Cloud Squatting Attack

Abdullah Al-Sultani

Agenda

1. What is the cloud and why?
2. What is the problem?
3. What did we do about it?
4. Question?

Whoami

- 🙋‍♂️ Abdullah
- 💼 Security Engineer @
- 📍 London
- ....

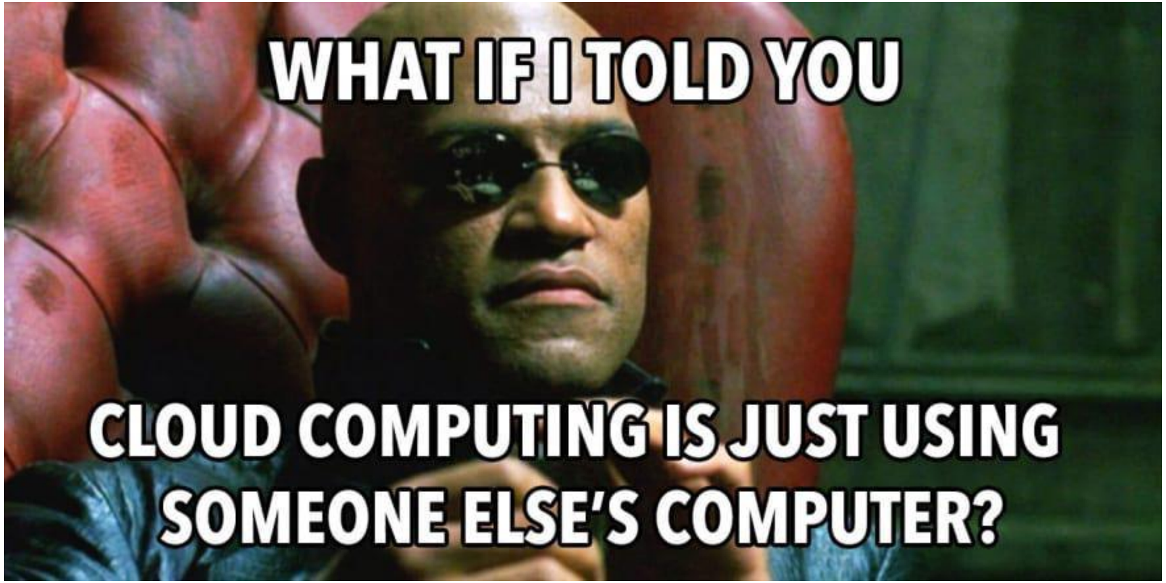
The cloud? What's that?

The cloud ☁

Instead of owning and managing physical hardware and software, users can rent or subscribe to resources and services from cloud providers. Cloud computing has become increasingly popular because it offers several advantages.

The cloud ☁

In simple words, someone's else computer.

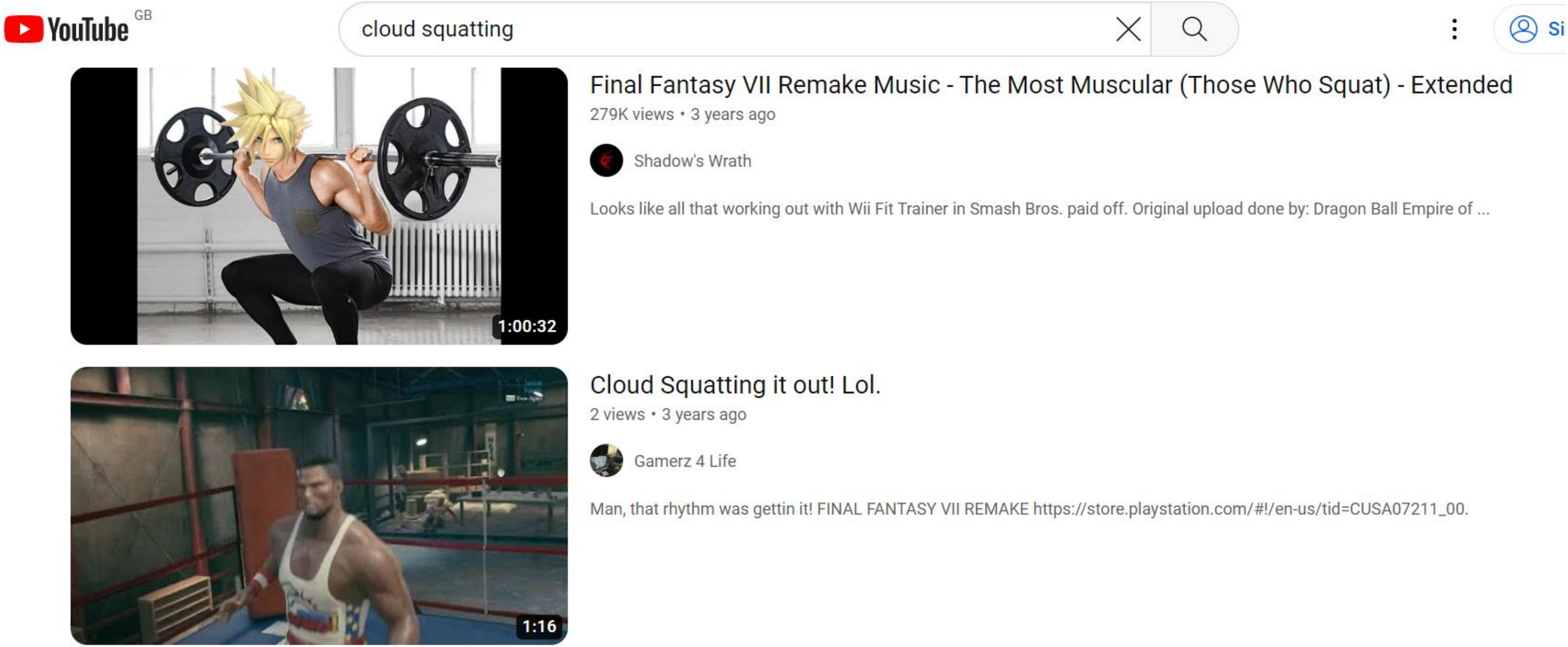


Why?

- On-Demand Resources
- Scalability
- Service Models: IaaS, PaaS and SaaS
- Deployment Models: Public, Private, ...etc
- Cost-Efficiency
- Accessibility
- Security and Compliance? What is this talk about then?

What is the problem?

Cloud squatting



cloud squatting

Final Fantasy VII Remake Music - The Most Muscular (Those Who Squat) - Extended

279K views • 3 years ago

Shadow's Wrath

Looks like all that working out with Wii Fit Trainer in Smash Bros. paid off. Original upload done by: Dragon Ball Empire of ...

Cloud Squatting it out! Lol.

2 views • 3 years ago

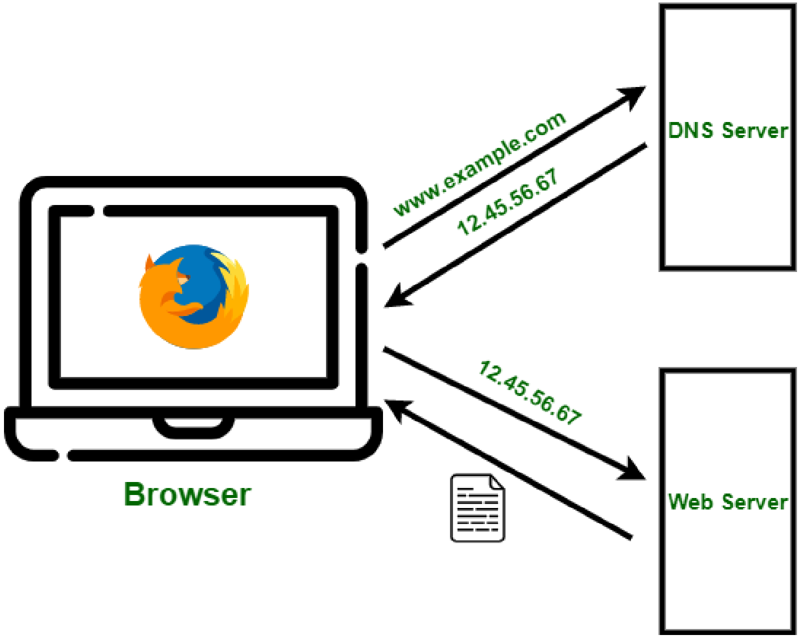
Gamerz 4 Life

Man, that rhythm was gettin it! FINAL FANTASY VII REMAKE https://store.playstation.com/#!/en-us/tid=CUSA07211_00.

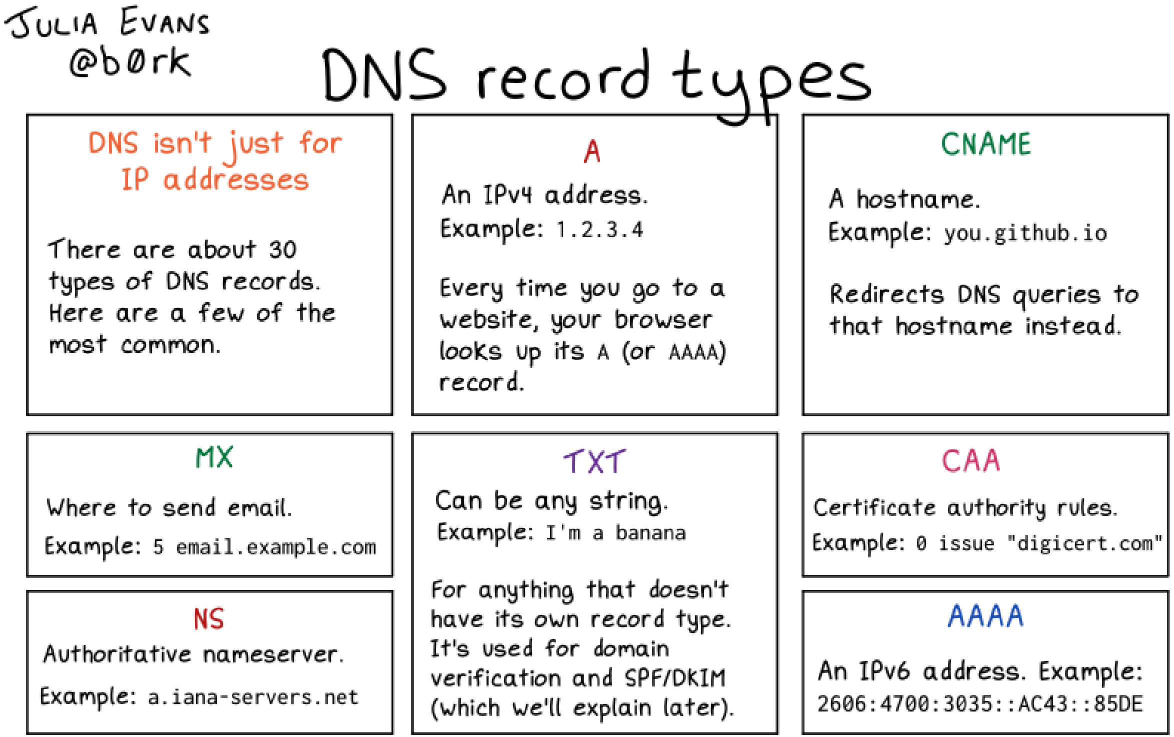
Cloud squatting

When organizations rent cloud servers, these servers get assigned an IP address. Customers connect to this IP address to send data. When the organization no longer uses the server, the IP address is reassigned to another user (maybe an evil one).

DNS


DNS Server
www.example.com
12.45.56.67
12.45.56.67
Web Server
Browser

DNS



Julia Evans
@b0rk

DNS record types

DNS isn't just for IP addresses

There are about 30 types of DNS records. Here are a few of the most common.

A

An IPv4 address.
Example: `1.2.3.4`

Every time you go to a website, your browser looks up its A (or AAAA) record.

CNAME

A hostname.
Example: `you.github.io`

Redirects DNS queries to that hostname instead.

MX

Where to send email.

Example: `5 email.example.com`

TXT

Can be any string.
Example: `I'm a banana`

For anything that doesn't have its own record type. It's used for domain verification and SPF/DKIM (which we'll explain later).

CAA

Certificate authority rules.
Example: `0 issue "digicert.com"`

NS

Authoritative nameserver.

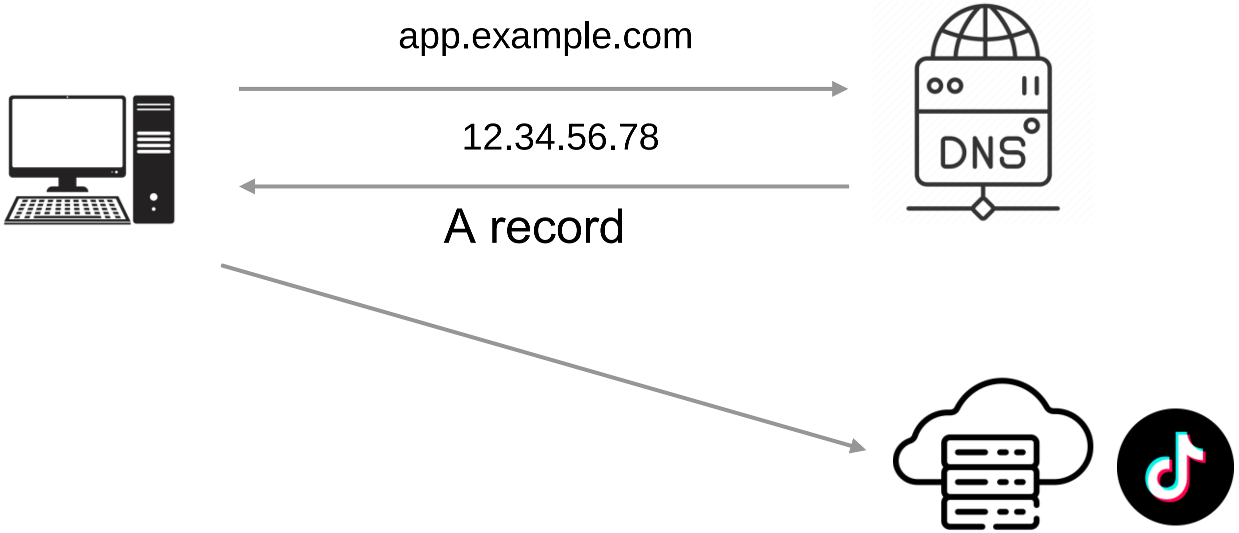
Example: `a.iana-servers.net`

AAAA

An IPv6 address. Example:
`2606:4700:3035::AC43::85DE`

Examples

Subdomain takeover



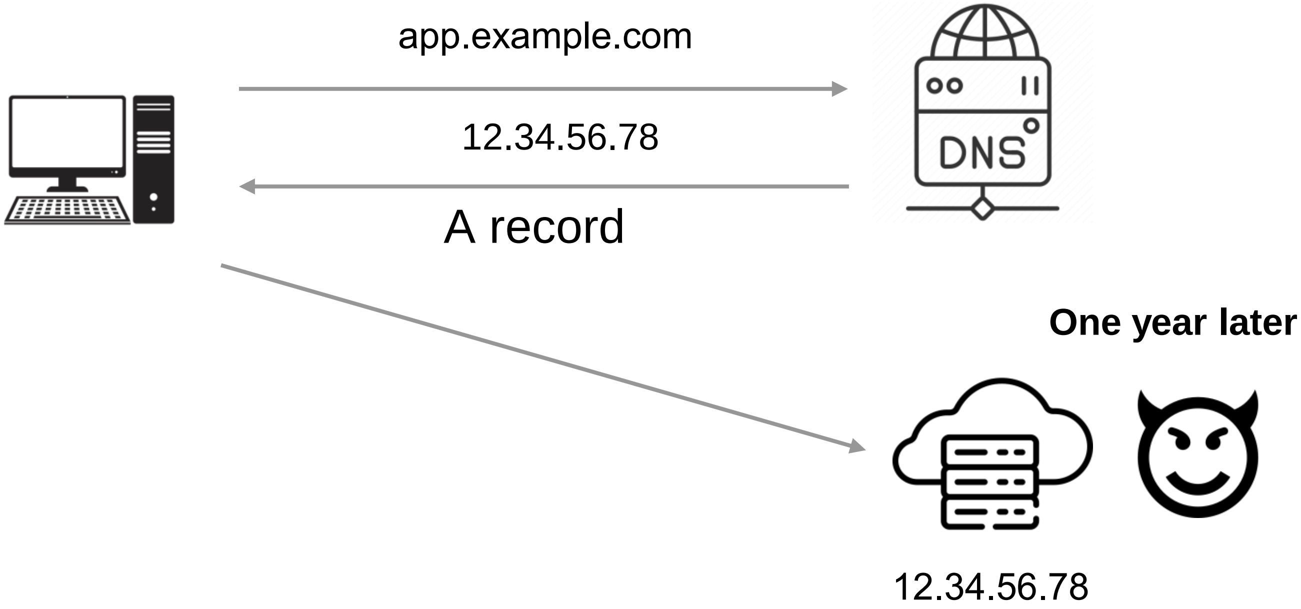
app.example.com

12.34.56.78

A record

12.34.56.78

Subdomain takeover



app.example.com

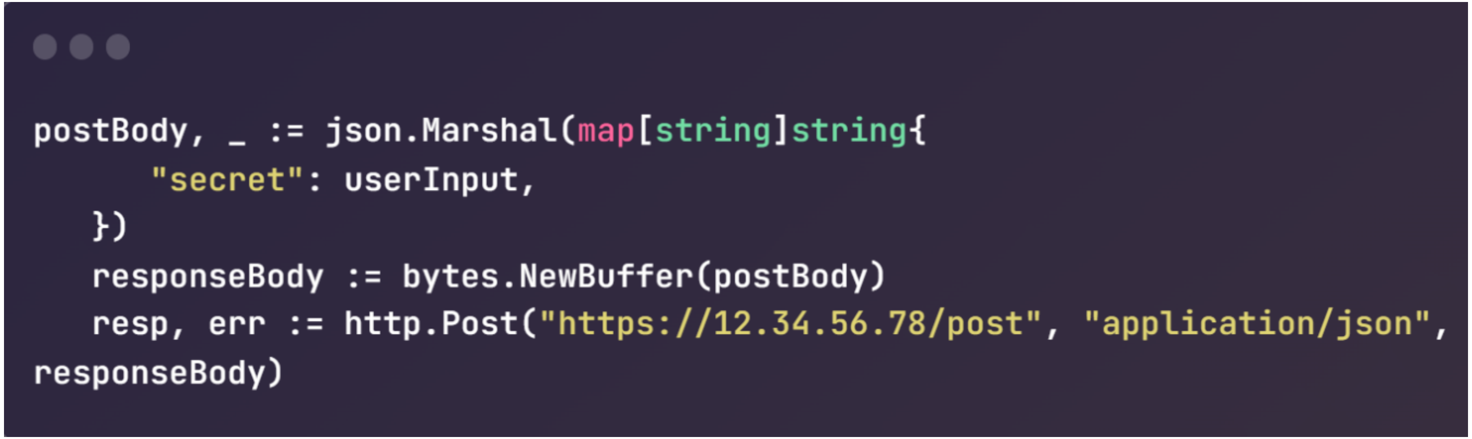
12.34.56.78

A record

One year later

12.34.56.78

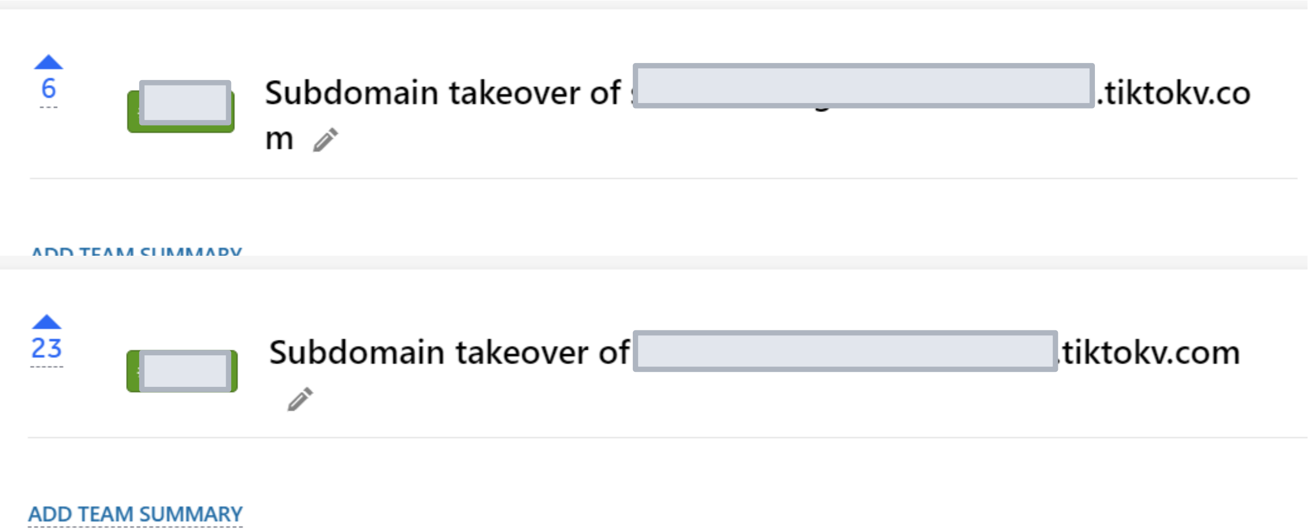
Data leak



```
postBody, _ := json.Marshal(map[string]string{
      "secret": userInput,
   })
   responseBody := bytes.NewBuffer(postBody)
   resp, err := http.Post("https://12.34.56.78/post", "application/json",
responseBody)
```

Motivaiton

Bug Bounty Reports



6 [redacted] Subdomain takeover of [redacted].tiktokv.com

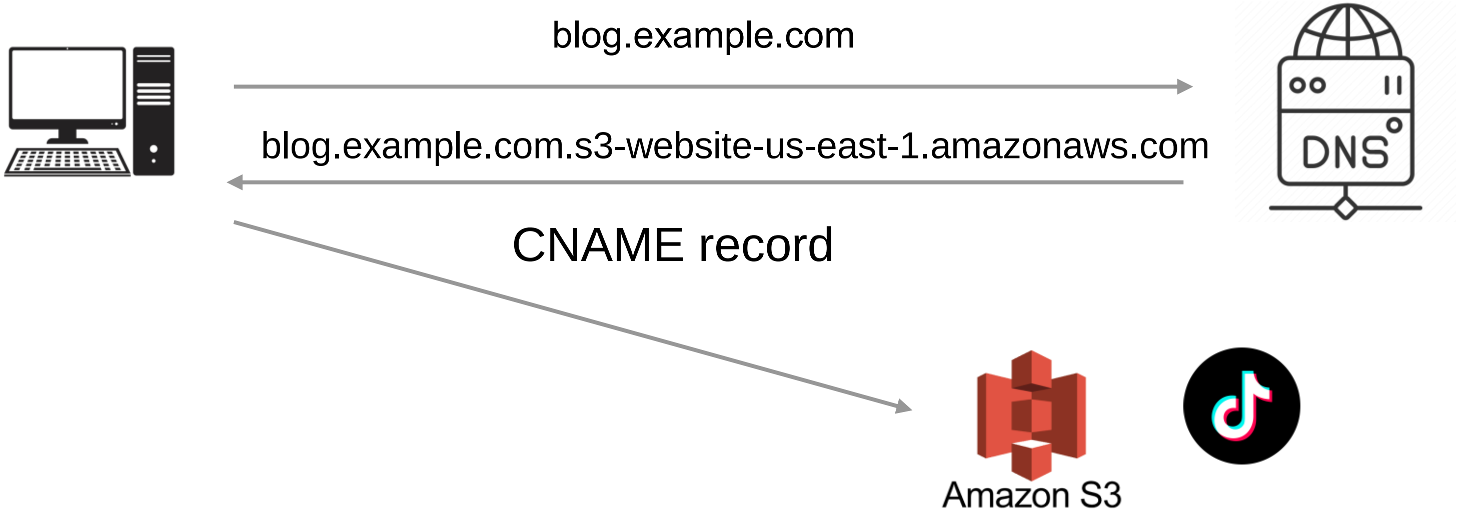
ADD TEAM SUMMARY

23 [redacted] Subdomain takeover of [redacted].tiktokv.com

ADD TEAM SUMMARY

Extension

Subdomain takeover

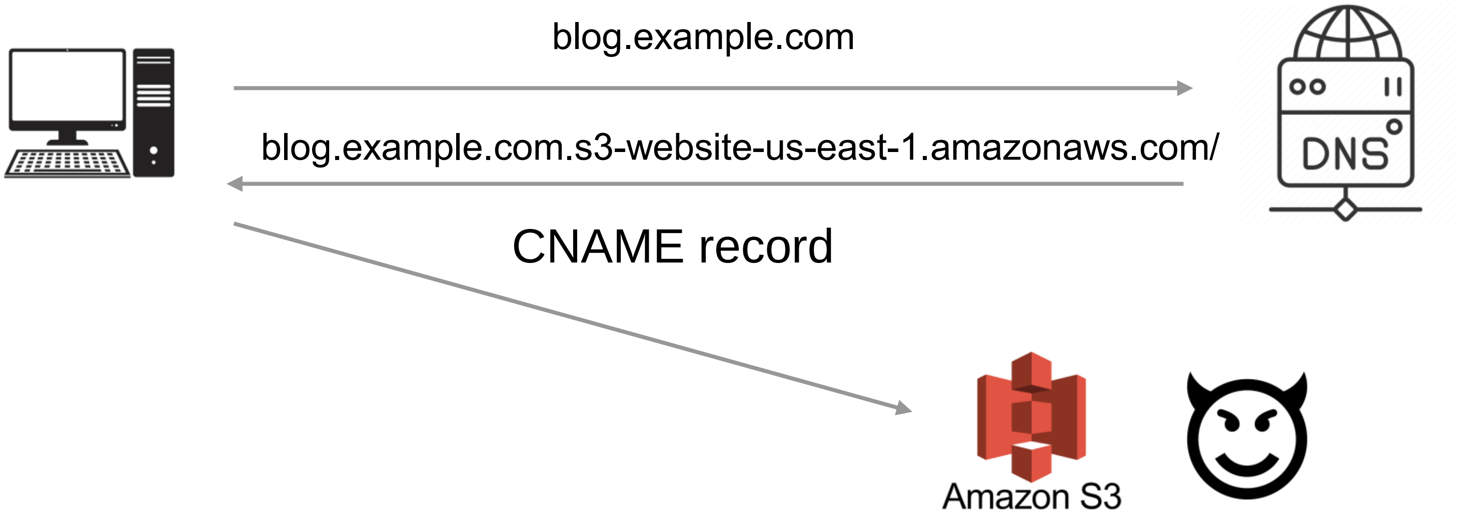


blog.example.com

blog.example.com.s3-website-us-east-1.amazonaws.com

CNAME record

Subdomain takeover



blog.example.com

blog.example.com.s3-website-us-east-1.amazonaws.com/

CNAME record

What did we do?

TODO

What do we need to collect?

- Our domains
- Our IP addresses that belong to cloud providers
- Cloud providers IP ranges
- 3rd party services that is vulnerable to takeover attacks

Our domains

- Too many to count!
- The savior: our DNS records

TODO

What do we need to collect?

- Our domains ✓
- Our IP addresses that belong to cloud providers
- Cloud providers IP ranges
- 3rd party services that is vulnerable to takeover attacks

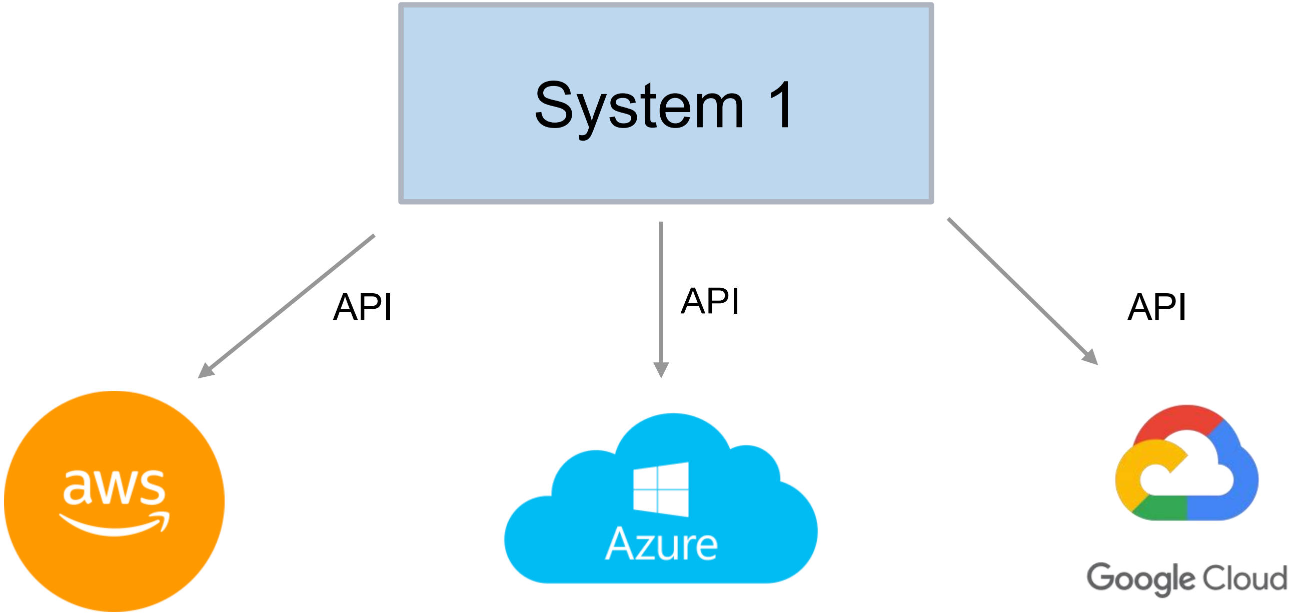
Our IPs that belong to cloud providers

- Too many to count as well!
- Two sources

System 1

System 2

Our IPs that belong to cloud providers



System 1

API

API

API

Our IPs that belong to cloud providers

System 2

Problems!

Our IPs that belong to cloud providers

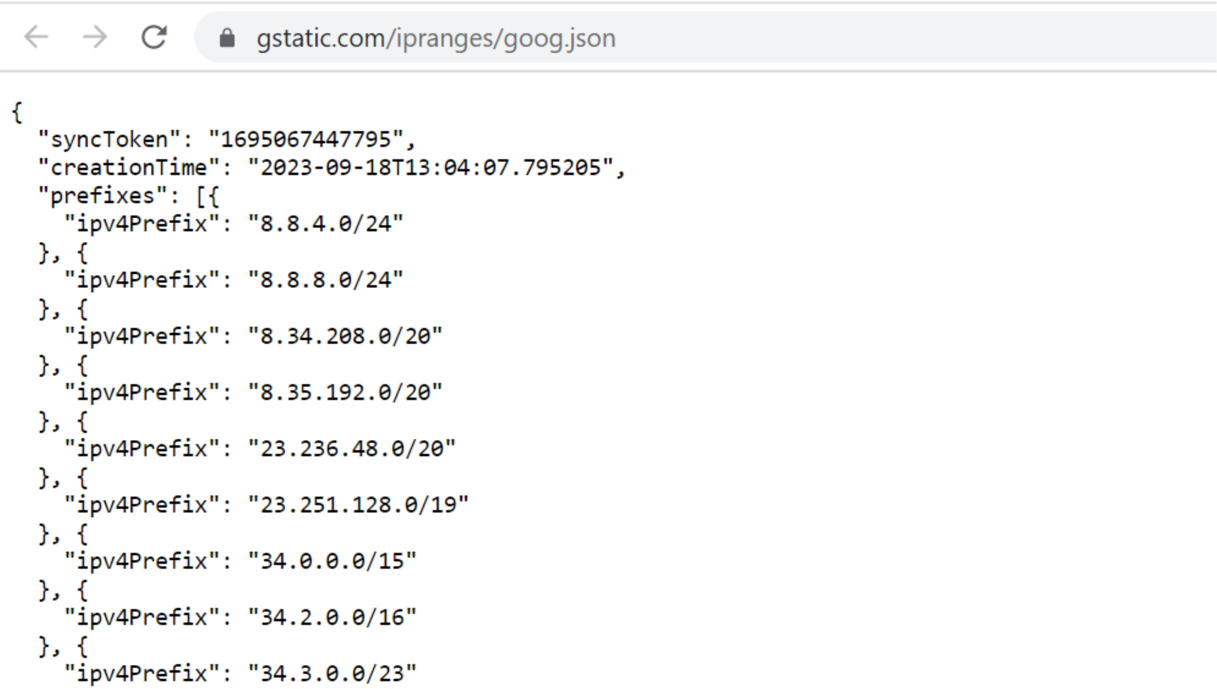
- Data redundancy: data deduplication
- Data discrepancy

TODO

What do we need to collect?

- Our domains ✓
- Our IP addresses that belong to cloud providers ✓
- Cloud providers IP ranges
- 3rd party services that is vulnerable to takeover attacks

Cloud providers IP ranges



gstatic.com/ipranges/goog.json

```
{
  "syncToken": "1695067447795",
  "creationTime": "2023-09-18T13:04:07.795205",
  "prefixes": [{
    "ipv4Prefix": "8.8.4.0/24"
  }, {
    "ipv4Prefix": "8.8.8.0/24"
  }, {
    "ipv4Prefix": "8.34.208.0/20"
  }, {
    "ipv4Prefix": "8.35.192.0/20"
  }, {
    "ipv4Prefix": "23.236.48.0/20"
  }, {
    "ipv4Prefix": "23.251.128.0/19"
  }, {
    "ipv4Prefix": "34.0.0.0/15"
  }, {
    "ipv4Prefix": "34.2.0.0/16"
  }, {
    "ipv4Prefix": "34.3.0.0/23"
```

Problems!

Cloud providers IP ranges

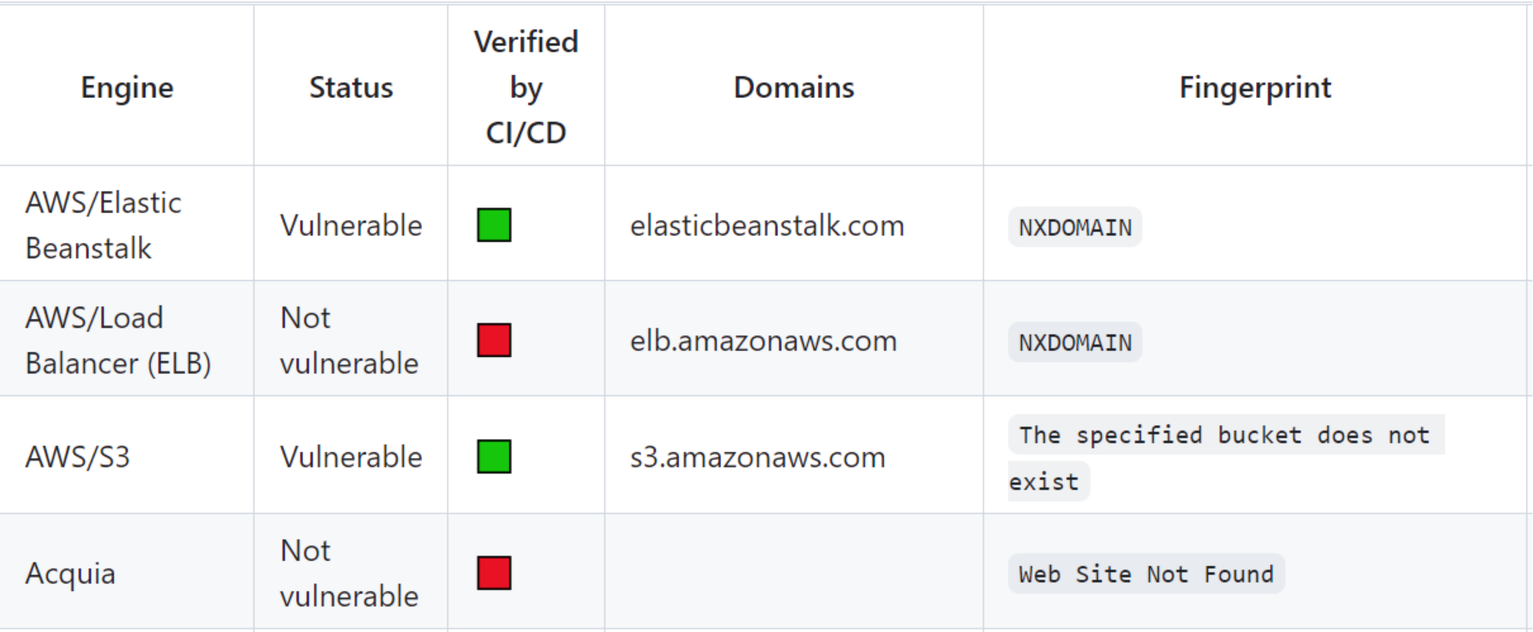
- No formal format!
- Not all providers have JSON list

TODO

What do we need to collect?

- Our domains ✓
- Our IP addresses that belong to cloud providers ✓
- Cloud providers IP ranges ✓
- 3rd party services that is vulnerable to takeover attacks

3rd party services



Engine	Status	Verified by CI/CD	Domains	Fingerprint
AWS/Elastic Beanstalk	Vulnerable	🟩	elasticbeanstalk.com	`NXDOMAIN`
AWS/Load Balancer (ELB)	Not vulnerable	🟥	elb.amazonaws.com	`NXDOMAIN`
AWS/S3	Vulnerable	🟩	s3.amazonaws.com	`The specified bucket does not exist`
Acquia	Not vulnerable	🟥		`Web Site Not Found`

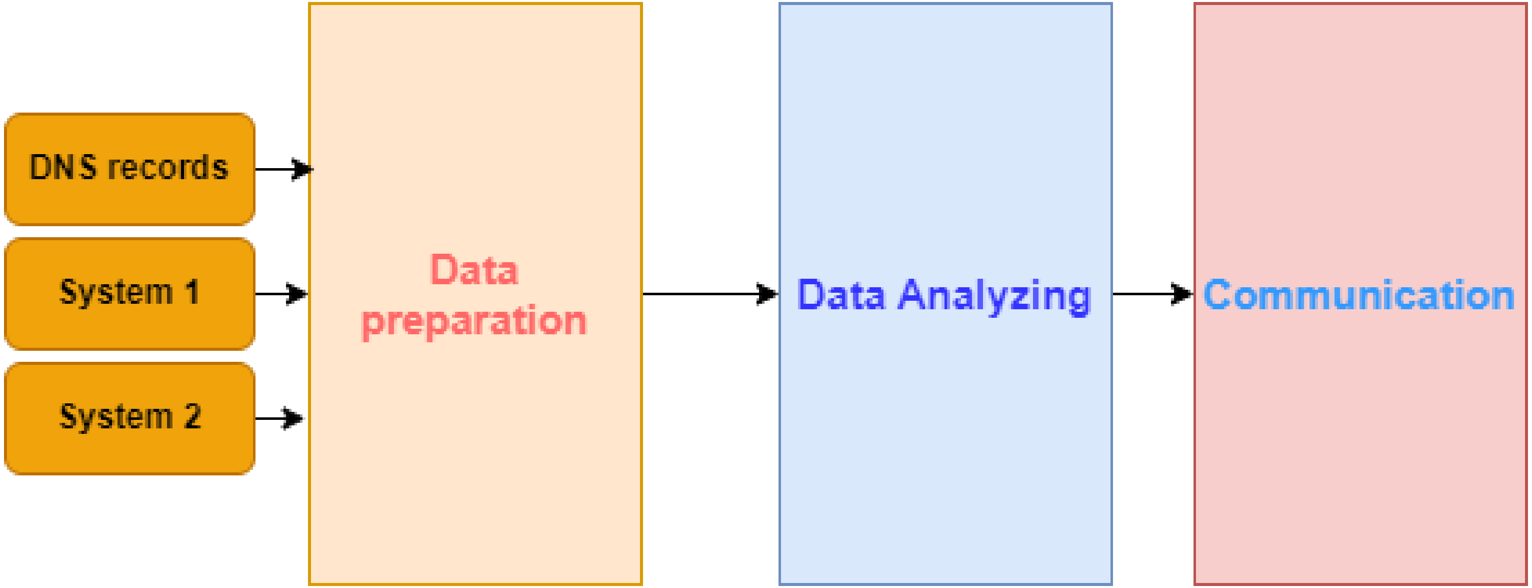
- https://github.com/EdOverflow/can-i-take-over-xyz

TODO

What do we need to collect?

- Our domains ✓
- Our IP addresses that belong to cloud providers ✓
- Cloud providers IP ranges ✓
- 3rd party services that is vulnerable to takeover attacks ✓

The workflow



Data prepration

- Pull data
- Remove deuplication

Data analyzing

- Iterate through domains
- If the domain has a vulnerable CNAME send an HTTP or a DNS request to find the fingerprint
- If the domain has an IP that belongs to cloud providers check if it is in our records and it is not expired

Data analyzing

- Iterate through IPs
- If IP is expired check if we are using it in any code or configuration file

Communication

- Send an alert to a channel (Lark, Slack, email, ...etc)

You?

DIY

- Your domain mgmt, scraping and brute-force
- Check for CNAME takeover with tools
- Check if an IP address is not alive
- Automate everything!

References

- CloudSquatting:The Risk of IP Reuse on Public Clouds
- Cloudsquatting berkeley
- Subdomain Takeover: Basics
- ....

Questions?

THANKS.

ByteDance