black hat®
MIDDLE EAST AND AFRICA

Demystifying Practical DoS Attacks

15 – 17 NOVEMBER 2022
RIYADH FRONT EXHIBITION CENTRE
SAUDI ARABIA

Mazin Ahmed (FullHunt.io)

STRATEGIC SPONSORS

SPIRE INFORMATION SECURED
IBM

GOLD SPONSORS

Infoblox
Honeywell

CO-ORGANISED BY

informatech
الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

DoS Attacks are Dead

Demystifying Practical DoS Attacks

Mazin Ahmed

BlackHat 2022

mazin@mazinahmed.net | @mazen160

About Me

Mazin Ahmed

- **AppSec and Offensive Security Engineer**
- **Founder of FullHunt.io**
- **Occasional Bug Bounty Hunter: Acknowledged by Facebook, Twitter, LinkedIn, Zoom, and more**
- **In love ❤️ with Cloud security, security automation, DevSecOps, distributed systems, and Web-App security**

Read more at **mazinahmed.net**

CLOUDFLARE The Cloudflare Blog

Subscribe to receive notifications of new posts:

Email Address Subscribe

Product News | Speed & Reliability | Security | Serverless | Zero Trust | Developers | Deep Dive | Life @Cloudflare

Cloudflare mitigates 26 million request per second DDoS attack

06/14/2022

Akamai

Blog > Security > Largest European DDoS Attack on Record

Largest European DDoS Attack on Record

Craig Sparling
July 27, 2022

Share

The Register

{* SECURITY *}

Palo Alto bug used for DDoS attacks and there's no fix yet

There goes the weekend...

Jessica Lyons Hardcastle

Fri 12 Aug 2022 // 23:17 UTC

4

A high-severity Palo Alto Networks denial-of-service (DoS) vulnerability has been exploited by miscreants looking to launch DDoS attacks, and several of the affected products won't have a patch until next week.

The vulnerability, tracked as CVE-2022-0028, received an 8.6 out of 10 CVSS score, and it affects PAN OS, the operating system in Palo Alto Networks' network security products. Panorama M-Series or Panorama virtual appliances, and Palo Alto Networks, have already had the issue fixed for cloud-based firewall and Prisma Access customers.

Google Cloud Blog

Identity & Security

How Google Cloud blocked the largest Layer 7 DDoS attack at 46 million rps

August 19, 2022

The problem still exists, and it’s getting worse…

Volume does not matter at DoS attacks

App-Level DoS is another nightmare

Notable Research

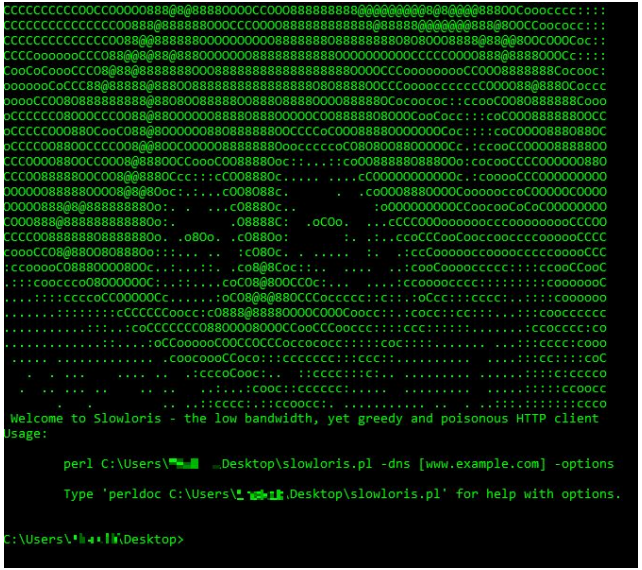
Notable Research: Slowloris (2005-2009)

One of the first Layer-7 DDoS attacks on HTTP Protocol.

Works by sending infinite number of HTTP request headers.

HTTP web-servers would try to wait, wait, and wait… until it can not process additional requests.

Apache, IIS are known to be affected.



Notable Research: XerXes (2010)

Developed by the famous American hacker, the Jester.

Used to take down WikiLeaks for two weeks from a single machine.

Potential leaked copy of Xerxes shows that it works by opening up thousands of TCP connections and sending continuous null packets.

The J3ST3r's laptop at The Spy Museum :)

https://twitter.com/IntlSpyMuseum/status/1128272399819059200

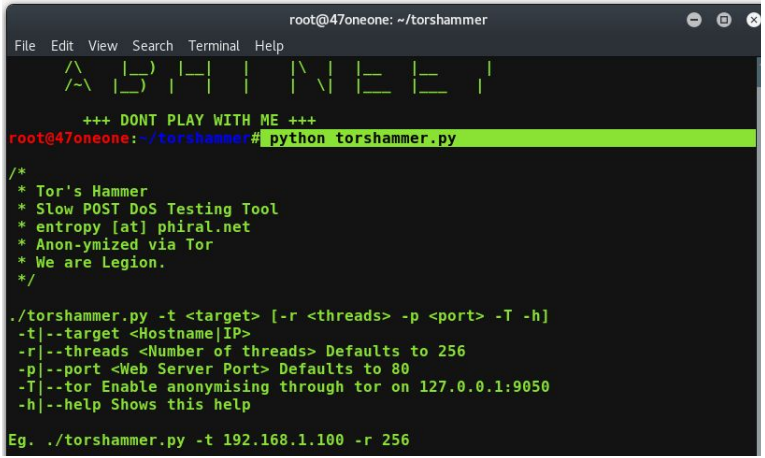
Notable Research: TorsHammer, R-U-D-Y (2012)

Variants of Slow Post HTTP Layer 7 Attacks.

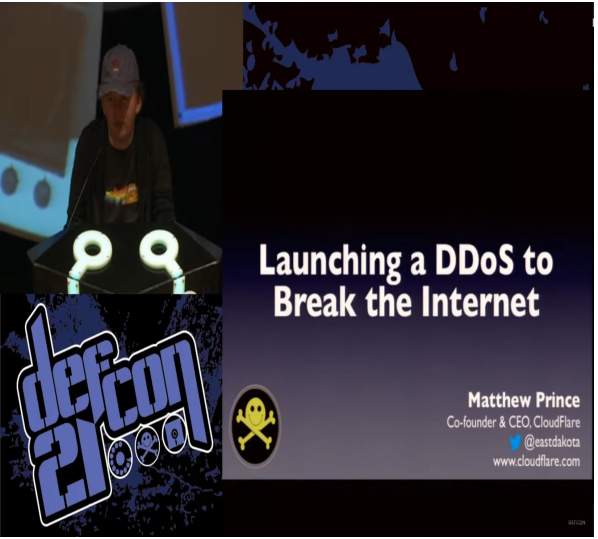
Focusing on different angles of stressing the HTTP transaction.

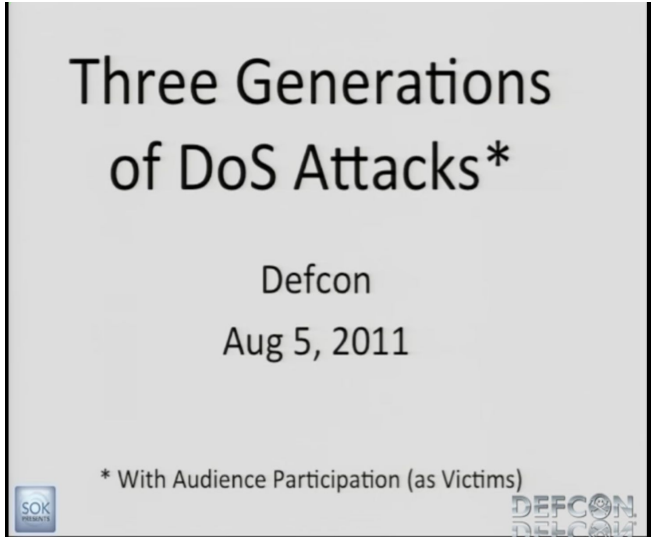
R-U-Dead-Yet by Raviv Raz.

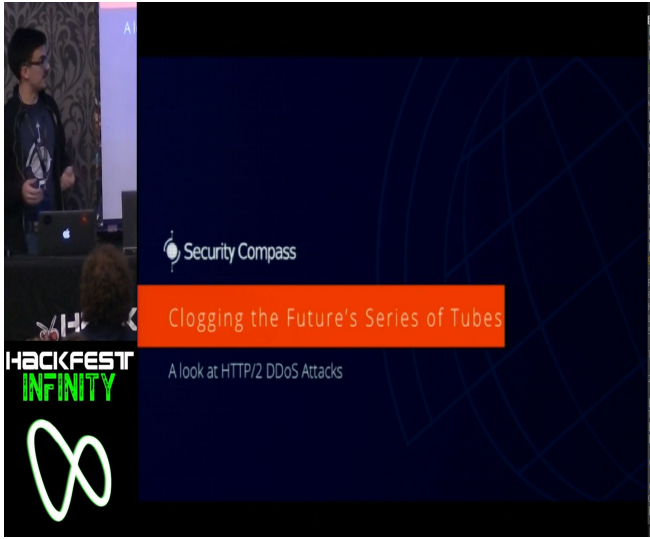
TorsHammer - by Anonymous.



DoS Attacks History - Amazing talks







TODAY

Stressful.IO — My Dream Security Tool

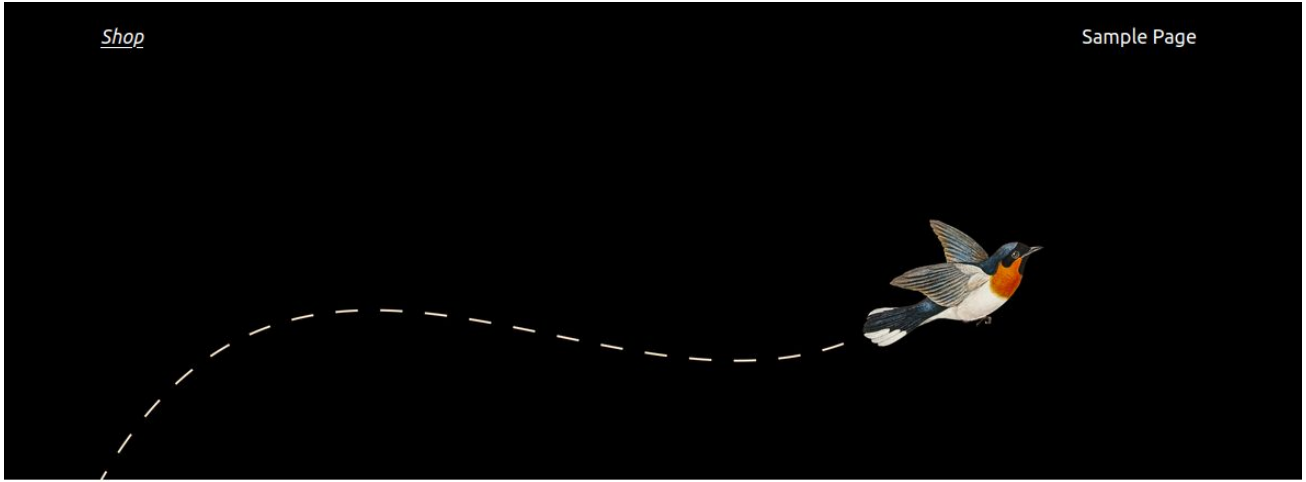
Stressful.IO - My Dream Security Tool

```
root@secbot  ~  ./stressful --playbook dev.yml
>>> Stressful-Engine (v0.3.4) <<<
INFO[2022-08-21T18:32:22Z] Setting playbook to: dev.yml
• Target:→ [redacted]
• IP Address:→ [redacted]
• Port:→ 443
• SSL:→ true
• Duration:→ 20s
• Name:→ test
• Description:→ HTTP Flooder
• Module:→ HttpGetFlooder_KeepAlive_loop
• Workers Count:→ 600
• IP Type:→ ipv4
```

Why Stress testing is evolving, and it will be a nightmare soon?

- Getting Ephemeral resources has became much accessible than ever been.
- Cost of running Cloud assets has significantly reduced.
- Launching DDoS with 1000 Gbps legally is possible today.
- Getting 46 Million HTTP Request per Second is possible today.
- Research and tools has became much accessible than ever in the market.
- Not to speak about Booters, Amplification Attacks, Internet Scans data that shows Amplification servers freely available to anyone.

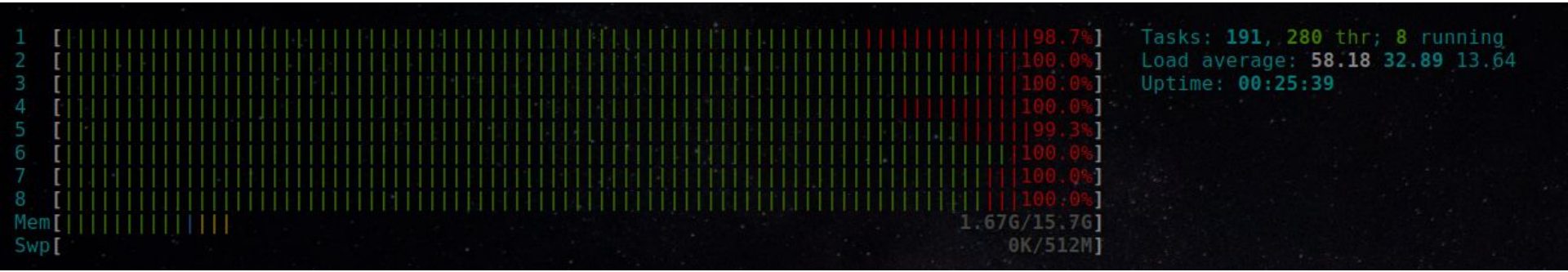
Stressful Framework in Action



Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Stressful Framework in Action



Stressful Framework in Action

Edinburgh Http Timeout 39.2s	**Amsterdam** TCP Connection Failed 0.0s	**Berlin** TCP Connection Failed 0.0s	**Brussels** Http Connect Failure 21.2s
Hamburg TCP Connection Failed 0.0s	**Buenos Aires** TCP Connection Failed 0.0s	**Milan** Http Timeout 30.2s	**Frankfurt** TCP Connection Failed --
Groningen TCP Connection Failed 0.0s	**São Paulo** TCP Connection Failed 0.0s	**Lelystad** TCP Connection Failed 0.0s	**Auckland** Http Connect Failure 24.1s
San Diego Http Timeout 30.1s	**London** Http Timeout 30.9s	**Beijing** TCP Connection Failed 0.0s	**Singapore** TCP Connection Failed 0.0s
Seoul Http Connect Failure 21.2s	**Jakarta** Http Connect Failure 21.4s	**New York** Http Connect Failure 24.1s	**New Delhi** Http Timeout 33.3s
Oslo TCP Connection Failed 0.0s	**Leipzig** Http Connect Failure 21.2s	**Vancouver** TCP Connection Failed 0.1s	**Los Angeles** Http Connect Failure 21.0s

Bug Bounties: Real-world companies

Company explicitly had a listing for Denial of Service in bug bounty scope.

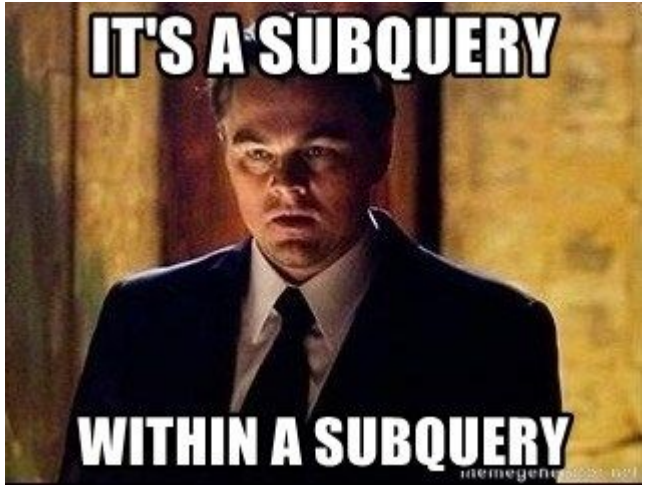
Mazen,

It's an amazing find :) Our server did infact became full on Apache and I had to reboot it. CentOS.

APIs can introduce DoS vulnerabilities

Processing APIs that requires significant resources:

- Headless rendering
- Data conversion through external subprocesses
- Report building that requires dozens of expensive DB queries.
- Any memory-expensive processing

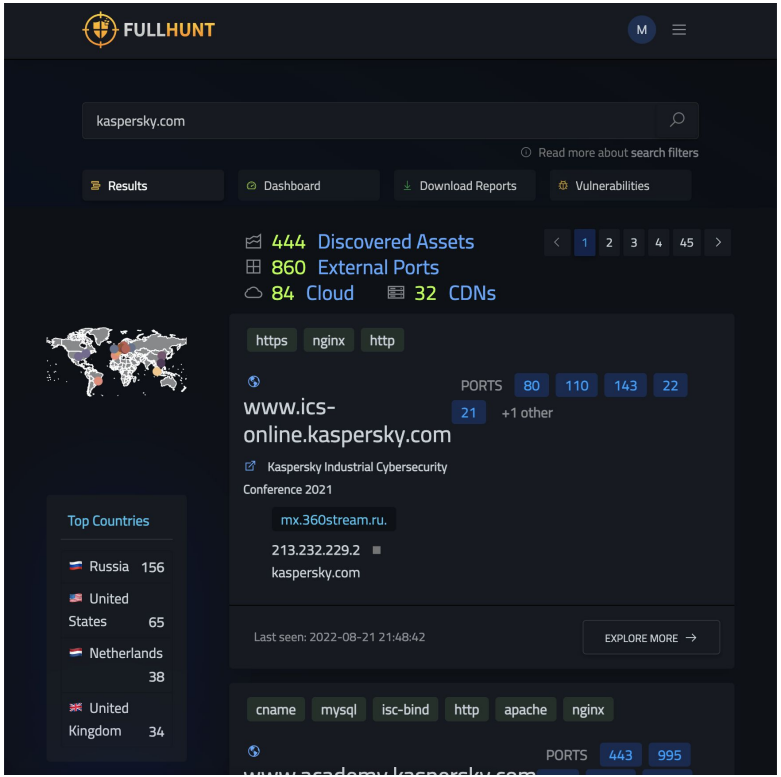


Real-World Bypasses of DDoS Defense Solutions

(You → CloudFlare/Imperva/Akamai → Target)

You can find servers that are not behind proxy with a single FullHunt query:

```
Domain:acme.org is_dos_defense:false
```



Real-World Bypasses of DDoS Defense Solutions

SSRFs

An endpoint can issue outbound requests can leak the origin host that is protected b CloudFlare.

Send Cancel

Target: https://ac101fb41f7cba2d809a73c200ae00c6.web-securit

Request

Pretty Raw Hex \n

```
1 POST /product/stock HTTP/1.1
2 Host: ac101fb41f7cba2d809a73c200ae00c6.web-security-academy.net
3 Cookie: session=xyNosiCGUwHtPVCF08tFbhkCyHQcplAH
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://ac101fb41f7cba2d809a73c200ae00c6.web-security-academy.ne
  t/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Origin:
  https://ac101fb41f7cba2d809a73c200ae00c6.web-security-academy.ne
  t
11 Content-Length: 107
12 Te: trailers
13 Connection: close
14
15 stockApi=
  http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fc
  heck%3FproductId%3D1%26storeId%3D1
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Connection: close
4 Content-Length: 3
5
6 203
```

Real-World Bypasses of DDoS Defense Solutions

Internet Scan Data

Search for HTTP/HTTPS assets that have keywords matching the target.

Connect to the IP while setting the Host header to the target host.

If accessible, launch stress tests there.

Tools & Databases

FullHunt Global Search

Shodan

ZoomEye

We </3 Cloud: Denial of Wallet Attacks

The attack would not take the site down, but will make the teams have a not so fun month.

It's not only AWS; this work on Azure, GCP, Alibaba Cloud, and Oracle Cloud.

Summit Route

Denial of Wallet Attacks on AWS

2020.06.08 RSS feed

The AWS incidents that make the news are normally data loss incidents (ex. a public S3 bucket), but one of the common ways people find out about a compromise is through their AWS bill, because a common incident that isn't made public is a compromised AWS key that is used to spin up EC2s to mine bitcoin. That attack is used for the personal gain of the attacker, but it is possible that an attacker just wants to bring hurt to you. Historically, this would have taken the form of a DDoS attack, but in the age of the cloud, that attack can be modified to be a Denial of Wallet attack, where the goal is to cause a high bill such that you run out of money.

When you have servers in a datacenter, and an attacker just wants to bring you hurt, they can DDoS you and your site goes down. When you run in the cloud, an attacker can do things such that your site might stay up, but you'll be bankrupt. This post will describe this concept, how it can be abused, and how it can be avoided.

This post comes about from this tweet:

M-x GNU Booty
@baphometadata

I love that multiple police departments just got slammed with a hardcore AWS bill because they all deployed the same poorly written app for snitching on protesters and it got flooded with kpop videos that weren't vetted or stored correctly.

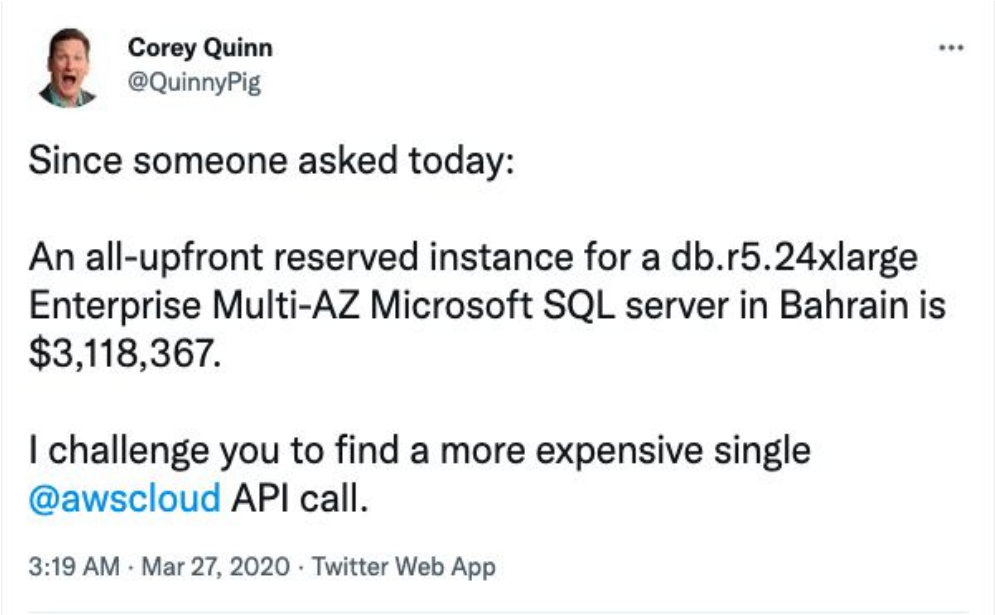
Bad devops is antifa praxis now.

8:46 AM · Jun 3, 2020 · Twitter Web App

2K Retweets 6.5K Likes

We </3 Cloud: Adventures in Bahrain?

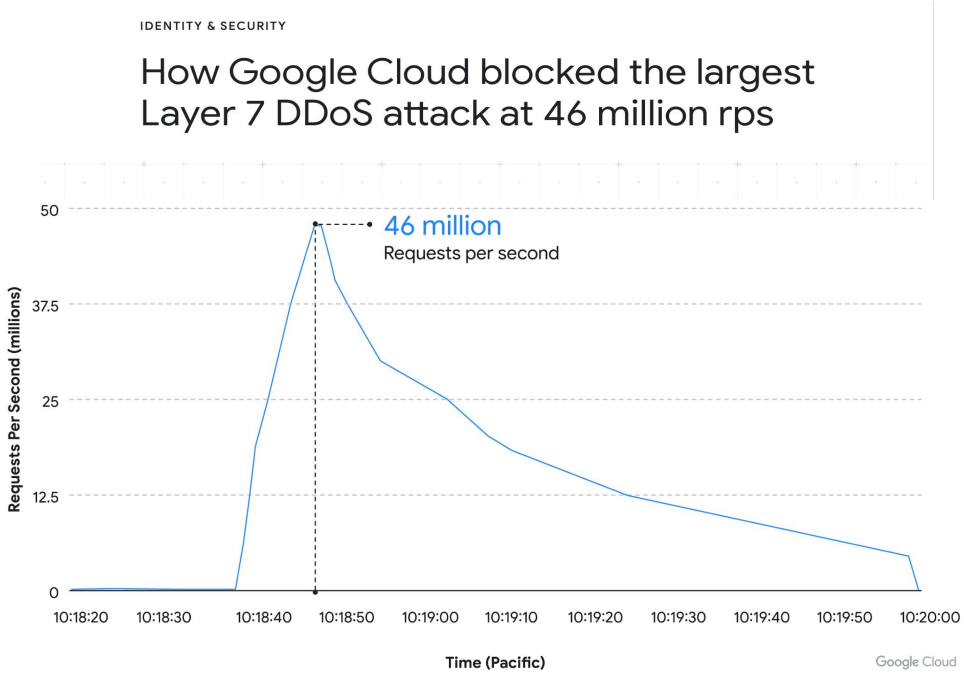
You can run a single AWS API call to launch SQL server in Bahrain (me-south-1), and it would cost an upfront payment of $3,118,367 USD.



Google Cloud DDoS Attack — August 2022
How can we simulate the attack?

GCP DDoS Attack - Can we do the same?

Google reported seeing “the largest Layer 7 DDoS attack at 46 million rps” In August 2022.



GCP DDoS Attack - Can we do the same?

<u>Total IPs involved: 5,256 IPs</u>

**** Total Attack: ****

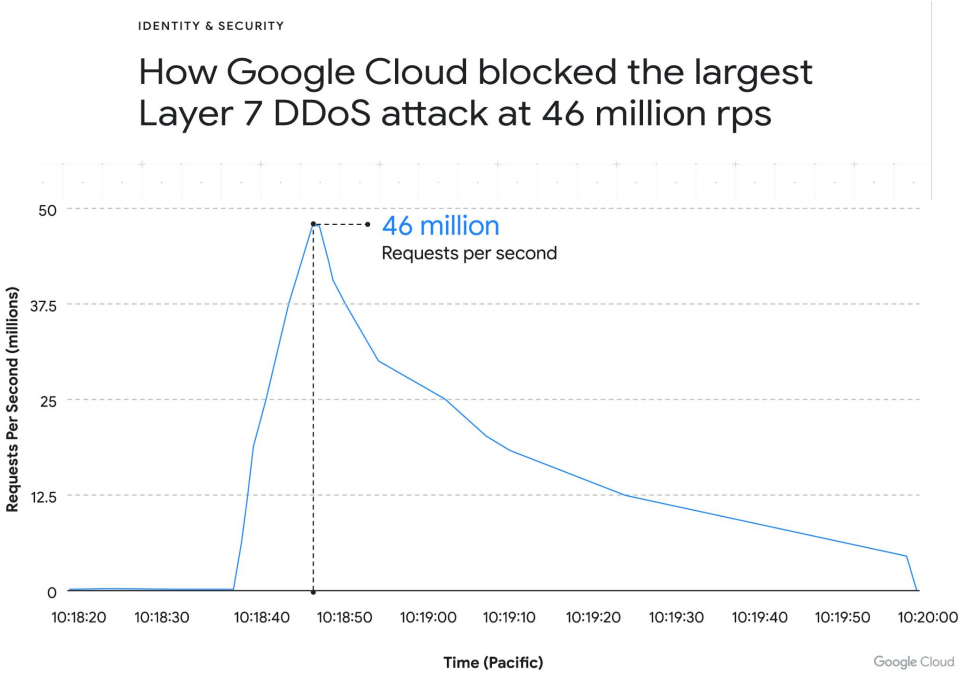
Peak: **46M RPS**

Average (from Google's own graph): **12.3M RPS**

**** Per IP: ****

Peak: 8,751 RPS

Average: 2,340 RPS

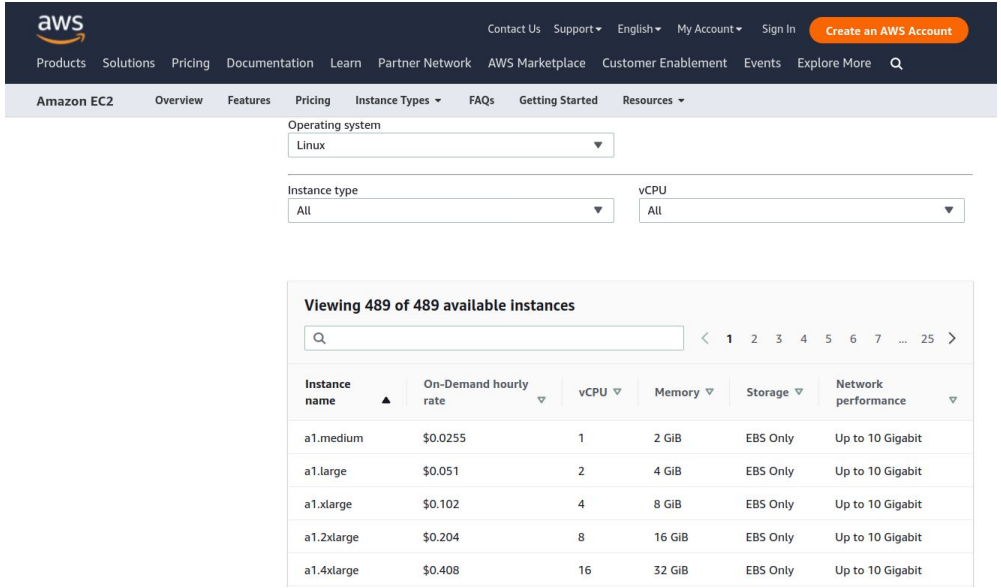


GCP DDoS Attack - Can we do the same?

<u>A1.large EC2 (on-demand):</u>
<u>$0.051 per hour</u>

$0.051 * 2 hours * 5,256 EC2s
= $536.112 USD

- This does not include Data Transfer and other similar fees.



Instance name	On-Demand hourly rate	vCPU	Memory	Storage	Network performance
a1.medium	$0.0255	1	2 GiB	EBS Only	Up to 10 Gigabit
a1.large	$0.051	2	4 GiB	EBS Only	Up to 10 Gigabit
a1.xlarge	$0.102	4	8 GiB	EBS Only	Up to 10 Gigabit
a1.2xlarge	$0.204	8	16 GiB	EBS Only	Up to 10 Gigabit
a1.4xlarge	$0.408	16	32 GiB	EBS Only	Up to 10 Gigabit

This is just me speaking out loud, there are tens of DoS topics that doesn't fit a single talk.

I will leave these for your own research:

- Amplification Attacks
- Amplification Protocols
- History of Attacks
- Volumetric Attacks
- Bad DDoS Incidents I haven't witnessed
- Extortion DDoS Incidents
- More in-depth ways to test out for unique DoS vectors
- HTTP Pipelining
- HTTP Response Poisoning DoS

Takeaways

- Availability is extremely important to organizations.
- We run pentests to identify security risks, **but we almost never run DDoS Simulations.**
- Most organizations **do not know whether their DDoS Defense solutions actually works.** (Trust, but verify?).
- We should think about all previous incidents in different industries, study each TTP used to launch DoS attacks against organizations, and test DDoS defenses.

Questions?

Mazin Ahmed
mazin@mazinahmed.net
Twitter: @mazen160

Thank you!

Mazin Ahmed
mazin@mazinahmed.net
Twitter: @mazen160