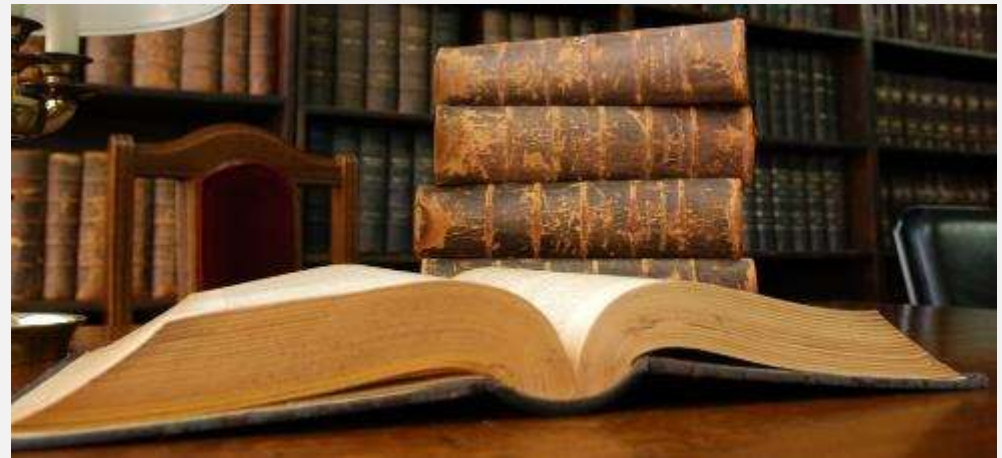
**Awareness
raising**

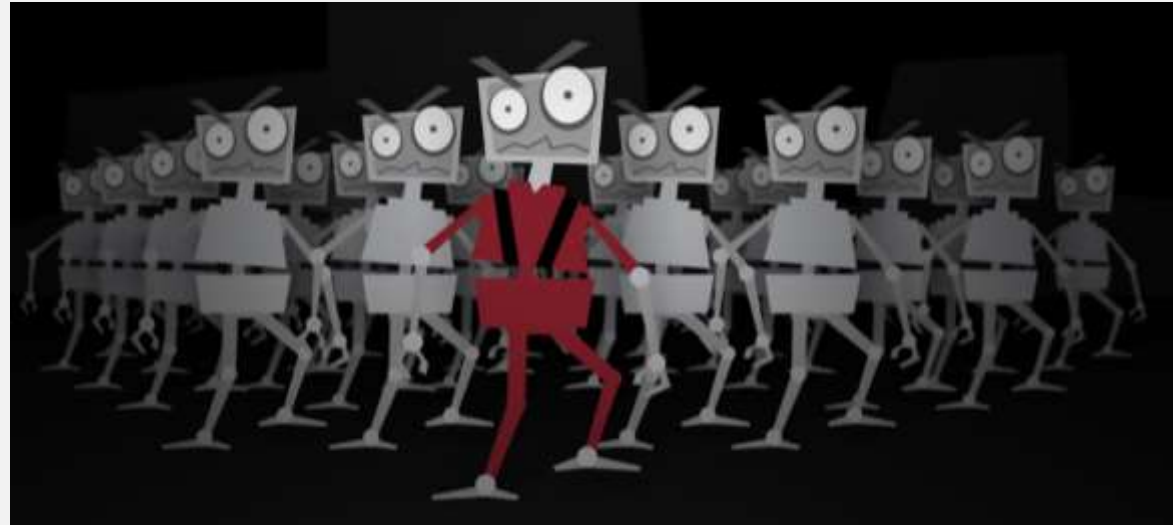
Learn for protect

OSINT reports

Cheatsheets

Best practices





Facts:

5,8 millions botnet related **evidences daily**

Close to **74.000** unique Spanish **IP addresses infected**

Information from **570 sinkholes** with **83** different **botnets**



Servicio ANTIBOTNET

Goals:

Botnet **mitigation** and **disinfection**

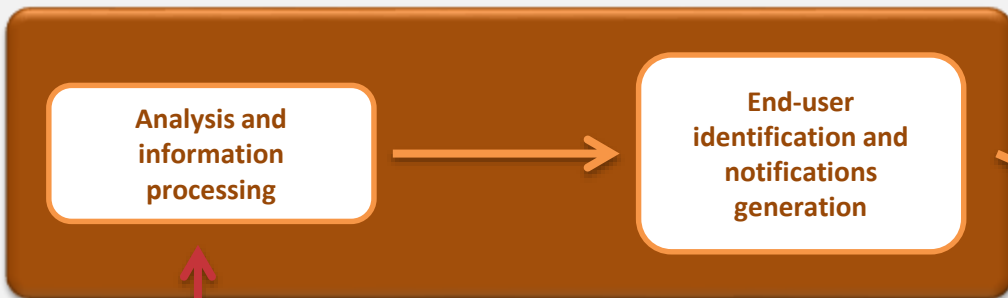
Realtime **IP check** service

End user **reporting**



AntiBotnet service

Telefonica



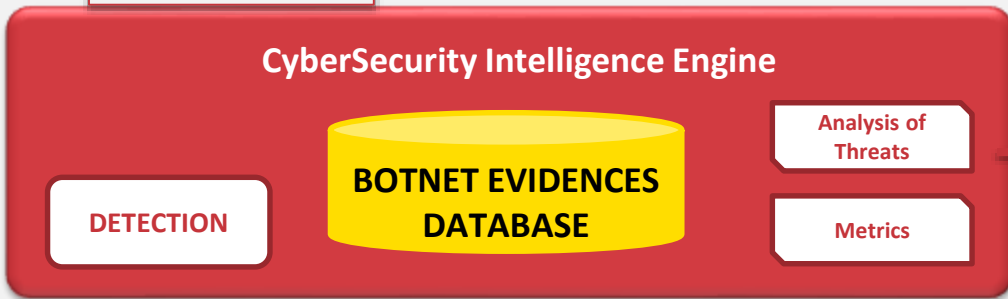
ANTIBOTNET SERVICE URL + Botnet Ticket



END USER

Feed (bots)

incibe_



OSI Oficina de Seguridad del Internauta

Servicio **ANTIBOTNET**

TRUSTED SOURCES

Threat Information and disinfection Tools

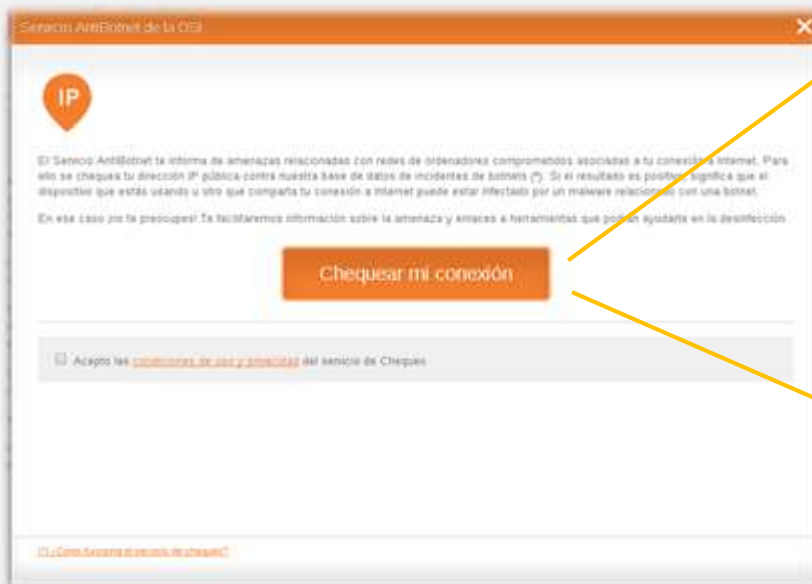
Awareness and Prevention



Descarga el **plugin** para tu navegador y te avisamos automáticamente



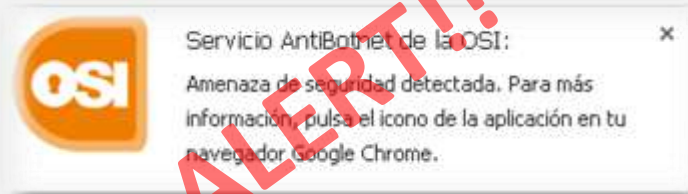
Online IP check





AntiBotnet service

Chrome extension



OSI Servicio AntiBotnet de la OSI:
Amenaza de seguridad detectada. Para más información, pulsa el icono de la aplicación en tu navegador Google Chrome.

ALERT!!!



OSI Servicio **ANTI BOTNET**

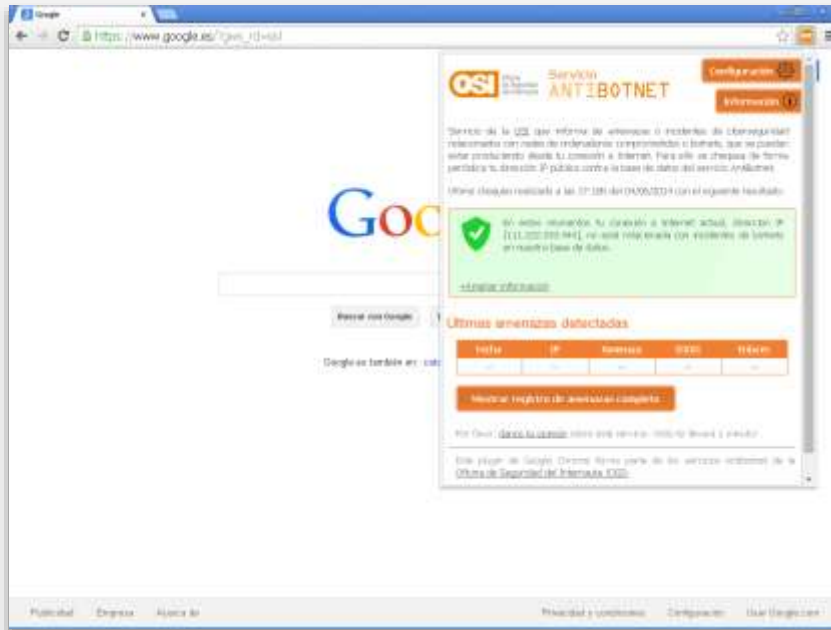
Servicio de la OSI que informa de amenazas o incidentes de ciberseguridad relacionados con redes de ordenadores comprometidos o botnets, que se pueden estar produciendo desde tu conexión a Internet. Para ello se chequea de forma periódica tu dirección IP pública contra la base de datos del servicio AntiBotnet. Última chequeo realizado a las 17:30 del 04/06/2014 con el siguiente resultado:

Alerta de seguridad: Alguna de las direcciones de tu red puede estar infectada como amenazas, botnets, de seguridad comprometidos o botnets asociados a la conexión a Internet actual, dirección IP: 111.222.222.444. Consulta la lista de amenazas detectadas.

Últimas amenazas detectadas

Fecha	IP	Amenaza	OSI	Tiempo
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado

[Ver el registro de amenazas completo](#)



OSI Servicio **ANTI BOTNET**

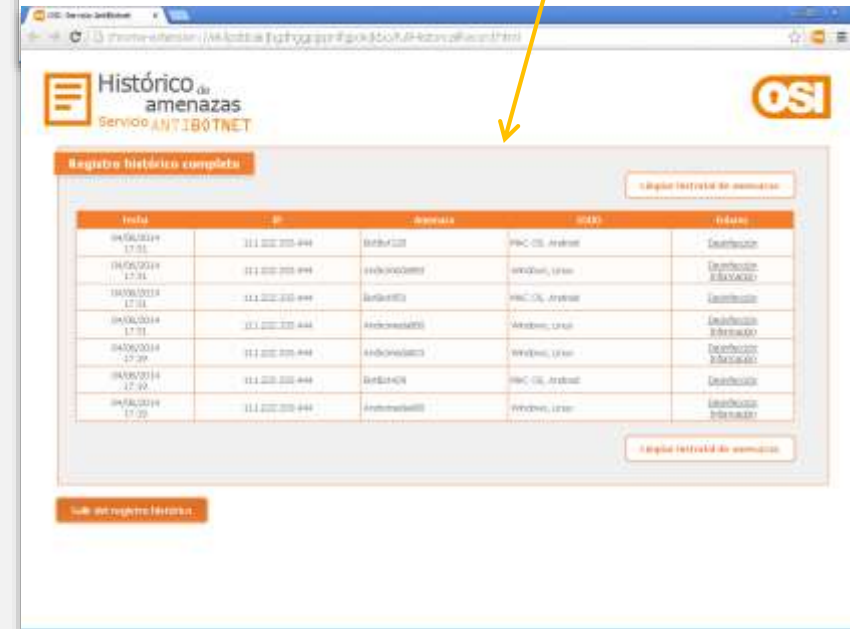
Servicio de la OSI que informa de amenazas o incidentes de ciberseguridad relacionados con redes de ordenadores comprometidos o botnets, que se pueden estar produciendo desde tu conexión a Internet. Para ello se chequea de forma periódica tu dirección IP pública contra la base de datos del servicio AntiBotnet. Última chequeo realizado a las 17:30 del 04/06/2014 con el siguiente resultado:

Seguro: No se ha detectado la conexión a Internet actual, dirección IP: 111.222.222.444, no está relacionada con redes de botnets o amenazas de datos.

Últimas amenazas detectadas

Fecha	IP	Amenaza	OSI	Tiempo
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado

[Ver el registro de amenazas completo](#)



Histórico de amenazas
Servicio **ANTI BOTNET**

Registro histórico completo

Fecha	IP	Amenaza	OSI	Tiempo
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado
04/06/2014 17:30	111.222.222.444	Botnet	Windows, Linux	Detectado



Detailed information about threat Disinfection tools (AV cleaners)

Zeus

¿Qué es?	Zeus es un malware de tipo troyano que infecta ordenadores con sistema operativo robando credenciales bancarias u obtener otro tipo de información relevante. Además este malware pasan a ser parte de una botnet, con lo que pueden ser utilizados para maliciosos.
¿Qué hace?	Este troyano fue diseñado inicialmente para robar información confidencial de los usuarios, por ejemplo la información del sistema, las credenciales de los usuarios y sus datos. En su alto grado de personalización puede adaptarse para recibir cualquier tipo de información. Además, los ordenadores infectados por Zeus son controlados mediante un servidor que habilita la posibilidad de que los bots realicen funciones adicionales, como desinstalar o modificar la configuración del sistema.
Otros nombres/Alías	Zbot
Sistemas afectados	Principalmente sistemas Windows: <ul style="list-style-type: none"> Windows XP Windows Vista Windows 7 Windows 8
¿Cómo fue infecta?	El troyano es distribuido principalmente a través de: <ul style="list-style-type: none"> Campañas de spam, mediante la suplantación de organizaciones como Facebook. Usuarios visitan un sitio web, mediante un enlace proporcionado, para infectar el sistema. Descarga directa desde Internet de archivos infectados. Sin embargo debido a la gran versatilidad y adaptabilidad de Zeus podrían ser usados otros métodos.
Cómo desinfectar mi equipo	http://www.csi.es/servicio-antibotnet/informacion/zeus
Más información	http://www.symantec.com/security_response/weblog.jsp?docid=2010-011016-3514 http://en.wikipedia.org/wiki/Zeus_(Trojan_horse)#

Servicio Antibotnet: Cleaners

Si has llegado aquí desde el Servicio AntiBotnet es porque se han identificado incidentes de seguridad relacionados con botnets asociados a tu dirección IP pública, es decir, a tu conexión a Internet. Recuerda que al dispositivo afectado es alguno de los que están o estaban conectados a Internet en tu red en el momento de la detección del incidente. No tiene porqué ser el equipo desde el que realizaste el chequeo.

Por lo tanto, el primer paso para desinfectarte es identificar cual es el equipo afectado. Los datos que te hemos proporcionado (fecha y hora de la detección del incidente y sistemas operativos a los que afecta), te ayudarán a la identificación.

A continuación te facilitamos un listado de herramientas, también llamadas cleaners, que podrán ayudarte a limpiar tu equipo de las principales botnets.

ESET Online Scanner	Kaspersky Virus Removal Tool	Comodo Cleaning Essentials	Sophos Virus Removal Tool	Panda Cloud Cleaner
Descargar	Descargar	Descargar	Descargar	Descargar

Recuerda que estas herramientas no sustituyen en ningún caso a los sistemas antivirus o anti-malware. Te recomendamos que estés al día de los **consejos** para prevenir infecciones y que utilices **herramientas de seguridad** en tus dispositivos.



AntiBotnet service

Estimado/a cliente:

Dentro del marco de colaboración público-privada que Telefónica de España, S. A. U. mantiene con la Administración española y en el ánimo de velar por la seguridad de sus usuarios de Internet, y en cumplimiento con lo dispuesto en el Real Decreto 34/2002, de 11 de julio[1], nos dirigimos a usted para avisarle de un incidente de seguridad por parte del Centro de Respuesta a Incidentes de Seguridad de Internet (CRISI) del cual se nos comunica que alguno de los equipos conectados a Internet [.....] podría estar afectado por un programa malicioso o botnets.

28/10/14

Según este aviso, con fecha [.....] y con la dirección IP [.....] de su conexión a Internet, algún equipo o dispositivo habría sido infectado por un programa malicioso o botnets, y por lo tanto se puede estar afectando a usted mismo e incluso a otros usuarios de Internet.

Procedimiento de desinfección

Para obtener más información sobre esta amenaza y proceder a la desinfección de su equipo, puede acceder a la web de la Oficina de Seguridad del Internauta (OSI) de las Tecnologías de la Comunicación (INTECO).

<http://www.osi.es/es/servicio-antibotnet>

Para introducir el siguiente código en la casilla que figura "Introduzca el código de incidente"

GFzo

[.....]

Información sobre la iniciativa AntiBotnet

La iniciativa AntiBotnet es un proyecto de colaboración público-privada puesto en marcha por los principales prestadores de servicios de la sociedad de la información, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) e INTECO.



OSI Oficina de Seguridad del Internauta

¿Quiénes somos? Encuesta de valoración Contacto Boletines **INTECO**

Ponte al día ¿Cuánto sabes? ¿Qué deberías saber? **¿Cómo protegerte?** ¿Necesitas ayuda?

Servicio AntiBotnet

Nuestro servicio AntiBotnet pone a tu disposición mecanismos para poder identificar si desde tu conexión a Internet (siempre que lo utilices dentro de España) se ha detectado algún incidente de seguridad relacionado con botnets, ofreciéndote información y enlaces a herramientas que te pueden ayudar en la desinfección de tus dispositivos.

Este servicio se ofrece de dos formas:

- La primera se lleva a cabo mediante los Proveedores de Acceso a Internet que colaboran con nosotros notificándote de los incidentes de seguridad que afectan a tu conexión. Si has recibido un mensaje de tu proveedor, consulta el código que te ha proporcionado y obtén la información directamente.
- La segunda es mediante el uso de nuestras herramientas online.

Si tu proveedor de acceso a Internet te ha enviado un código de incidente

Usa el servicio online y obtén respuesta al instante

Consulta tu código

Chequea tu conexión

¿Cómo funciona el servicio de notificación de códigos?

¿Cómo funciona el servicio de chequeo?

(*) Actualmente este servicio se encuentra en fase piloto y se está llevando a cabo con la colaboración de los principales prestadores de servicios de la sociedad de la información.

Descarga el plugin para tu navegador y te avisamos automáticamente



El código GFzo está asociado a la siguiente amenaza o problema de seguridad:



torpig

[Información sobre esta amenaza](#)

Afecta a los sistemas operativos: Windows, MacOS

[Información de ayuda para la desinfección](#)

Botnet Torpig

Acepto las [condiciones de uso y privacidad](#)

¿Qué es?	Es un tipo de malware que toma control de los equipos comprometidos para comunicarlos con un servidor de control. A este servidor envía datos robados de la víctima y a su vez recibe configuraciones con objeto de robar información y controlar la máquina infectada.
¿Qué hace?	Se conecta bajo demanda o periódicamente con el servidor de control para recibir configuraciones o enviar datos robados. Interviene en la navegación web y provoca redirecciones a urls maliciosas simulando sitios legítimos como bancos, servidores de correo, etc. De esta forma logra obtener información concreta de la víctima, tales como datos de formularios de login, cuentas de correo y sitios web, servidores FTP, contraseñas de Windows, etc.
Otros nombres/Alías	Sinawal, Anserin
Sistemas afectados	Principalmente sistemas Windows: <ul style="list-style-type: none"> • Windows XP • Windows Vista • Windows 7 • Windows 8
¿Cómo me infecta?	La infección parte de una primera fase que sucede al visitar un servidor web malicioso o comprometido. Desde ésta, se descarga un programa denominado Mebroot que modifica el sector de arranque del ordenador infectado e inicia la segunda fase de la infección. En esta segunda fase, Mebroot se conecta con un servidor de control desde donde se distribuye el malware Torpig en sí. Torpig se instala inyectándose en aplicaciones del sistema y convirtiéndolo en un "ordenador zombi" o "bot" bajo control de un servidor central. Una vez completada la infección con Torpig, el malware obtendrá datos de la máquina comprometida y los enviará al servidor de control.
Cómo desinfectar mi equipo	http://www.osi.es/servicio-antibotnet/cleaners
Más información	http://en.wikipedia.org/wiki/Torpig#

Questions?

Thank you!

Javier Berciano
javier.berciano@incibe.es