Botnet

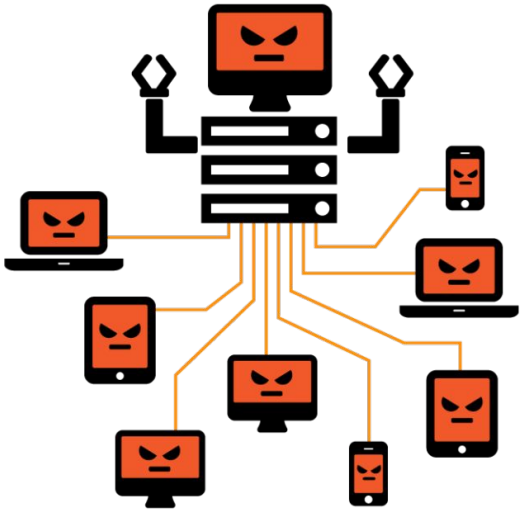
Alejandra González Vélez
Angie Valentina Córdoba Pinzón
Miguel Angel Romero Rosas

Qué es un Botnet?

Una botnet es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar malware o realizar ataques de denegación de servicio distribuido (DDoS) sin el conocimiento o el consentimiento de los propietarios reales de los equipos.

Qué es un Botnet?

Los botnets pequeños pueden incluir cientos de PCs infectados, mientras que los mayores utilizan millones de equipos. A menudo, se entiende el botnet como una entidad única, sin embargo los creadores de este malware lo venden a cualquiera que pague por él. Por este motivo, existen docenas de botnets separados usando el mismo malware y operando a la vez.



¿Cómo infecta al equipo?

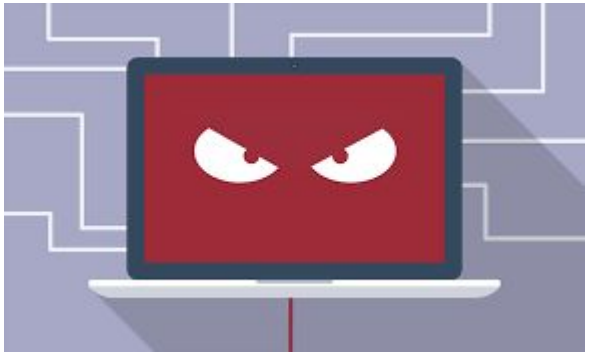
- Ataques drive-by downloads

El proceso requiere de diferentes pasos y el atacante debe encontrar una página web con una vulnerabilidad que pueda explotar. Entonces, el hacker carga su código malicioso en la página y explota la vulnerabilidad en un navegador web como Google Chrome o Internet Explorer. El código redirige el navegador del usuario a otro site controlado por el delincuente donde el código bot se descarga e instala en el equipo.

¿Cómo infecta al equipo?

- Email

El proceso es más simple. El atacante envía una gran cantidad de spam, donde se adjunta un archivo Word o PDF con un código malicioso o un enlace a la página que aloja el código.

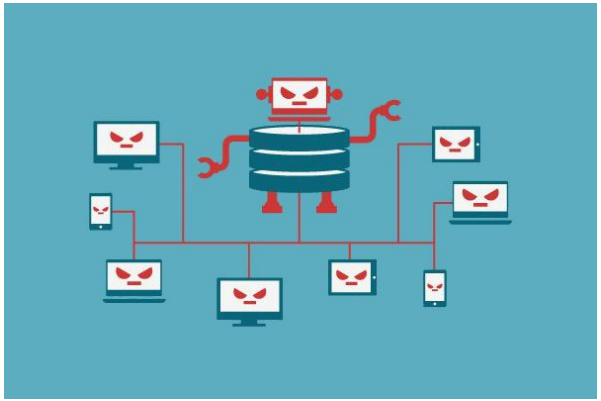


Usos

El uso más común de los botnets son lo ataques DDoS. Estos ataques utilizan la potencia del ordenador y el ancho de banda de cientos o miles de equipos para enviar gran cantidad de tráfico a una página web específica y sobrecargar dicho site. Existen diferentes tipos de ataques DDoS, pero el objetivo siempre es el mismo: colapsar una web.

¿En qué parte se encuentra el ataque informático?

Un número significativo de botnets utilizan HTTP para implementar los C&C. Dado que se trata de un protocolo sin estado, no permite que los herders envíen comandos a los drones en tiempo real, por lo cual el bot debe consultar la existencia de nuevos comandos en forma periódica.



¿Diferencias entre Demonio y Zombie?

Un demonio, es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Este tipo de programas se ejecutan de forma continua (infinita), vale decir, que aunque se intente cerrar o matar el proceso, este continuará en ejecución o se reiniciará automáticamente. Todo esto sin intervención de terceros y sin dependencia de consola alguna.

¿Diferencias entre Demonio y Zombie?

Las máquinas zombies son computadoras infectadas por algún tipo de malware, al servicio de terceras personas para ejecutar actividades hostiles con total desconocimiento del propietario o administrador del equipo. La misión de los botnet es la de gestionar las máquinas zombies creando una infraestructura común de mando y control.

Captura Wireshark

4	0.240072	10.7.17.101	169.239.129.23	HTTP	378 GET /A HTTP/1.1
6	0.479163	169.239.129.23	10.7.17.101	HTTP	447 HTTP/1.1 200 OK
11	4.295122	10.7.17.101	169.239.129.23	HTTP	113 GET /B HTTP/1.1
13	4.534433	169.239.129.23	10.7.17.101	HTTP	607 HTTP/1.1 200 OK
14	4.589158	10.7.17.101	169.239.129.23	HTTP	94 GET /donate HTTP/1.1
629	6.527674	169.239.129.23	10.7.17.101	HTTP	563 HTTP/1.1 200 OK

```
Host: t69c.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://t69c.com/A]
[HTTP request 1/1]
[Response in frame: 6]
```