TrackUZ: Una propuesta para control de tráfico malicioso sobre Packeteer ©

Victor Pérez Roche

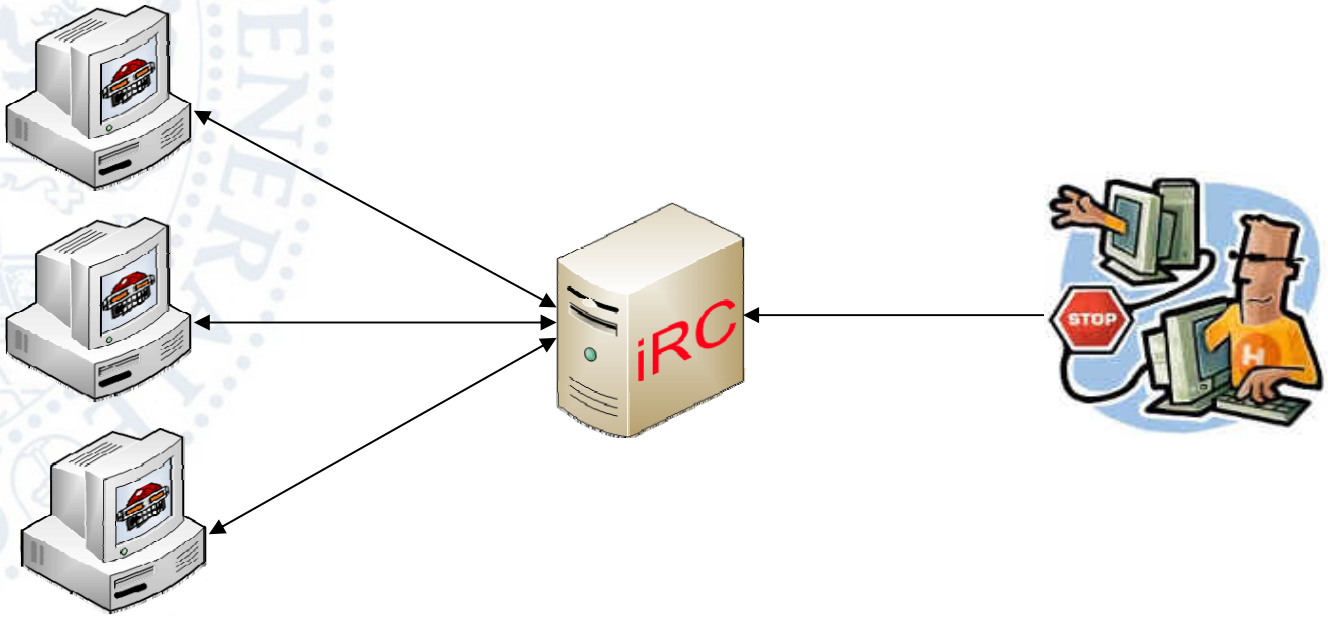
vroche@unizar.es

Índice

BOT-NETS

- Infecciones masivas de SO Windows

- iRC-BOTS: SpyBOT, SDBot ...



Introducción: Una BOTNET real

Primera intrusión controlada por TrackUZ

Septiembre-Octubre 2004

Introducción: Objetivos

Objetivos fijados

- Detección de máquinas infectadas
- Bloqueo de acceso a la red de esas máquinas
- Contacto con el usuario

Gestor de ancho de banda Packeteer ©

PacketShaper de Packeteer

- Gestor de ancho de banda.
- Clasificación de tráfico a nivel de aplicación.

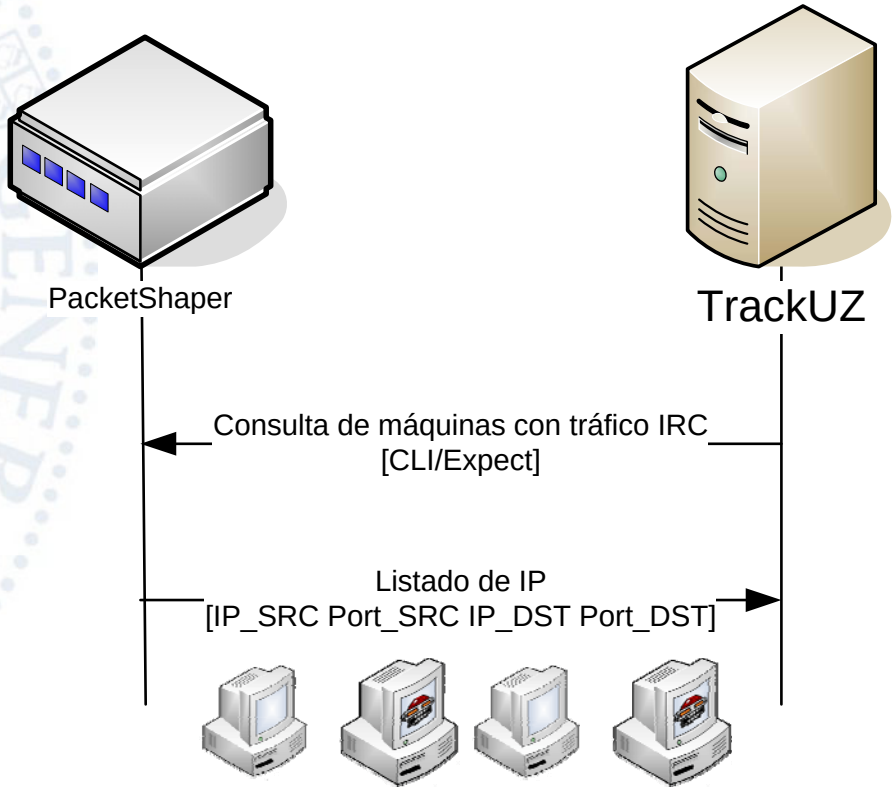
Otros usos

- Conocer qué máquinas están haciendo iRC.
- Comunicación con el usuario redirigiendo sus peticiones HTTP a una página informativa.

- Redhat Linux

- Apache, MySQL, expect y PHP

1.- Buscamos tráfico iRC en nuestra Red



2.- Búsqueda de la evidencia

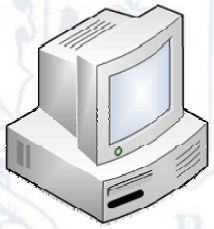
Necesitamos de alguna prueba que nos confirme que una máquina está realmente comprometida

¿  ? ¿  ?

Utilizaremos un método cuantitativo de puntuación de HECHOS de comportamiento observables en la LAN y la WAN

2.1- Protocolo AUTH/IDENT

Protocolo utilizado por servidores de Internet, fundamentalmente POP, IMAP, SMPT e IRC. En el puerto 113 se publica información del usuario que desea realizar una conexión.



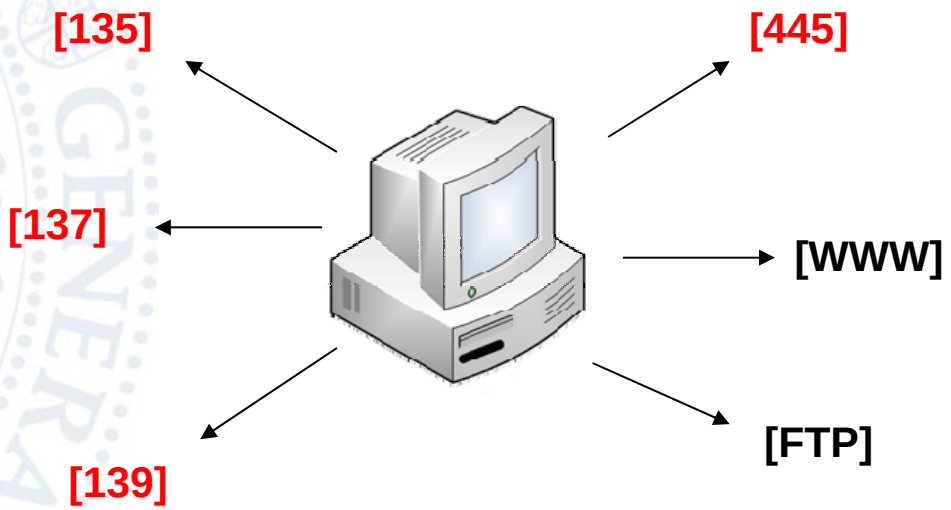
[port. 113] = Ø

[port. 113] = " : USERID : UNIX : vaspyc "

Identificador aleatorio cada vez

2.2- Comportamiento en la LAN

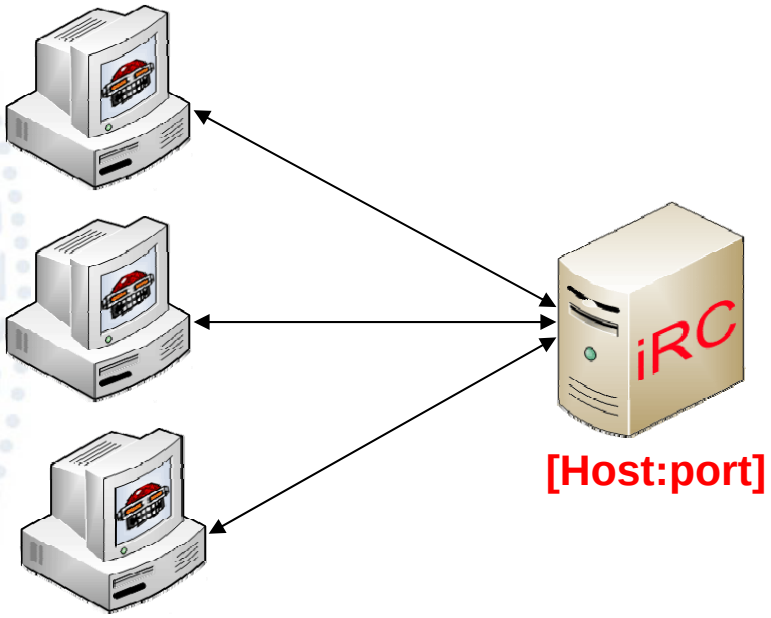
Nº de Conexiones a determinados puertos



En general, salvo para servidores, > 30 cnx =

[WWW/FTP] : Utilizados solo a nivel estadístico, no son representativos

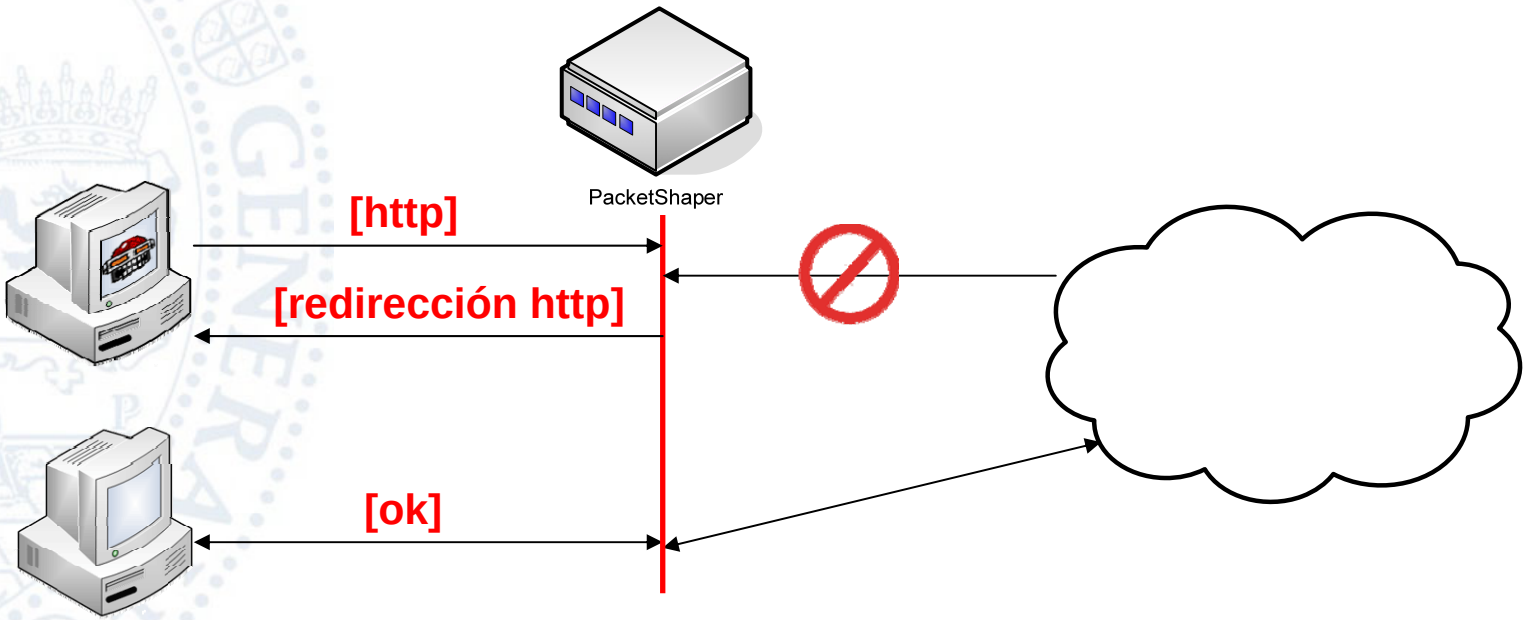
2.3- Varias máquinas conectadas al mismo servidor IRC



MUY sospechoso y bajo índice de falsos positivos,

aunque parezca mentira …

3.- Limitación del acceso a la red y comunicación al usuario



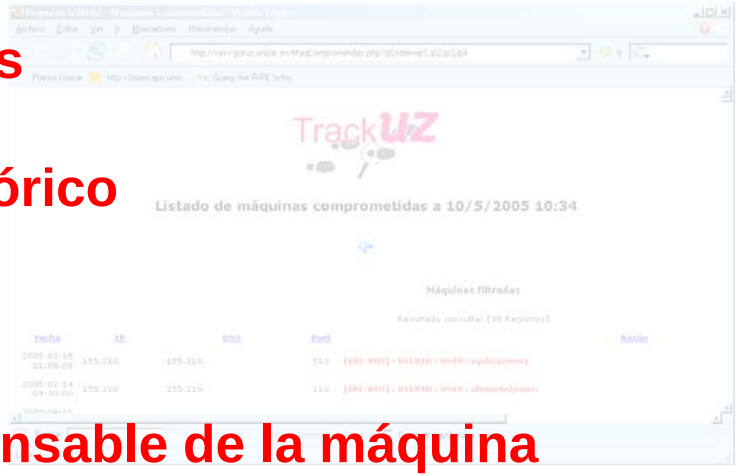
Control en base a dirección IP vía Packeteer.

Se desecha todo el tráfico excepto HTTP, que se redirecciona

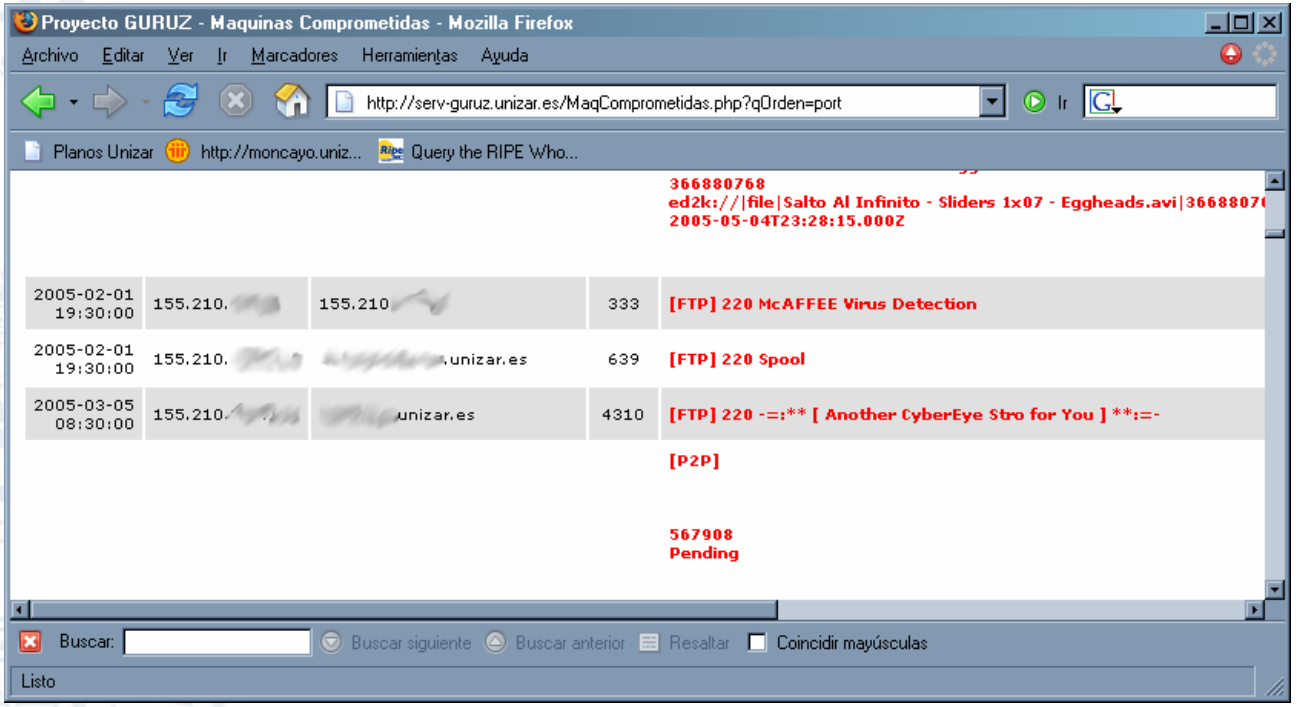
3.- Redirección HTTP

4.- Gestión de máquinas comprometidas

- Notificación vía mail al responsable de la aplicación TrackUZ de máquinas sospechosas y confirmadas
- Gestión de entradas y salidas, con histórico
- “Lista blanca” de IPs no bloqueables
- Envío de e-mail a la dirección del responsable de la máquina
- Salida manual de la lista “negra”



Metodología similar para protocolo FTP



1.- Detección de servidores de warez

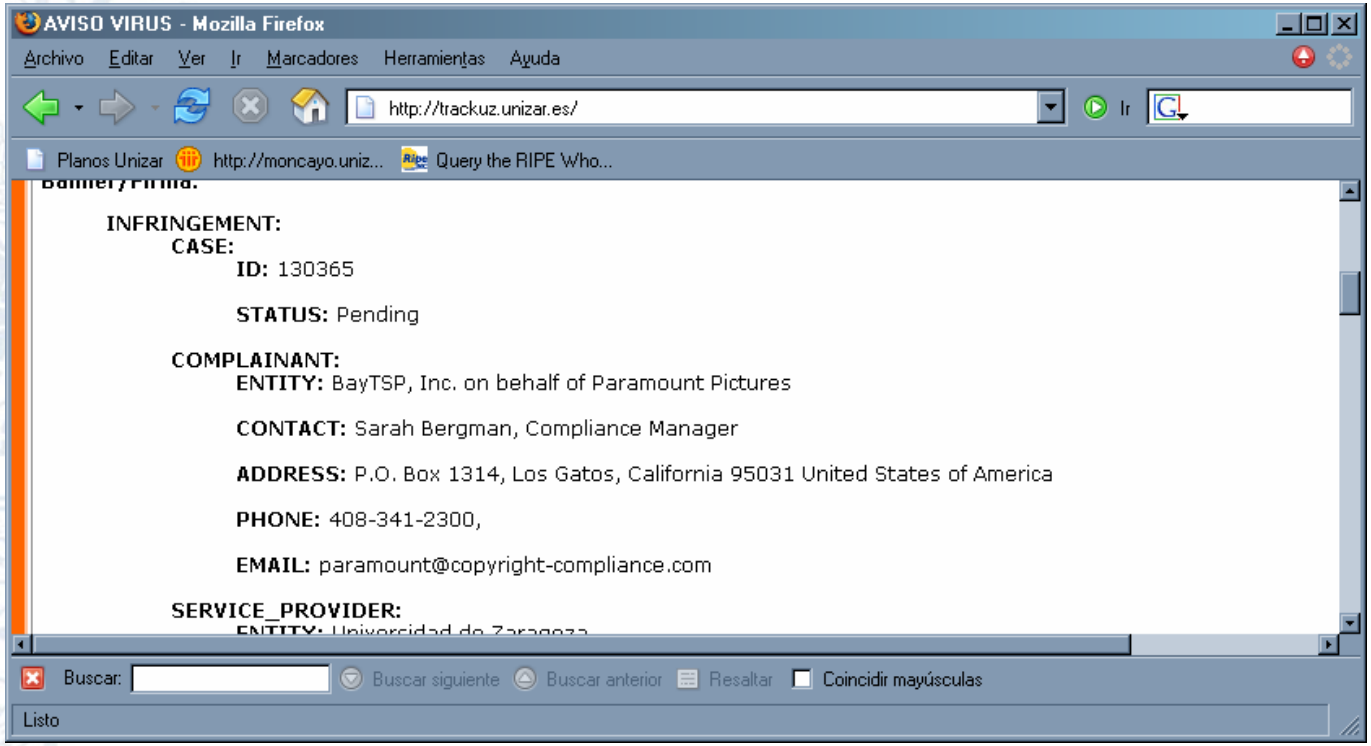
2.- Censo de los servidores FTP presentes en la red

Igualmente para servidores HTTP

1.- Censo de los servidores HTTP presentes en la red

TrackUZ: Efectos laterales 3 / 3

Control vía redirección de HTTP de denuncias de compartición de archivos con copyright



TrackUZ: Resultados 1 / 2

Resultados desde 01/01/2005

[Sobre una red de +10.000 nodos]

- 124 Máquinas con iRC-BOT detectadas y bloqueadas

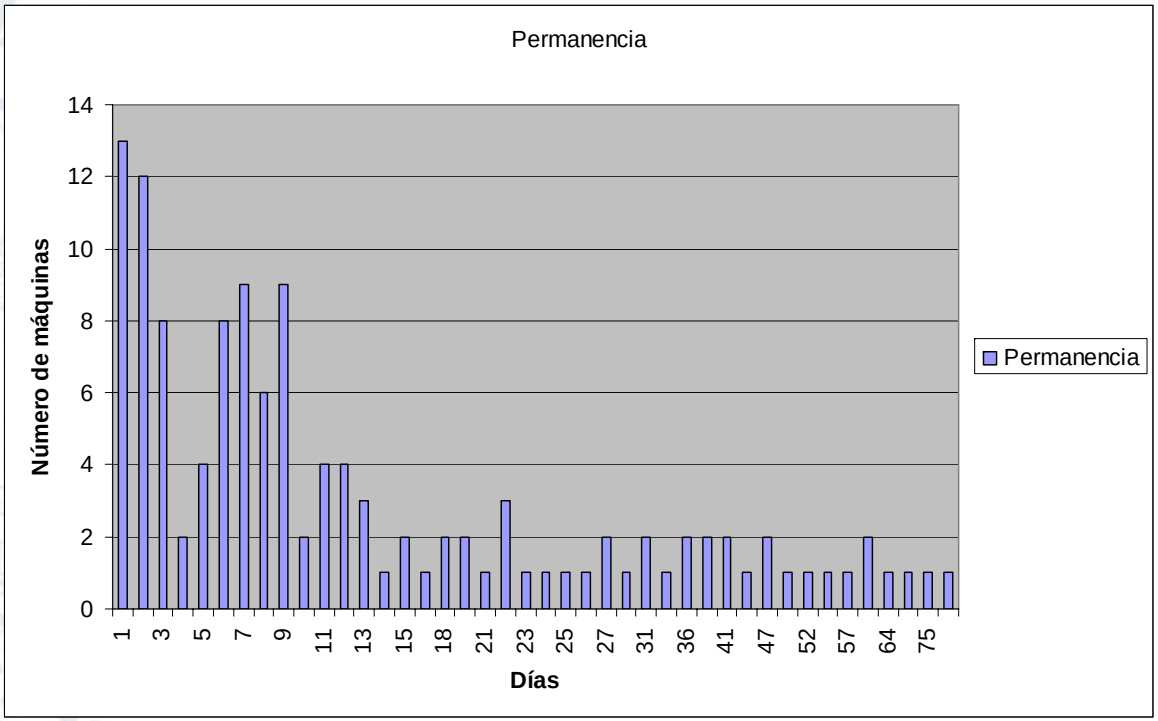
- 25 Máquinas comprometidas con servidores FTP

- 15 Máquinas bloqueadas por denuncias de copyright

Latencia del sistema: 15 minutos

TrackUZ: Resultados 2 / 2

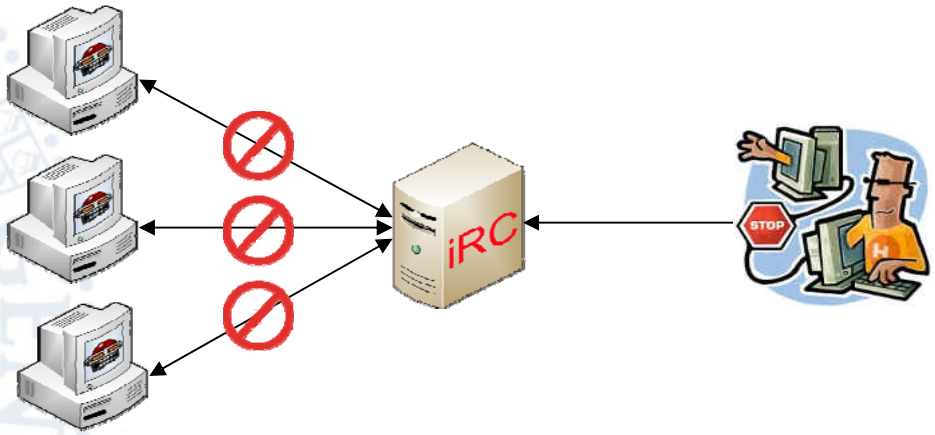
- **Media de permanencia en la lista negra: 15 días**



- **Media de máquinas en lista negra: 40**

Fortalezas del método 1 / 2

Corte de la transmisión entre el “hacker“ y la máquina comprometida



1.- (Normalmente) Se evita que el virus/gusano se siga propagando

2.- Se evita que el código malicioso se auto-actualice

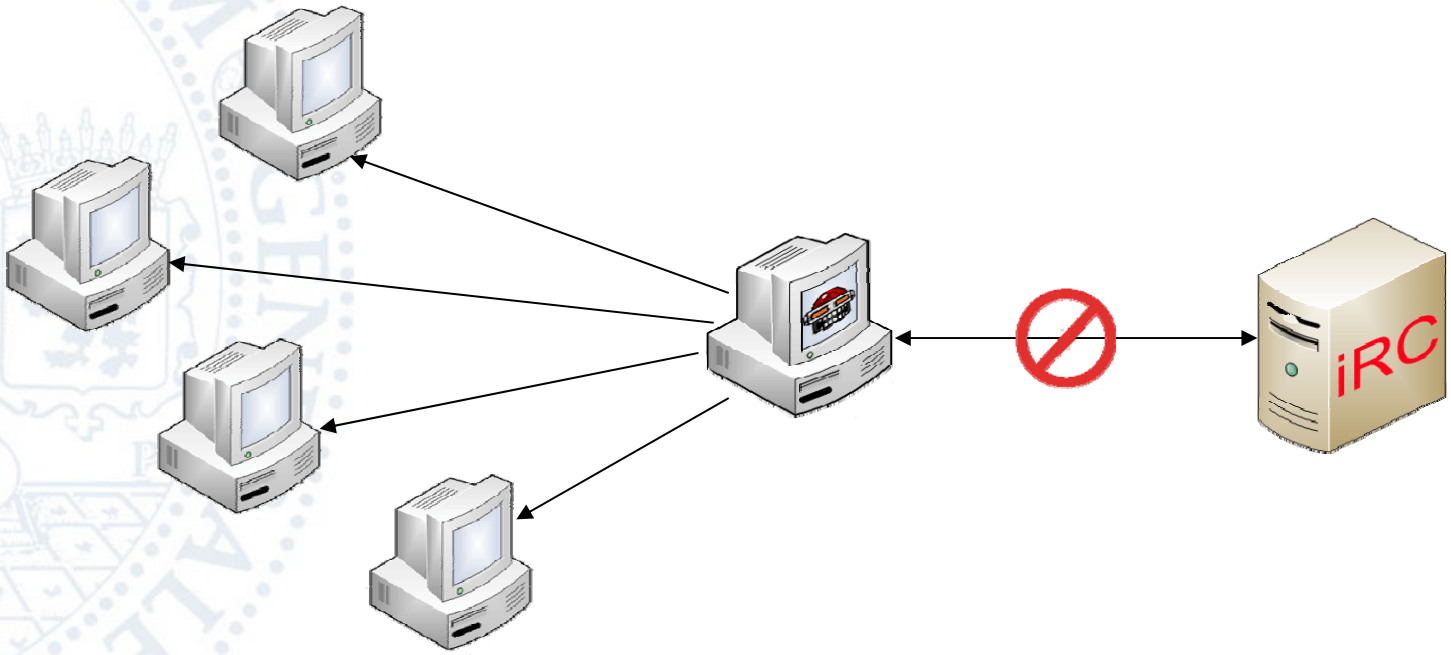
3.- Se evita que se puedan generar ataques DDoS

3.- Se le informa al usuario de la situación

Autogestión de las máquinas infectadas

- El 60% de los casos se solucionan directamente por el usuario actualizando el sistema operativo y el antivirus

No se corta el tráfico en la intranet



Falsos positivos / Falsos negativos

Difícilmente cuantificable:

- Packetshaper no siempre clasifica bien

- Problema del timing: Una máquina puede estar infectada y no presentar actividad sospecha. [Solución = hits]

Debilidades del método 3/3

- Solución surgida de una situación puntual

- NO tiene vocación de IDS

- NO plantea soluciones genéricas al problema de los BOTs, existen otras familias p.e. Agobot que no serían detectadas por este método

Utilización de SNORT

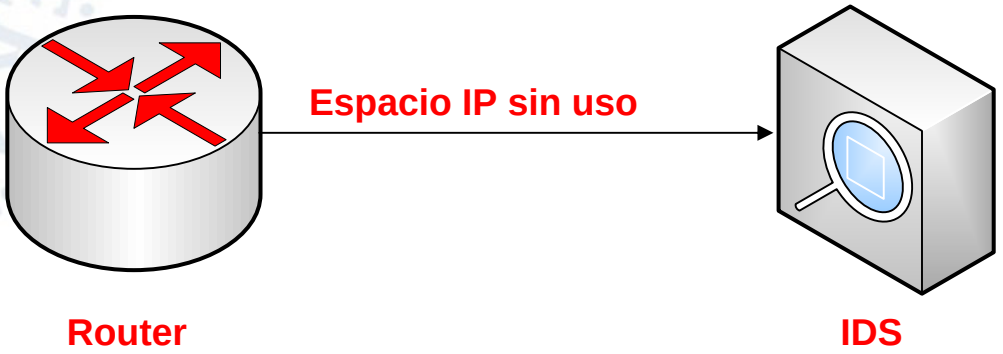
- Posibilidad de colocar varias sondas en la red con coste reducido

Futuro...

HoneyNet

The Honeynet PROJECT®

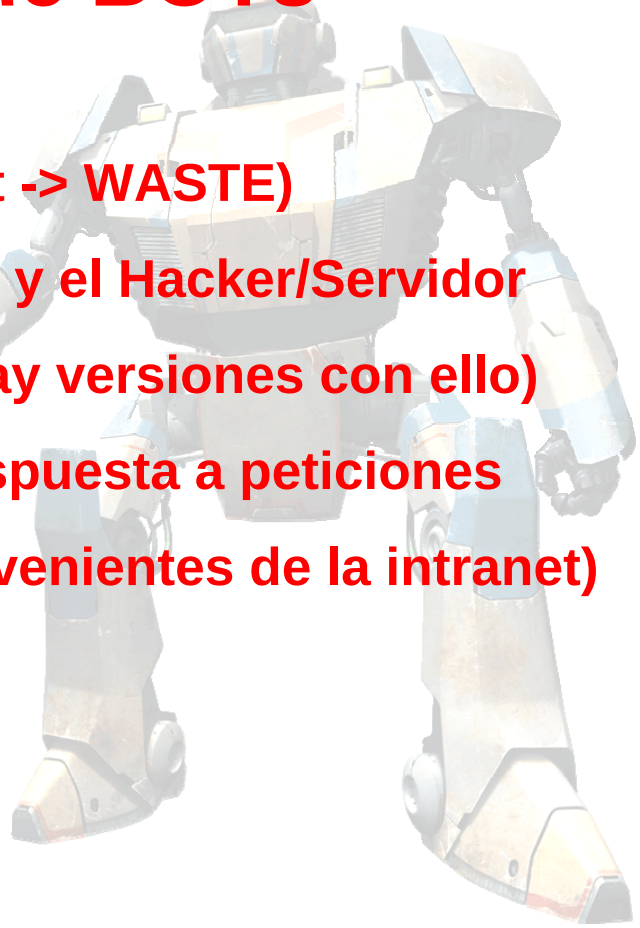
DarkNets



Nuevos modelos de BOTs

- NO utilización del protocolo IRC (Agobot -> WASTE)
- Cifrado de la comunicación entre el BOT y el Hacker/Servidor
- Instalación de rootkits por defecto (ya hay versiones con ello)
- Utilización de tecnología selectiva de respuesta a peticiones

(p.e. No responder a comunicaciones provenientes de la intranet)



¡Muchas gracias!

¿Preguntas?

Bibliografía: Documentación

Phatbot
http://www.lurhq.com/phatbot.html

Know Your Enemy: Tracking Botnets
http://www.honeynet.org/papers/bots/

The Honeynet Project
http://www.honeynet.org/

M. St. Johns. Identification protocol, February 1003. Request for Comments: RFC 1413
http://www.faqs.org/rfcs/rfc1413.html

Felix C. Freiling and Thorsten Holz and Georg Wicherski, April 2005
Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-Of-Service Attacks
http://honeynet.spenneberg.org/papers/individual/

Snort a libpcap-based sniffer/logger
http://www.snort.org

Spanish Honeynet Project
http://www.honeynet.org.es/

Bibliografía: Herramientas

Netcat
http://www.securityfocus.com

Nmap
http://www.insecure.org/nmap

Ethereal
http://www.ethereal.com

Sysinternals (varias)
www.sysinternals.com

Active Ports - SmartLine
http://www.protect-me.com/freeware.html

mIRC
http://www.mirc.com

Bibliografía: Desarrollo

Packeteer
http://www.packeteer.com/

Expect
http://expect.nist.gov/

MySQL
http://www.mysql.com

PHP
http://www.php.net