

# Jornadas “Espacios de Ciberseguridad”

## ¿Mi ordenador es un zombi?

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

INSTITUTO NACIONAL DE  
CIBERSEGURIDAD  
SPANISH NATIONAL  
CYBERSECURITY INSTITUTE



Esta presentación se publica bajo licencia Creative Commons del tipo:  
Reconocimiento – No comercial – Compartir Igual  
<http://creativecommons.org/licenses/by-nc-sa/4.0/>

# Índice

## 1. INCIBE - ¿Qué es?

2. Introducción a la ciberseguridad

3. Objetivos del curso

4. Malware

5. Botnets

6. Práctica: construyendo una botnet

1. Infección

2. Explotación

3. Detección y desinfección

7. Contramedidas

8. Resumen

9. Otros datos de interés

# INCIBE - ¿Qué es?

El Instituto Nacional de Ciberseguridad de España (**INCIBE**) es una sociedad dependiente del Ministerio de Energía y Turismo y Agenda Digital (**MINETAD**) a través de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (**SESIAD**).

INCIBE es la entidad de referencia para el desarrollo de la **ciberseguridad** y de la **confianza digital** de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos (Agenda Digital para España, aprobada en Consejo de Ministros el 15 de Febrero de 2012).

Como **centro de excelencia**, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia , INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

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



# INCIBE - ¿Qué es?

## Pilares fundamentales sobre los que se apoya la actividad de INCIBE

- **Prestación de servicios** de protección de la privacidad, prevención y reacción a incidentes en ciberseguridad
- **Investigación** generación de inteligencia y mejora de los servicios
- **Coordinación** colaboración con entidades públicas y privadas, nacionales e internacionales

## Área de Operaciones



# Jornadas “Espacios Ciberseguridad”

## Características Jornadas

### JORNADAS PARA ALUMNOS



Alumnos de Bachiller y FP tecnológicos.  
1 temática por centro (de las 8 posibles).

Grupos de entre 20 y 30 alumnos.  
Duración 3h , en una única sesión.

<https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes>  
[espaciosciberseguridad@incibe.es](mailto:espaciosciberseguridad@incibe.es)

### JORNADAS PARA PROFESORES



Profesores de Bachiller y FP tecnológicos.  
Duración 9 horas en dos sesiones de 4,5h.

Grupos de entre 20 y 30 docentes.  
Formación para impartir las 8 temáticas de manera autónoma.

<https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/profesores>  
[espacioscs\\_profesores@incibe.es](mailto:espacioscs_profesores@incibe.es)

### MATERIALES ON-LINE (YA DISPONIBLES EN LA PÁGINA WEB DE LAS JORNADAS)

PPT's de las 8 jornadas para alumnos

Videos de la impartición de las 8 jornadas íntegras

Documentación adicional para cada jornada:

Conocimientos previos de los alumnos.

Resumen de contenidos y vídeo píldoras de 5min sobre el contenido de cada jornada.

Material complementario para seguir investigando y aprendiendo sobre cada una de las materias.

Materiales para la impartición de los talleres por parte de los profesores:

PPT presentada en la jornada de **profesores**.

**Dossier completo** con la explicación detallada de todas las jornadas de alumnos así como los temas generales para la preparación de los entornos de prácticas.

### ¿Qué temáticas se tratan en las jornadas?

Se tratará de manera monográfica una de las ocho temáticas siguientes (a decidir por parte del centro):

 <b>Mi ordenador es un zombi</b> Funcionamiento de las redes botnets, así como, su proceso de creación e infección.	 <b>Programación segura de sitios web</b> Identificación de los principales requisitos a tener en cuenta para desarrollar aplicaciones web seguras.
 <b>Fundamentos del análisis de sitios Web</b> Funcionamiento de un sitio Web. Detección, identificación, análisis y forma de explotar las vulnerabilidades web.	 <b>Fundamentos del análisis de sistemas</b> Identificación, análisis y explotación de las principales vulnerabilidades de los servicios soportados por un servidor.
 <b>Análisis de malware en Android</b> Prácticas más habituales de análisis de malware en dispositivos Android.	 <b>Seguridad Wifi</b> Seguridad de los dispositivos Wifi. Funcionamiento de un punto de acceso falso.
 <b>Espionaje y cibervigilancia</b> Análisis de las diferentes técnicas y herramientas utilizadas para realizar los labores de espionaje y cibervigilancia.	 <b>Forense en Windows</b> En qué consiste y principales técnicas del análisis forense en sistemas Windows.



# Índice

1. INCIBE - ¿Qué es?
- 2. Introducción a la ciberseguridad**
3. Objetivos del curso
4. Malware
5. Botnets
6. Práctica: construyendo una botnet
  1. Infección
  2. Explotación
  3. Detección y desinfección
7. Contramedidas
8. Resumen
9. Otros datos de interés

# Introducción a la ciberseguridad

## Evolución de las Tecnologías de la Información

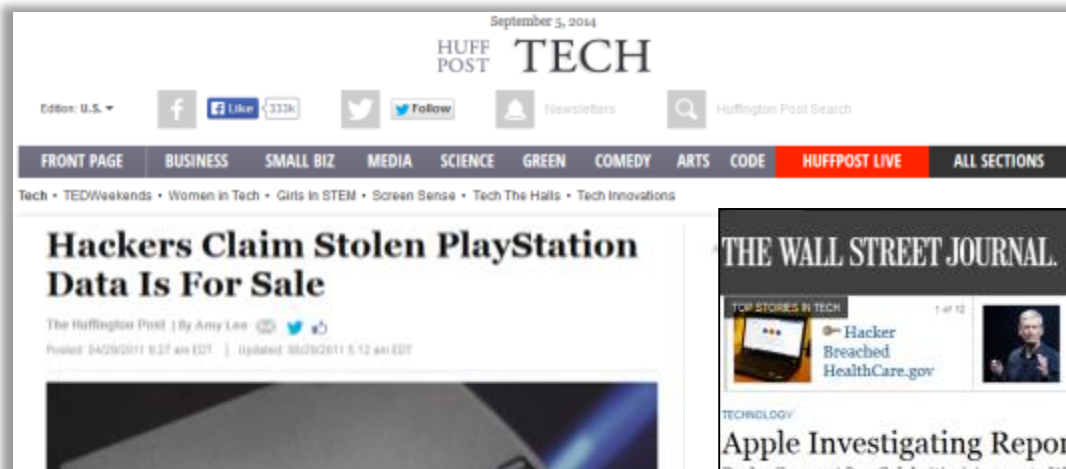
- La **información** es uno de los principales activos de una empresa.
- Las empresas almacenan y gestionan la información en los **Sistemas de Información**.
- Para una empresa resulta fundamental proteger sus Sistemas de Información para que su información esté a salvo. Dificultades:
  - El entorno donde las empresas desarrollan sus actividades es cada vez más complejo debido al desarrollo de las tecnologías de información y otros factores del entorno empresarial
  - El perfil de un ciberdelincuente de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar) en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede llegar a ser.
- Es fundamental poner los medios técnicos y organizativos necesarios para garantizar la seguridad de la información. Para lograrlo hay que garantizar la **confidencialidad**, **disponibilidad** e **integridad** de la información.





# Introducción a la ciberseguridad

## Casos notorios



### Bonopark denunciará los ataques al sistema informático de BiciMad





# Introducción a la ciberseguridad

## Seguridad de la Información

La seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información:

- La **confidencialidad** es la propiedad de prevenir la divulgación de información a personas no autorizadas.
- La **integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- La **autenticidad**: la información es lo que dice ser o el transmisor de la información es quien dice ser.
- El **no repudio**: Estrechamente relacionado con la Autenticidad. Permite, en caso de ser necesario, que sea posible probar la autoría u origen de una información.



# Introducción a la ciberseguridad

## Riesgos para los Sistemas de Información

¿Qué son los riesgos en los sistemas de información?

- Las amenazas sobre la información almacenada en un sistema informático.

Ejemplos de riesgos en los sistemas de información

- **Daño físico:** fuego, agua, vandalismo, pérdida de energía y desastres naturales.
- **Acciones humanas:** acción intencional o accidental que pueda atentar contra la productividad.
- **Fallos del equipamiento:** fallos del sistema o dispositivos periféricos.
- **Ataques internos o externos:** hacking, cracking y/o cualquier tipo de ataque.
- **Pérdida de datos:** divulgación de secretos comerciales, fraude, espionaje y robo.
- **Errores en las aplicaciones:** errores de computación, errores de entrada, etc.



# Introducción a la ciberseguridad

## La figura del HACKER

¿Qué es un hacker?

Experto en seguridad informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

¿Qué tipos de hackers existen en función de los objetivos que tienen?



**Black Hat Hackers:** Suelen quebrantar la seguridad de un sistema o una red con fines maliciosos.



**White Hat Hackers:** normalmente son los que penetran la seguridad de los sistemas bajo autorización para encontrar vulnerabilidades. Suelen ser contratados por empresas para mejorar la seguridad de sus propios sistemas.



**Gray (Grey) Hat Hackers:** Son una mezcla entre los dos anteriores puesto que tienen una ética ambigua. Normalmente su cometido es penetrar en sistemas de forma ilegal para luego informar a la empresa víctima y ofrecer sus servicios para solucionarlo.

# Introducción a la ciberseguridad

## Clases de ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación:** se crean productos, tales como páginas web o tarjetas magnéticas falsas.



# Introducción a la ciberseguridad

## Técnicas de hacking

- **Spoofing:** se suplanta la identidad de un sistema total o parcialmente.
- **Sniffing:** se produce al escuchar una red para ver toda la información transmitida por ésta.
- **Man in the middle:** siendo una mezcla de varias técnicas, consiste en interceptar la comunicación entre dos interlocutores posicionándose en medio de la comunicación y monitorizando y/o alterando la comunicación.
- **Malware:** se introducen programas dañinos en un sistema, como por ejemplo un virus, un keylogger (herramientas que permiten monitorizar las pulsaciones sobre un teclado) o rootkits (herramientas que ocultan la existencia de un intruso en un sistema).
- **Denegación de servicio:** consiste en la interrupción de un servicio sin autorización.
- **Ingeniería social:** se obtiene la información confidencial de una persona u organismo con fines perjudiciales. El Phishing es un ejemplo de la utilización de ingeniería social, que consigue información de la víctima suplantando la identidad de una empresa u organismo por internet. Se trata de una práctica muy habitual en el sector bancario.
- Adicionalmente existen multitud de ataques como **XSS**, **CSRF**, **SQL injection**, etc.

# Introducción a la ciberseguridad

## Mecanismos de defensa

Ante esta figura, ¿cómo pueden protegerse las compañías con las nuevas tecnologías?

Los principales sistemas y más conocidos son los siguientes:

- **Firewall:** sistemas de restricción de tráfico basado en reglas.
- **Sistemas IDS / IPS:** sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.
- **Honeypot:** equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.
- **SIEM:** sistemas de correlación de eventos y generación de alertas de seguridad.
- **Antimalware:** sistemas de detección de malware informático.





# Introducción a la ciberseguridad



**Las prácticas del taller se realizan sobre un entorno controlado.**

**Utilizar las técnicas mostradas en el presente taller sobre un entorno real como Internet, puede ocasionar problemas legales.**

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
- 3. Objetivos del curso**
4. Malware
5. Botnets
6. Práctica: construyendo una botnet
  1. Infección
  2. Explotación
  3. Detección y desinfección
7. Contramedidas
8. Resumen
9. Otros datos de interés

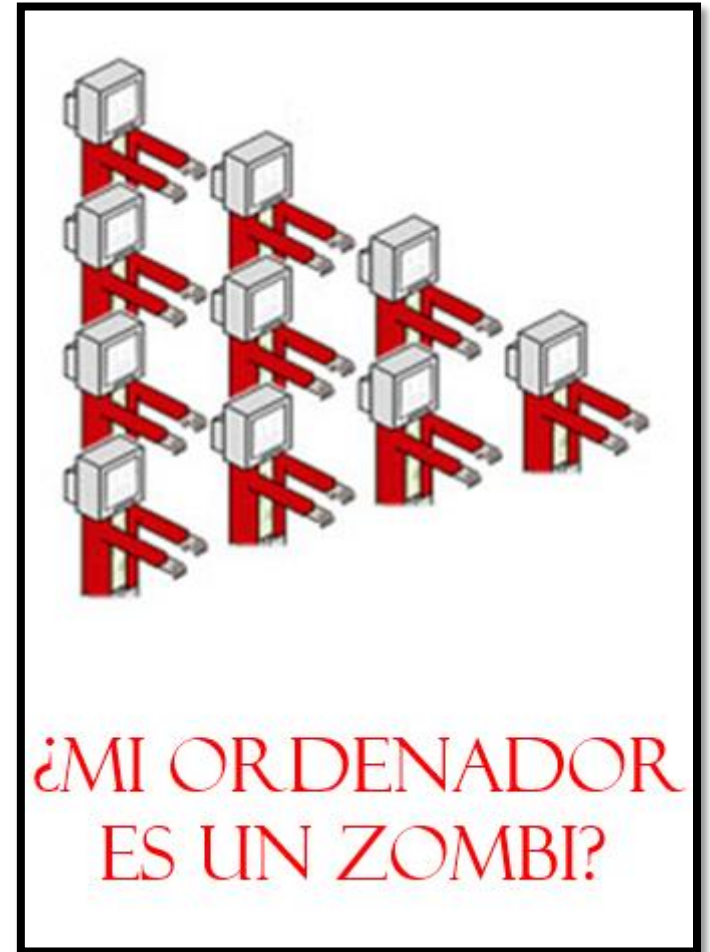
# Objetivos del curso

## ¿Qué vamos a aprender hoy?

- ¿Qué es el malware?
  - Virus.
  - Gusanos.
  - troyanos.
- Botnets:
  - Concepto.
  - Formación.
  - Ejemplos.
- ¿Cómo me protejo de las botnets?

## ¿Cómo lo vamos a aprender?

1. Teoría.
2. Práctica:
  - a. Ejercicios prácticos a lo largo de la presentación.
  - b. Práctica final “Construyendo, detectando y eliminando una botnet real”.



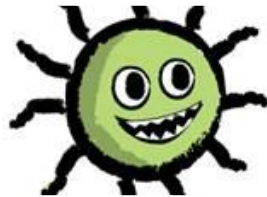
# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
- 4. Malware**
5. Botnets
6. Práctica: construyendo una botnet
  1. Infección
  2. Explotación
  3. Detección y desinfección
7. Contramedidas
8. Resumen
9. Otros datos de interés

# Malware

## ¿Qué es el malware? (I)

- El Malware es el software que tiene objetivos maliciosos. Por ejemplo:
  - Borrado de información
  - Robo de información
  - Denegación de servicio
  - **Control remoto**
  - Etc.
- Se suele clasificar por su capacidad de propagación. Las tres grandes familias son:
  - Virus
  - Troyanos
  - Gusanos



Virus



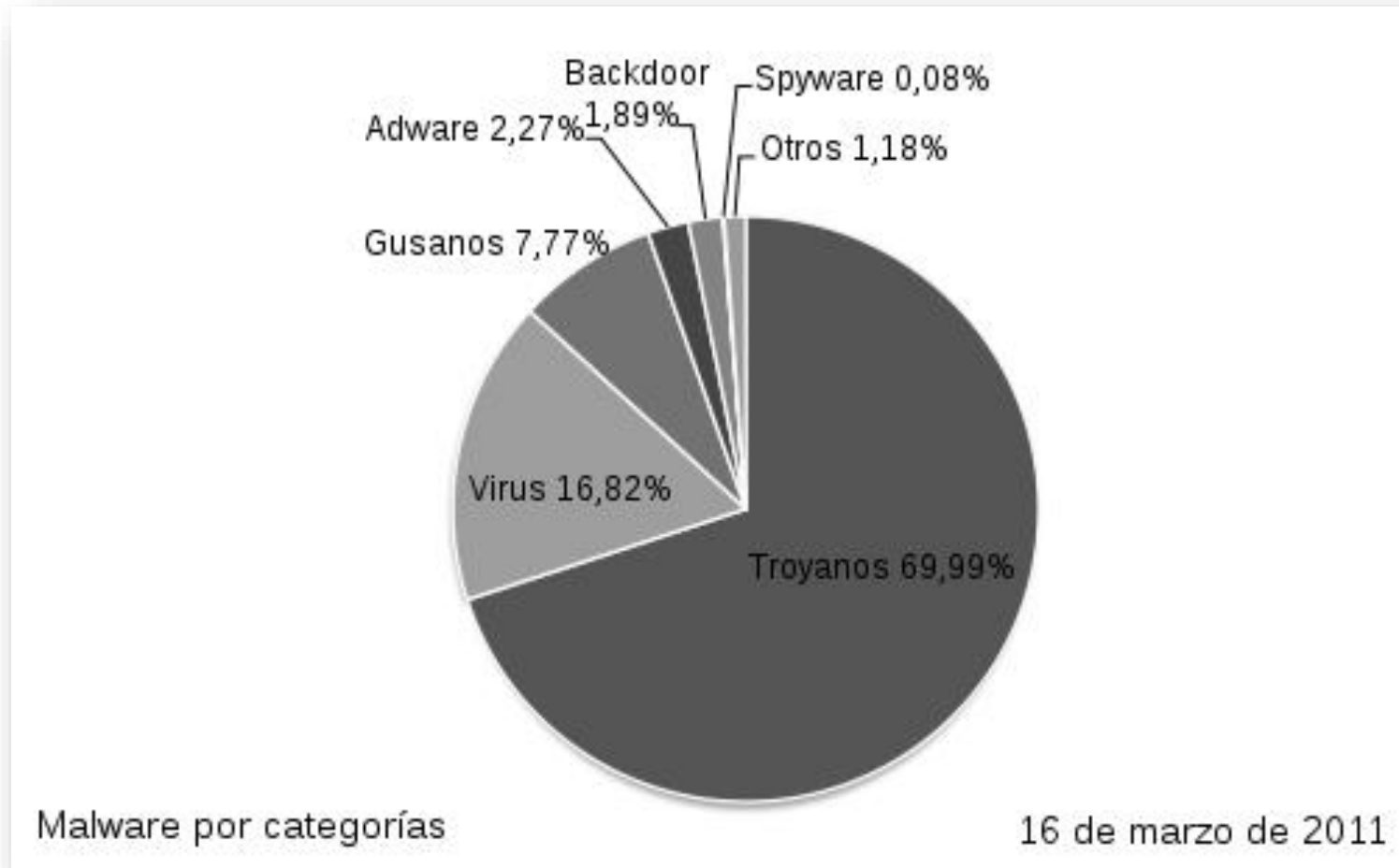
Gusanos



Troyanos

# Malware

## ¿Qué es el malware? (II)



Fuente: <http://es.wikipedia.org/wiki/Malware>



# Malware

## ¿Qué es el malware? (III): Ciclo de vida del malware

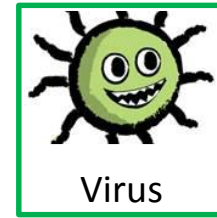


Fuente: <http://es.wikipedia.org/wiki/Malware>

# Malware

## Virus

- El virus es un tipo específico de malware.
- Es común llamar “virus” al malware, pero en realidad es solo un subconjunto.
- Su nombre viene por su parecido a los virus reales (infección y propagación).
- Para su propagación necesitan que cierta interacción por parte del usuario.



Virus

Gusanos

Troyanos

### VIRUS

Infecta otros programas

Capacidad de mutación

Capacidad de cifrado



Altera datos

Corrompe ficheros

Auto-propagación

# Malware



Virus



Gusanos



Troyanos

## Gusanos (worms)

- Los gusanos (habitualmente llamados worms) son **programas maliciosos** que se propagan por la red de forma automática.
- Los gusanos se transmiten explotando vulnerabilidades de los sistemas sin que el usuario tenga que interactuar con ellos de ninguna manera.
- Este tipo de malware es habitual en teléfonos, ya que este tipo de dispositivo conectado es idóneo para una propagación rápida.
- Un gusano muy famoso, **Stuxnet**, es un malware supuestamente desarrollado por Israel y Estados Unidos diseñado para infectar **infraestructuras críticas** que infectó a 60.000 equipos en Irán.



# Malware



Virus



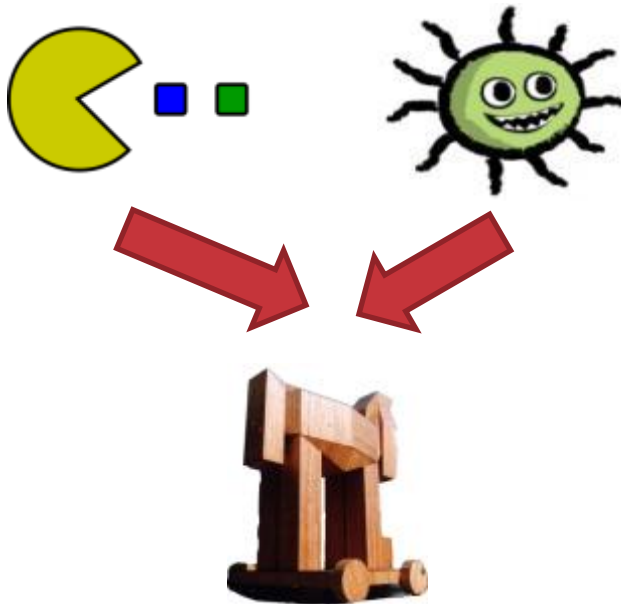
Gusanos



Trojanos

## Trojanos

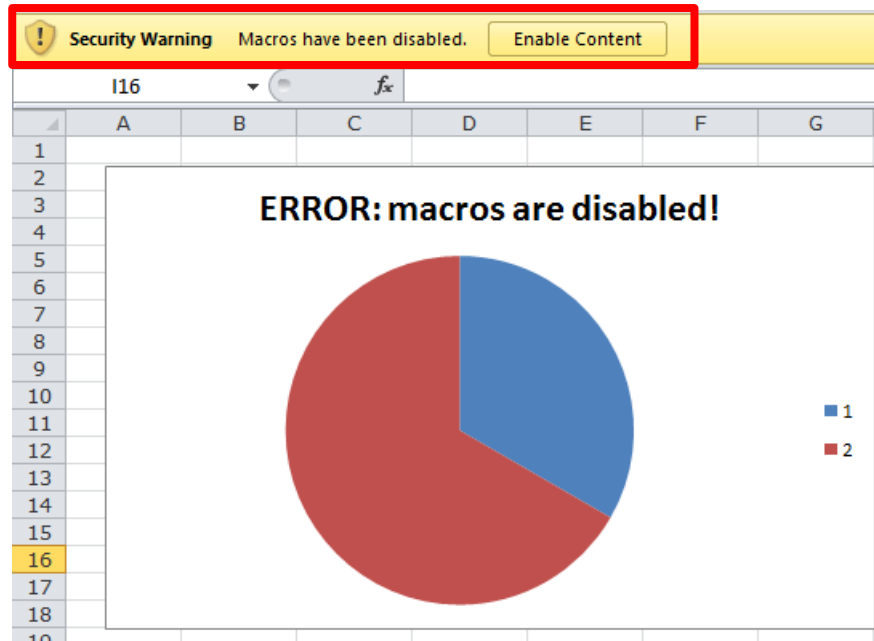
- Un **troyano** o caballo de Troya es un **programa malicioso** (malware) que se presenta al usuario como un programa **aparentemente inofensivo**.
- El término proviene de la **Odisea** de Homero.



# Malware

## Ejemplo de Virus de Macro “troyanizado”

- El fichero “estadisticas\_uso\_de\_software.xls” contiene un programa malicioso. En apariencia, el fichero **parece contener información inofensiva**.
- Al abrir el fichero, Microsoft Excel avisa del contenido de código ejecutable. Sin embargo, **la mayoría de los usuarios seguirá adelante con la ejecución:**

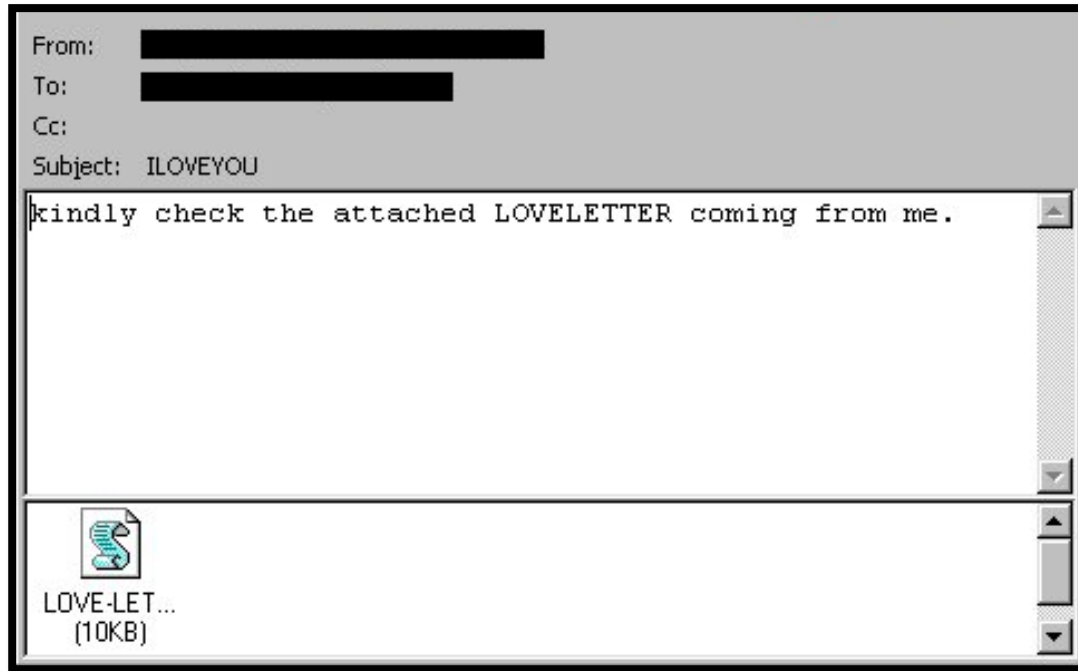


Ejecuta la macro para ver lo que ocurre... No te preocupes, realmente es inofensivo



# Malware

## Ejemplo de gusano: “I love you” (I)



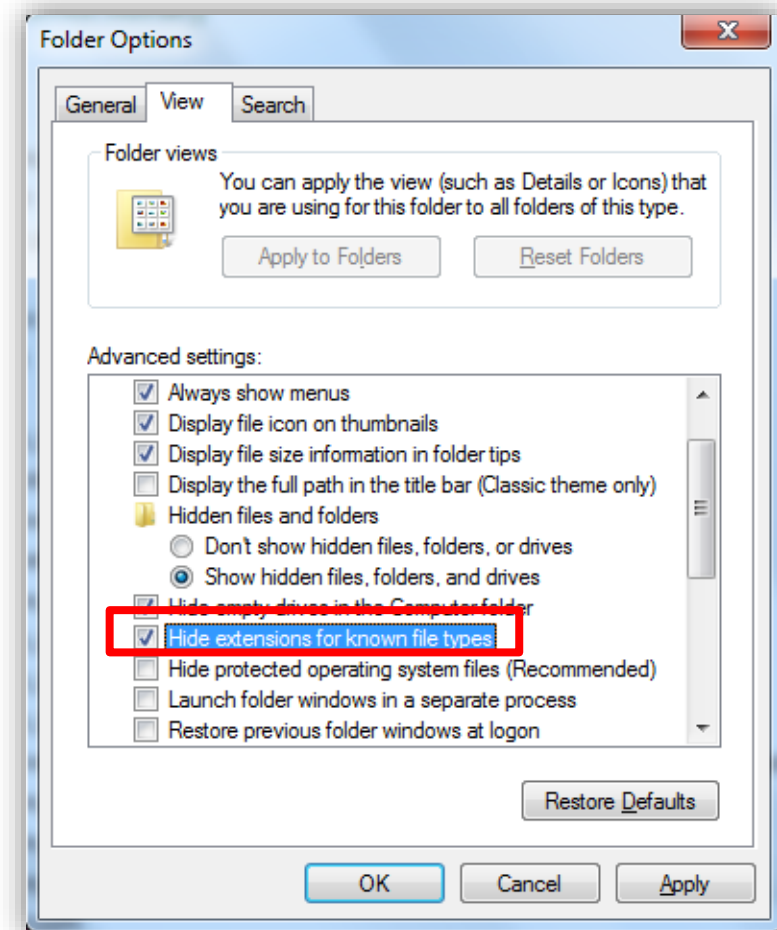
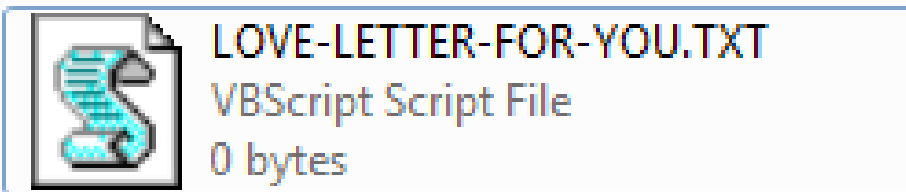
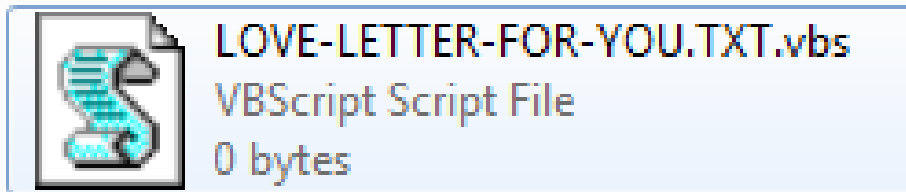
- El gusano **se propaga automáticamente**, mandando un correo electrónico a todos los contactos de Outlook.
- Tras propagarse, causa graves daños en los ficheros del ordenador infectado, borrando y sobrescribiendo ficheros.



# Malware

## Ejemplo de gusano: “I love you” (II)

- El nombre del fichero ejecutable, **“LOVE-LETTER-FOR-YOU.TXT.vbs”**, aprovechaba que Windows oculta las extensiones conocidas para parecer un fichero de texto:



¿Cómo evitarlo?

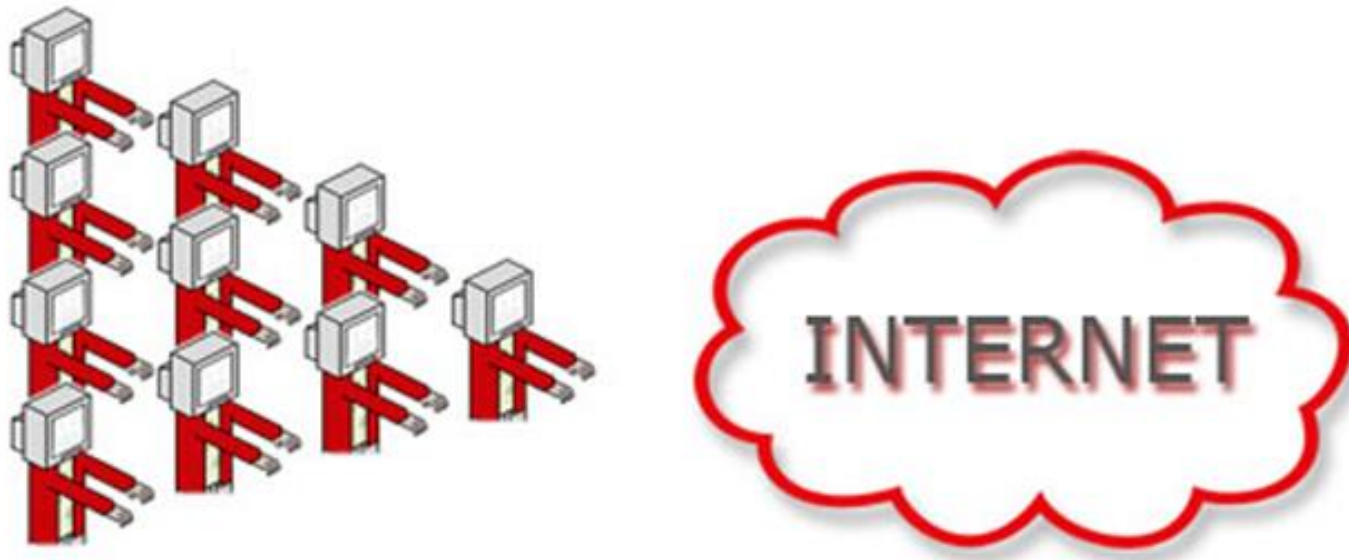
# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Malware
- 5. Botnets**
6. Práctica: construyendo una botnet
  1. Infección
  2. Explotación
  3. Detección y desinfección
7. Contramedidas
8. Resumen
9. Otros datos de interés

# Botnets

## Botnets (I)

- Una botnet es una **red de ordenadores infectados** controlados por un ciberdelincuente.



- Los ordenadores infectados obedecerán a las órdenes del ciberdelincuente, de forma que éste dispone de un “ejército” de ordenadores listos para realizar operaciones maliciosas en Internet en cualquier momento.

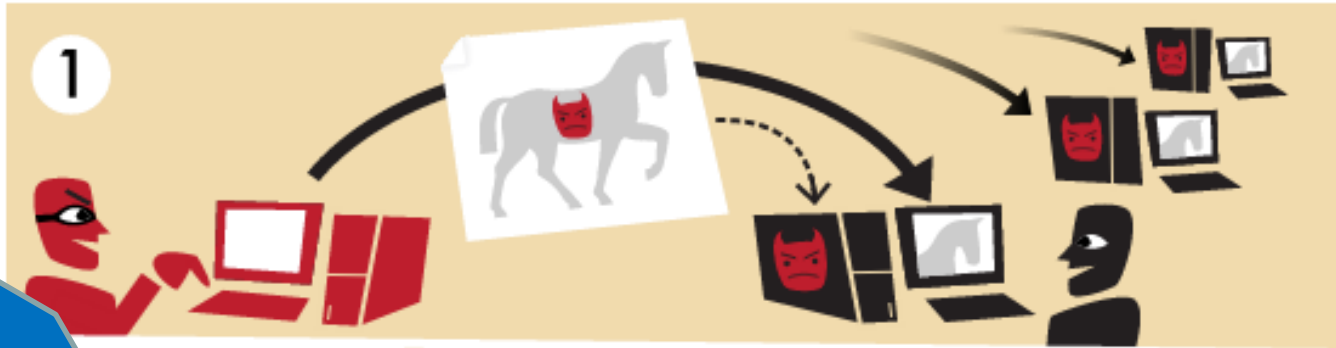
# Botnets

## Botnets (II): ciclo de vida



# Botnets

## Botnets (III): ciclo de vida

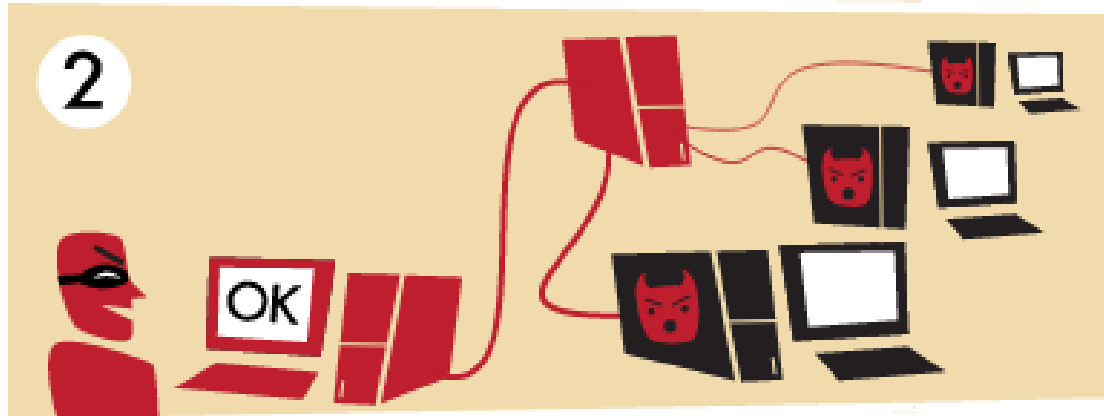


1

Infección: el atacante infecta ordenadores personales de usuarios por medio de troyanos.

# Botnets

## Botnets (IV): ciclo de vida



2

El atacante forma así una red de miles de ordenadores controlados por un servidor *Command and Control*.

# Botnets

## Botnets (V): ciclo de vida



3

Una tercera parte malintencionada compra acceso a la botnet para realizar acciones maliciosas, como por ejemplo:

- Ataques de denegación de servicio distribuidos (DDoS)
- Envío de Spam
- Fraude de clicks

# Botnets

## Botnets (VI): ciclo de vida



4

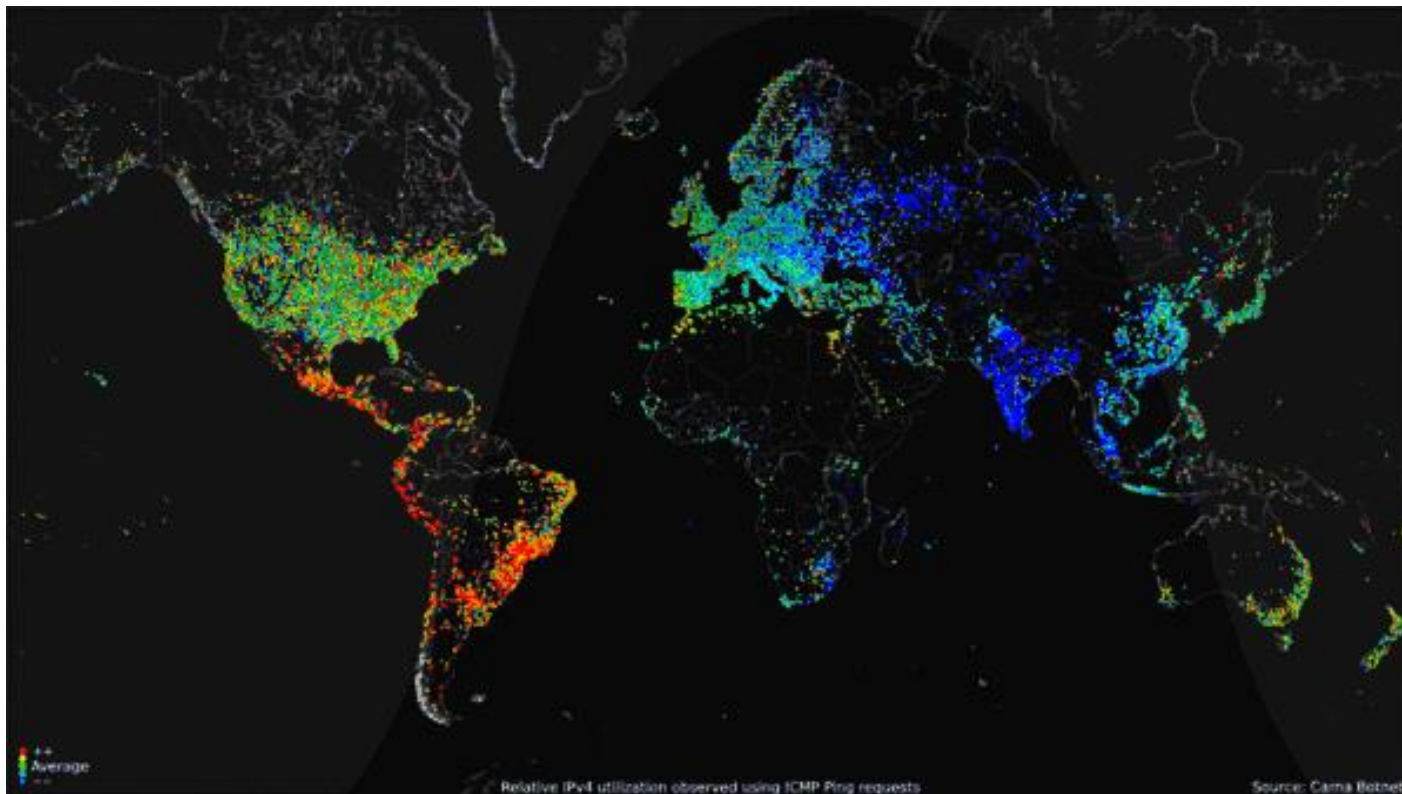
Se lanza el ataque distribuido. En este ejemplo, se utiliza la botnet para enviar millones de correos publicitarios.



# Botnets

## Botnets (VII): Ejemplos

- Carna Botnet:



- Carna Botnet fue una red de 420.000 dispositivos infectados.

# Botnets

## Botnets (VIII): Ejemplos

- ZeroAccess botnet
  - La botnet ZeroAccess fue una botnet especializada en minería de bitcoin y click fraudulento.
  - Se estima que la red minó unos 2,7 millones de dólares en bitcoins.



El bitcoin es una moneda electrónica creada en 2009. La generación (“minería”) de bitcoins necesita **potencia computacional**, algo que se puede conseguir con una red de ordenadores distribuidos.

Fuentes: <http://www.reuters.com/article/2014/02/24/us-bitcoin-security-idUSBREA1N1JO20140224> y <https://bitcoin.org/es/como-funciona>

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Malware
5. Botnets
- 6. Práctica: construyendo una botnet**
  1. Infección
  2. Explotación
  3. Detección y desinfección
7. Contramedidas
8. Resumen
9. Otros datos de interés

# Introducción a la ciberseguridad



Las prácticas del taller se realizan sobre un entorno controlado. Utilizar las **técnicas** mostradas en el presente taller **sobre un entorno real como Internet**, puede ocasionar **problemas legales**.

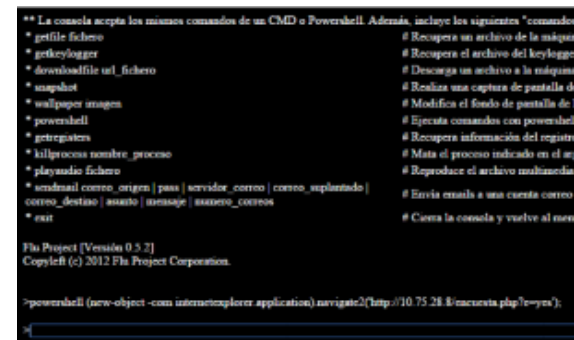
# Práctica: “Construyendo una botnet”

## Introducción

- En esta práctica utilizaremos el troyano **Flu Project** para construir una botnet.



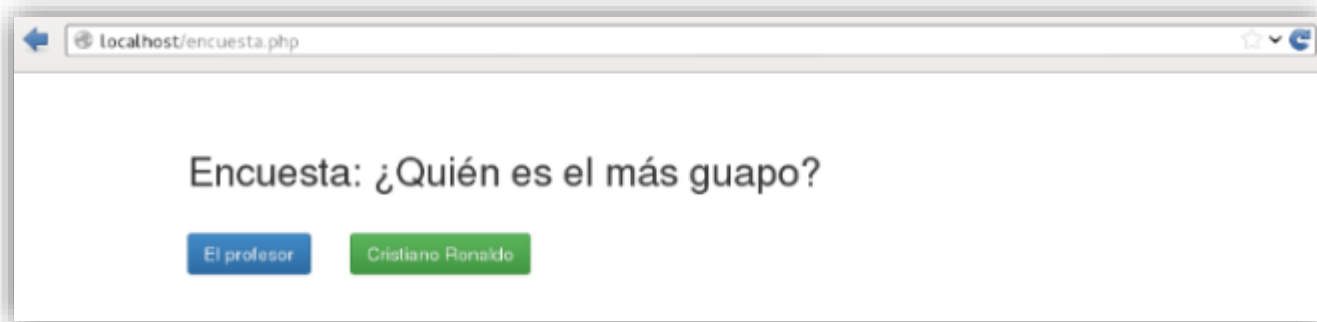
- El software Flu, desarrollado por Flu Project (<http://www.flu-project.com>), es una herramienta tipo troyano que permite controlar máquinas de manera remota.
- Se trata de una aplicación Open Source, desarrollada como prueba de concepto para analizar el funcionamiento de herramientas maliciosas y diseñar medidas anti-malware.



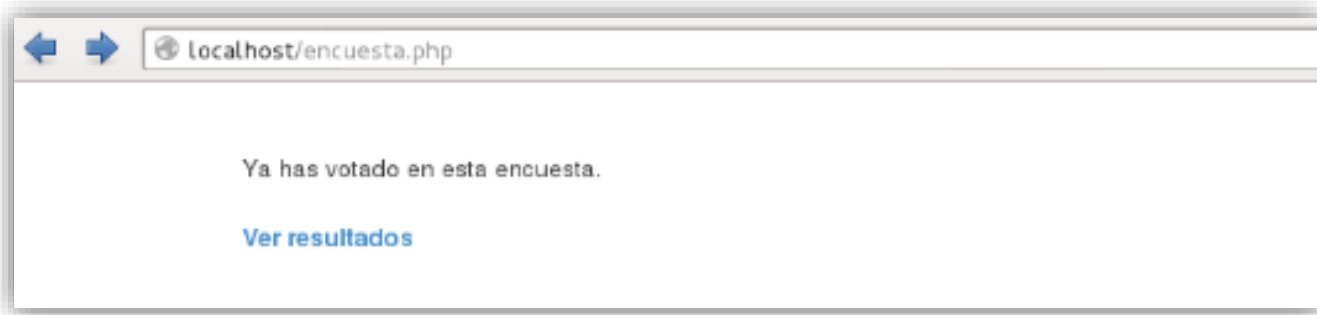
# Práctica: “Construyendo una botnet”

## Objetivo

- Objetivo: realizar un fraude de clics para falsear los resultados de una encuesta:



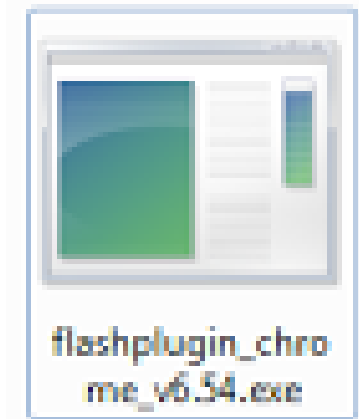
- El pirata informático quiere falsear el resultado de esta encuesta. Podría intentar votar muchas veces, pero como suele ser habitual, no es posible votar más de una vez:



# Práctica: “Construyendo una botnet”

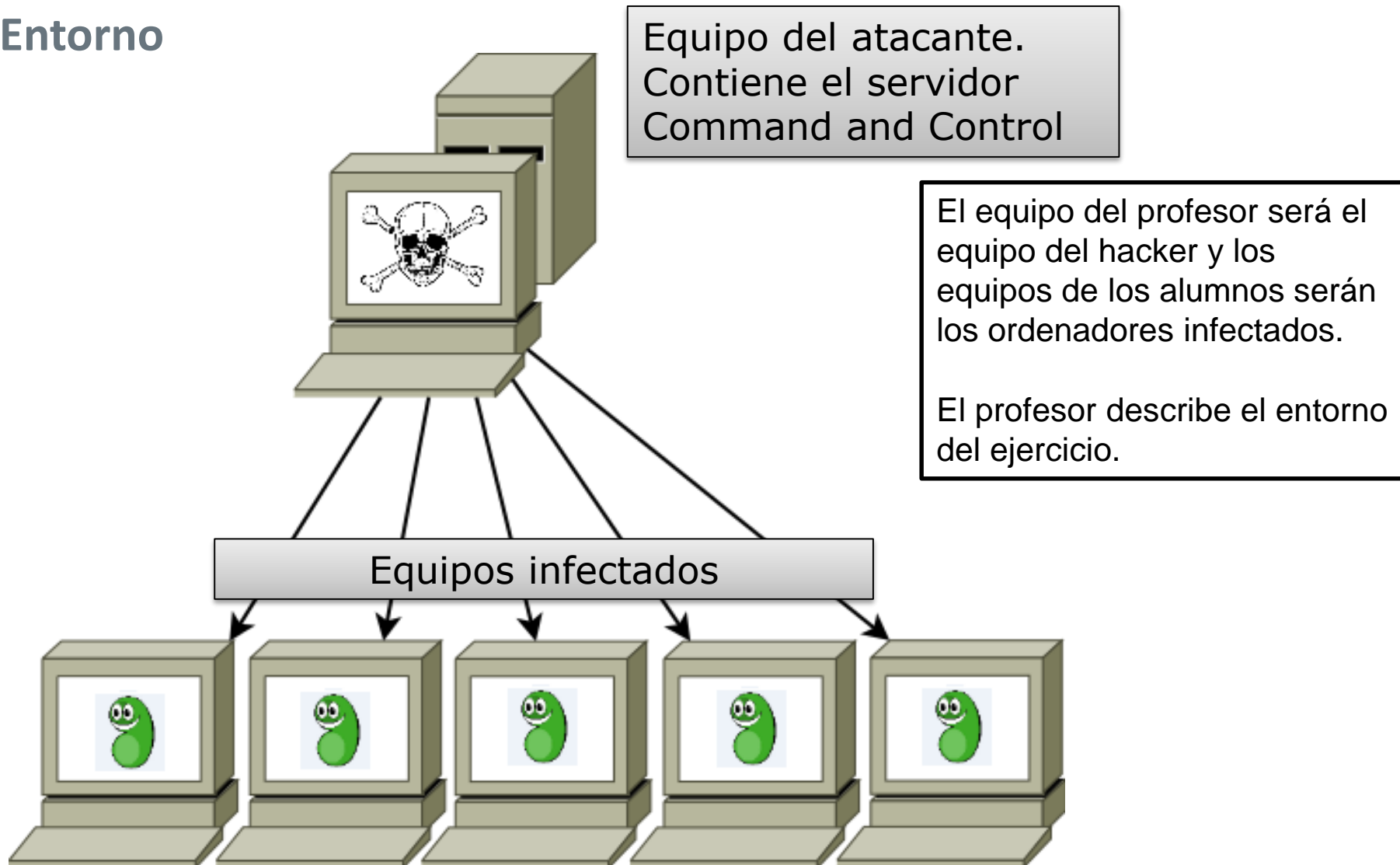
## Funcionamiento

- La botnet está compuesta por dos elementos:
  - **Ciente:** programa malware que se instala en ordenadores comprometidos. Recibe las órdenes del servidor Command and Control.
    - Poniéndole un nombre engañoso, “flashplugin\_chrome\_v6.54.exe”, podemos engañar al usuario.
  - Servidor: servidor **Command and Control** que nos permitirá controlar la red de ordenadores infectados.



# Práctica: “Construyendo una botnet”

## Entorno





# Práctica: “Construyendo una botnet”

## Herramientas



El conocido servidor web **Apache HTTP Server** permitirá al atacante instalar la aplicación Command and Control así como una página web maliciosa para infectar a los usuarios.



El servidor Command and Control de **Flu** se instala sobre el servidor Apache



**Beef** es una herramienta que permite tomar el control de navegadores web. Se usará para infiltrar el troyano Botnet.

Fuentes: <http://httpd.apache.org/>, <http://www.flu-project.com/> y <http://beefproject.com/>

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Malware
5. Botnets
6. Práctica: construyendo una botnet
  - 1. Infección**
  2. Explotación
  3. Detección y desinfección
7. Contramedidas
8. Resumen
9. Otros datos de interés

# Práctica: “Construyendo una botnet”

## Paso 1: Infección (I)

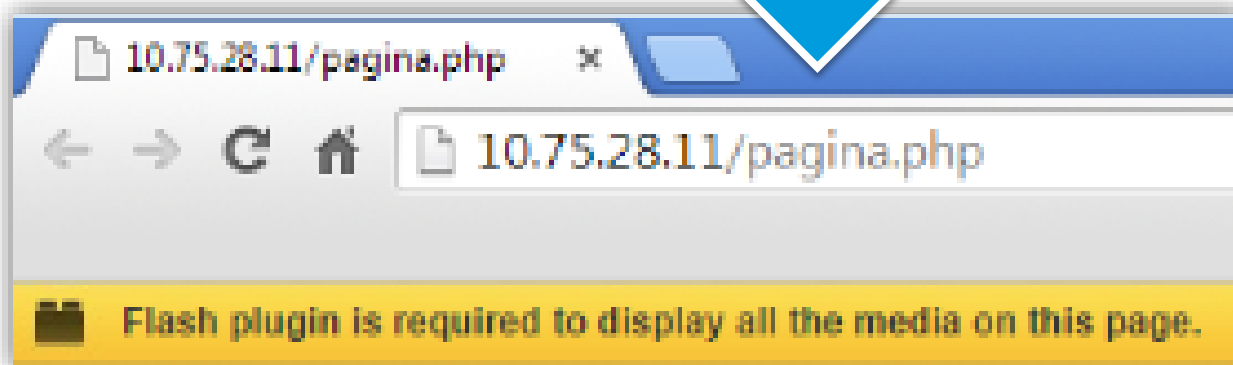
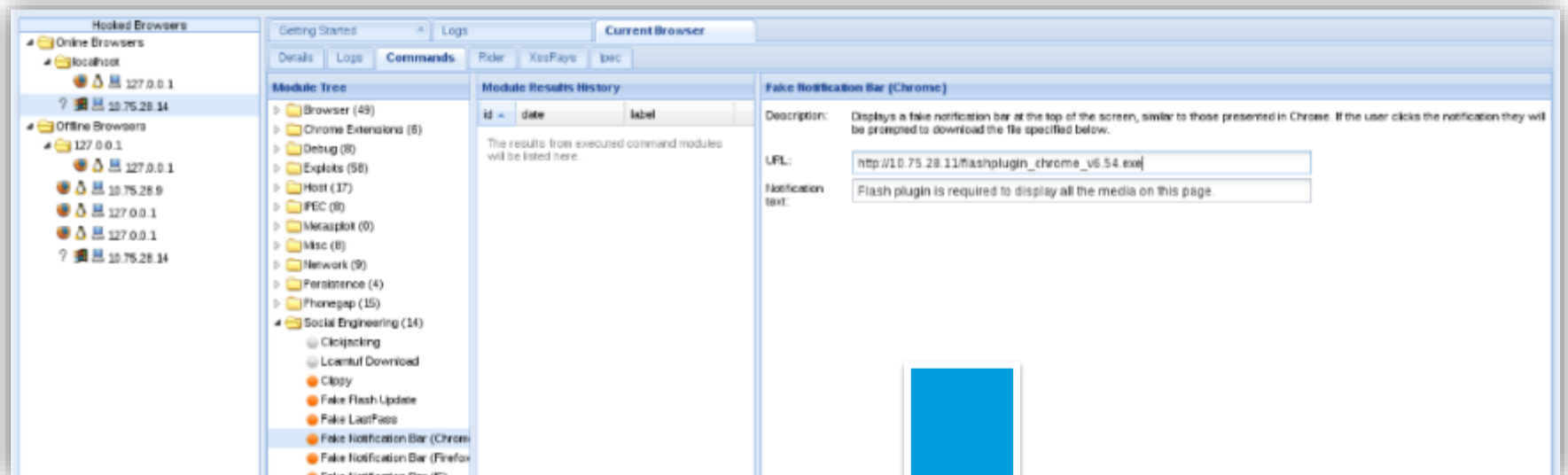
- Conectarse a la página web del atacante:



# Práctica: “Construyendo una botnet”

## Paso 1: Infección (II)

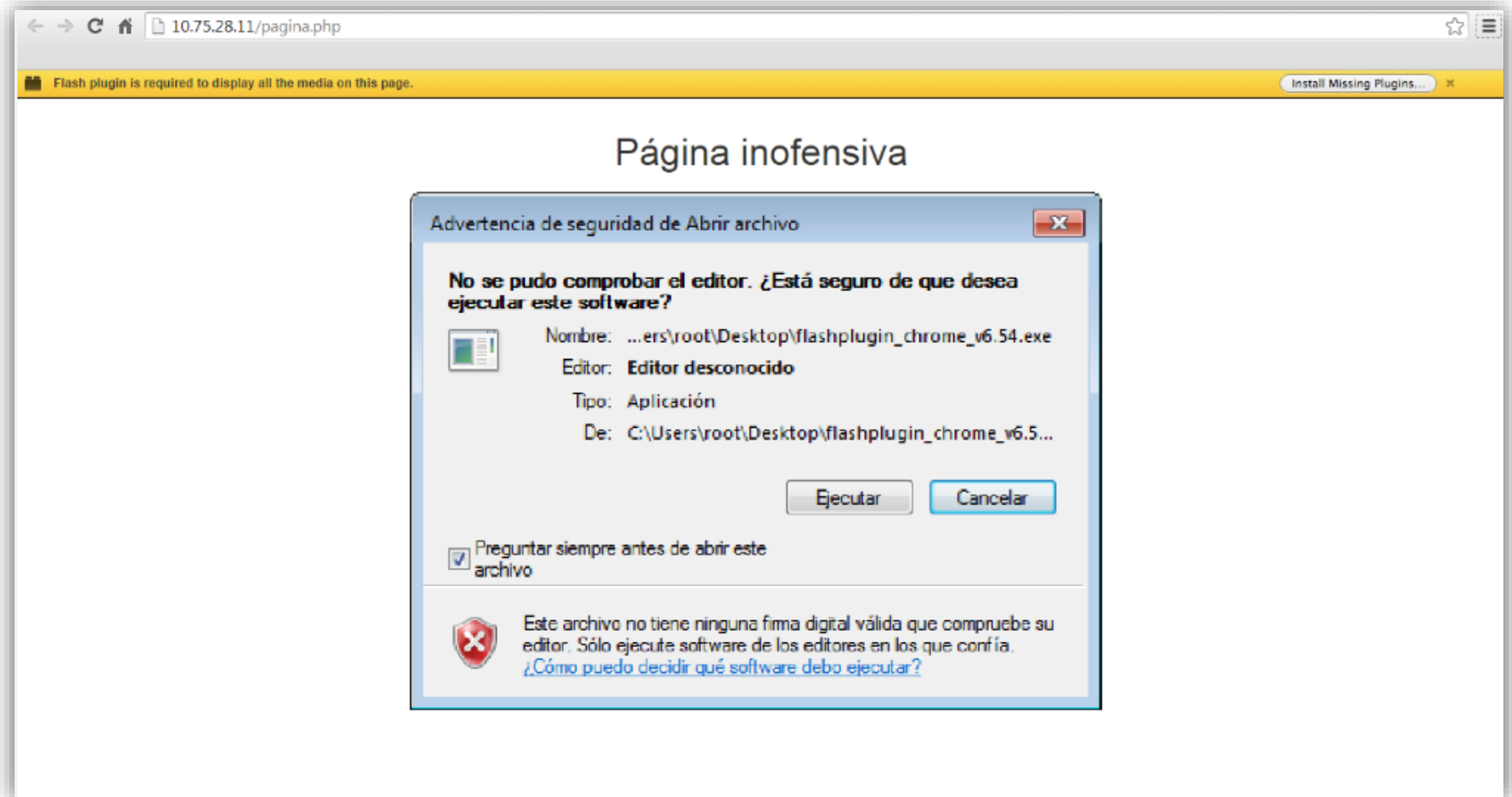
- El atacante utiliza Beef para mostrar un mensaje engañoso al usuario:



# Práctica: “Construyendo una botnet”

## Paso 1: Infección (III)

- El usuario se descarga el programa y lo ejecuta:



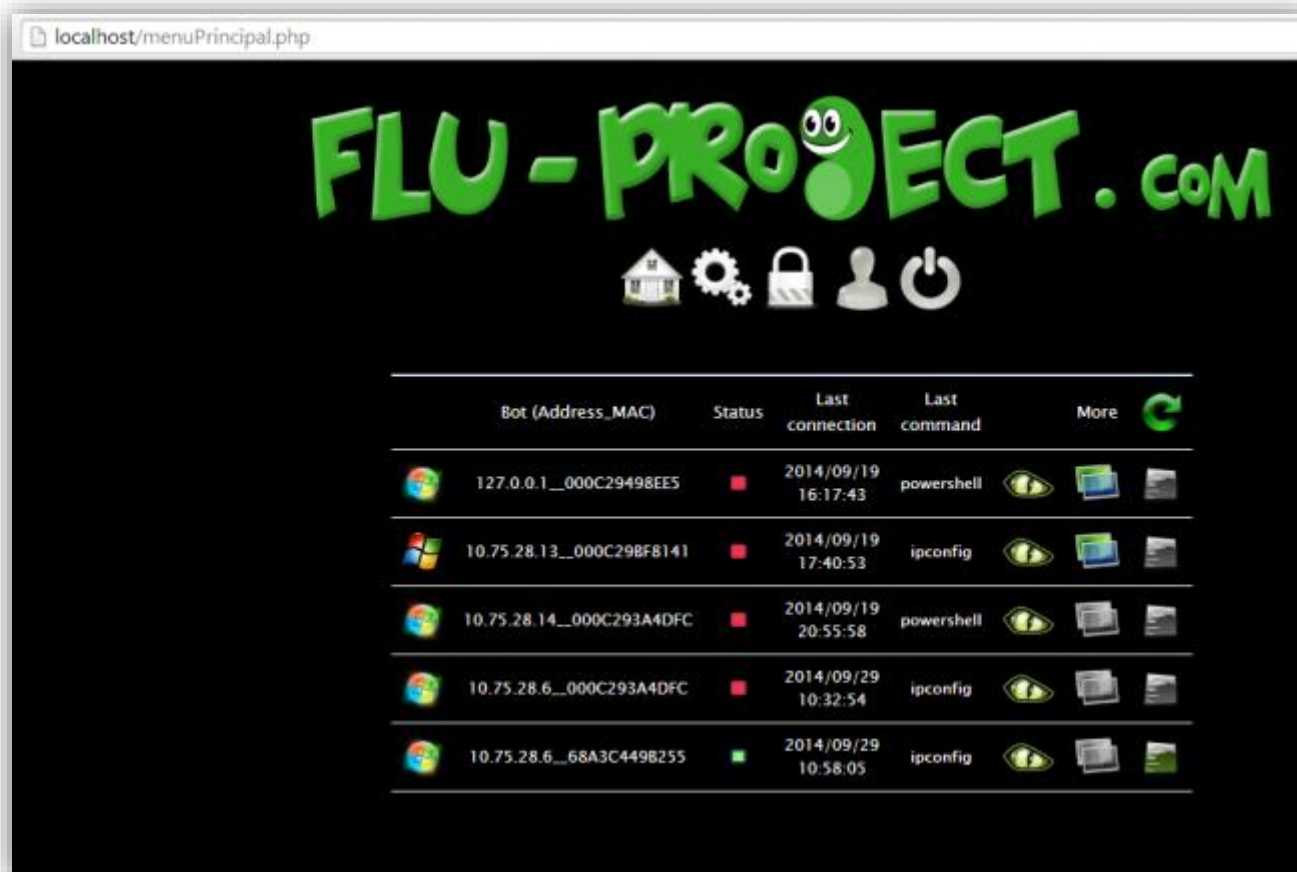
# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Malware
5. Botnets
6. Práctica: construyendo una botnet
  1. Infección
  - 2. Explotación**
  3. Detección y desinfección
7. Contramedidas
8. Resumen
9. Otros datos de interés

# Práctica: “Construyendo una botnet”

## Paso 2: Explotación (I)

- El atacante puede ahora controlar el ordenador de forma remota mediante la herramienta **Command and Control** de Flu:



# Práctica: “Construyendo una botnet”

## Paso 2: Explotación (II)

- La herramienta dispone de un intérprete de órdenes que permite ejecutar comandos en la máquina remota y recibir la salida.
- Ejemplo: el comando “**ipconfig**” nos permite obtener información sobre el estado de la red en la máquina remota:



```
>ipconfig
Configuraci?n IP de Windows

Adaptador de Ethernet Conexi?n de red Bluetooth:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS espec?fico para la conexi?n. . . :

Adaptador de Ethernet Conexi?n de ?rea local:

Sufijo DNS espec?fico para la conexi?n. . . : ascmadlab.com
V?nculo: direcci?n IPv6 local. . . : fe80::d48e:c63c:3e3e:25a5%11
Direcci?n IPv4. . . . . : 10.75.28.6
M?scara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada. . . . . : 10.75.28.1

Adaptador de t?nel isatap.ascmadlab.com:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS espec?fico para la conexi?n. . . : ascmadlab.com

Adaptador de t?nel Conexi?n de ?rea local* 6:

Sufijo DNS espec?fico para la conexi?n. . . :
Direcci?n IPv6. . . . . : 2001:0:9d38:6ab8:142c:2297:2be0:301d
V?nculo: direcci?n IPv6 local. . . : fe80::142c:2297:2be0:301d%13
Puerta de enlace predeterminada. . . . . :

Adaptador de t?nel isatap.{20C59A85-990E-45A0-AE5D-8B88F45F14E9}:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS espec?fico para la conexi?n. . . :

>
```



# Práctica: “Construyendo una botnet”

## Paso 2: Explotación (III)

- El troyano también registra todas las pulsaciones de teclado (**keylogger**). La herramienta permite al atacante obtener estos datos para, por ejemplo, robar contraseñas.



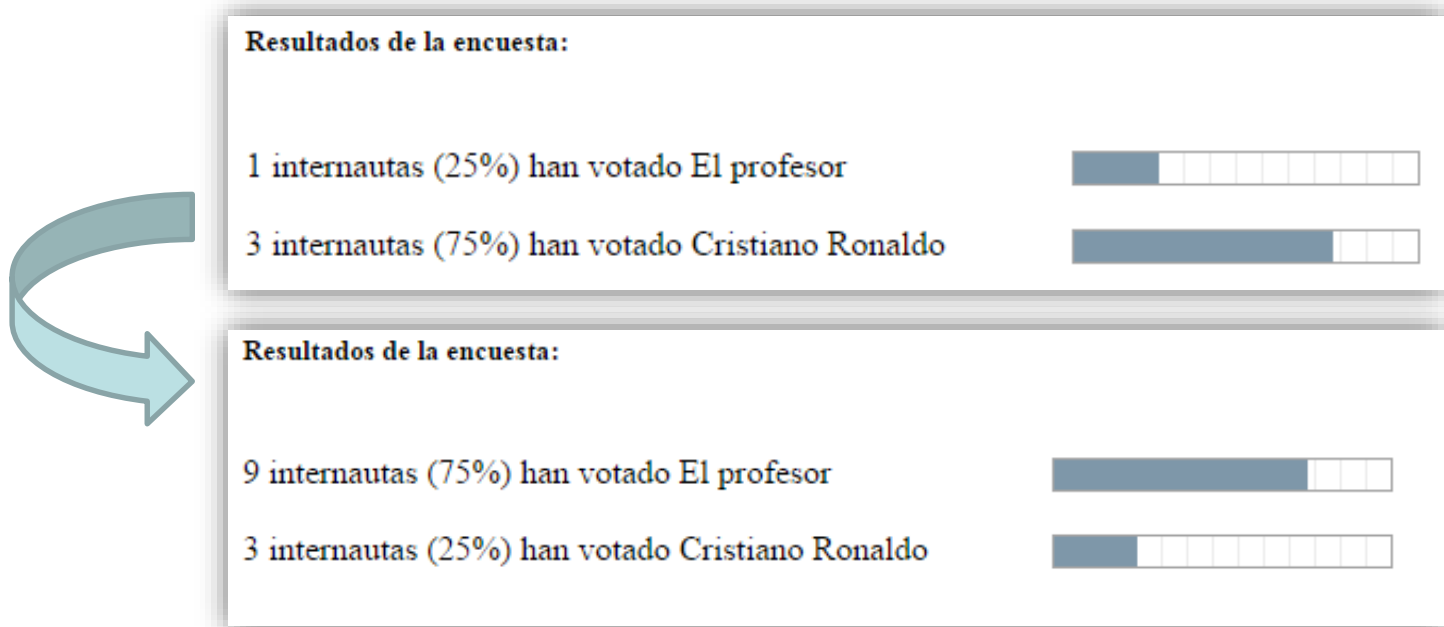
# Práctica: “Construyendo una botnet”

## Paso 2: Explotación (IV)

- Utilizaremos ahora nuestra botnet para falsear los resultados de la encuesta.
  - Un comando permite navegar a una página sin que el usuario de la máquina infectada se dé cuenta:

```
>powershell (new-object -com internetexplorer.application).navigate2('http://10.75.28.8/encuesta.php?c=yes');
```

- Haciéndolo en cada máquina, podemos realizar un gran número de votaciones y falsear el resultado de la encuesta:



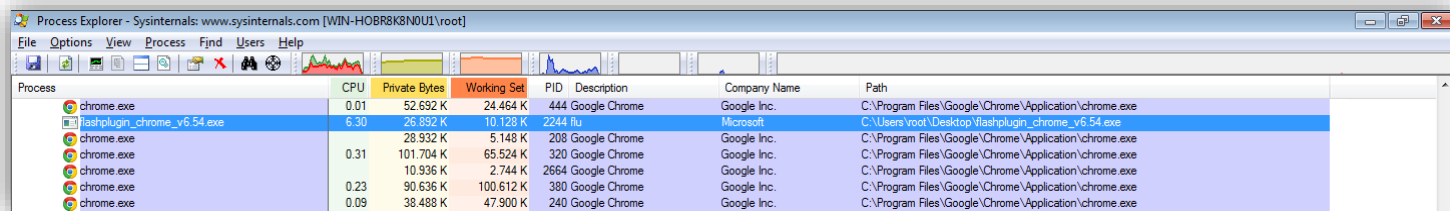
# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Malware
5. Botnets
6. Práctica: “Construyendo una botnet”
  1. Infección
  2. Explotación
  - 3. Detección y desinfección**
7. Contramedidas
8. Resumen
9. Otros datos de interés

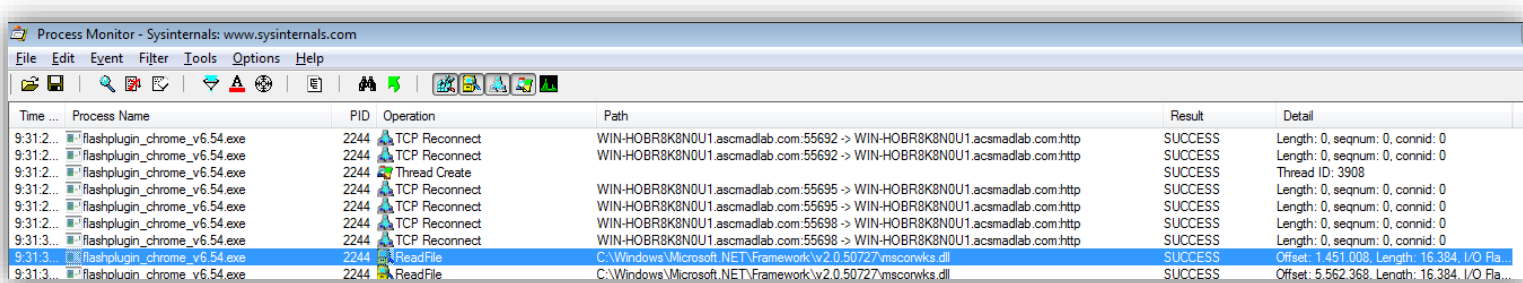
# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (I)

- Cualquier antivirus debería detectar este virus, pero haremos una detección manual para analizar su comportamiento.
- El troyano puede intentar ocultarse en el administrador de tareas (haciendo uso de un rootkit bajo una cuenta con privilegios de administración), pero el programa **Process Explorer** (herramienta comprada por Microsoft) sí que lo lista (**flashplugin\_chrome\_v6.54.exe**):



- La herramienta **Process Monitor** permite ver las acciones realizadas por un proceso. Se puede ver en la siguiente captura de pantalla la actividad del troyano:



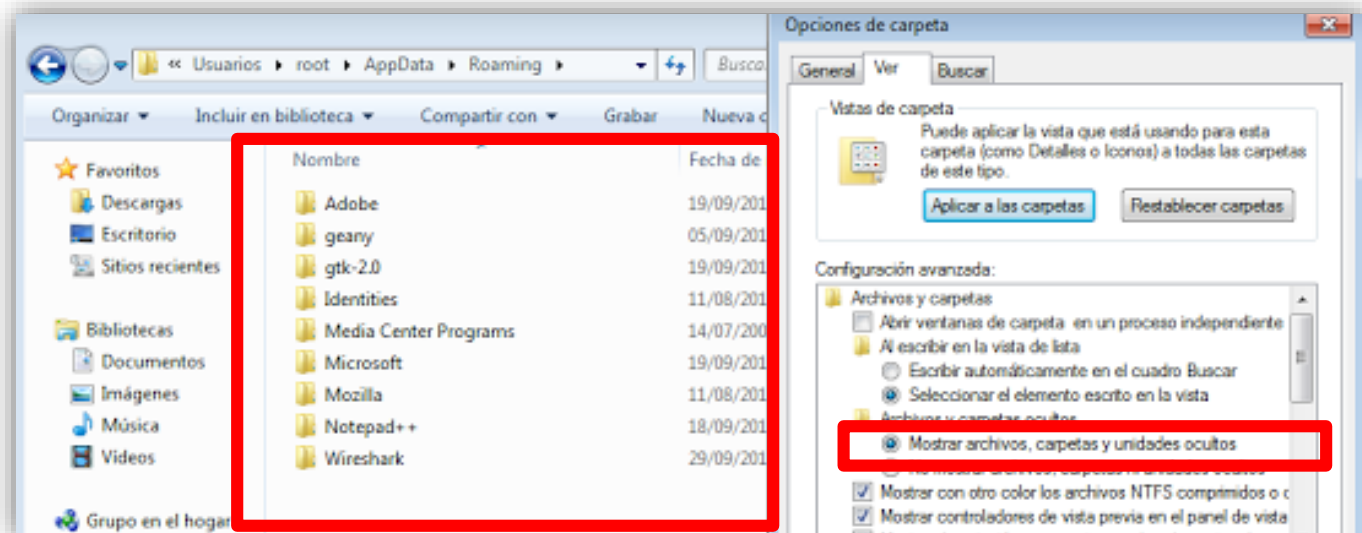
# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (II)

- Mirando en detalle los eventos del proceso, se puede observar que periódicamente escribe un fichero:

10:08:...	flashplugin_chrome_v6.54.exe	2244	TCP Send	WIN-HOBR8K8N0U1.ascmadlab.com:57900 -> WIN
10:08:...	flashplugin_chrome_v6.54.exe	2244	TCP Receive	WIN.HOBR8K8N0U1.ascmadlab.com:57900 -> WIN
10:08:...	flashplugin_chrome_v6.54.exe	2244	CreateFile	C:\Users\root\AppData\Roaming\abamvfavkv.bt
10:08:...	flashplugin_chrome_v6.54.exe	2244	QueryStandardInformationFile	C:\Users\root\AppData\Roaming\abamvfavkv.bt
10:08:...	flashplugin_chrome_v6.54.exe	2244	WriteFile	C:\Users\root\AppData\Roaming\abamvfavkv.bt
10:08:...	flashplugin_chrome_v6.54.exe	2244	CloseFile	C:\Users\root\AppData\Roaming\abamvfavkv.bt
10:08:...	flashplugin_chrome_v6.54.exe	2244	TCP Send	WIN.HOBR8K8N0U1.ascmadlab.com:57900 -> WIN

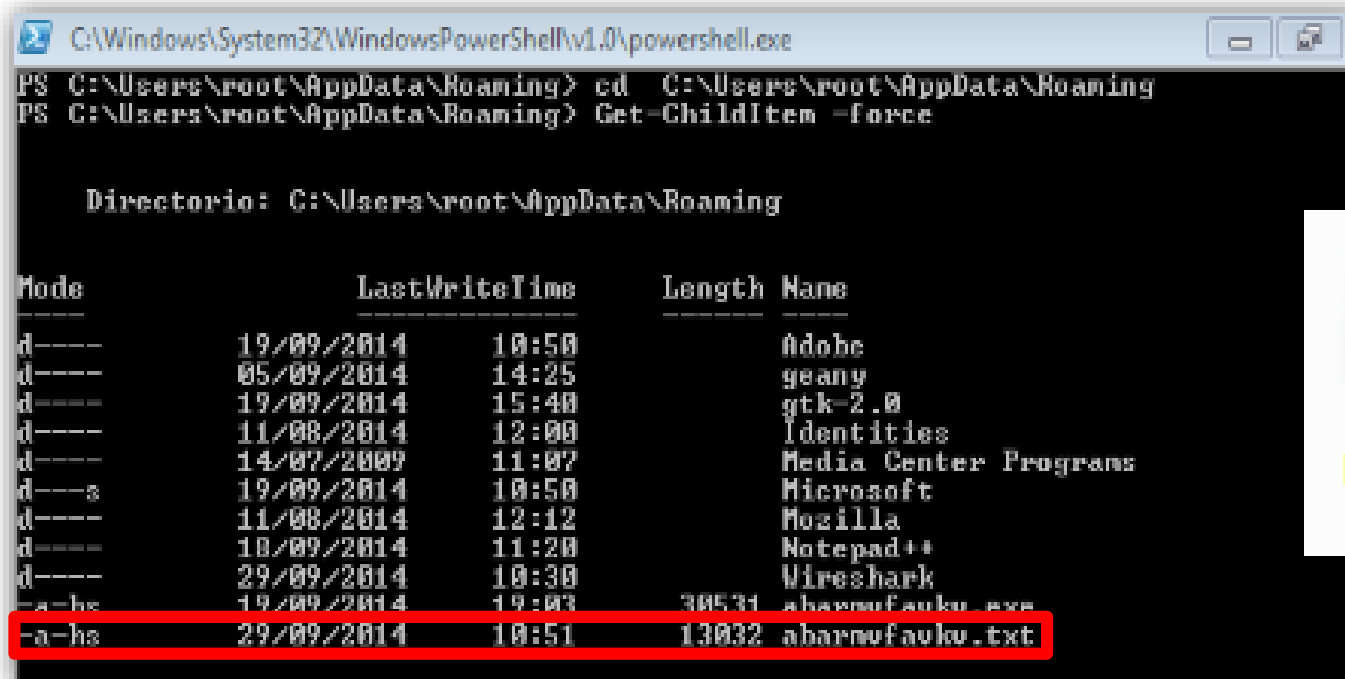
- Sin embargo, parece que la carpeta no contiene este fichero, incluso con la opción de “mostrar archivos ocultos”:



# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (III)

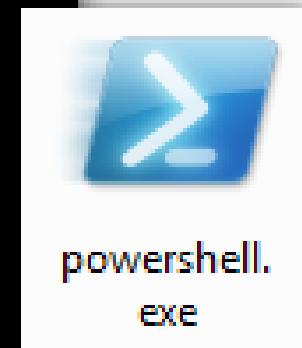
- Esto ocurre porque el archivo está marcado como archivo oculto de sistema, ocultándose así de forma más efectiva. Para ver este tipo de archivos, se puede utilizar también la línea de comandos de Windows, **PowerShell**:
  - 1) Navegamos hasta C:\Users\root\AppData\Roaming
  - 2) Ejecutamos “Get-ChildItem **-force**”, dónde “**force**” indica que se desea forzar la visualización de todos los archivos, incluidos los archivos ocultos y/o de sistema.



```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Users\root\AppData\Roaming> cd C:\Users\root\AppData\Roaming
PS C:\Users\root\AppData\Roaming> Get-ChildItem -force

Directorio: C:\Users\root\AppData\Roaming

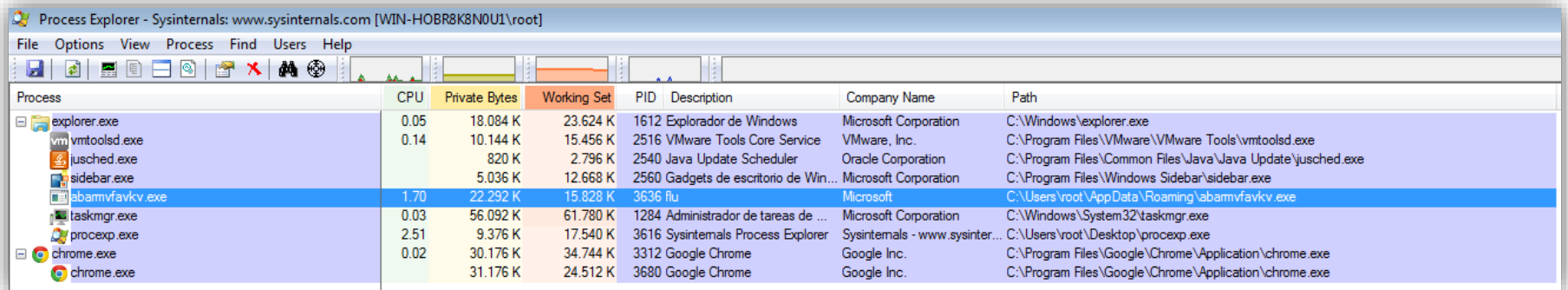
Mode                LastWriteTime         Length Name
----                -
d-----          19/09/2014         10:50      Adobe
d-----          05/09/2014         14:25      geany
d-----          19/09/2014         15:40      gtk-2.0
d-----          11/08/2014         12:00      Identities
d-----          14/07/2007         11:07      Media Center Programs
d-----          19/09/2014         10:50      Microsoft
d-----          11/08/2014         12:12      Mozilla
d-----          10/09/2014         11:20      Notepad++
d-----          29/09/2014         10:30      Wireshark
-a-hs          19/09/2014         30531  abarnwfauku.exe
-a-hs          29/09/2014         13032  abarnwfauku.txt
```



# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (IV)

- Si reiniciamos el ordenador, veremos que el proceso ha cambiado de nombre y de ubicación. Ahora, se llama **abarmvavkv.exe**:



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Path
explorer.exe	0.05	18.084 K	23.624 K	1612	Explorador de Windows	Microsoft Corporation	C:\Windows\explorer.exe
vmtoolsd.exe	0.14	10.144 K	15.456 K	2516	VMware Tools Core Service	VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
jusched.exe		820 K	2.796 K	2540	Java Update Scheduler	Oracle Corporation	C:\Program Files\Common Files\Java\Java Update\jusched.exe
sidebar.exe		5.036 K	12.668 K	2560	Gadgets de escritorio de Win...	Microsoft Corporation	C:\Program Files\Windows Sidebar\sidebar.exe
abarmvavkv.exe	1.70	22.292 K	15.828 K	3636	flu	Microsoft	C:\Users\root\AppData\Roaming\abarmvavkv.exe
taskmgr.exe	0.03	56.092 K	61.780 K	1284	Administrador de tareas de ...	Microsoft Corporation	C:\Windows\System32\taskmgr.exe
procexp.exe	2.51	9.376 K	17.540 K	3616	Sysinternals Process Explorer	Sysinternals - www.sysinter...	C:\Users\root\Desktop\procexp.exe
chrome.exe	0.02	30.176 K	34.744 K	3312	Google Chrome	Google Inc.	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		31.176 K	24.512 K	3680	Google Chrome	Google Inc.	C:\Program Files\Google\Chrome\Application\chrome.exe

- Esta característica (cambio de nombre y/o de ubicación) es una característica típica de los virus que disminuye la probabilidad de ser detectado.



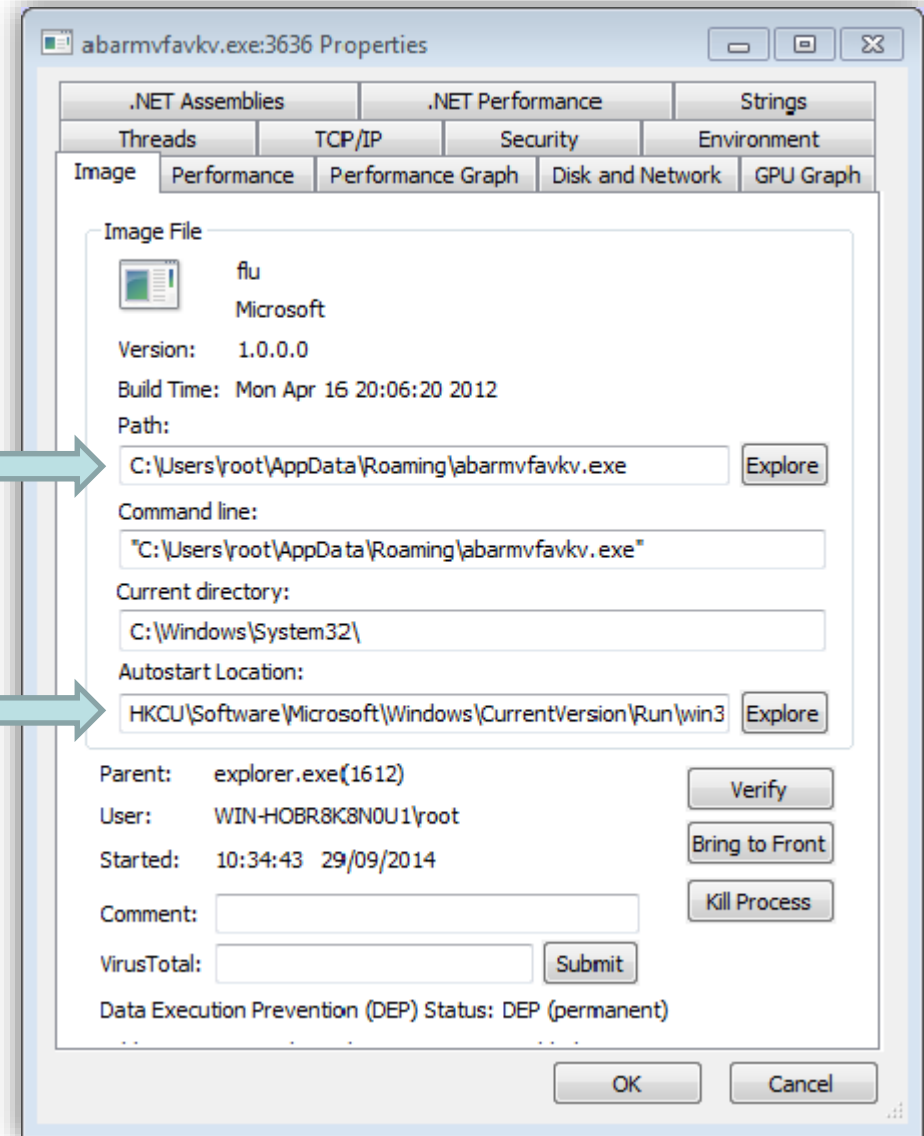
# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (V)

- Abriendo las propiedades del proceso, se obtiene información interesante:

Ruta del archivo ejecutable origen del proceso (.exe).

Entrada del registro que define el autoarranque (el troyano se ejecuta al iniciarse Windows).

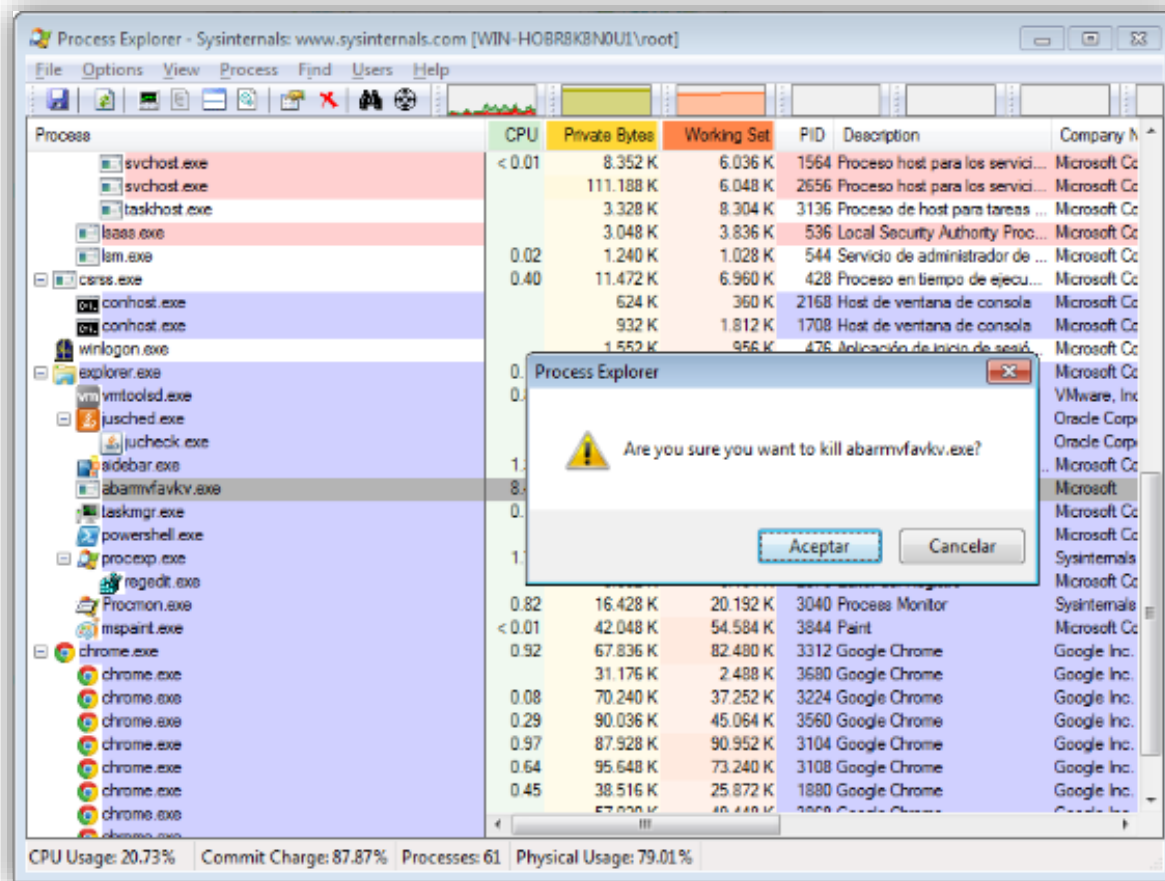




# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (VI)

- Antes de borrar el archivo, es necesario terminar el proceso, ya que Windows no permite la eliminación de archivos en ejecución. Para terminar el proceso, utilizaremos **Process Explorer**:



# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (VII)

- Ahora eliminamos el troyano utilizando **PowerShell**:
- El comando “**rm -force**” permite eliminar archivos de sistema:

```
PS C:\Users\root\AppData\Roaming>
PS C:\Users\root\AppData\Roaming>
PS C:\Users\root\AppData\Roaming> rm -force abarmvavkv.exe
PS C:\Users\root\AppData\Roaming>
PS C:\Users\root\AppData\Roaming>
PS C:\Users\root\AppData\Roaming> Get-ChildItem -force
```

Directorio: C:\Users\root\AppData\Roaming

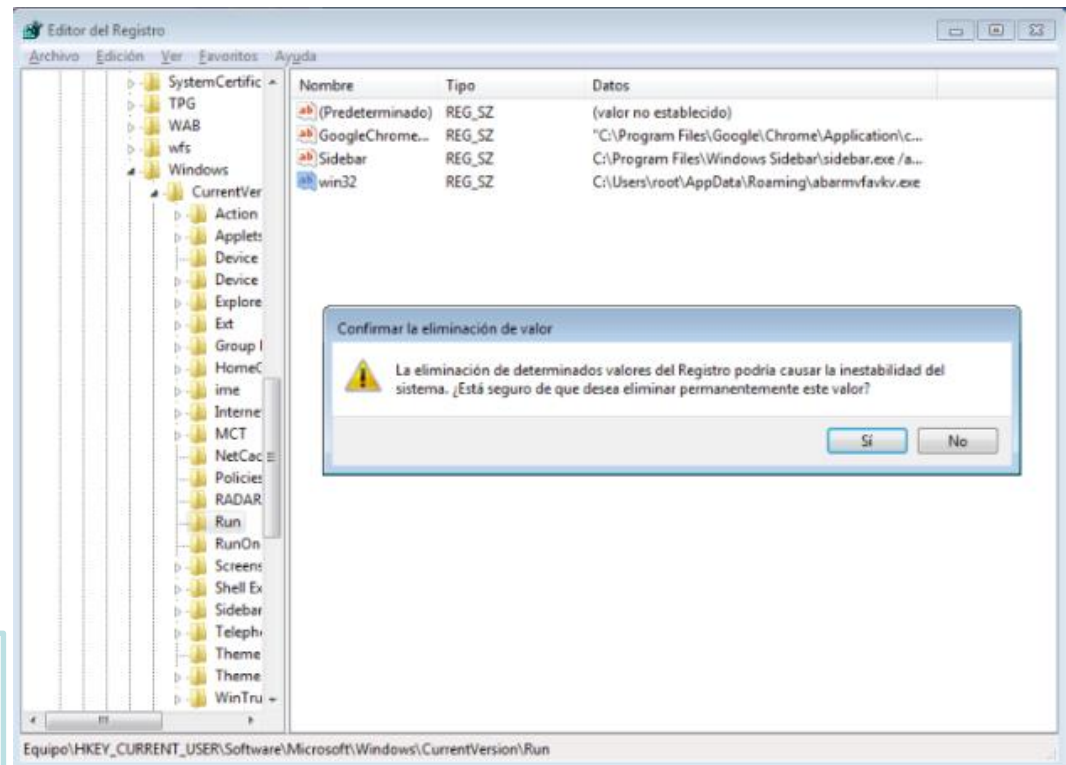
Mode	LastWriteTime	Length	Name
d----	19/09/2014 10:50		Adobe
d----	05/09/2014 14:25		geany
d----	19/09/2014 15:40		gtk-2.0
d----	11/08/2014 12:00		Identities
d----	14/07/2009 11:07		Media Center Programs
d---s	19/09/2014 10:50		Microsoft
d----	11/08/2014 12:12		Mozilla
d----	18/09/2014 11:20		Notepad++
d----	29/09/2014 10:30		Wireshark
-a-hs	29/09/2014 11:04	13947	abarmvavkv.txt

```
PS C:\Users\root\AppData\Roaming>
```

# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (VIII)

- El último paso consiste en borrar la entrada del registro de Windows infectada.



El registro de Windows es una base de datos que almacena los ajustes de configuración y opciones en los sistemas operativos Microsoft Windows.

# Práctica: “Construyendo una botnet”

## Paso 3: Detección y desinfección (IX)

- Para asegurarnos que no queda rastro del virus, utilizaremos la opción de comprobación del generador de bots:



# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Malware
5. Botnets
6. Práctica: construyendo una botnet
  1. Infección
  2. Explotación
  3. Detección y desinfección
- 7. Contramedidas**
8. Resumen
9. Otros datos de interés

# Contramidas

## ¿Cómo me defiendo de las botnets? (I)

- Aplicar las medidas de seguridad generales frente a todo tipo de malware:
  - Ten cuidado con lo que descargas y ejecutas:



Fuentes: <https://blog.malwarebytes.org/intelligence/2012/10/pick-a-download-any-download/>

# Contramidas

## ¿Cómo me defiendo de las botnets? (II): Antivirus

- Un antivirus es un programa especial diseñado para **detectar y eliminar malware**.
- Utilizan diversos métodos para detectar los virus:
  - **Detección basada en firmas:** es el método más común. Analiza el fichero y lo compara contra una base de datos de virus conocidos. No es eficaz en malware desconocido.
  - **Detección heurística:** analiza el fichero en busca de patrones que habitualmente se encuentran en los virus. Permite, a veces, detectar virus que aún no se han reportado.
  - **Detección basada en el comportamiento:** analiza el comportamiento del ejecutable, detectando acciones sospechosas (borrado de ficheros, etc.)
  - **Detección en sandbox:** ejecuta el programa sospechoso en un entorno virtual seguro, del cuál no se puede salir, y realiza una detección basada en comportamiento.





# Contramidas

## ¿Cómo me defiendo de las botnets? (III) : Antivirus

- ¡Cuidado con los falsos Antivirus!
  - Los falsos antivirus son malware muy extendidos. Muestran a la víctima **falsas amenazas de seguridad**, incitándole a instalar falsos antivirus que en realidad son virus.
  - A comienzos de 2014, la página oficial de Dailymotion fue pirateada y mostraba falsas advertencias de antivirus, el falso antivirus se sirvió a través de anuncios de terceros (redirigiendo automáticamente al usuario) mostrados en DailyMotion.

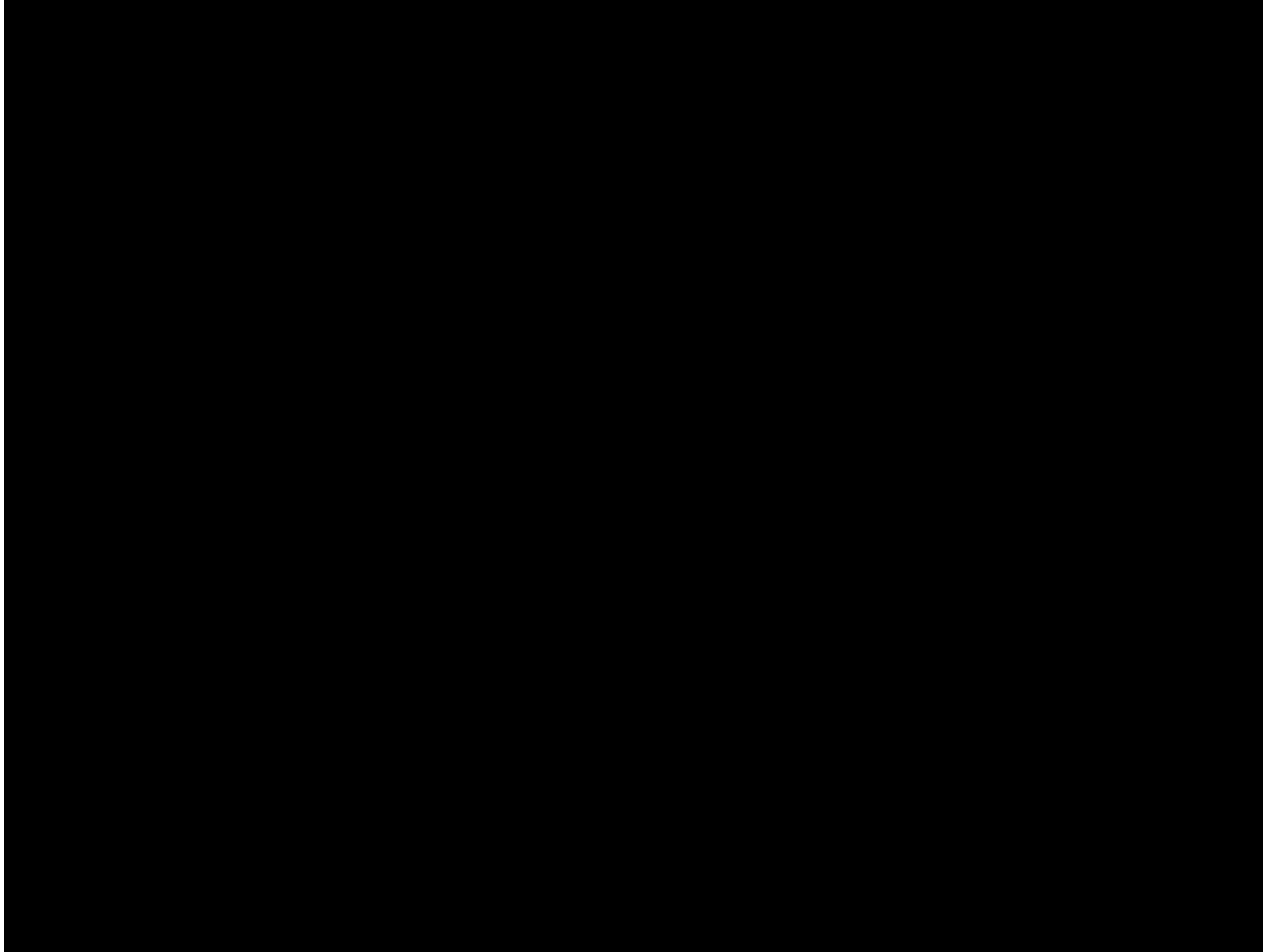


Fuentes: <http://arstechnica.com/security/2014/02/what-a-fake-antivirus-attack-on-a-trusted-website-looks-like/>,  
<https://www.youtube.com/watch?v=7xKmAsSzJv0>



# Contram medidas

## ¿Cómo me defiendo de las botnets? (IV) : Antivirus



Fuentes: <http://arstechnica.com/security/2014/02/what-a-fake-antivirus-attack-on-a-trusted-website-looks-like/>,  
<https://www.youtube.com/watch?v=7xKmAsSzJv0>

# Contramidas

## ¿Cómo me defiendo de las botnets? (V): VirusTotal

- VirusTotal:
  - Empresa española adquirida en 2012 por Google.
  - Permite subir archivos sospechosos para que sean analizados on-line por numerosos antivirus.



Nombre: TrueCrypt-7.2.exe

Detecciones: 0 / 53

Fecha de análisis: 2014-10-06 08:49:26 UTC ( hace 1 minuto )

😊 Probablemente inofensivo Todo indica que este archivo es seguro.

Antivirus	Resultado	Actualización
AVG	✓	20141006
AVware	✓	20141004
Ad-Aware	✓	20141006
AegisLab	✓	20141006

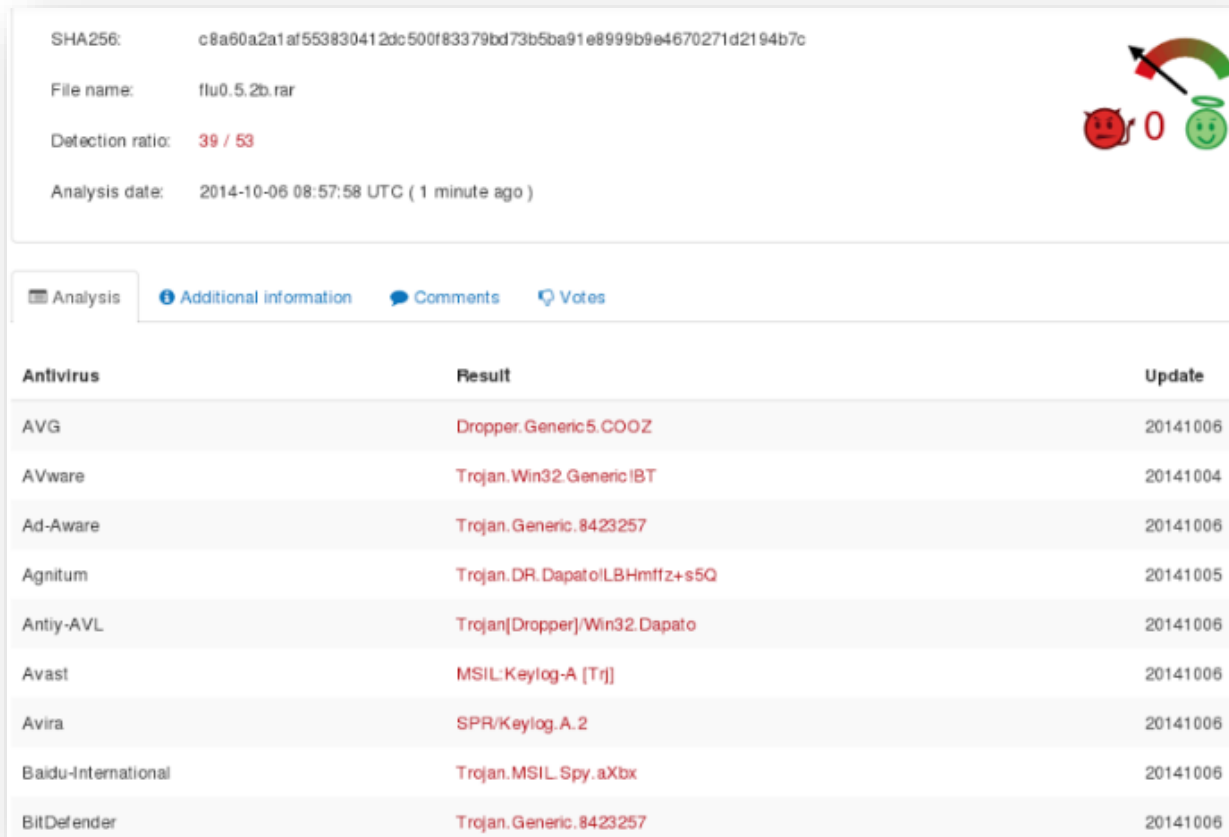
- Si subes un virus creado por ti mismo a VirusTotal, lo más probable es que en pocos días las bases de datos de la mayoría de los antivirus lo incorporen como archivo malicioso.

Fuente: <https://www.virustotal.com/es/>

# Contramidas

## ¿Cómo me defiendo de las botnets? (VI): VirusTotal

- Práctica: sube el virus Flu a VirusTotal para ver el resultado:



SHA256: c8a60a2a1af553830412dc500f83379bd73b5ba91e8999b9e4670271d2194b7c

File name: flu0.5.2b.rar

Detection ratio: 39 / 53

Analysis date: 2014-10-06 08:57:58 UTC ( 1 minute ago )

Analysis Additional information Comments Votes

Antivirus	Result	Update
AVG	Dropper.Generic5.COOZ	20141006
AVware	Trojan.Win32.GenericIBT	20141004
Ad-Aware	Trojan.Generic.8423257	20141006
Agnitum	Trojan.DR.Dapato!LBHmfz+s5Q	20141005
Antiy-AVL	Trojan[Dropper]/Win32.Dapato	20141006
Avast	MSIL:Keylog-A [Trj]	20141006
Avira	SPR/Keylog.A.2	20141006
Baidu-International	Trojan.MSIL.Spy.aXbx	20141006
BitDefender	Trojan.Generic.8423257	20141006

Fuente: <https://www.virustotal.com/es/>

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Malware
5. Botnets
6. Práctica: construyendo una botnet
  1. Infección
  2. Explotación
  3. Detección y desinfección
7. Contramedidas
- 8. Resumen**
9. Otros datos de interés

# Resumen

## Resumen de conceptos

- Una **botnet** es una red de ordenadores infectados controlados por un ciberdelincuente.
- Las botnets suelen ser compradas o alquiladas para fines maliciosos, como pueden ser ataques de denegación de servicio o fraude de clics (por ejemplo, falsear una encuesta).
- Los ordenadores son infectados por malware que los convierten en nodos de la red.
- Los mecanismos de defensa son los habituales frente a malware: un uso responsable del ordenador y un buen antivirus.

# Resumen

## Cuestiones

1. ¿Qué es un troyano?
2. ¿Para qué se utilizan las botnets? Ejemplos.
3. ¿Qué es un servidor Command and Control?
4. ¿Cómo se convierte un ordenador en un zombi?
5. ¿Qué recomendarías para defenderse frente a infecciones?

# Resumen

## Respuestas

1. Un troyano es un tipo de malware. Es un programa que es aparentemente inofensivo pero que realiza acciones maliciosas como borrar información del ordenador, cifrar los ficheros del equipo recabar información para enviarla a un atacante remoto, control remoto, etc.
2. Las botnets son utilizadas por los ciberdelincuentes para dar órdenes que luego ejecutarán los ordenadores zombies de esa red. Se suelen utilizar para enviar spam, hacer ataques de Denegación de Servicio, fraude de clicks, etc.
3. Se llama así al servidor que controla la red de ordenadores infectados por la botnet.
4. Un ordenador se convierte en un zombie cuando se instala un troyano cuya acción maliciosa sea formar parte de una botnet
5. Debemos tener un antivirus debidamente actualizado ejecutándose en nuestro ordenador y, siempre, tener cuidado con lo que uno se descarga y ejecuta en el ordenador; en caso de tener dudas sobre la legitimidad de algún fichero, se pueden emplear herramientas como la Web de VirusTotal.

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Malware
5. Botnets
6. Práctica: construyendo una botnet
  1. Infección
  2. Explotación
  3. Detección y desinfección
7. Contramedidas
8. Resumen
- 9. Otros datos de interés**



# Otras Actuaciones de interés

Si te gusta la ciberseguridad y quieres profundizar en este tema en INCIBE se están desarrollando las siguientes actividades y eventos de ciberseguridad:



**Formación especializada en ciberseguridad:** MOOC que se desarrollan a través de la plataforma de formación de INCIBE (<https://www.incibe.es/formacion>) sobre conceptos avanzados en ciberseguridad tales como ciberseguridad industrial, seguridad en dispositivos móviles, programación segura, malware y sistemas TI.



**Programa de becas:** Programa de becas anual en el que se establecerán diferentes tipologías de becas: formación de cursos especializados y másteres en ciberseguridad, y becas de investigación. Todas las publicaciones de este tipo se realizará a través de la siguiente página: <https://www.incibe.es/ayudas>



**Evento de ciberseguridad – CyberCamp** (<http://cybercamp.es>).

CyberCamp es el evento internacional de INCIBE para **identificar**, **atraer** y **promocionar el talento** en ciberseguridad. Identificar trayectorias profesionales de los jóvenes talento.

Detectar y promocionar el talento mediante talleres y retos técnicos.

Atraer el talento ofreciendo conferencias y charlas de ciberseguridad por profesionales y expertos de primer nivel.

Y muchas cosas más....

Evento para **familias**, contando con actividades de concienciación y difusión de la ciberseguridad para padres, educadores e hijos.

Promoción de la **industria** e **investigación** en ciberseguridad.

Gracias  
por tu atención

Contáctanos

**Contacto (más información y dudas sobre las jornadas):**



**[espaciosciberseguridad@incibe.es](mailto:espaciosciberseguridad@incibe.es)**

**En las redes sociales:**



@Incibe  
@Certs\_  
@Osiseguridad  
@CyberCampES  
@CyberEmprende\_



Oficina de Seguridad del internauta  
CyberCamp



INCIBE  
OSIseguridad



Pág. INCIBE  
Grupo INCIBE

**En la sede:**

Avenida José Aguado, 41 - Edificio INCIBE  
24005 León  
Tlf. 987 877 189

**En los sitios web:**

[www.incibe.es](http://www.incibe.es)  
[www.osi.es](http://www.osi.es)  
[www.cybercamp.es](http://www.cybercamp.es)  
[www.certs.es](http://www.certs.es)

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

INSTITUTO NACIONAL DE  
CIBERSEGURIDAD  
SPANISH NATIONAL  
CYBERSECURITY INSTITUTE

 **incibe\_**



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ENERGÍA, TURISMO  
Y AGENDA DIGITAL