“Hey, honey, can websites catch on fire?”
The Anatomy of a DDoS

Janna Hilferty
DevOps Engineer
Twitter: @warjanna
Blog: https://techgirlkb.guru
TOC

What is a DDoS?  Mitigation techniques
Botnets & Malware  Prevention & Legislation
IoT Threat Landscape  Q&A
Attacks & the OSI model
DDoS = Distributed Denial of Service
A malicious attempt to disrupt normal traffic of a targeted server, service or network ...
... by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

- Cloudflare
Visualization of a DDoS - IPViking from Norse Corp
Modern DDoS Examples
1.3TB/s: Github Memcached Servers (2018)

Real-time traffic from the DDoS attack.

AKAMAI
Android-based WireX attacks (2017)
1.1TB/s Mirai botnet attacks (2016)

Mira botnet infections globally. (Image courtesy of Imperva.)
Level 3/DynDNS attacks (2016)

A depiction of the outages caused by the Mirai attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.
DDoS attackers may seek a ransom, revenge, secure data, or simply to disarm your business.
Cost of a DDoS

On average, the cost of a DDoS attack for enterprises was $2 million, and the cost of a DDoS attack for small and medium-sized businesses (SMBs) was $120,000.

- Kaspersky 2017 study
Cost of a DDoS

1. On average, the cost of a DDoS attack for enterprises was $2 million, and the cost of a DDoS attack for small and medium-sized businesses (SMBs) was $120,000.
   - Kaspersky 2017 study

2. 49% of DDoS attacks last between 6-24 hours, averaging $40,000/hr.
   - Incapsula study
Cost of a DDoS

33% of respondents acknowledged customer data theft, and 19% of respondents suffered intellectual property loss.

- Incapsula study

Janna Hilferty
@warjanna
Cost of a DDoS

33% of respondents acknowledged customer data theft, and 19% of respondents suffered intellectual property loss.

- Incapsula study

64% of respondents say reputation damage is the main consequence of a denial-of-service attack. This is followed by diminished productivity for IT staff (35%) and revenue losses (33%).

- Ponemon Institute (Akamai study)

Janna Hilferty
@warjanna
Botnet
Botnet = robot + network
Structure of a botnet

Bot herder
Structure of a botnet

Bot herder  Malware

Janna Hilferty
@warjanna
Structure of a botnet

Bot herder

Malware

Zombies

Janna Hilferty
@warjanna
IoT Threat Landscape

Janna Hilferty
@warjanna
Landscape
Internet of Things

The sphere of internet-connected devices is changing faster than regulation and security patches can keep up.
Landscape
Internet of Things

The sphere of internet-connected devices is changing faster than regulation and security patches can keep up.

Implications:

- Security settings
- Factory-default passwords
- Peer-to-peer communications
- Open ports
- ‘Listening’ devices
- Open databases/cloud drives
The sphere of internet-connected devices is changing faster than regulation and security patches can keep up.

Implications:

- Security settings
- Factory-default passwords
- Peer-to-peer communications
- Open ports
- ‘Listening’ devices
- Open databases/cloud drives

SANITY CHECKS

When was the last time you checked your router, thermostat, wireless speakers, or smart doorbell for a security update?

Janna Hilferty
@warjanna
Rule #1: Every internet-connected device is a potential entry-point for malware.
Rule #2: If you can install malware on it, an attacker can harness it to attack you & others.
IoT + Malware = <3

MALWARE

MALWARE EVERYWHERE
Scanning for open ports
Click-fraud & spam
R u a bot?

The users of devices with malware are often completely unaware their device is being remotely controlled by the attacker.
Attacks & the OSI Model
The OSI model

Kind of like all the layers of an internet cake.
1 - Physical Layer
2 - Data Link Layer
3 - Network Layer
4 - Transport Layer
5 - Session Layer
6 - Presentation Layer
7 - Application Layer
DDoS and the OSI model

Most attacks happen on layers 3 (Network), 4 (Transport), and 7 (Application).

Layer 3 attacks: IP Spoofing, ICMP floods, Packet sniffing

Layer 4 attacks: Syn floods

Layer 7 attacks: HTTP floods (botnets), DNS poisoning, DNS amplification
Mitigation Techniques
The best mitigation is to protect against DDoS *before it happens.*
DDoS mitigation: unprotected server

1

Unprotected origin server
DDoS mitigation: unprotected server

1. Unprotected origin server
2. Attacker identifies origin server IP and sends traffic
DDoS mitigation: unprotected server

1. Unprotected origin server
2. Attacker identifies origin server IP and sends traffic
3. Firewall added, but attackers bypass (origin already known)

Janna Hilferty
@warjanna
DDoS mitigation: unprotected server

1. Unprotected origin server
2. Attacker identifies origin server IP and sends traffic
3. Firewall added, but attackers bypass (origin already known)
4. Migration of origin server required
DDoS mitigation: protected server

1. Protected origin server
DDoS mitigation: protected server

1. Protected origin server
2. Attack is deflected at the firewall OR network soaks attack
DDoS mitigation: protected server

1. Protected origin server
2. Attack is deflected at the firewall OR network soaks attack
3. No downtime or migration required - origin server remains online.

Janna Hilferty
@warjanna
DDoS Protection Services

01 | Managed WAF services

02 | Caching and CDN services

03 | In-server protection
Prevention
What is action is being taken against DDoS attackers?
Legislation against DDoS

01 | Computer Fraud & Abuse Act (USA)

02 | Police & Justice Act (UK)
Anonymous petitions White House to label DDoS as “free speech”
2016
Europol partnership against DD4BC
FBI asks DDoS victims to come forward
2017
UK, US, Netherlands partner to take down webstresser.org
Mirai botnet creators assist FBI to take down new attackers
2018
Interpol goes after users of webstresser.org
2019
FBI takes down 15 DDoS-for-hire websites
Q&A
Thank you.

Janna Hilferty
DevOps Engineer
Twitter: @warjanna
Blog: https://techgirlkb.guru