Botnets

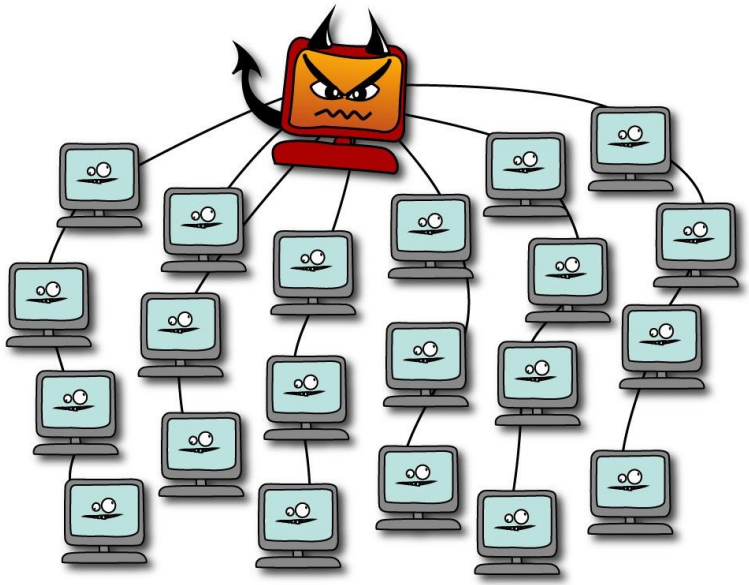
Cracking y DoS distribuidos

¿Qué son las Botnets?

Serie de máquinas y dispositivos conectados a Internet, controlados por un software de comando y control.

En general hablamos de botnet cuando los usuarios no saben que forman parte de esta red y por lo tanto tiene una connotación negativa.

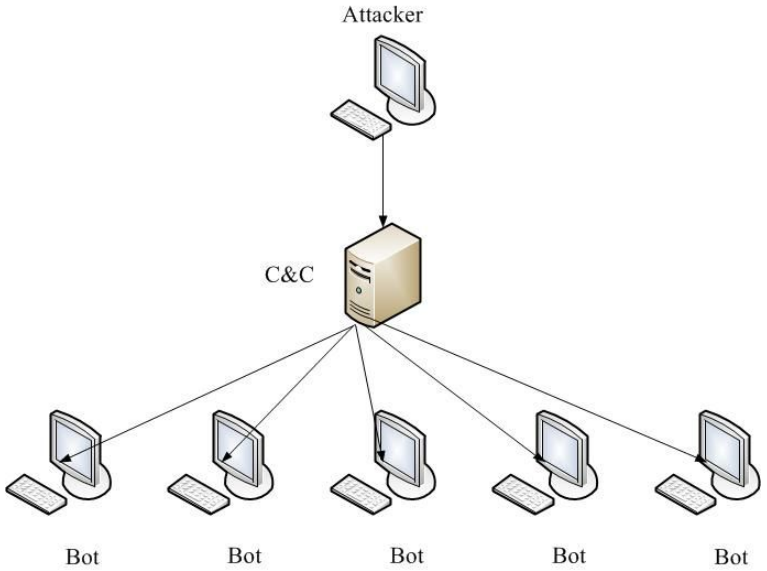
Puede ser vista como un sistema distribuido.



Tipos de botnets

- Centralized
  - IRC
  - HTTP
  - TCP

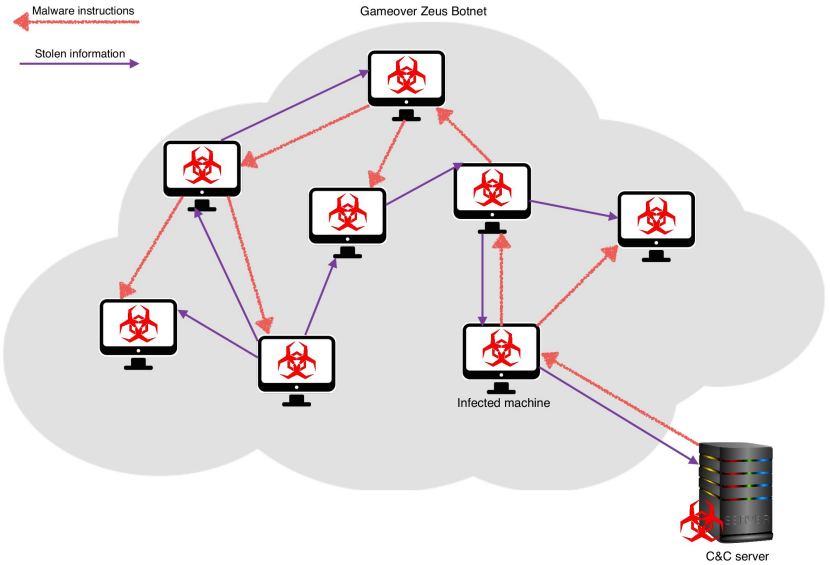
Se basan en utilizar un servidor central para enviar comandos a los distintos bots.



Tipos de botnets

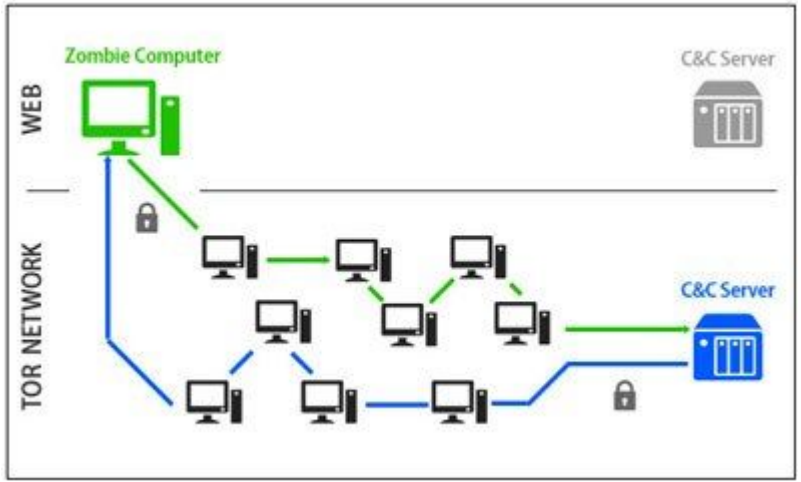
- Peer to peer (P2P)

El atacante envía un comando a algunas botnets que él conozca, y estas lo envían por la red.



Tipos de botnets

- TOR



¿Cómo se construyen?

- Mediante un engaño a los usuarios para descargar el software.
  - Correos electrónicos
  - Sitios web de forma manual.
  - Sitios web de forma automática (Exploits Drive-by, ActiveX, Java Applets).
- Infecciones sin interacción con la víctima:
  - Exploits locales o remotos.
- Mecanismos de escaneo y propagación.

Usos

- **Denegación de servicios distribuido (DDoS).**
- **Cracking.**
- Adwares (publicidad no deseada).
- Spam de correos.
- Minería de criptomonedas.
- Spyware (robar información sensible).
- Auto propagación.
- ...

Ejemplos de botnets hoy en dia.

- Conficker, Mariposa, BredoLab
- Star wars twitter botnet
- Mirai, Hajime, Satori IoT

Cracking

- Recuperar contraseñas a partir de datos almacenados y/o transmitidos por un computador.
- Normalmente adivinando contraseñas y probandolas contra un hash criptográfico.

Tipos de ataque

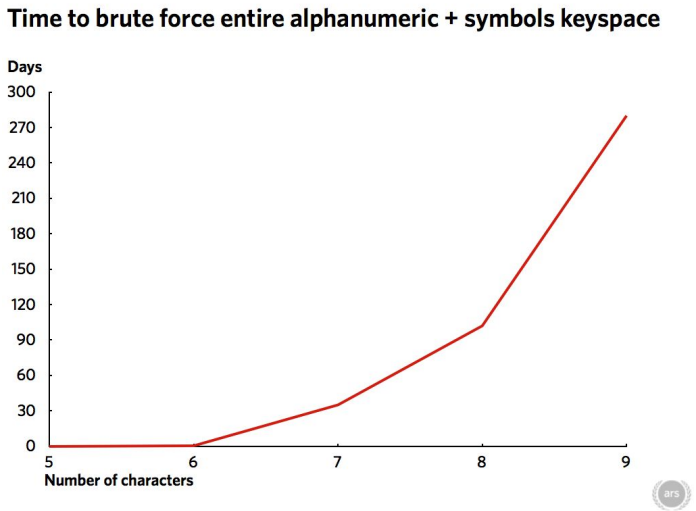
- Fuerza bruta.
- Diccionario.
- Diccionario con reglas.

Ataque por fuerza bruta

Ventajas:

- Probar todas las combinaciones posibles para distintos conjuntos de caracteres.
- Permite encontrar contraseñas sin patrones aparentes.

Desventajas:



Ataque con diccionario

Ventajas:

- Se basa en que la mayoría de las personas ocupa palabras reales como contraseñas.
- Se prueba un conjunto de palabras comunes, de forma previa a un posible ataque por fuerza bruta.
- Mucho más rápido que el ataque por fuerza bruta.
- Permite encontrar contraseñas de mayor largo.

Desventajas:

- Simplemente cambiar una letra de la palabra por un número rompe este ataque.

Ataque con diccionario y reglas

- Se basa en el ataque por diccionario, pero ocupando reglas que modifican las palabras de este.
- Algunos ejemplos de reglas podrían ser:
  - Cambiar determinadas letras por números o símbolos (e por 3, s por $).
  - Agregar la secuencia 123 al final de la palabra.
  - Capitalizar la primera letra.
  - ...

Porcentaje de acierto en LifeBoat

LifeBoat es una base de datos filtrada de una comunidad de un juego online. Contra esta se probaron distintos diccionarios con reglas.

Rule	Total Candidates	Cracked	% Cracked
dive	1,421,219,827,456	2,843,085	65.64
_NSAKEY.v2.dive	1,768,370,620,544	2,784,741	64.30
generated2	933,992,405,632	2,606,565	60.18
d3ad0ne	489,063,363,712	2,580,399	59.58
rockyou-30000	430,298,880,000	2,557,422	59.05
T0XICv1	171,129,864,576	2,357,989	54.44
InsidePro-HashManager	92,801,125,120	2,247,349	51.89

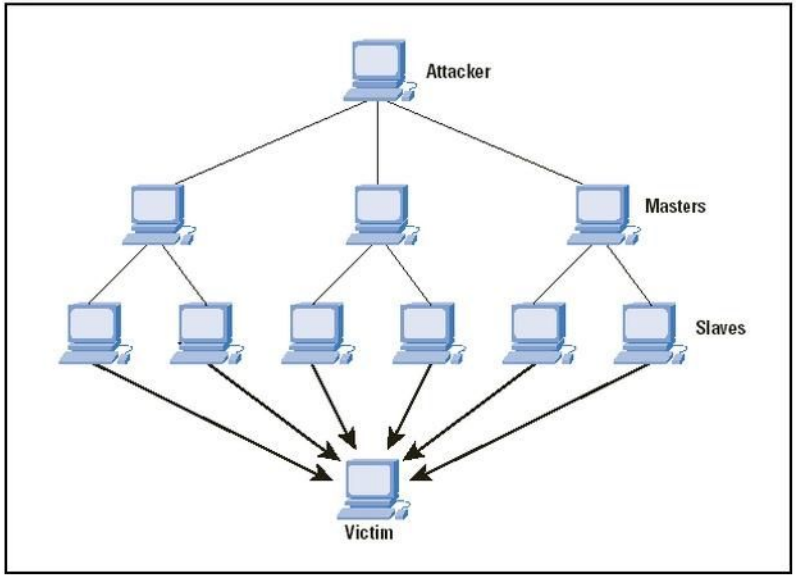
Porque cracking distribuido?

Demo

Ataque de denegación de servicio distribuido

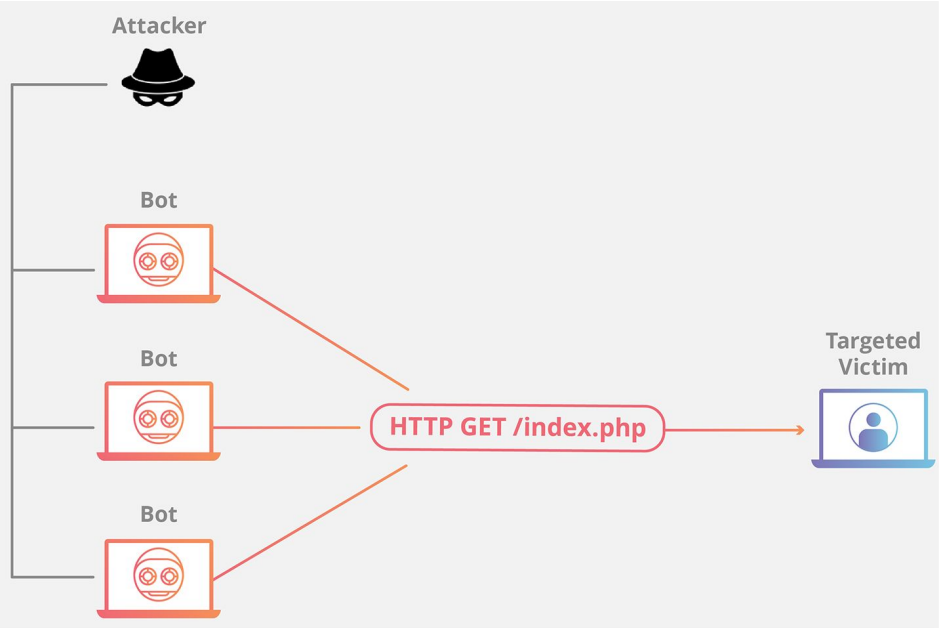
Es un tipo de ataque cuyo objetivo es inhabilitar un servidor, servicio o infraestructura.

Comúnmente utilizan botnets que hacen distintas peticiones a la víctima.



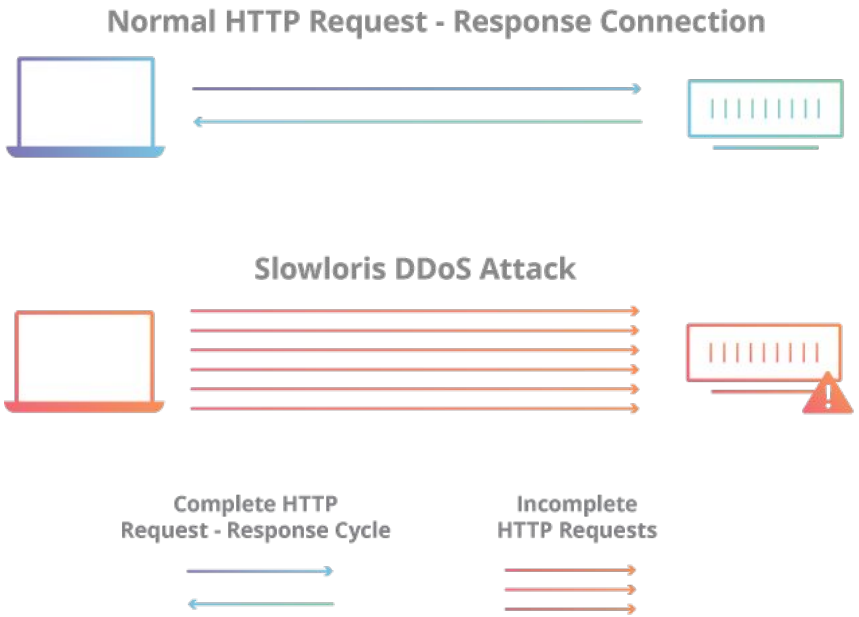
Tipos de ataque DDoS

HTTP Flood



Consiste en realizar muchas request HTTP a recursos del servidor, de tal forma de que este no pueda responderlas todas y deje de aceptar peticiones.

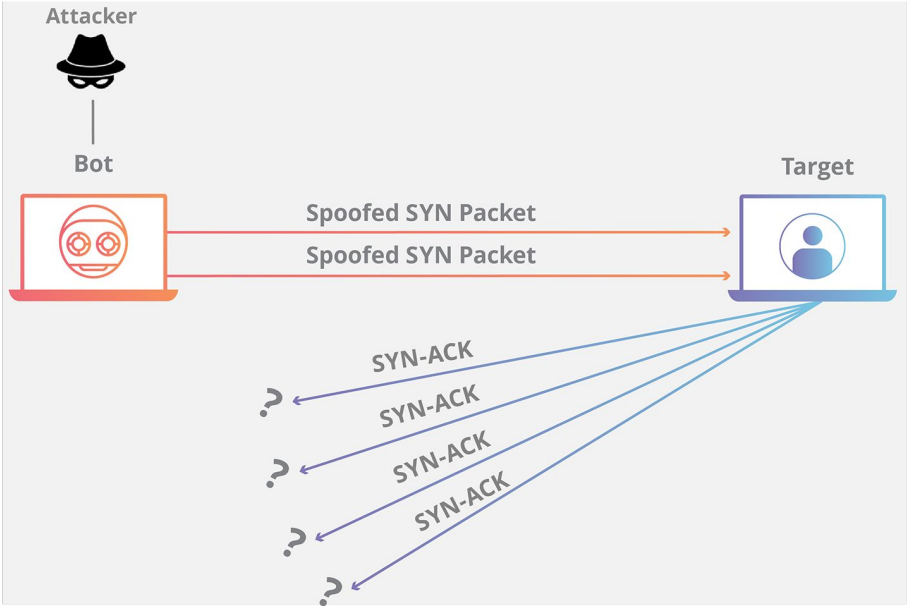
HTTP Flood (Slowloris)



Consiste en enviar muchas requests incompletas, y seguir enviando paquetes de estas requests para que el servidor no pueda cerrar las conexiones.

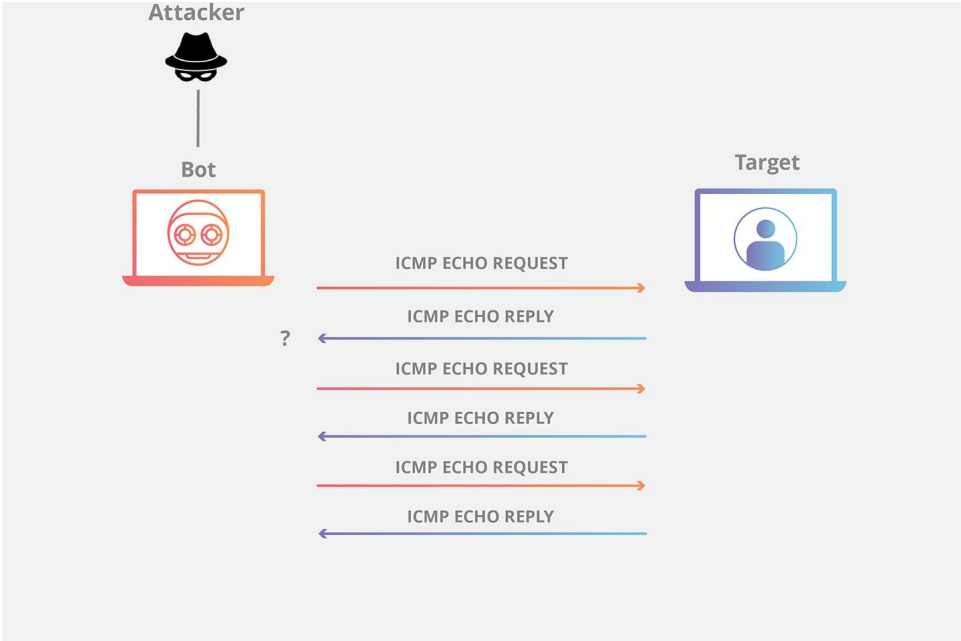
Es difícil de detectar (ya que son request válidas) y no se requiere una botnet necesariamente.

TCP Sync Flood



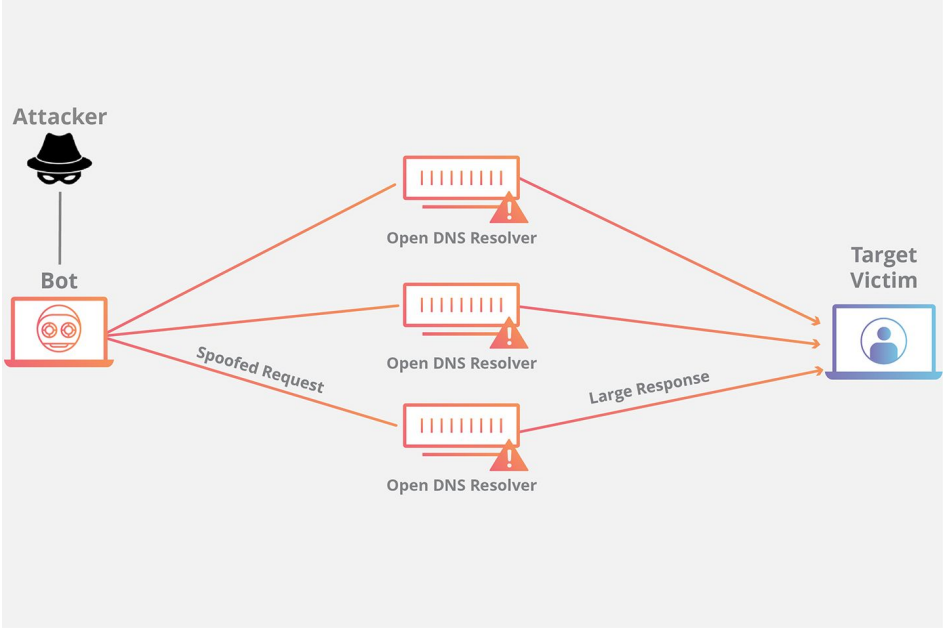
Aprovecha el protocolo TCP para enviar paquetes SYN con la ip de origen alterada, de tal forma de que el servidor envíe los paquetes SYN-ACK a entes que no están al tanto de estas conexiones.

ICMP echo request flood



Similar a HTTP flood, pero ocupando el protocolo ICMP.

Amplified DDoS



Consiste en enviar requests con ip's de origen alteradas a servidores para que envíen su respuesta a la víctima.

Se llaman amplificadas ya que se envían requests pequeñas y se obtienen respuestas de grandes volúmenes.

Amplified DDoS

UDP-based Amplification Attacks

Protocol	Bandwidth Amplification Factor
Memcached	50000
NTP	556.9
CharGen	358.8
DNS	up to 179 [51]
QOTD	140.3
Quake Network Protocol	63.9
BitTorrent	4.0 - 54.3 [52]
SSDP	30.8
Kad	16.3
SNMPv2	6.3
Steam Protocol	5.5
NetBIOS	3.8

Mitigación

- Son muy difíciles de mitigar, porque cuesta distinguir de antemano entre conexiones reales y conexiones del ataque.
- Los servicios de mitigación más importantes se basan en “aguantar” todo el tráfico y redirigir las solicitudes válidas.
- Ejemplo: Akamai Prolexic

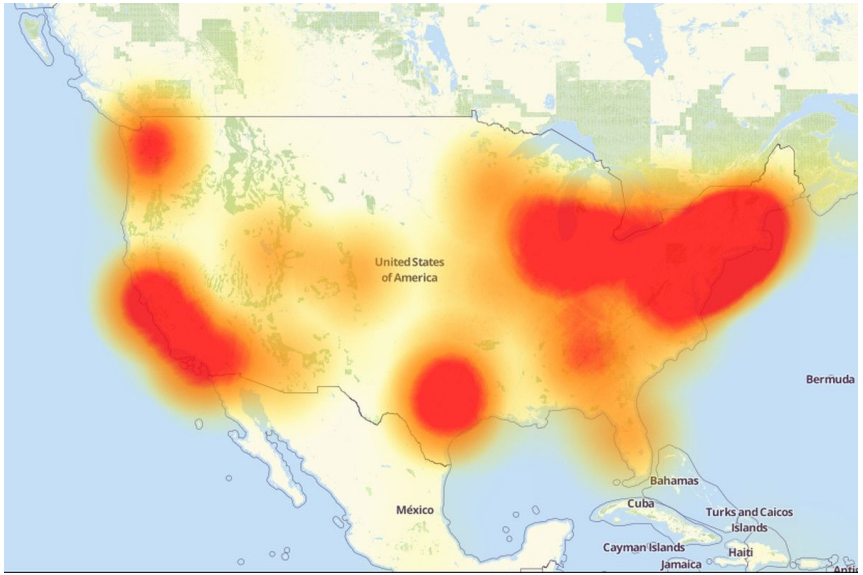
Ejemplos

Ataque a Spamhause

- Ataque realizado el año 2013.
- 300 Gb/s (el más grande hasta esa fecha)
- Dirigido a empresa que provee listas de *spammers* y que es utilizada por muchos servicios.
- Como consecuencia se genera un gran tráfico de correo spam por Internet.
- Casi colapsa el nodo de Internet del Reino Unido.

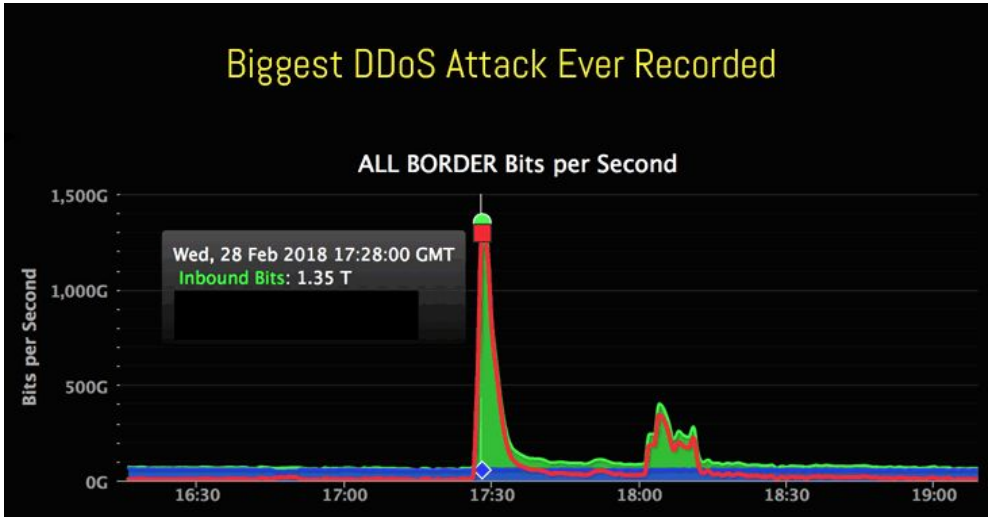
Ataque a Dyn

DDoS realizado el 21 de octubre de 2016, ocupando la botnet Mirai.



Ataque a Github

- DDoS realizado el 28 de Febrero de 2018.
- Se ocuparon servidores memcached para amplificar el ataque.
- 1,35 Tb/s



¡Muchas gracias!

El código usado para la demo se puede visitar en:

https://github.com/Mdelaf/botnet-demo