Realizado por:
Daniel Sánchez Álvarez

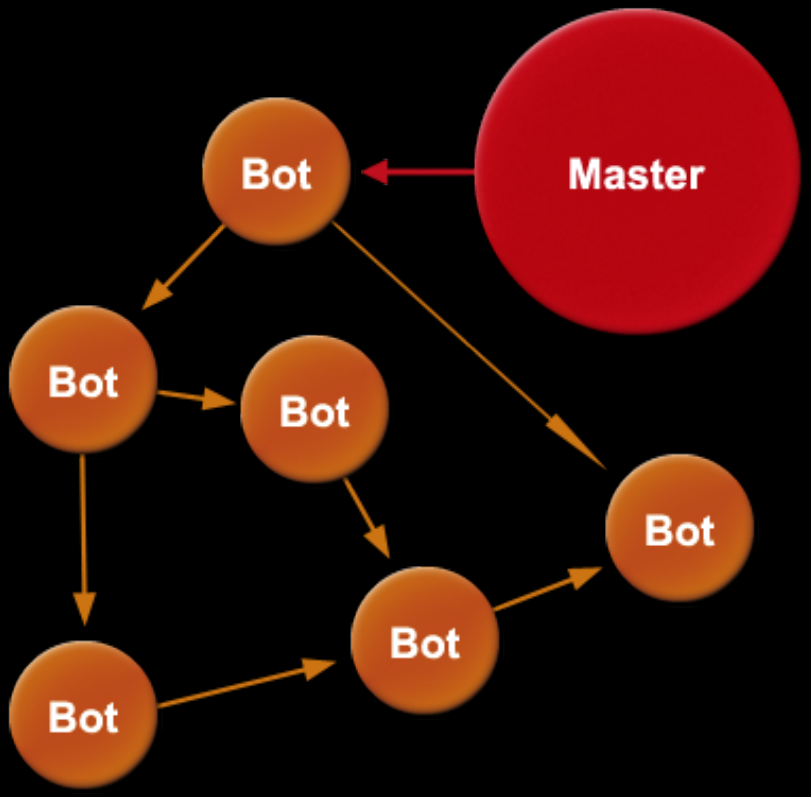
Red Zombie

¿QUE SON?

Es una red de equipos infectados por códigos maliciosos que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida.

¿COMO SE CREAN?

El hacker hace un programa capaz de ocultarse en el sistema operativo del ordenador víctima y quedarse a la espera de instrucciones.



¿COMO ENTRAN EN NUESTRO ORDENADOR?

El malware se puede distribuir mediante una multitud de métodos:

- Al abrir un documento adjuntado a un correo electrónico.
- Acceso a paginas con vulnerabilidades.
- Ejecutar alguna aplicación en internet.

¿COMO FUNCIONAN?

1. Infección y descarga de binario camuflado a través de exploit o ingeniería social.

2. Binario se desempaqueta e instala.

3. Eliminación de configuraciones de seguridad, para supervivencia.

4. Actualización de configuración y envío de datos de ubicación de componentes a descargar.

5. Descarga de últimos componentes y el software real de la Botnet camuflado.

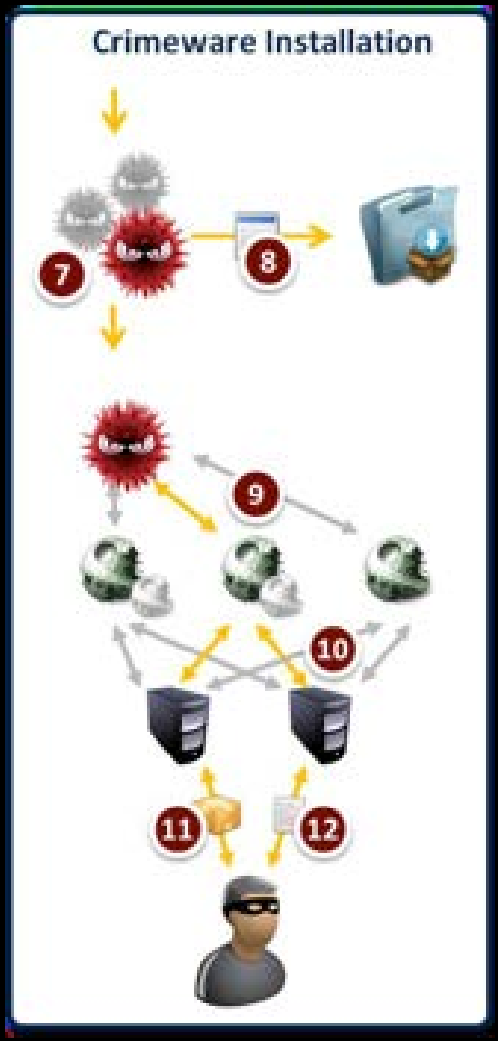
6. Extracción e instalación del binario final de la Botnet.

¿COMO FUNCIONAN?

7. Limpieza de binarios antiguos y rastros de infección.

8. Envío de información robada e intento de comunicación con C&C.

9. Se dispone de una solución de FrontEnd y balanceo para la comunicación-

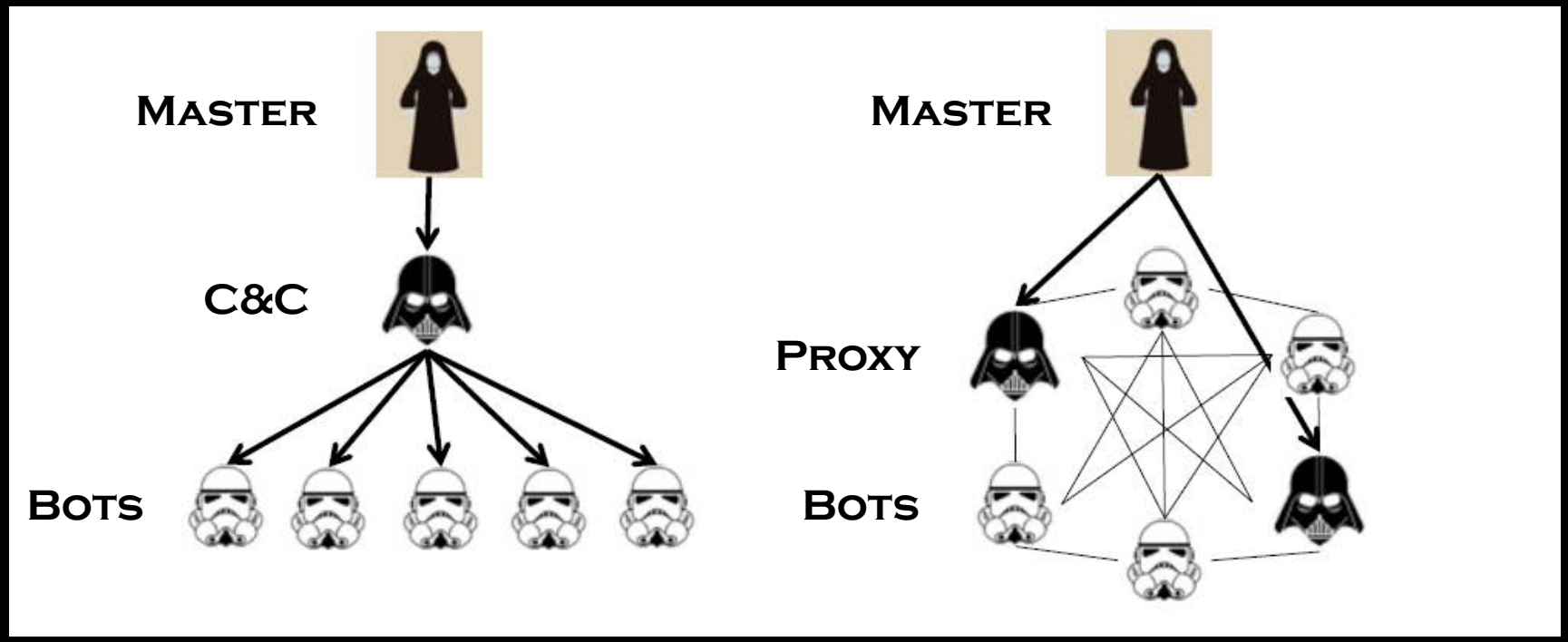


10. Comúnmente se usan proxies intermedios para proteger el controlador.

11. Actualización periódica de los agentes binarios, para evitar la detección de las casas de antivirus.

12. Actualización periódica de las configuraciones y el funcionamiento de los bots.

TIPOS DE BOTNETS



Arquitectura Jerárquica

- Basadas en protocolos clásicos:
  - IRC, HTTP.
- Mas innovadores:
  - Redes sociales (Twitter, ..)
  - Aplicaciones Web (Pastebin, ..)
  - Esteganografía (Flickr, ..)

Arquitectura P2P

- Basadas en protocolos P2P:
  - Kadmelia.
  - Overnet.
  - BitTorrent.

¿QUE FINES PERSIGUEN?

¡¡Ganar dinero!!

Pero... ¿Como lo hacen?

Los dueños de la Bonet alquilan una serie de servicios a todo aquel que quiera pagar por ello.

La lista de servicios que pueden ofrecer es interminable, pero estos son los más comunes:

¿QUE FINES PERSIGUEN?

1. Envío de correo basura

El creador de la Bonet da órdenes a los zombis para que capturen direcciones nuevas y operativas de correo electrónico y les envíen la publicidad que el cliente ha pagado por enviar.

Responsables del 85% del spam que circula por la red.

¿QUE FINES PERSIGUEN?

2. Robo de Información

El bot puede llevar incorporado un sniffer, que es un programa que escucha todo el tráfico de internet que pasa por nuestro ordenador y captura nombres de usuario y contraseñas para sitios conocidos como paypal, hotmail, ebay, etc.

También pueden conseguir números de tarjeta, números de cuentas bancarias y datos suficientes para gastar el dinero que hay en esas cuentas.

¿QUE FINES PERSIGUEN?

3. Distribución de material ilegal

Las botnets pueden ser alquiladas para alojar archivos de contenido ilícito. Nuestro ordenador zombi podría utilizarse para distribuir pornografía infantil por ejemplo, sin enterarnos nosotros de nada. En caso de desmantelarse la red de pornografía nuestro ordenador estaría implicado en el delito.

¿QUE FINES PERSIGUEN?

4. Ataque distribuido de denegación de servicio (DDoS)

Una empresa puede pagar una Botnet para que ataque a la red de una empresa de la competencia con el fin de inutilizarla durante un tiempo.

Al ser los atacantes muy numerosos y sumar entre ellos mucho más ancho de banda que la víctima no hay forma de evitar este ataque.

La red víctima quedará incomunicada durante todo el tiempo que dure el ataque, los servidores pueden llegar a bloquearse.

¿COMO SE DETECTAN?

Pasivas: recogida y observación

- Análisis de tráfico DNS
- Análisis de registros de flujos de tráfico
- Inspección del contenido del trafico
- Análisis de registros de SPAM
- Honeypot
- Ingeniería inversa
- Análisis forense
- Feedback de Antivirus

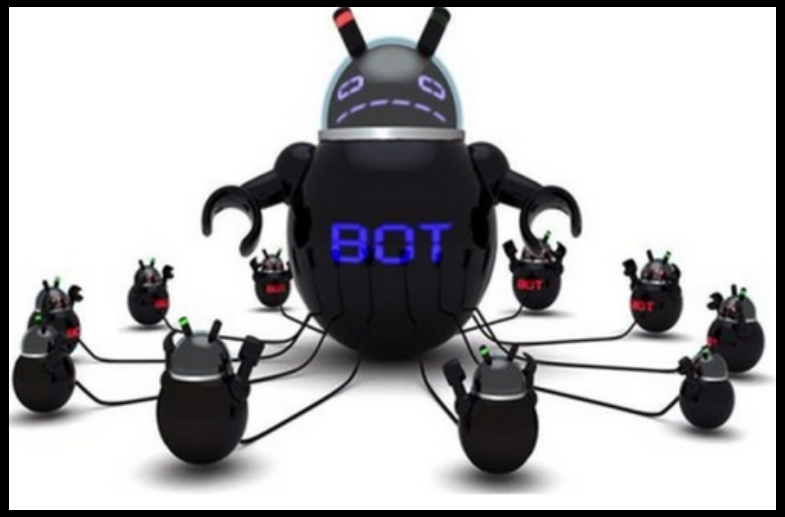
Activas: interacciones con el que origina el trafico

- Sinkholing
- Infiltración
- Enumeración P2P
- DNS cache snooping
- Monitorización IRC

¿COMO SE CONTROLAN?

Con el paso del tiempo los protocolos para el control de botnets han evolucionado, siendo estos los mas usados:

- Puertos fijos y Puertas traseras
- IRC (Chat)
- HTTP
- P2P
- Redes Sociales (Twitter)



¿COMO SE CONTROLAN?

1. Puertos Fijos y Puertas Traseras

Permite al atacante conectarse directamente y controlar el sistema infectado.

Gran numero de sistemas con puertas traseras "disponibles".

Ineficiente.

Cortafuegos activo por defecto con el service pack 2 Windows XP.

¿COMO SE CONTROLAN?

2. IRC (Chat)

Forma tradicional de control ha sido a través de un típico chat.

- ✓ Es la mas utilizada debido a su sencillez y comodidad de uso.
- ✗ Comandos enviados sin cifrar.
- ✗ Cualquiera podría unirse al canal.

¿COMO SE CONTROLAN?

2. IRC (Chat)

Mostrar salones | Entrar al salón | Cambiar sobrenombre | Emoticón | Estado | Propiedades

11:04		Ingresando al salón de chat...
		Ha iniciado una conversación en inkietos el lunes 23/11/2009 11:04:17
11:20		-> PERIODISMO01905 ha entrado a inkietos
11:39		-> TEST305097 ha entrado a inkietos
12:18		-> JESUS9-NUEVO339 ha entrado a inkietos
12:19		-> SULLY390969 ha entrado a inkietos
12:21		-> RODRIGUE-867203 ha entrado a inkietos
12:26		<- JESUS9-NUEVO339 ha sido desconectado (Client exited)
12:29		<- RODRIGUE-867203 ha sido desconectado (Ping timeout)
12:31		-> USER1484202 ha entrado a inkietos
12:38		<- TEST305097 ha sido desconectado (Client exited)
12:39		<- SULLY390969 ha sido desconectado (Client exited)
13:00		-> OCOLAPINTO405 ha entrado a inkietos
13:08		-> RECEPCION811443 ha entrado a inkietos
		-> INTERNET120898 ha entrado a inkietos
13:10		-> TEST421388 ha entrado a inkietos
		-> VICTOR-53C39FA0 ha entrado a inkietos
13:14		<- TEST421388 ha sido desconectado (Client exited)
13:16		<- VICTOR-53C39FA0 ha sido desconectado (Client exited)
13:22		<- INTERNET120898 ha sido desconectado (Client exited)
13:36		-> NATERS-39EFBD5A ha entrado a inkietos
13:54		-> DANIEL1825272 ha entrado a inkietos
13:58	abc	**!YoSoyTuAmo**
14:06	RECEPCION811443	-=Infectar=-: Unidad F: infectada
14:08		<- PERIODISMO01905 ha sido desconectado (Client exited)
14:12		-> GERENCIA149572 ha entrado a inkietos

abc
DANIEL1825272
GERENCIA149572
LUCY220475
NATERS-39EFBD5A
OCOLAPINTO405
PUNK847369
RECEPCION811443
res0
USER1484202

¿COMO SE CONTROLAN?

3. HTTP

Para eludir los cortafuegos, los atacantes idearon una nueva forma de comunicar los zombies con el controlador

- Los cortafuegos permitían conexiones hacia una web.
- HTTP permite cifrar de forma sencilla el trafico.
- Dirigidas a una web, y gestionarlas cómodamente como un panel de control tradicional.

¿COMO SE CONTROLAN?

3. HTTP

Blackshades Bot - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://www.yosoyhumilde.com/movil/bots.php?scr=FC901DF7

Más visitados

Blackshades Bot

Bots

Main | Bots | Logs | Passwords | Commands | DDoS | Settings | Logout

Show by: All Search: Show

ID	HWID	WAN	PC Name	User name	Country	Last seen
69	DC7C8E94	190.81	SHADOW_LITE_SP3	Administrador	Peru	2012-03-01 21:20:26
70	601F769F	195.86	PC	support	United Kingdom	2012-02-22 05:02:35
71	3C3E8BBE	201.24	CONTABILIDAD	Contabilidad	Chile	2012-02-29 10:45:51
72	ECC2EF29	64.179	WAREHOUSE01	fadistephan	United States	2012-03-01 16:39:15
73	14210986	188.99	C2F3F0B206C14E9	luser	United States	2012-02-22 13:25:23
74	18C993CD	88.29.	KIRA	Propietario	Spain	2012-03-01 05:30:45
75	B863B328	66.56.	VIC-KUUTPZTY7U6	vic	United States	2012-02-24 09:13:37
76	FC901DF7	201.22	DESKTOP	Administrador	Spain	2012-02-29 22:49:46

[redacted] Administrador-DESKTOP (ID: FC901DF7) [2011-09-20 19:48:54]

Terminado

BLACKSHADES

¿COMO SE CONTROLAN?

4. P2P

En los últimos años se observan métodos alternativos para controlar las botnets, destinados a eludir en lo posible que la red resulte detectada.

- ✓ Al no tener servidor central la eliminación de esta es mas difícil.
- ✗ Los proxies no están bajo el control del atacante.
- ✗ Alguien podría hacerse pasar por un proxy e infiltrarse en la Botnet.

¿COMO SE CONTROLAN?

5. Redes Sociales (Twitter)

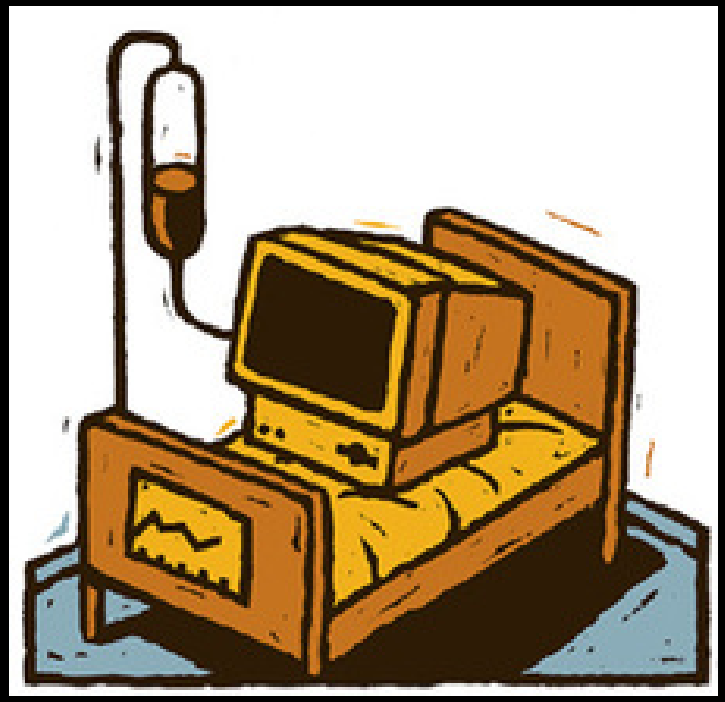
Las redes sociales son actualmente uno de los focos de infección preferidos para alojar botnets.

✓ Los mensajes se hayan codificados de forma que resulten incomprensibles.

✗ Susceptible de que la Bot sea descubierta.

¿COMO IMPEDIMOS SER INFECTADOS?

Lo primordial es tener nuestro sistema totalmente actualizado, esto es válido para cualquier sistema operativo que utilicemos. En caso de usar Windows debemos tener instalado un antivirus que se actualice todos los días como mínimo, así como un cortafuegos actualizado también.



COMERCIALIZACION

Datos completos de una persona → 7 $

Lista de 1.000.000 direcciones → 20 – 100 $

Cuentas de servicios online → 7 – 15 $

Cuentas bancarias → 1 – 1500 $

Spam 100.000 direcciones → 70 $

Spam decenas de millones de direcciones → 1000 $

Mantener una pagina de Phishing → 1000 – 2000 $/mes

DDoS → 10 $/hora 50 $/día 150 $/semana 1200 $/mes

Botnet de 2000 bots → 200 $

Red Shadow 100.000 bots → 37.290 $

Código fuente Zeus → 500 $

BOTNETS FAMOSAS

Zeus → Creada en 2007 → 3.600.000 bots

Mariposa → Creada en 2008 → 13.000.000 bots

Conficker → Creada en 2008 → 10.500.000 bots

Bredolab → Creada en 2009 → 30.000.000 bots

DATOS INTERESANTES

- Un estudio realizado en 2009 por diversas consultoras informáticas revelo que el 64% de los juegos electrónicos que se descargan en internet están infectados con malware.

- También es muy significativa la propagación de troyanos que descargan un ejecutable disfrazado de códec durante la reproducción de un fichero multimedia.

- Existencia de virus que permite ocultar al antivirus y el usuario que el sistema esta infectado.

- El 85% del spam que circula por la red es causado por botnets.

FIN