Plataforma Automatizada de Detección de Malware

Presentado por Ferran Pichel Llaquet
codirigido por Miguel Ángel Domínguez
y dirigido por Marc Moreno Berengué.

Proyecto realizado en la empresa
Internet Security Auditors, S.L.

Índice de Contenidos

1. **Objetivos:** Problemática Actual

- Vulnerabilidades en sistemas de usuario
- Vulnerabilidades en aplicaciones externas
- Vulnerabilidades en portales web de entidades
- Desconocimiento de los usuarios
- Intereses

Infecciones de Malware

1. **Objetivos:** Solución

No existe una solución que al aplicarla garantice un 100% de protección.

La única solución es la prevención:

- *Diseñar una capa de seguridad en la aplicación web*
- ***Análisis constante y periódico de la aplicación web***

Desde Internet Security Auditors, S.L. se ofrece un servicio de análisis periódico

1. Objetivos

Diseñar e implementar una plataforma que permita:

- Solucionar deficiencias detectadas en el software de análisis
- Centralización de los diferentes resultados
- Integración de logs en el *syslog* del sistema
- Sistema de alarmas en tiempo real

Índice de Contenidos

2. **Análisis:** Solución Actual

En **Internet Security Auditors, S.L.** se realizan un total de 24 ciclos diarios, enviando un informe al terminar.

Prioridad	Ciclos diarios
1	24
2	12
3	8
4	6

En cada ciclo:

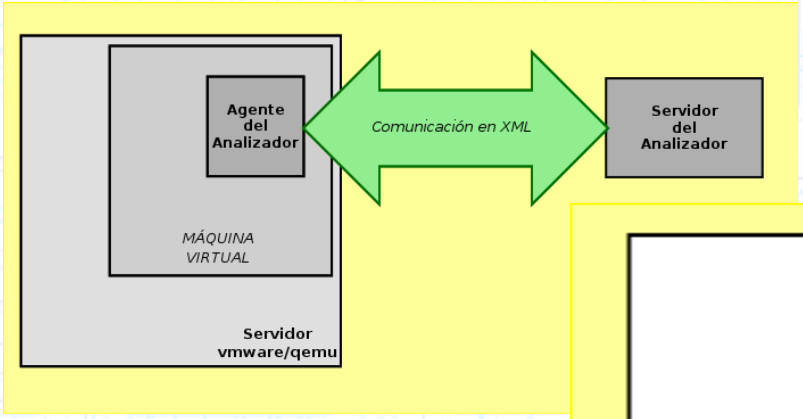
- Seleccionar dominios a analizar dependiendo de su prioridad

- Conocer los recursos que lo componen (*crawling*)

- Cargar cada uno de los recursos y analizar el sistema (H*oneyClient*)

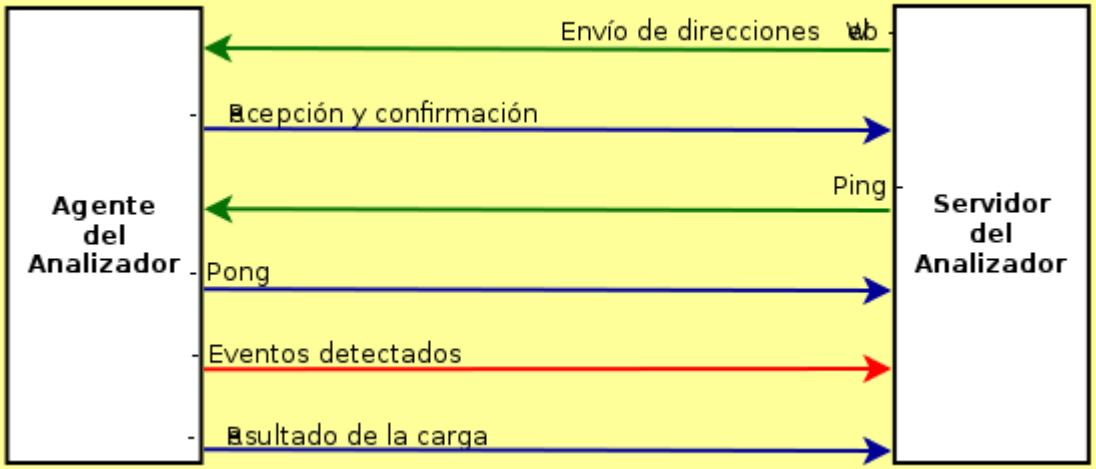
- Recolectar resultados

2. Análisis: Software HoneyClient



Arquitectura

Protocolo

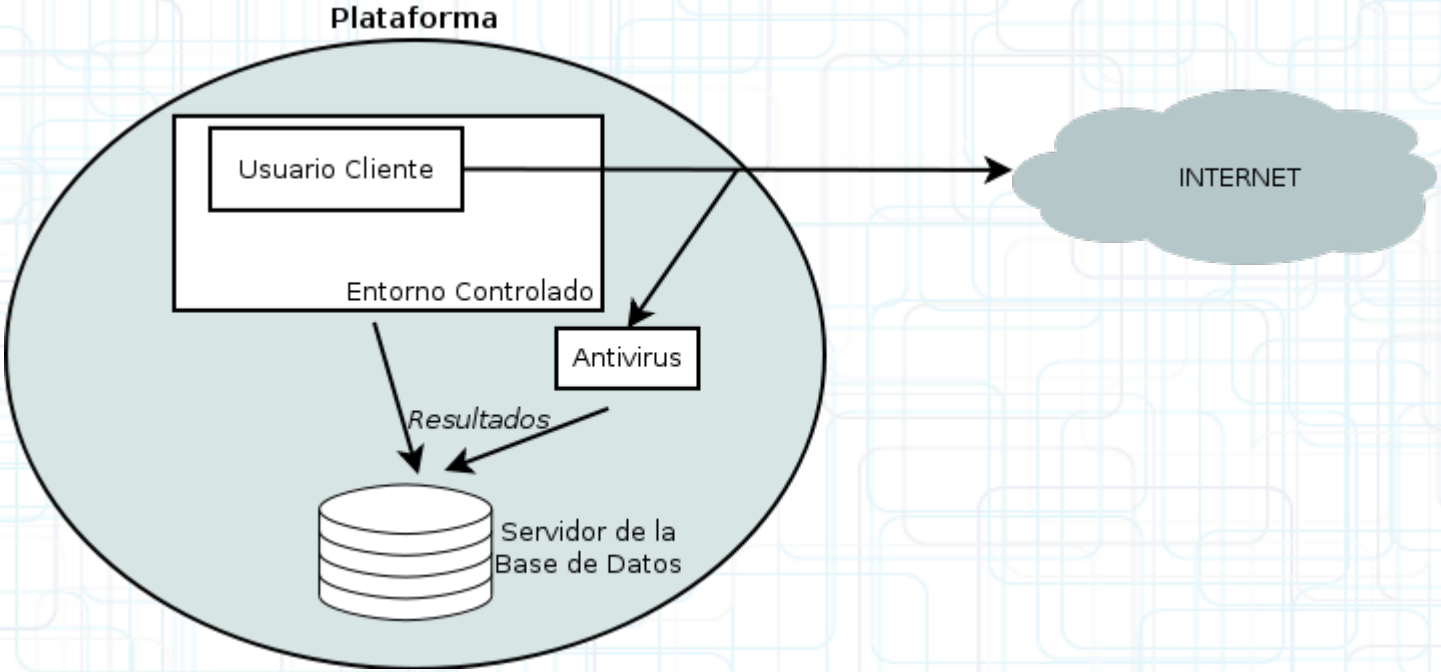


Deficiencias actuales:

- Algoritmo de análisis de la aplicación deficiente
- Problemas de ejecución continuada

Índice de Contenidos

3. Implementación: Nueva Plataforma



Arquitectura de la nueva plataforma automatizada que realiza análisis continuos a dominios, tanto de *malware* como antivirus.

3. Implementación: Módulos

Se han divido las funcionalidades en módulos:

- **Crawling**
  Proceso de crawling y gestión de resultados

- **HoneyClient**
  Análisis HoneyClient y antivirus, junto la gestión de los resultados

- **Gestor Principal**
  Configuración de cada uno de los módulos

3. Implementación: Gestor Principal

Análisis de las funcionalidades:

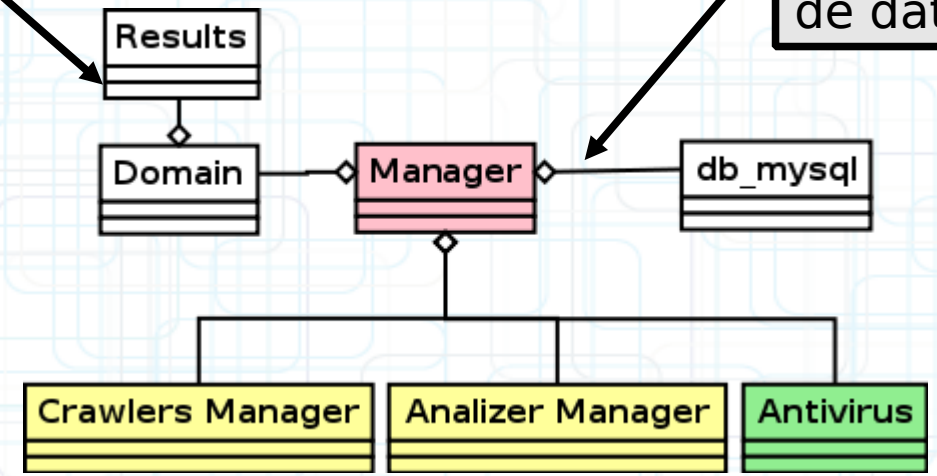
- Controlar ejecución de los diferentes gestores:
  - *Crawling* Analizador Alertas y Antivirus
- Recolección y almacenamiento de resultados
- Control de los diferentes ciclos
- Planificación de cada ciclo en base a la prioridad y el número de máquinas virtuales disponibles:

Cada dominio debe analizarse con todas las máquinas virtuales posibles

3. Implementación: Gestor Principal - diseño

A cada dominio se le asocian los diferentes resultados

Sólo el gestor principal interactua con la base de datos



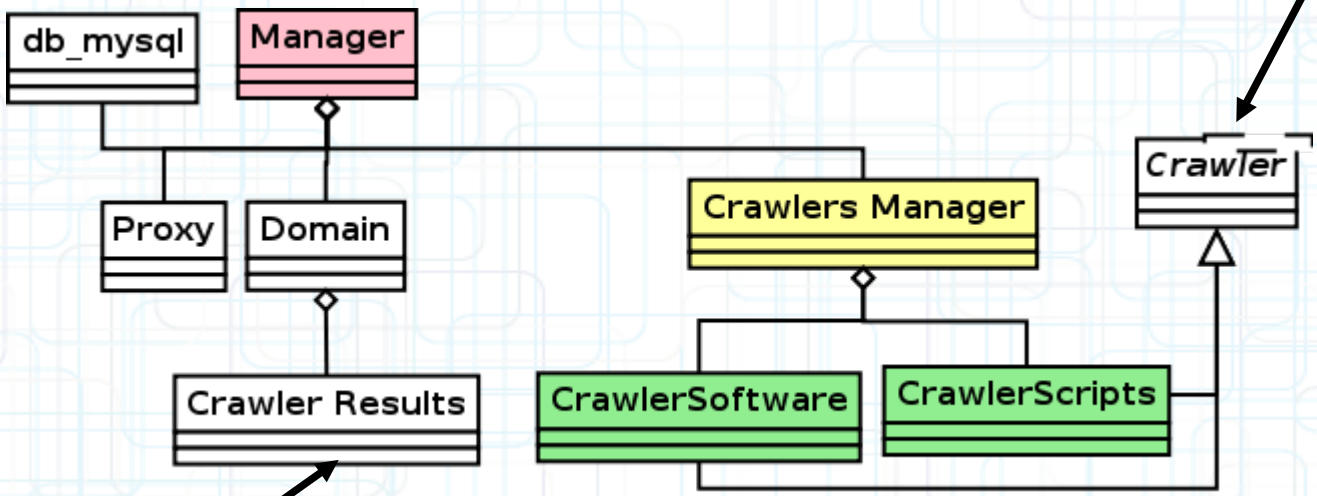
3. Implementación: Gestor de Crawling

Análisis de las funcionalidades:

- Ejecución paralela de varios procesos
- Recolección de resultados
- Soporte para el *software de crawling* utilizado
- Soporte para *scripts* concretos para un dominio
- Permitir añadir nuevos módulos

3. Implementación: Gestor de Crawling - diseño

Cada nodo de *crawling* hereda de una misma clase abstracta para facilitar futuros añadidos



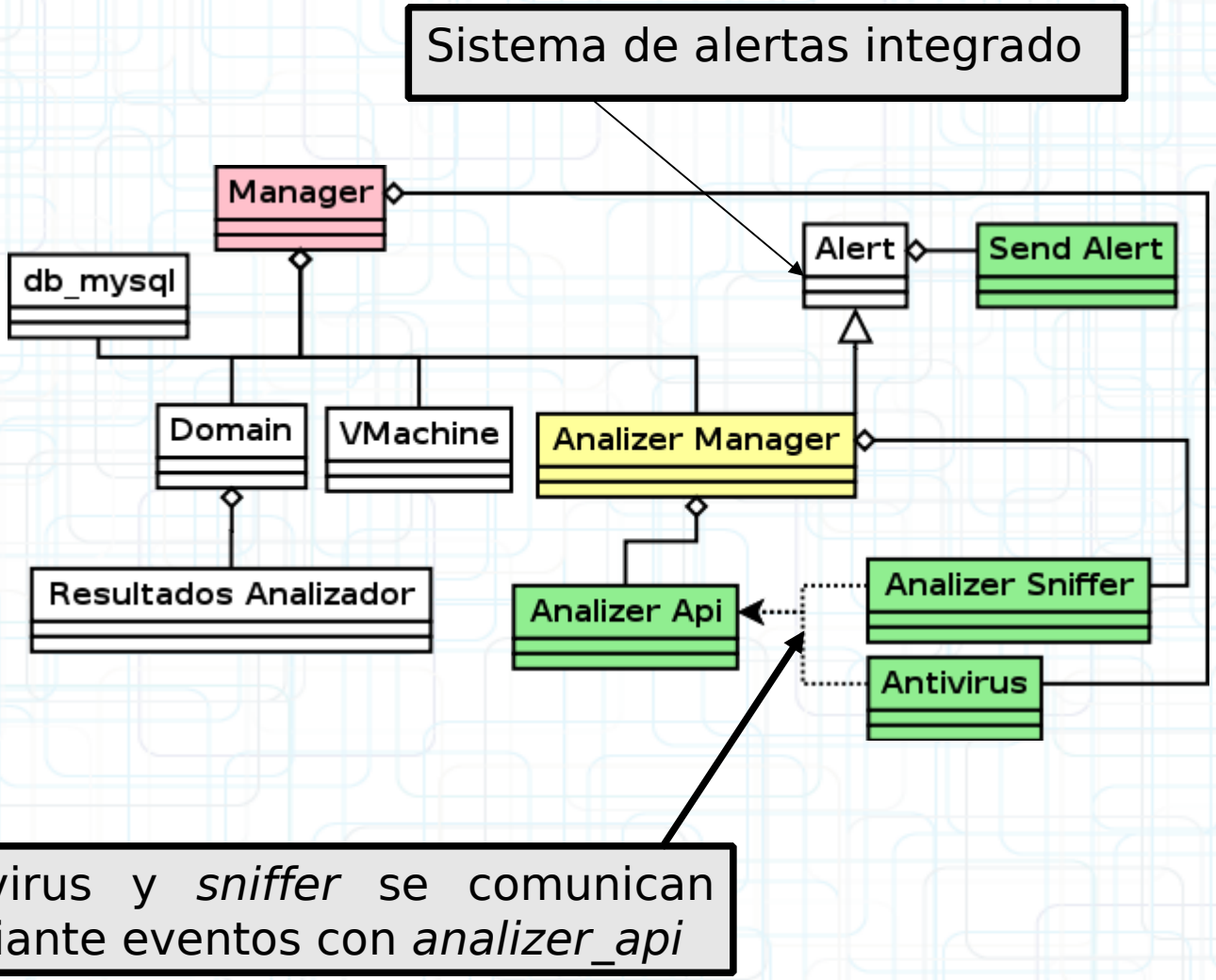
Independiza los resultados del nodo *crawler* utilizado

3. Implementación: Gestor de Analizador

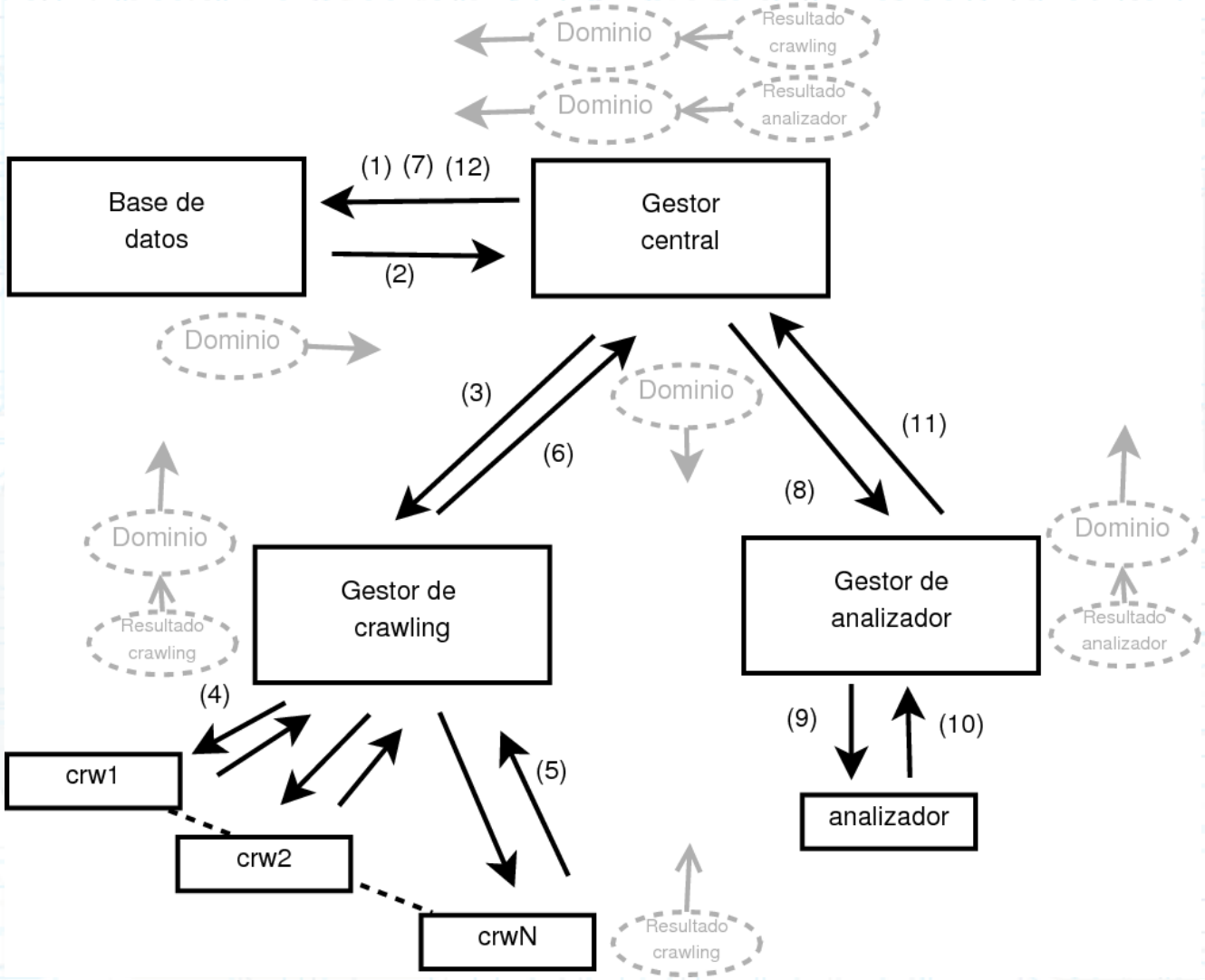
Análisis de las funcionalidades:

- Controlar aplicación *HoneyClient* sin intrusismo
- Permitir una ejecución paralela para un futuro
- Solucionar errores de ejecución continua
- Solucionar errores en el proceso de identificación de una infección
- Envío de alertas al detectar acciones maliciosas

3. Implementación: Gestor Analizador - diseño



3. Implementación: Funcionamiento General



Índice de Contenidos

4. **Resultados:** Informes Diarios

internet security auditors — Informe de Análisis — Servicio de Vigilancia **Anti-Malware** — Fri Sep 11 02:01:47 2009

Ámbito

Estado	Dominio	Ciclos
☣	www.test.com	24
✓	www.domain.com	24
✓	www.domain.com	12
✓	www.domain.com	12
✓	www.domain.com	12
✓	www.domain.com	12
✓	www.domain.com	12
✓	www.domain.com	12
✓	www.domain.com	8
✓	www.domain.com	7
✓	www.domain.com	6
✓	www.domain.com	6

Los ciclos representan el número de escaneos realizados en un periodo de 24 horas

Debido a problemas de conectividad con el servidor, no se ha podido realizar la totalidad de los ciclos.

Estado	Dominio	Ciclos
☣	www.test.com	24
✓	www.domain.com	24
✓	www.domain.com	12

Resultados

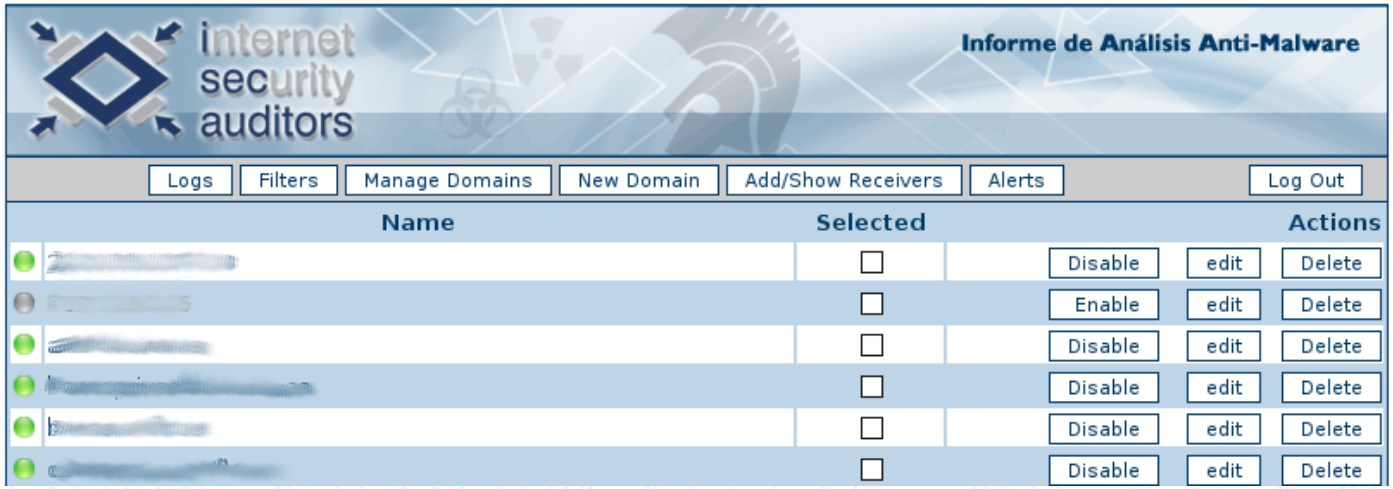
www.test.com

http://diversitech.eu/es/pdfs/Pro-Universal_Granular_Coil_CleanerCOSHH.pdf

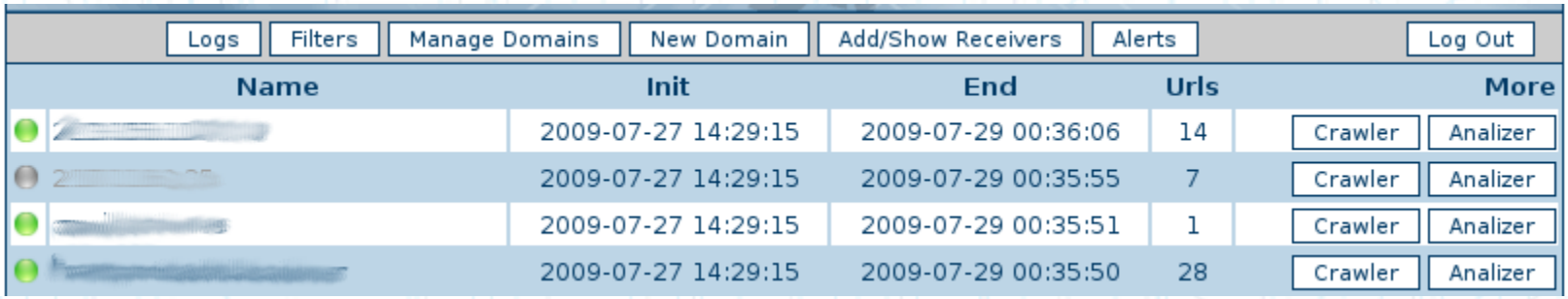
3056	C:\Archivos de programa\Adobe\Reader 8.0\Reader\AcroRd32.exe	
10/9/2009 4:0:27.12	DeleteValueKey	HKCU\Software\Adobe\Acrobat Reader\8.0\AdobeViewer\MaxDoc
10/9/2009 4:0:27.12	DeleteValueKey	HKCU\Software\Adobe\Acrobat Reader\8.0\AdobeViewer\MaxApp
10/9/2009 4:0:27.12	DeleteValueKey	HKCU\Software\Adobe\Ac... \PrintToFile
10/9/2009 4:0:27.28	SetValueKey	HKCU\Software\Adobe\Acrobat Reader\8.0\NoTimeOut\smailto
10/9/2009 4:0:27.28	SetValueKey	HKCU\Software\Adobe\Acrobat Reader\8.0\Originals \sProofingSpace
10/9/2009 4:0:27.43	SetValueKey	HKCU\Software\Adobe\Acrobat Reader\8.0\Selection \aDefaultSelect
10/9/2009 4:0:27.168	SetValueKey	HKCU\Software\Adobe\Adobe Acrobat\8.0\DiskCabs \bCollab_OfflineDocs
10/9/2009		HKCU\Software\Adobe\Adobe Acrobat\8.0\DiskCabs

4. **Resultados:** Acceso web a los datos

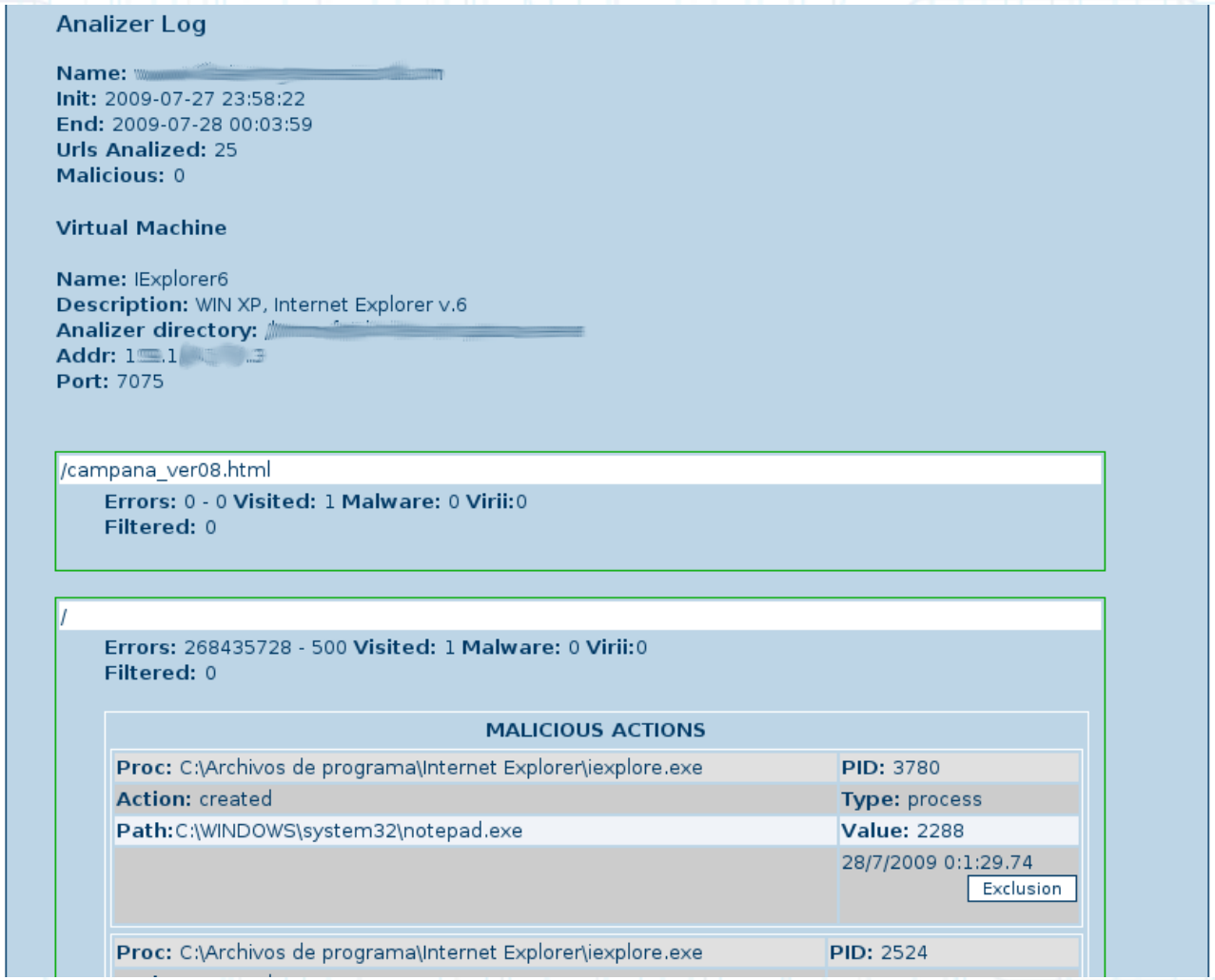
- Gestión cómoda de dominios:



- Visualización detallada de los resultados por ciclo:



4. **Resultados:** Acceso web a los datos



Analizer Log

Name: [redacted]
Init: 2009-07-27 23:58:22
End: 2009-07-28 00:03:59
Urls Analized: 25
Malicious: 0

Virtual Machine

Name: IExplorer6
Description: WIN XP, Internet Explorer v.6
Analizer directory: [redacted]
Addr: 1[redacted].1[redacted].3
Port: 7075

/campana_ver08.html

Errors: 0 - 0 **Visited:** 1 **Malware:** 0 **Virii:**0
Filtered: 0

/

Errors: 268435728 - 500 **Visited:** 1 **Malware:** 0 **Virii:**0
Filtered: 0

MALICIOUS ACTIONS

Proc: C:\Archivos de programa\Internet Explorer\iexplore.exe	**PID:** 3780
Action: created	**Type:** process
Path:C:\WINDOWS\system32\notepad.exe	**Value:** 2288
	28/7/2009 0:1:29.74 Exclusion
Proc: C:\Archivos de programa\Internet Explorer\iexplore.exe	**PID:** 2524

Índice de Contenidos

6. Conclusiones

Conclusiones:

- *La gestión de los procesos de crawling es eficiente y robusta*
- *El analizador es controlado al detalle*
- *Se centraliza la información coherentemente en la BD*
- *Intervención humana mucho menor*
- *Resultado satisfactorio*

6. Conclusiones: Mejoras

Mejoras:

- *Permittir el envío de informes en otros formatos: PDF, XML...*
- *Permitir el envío de informes por otros canales: Mail, SMS...*
- *Añadir cualquier funcionalidad necesaria para mejorar el servicio o la detección*

Plataforma Automatizada de Detección de Malware

GRACIAS

Presentado por Ferran Pichel Llaquet
codirigido por Miguel Ángel Domínguez
y dirigido por Marc Moreno Berengué

Septiembre 2009