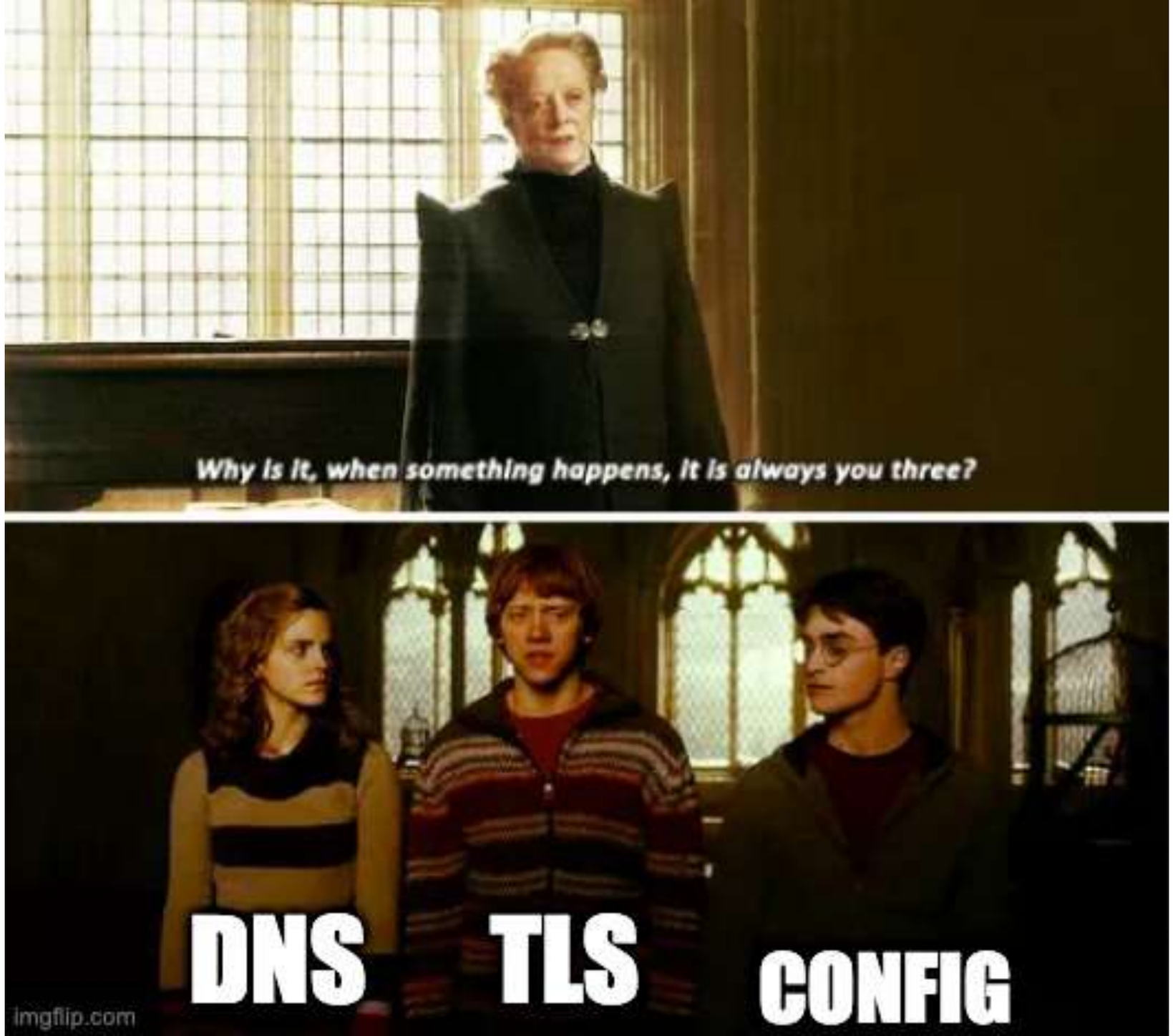
Why Is It Always DNS, TLS, and Bad Configs?

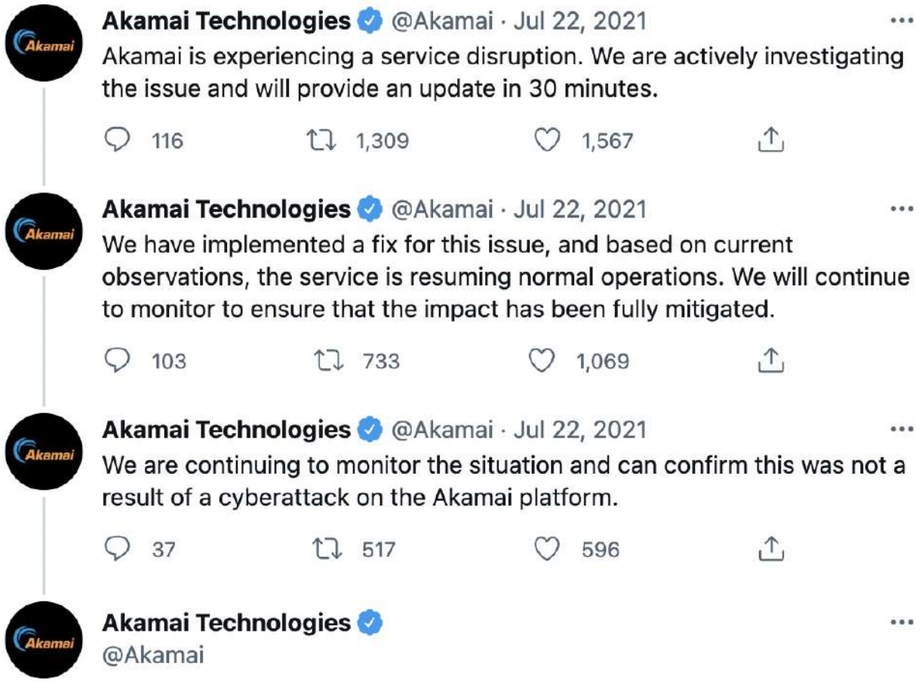
Philipp Krenn @xeraa



elastic

@xeraa

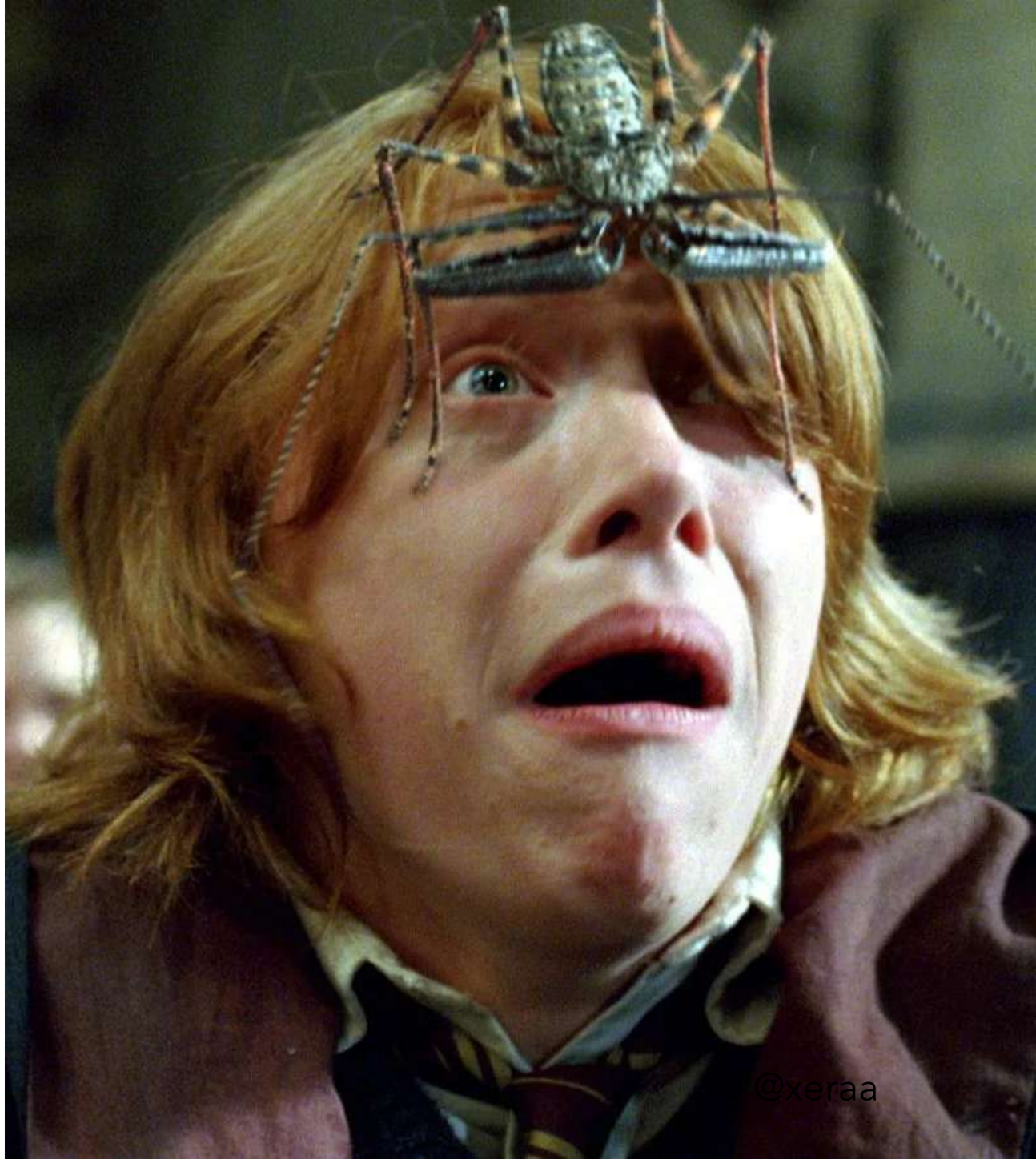
DNS



https://twitter.com/Akamai/status/1418271515192270850

Me: Moving DNS server and watching stuff disappear

TLS



@xeraa

What Exactly Went Wrong With Microsoft Azure?

Officials from Microsoft have confirmed that on March 15th an “an error occurred in the rotation of keys used to support Azure AD's use of OpenID, and other, Identity standard protocols for cryptographic signing operations.”

As part of Microsoft’s standard security practices, an automated system eliminates redundant keys. According to Microsoft, for the last few weeks “a particular key was marked as 'retain' for longer than normal to support a complex cross-cloud migration. This exposed a bug where the automation incorrectly ignored that 'retain' state, leading it to remove that particular key."

Once that key was removed, any app using Azure AD authentication immediately started rejected tokens that were signed with the removed key. The result? All Microsoft users that attempted to login to affected apps and third-party services were rejected.

While Microsoft did swiftly take action to mitigate the impact, the outage couldn’t be immediately reversed due to “different server implementations that handle caching differently”. It wasn’t until the affected apps had picked up the updated key metadata and refreshed their caches that users could regain access to their accounts.

On the outage, Microsoft released a statement expressing that they “understand how incredibly impactful and unacceptable this is and apologize deeply. "We are continuously taking steps to improve the Microsoft Azure Platform and our processes to help ensure such incidents do not occur in the future."

https://www.venafi.com/blog/what-do-we-know-about-microsoft-azure-outage

Microsoft Azure service restored after being downed by expired SSL certificate

By John Ribeiro
PCWorld | FEB 23, 2013 9:15 AM PST

Microsoft's Azure cloud platform faced a worldwide outage in its storage services from Friday afternoon because of an expired SSL (secure sockets layer) certificate. The company reported services were restored Saturday.

The company also reported problems with its Xbox Music and Video Store services.

The service problems come on a day the company said it was recently a victim of a cyberattack similar to ones that targeted Apple and Facebook.

https://www.pcworld.com/article/456965/microsofts-azure-service-falls-to-expired-ssl-certificate.html

Bad Config

elastic

"Facebook can't be down, can it?", we thought, for a second.

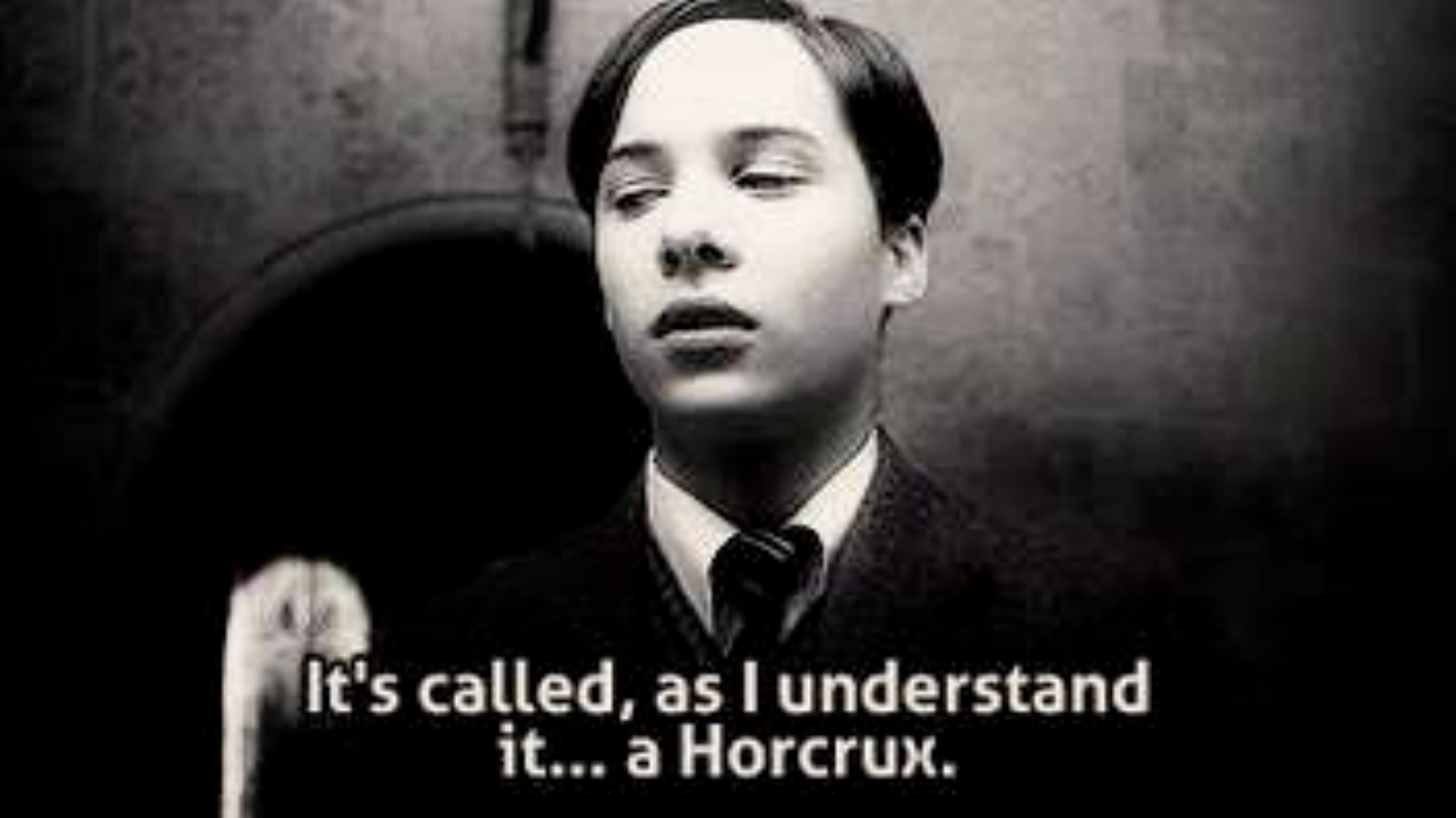
Today at 15:51 UTC, we opened an internal incident entitled "Facebook DNS lookup returning SERVFAIL" because we were worried that something was wrong with our DNS resolver 1.1.1.1. But as we were about to post on our public status page we realized something else more serious was going on.

Social media quickly burst into flames, reporting what our engineers rapidly confirmed too. Facebook and its affiliated services WhatsApp and Instagram were, in fact, all down. Their DNS names stopped resolving, and their infrastructure IPs were unreachable. It was as if someone had "pulled the cables" from their data centers all at once and disconnected them from the Internet.

This wasn't a DNS issue itself, but failing DNS was the first symptom we'd seen of a larger Facebook outage.

How's that even possible?

https://blog.cloudflare.com/october-2021-facebook-outage/


It's called, as I understand
it... a Horcrux.


Health Checks

Structure

Outside the network

On the network

On the host

Outside the Network

DNS

Outside firewall

Load balancer

Outside network

Service availability

On the Network

TLS

Inside network

Service availability

Compare latency to outside

On the Host

Service Availability
Local proxy vs service
Access to database
Compare latency to others

Developer 🥑

Overview
Alerts
Cases

Logs
Stream
Anomalies
Categories

Metrics
Inventory
Metrics Explorer

APM
Services
Traces
Dependencies
Service Map

Uptime
Monitors
TLS Certificates

User Experience
Dashboard

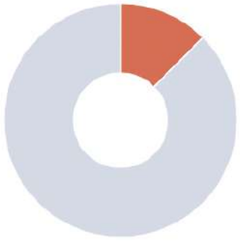
Monitors

Last 15 minutes Show dates Refresh

Search by monitor ID, name, or url (E.g. http://)

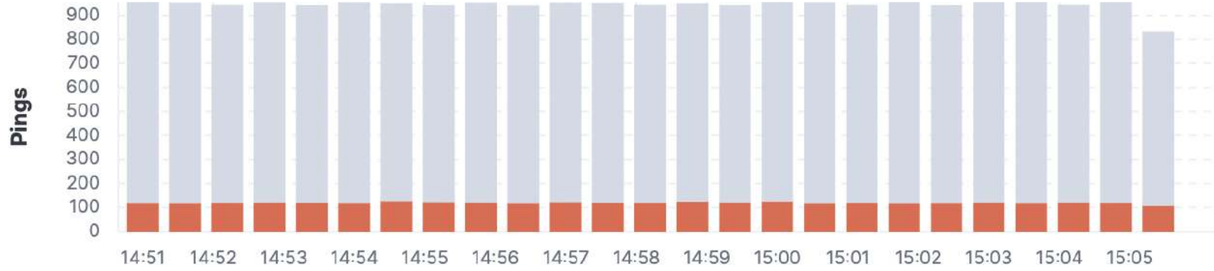
Location 0 | Port 15 | Scheme 3 | Tag 0

32 Monitors



Down 4
Up 28

Pings over time



Monitors

All Up Down

Status	Name	Url	Tags	TLS Certificate	Downtime history	Status alert
Up in 1/1 location, Checked 3:05:54 PM	opbeans-python-deco-green-6bb896c8bc-r4qvl HTTP Ping	http://10.12.8.16:3000		--	--	

```
- type: icmp
  name: Host ping
  hosts: ["xeraa.wtf"]
  schedule: '*/5 * * * * * *'
- type: tcp
  name: MySQL and PostgreSQL ping
  hosts: ["db.xeraa.wtf"]
  ports: [3306,5432]
  schedule: '@every 5s'
- type: http
  name: Server status
  schedule: '@every 5s'
  hosts: ["https://xeraa.wtf/status"]
```

Observability

Overview
Alerts
Cases

Logs
Stream
Anomalies
Categories

Metrics
Inventory
Metrics Explorer

APM
Services
Traces
Dependencies
Service Map

Uptime
Monitors
TLS Certificates

TLS Certificates (4)

Refresh

Search certificates

Status	Common name	Monitors	Issued by	Valid until	Age	Fingerprints
OK for a month	demo.elastic.co	auto-http-0X4FA94B0313EE0BC4-debdfec4c62e9997	R3	05/31/2022 8:39 AM	57 days	SHA 1 SHA 256
OK for 8 months	www.elastic.co	auto-http-0X4FA94B0313EE0BC4-f2bd00f715add916	GlobalSign Atlas R3 DV TLS CA H2 2021	12/28/2022 8:42 PM	152 days	SHA 1 SHA 256
OK for a year	github.com	auto-http-0X4FA94B0313EE0BC4-c7eca2f6ea089820	DigiCert TLS Hybrid ECC SHA384 2020 CA1	03/16/2023 12:59 AM	44 days	SHA 1 SHA 256
OK for a year	www.bbc.com	auto-http-0X4FA94B0313EE0BC4-78ebd16eaca0565d	GlobalSign RSA OV SSL CA 2018	04/05/2023 3:51 PM	55 days	SHA 1 SHA 256

Rows per page: 10

```
- type: http
  name: Server processing
  schedule: '@every 5s'
  hosts: ["https://xeraa.wtf/add"]
  check.request:
    method: POST
    headers:
      'Content-Type': 'application/x-www-form-urlencoded'
    body: "name=first&email=someemail%40someemailprovider.com"
  check.response:
    status: [200]
    body:
      - Saved
      - saved
```

Synthetic Monitoring

Conclusion

Health Checks

Cheap, fast, overview
Addition to observability

Why Is It Always DNS, TLS, and Bad Configs?

Philipp Krenn @xeraa