Telefónica

ACDC
the Advanced Cyber Defence Centre

Lucha contra las Botnets

Telefónica I+D

12.11.2013

¿Qué es una botnet?

Microsoft

El término *bot* es el diminutivo de robot. Los delincuentes distribuyen software malintencionado (también conocido como malware) que puede convertir su equipo en un bot (también conocido como zombie).

Los delincuentes suelen usar bots para infectar una gran cantidad de equipos. Estos equipos crean una red, también conocida como *botnet*.

Los delincuentes usan botnets para enviar mensajes de correo electrónico no deseados, propagar virus, atacar equipos y servidores y cometer otros tipos de delitos y fraudes.

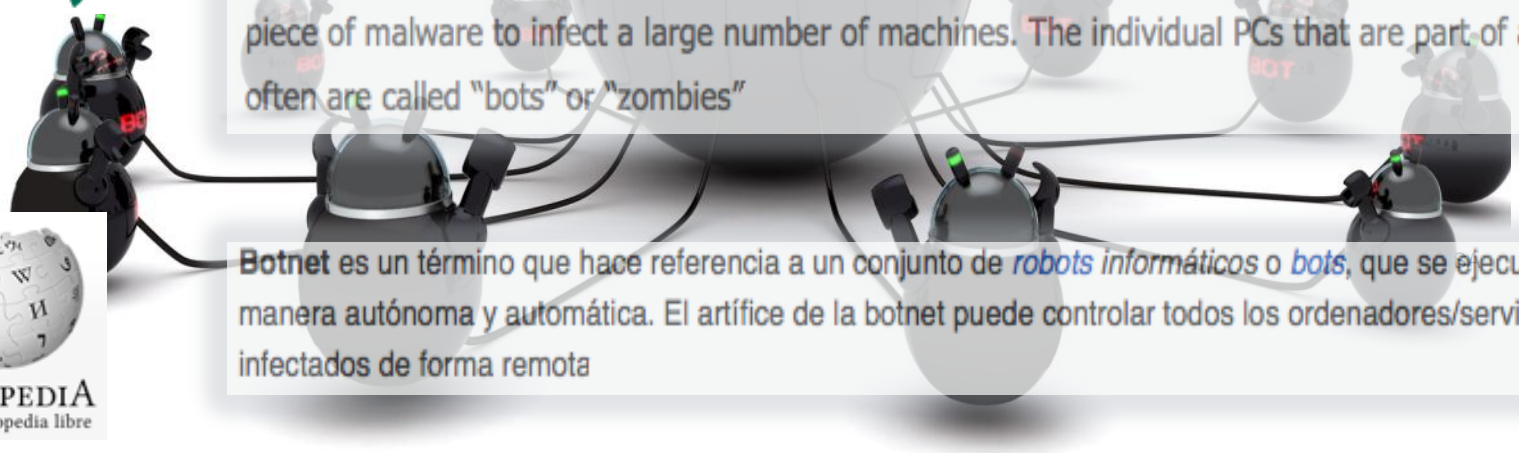
INTECO

Instituto Nacional de Tecnologías de la Comunicación

Estas redes son conjuntos de ordenadores que han sido infectados con un tipo de software malicioso, con funcionalidad de puerta trasera (*backdoor*), que permite al atacante controlar dichas maquinas sin tener acceso físico a ellas y sin el conocimiento del propietario.

KASPERSKY

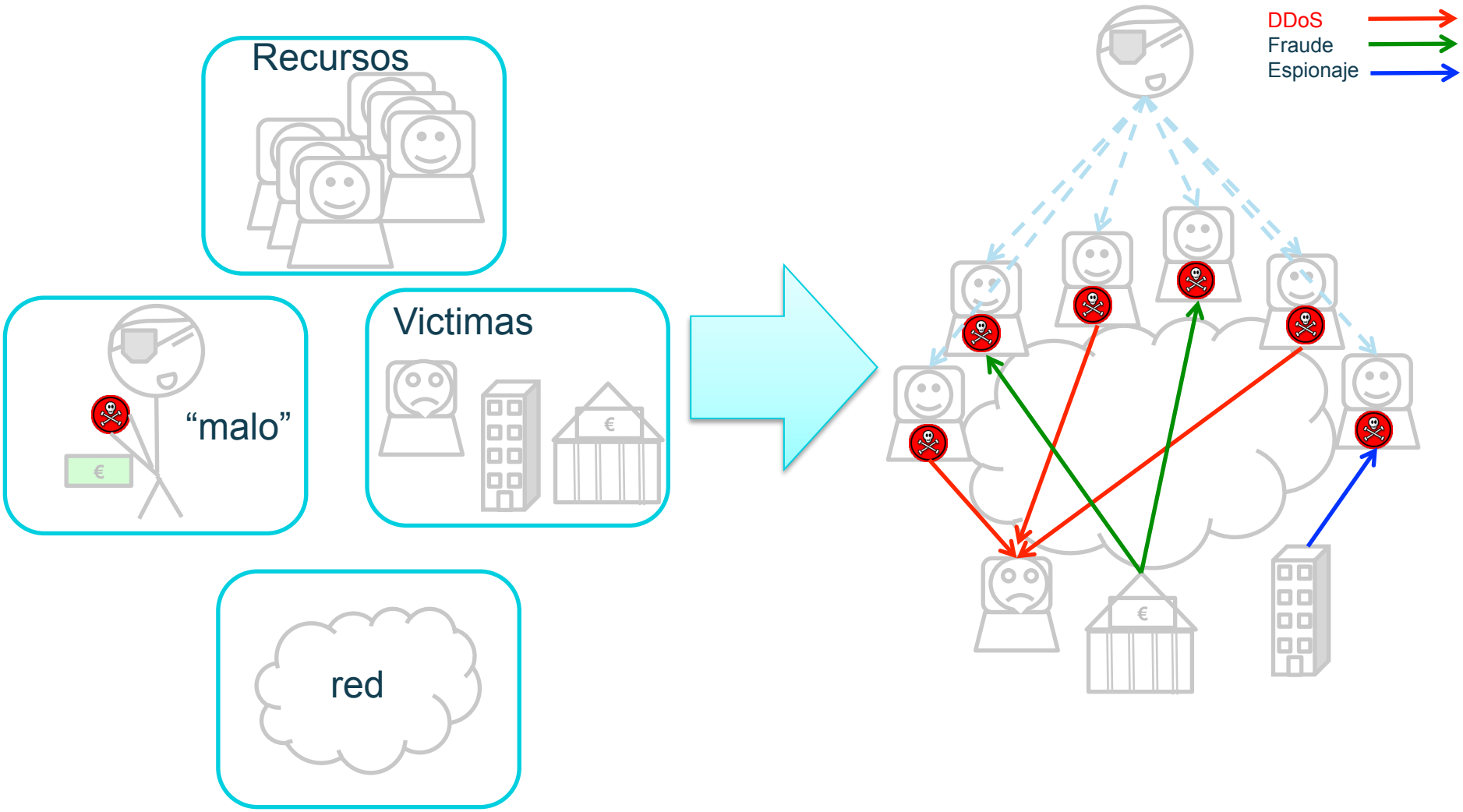
Botnet is the generic name given to any collection of compromised PCs controlled by an attacker remotely. Botnets generally are created by a specific attacker or small group of attackers using one piece of malware to infect a large number of machines. The individual PCs that are part of a botnet often are called "bots" or "zombies"



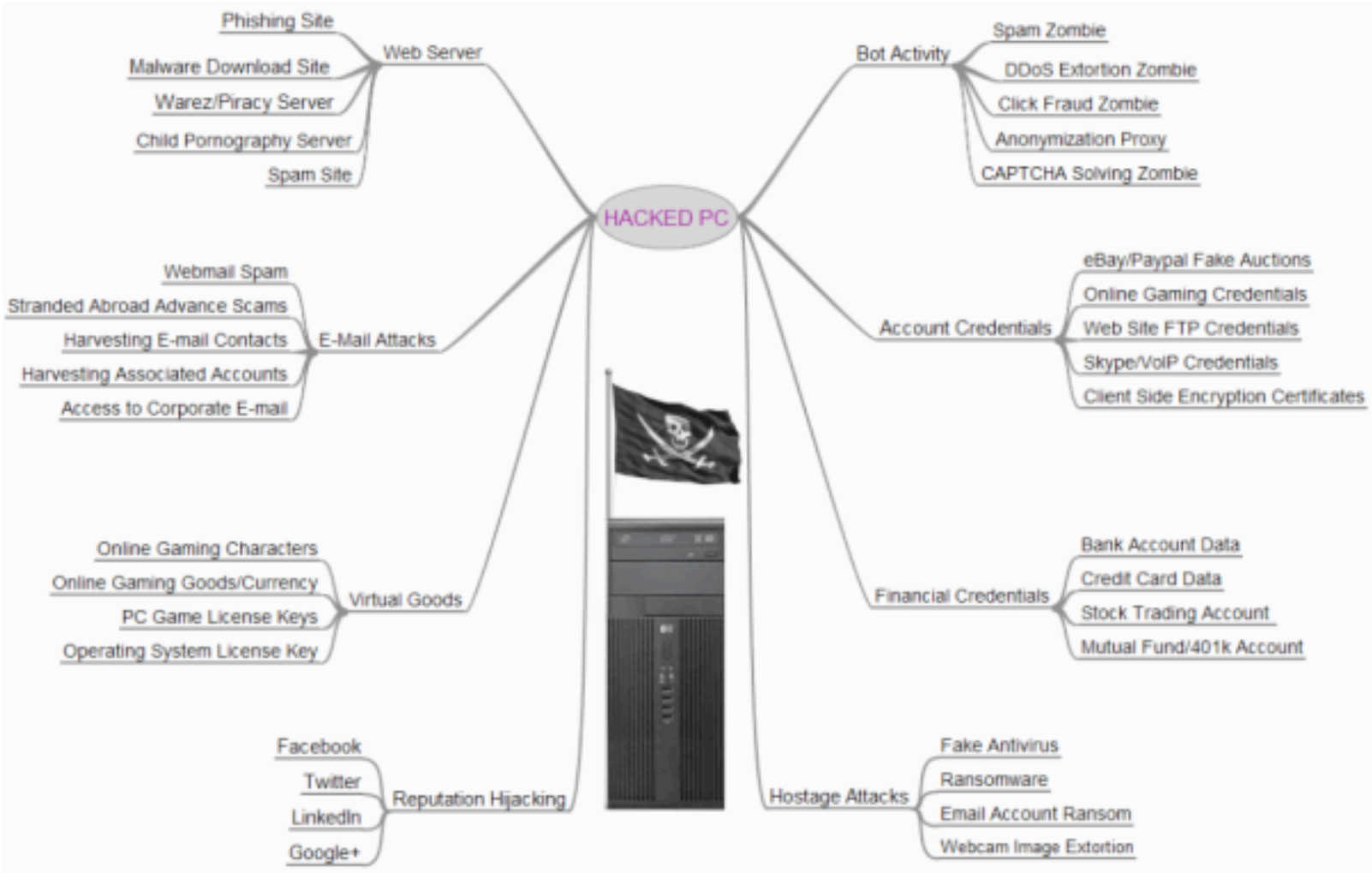
WIKIPEDIA
La enciclopedia libre

Botnet es un término que hace referencia a un conjunto de *robots informáticos* o *bots*, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota

¿Quienes son los actores?



¿Para que quiero una Botnet?

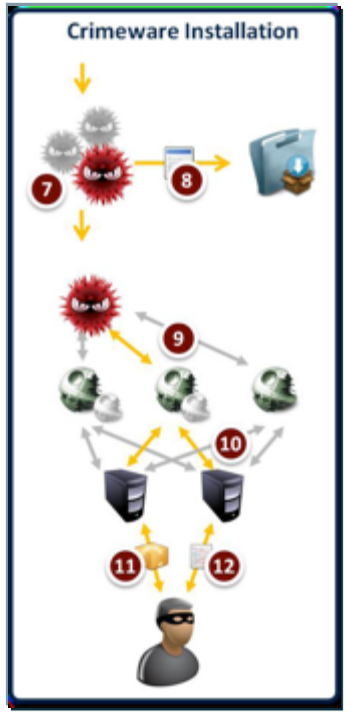


http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

¿ Como funcionan las Botnets ?

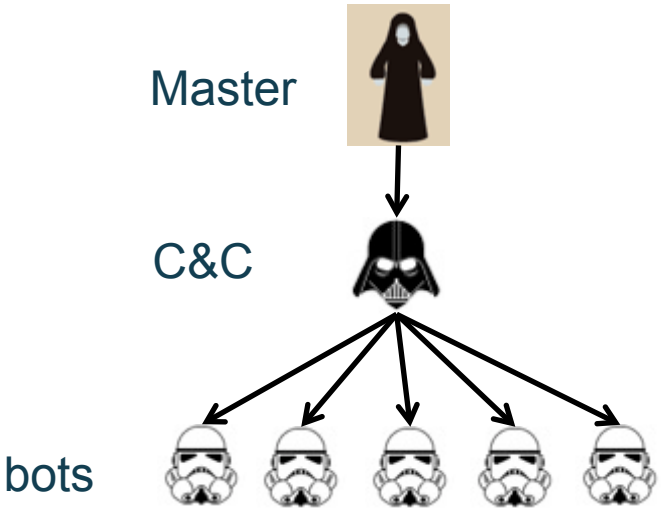
① Infección y descarga de binario camuflado a través de exploit o ingeniería social.
② Binario se desempaqueta e instala
③ Eliminación de configuraciones de Seguridad, para supervivencia
④ Actualización conf, y envío datos de ubicación de componentes a descargar
⑤ Descarga de últimos componentes y el software real de la Botnet camuflado
⑥ Extracción e instalación del binario final de la botnet

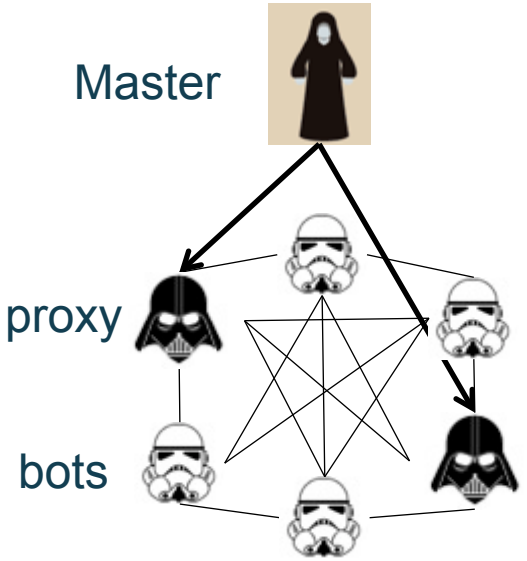
⑦ Limpieza de binarios antiguos y rastros de infección
⑧ Envío de información robada e intento de comunicación con C&C
⑨ Se dispone de una solución de FrontEnd y balanceo para la comunicación
⑩ Comúnmente se usan proxies intermedios para proteger el controlador
11 Actualización periódica de los agentes binarios, para evitar la detección de las casas de antivirus
12 Actualización periódica de las configuraciones y el funcionamiento de los bots.



Referencia: Behind Today's Crimeware Installation Lifecycle. Damballa

Tipos de Botnets





- Arquitectura Jerárquica:
  - Basadas en protocolos clásicos:
    - IRC, HTTP/S
  - ó innovadores:
    - Redes sociales (twitter,..)
    - Aplicaciones Web (Pastebin,..)
    - Esteganografía (flickr,…)
  - Técnicas de supervivencia:
    - FastFlux
    - DGA

- Arquitectura P2P:
  - Basadas en protocolos P2P:
    - Kadmelia, Overnet, bitTorrent,…
  - IPs controladores se distribuyen en la red
  - Backup basado en Jerarquía.

Vale, ¿Me tengo que preocupar?

Mi actitud	No me interesa, gracias	Estoy preocupado. ¿qué puedo hacer?
1 	• Te pueden robar dinero y tiempo • Te pueden extorsionar • *No te puede pasar nada*	• Mantén tus equipos actualizados • *Instala un Antivirus* • *Aprende*
2 	• …….	• Tengo que inventar mejores maneras de que no detecten mi Botnet
3 	• Te van a robar • Te vas a quedar sin negocio • Te van a extorsionar • Lo va a saber todo el mundo	• Invertir en Servicios de Seguridad • Prepararme para recibir ataques
4 	• Te vas a costar dinero • Lo va a saber todo el mundo	• Cuantas botnets tengo en mi red (porque tienes seguro) • *Invertir en erradicarlas*

¿No estas convencido?

- Conficker.
  - Desde 2008, y en activo.
  - Cuantas reclamaciones de clientes a su Centro de soporte podrían evitarse?

Conficker-ES

Position	ASN	Country	AS Name AS	Description	Routed Space	Unique A+B IPs	A+B Chart	Unique C IPs	C Chart	Unique Aggregate IPs	Aggregate Chart
12	3352	ES	TELEFONICA-DATA	ESPANA TELEFONICA DE ESPANA	9,935,414	20,360 (0.2%)		0 (0%)		20,360 (0.2%)	
55	6739	ES	ONO	AS Cableuropa - ONO	3,566,072	4,040 (0.11%)		0 (0%)		4,040 (0.11%)	
60	12715	ES	JAZZNET	Jazz Telecom S.A.	1,934,266	3,690 (0.19%)		0 (0%)		3,690 (0.19%)	
78	12479	ES	UNI2	AS France Telecom Espana SA	5,331,656	2,885 (0.05%)		0 (0%)		2,885 (0.05%)	
97	12357	ES	COMUNITEL	VODAFONE ESPANA S.A.U.	1,769,960	2,312 (0.13%)		0 (0%)		2,312 (0.13%)	
226	12334	ES	R	Cable y Telecomunicaciones Galicia, S.A.	499,648	770 (0.15%)		0 (0%)		770 (0.15%)	
255	12430	ES	VODAFONE_ES	VODAFONE ESPANA S.A.U.	604,138	677 (0.11%)		0 (0%)		677 (0.11%)	
326	766	ES	REDIRIS	Entidad Publica Empresarial Red.es	1,584,568	525 (0.03%)		0 (0%)		525 (0.03%)	
392	12338	ES	EUSKALTEL	Euskaltel S.A.	483,306	438 (0.09%)		0 (0%)		438 (0.09%)	
427	29119	ES	SERVIHOSTING	AS ServiHosting Networks S.L.	417,936	388 (0.09%)		0 (0%)		388 (0.09%)	

http://www.shadowserver.org/wiki/pmwiki.php/Infections/Conficker-ES

- DNSChanger.
  - Troyano con impacto en los ISP:
    - Existió un apoyo concreto de los CERT para la identificación de Usuarios infectados.
    - Los ISP tuvieron que hacer frente ($$$) al problema de avalancha de reclamaciones si desaparecían los DNS gestionados por ISC.org

Vale, ¿Me tengo que preocupar?

Mi actitud	No me interesa, gracias	Estoy preocupado. ¿qué puedo hacer?
1 	• Te pueden robar dinero y tiempo • Te pueden extorsionar • *No te puede pasar nada*	• Mantén tus equipos actualizados • *Instala un Antivirus* • *Aprende*
2 	• …….	• Tengo que inventar mejores maneras de que no detecten mi Botnet
3 	• Te van a robar • Te vas a quedar sin negocio • Te van a extorsionar • Lo va a saber todo el mundo	• Invertir en Servicios de Seguridad • Prepararme para recibir ataques
4 	• Te vas a costar dinero • Te van a extorsionar • Lo va a saber todo el mundo	• Cuantas botnets tengo en mi red (porque tienes seguro) • Invertir en erradicarlas

¿Y cómo se pueden detectar?

Pasivas: recogida y observación

- Análisis de trafico DNS
- Análisis de registros de flujos de tráfico
- Inspección del contenido del tráfico
- Análisis de registros de SPAM
- Honeypot
- Ingeniería inversa
- Análisis forense
- Feedback de Antivirus

Activas: Interacciones con el que origina el tráfico

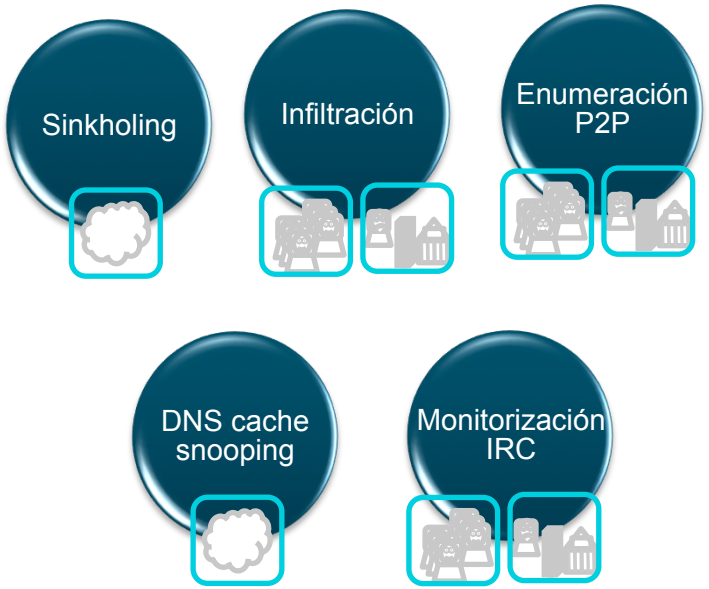
- Sinkholing
- Infiltración
- Enumeración P2P
- DNS cache snooping
- Monitorización IRC

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/workshop-presentations/daniel-plohmann-presentation/

¿Y cómo se pueden detectar?

Pasivas: recogida y observación

Activas: Interacciones con el que origina el tráfico



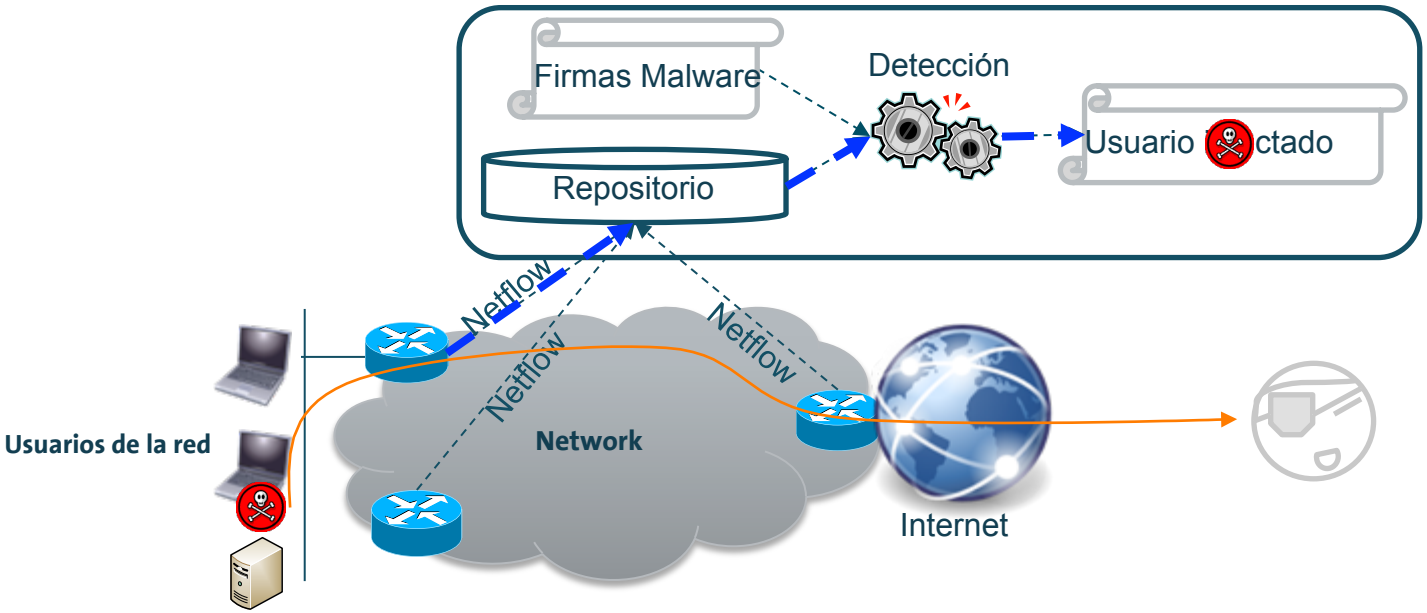
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/workshop-presentations/daniel-plohmann-presentation/

¿Y cómo se pueden detectar?

Un ejemplo de operador de red

- Registro del tráfico agregado en los nodos de una red.
  - Protocolo Netflow/IPFIX
  - Muestreado 1:10,1:1000,1:10000 si el ancho de banda es muy elevado (10-100Gbps)
  - Almacenamiento en servidores para su análisis.
- Análisis y detección de Botnets:
  - Firmas basadas en : IP destino + Protocolo + Puerto

Análisis de registros de flujos de tráfico



¿Y cómo se pueden mitigar?

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/workshop-presentations/daniel-plohmann-presentation/

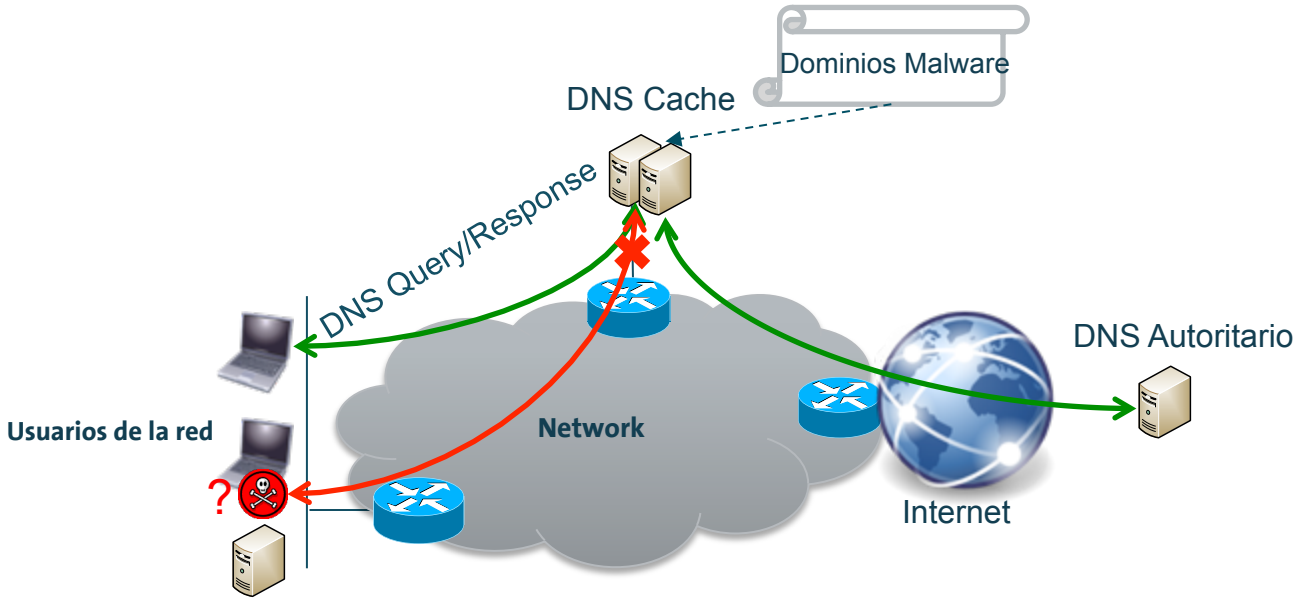
¿Y cómo se pueden mitigar?

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/workshop-presentations/daniel-plohmann-presentation/

¿Y cómo se pueden mitigar?

Un ejemplo de operador de red

- Análisis del tráfico DNS:
  - Copia del tráfico DNS: Tap, port mirrorring
  - Análisis en los propios Servidores DNS
- Detección y mitigación de usuarios infectados por Botnets:
  - Basado en Listas negras de dominios maliciosos
  - DNS responde a estos dominios con “NX Domain”
    - ISC BIND 9 y la función RPZ*



Diferentes estrategias

- Soluciones individuales
  - Yo detecto el malware en mi red.
  - ¿cuál es el problema?
    - Detección limitada
  - ¿cuál es la ventaja?
    - Fácil de implementar.

- Mi proveedor es mi amigo
  - Suministradores con información global
  - ¿cuál es el problema?
    - Hay que pagar
    - Tu red es parte de la información
    - Dependes de una fuente única
  - ¿cuál es la ventaja?
    - Fácil de implementar
    - Mayor detección.

- Colaboración
  - Acuerdos de intercambio de información
  - ¿cuál es el problema?
    - Tu red es parte de la información
    - No es fácil de implementar
  - ¿cuál es la ventaja?
    - La mayor detección.
    - Flexible

ACDC

the Advance Cyber Defence Centre

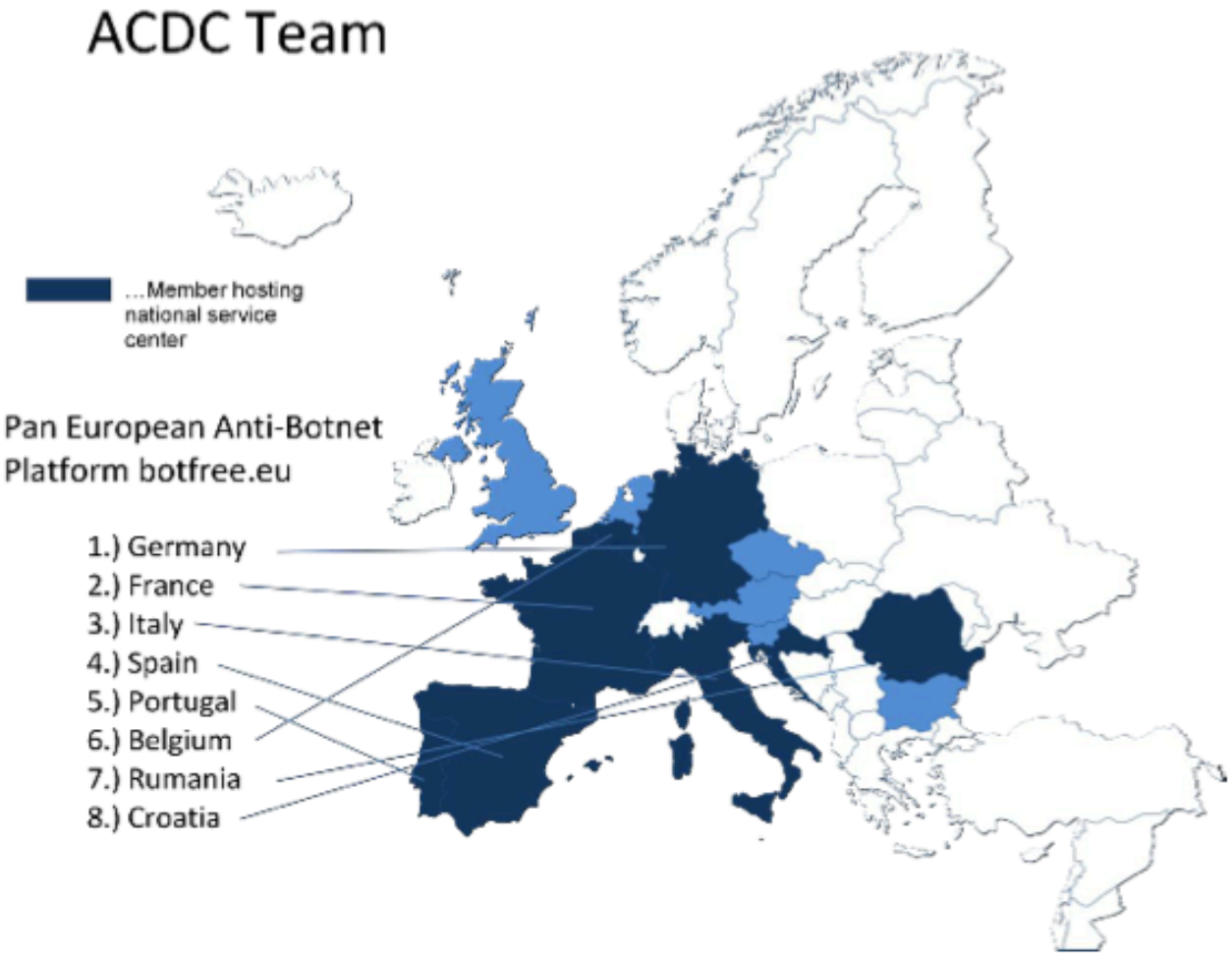
- Proyecto de innovación Europeo centrado en la lucha contra las **Botnets**
  - Participación conjunta de varios países de la UE
  - Diferentes tipos de redes y organizaciones
    - Telefónica esta representada por Telefónica I+D
  - Objetivos que se persiguen:
    - Compartición de información entre todos los miembros
    - Mejorar la detección y erradicación de Botnets en el ámbito Europeo
    - Concienciación y colaboración de organismos, empresas y ciudadanos.
  - Resultados esperados:
    - Conjunto de soluciones *on-line* para detectar y mitigar los efectos de las botnets.
    - Generación de mejores prácticas conjuntas
    - Disponibilidad de un Repositorio Centralizado
    - Centros de Soporte

¿Quién Participa?

28 partners

(Muestra representativa)

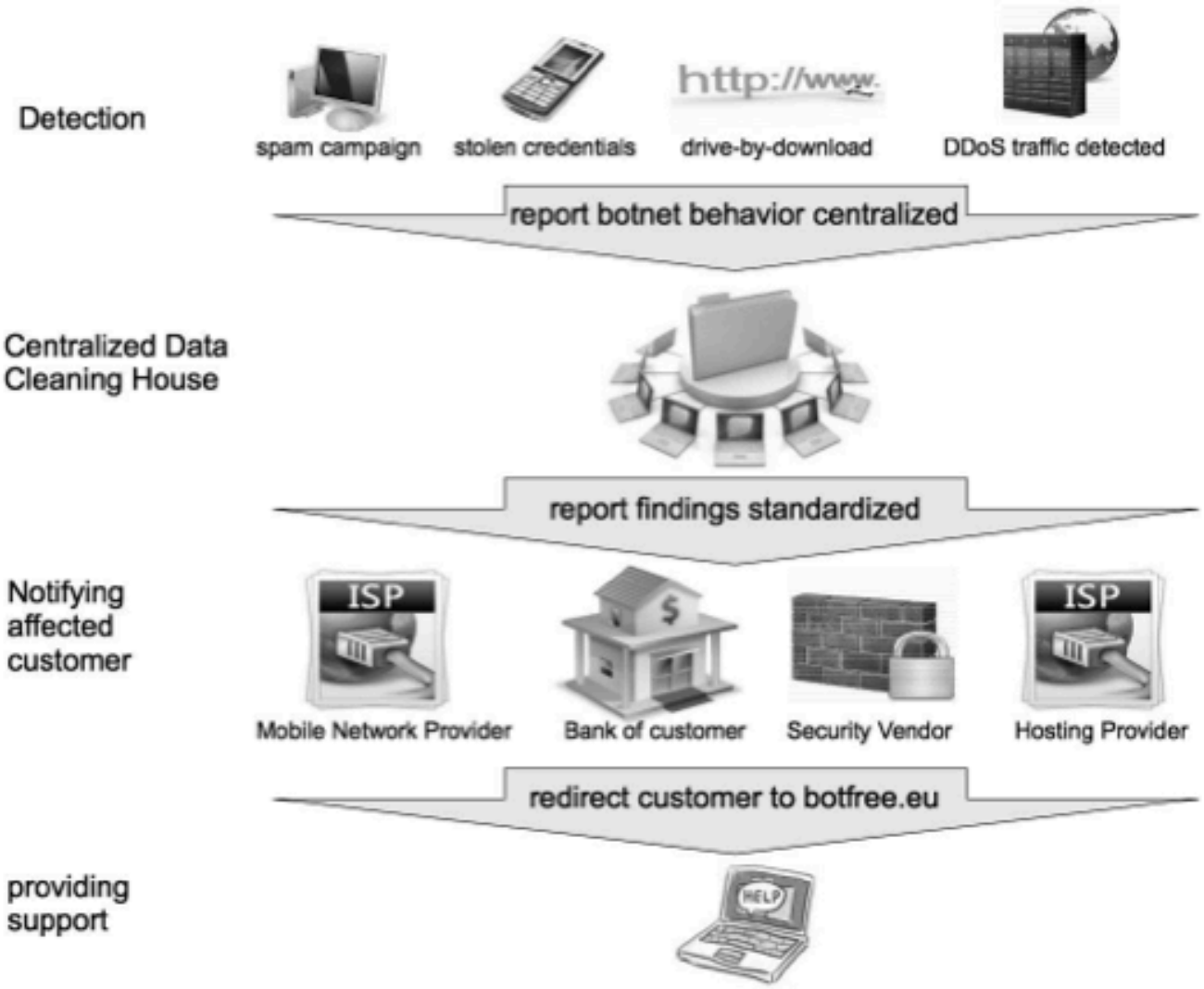
¿Quién Participa?



¿Cómo se esta trabajando?

- Organización del proyecto
  - WP1 – Especificación y Requisitos del Proyecto
    - Formatos de intercambio, especificaciones del Software, Arquitectura,…
  - WP2 - Desarrollo de los componentes y la tecnología
    - Programación del software y las interconexiones.
  - WP3 – Planificación, pruebas y desarrollos de experimentos.
    - Definición y ejecución de las pruebas y las conexiones de los socios.
  - WP4 – Evaluar e incentivar la mitigación de las Botnets
    - Elaborar métricas de eficiencia en la mitigación y evaluar resultados del piloto
  - WP5 – Diseminación, explotación y viabilidad a largo plazo
    - Información, concienciación social, formación, modelos de explotación, y implicaciones legales.
  - WP6 – Gestión de los perfiles de los usuarios
    - Identificar y categorizar tipos de organizaciones de interes, establecer plataformas sociales de comunicación

Arquitectura



- ✓ Sensores de red
- ✓ Herramientas de análisis

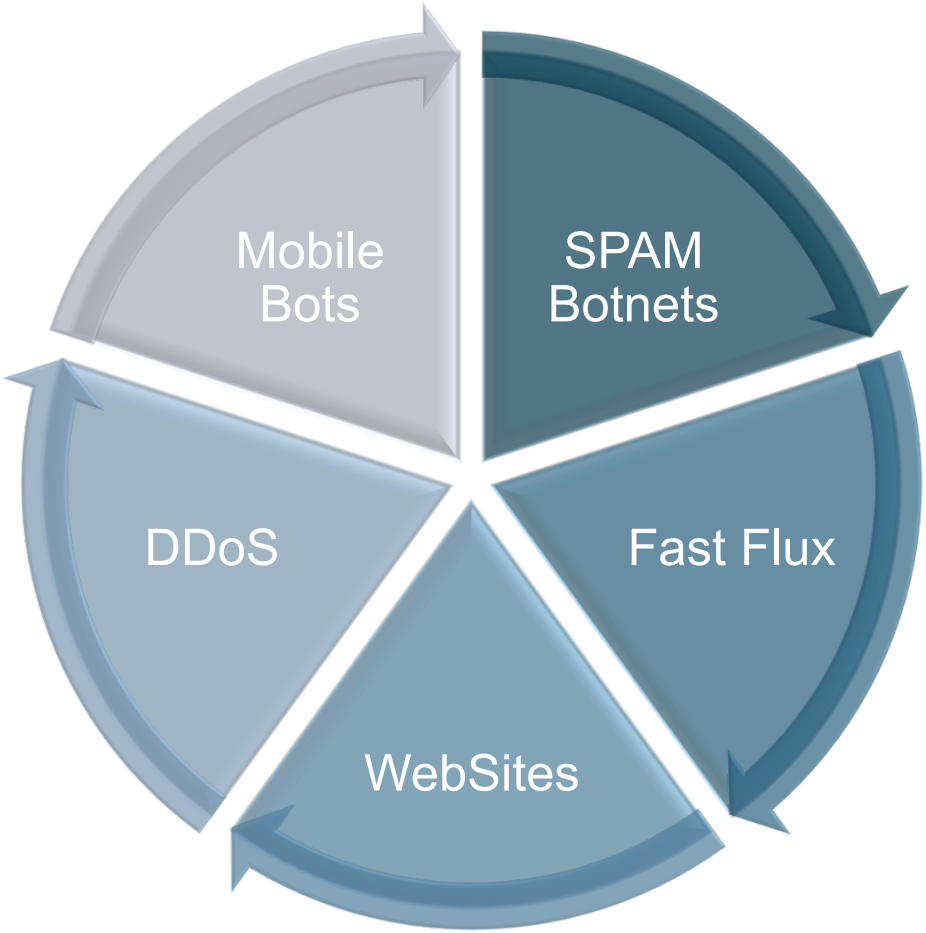
- ✓ Clasificación
- ✓ Bases de datos
- ✓ Visibilidad

- ✓ Notificación victimas
- ✓ Mitigación malware

- ✓ Centros de Soporte
- ✓ Ayuda

Tipos de Botnets

- El proyecto se ha dividido en los siguientes casos:



¿Cómo intercambiar al información?

Formatos y protocolos preferentes.

X-ARF (http://www.x-arf.org/)

- Formato tipo E-mail para reporte de abusos de red (spam, DoS, legal,..)
- Legible por sistemas automáticos y por personas
- Encaja para el uso por sensores de red para intercambiar información, como ISPs, agenciar gubernamentales y usuarios
- Código abierto y gratuito.

IODEF (RFC 5070)

- Especializado para el intercambio de datos etnre CERT/CSIRTs.
- Hace uso de plantillas XML para aojar la información.
- Uso de API tipo REST sobre HTTP.

STIX/TAXII (Mitre)

- STIX: Structured Threat Information eXpression. Lenguaje estandarizado de datos
- TAXII: Trusted Automated eXchange of Indicator Information. Definición de tipos de mensajes de transporte.
- Solución de gran complejidad, pero permite caracterizar modelos de Ciberamenazas.

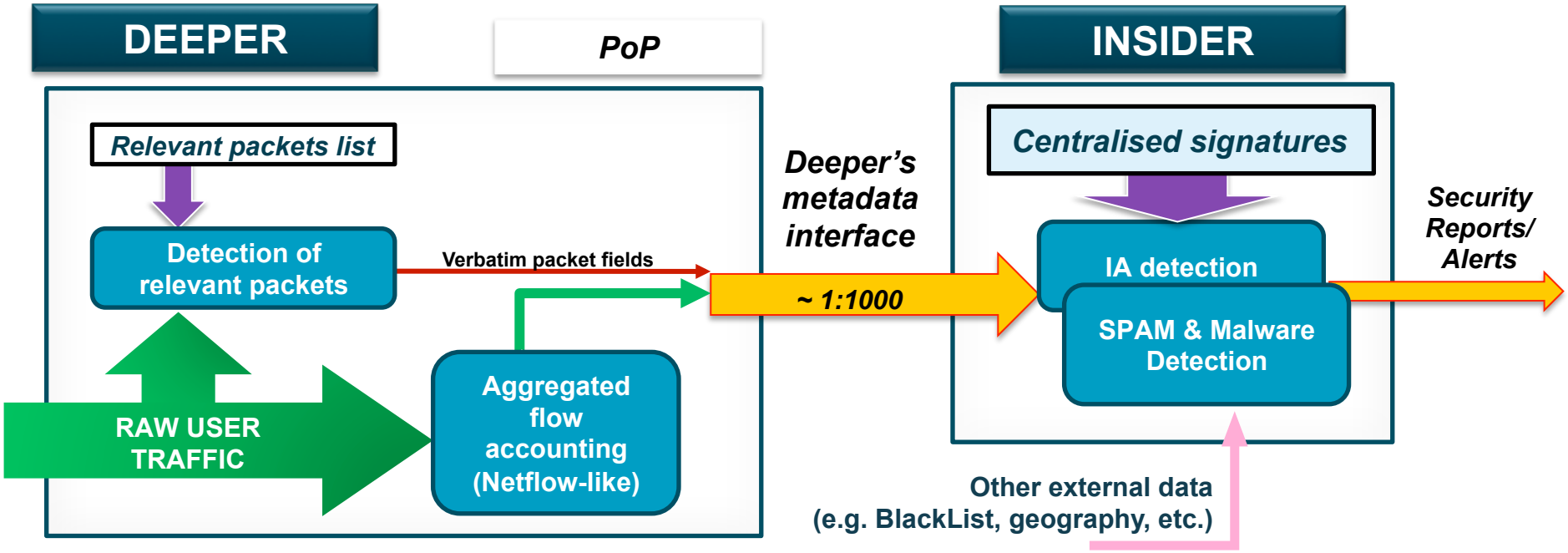
Primeros resultados

- Ya se dispone de los primeros resultados
  - Portal Web con la información de distintos Sensores
  - Protocolo de transporte HTTPS
  - Formato de datos STIX
  - A través de Internet

¿Que estamos haciendo en TI+D?

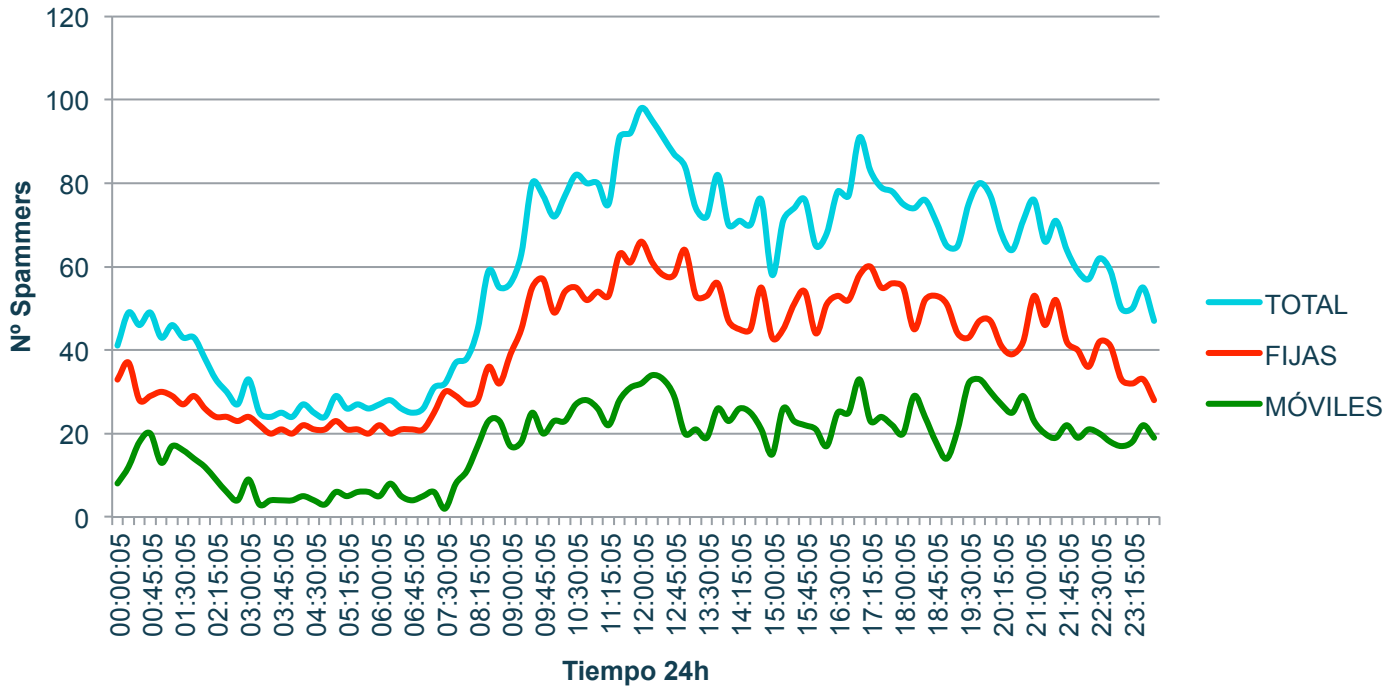
- Spam-Bot Detection.
  - Sensor de red para identificar usuarios de ISP infectados por SpamBots.
    - Fuente de datos -> Información de trafico de red
    - Detección basado en reglas
- DNS-based BOT Detection.
  - Sensor de red basado en el análisis de tráfico DNS para identificar usuarios de ISP infectados por botnets
    - Fuente de datos -> Información de trafico de red
    - Detección basado en reglas
- Smart Bot Detection.
  - Sensor de red basado en el análisis de tráfico basado en modelos de clusterización para identificar usuarios de ISP infectados por botnets
    - Detección basado en algoritmos de inteligencia artificial
- ISP Data Adaptor.
  - Adaptador orientado a un operador de red, para gestionar el intercambio de información a importa e exportar (filtrado, anonimización,..)
- HP Sentinel
  - Sensor y mitigador basado en el análisis del tráfico DNS para identificar usuarios infectados por botnets

SPAM bot, DNS bot & SMART bot detector



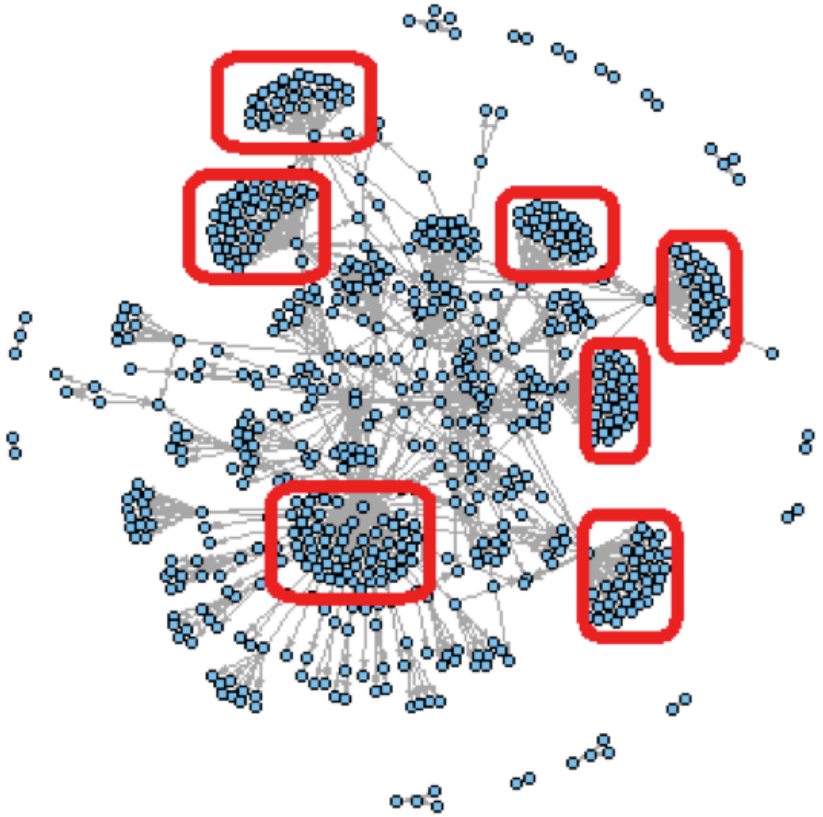
- Deeper. DPI basado en HW de uso genérico (servidor). Desarrollado en Telefónica I+D. En fase pre-industrial
  - Deeper permite extraer información relevante (a nivel payload), comprimirlo y exportarlo. Se combina con información de flujos de trafico. Permite exportar e interpretar la información fuera del equipo
  - Insider. Permite interpretar el trafico de manera centralizada, y aplicar firmas de detección complejas.
- Se están desarrollando e implementando Firmas de detección de la existencia de Botnets, mediante reglas simples e inteligencia artificial.

Ejemplo SPAM-bot detection



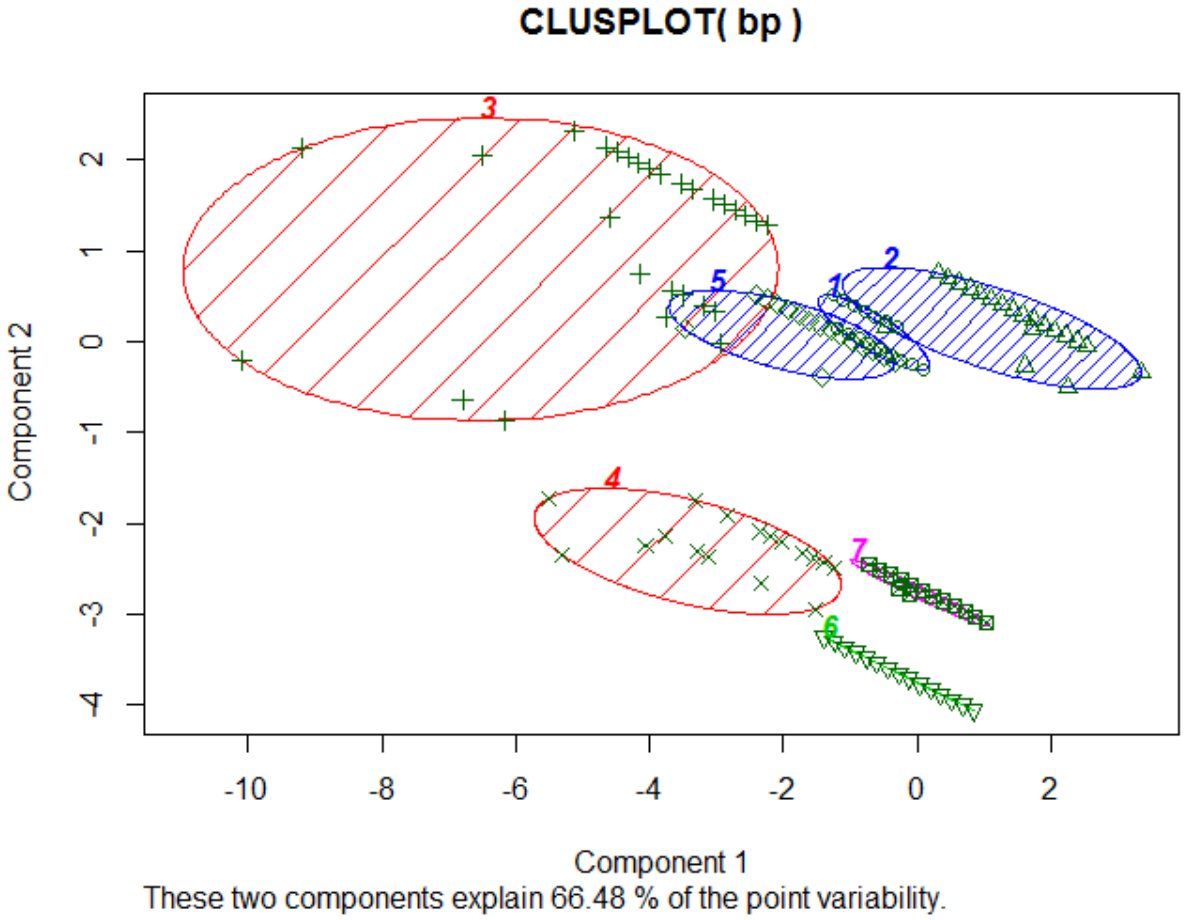
SmartBot Detector

- Relaciones entre las ips de Botnets (filtrada por nº de conexiones)



SmartBot Detector

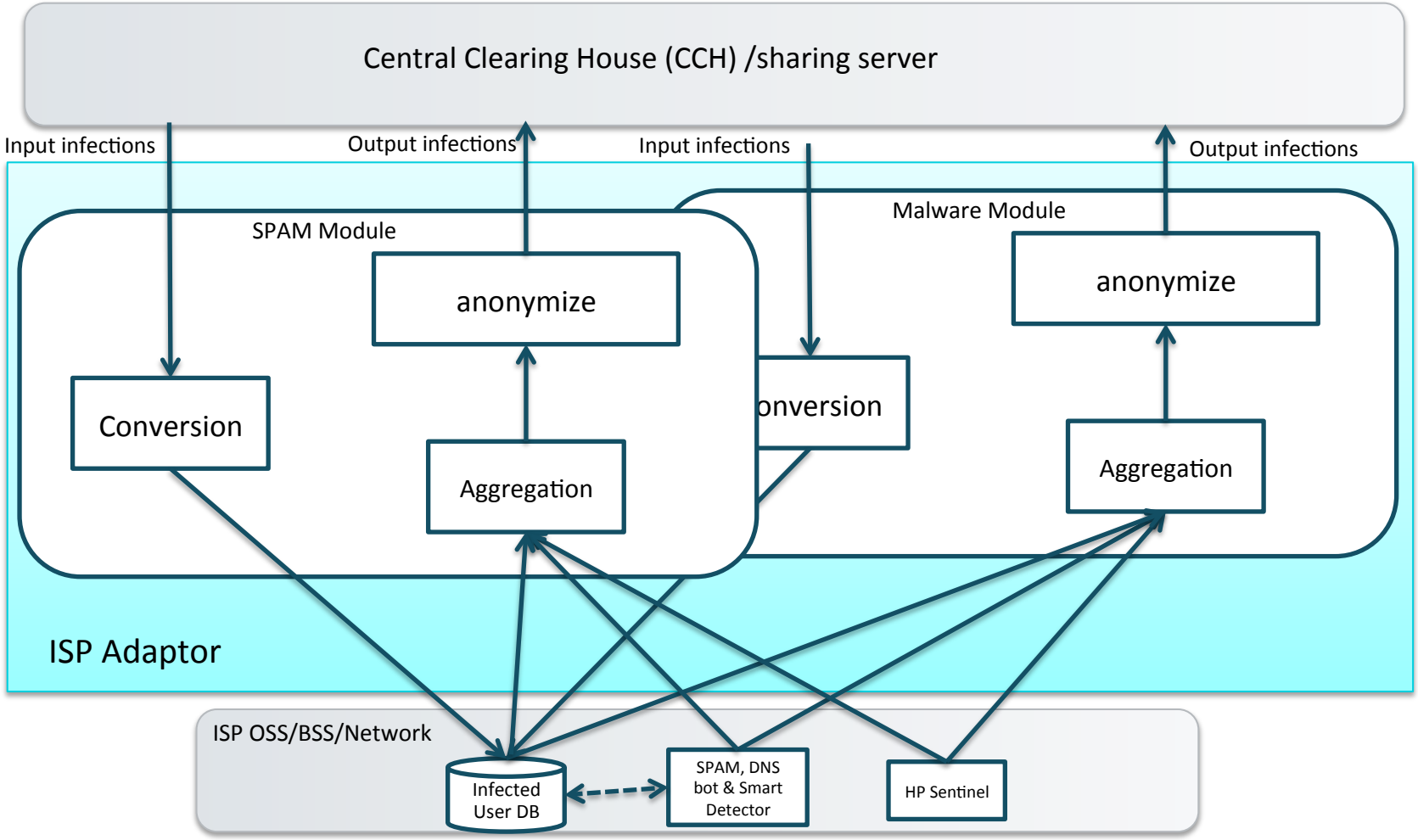
Clusters encontradors → Identificación de IPs → Ranking ips peligrosas



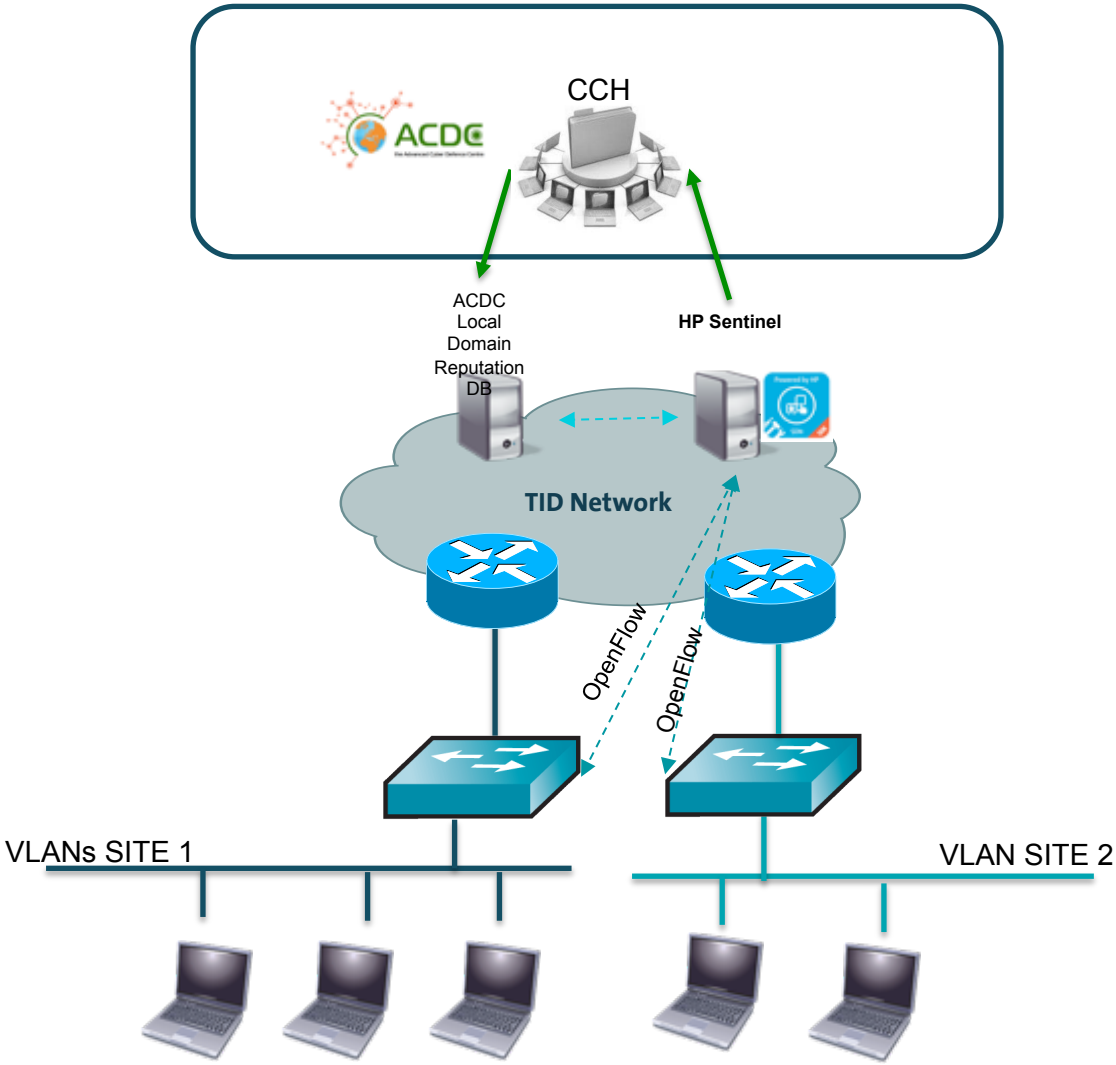
Cluster 1
Ip234
Ip67
…
ip455

Cluster 7
Ip56
Ip894
…
ip153

ISP Adaptor

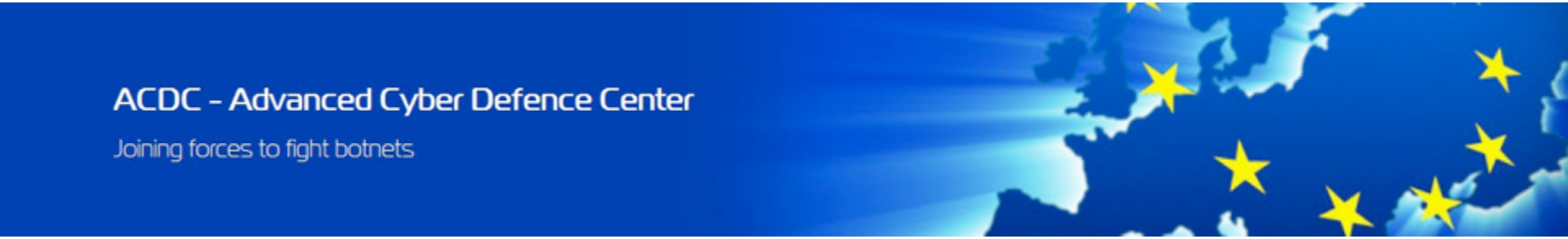

Central Clearing House (CCH) /sharing server
Input infections
Output infections
Input infections
Output infections
SPAM Module
anonymize
Conversion
Aggregation
onversion
Malware Module
anonymize
Aggregation
ISP Adaptor
ISP OSS/BSS/Network
Infected User DB
SPAM, DNS bot & Smart Detector
HP Sentinel

HP Sentinel


CCH
ACDC
Local
Domain
Reputation
DB
HP Sentinel
TID Network
OpenFlow
OpenFlow
VLANs SITE 1
VLAN SITE 2

¿Quieres participar?

- ACDC es un proyecto colaborativo
- ACDC es un proyecto abierto
- ¿Estas interesado?
  - ACDC ofrece firmar una carta de interés. No compromete.
    - www.acdc-project.eu/wp-content/uploads/2013/10/LoI-external-consultative-board-ACDC-template.docx



¿Quieres aprender mas?

Botnets

- Informe ENISA sobre las Botnets.
  - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/workshop-presentations/daniel-plohmann-presentation/
- Coursera Malware
  - https://www.coursera.org/course/malsoftware

ACDC

- Portal global del ACDC
  - www.botfree.eu
- Portal para la comunidad (próximamente en 2014)
  - www.acdc-project.eu/


Telefónica