

**With Infinite Scale
Comes Infinite Bill**
(and Bankruptcy)

**Scaling Can Become A
Security Risk**

whoami

Chandrapal Badshah

Secure Cloud Environments of FinTechs

Security Researcher & Trainer

badshah@badshah.io



DISCLAIMER

This presentation explores potential cloud weaknesses for educational purposes only; any exploitation of these weaknesses is *STRONGLY DISCOURAGED*, and the presenter assumes no responsibility for misuse of this information.

If You Are Made To

Scale your resources ~~as per your need.~~
~~Just pay as you use.~~



You MUST

For What You Used

- ~~Every Cloud Provider~~

Denial Of Wallet

(Exhaustion of Wallet)

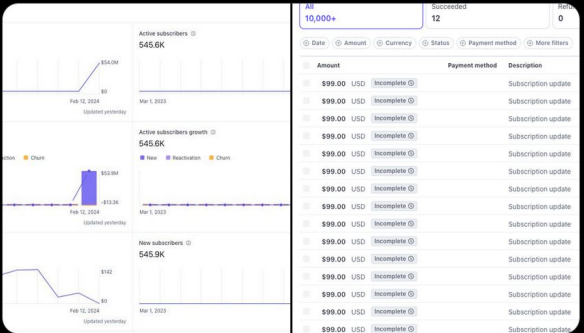


Serverless Platforms are infamous for DoW

Michael Aubry — BasedLabs.ai
@michaelaubry

What is happening?! Someone spammed EchoFox and spiked my @vercel bill to \$23k and caused 56k+ accounts and trials

Can someone at @stripe or vercel explain, wtf



The dashboard shows a line chart for 'Active subscribers' with a value of \$45.6K. Below it, a bar chart shows 'Active subscribers growth' with a value of \$13.9K. A table lists 'New subscribers' with a value of \$45.9K. To the right, a table of subscription updates shows 12 items, all with an amount of \$99.00 USD and a status of 'Incomplete'.

4:29 AM · Feb 14, 2024 · 549.8K Views

Vercel

Netlify just sent me a \$104K bill for a simple static site **Question** self.webdev

Submitted 7 months ago * by liubanghoudai24

So I received an email from Netlify last weekend saying that I have a \$104,500.00 bill overdue. At first I thought this is a joke or some scam email but after checking my dashboard it seems like I am truly owing them 104K dollars:

That's 190TB bandwidth in 4 days

Overdue invoices Total: \$104,500.00

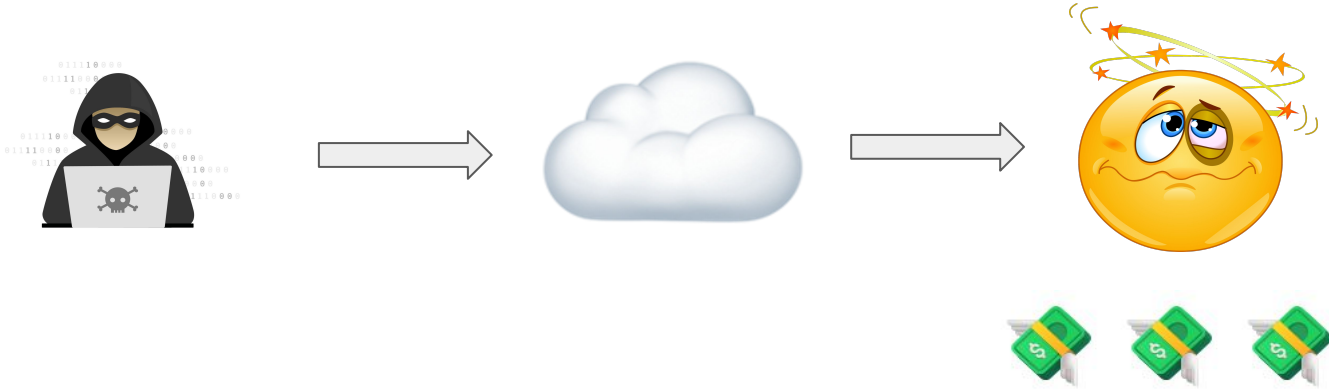
Due on Feb 24 \$104,500.00

- Feb 14: 229 Extra Bandwidth (\$12,595.00)
- Feb 15: 552 Extra Bandwidth (\$30,360.00)
- Feb 16: 607 Extra Bandwidth (\$33,385.00)
- Feb 19: 512 Extra Bandwidth (\$28,160.00)

[Contact billing support](#)

Netlify

Pattern of Denial of Wallet Attacks



Your Cloud Bill \triangleright Your Financial Capacity = Bankrupt / Close account

Cloud Native Services Are (Kind of) Serverless

- Infra resource based pricing is replaced by “creative” pricing
- Charges based per requests and data transfer

Storage pricing				
S3 Standard - General purpose storage for any type of data, typically used for frequently accessed data				
First 50 TB / Month				\$0.025 per GB
Next 450 TB / Month	PUT, COPY, POST, LIST	GET, SELECT, and all other	Lifecycle Transition	Data Retrieval
Over 500 TB / Month	requests (per 1,000)	requests (per 1,000)	requests into (per 1,000)	Data retrievals (per GB)
	Data Transfer OUT From Amazon S3 To Internet			
	AWS customers receive 100GB of data transfer out to the internet free each month, aggregated across all AWS Services and Regions (except China and GovCloud). The 100 GB free tier for data transfer out to the internet is global and does not apply separately or individually to AWS Regions.			
	S3 Standard			
				First 10 TB / Month \$0.1093 per GB
				Next 40 TB / Month \$0.085 per GB
				Next 100 TB / Month \$0.082 per GB
				Greater than 150 TB / Month \$0.08 per GB

Denial of Wallet Demo
Amazon S3

Attacking S3 Bucket

With Object Listing Enabled and Zero Objects

1 million requests to S3 bucket with 100 concurrent threads

20 mins, ~800 MB, \$5 Charge to victim

VPS Providers - \$5/mo = 1 TB bandwidth

Send more than **1 billion requests** to cause bill **\$5000+ to victim**

What if you don't use those Cloud Native services?

What if your staging account credentials were leaked? 😱

With only **full RDS permissions** `rds:*` 😬

And you don't use RDS service 🙄

- ✅ Don't worry about data exfiltration
- ✅ Don't worry about privilege escalation
- ✅ Don't worry about deleting critical databases or ransomware
- 😬 But.. What if the attacker creates a database?

Costly Services, Subscriptions and Provisioning

Instance name ▾	RI upfront fee ▾	RI monthly fees* ▾	RI effective hourly rate** ▾	Savings over On-Demand ▾	On-Demand rate ▾
db.x2iedn.32xlarge	\$4,589,462	\$0.00	<u>\$174.637</u>	12%	\$198.4512
db.x2iedn.24xlarge	\$3,442,096	\$0.00	<u>\$130.978</u>	12%	\$148.8384
db.x1.32xlarge	\$3,185,897	\$0.00	<u>\$121.229</u>	12%	\$137.4480
db.r6i.32xlarge	\$2,693,952	\$0.00	<u>\$102.510</u>	12%	\$116.2240
db.x2iedn.16xlarge	\$2,294,731	\$0.00	<u>\$87.319</u>	12%	\$99.2256
db.r5d.24xlarge	\$2,190,270	\$0.00	<u>\$83.344</u>	12%	\$94.4940

Reserved Instances may not be transferred, sold, or cancelled and the one-time fee is non-refundable.

Are You Vulnerable?

Have you **exposed** any **auto-scalable cloud service / resource** to the internet?

Is the **price dependent** on **number of requests or data transfer**?

What stops **anyone with privileges** from **launching/subscribing to costly cloud services**?

What's the Remediation?

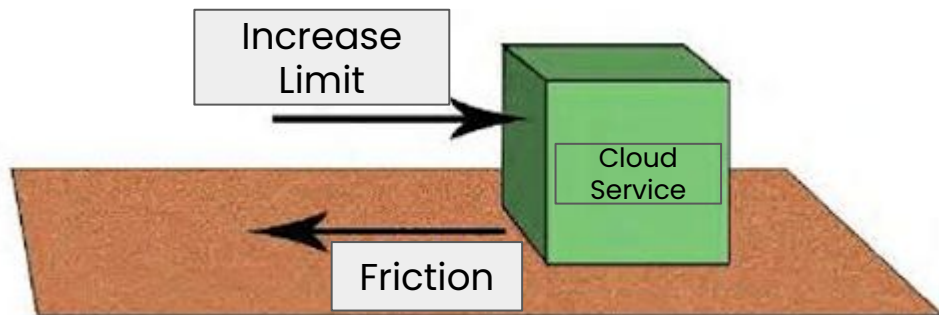
This bug class needs effort from both sides of "Shared Responsibility" model



Suggestions to Cloud Service Providers

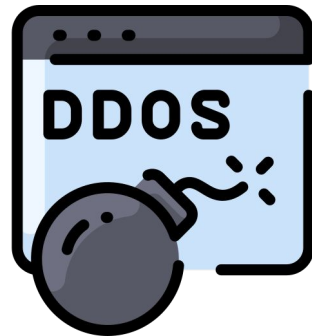
Set Smaller Quotas & Increase Limit Gradually

- Set smaller default quotas
- Increase the quotas gradually
- Add some friction before expensive cloud actions
 - Email verification / Mandatory MFA *before* reserving 100,000 USD instance



DDoS Protection shouldn't be costly

- Cost of launching DDoS \ll Cost of defending against DDoS
- DDoS protection should be a feature
- Make it easier to report if your cloud resources/IPs are involved in DDoS attack



Other great features for cloud customers

- Option to explicitly enable / disable services
- Faster billing anomaly detection at low cost
- Automated emails when systems hit limits of scaling



Suggestions to Cloud Customers

PREVENTIVE

Check for the red flags

- Check all services you use/enabled in your cloud account with the DoW pattern
 - Auto Scaling
 - Priced per requests/data
 - Expensive actions (services, subscriptions, etc)
- Block access to services and actions that are not needed
 - AWS Org SCPs / GCP Org Policies / Azure Policies
 - Don't grant access to it on IAM level

PREVENTIVE

Sample AWS SCP to Block Expensive Actions

Safeguard SCP

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "route53domains:RegisterDomain",
        "route53domains:RenewDomain",
        "route53domains:TransferDomain",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseHostReservation",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:PurchaseScheduledInstances",
        "rds:PurchaseReservedDBInstancesOffering",
        "dynamodb:PurchaseReservedCapacityOfferings",
        "s3:PutObjectRetention",
        "s3:PutObjectLegalHold",
        "s3:BypassGovernanceRetention",
```

PREVENTIVE

Limit Exposure of Cloud Native Resources to Internet Users

Ex: S3 Buckets, Cloud Access Keys, API keys, etc

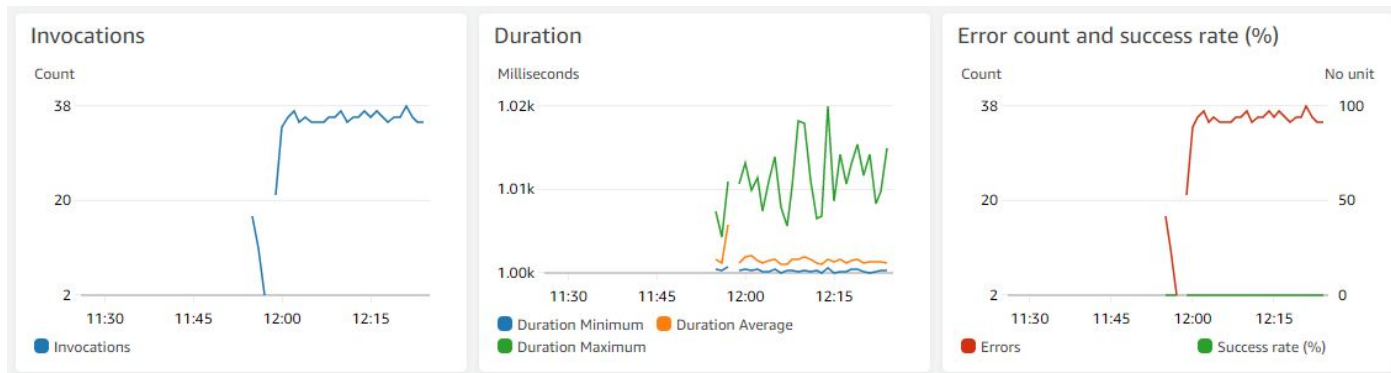


Uses: Cut down access,
redirect, caching,
ratelimit, etc

DETECTIVE & REACTIVE

Setup Monitoring & Billing Alerts

- Monitor your applications - API invocations, errors, throttles, etc
- Add incremental Billing Alerts for your cloud platforms
- Utilize features for “Anomaly Detection”
- Faster Detection == Lesser Damage



Security Strategy To Defend Against DoW

DETECTIVE &
REACTIVE

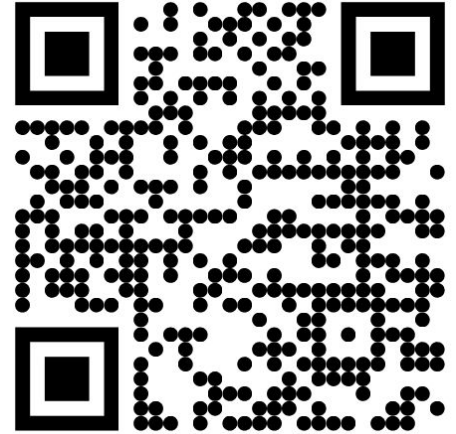
- Enable Monitoring and incremental Billing Alerts
- **Runbook:** If there's a DoW attack, make the resource inaccessible

PREVENTIVE

- Check all services that might be vulnerable to DoW
- Disable/Restrict unwanted services
- Limit exposure of auto-scalable cloud native resources to internet

Thank You Any Questions?

Reach out at
badshah@badshah.io



LinkedIn