Login API Security

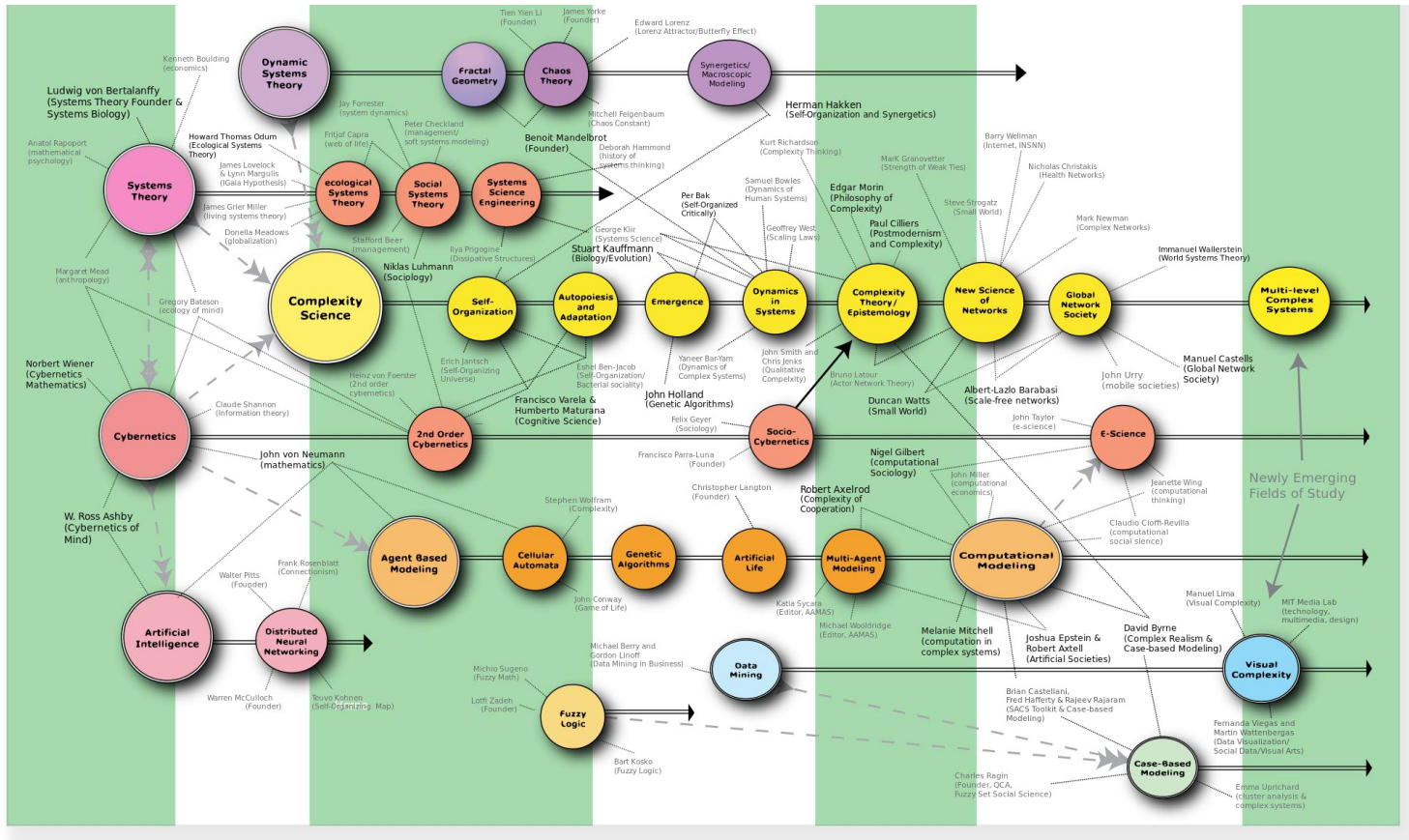
Is that you who attacks my system?

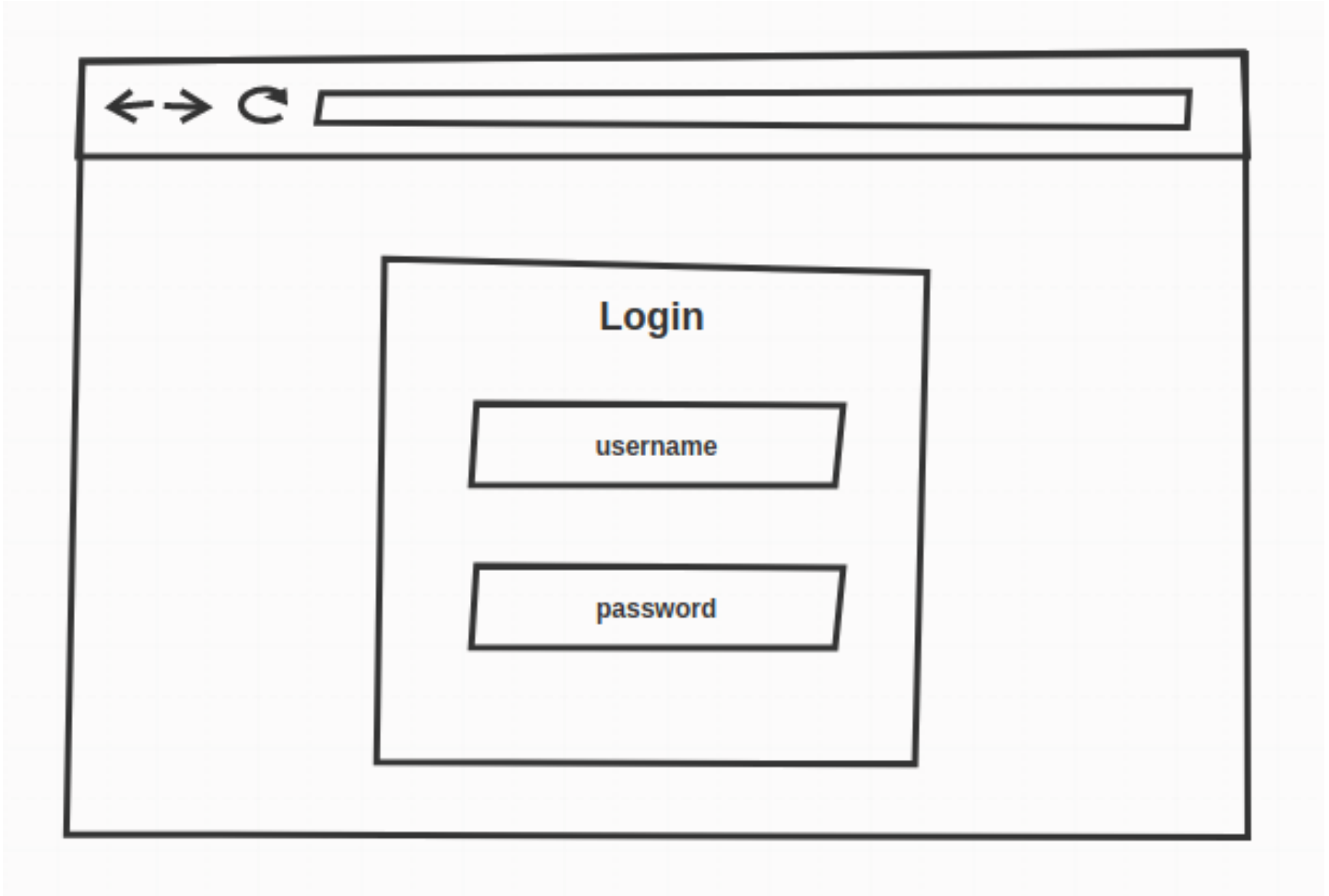
Jacek Milewski

jacek.milewski.k@gmail.com

@jacek_mil

The spotlight on…




Login
username
password

Facts

The reality we're in

Millions of Microsoft users are reusing passwords

By Anthony Spadafora December 05, 2019

44 million Microsoft users are guilty of credential reuse

https://www.techradar.com/news/millions-of-microsoft-users-are-reusing-passwords

Millions of Microsoft users are reusing passwords

By Anthony Spadafora December 05, 2019

44 million Microsoft users are guilty of credential reuse

*"scanned user accounts by using a database of more than **three billion** leaked credentials"*

"For the leaked credentials for which we found a match, we force a password reset"

https://www.techradar.com/news/millions-of-microsoft-users-are-reusing-passwords

Millions of stolen corporate logins leaked online

By Anthony Spadafora November 01, 2019

21 million credentials from Fortune 500 companies breached.

https://www.techradar.com/news/millions-of-stolen-corporate-logins-are-available-to-buy-online

Millions of stolen corporate logins leaked online

By Anthony Spadafora November 01, 2019

21 million credentials from Fortune 500 companies breached.

"Out of the 21m credentials, only 4.9m were fully unique passwords"

"top 5 passwords: password, 1qaz2wsx, career121, abc123 and passwordI"

"retail sector had the highest percentage of weak passwords at 47% followed by telecommunications at 37% and industrials at 37%"

https://www.techradar.com/news/millions-of-stolen-corporate-logins-are-available-to-buy-online

Nearly 620 million stolen accounts for sale on dark web

By Mike Moore February 12, 2019

Number of popular sites have user account information stolen and put up for sale.

https://www.techradar.com/news/nearly-620-million-stolen-accounts-for-sale-on-dark-web

Nearly 620 million stolen accounts for sale on dark web

By Mike Moore February 12, 2019

Number of popular sites have user account information stolen and put up for sale.

"For the equivalent of $20,000 in Bitcoin"

Your account costs 0,00003$

31 000 accounts for 1$

https://www.techradar.com/news/nearly-620-million-stolen-accounts-for-sale-on-dark-web

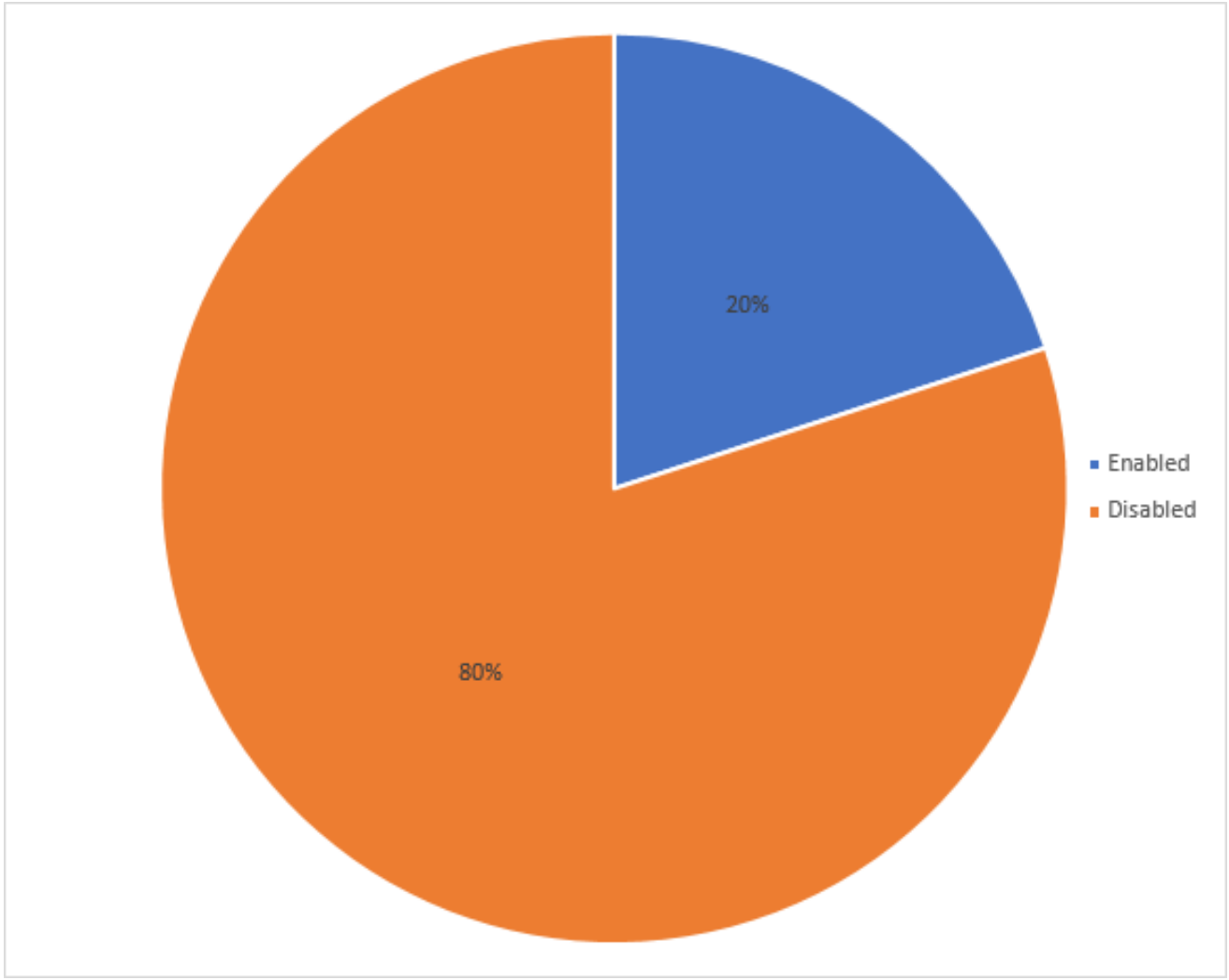
hashes.org

ID	Name (Algorithm)	#Hashes	Left	Found	Recovered	Updated
7290	Have I been Pwned V6 SHA1	17'332'964	203	17'332'761	100%	2020.06.23 04:11:44
7224	Kingdomcraze.com MD5 / BCRYPT	101'898	84'273	17'625	17.3%	2020.06.19 18:35:59
7176	Studytonight.com MD5CRYPT	72'491	56'726	15'765	21.75%	2020.06.21 14:21:47
7174	Sinlyxe.cc MD5	754	225	529	70.16%	2020.06.20 19:03:50
7173	Sneaker-groups.com MYBB	464	148	316	68.1%	2020.06.08 22:17:59
7172	Sinfulsite.com (without argon) MYBB / BCRYPT	3'127	2'821	306	9.79%	2020.06.08 22:59:10
7171	Pasteware.team MYBB	1'632	949	683	41.85%	2020.06.08 22:59:10
7170	3djobs.com VBULLETIN	307'703	277'689	30'014	9.75%	2020.06.15 04:28:35
7166	Mathway.com WORDPRESS	17'058'517	560'498	16'498'019	96.71%	2020.06.14 19:09:03
7164	360Icons VBULLETIN	101'864	41'528	60'336	59.23%	2020.06.11 23:51:46
7163	Ikov MD5(PLAINSALT)	316'538	35'592	280'946	88.76%	2020.06.07 18:22:10

```
0201f121a96a6ba14ef2b12eb78df735:Molley123
02516850c8216a72169cf2d61a87c124:Cornflakes2
027abece3851bf3b538f44636189cd32:Pa00wor0
058659d5c6e71c552ca18a81e686c724:asd156324
05a83dd93718b0c9ae202a2ff123f214:CurryKing
05b465d18b0392839a128f4312bfd4bd:yaoyuan123
06ad52ea9eeb81b947874d3130c34329:jonas0306
06c36a61e2cb2f3c6a2c512eb9aa33fa:Aleksandra1
07514f72fed57b5b3644c267dbd84bb1:bobmarley123
0794eb15be87d8b4878f8b891ec2d7d3:enesqenc1
07f96682839467806efa13903379ed3d:m123123..
0ae82173e69b80e34a7790a841a43a01:england10
0cfe375e9bbc0b0abc4cfbcfe8669284:yusuf123123
0d40776e16e72a1c4ea81f2c73aa282f:E46372
0da21eca396b1532f6cccf167234b441:Password124
0f1dd9d458f9389c0f86ec984d52bc4d:lw2009268
0f1ea11e525e76ed02ea2c691f06cf61:exile777
10e7f197742cf3c37f1e864167085909:Simsim11
1554698cdf30a005f0b69228c54f3155:Yasin123
176a0e25b43883aaa09feddd4a01b34e:Aerocool79
18b876636628f34252b578a7c705b7ee:wnr316
1a6fa8ca06f3365fa1332bfb756e1765:Dogman123
1bfa4c4e5740f616ea27e68b37ffede2:621dd
1c4fbe7a5fcd8cdeee6fccd2ea48da88:Mikolaj112
```

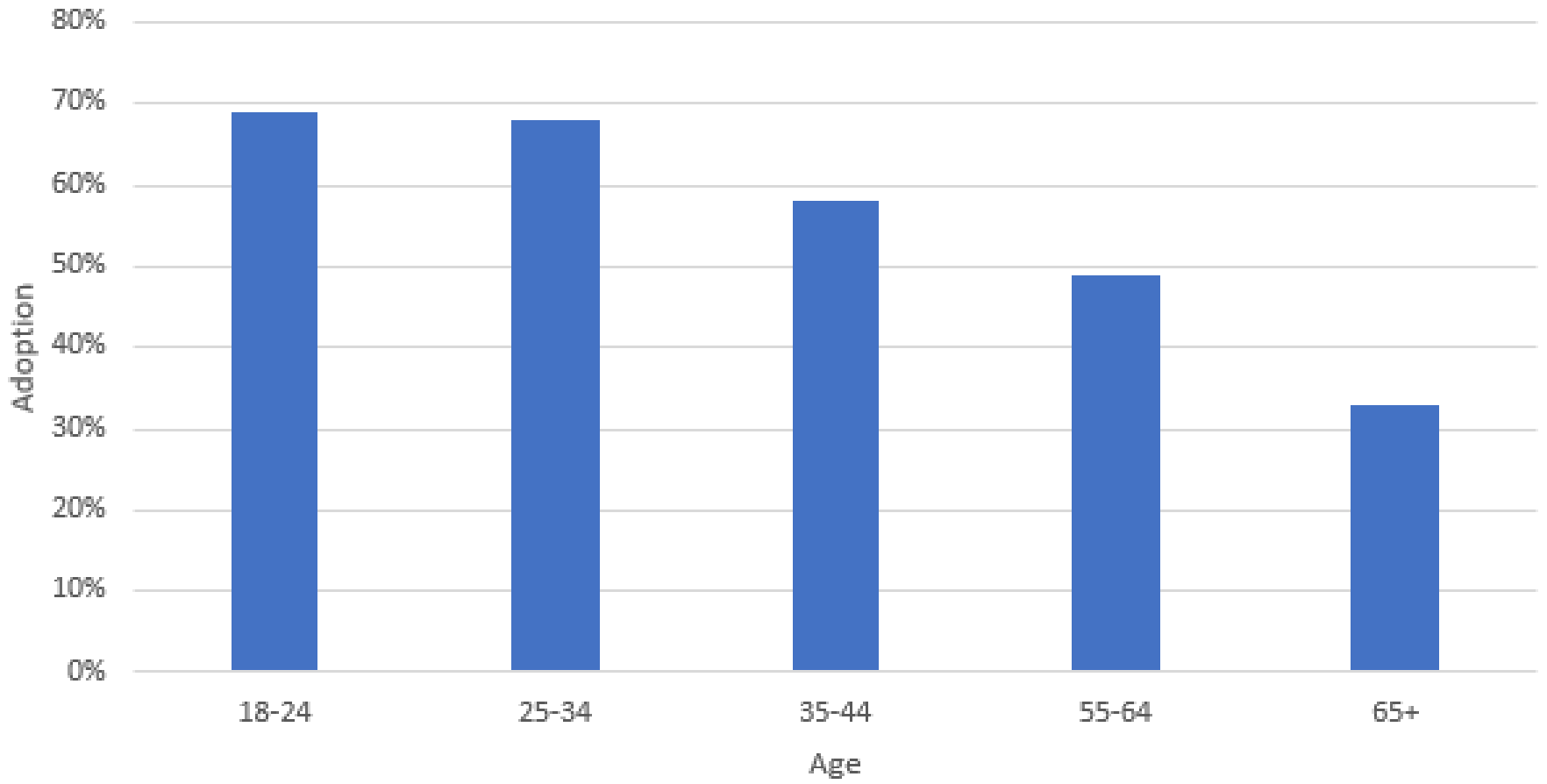
hashes.org

2FA config in companies using Office 365



https://venturebeat.com/2018/08/22/global-survey-reveals-low-adoption-of-multi-factor-authentication-for-office-365/

2FA adoption vs age



https://www.sans.org/reading-room/whitepapers/authentication/paper/37607

https://www.darkreading.com/application-security/younger-generations-drive-bulk-of-2fa-adoption/d/d-id/1336581

https://haveibeenpwned.com/Passwords

https://breachalarm.com/

Is it about me?

Who would ever want to attack me?

"Why would anybody want to break my user's account?"

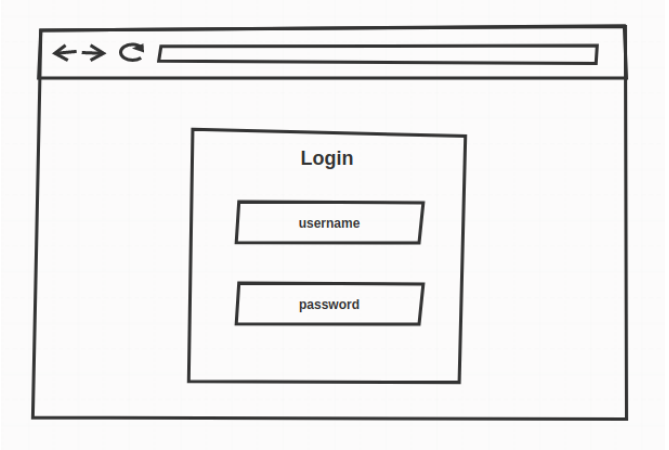
"My service is small, no sensitive data here"

The story

How they were improving and how we followed

Credentials Stuffing

Trying leaked logins and passwords



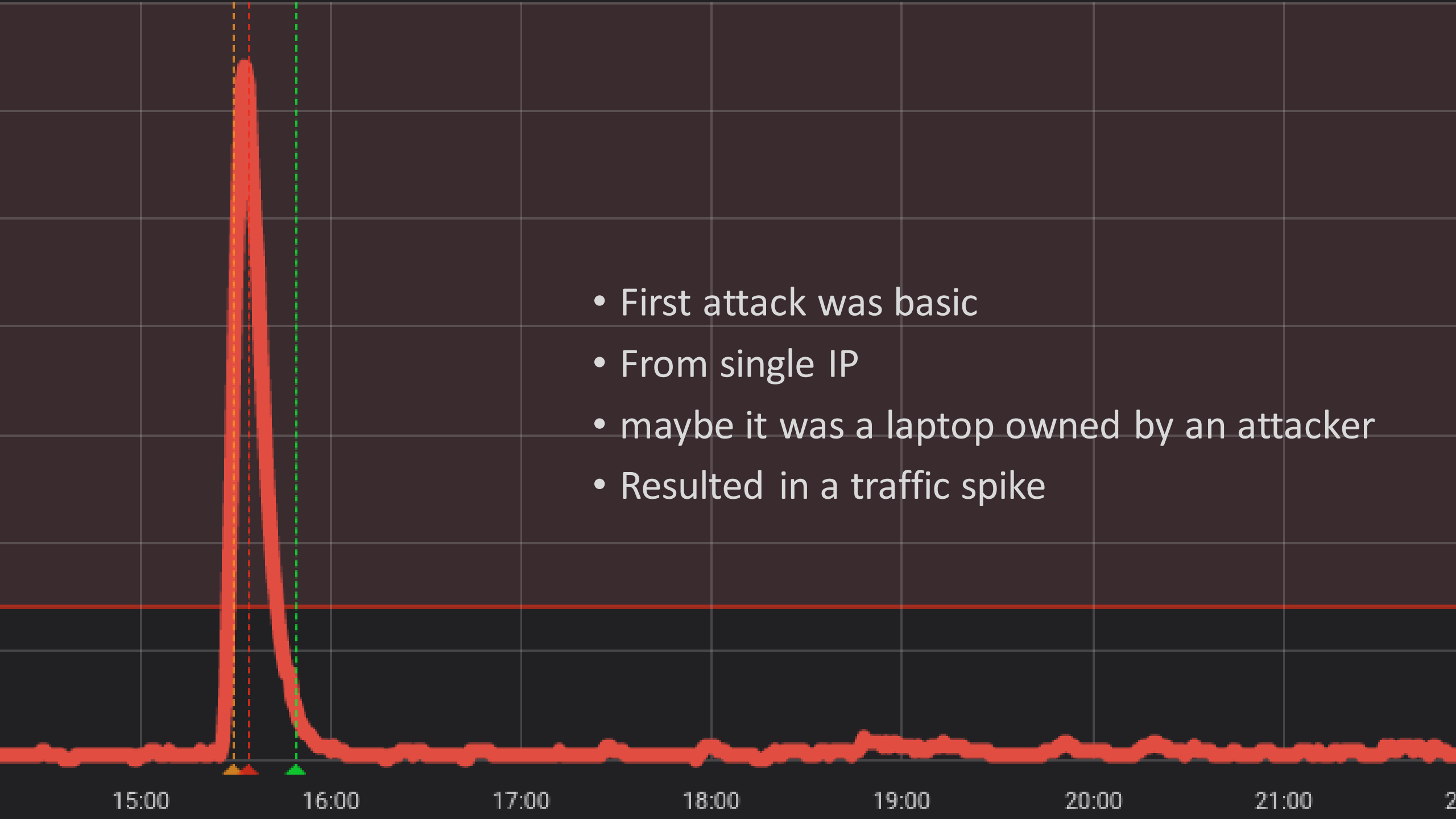
10-million-password-list-top-100.txt

10-million-password-list-top-1000.txt

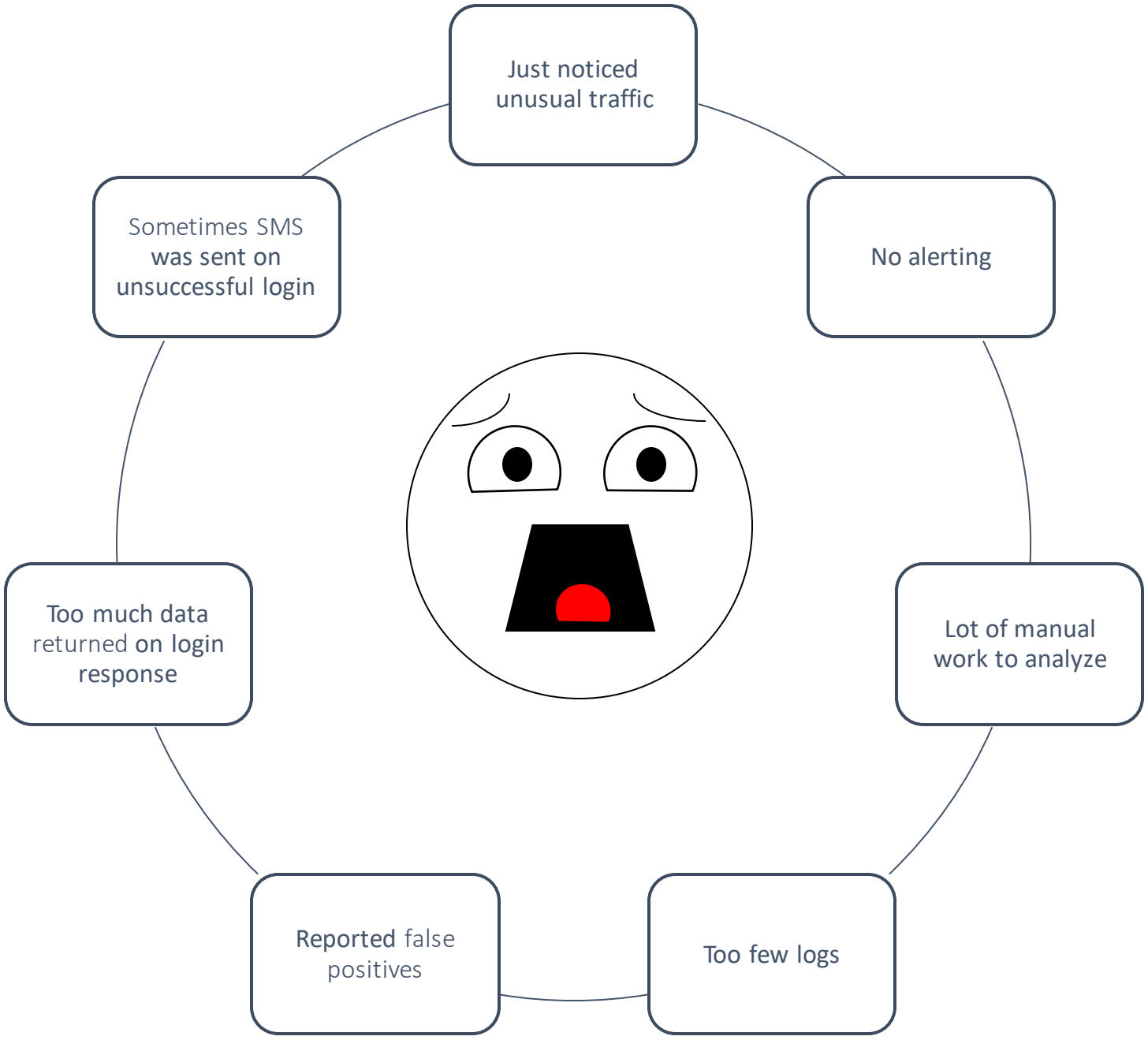
Password Spraying

Trying common publicly known passwords

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html
https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials



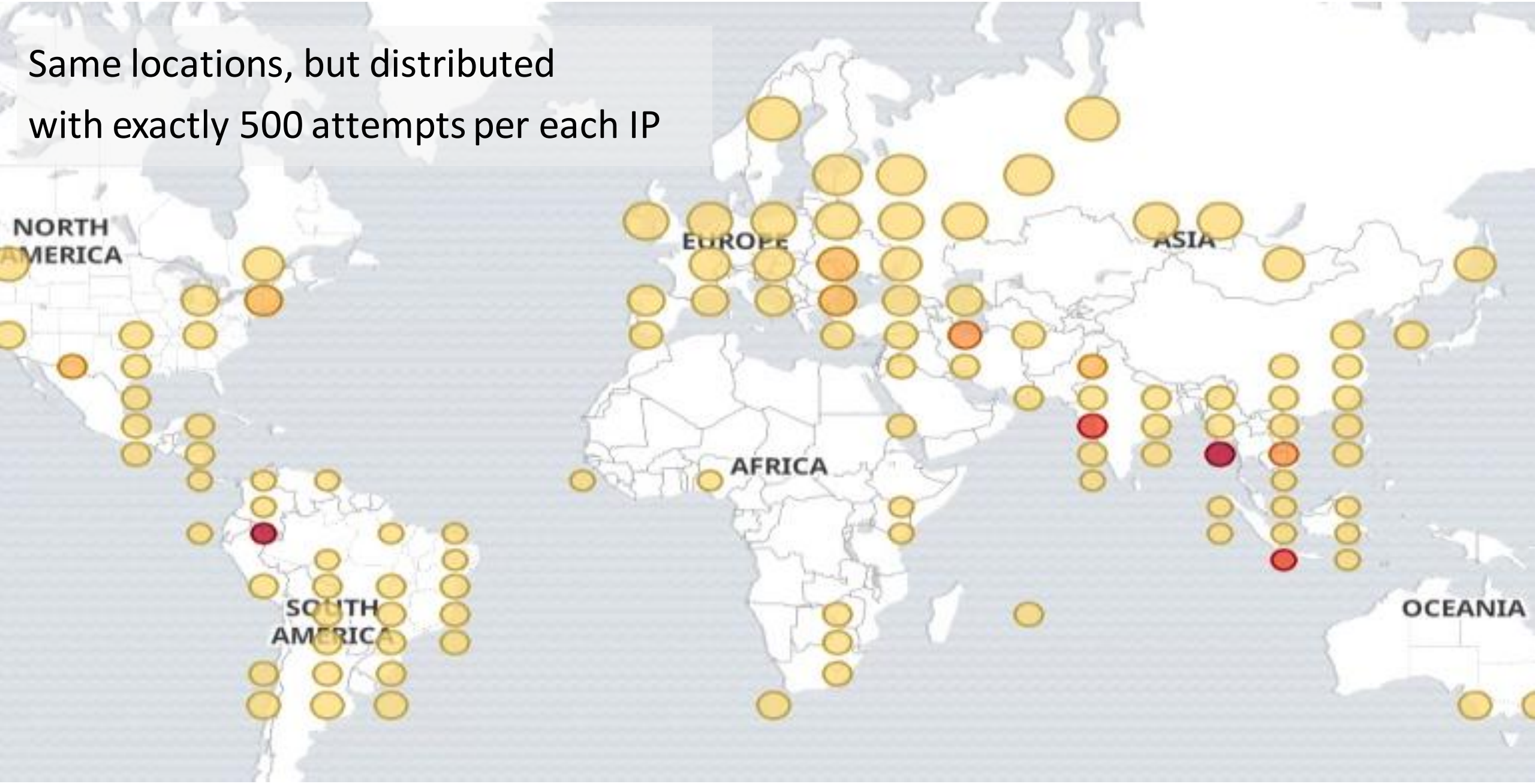
- First attack was basic
- From single IP
- maybe it was a laptop owned by an attacker
- Resulted in a traffic spike


Just noticed unusual traffic
No alerting
Lot of manual work to analyze
Too few logs
Reported false positives
Too much data returned on login response
Sometimes SMS was sent on unsuccessful login

Same type, but from single, distant location

India, Thailand, Indonesia, Argentina, Brazil

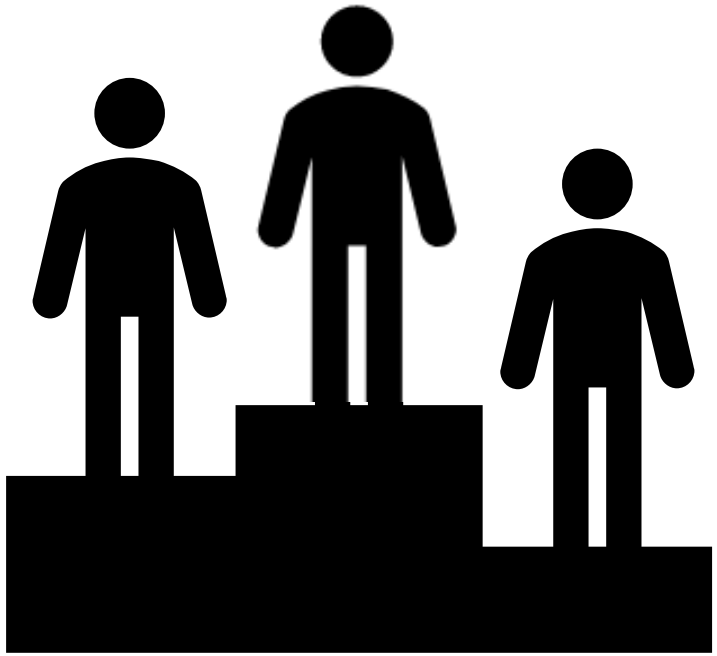
Same locations, but distributed
with exactly 500 attempts per each IP



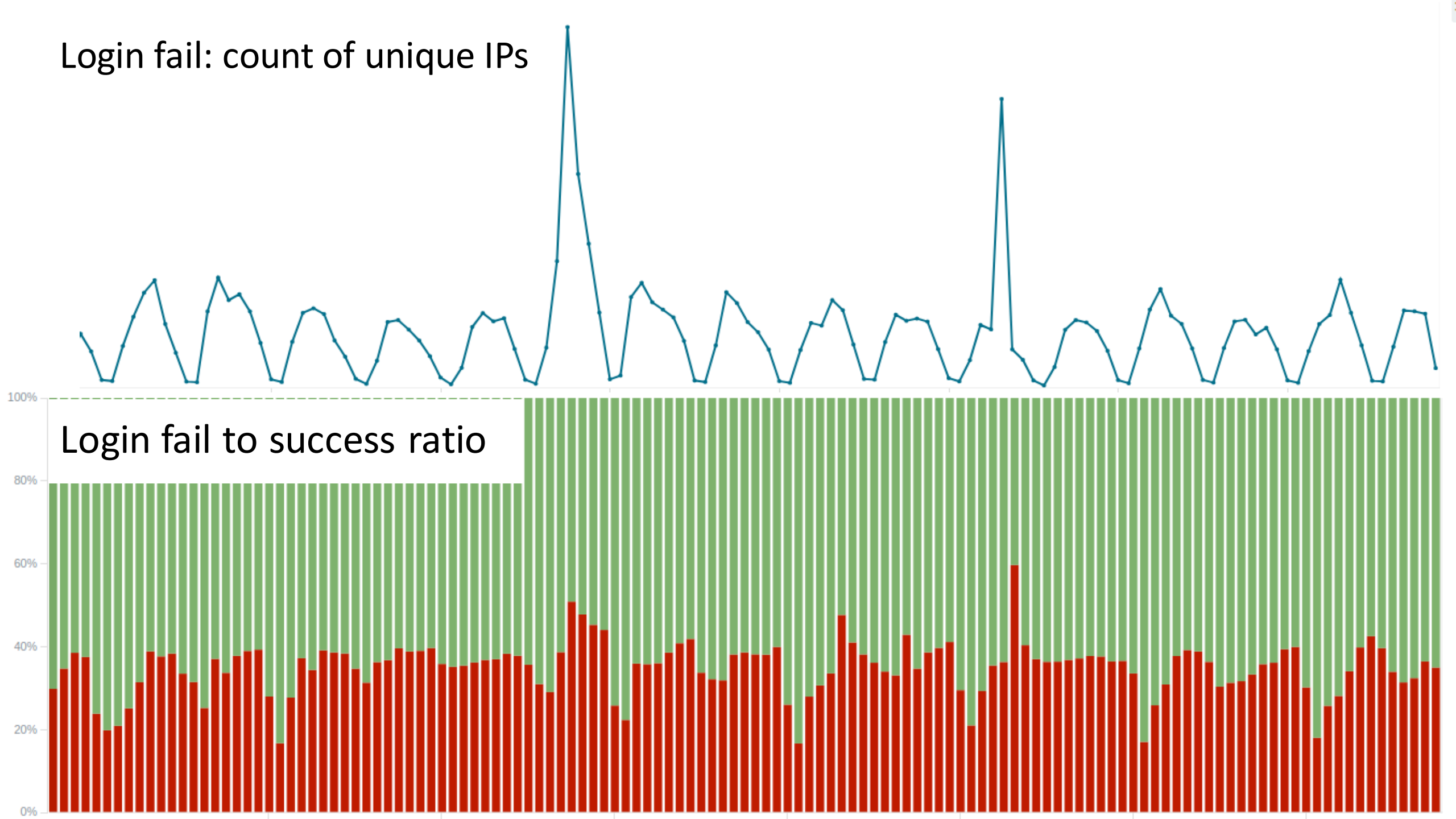
The winner is…

- One request per IP address
- All IPs from one, unexpected country
- Very frequent attempts

The winner is…



- One request per IP address
- All IPs from one, unexpected country
- Very frequent attempts
- No success

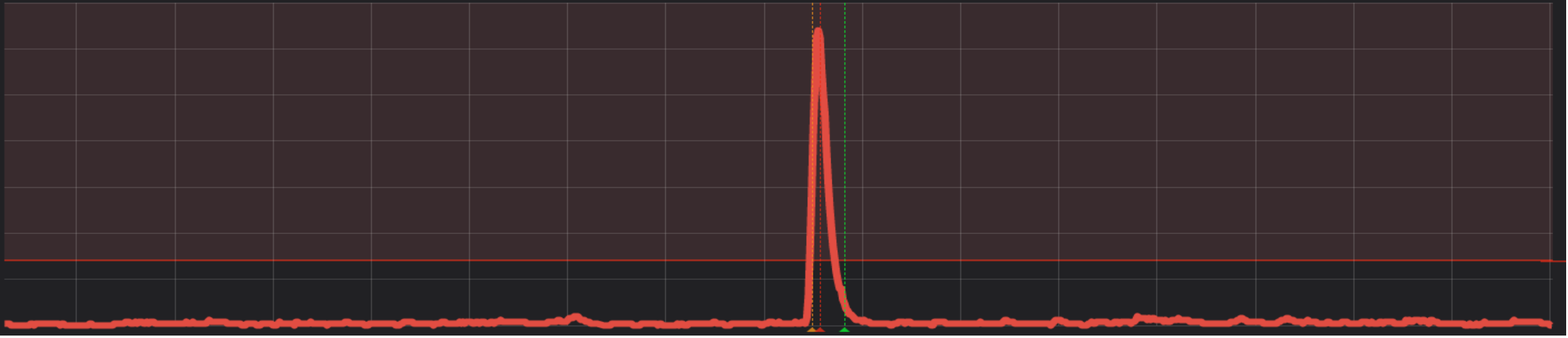

Login fail: count of unique IPs
Login fail to success ratio
100%
80%
60%
40%
20%
0%

Next improvement?

- More patience – do it slowly
- Or do it faster
- Buy better credential databases
- You never know
  - Whether they are improving
  - Or your tools are improving
  - You're still under sophisticated attack

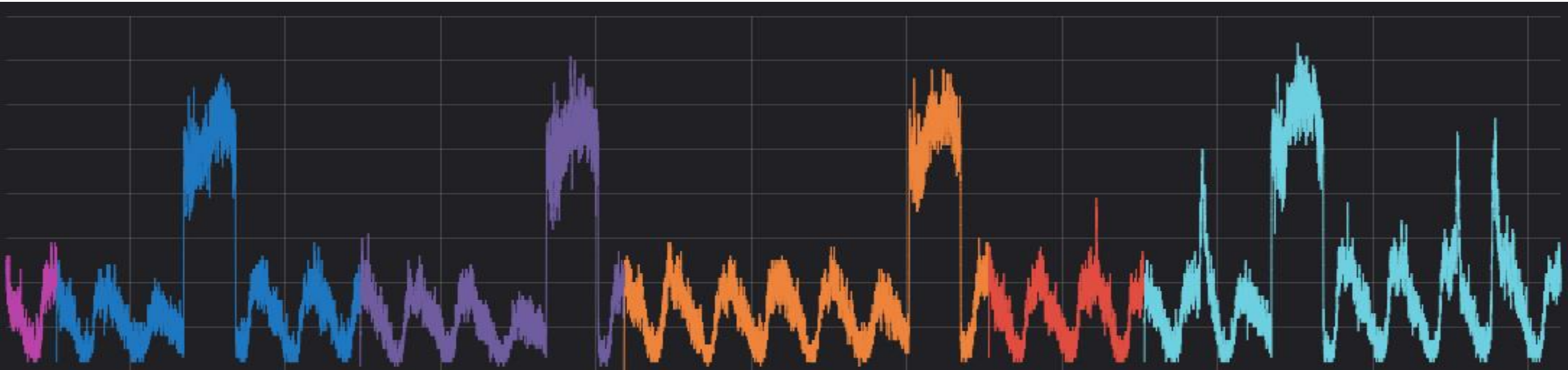
Alerting

How we know

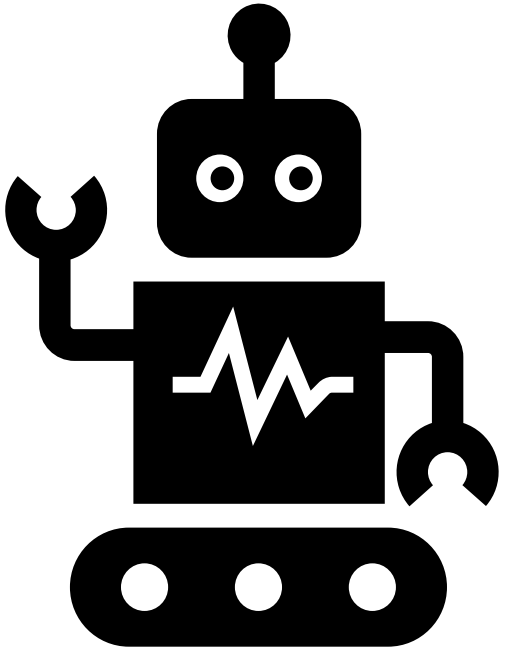


Two things to watch:

1. Traffic spikes
2. Suspicious activity



How to analyze



- Once it happened, it will happen again
- Automate
- Watch misbehaving accounts that do not follow usual patterns
- Monitor when the specificity of the attack changes

What we do

1. Cut off the access
2. Check activity: GDPR and business
3. Report incident
4. Inform users
5. Prevent

Detection vs. prevention

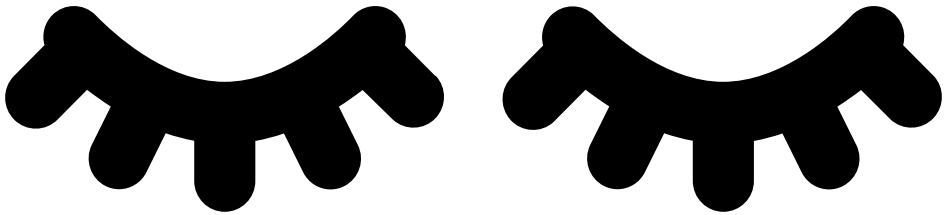
- You can miss precise attacks, for single account
- Most dangerous, because targeted against single user
- Easier to prevent it than detect

`qwerty123` Common Passwords Usage

`Spr!ng2020` zxcvbn: Password Strength Estimation

https://github.com/dropbox/zxcvbn
https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials

After login success, what they do?



Don't have time to analyze the report?

They're checking the user, not us?

Don’t care about our data, but the password reuse?

We were not their target?

They do it for fun?

Why they didn't attack us before?

- new product announced in the TV
- free liters of fuel
- Improved monitoring and alerting

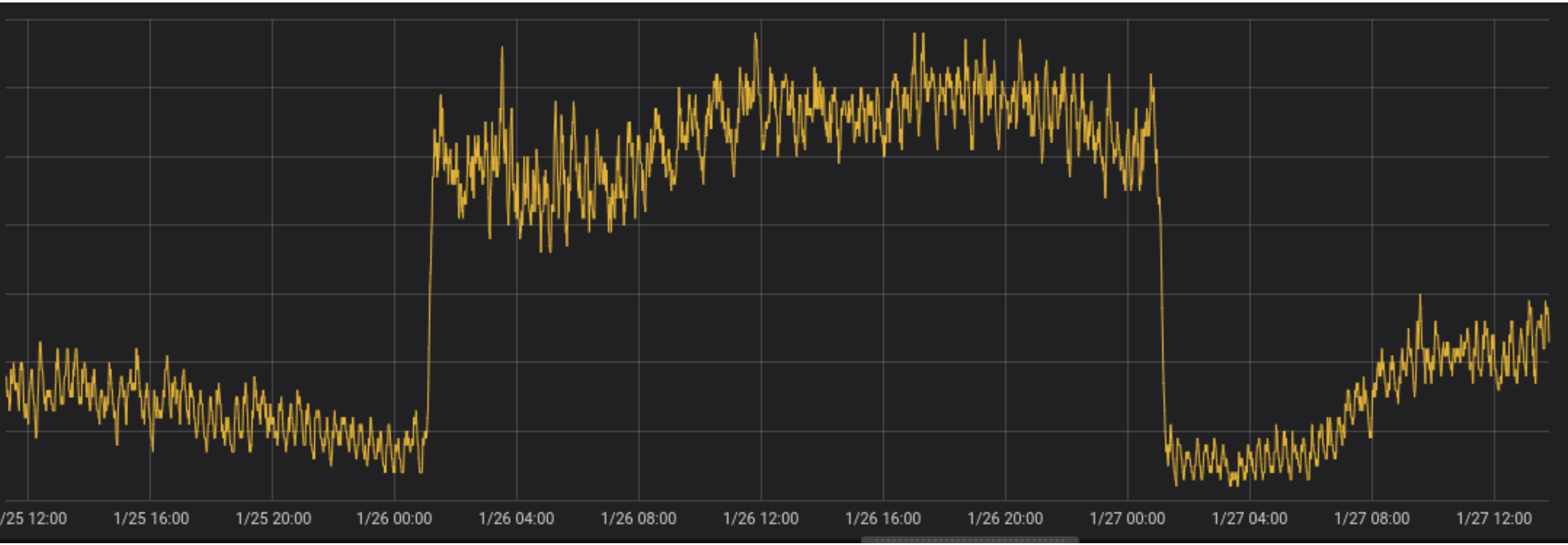
Quiz

How they do it

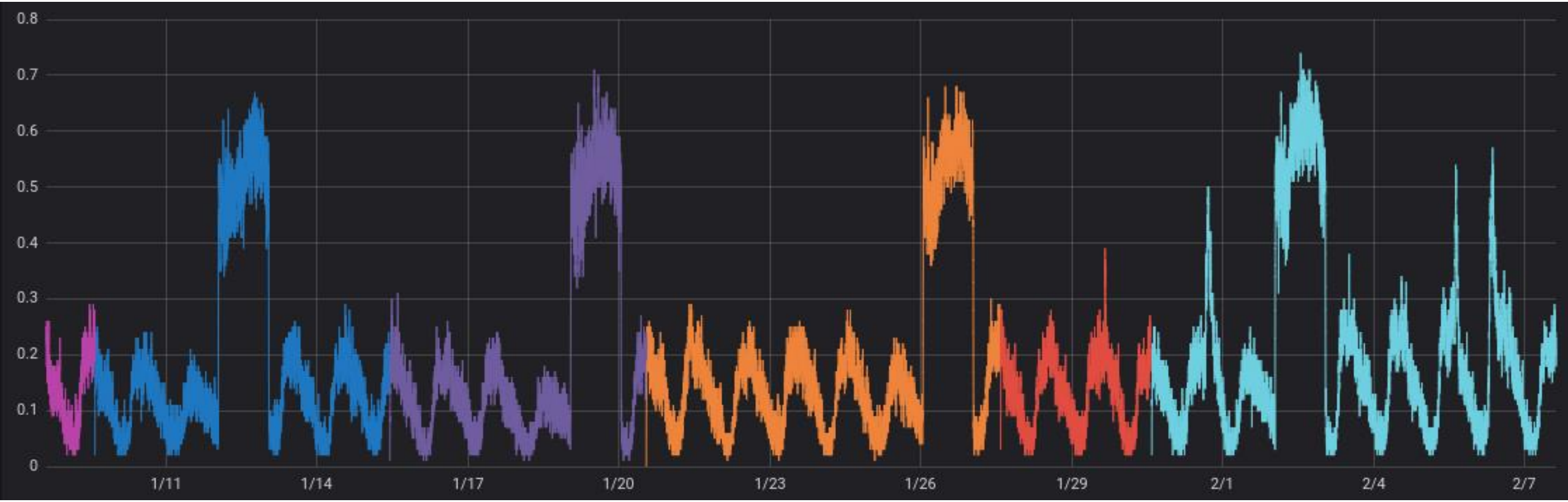
Disclaimer

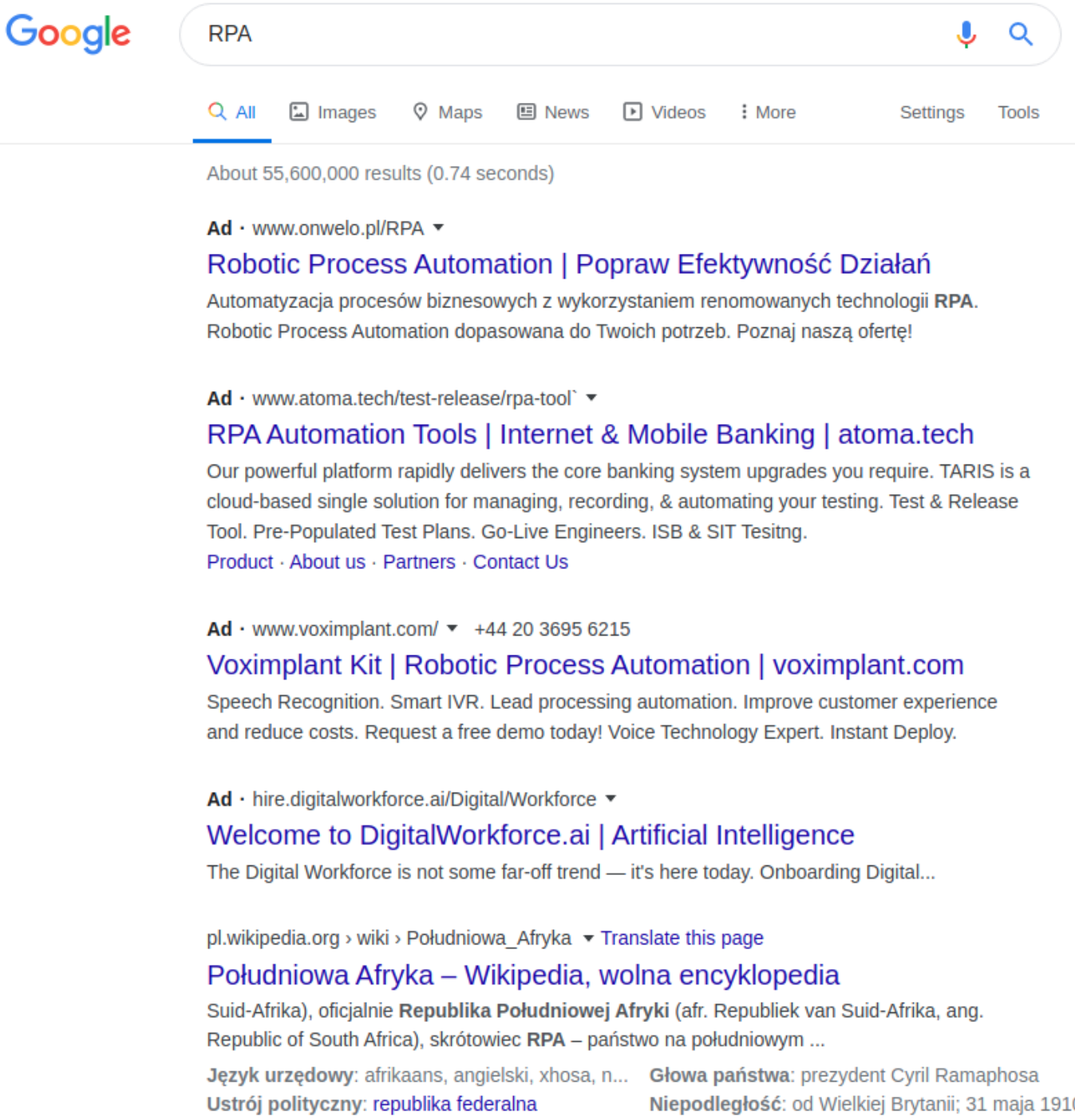
- Showing production metrics
- Not disclosing too much
- Just the traffic change is interesting
- You don't know
  - Order of magnitude on value axis
  - Unit on value axis – delta, count, ops, percentage
  - How much instances we have
  - Load Balancer algorithm
  - Rate limiting rules
  - Dates and hours

Is this an attack?



How about now?





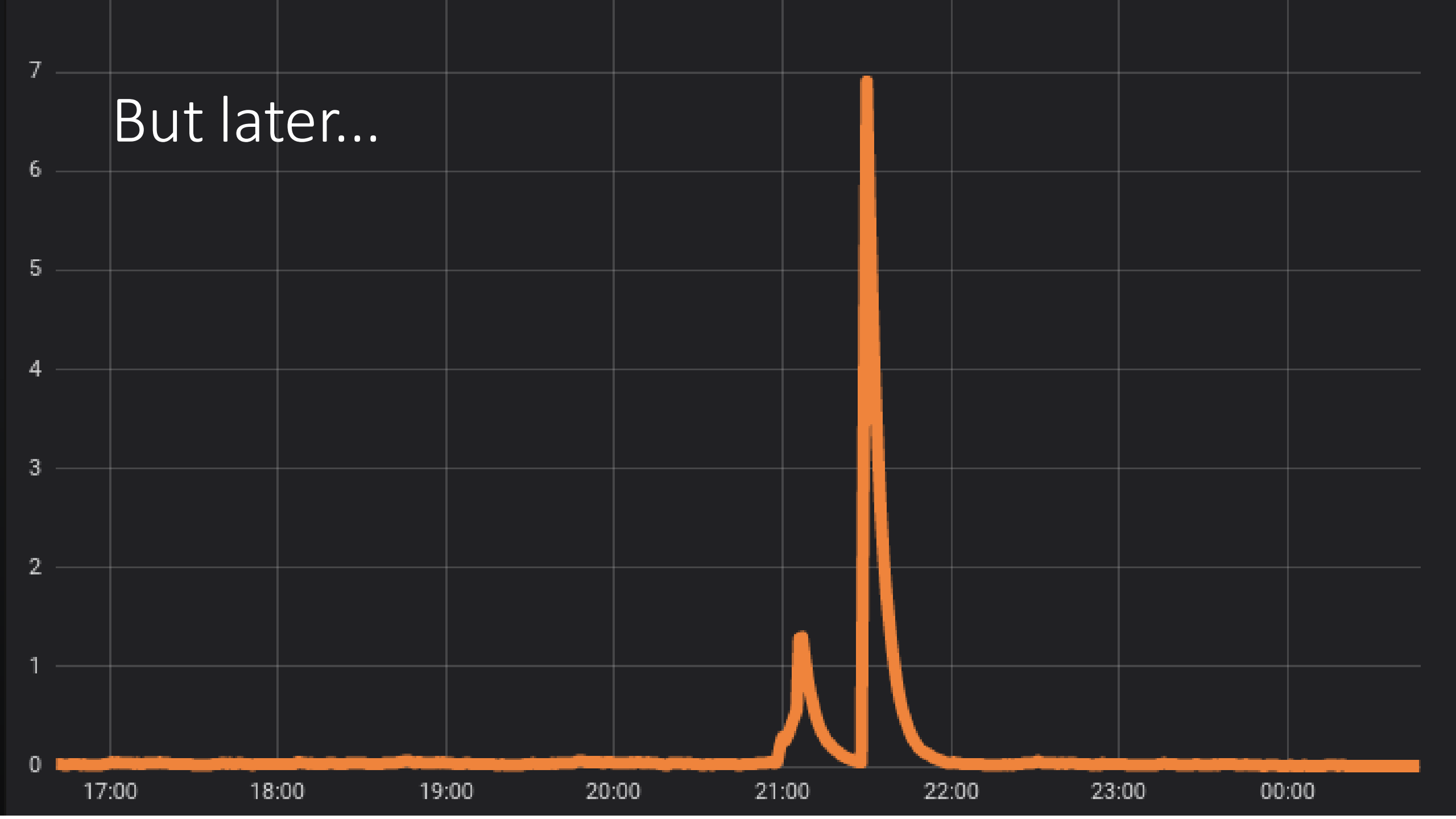
- From single IP
- Every week
- Still having login failures


This one is big
8
7
6
5
4
3
2
1
0
18:30
19:00
19:30
20:00
20:30
21:00

Wait… what?…

```
POST /login/

{
  "email": "{enter-value}"
}
```


But later...
7
6
5
4
3
2
1
0
17:00
18:00
19:00
20:00
21:00
22:00
23:00
00:00

Ah... Now you have it

```
POST /login/

{
  "email": "some@email.com"
}
```

Impact

388 IP addresses

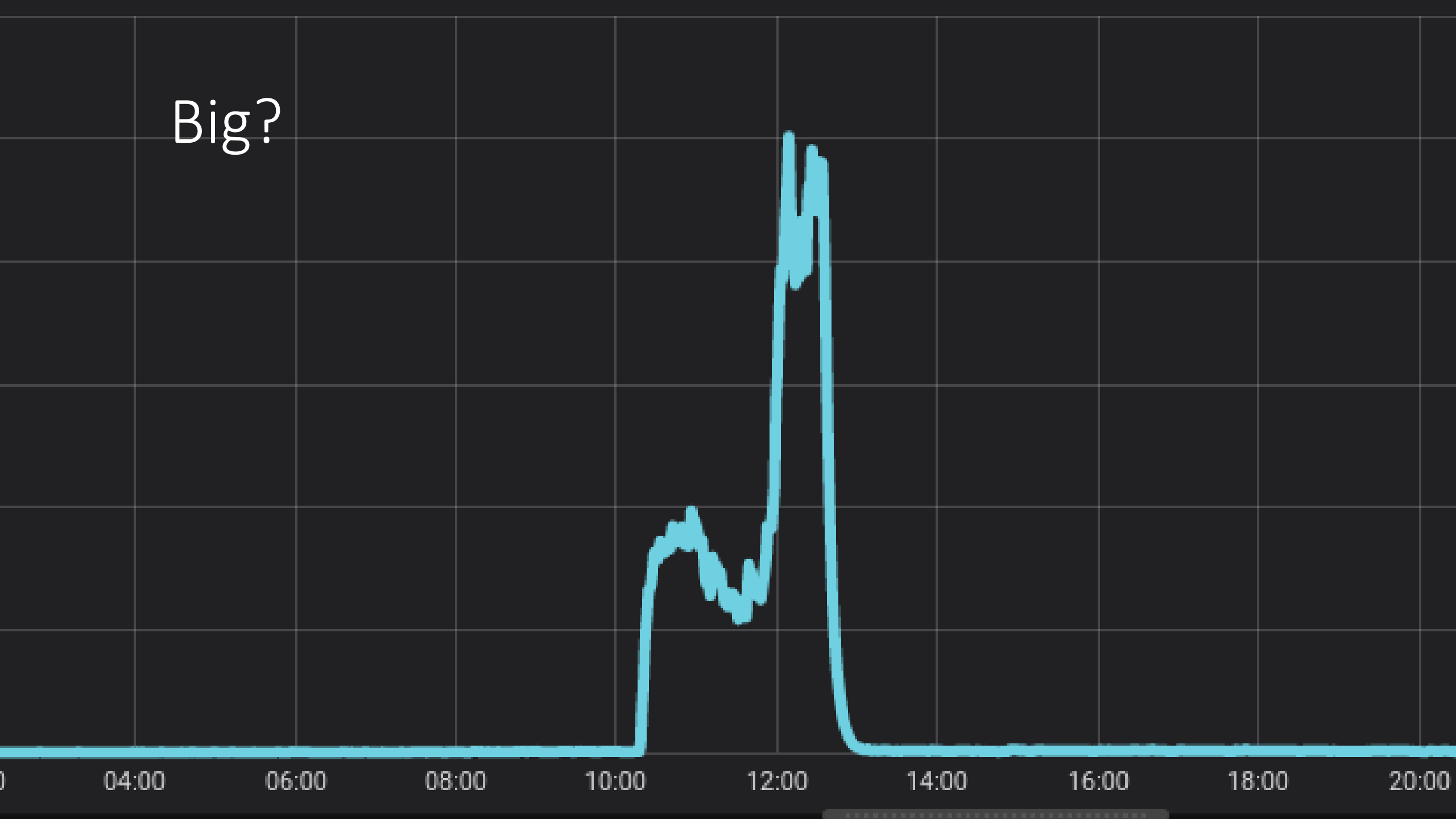
16k requests

11k stopped by Rate Limiter

5k emails tried

1 attempt per account

5 minutes


Big?
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00

Impact

973 IP addresses

98k requests

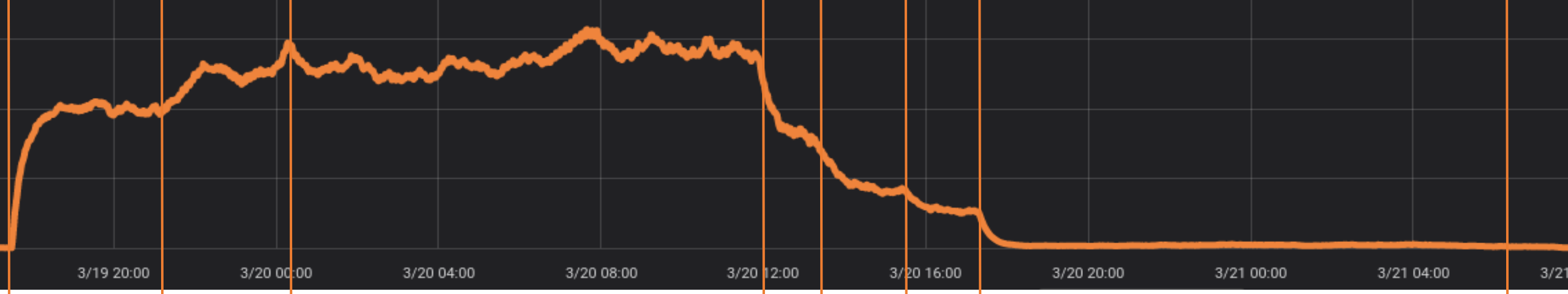
300 requests stopped by Rate Limiting

98k emails attacked

2 hours

Long one


16
14
12
10
8
6
4
2
0
3/19 16:00
3/19 20:00
3/20 00:00
3/20 04:00
3/20 08:00
3/20 12:00
3/20 16:00
3/20 20:00
3/21 00:00
3/21 04:00
3/21 08:00
3/21 12:00



Start

Gaining speed

Spike

Block Thailand, Brasil, Indonesia, China, India

Block Albania, Argentina, Bangladesh, Iran, Pakistan, South Africa (ZA), Viet Nam

Blocked Russia, Ukraine, Turkey, Republic of Korea, Bulgaria, Spain, Iraq, Nepal, Moldovia, Chile

Whitelist trusted countries

End

Impact

5000+ IP addresses

1.8M requests

1.4M emails tried

37 hours

Bonus

All attacked emails where from Danish domains

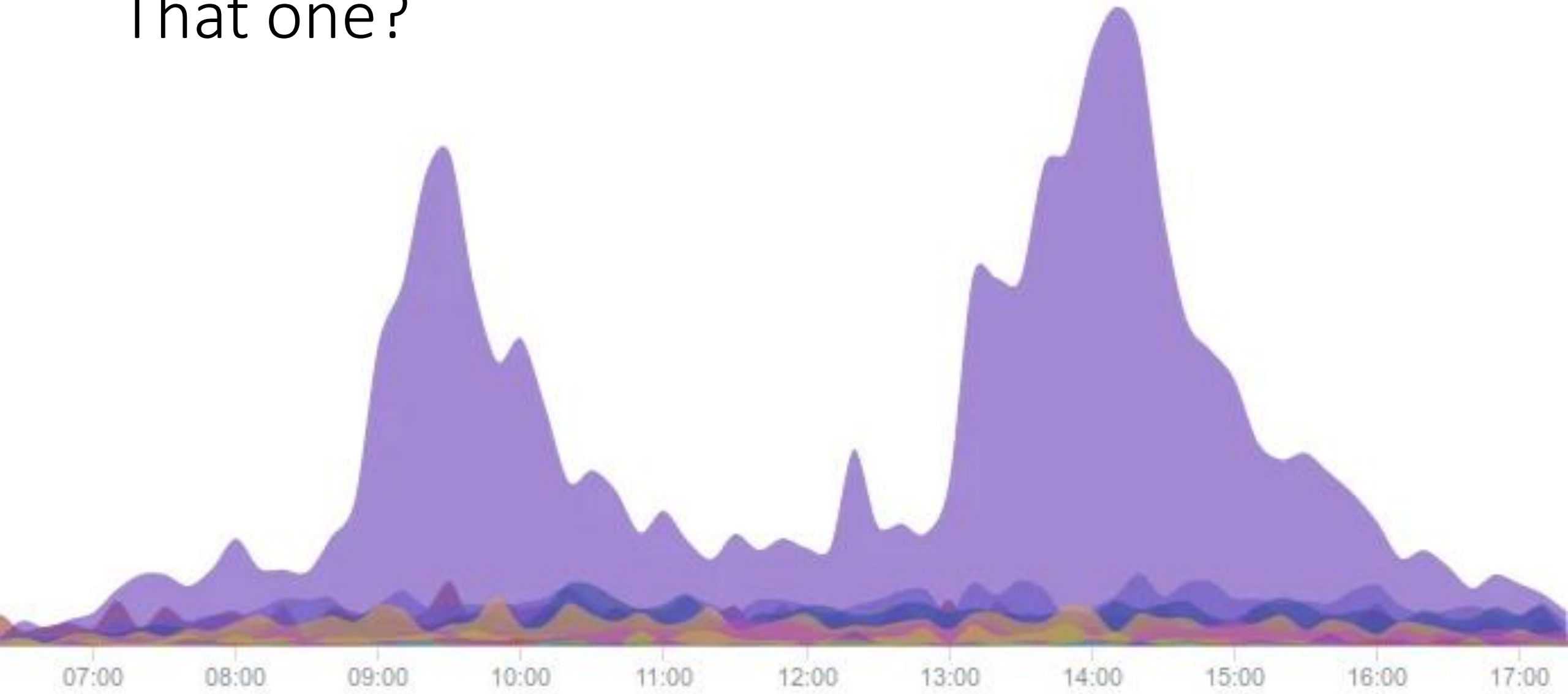
1.4M attacked emails

Denmark population is <6M

Lessons learned

Automate Firewall rules

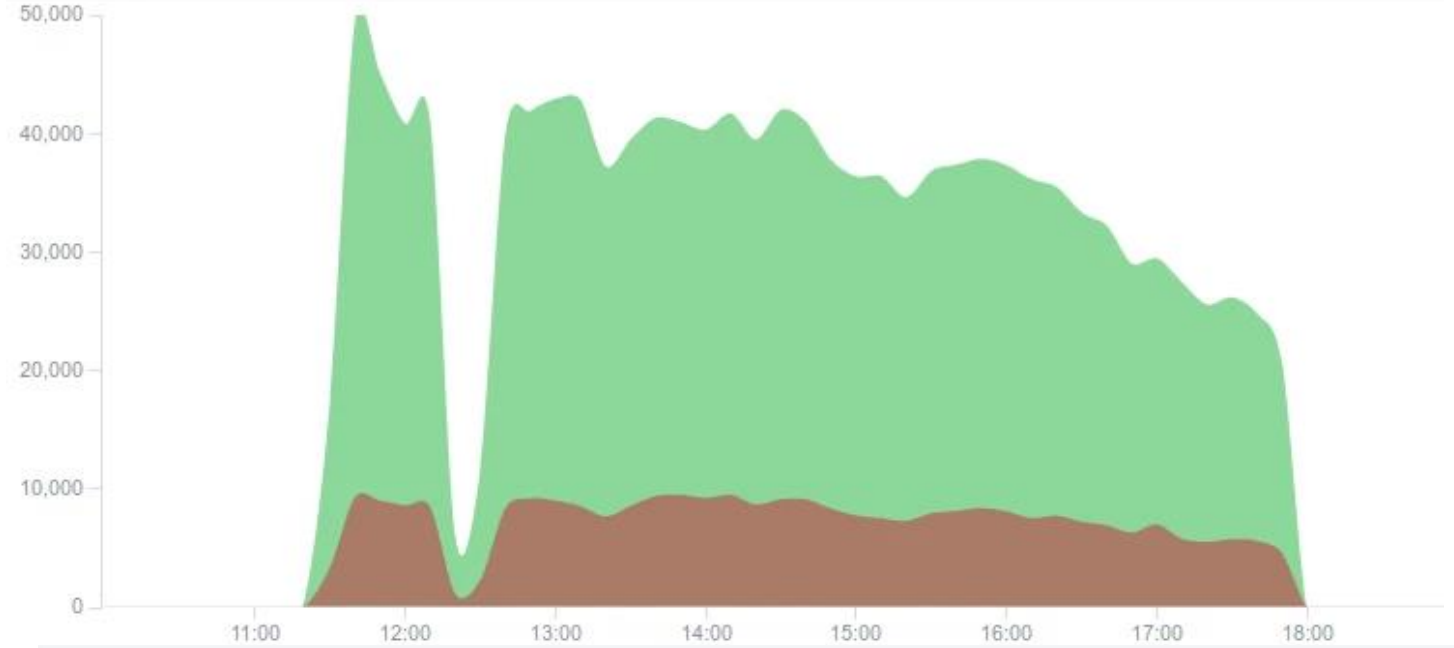
That one?



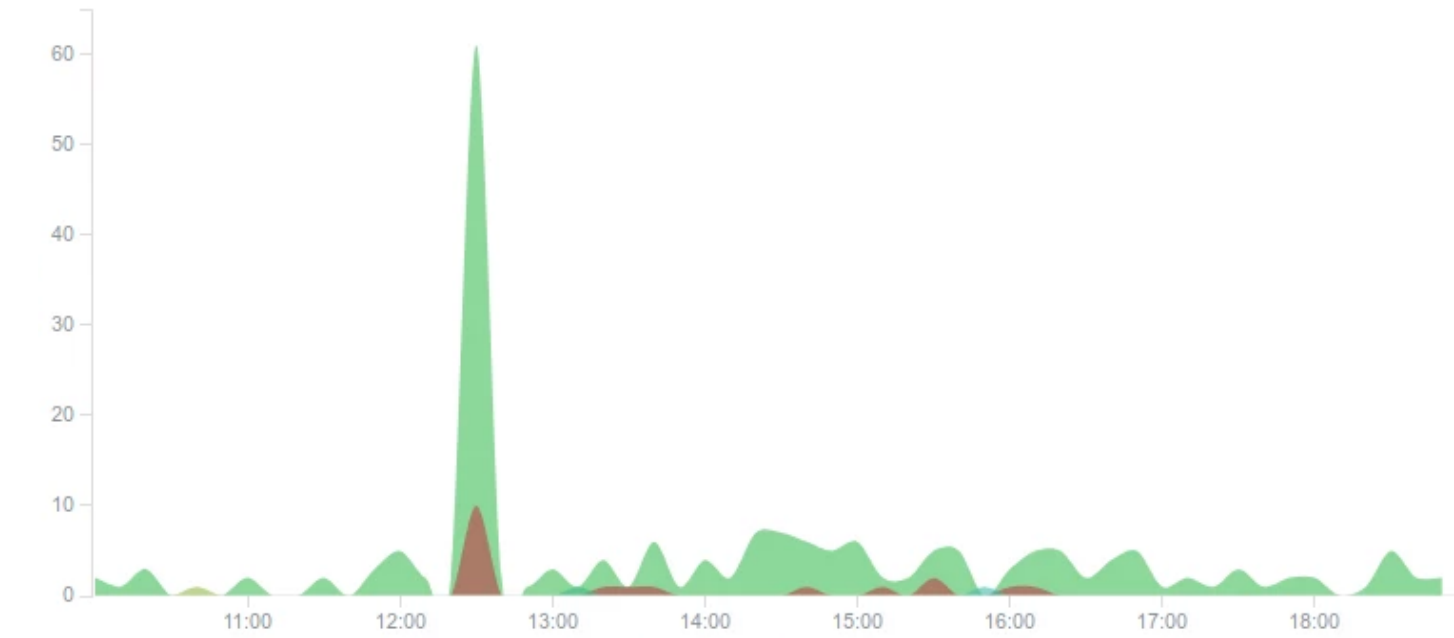
Marketing campaigns

> Hi,
> I would like to inform you that we have planned push notification campaign tomorrow that may cause traffic increase
> Push notification sendout time:
>
> 30th, at 10:00 AM (GMT +2:00),
>
> Best regards,

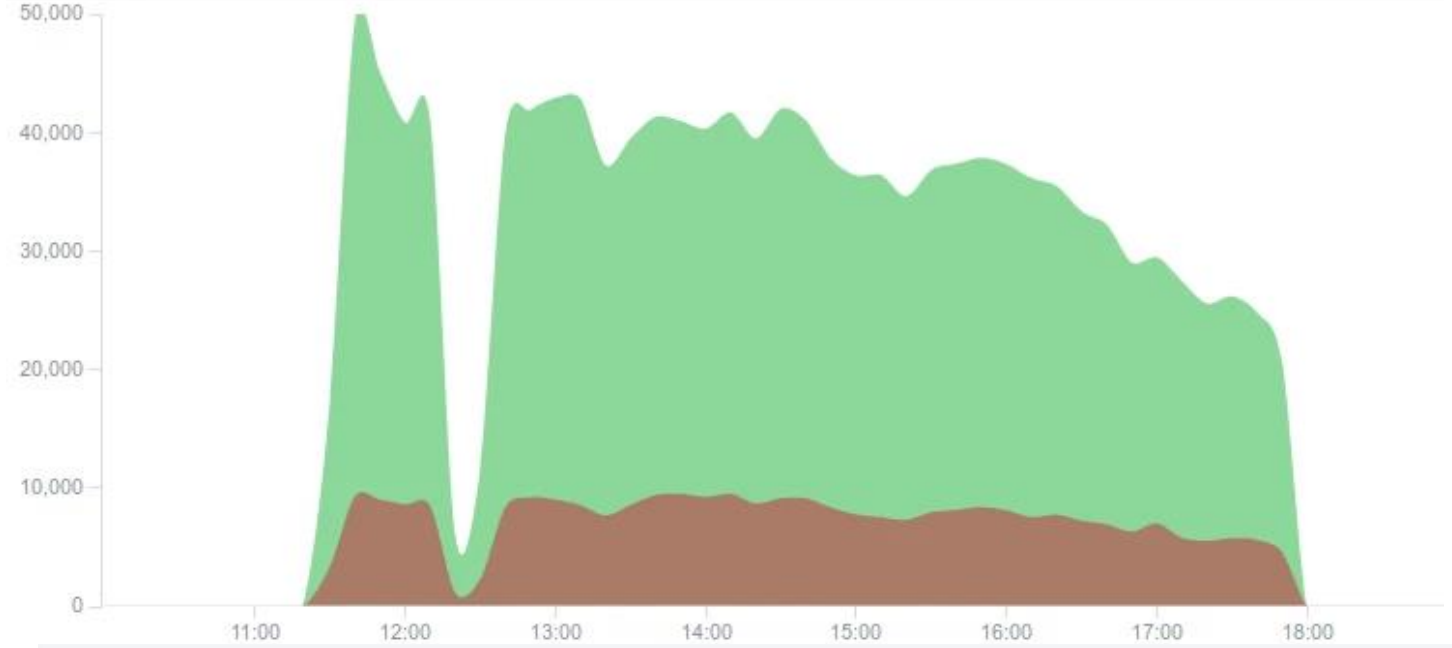
LOGIN_FAIL per selected countries



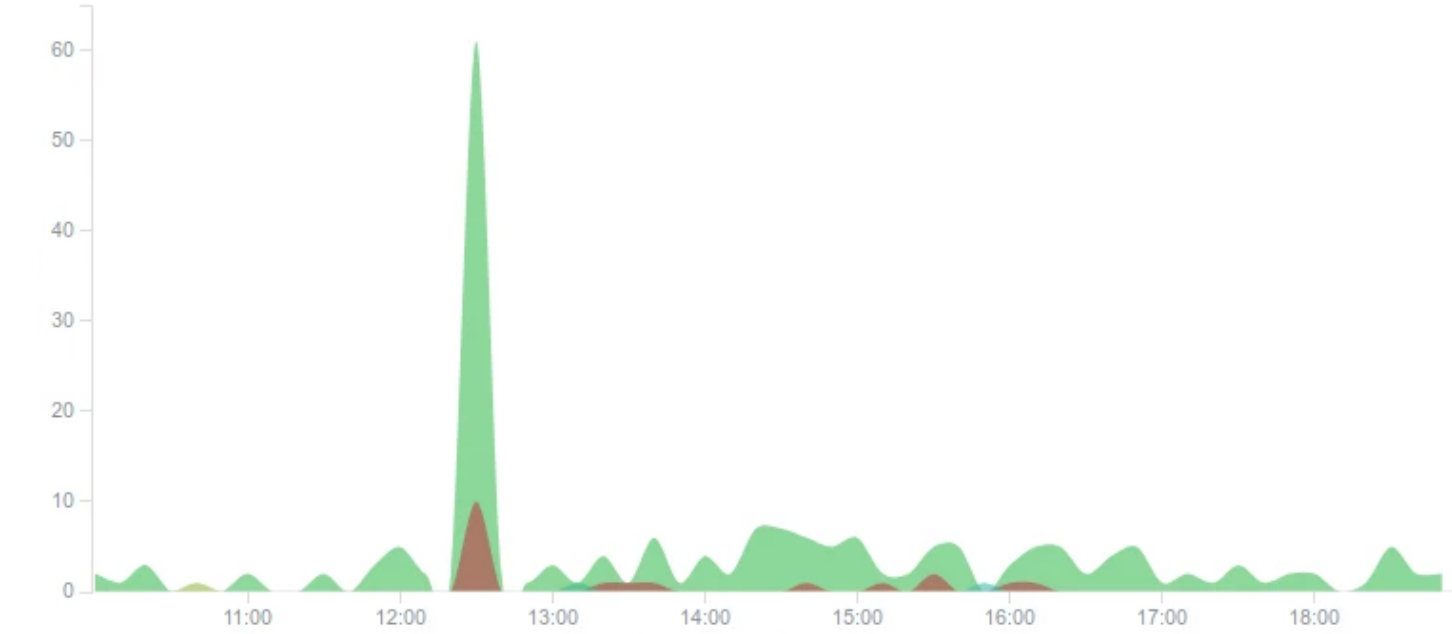
LOGIN_OK per selected countries



LOGIN_FAIL per selected countries



LOGIN_OK per selected countries



68 LOGIN_OKs during the break in LOGIN_FAIL

- Email from domain serving `Encrypted Email Accounts Based in <safe country>`
  - We know that email address
  - Account created just before the attack
- MVNO mobile phone number
  - Number confirmed with SMS code
  - We know from which country
  - We know that this country requires prepaid cards to be registered

How we protect

How to stop it

Any ideas?

Procedures

- Incident handling

Additional protection

- 2FA
- reCaptcha
- Detect Login from new device

Limiting traffic

- Rate Limiting
- Block account after login failures
- Block headless browsers / require JavaScript

Blacklisting

- IP Blacklisting
- Country Blacklisting

Password requirements

- Enforce stronger passwords
- Enforce password change

https://blog.shapesecurity.com/2017/07/12/how-cybercriminals-bypass-captcha/
https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Responsibility?

Users?

Developers?

Security?

Support?

Culture

Any advice?

1. Do not return more data than needed
2. Be careful on sending communication to users
3. First class monitoring from day one
4. Have a mechanism to secure suspected user accounts
5. Use trusted Identity Providers
6. Use 2FA

Are you attacked?

Do you know?

Thank you

Jacek Milewski