

BOTNETs

Fundamentos de Redes

Pablo Alvarez, Javier Sáez

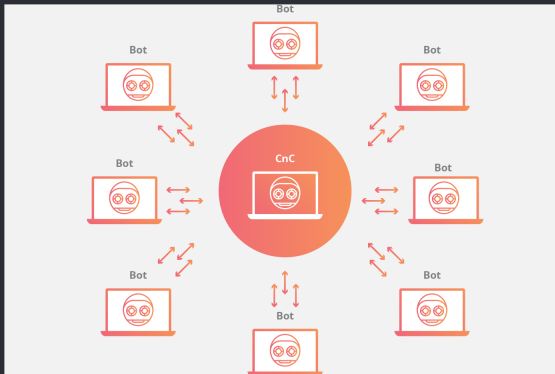
Índice

1. ¿Qué es una Botnet?
2. ¿Cómo se forma una botnet?
3. Estructura de una botnet
 - 3.1 Arquitectura
 - 3.2 Componentes
 - 3.3 Protocolos de control
4. ¿Qué hace una Botnet?
5. Cómo saber si formo parte de una botnet
6. Cómo evitarlo
7. Botnets famosas

¿Qué es una Botnet?

- Botnet = bot (robot) + net (network o red)
- Red de dispositivos informáticos (PCs, smartphones, dispositivos IoT...) que son controlados de forma remota por otro equipo.
- Pueden llegar a controlar cientos de miles de equipos

- **Bot:** aplicación software que ejecuta scripts a través de Internet
- **C&C:** Command and Control Software



Índice

1. ¿Qué es una Botnet?
2. ¿Cómo se forma una botnet?
3. Estructura de una botnet
 - 3.1 Arquitectura
 - 3.2 Componentes
 - 3.3 Protocolos de control
4. ¿Qué hace una Botnet?
5. Cómo saber si formo parte de una botnet
6. Cómo evitarlo
7. Botnets famosas

¿Cómo se forma una botnet?

- Creación del virus (bot) y propagación a través de la red
- Sistemas Windows y Mac OS:
 - Distribución de software ilícito (cracks, descargas P2P...)
 - Vulnerabilidades conocidas de Windows
- Sistemas UNIX:
 - telnet
 - SSH
 - Ataques a bugs conocidos
- El bot se conecta a un servidor C&C
- La red está lista para ser utilizada o vendida

Índice

1. ¿Qué es una Botnet?
2. ¿Cómo se forma una botnet?
3. Estructura de una botnet
 - 3.1 Arquitectura
 - 3.2 Componentes
 - 3.3 Protocolos de control
4. ¿Qué hace una Botnet?
5. Cómo saber si formo parte de una botnet
6. Cómo evitarlo
7. Botnets famosas

Arquitectura de una botnet

Existen dos formas principales de trabajar con una botnet en cuanto a interconexión entre máquinas se refiere:

- Modelo Cliente-Servidor
- Modelo P2P

Arquitectura de una botnet

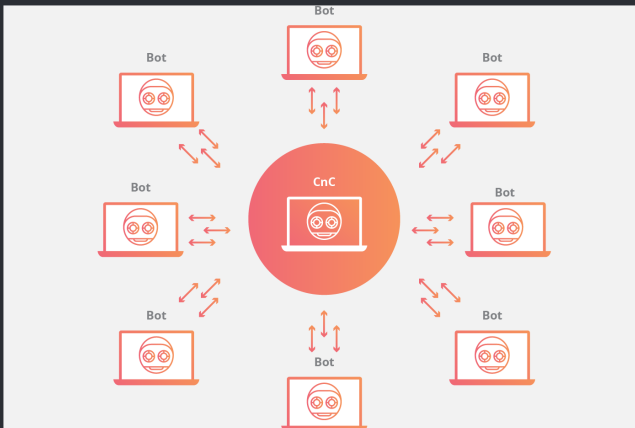
Modelo cliente-servidor

- Bots controlados por un servidor centralizado
- Conexión mediante software C&C
- Distintas topologías
- Son vulnerables

Arquitectura de una botnet

Topología de estrella

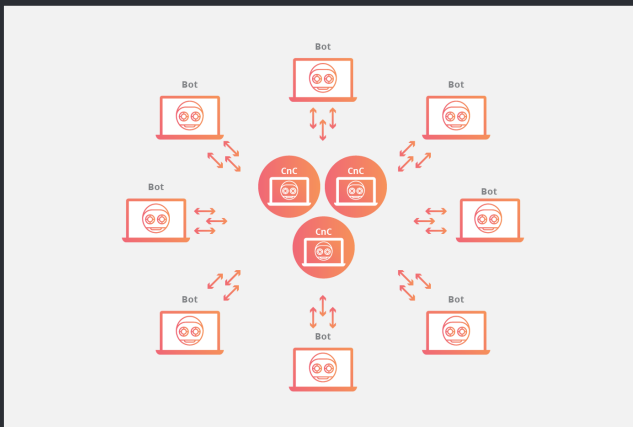
- Un servidor central controla cada uno de los bots



Arquitectura de una botnet

Topología multiservidor

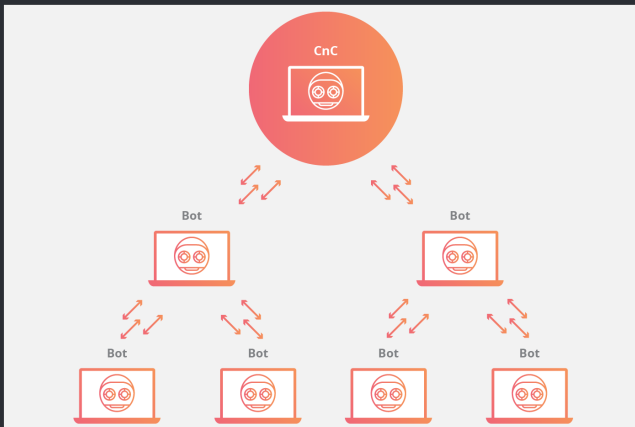
- Los bots son controlados por varios servidores centralizados



Arquitectura de una botnet

Topología jerárquica

- Se establece una relación de jerarquía entre bots



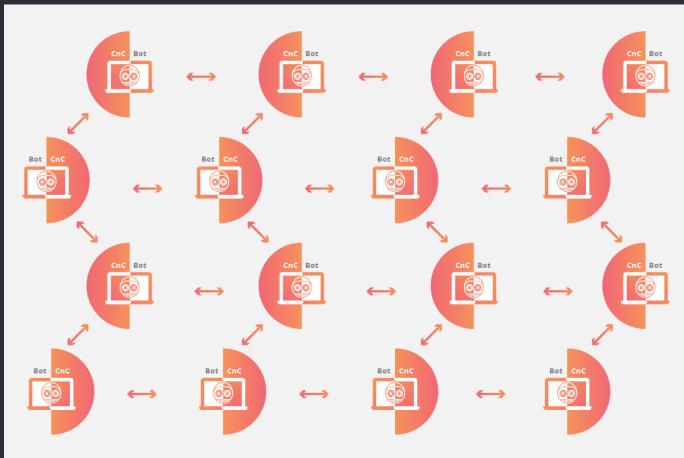
Arquitectura de una botnet

Modelo P2P

- Usa componentes de redes P2P
- La estructura forma parte de la botnet
- Computadores de confianza: acceso limitado
- Control de errores automático

Arquitectura de una botnet

Modelo P2P



Componentes de una botnet

Una botnet tiene 3 componentes:

1. Pastor (BotMaster o Botherder)
2. Protocolos de control
3. Zombies

Protocolos de control

Los protocolos de control se refieren a la forma de captar zombies e interactuar con ellos. Los protocolos más importantes son:

- Telnet
- IRC

`: herder!herder@channel.comTOPIC#attackDDoSwww.google.es`

`: botA!botA@infected.netANSWER#attacklamattackingwww.google.es`

- P2P

Índice

1. ¿Qué es una Botnet?
2. ¿Cómo se forma una botnet?
3. Estructura de una botnet
 - 3.1 Arquitectura
 - 3.2 Componentes
 - 3.3 Protocolos de control
4. ¿Qué hace una Botnet?
5. Cómo saber si formo parte de una botnet
6. Cómo evitarlo
7. Botnets famosas

¿Qué hace una Botnet?

Las botnets se usan generalmente para llevar a cabo actividades que generen beneficios económicos.

- Controla una gran cantidad de dispositivos de manera fácil.
- Simplifica la automatización de tareas complejas
- Permite usar la potencia de varios PC's para realizar una tarea

Buenos usos

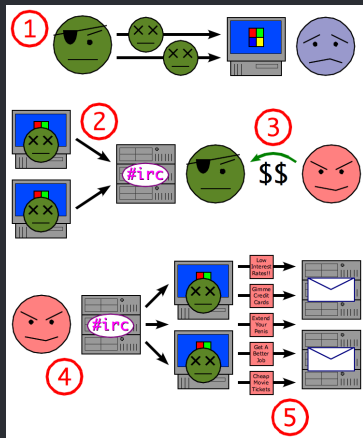
- **Computación paralela**
- **Minería de Bitcoins:** utilizar el procesamiento de los bots para generar bitcoins

Usos maliciosos

- **Envío de Spam** : enviar correos basura para transmitir virus, phishing...
- **Ataques DDoS**: hacer que una página web deje de funcionar
- **Manipulación de encuestas**: llevar a cabo votaciones masivas
- **Abuso de los servicios de pago por publicidad**: acceder a páginas de publicidad que generen beneficios económicos
- **Obtención de datos personales**: recopilar información del usuario de un dispositivo infectado

Ejemplo

Usando una botnet para enviar Spam



1. El operador de la botnet manda virus/gusanos/etc a los usuarios.
2. Los PCs entran en el IRC o se usa otro medio de comunicación.
3. El Spammer le compra acceso al operador de la Botnet.
4. El Spammer manda instrucciones a los PC infectados...
5. ... causando que éstos envíen Spam a los servidores de correo.

Índice

1. ¿Qué es una Botnet?
2. ¿Cómo se forma una botnet?
3. Estructura de una botnet
 - 3.1 Arquitectura
 - 3.2 Componentes
 - 3.3 Protocolos de control
4. ¿Qué hace una Botnet?
- 5. Cómo saber si formo parte de una botnet**
6. Cómo evitarlo
7. Botnets famosas

Cómo saber si formo parte de una botnet



- Las botnets son difíciles de detectar
- Los bots permanecen ocultos hasta que realizan alguna tarea
 - Ralentizan el dispositivo
 - Aparición de mensajes extraños
 - Fallos concretos
- Herramientas y software específico

Índice

1. ¿Qué es una Botnet?
2. ¿Cómo se forma una botnet?
3. Estructura de una botnet
 - 3.1 Arquitectura
 - 3.2 Componentes
 - 3.3 Protocolos de control
4. ¿Qué hace una Botnet?
5. Cómo saber si formo parte de una botnet
6. Cómo evitarlo
7. Botnets famosas

Cómo evitarlo

No es fácil: depende del SO, del software de seguridad, etc.

- Servicio anti-botnets de OSI
<https://www.osi.es/es/servicio-antibotnet>
- Herramienta anti-bots de INCIBE
<https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antibotnet>
- Antivirus específicos: Rubotted
- Usar un navegador actualizado

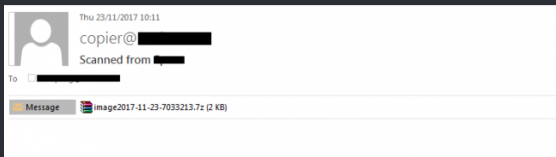
Índice

1. ¿Qué es una Botnet?
2. ¿Cómo se forma una botnet?
3. Estructura de una botnet
 - 3.1 Arquitectura
 - 3.2 Componentes
 - 3.3 Protocolos de control
4. ¿Qué hace una Botnet?
5. Cómo saber si formo parte de una botnet
6. Cómo evitarlo
7. Botnets famosas

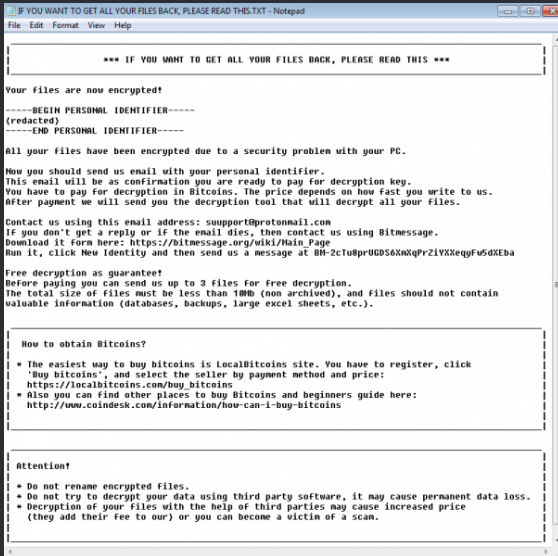
Botnets famosas

Botnet Necurs

- Responsable de una gran campaña de phishing
- Descubierta el 23 de noviembre, ya había enviado 12 millones de emails
- Ransomware Scarab:
 - Cifra ordenadores con Windows
 - Desactiva opciones de recuperación
 - Exige al usuario un pago en bitcoins
- Emails de la forma:



- El mensaje de rescate es el siguiente:



IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT - Notepad

File Edit Format View Help

*** IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS ***

Your files are now encrypted!

-----BEGIN PERSONAL IDENTIFIER-----
{redacted}
-----END PERSONAL IDENTIFIER-----

All your files have been encrypted due to a security problem with your PC.

Now you should send us email with your personal identifier.
This email will be as confirmation you are ready to pay for decryption key.
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.

Contact us using this email address: support@protonmail.com
If you don't get a reply or if the email dies, then contact us using Bitmessage.
Download it from here: https://bitmessage.org/wiki/Main_Page
Run it, click New Identity and then send us a message at BM-2ctU8prUGDS6XnXqPrZiVXXeqyFu5dXEba

Free decryption as guarantee!
Before paying you can send us up to 3 files for Free decryption.
The total size of files must be less than 100Mb (non archived), and files should not contain valuable information (databases, backups, large excel sheets, etc.).

How to obtain Bitcoins?

- * The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price:
<https://localbitcoins.com/buy-bitcoins>
- * Also you can find other places to buy Bitcoins and beginners guide here:
<http://www.coindesk.com/information/how-can-i-buy-bitcoins>

Attention!

- * Do not rename encrypted files.
- * Do not try to decrypt your data using third party software, it may cause permanent data loss.
- * Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Botnets famosas

Botnets extractoras

- Malware con tecnología blockchain capaz de instalar software de extracción de criptomonedas
- 1.650.000 ataques de este tipo en lo que va de año
- Usa dos botnets
 - 5.000 PCs, 165.000 euros mensuales
 - 4.000 PCs, 25.000 euros mensuales
- Distribución mediante programas de adware
- Se suelen extraer las criptomonedas Zcash y Monero: transacciones anónimas

Botnets famosas

GameOver Zeus

- Relacionada con el ransomware Cryptolocker
- Variante de un troyano bancario usado para el robo de credenciales
- Utiliza redes P2P
- Añade código en el navegador para interceptar el envío de usuarios y contraseñas
- Desmantelada por el FBI en junio de 2014



Botnets famosas

ZeroAccess botnet

- Troyano que afecta a sistemas Windows
- Usada para minería de Bitcoins y fraude en campañas online de anuncios
- Distribuido a través de páginas comprometidas que aprovechan vulnerabilidades del sistema

