BotNet

Grupo de cordinación de Seguridad, IRIS-CERT

26 de Octubre de 2004

Indice

- Zombies, bot, etc.
- Funcionamiento de las botnet
- Localización y eliminación.

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 definiciön se generaliza a programas “sirvientes” , que realizan determinadas acciones en base comandos emitidos desde el controlador.

Zombies:

- Maquinas 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 vulnerabildades 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 (finales 2004)

- 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

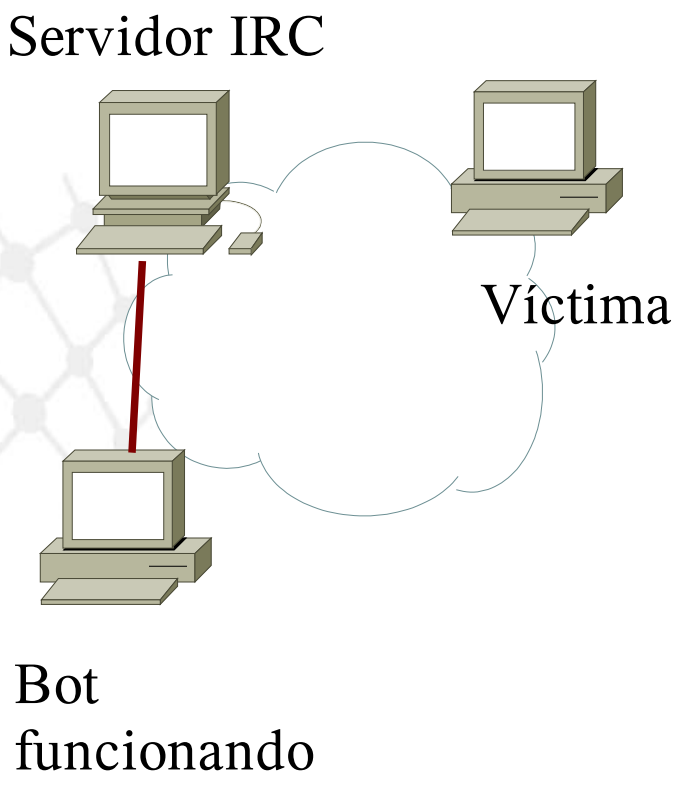
El gran bazar

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

Inicio de una Botnet

Compromiso vía botnet



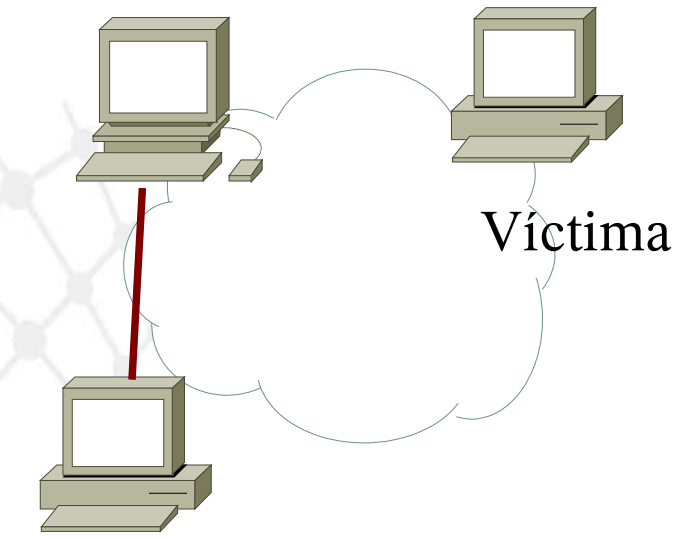
Inicialmente:

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.

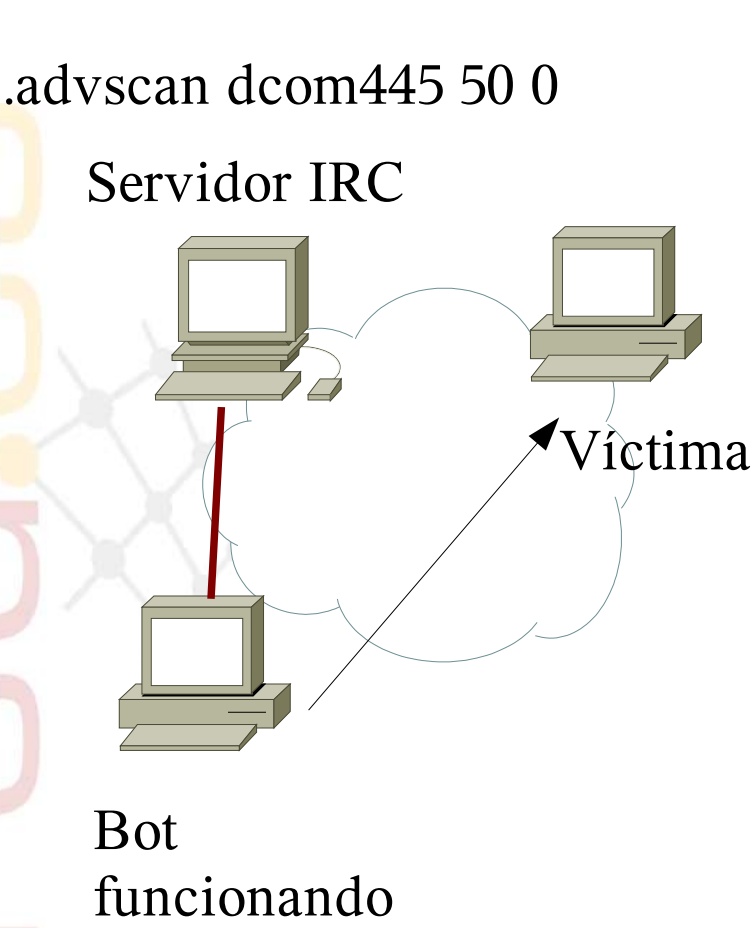
Compromiso vía botnet (I)

.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)



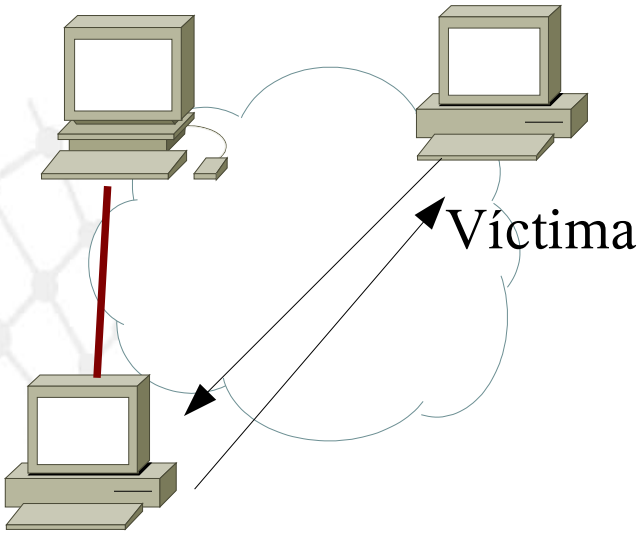
1)Vía IRC el atacante cambia el titulo o “topic” del canal para que los bots / zombies empiecen a atacar.

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)

.advscan dcom445 50 0

Servidor IRC



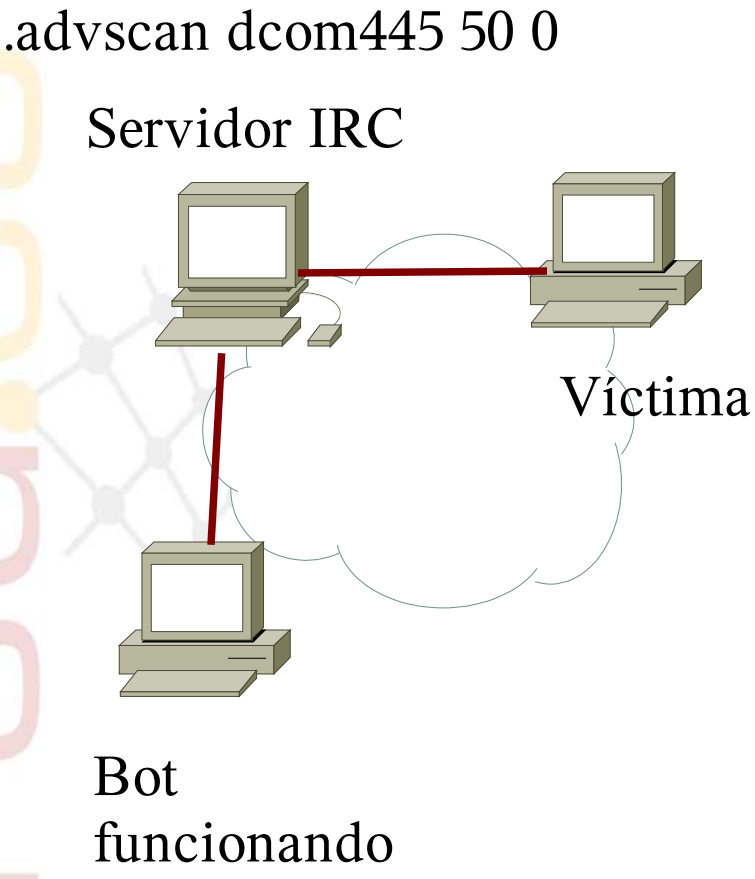
Bot funcionando

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]

¿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" .

BotNet : Detección y Control

Medidas proactivas (antes de que ocurran):

- Actualización de equipos (¿imposible ?)
- Filtrado entrante y saliente de servicios conflictivos (microsoft, principalmente)
  - No evita los usuarios "viajantes" ni los accesos VPN.
  - ¿Medidas de control en accesos VPN ?
- Monitorización de tráfico
  - Filtros de acceso
  - Flujos entrantes y salientes (Netflow, sflow)
  - Detección de los ataques antes de que sean reportados
- Monitorización de consultas DNS

Detección desde RedIRIS

Difusión de equipos comprometidos empleados como servidores IRC en listas restringidas de seguridad.

- Dirección IP
- Puerto

Desde IRIS-CERT:

- ❑ Comprobación de tráfico en los troncaless
- ❑ Notificación a las Instituciones con equipos infectados.
- ❑ Escasa resopuesta sobre el tipo de incidente
  - "Virus elimilado"

Eliminación

Medidas Reactivas (Una vez que ocurren):

- Los bots NO son siempre detectados por los antivirus
  - Modificaciones diarias de los binarios
  - Encriptación y compresión de los programas
- Analizar el equipo.
  - HijacThis ,
  - Seccheck (http://wwww.mynetwatchman.com/tools/sc)
  - Herramientas del sistema
- Tratar de determinar e informar sobre:
  - Binarios instalados
  - Fecha de instalación
  - Servidor de IRC utilizado (¿vía flujos ?)

Futuro

Emplea de canales de control más difíciles de detectar:

- Conexiones encriptadas entre servidores
- Protocolos distintos de IRC (en puertos no estandard)

Modificaciones a nivel de núcleo (rootkit) para evitar su detección

(Gran parte de las Botnet todavía no incorporan rootkit)

Mayor uso de botnet para acciones ilegales.