GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_ WORKING FOR DIGITAL TRUST
certsi_ SECURITY AND INDUSTRY CERT

Information sharing with private sector: Spanish overview

Javier Berciano
Head of Incident Handling

FIRST Improving Security Together

FIRST Regional Symposium for Arab and African Regions
November 2016

Strategy

National Institute for CyberSecurity

Digital Agenda for Spain

(15/02/2013)

General Objectives

- *Reflect the Government's strategy in the digital and telecom field*
- *Compliance with the objectives of the Digital Agenda for Europe*

6 Objectives

Objetctive 4. Strenghten trust in the digital enviroment
4.2. Strengthen capabilities to digital trust

9 Action Plans **Plan to improve Trust in the Digital Field**

SES-SETSI Agreement

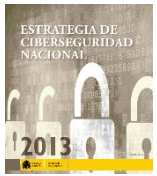
(04/10/2012 - 21/10/2015 -)

certsi_

SECURITY AND INDUSTRY CERT

- **Combating cybercrime and cyberterrorism**
- **Critical infrastructure Protecion**
- **Dissemination, awareness, education and training**

National Cybersecurity Strategy



(5/12/2013)

INCIBE involvement

3rd Action Line:

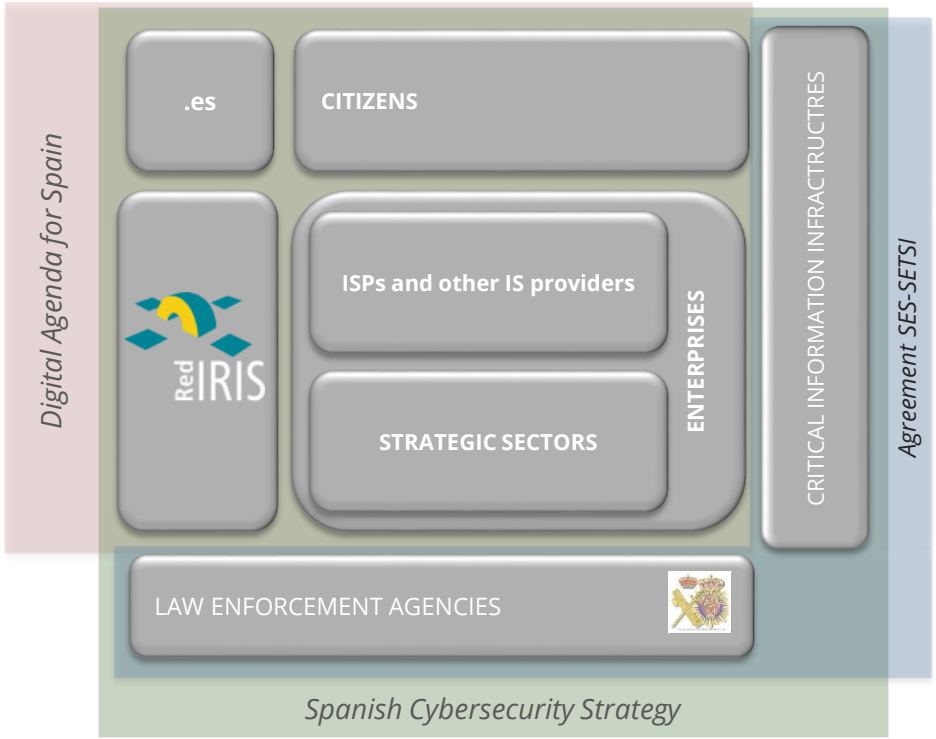
- **CIP Regulation implementation**
- **Capabilities and collaboration**
- **Cyberexercises with the private sector**
- **Simulation models in CII**

Other action Lines:

- **National and international organization and coordination.**
- **Cyberterrorism and cybercrime investigation capacities**
- **Public-private Partnership**
- **Generation and management of talent, promotion of innovation and competitiveness**
- **Cybersecurity culture**

certsi_
SECURITY AND INDUSTRY CERT

Cybersecurity capacity for…



Incidents by constituency

Incidents handled
in 2015

49.976

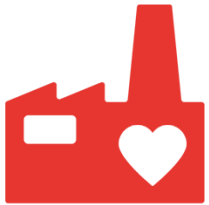
45.689

The public and companies

Red IRIS

4.153

Academic Network (RedIRIS)



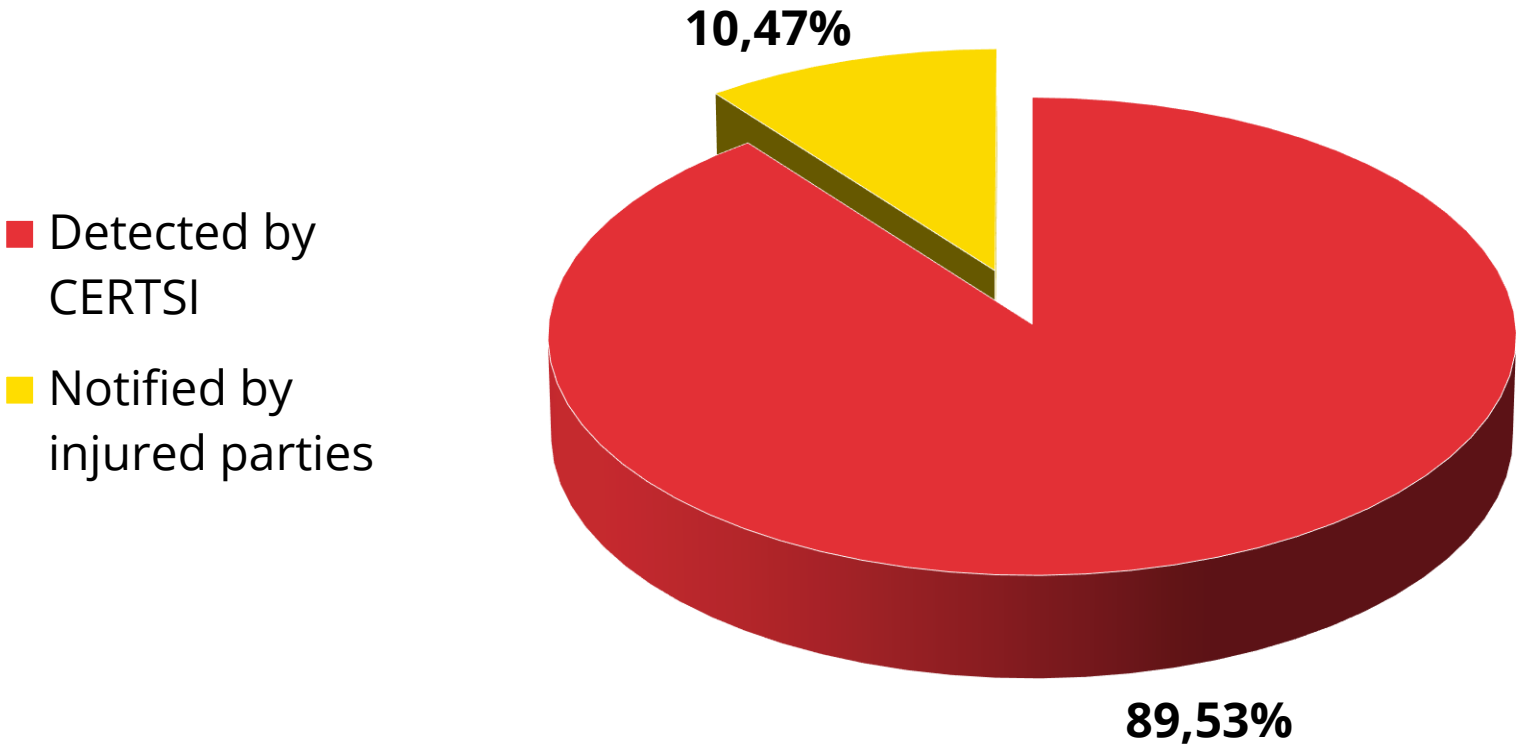
134

Critical Infrastructure

Types of incidents 2015

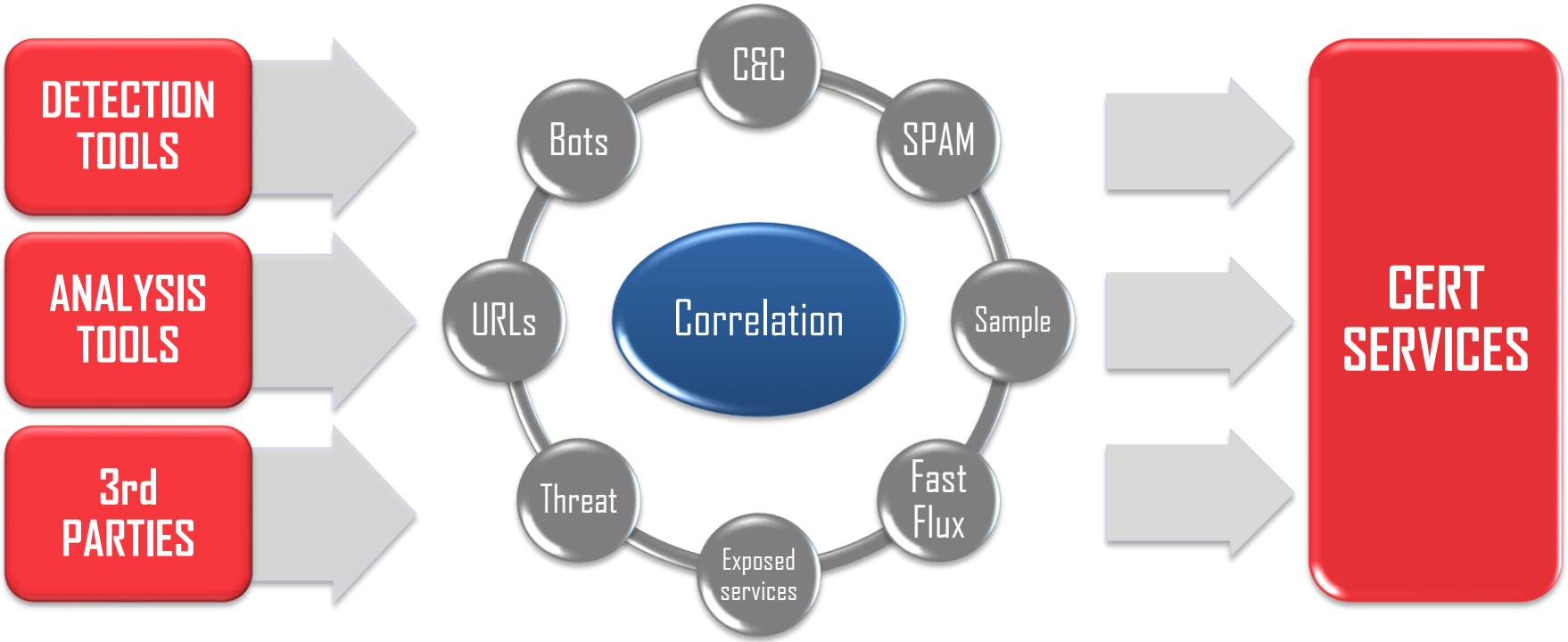
16.054	Unauthorised access
15.177	Viruses, trojans, worms, spyware
13.410	Fraud
2.905	Other
1.275	Spam
794	Denial of service
335	Network scans
26	Information theft

Incidents by detection source 2015



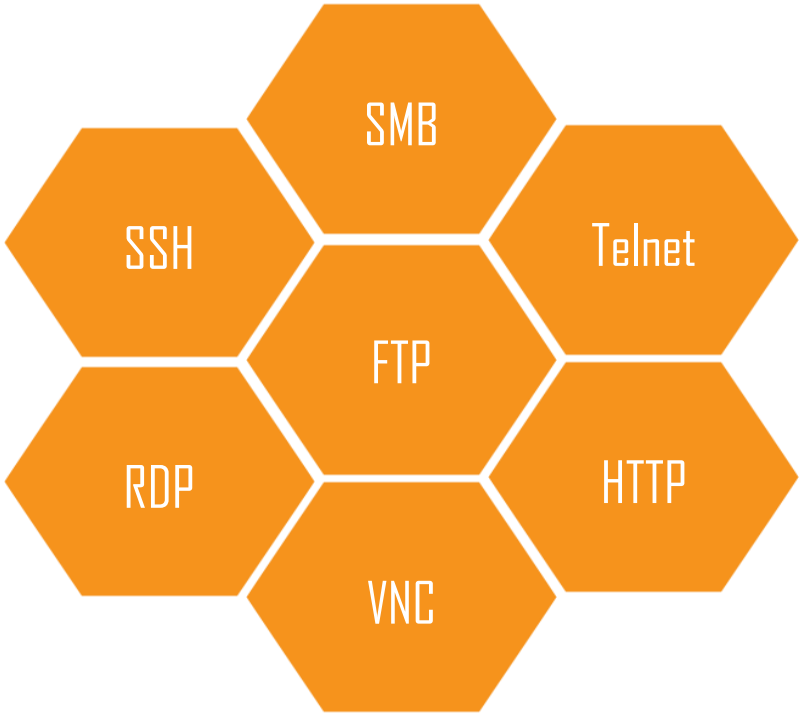
Intelligence model

Intell model

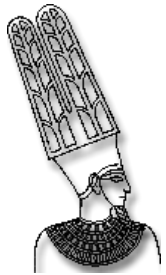


Spamtraps

Honeypots

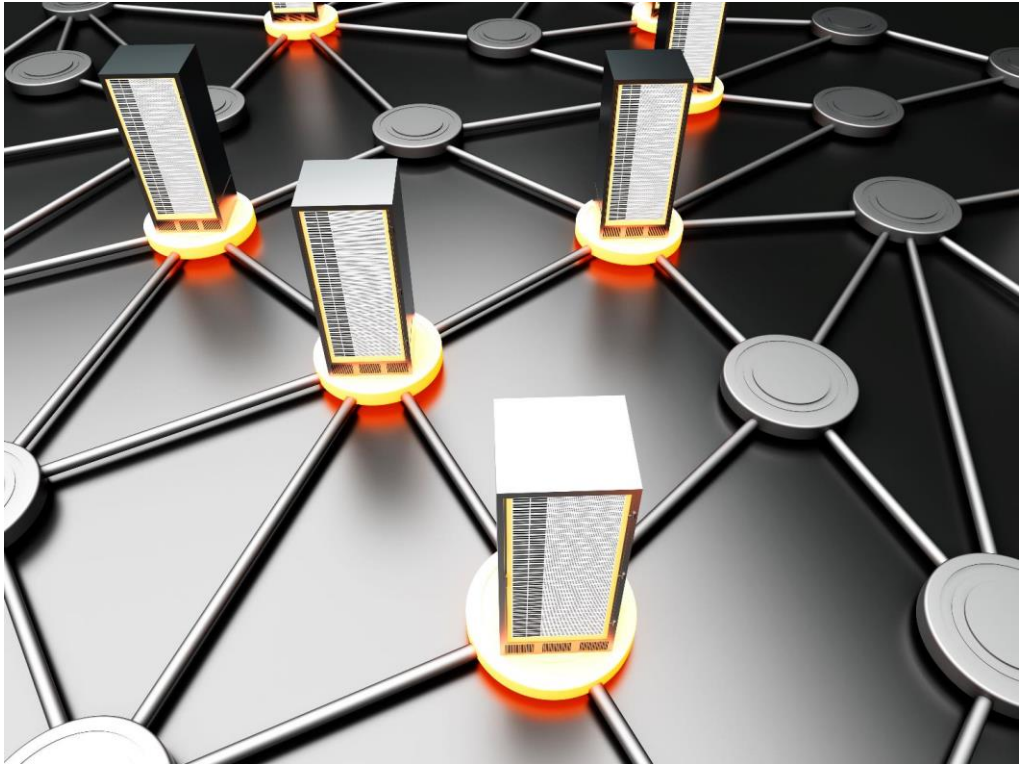


kippo
SSH Honeypot



Glastopf

Skanna



dominios es

.NET
.NAME
.COM

... hosted in Spain

VERISIGN

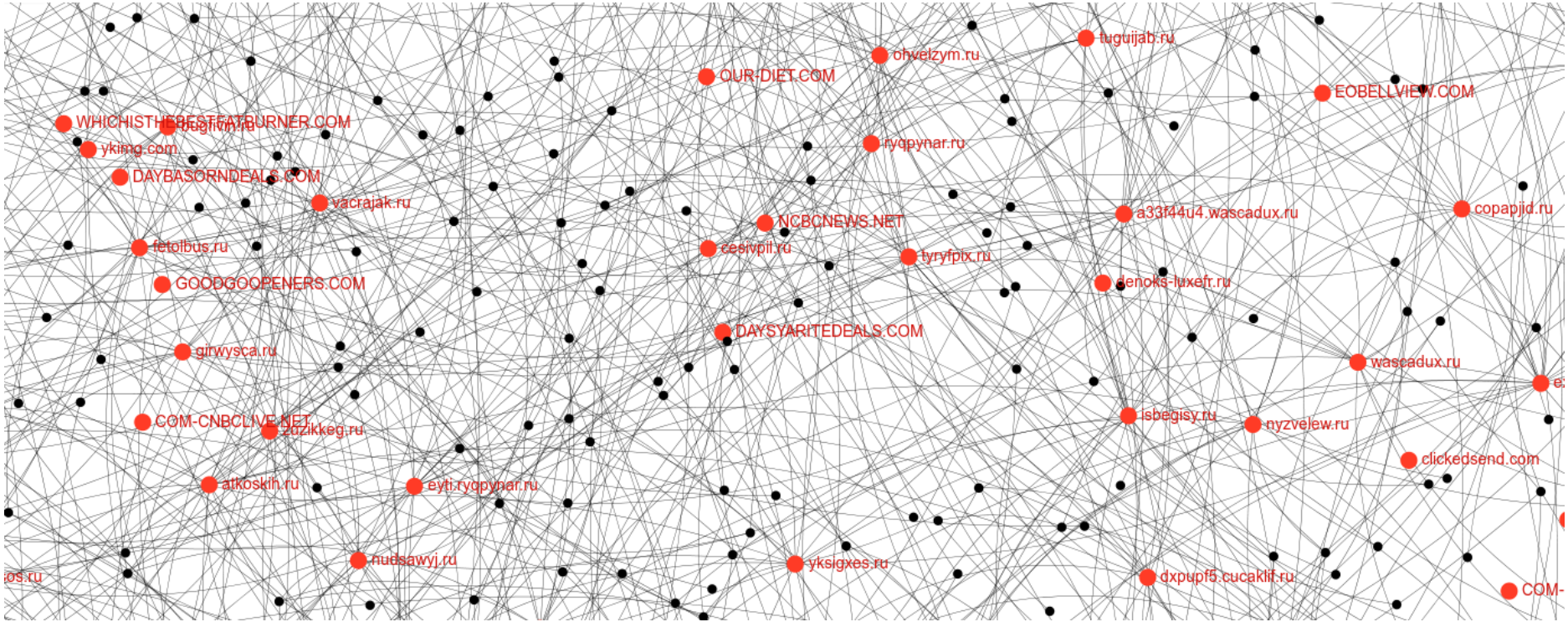
Jennings 2

virustotal

cuckoo

FireEye

Fast-flux


tuguijab.ru
ohvelzym.ru
OUR-DIET.COM
EOBELLVIEW.COM
WHICHISTHEBESTFATBURNER.COM
yking.com
ryqpynar.ru
DAYBASORNDEALS.COM
vacrajak.ru
a33f44u4.wascadux.ru
copapjid.ru
NCBCNEWS.NET
cesivpil.ru
tyryfpix.ru
fetolbus.ru
GOODGOOPENERS.COM
denoks-luxeft.ru
DAYSYARITEDEALS.COM
girwysca.ru
wascadux.ru
COM-CNBCLIVE.NET
zozikkeg.ru
sbegisy.ru
nyzvelew.ru
clickedsend.com
atkoskih.ru
eyti.ryqpynar.ru
nudsawyj.ru
yksigxes.ru
dxpupf5.cucaklif.ru

Third party information


The Challenge

Spanish approach

icaro_

Information sharing

Servicio
ANTIBOTNET

icaro_

Information Sharing with Strategic companies and National CERT/CSIRT

ICARO goals

- **Share knowledge with strategic companies**
- **Increase detection capabilities on private sector**
- **Define a neutral Spanish hub**
- **Increase automation in early warning**

ICARO goals

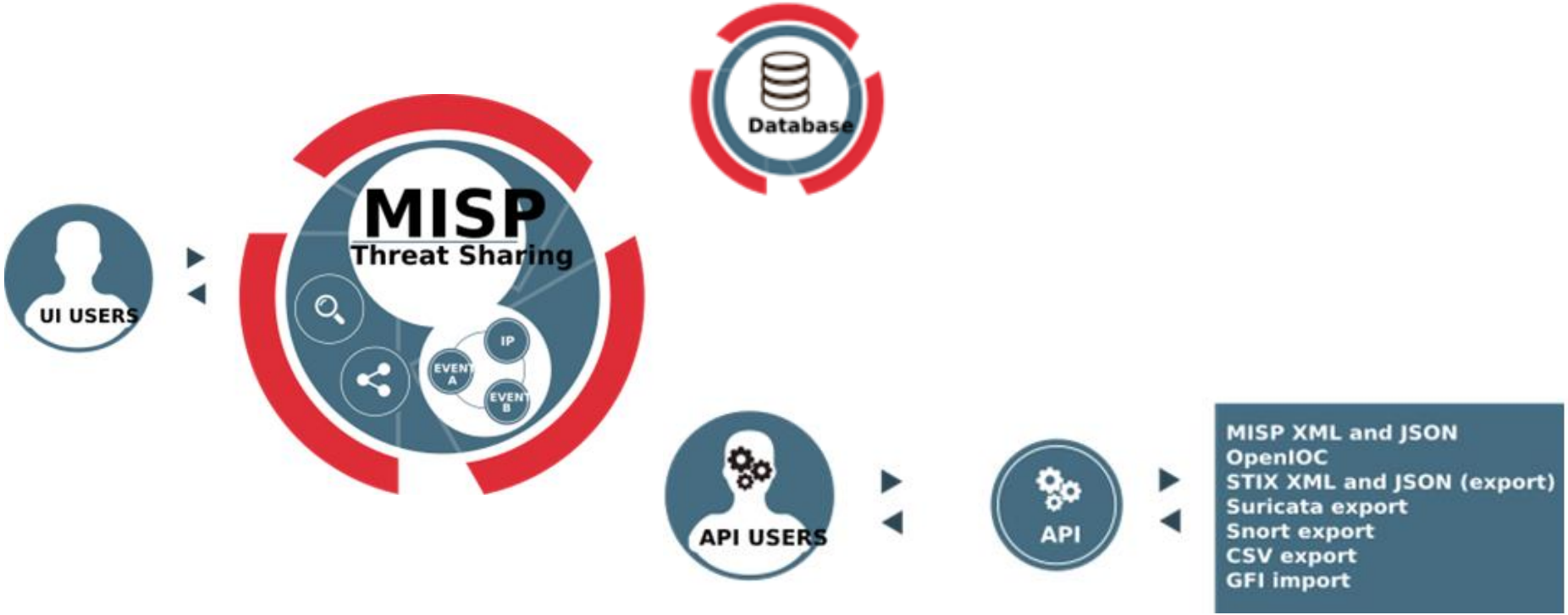
Real and active threats (no takedowns)

Useful for a sector or more

Examples:

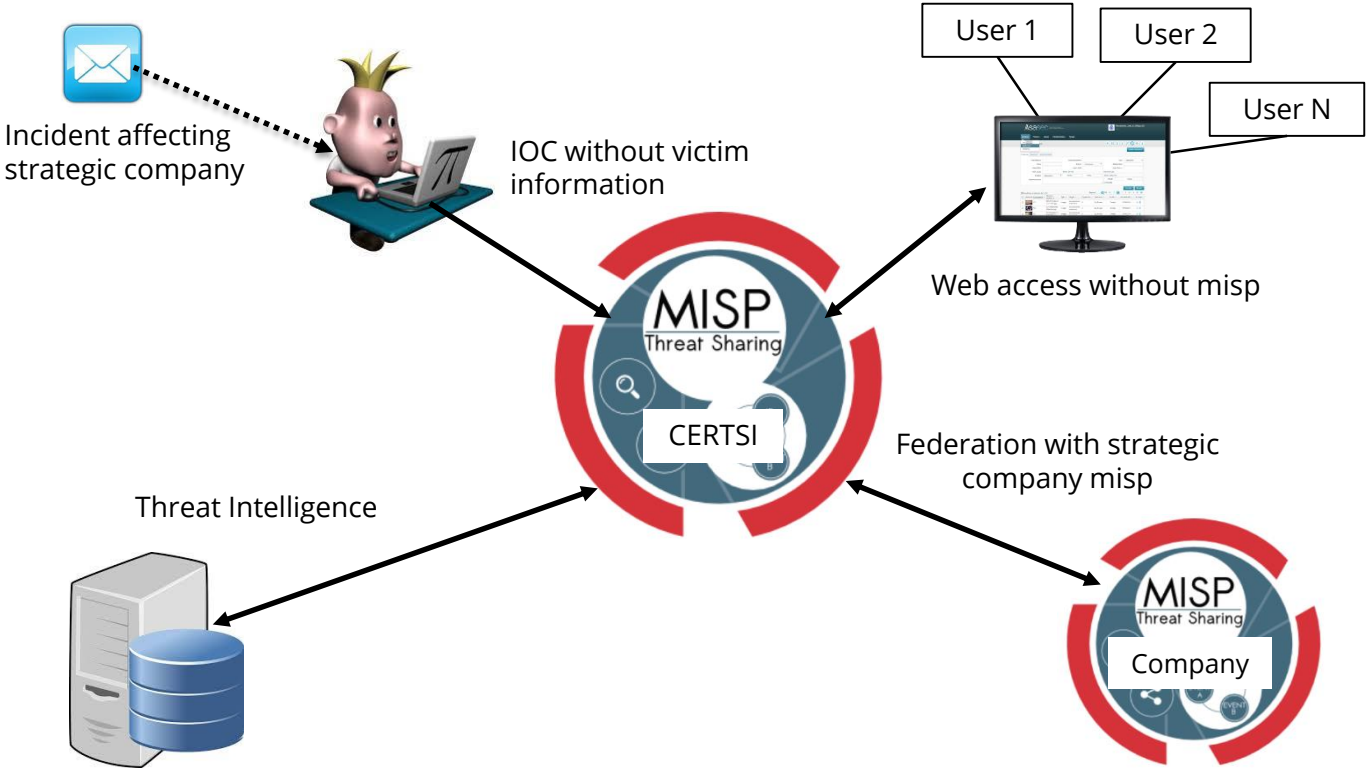
- ✓ Malware targeting Spanish companies
- ✓ Botnet/Trojan infection campaigns
- ✓ Information about DDoS extortion groups
- ✓ Ransomware campaigns
- ✓ APT

Malware Information Sharing Platform

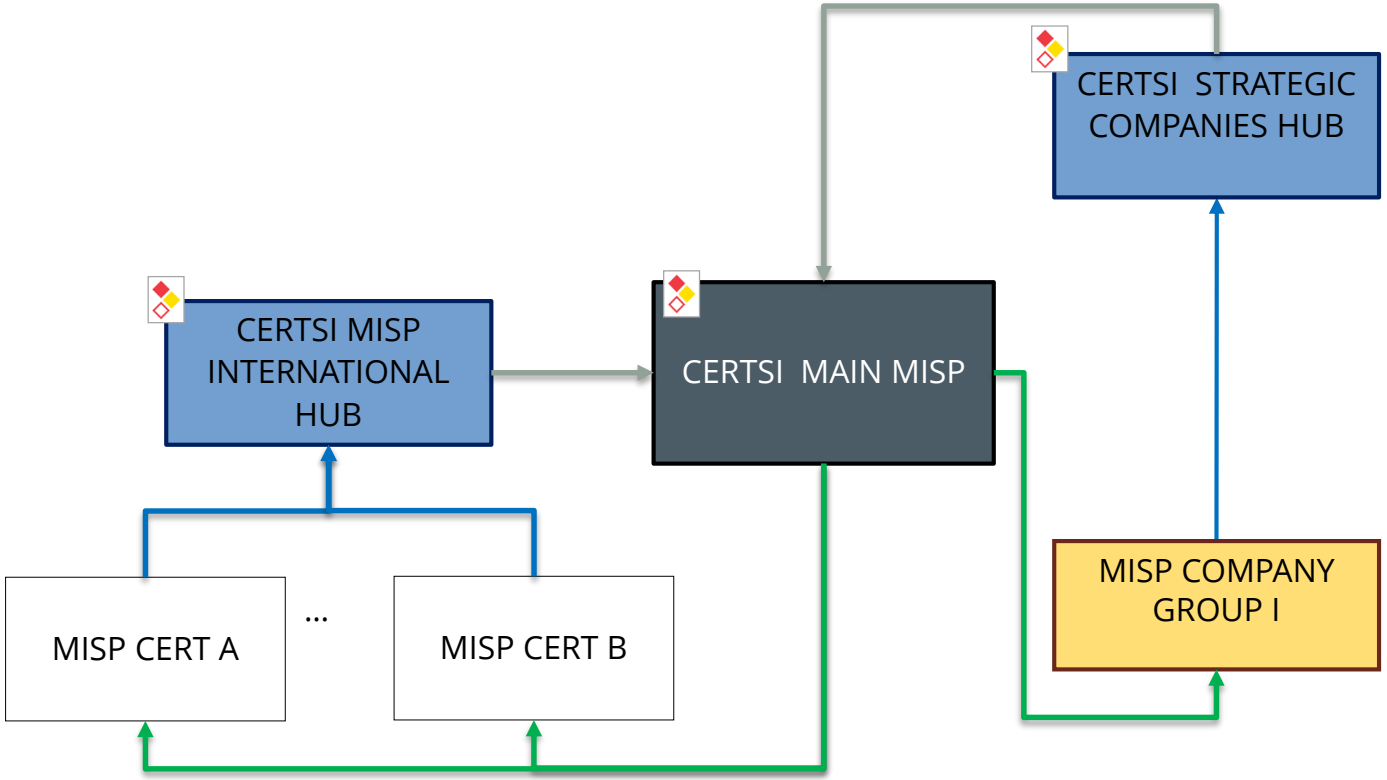


http://www.misp-project.org/

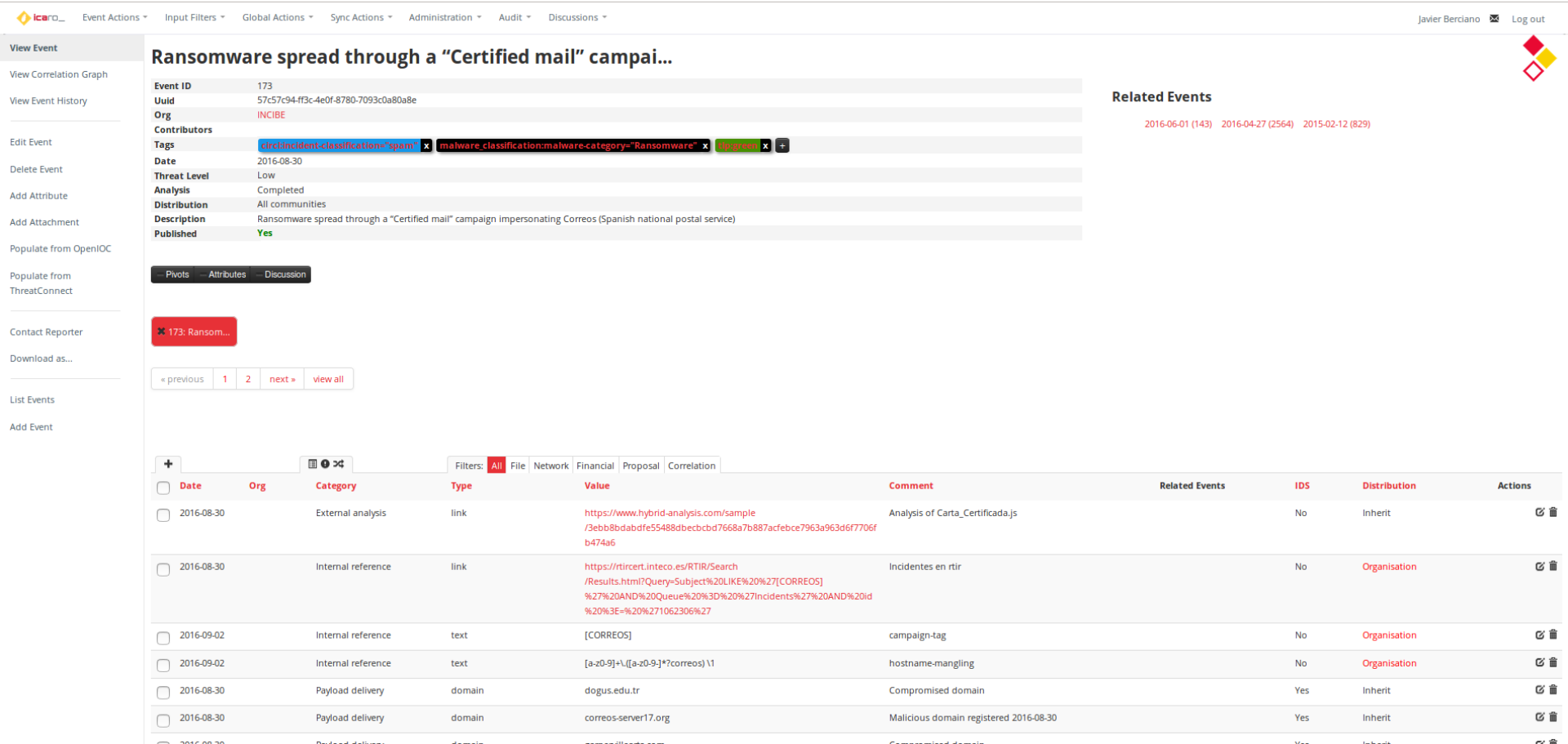
Model


Incident affecting strategic company
IOC without victim information
User 1
User 2
User N
Web access without misp
MISP
Threat Sharing
CERTSI
Federation with strategic company misp
Threat Intelligence
MISP
Threat Sharing
Company

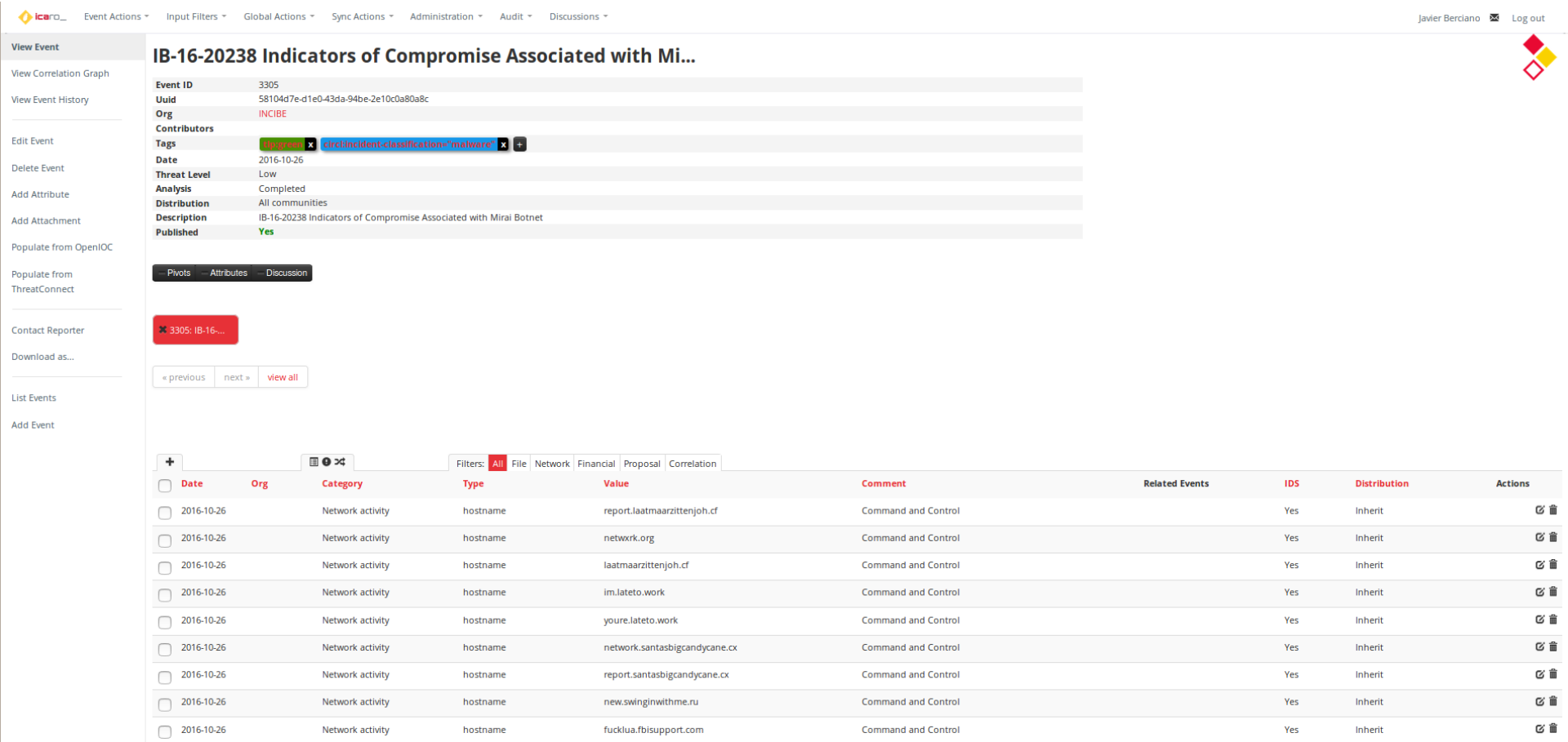
Arquitecture



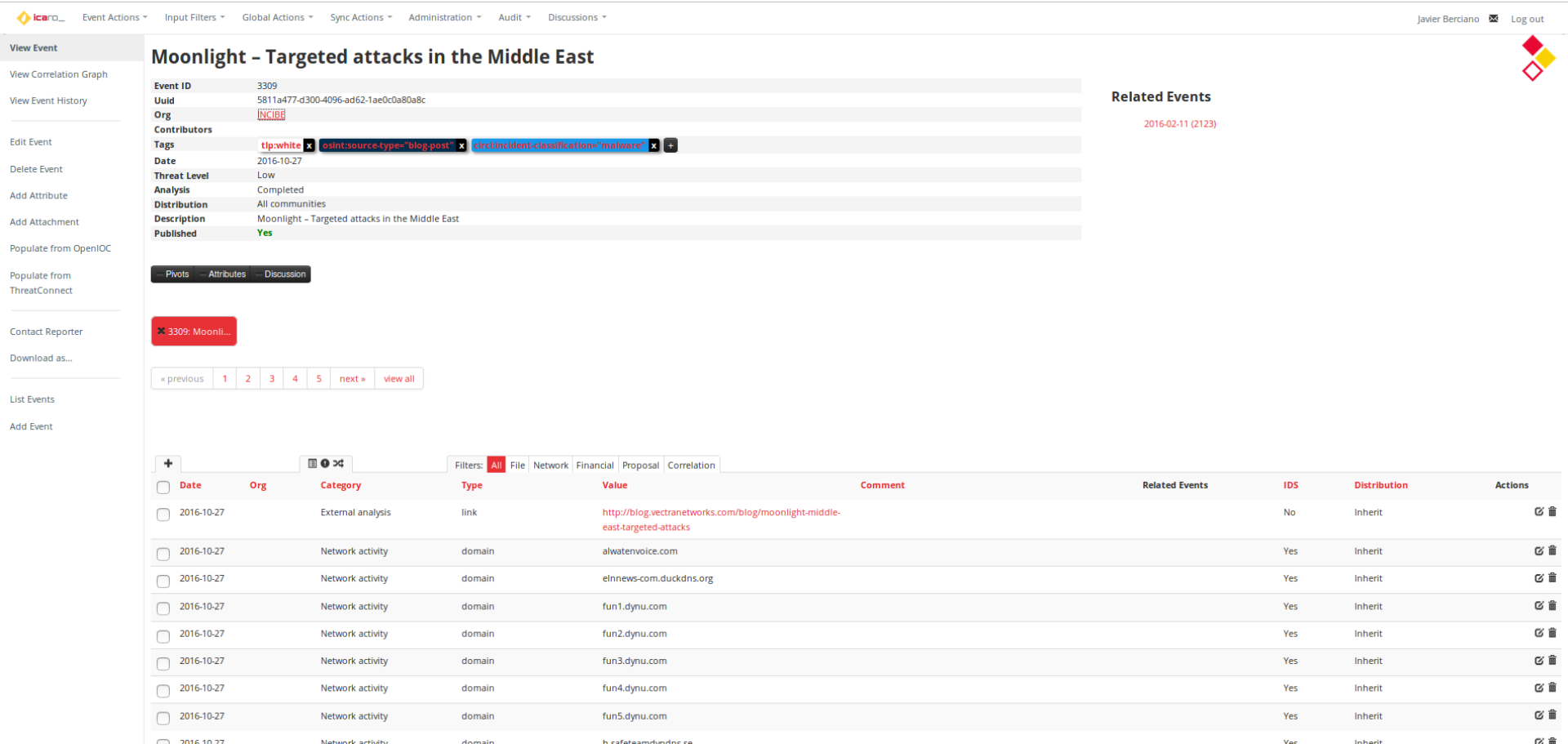
Examples


Event Actions
Input Filters
Global Actions
Sync Actions
Administration
Audit
Discussions
Javier Berciano
Log out
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from OpenIOC
Populate from ThreatConnect
Contact Reporter
Download as...
List Events
Add Event
Ransomware spread through a "Certified mail" campai...
Event ID 173
Uuid 57c57c94-ff3c-4e0f-8780-7093c0a80a8e
Org INCIBE
Contributors
Tags circl:incident-classification="spam" malware_classification:malware-category="Ransomware" tlp:green
Date 2016-08-30
Threat Level Low
Analysis Completed
Distribution All communities
Description Ransomware spread through a "Certified mail" campaign impersonating Correos (Spanish national postal service)
Published Yes
Related Events
2016-06-01 (143) 2016-04-27 (2564) 2015-02-12 (829)
Pivots Attributes Discussion
173: Ransom...
« previous 1 2 next » view all
Filters: All File Network Financial Proposal Correlation
Date Org Category Type Value Comment Related Events IDS Distribution Actions
2016-08-30 External analysis link https://www.hybrid-analysis.com/sample/3ebb8bdabdfe55488dbecbcbd7668a7b887acfebce7963a963d6f7706fb474a6 Analysis of Carta_Certificada.js No Inherit
2016-08-30 Internal reference link https://rtircert.inteco.es/RTIR/Search/Results.html?Query=Subject%20LIKE%20%27[CORREOS]%27%20AND%20Queue%20%3D%20%27Incidents%27%20AND%20Id%20%3E=%20%271062306%27 Incidentes en rtir No Organisation
2016-09-02 Internal reference text [CORREOS] campaign-tag No Organisation
2016-09-02 Internal reference text [a-z0-9]+\.([a-z0-9-]*?correos) \1 hostname-mangling No Organisation
2016-08-30 Payload delivery domain dogus.edu.tr Compromised domain Yes Inherit
2016-08-30 Payload delivery domain correos-server17.org Malicious domain registered 2016-08-30 Yes Inherit

Examples


Event Actions
Input Filters
Global Actions
Sync Actions
Administration
Audit
Discussions
Javier Berciano
Log out
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from OpenIOC
Populate from ThreatConnect
Contact Reporter
Download as...
List Events
Add Event
IB-16-20238 Indicators of Compromise Associated with Mi...
Event ID 3305
Uuid 58104d7e-d1e0-43da-94be-2e10c0a80a8c
Org INCIBE
Contributors
Tags tlp:green circl:incident-classification="malware"
Date 2016-10-26
Threat Level Low
Analysis Completed
Distribution All communities
Description IB-16-20238 Indicators of Compromise Associated with Mirai Botnet
Published Yes
Pivots
Attributes
Discussion
3305: IB-16-...
« previous
next »
view all
Filters: All File Network Financial Proposal Correlation
Date Org Category Type Value Comment Related Events IDS Distribution Actions
2016-10-26 Network activity hostname report.laatmaarzittenjoh.cf Command and Control Yes Inherit
2016-10-26 Network activity hostname netwxrk.org Command and Control Yes Inherit
2016-10-26 Network activity hostname laatmaarzittenjoh.cf Command and Control Yes Inherit
2016-10-26 Network activity hostname im.lateto.work Command and Control Yes Inherit
2016-10-26 Network activity hostname youre.lateto.work Command and Control Yes Inherit
2016-10-26 Network activity hostname network.santasbigcandycane.cx Command and Control Yes Inherit
2016-10-26 Network activity hostname report.santasbigcandycane.cx Command and Control Yes Inherit
2016-10-26 Network activity hostname new.swinginwithme.ru Command and Control Yes Inherit
2016-10-26 Network activity hostname fucklua.fbisupport.com Command and Control Yes Inherit

Examples


Event Actions
Input Filters
Global Actions
Sync Actions
Administration
Audit
Discussions
Javier Berciano
Log out
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from OpenIOC
Populate from ThreatConnect
Contact Reporter
Download as...
List Events
Add Event
Moonlight – Targeted attacks in the Middle East
Event ID 3309
Uuid 5811a477-d300-4096-ad62-1ae0c0a80a8c
Org INCIBE
Contributors
Tags tlp:white osint:source-type="blog-post" circl:incident-classification="malware"
Date 2016-10-27
Threat Level Low
Analysis Completed
Distribution All communities
Description Moonlight – Targeted attacks in the Middle East
Published Yes
Related Events
2016-02-11 (2123)
Pivots
Attributes
Discussion
3309: Moonli...
« previous
1
2
3
4
5
next »
view all
Filters: All File Network Financial Proposal Correlation
Date
Org
Category
Type
Value
Comment
Related Events
IDS
Distribution
Actions
2016-10-27 External analysis link http://blog.vectranetworks.com/blog/moonlight-middle-east-targeted-attacks No Inherit
2016-10-27 Network activity domain alwatenvoice.com Yes Inherit
2016-10-27 Network activity domain elnnews-com.duckdns.org Yes Inherit
2016-10-27 Network activity domain fun1.dynu.com Yes Inherit
2016-10-27 Network activity domain fun2.dynu.com Yes Inherit
2016-10-27 Network activity domain fun3.dynu.com Yes Inherit
2016-10-27 Network activity domain fun4.dynu.com Yes Inherit
2016-10-27 Network activity domain fun5.dynu.com Yes Inherit

Servicio

ANTIBOTNET

Information Sharing with ISP to involve SME and citizens

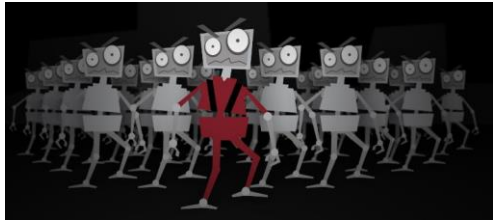
AntiBotnet service

The **objetive** of the Antibotnet Service is the mitigation of botnets from the point of view of the **disinfection** of the users' devices infected: **bots**. Also the service is way to inform and aware users about this problems.

This service is a result of the work developed day to day by INCIBE in collaboration with other national and international entities in fighting against botnets:

- An average of **5,2 million evidences of botnet connections** from Spain daily.
- An average of **59.500 unique IPs affected** daily in Spain.
- Data from close to **900 sinkholes**, which correspond approximately with **129 families** of botnets.

Spain is pioneer in this kind of initiative alongside countries such Germany, Japan or Sweden.

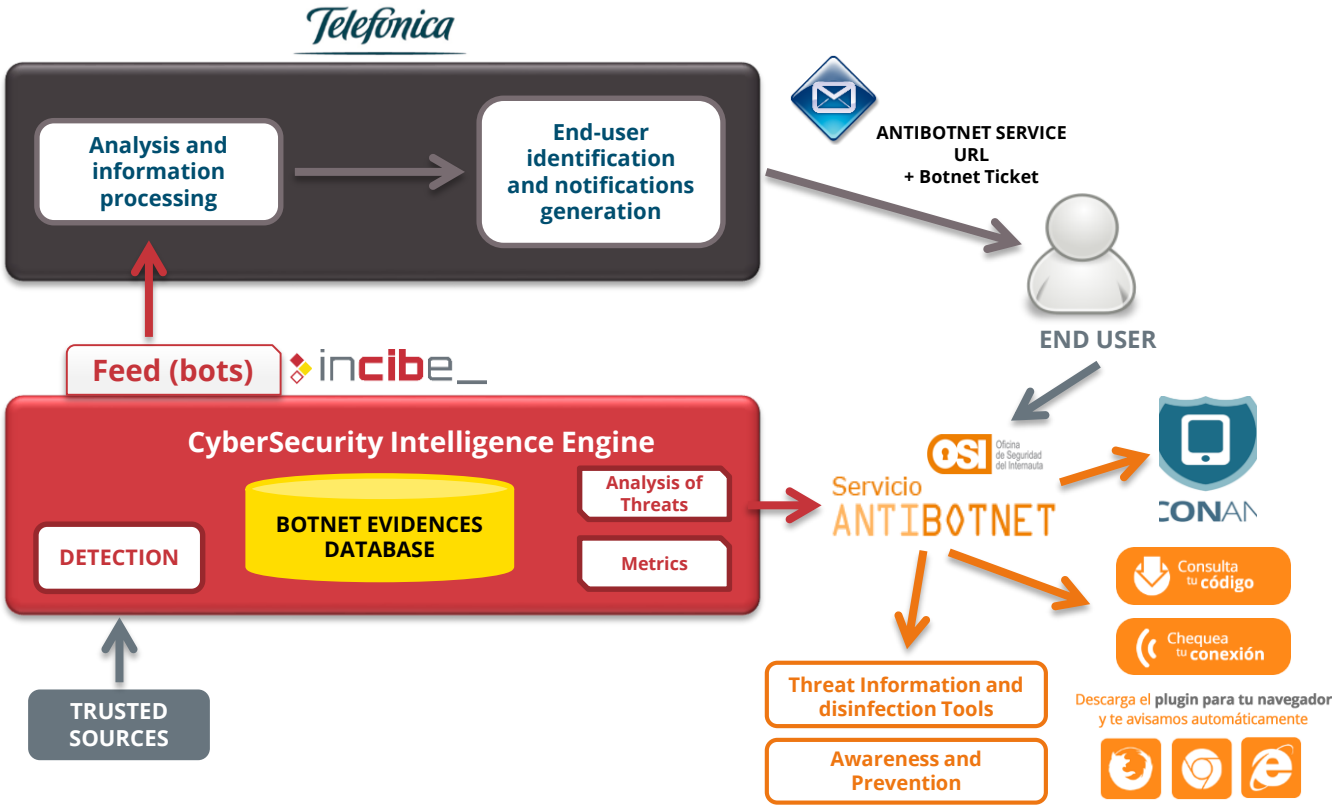


AntiBotnet service

Antibotnet Service is offered to end-users through **five different ways**:

- **Online Service:** End-users can check online if their public IP is involved in botnet activity.
- **Plugin Service:** Plugin available for Google Chrome, Firefox and Internet Explorer to check the IP periodically and automatically, in order to alert the end-user in case of a positive is detected.
- **CONAN Mobile:** Application for Android devices, which helps to check the level of security of mobile devices developed by INCIBE. This app integrates the functionality of the Antibotnet Service, giving botnet alerts in case a positive is detected on wifi networks.
- **ISP Notification:** The Spanish ISP Telefónica collaborates with us notifying end-users by email about botnet related incidents that affect their internet connection. INCIBE gives to Telefónica every day a feed containing bot evidences related to their ASNs. With this information, Telefónica can identify end-user lines affected and therefore notify.
- **API for companies:** API that allows IT personal to integrate the service in their network monitoring systems. This service is oriented to companies

AntiBotnet service



Step 1: Sign an agreement

- Clearly define the aim of the service
- Define the obligations by the ISP
  - People accessing the information
  - Avoid commercial use
  - Ensure confidentiality
  - Inform back with issues and indicators
- Duration and termination
- Policy of use
- Protection of privacy
- Set the technical terms
  - AS numbers of the ISP
  - IP address for accessing

Step 2: Access method and taxonomy

- IP restricted WebDAV
- CSV file
- Every 24 hours

FIELD	TYPE
Timestamp	yyyy-mm-dd hh:mm:ss
Source IP Address	IPv4 Address
Source port	Integer
Destination IP Address	IPv4 Address
Ticket number	Alphanumeric
Malware	String
ASN Source IP Address	Long
Destination URL	String
http referer	String
Protocol	String

Step 3: Notification end user

[redacted]
[redacted]

(e-mail#N16-0039060-916318343-AntiBotnet) Notificación de Ciber-Seguridad en colaboración con INCIBE.

Presentation

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 nuestros clientes y del resto de usuarios de Internet, y en cumplimiento con lo dispuesto en la Disposición adicional novena de la Ley
34/2002, de 11 de julio[1], nos dirigimos a usted para informarle que hemos recibido un aviso de seguridad por parte del Centro de Respuesta a Incidentes de Seguridad e Industria (CERT-SI)[2]; a través del cual se nos comunica que alguno de los equipos conectados a su conexión a Internet asociada a la línea 916[redacted] podría estar afectado por un programa malicioso relacionado con redes de ordenadores zombie o botnets.

Según este aviso, con fecha 2016-01-31 00:03:02 y con la dirección IP 83.50.[redacted], que en ese momento estaba utilizando su conexión a Internet, algún equipo o dispositivo habría tenido comunicación con la red de ordenadores zombie Mevade, y por lo tanto se pueden estar realizando actividades maliciosas sin su conocimiento, que podrían afectarle a usted mismo e incluso a terceros.

Technical data
Disinfection procedure

==========
Procedimiento de desinfección
==========

Para obtener más información sobre esta amenaza y ayudarle en el proceso de desinfección de sus dispositivos, puede acceder a la web de la Oficina de Seguridad del Internauta (OSI) perteneciente al Instituto Nacional de Ciberseguridad (INCIBE)[3].

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

e introducir el siguiente código en la casilla que figura "Consulta tu código": CFY[redacted]

==========
Información sobre la iniciativa AntiBotnet
==========

Initiative information

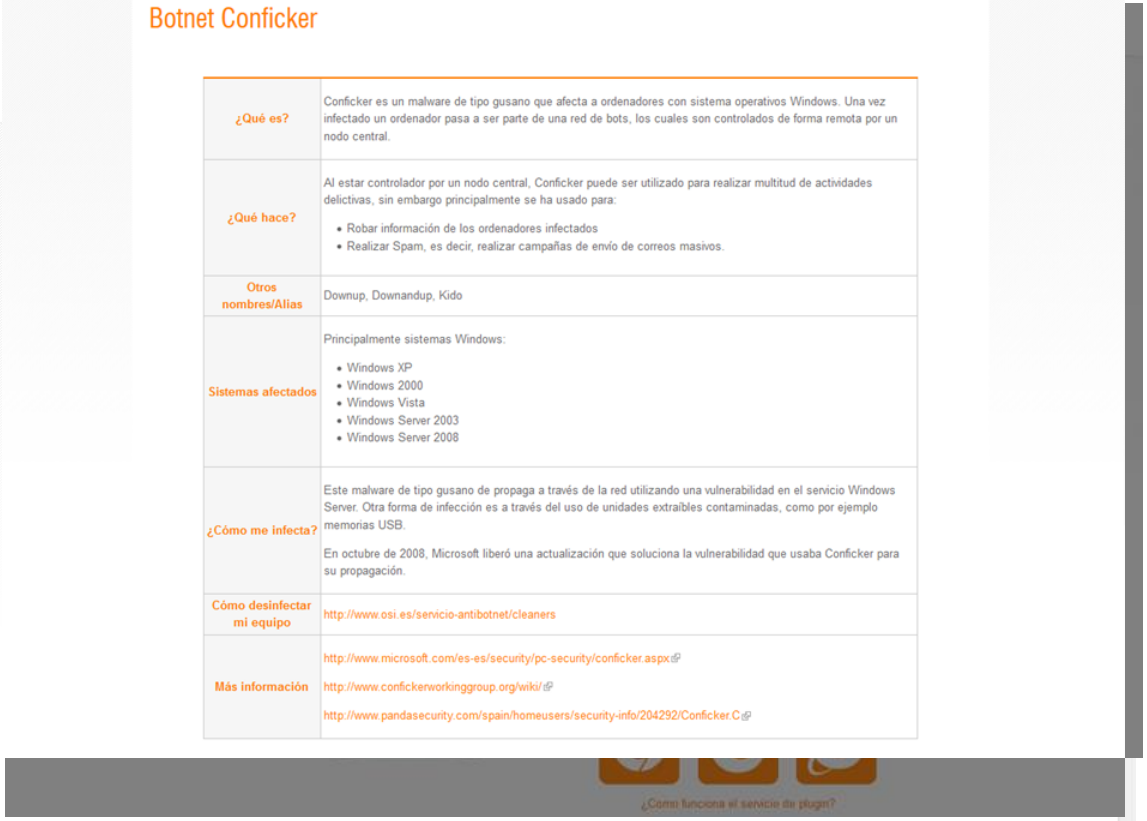
La iniciativa AntiBotnet es un proyecto de colaboración público-privada puesto en marcha por los principales prestadores de servicios de la sociedad de la información, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) e INCIBE.

Su finalidad es proporcionar la información y herramientas necesarias para la desinfección de dispositivos afectados por incidentes de Ciberseguridad relacionados con redes de ordenadores zombie o botnets, contribuyendo así a un Internet más confiable y seguro para todos.

Toda la información de los Servicios AntiBotnet en http://www.osi.es/es/servicio-antibotnet

Para ayuda adicional o dudas relativas al servicio puede contactar con el servicio de soporte de la OSI a través de su página web:
https://www.osi.es/contacto.

Step 4: Malware information



Botnet Conficker

¿Qué es?	Conficker es un malware de tipo gusano que afecta a ordenadores con sistema operativos Windows. Una vez infectado un ordenador pasa a ser parte de una red de bots, los cuales son controlados de forma remota por un nodo central.
¿Qué hace?	Al estar controlador por un nodo central, Conficker puede ser utilizado para realizar multitud de actividades delictivas, sin embargo principalmente se ha usado para: • Robar información de los ordenadores infectados • Realizar Spam, es decir, realizar campañas de envío de correos masivos.
Otros nombres/Alias	Downup, Downandup, Kido
Sistemas afectados	Principalmente sistemas Windows: • Windows XP • Windows 2000 • Windows Vista • Windows Server 2003 • Windows Server 2008
¿Cómo me infecta?	Este malware de tipo gusano de propaga a través de la red utilizando una vulnerabilidad en el servicio Windows Server. Otra forma de infección es a través del uso de unidades extraíbles contaminadas, como por ejemplo memorias USB. En octubre de 2008, Microsoft liberó una actualización que soluciona la vulnerabilidad que usaba Conficker para su propagación.
Cómo desinfectar mi equipo	http://www.osi.es/servicio-antibotnet/cleaners
Más información	http://www.microsoft.com/es-es/security/pc-security/conficker.aspx http://www.confickerworkinggroup.org/wiki/ http://www.pandasecurity.com/spain/homeusers/security-info/204292/Conficker.C

¿Cómo funciona el servicio de plugin?

Step 5: Disinfection

Servicio Antibotnet: Cleaners

Si has llegado aquí 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 el dispositivo afectado es alguno de los que están o estaban conectados a Internet en tu red en el momento de la detección del incidente.

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.

Para maximizar las posibilidades de desinfección, recomendamos utilizar dos cleaners.

Escoge uno de la zona roja, y una vez hayas terminado, desinstálalo y utiliza otro de la zona azul:

Kaspersky Virus Removal Tool	Sophos Virus Removal Tool	Panda Cloud Cleaner	Norton Power Eraser
KASPERSKY	SOPHOS		
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.

Cómo desinfectar mi equipo	http://www.osi.es/servicio-antibotnet/cleaners
Más información	http://www.microsoft.com/es-es/security/pc-security/conficker.aspx http://www.confickerworkinggroup.org/wiki/ http://www.pandasecurity.com/spain/homeusers/security-info/204292/Conficker.C

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, ofreciendote 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 operadores de servicios de Internet que colaboran con nosotros** notificándote de los incidentes de seguridad que afectan a tu conexión. Si has recibido un mensaje de tu operador, consulta el código que te ha proporcionado y obtén la información directamente.
- La segunda es **mediante el uso de nuestras herramientas online**.

Si tu operador de servicios de Internet te ha enviado un **código de incidente**

Consulta tu **código**

¿Cómo funciona el servicio de notificación de códigos?

(*) Actualmente este servicio se encuentra en fase piloto y se está llevando a cabo con la colaboración de:

Telefónica

Usa el **servicio online** y obtén respuesta al instante

Chequea tu **conexión**

¿Cómo funciona el servicio de chequeo?

ó

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

¿Como funciona el servicio de plugin?

Servicio AntiBotnet de la OSI

Servicio AntiBotnet

¡Cuidado!

¡Alguno de los dispositivos de tu red puede estar infectado! Hemos identificado incidentes de seguridad relacionados con botnets asociados a tu conexión a Internet actual, dirección IP **193.153.83.8** .

Las amenazas o problemas identificados son:

⚠ Conficker

Información sobre esta amenaza

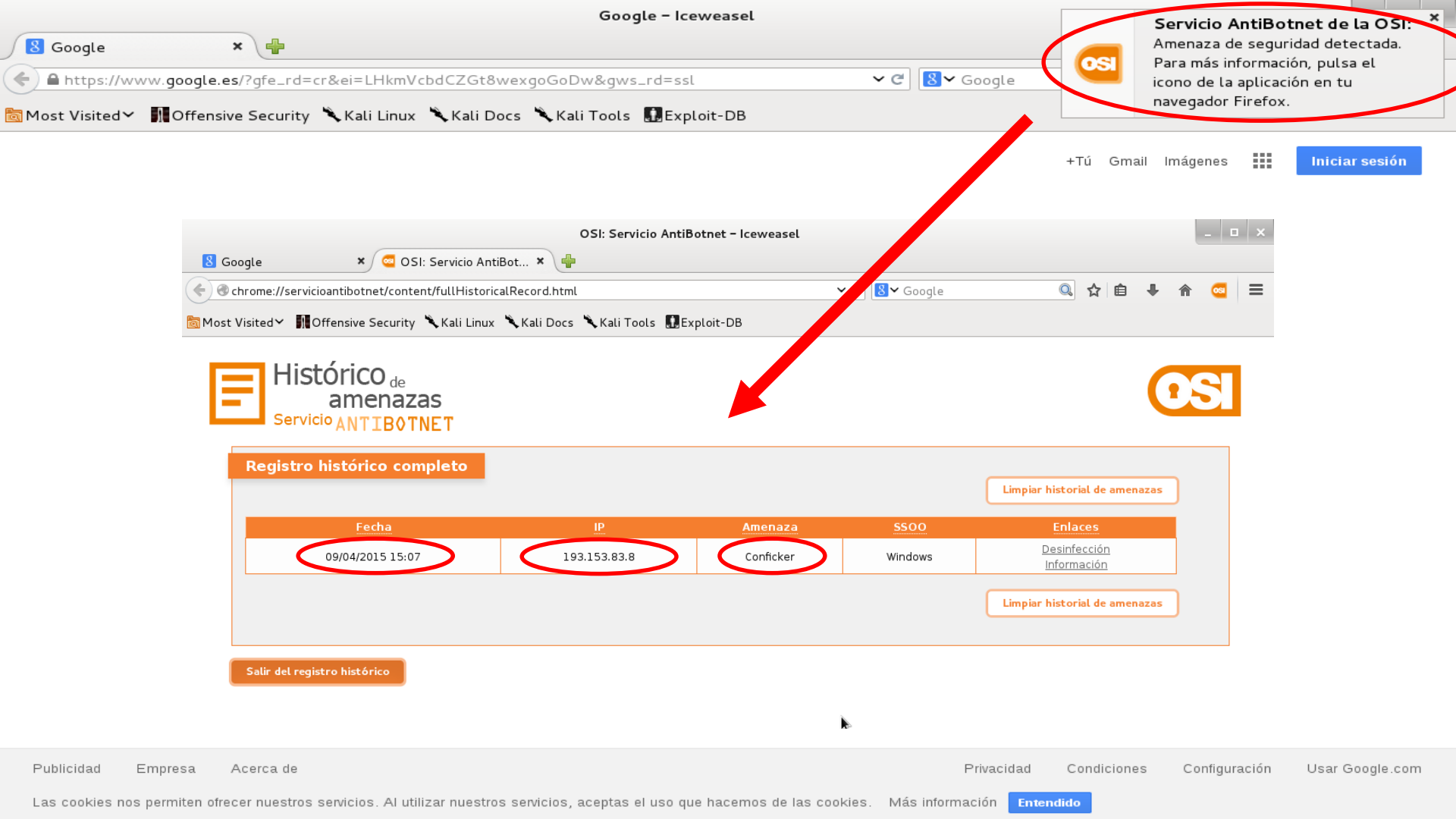
Afecta a los sistemas operativos: Windows

Información de ayuda para la desinfección

Te recomendamos que ejecutes periódicamente este servicio mediante la instalación de nuestro plugin de chequeo.

Instálalo en tu navegador y te avisaremos de forma automática si tu dirección IP pública aparece en nuestra base de datos de incidentes de botnets.

Por favor, danos tu opinión sobre este servicio. ¡Sólo te llevará 1 minuto!


Google – Iceweasel
Google
https://www.google.es/?gfe_rd=cr&ei=LHkmVcbdCZGt8wexgoGoDw&gws_rd=ssl
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Servicio AntiBotnet de la OSI:
Amenaza de seguridad detectada.
Para más información, pulsa el icono de la aplicación en tu navegador Firefox.
+Tú
Gmail
Imágenes
Iniciar sesión
OSI: Servicio AntiBotnet – Iceweasel
OSI: Servicio AntiBot...
chrome://servicioantibotnet/content/fullHistoricalRecord.html
Histórico de amenazas
Servicio ANTIBOTNET
Registro histórico completo
Limpiar historial de amenazas
Fecha
IP
Amenaza
SSOO
Enlaces
09/04/2015 15:07
193.153.83.8
Conficker
Windows
Desinfección
Información
Limpiar historial de amenazas
Salir del registro histórico
Publicidad
Empresa
Acerca de
Privacidad
Condiciones
Configuración
Usar Google.com
Las cookies nos permiten ofrecer nuestros servicios. Al utilizar nuestros servicios, aceptas el uso que hacemos de las cookies.
Más información
Entendido

Statistics

- Since the beginning of the Antibotnet Service, in June 2014, the service has received more than **255.000 visits**.
- Since the beginning of the collaboration with Telefónica, in November 2014, INCIBE has notified to Telefónica **17.286.277** unique IPs as bot evidences.
- Telefónica has sent **278.895 notifications** to **22.590 different end-users**.
- Each month **765 new customers** on average are notified by Telefónica.
- More than **19.600 tickets** have been consulted on our website.
- More than **24.400 downloads** of the plugins.
- After 5 weeks since the last notification, evidences have stopped to appear in the **45,73%** of notified end-users, whom could be determined to have been disinfected.

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

certsi_
SECURITY AND INDUSTRY CERT

Thank you!

Javier Berciano
javier.berciano@incibe.es