Exploring DNSBL query traffic

Subtitle

SPAMHAUS

DNSBL - DNS based Block List

Like DNS, an -awesome- distributed database, but now of reputational data.

First done by Eric Ziegast back in 1997, widely supported these days.

Usually used for IP addresses (v4 & v6), host and domain names, hashes (files, emails), ...

Anatomy of a lookup - IP

Want to know about 192.0.2.1?

```
A 1.2.0.192.zen.spamhaus.org
-> 127.0.0.3 -> Spam emitter
```

Anatomy of a lookup - Hostname

Want to know about hostname.example.tld?

```
A hostname.example.tld.dbl.spamhaus.org
-> NXDOMAIN -> OK Hostname
```

Anatomy of a lookup - Hash

Want to know about

`3d0bb4e19a649369d33ba9670866a51711add65a48204a6713e20842a2811963`?

SHA256 -> Base32 ->

```
A adtr46epieqvm7c3geodzctxo2huqso34t3yylvbcmpoaa3gsba._file.hbl.spamhaus.org
-> 127.0.3.10 -> Malicious file
```

DNS Infrastructure

Anycast authoritative for the main zone

Delegated NS for the DNSBL content, with regional clusters.

Special DNS server made for DNSBL type zones - CIDRs, exclusions, wildcards, supports very large zones.

Query traffic - What we're expecting

Mailservers looking up IPs that send email.

Mailservers looking up domains in email

- Not just body, also rDNS, HELO/EHLO, From, etc
- A/NS IPs for said domains

Things we shouldn't see, but expect to see anyway.

Query traffic - What we're actually seeing

All the previous things - mostly good!

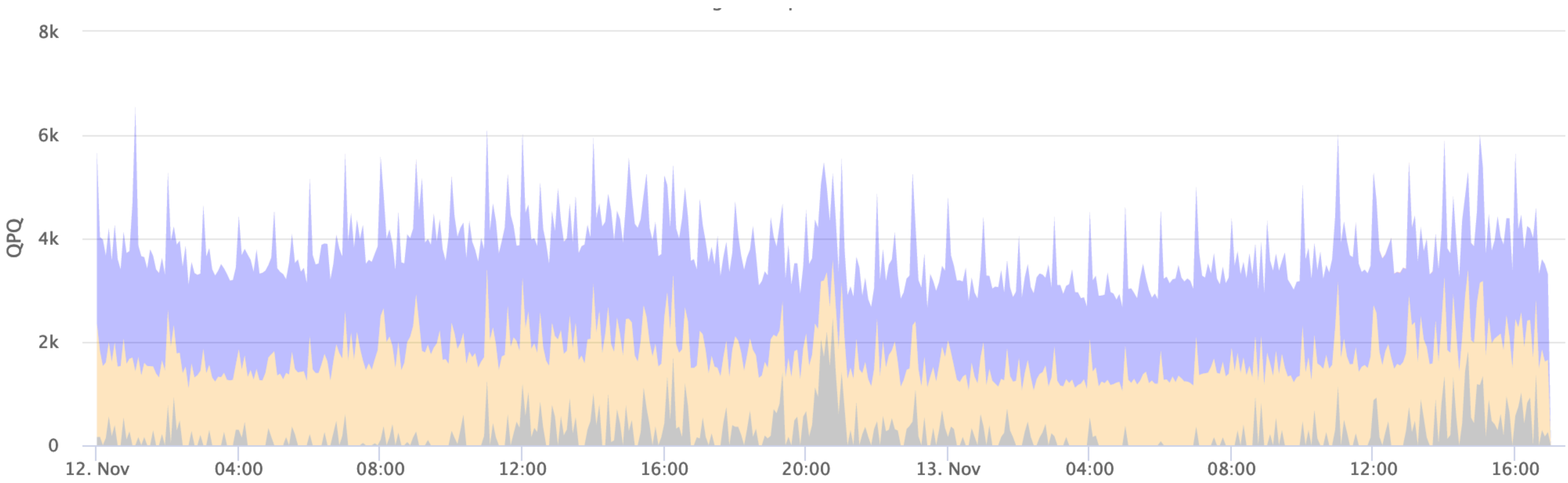
Misconfigs, leaks

Bad actors doing bad things

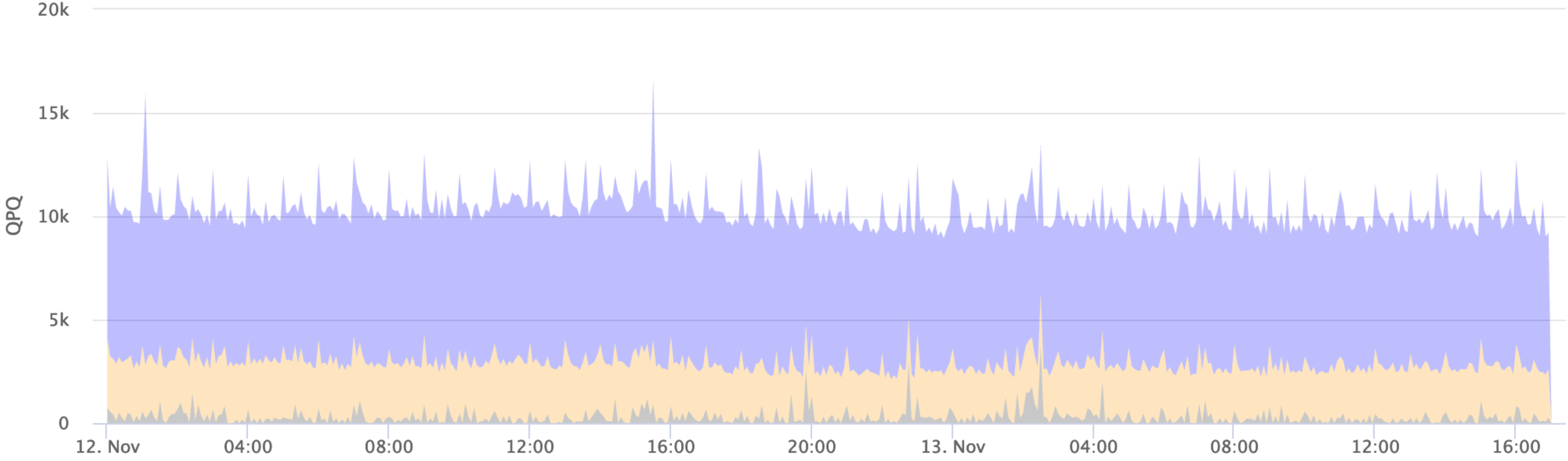
Things deserving of WAT

WAT

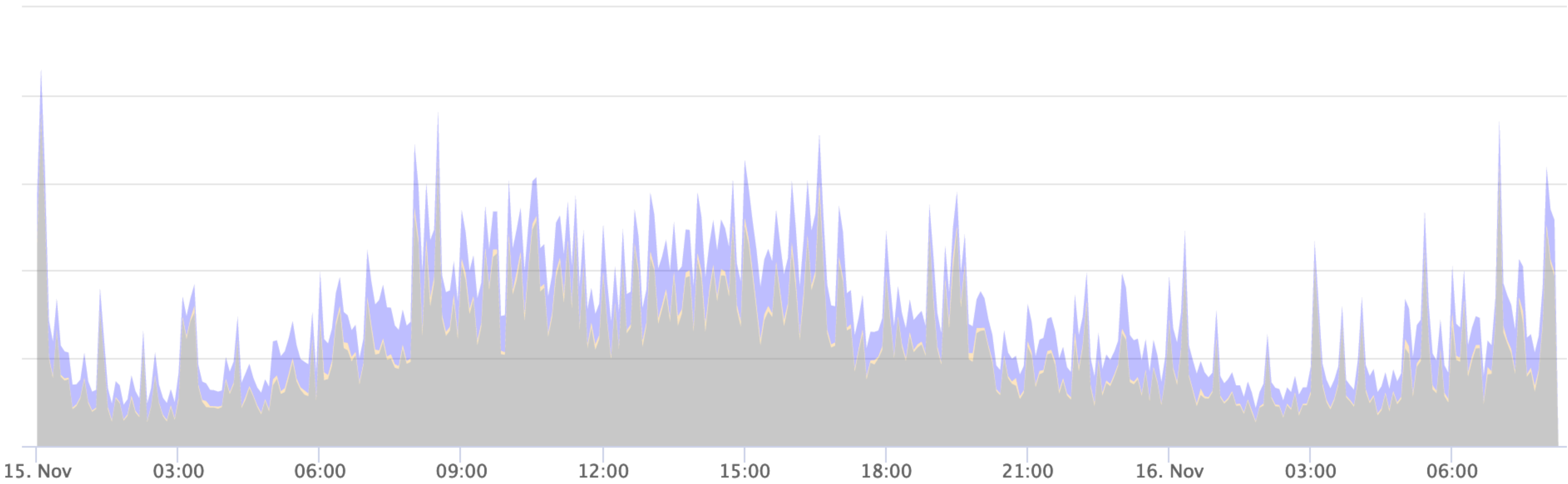
192.168.0.0/24


8k
6k
4k
2k
0
QPQ
12. Nov
04:00
08:00
12:00
16:00
20:00
13. Nov
04:00
08:00
12:00
16:00

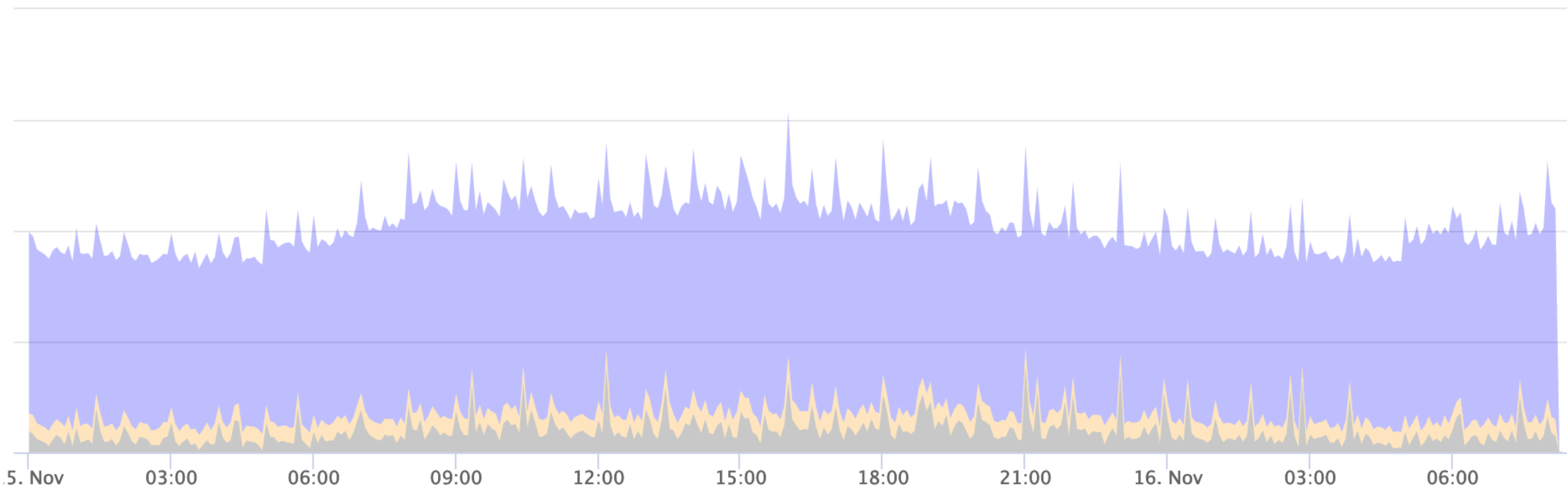
192.168.1.0/24


20k
15k
10k
5k
0
QPQ
12. Nov
04:00
08:00
12:00
16:00
20:00
13. Nov
04:00
08:00
12:00
16:00

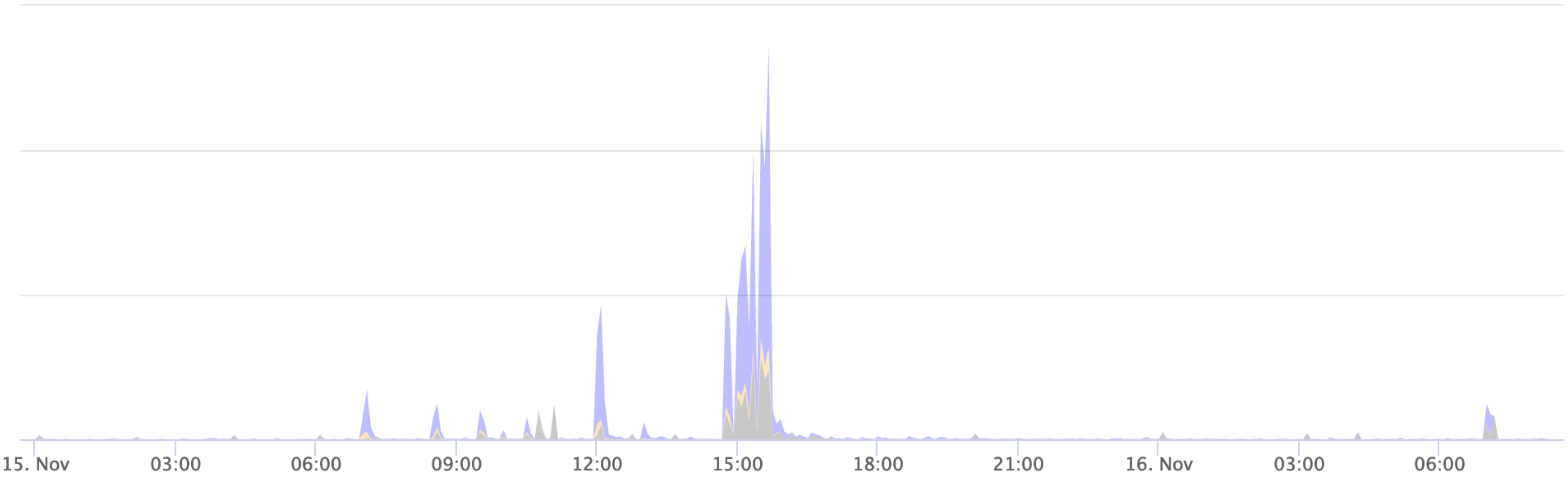
Big global sender - twitter.com



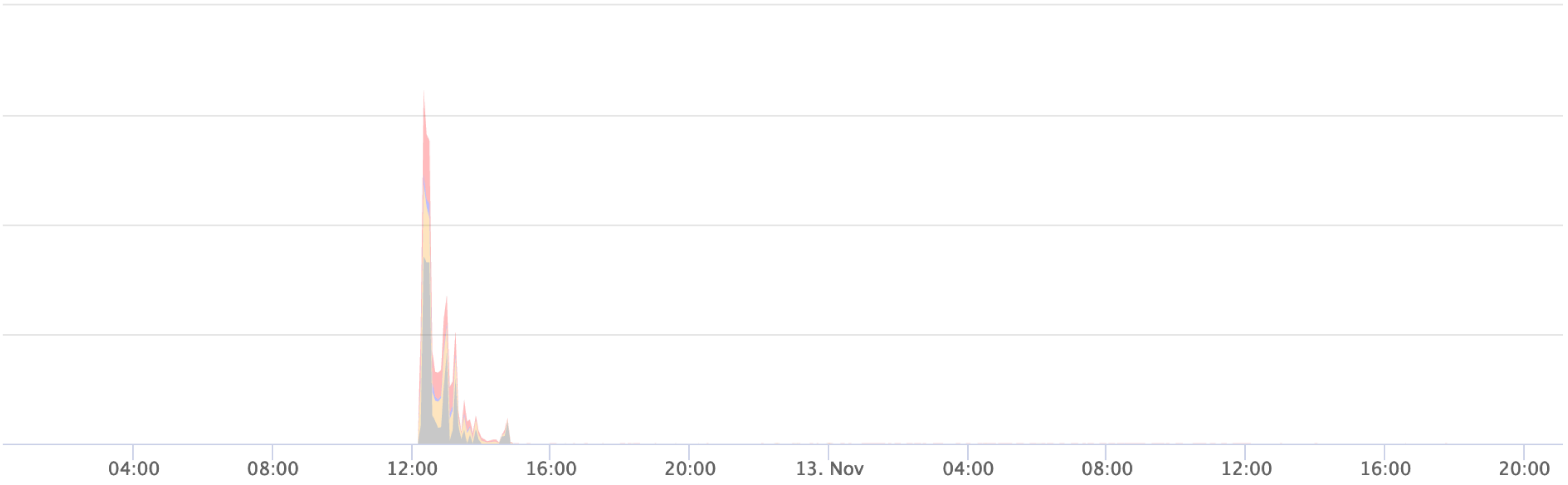
Big global sender - facebook.com



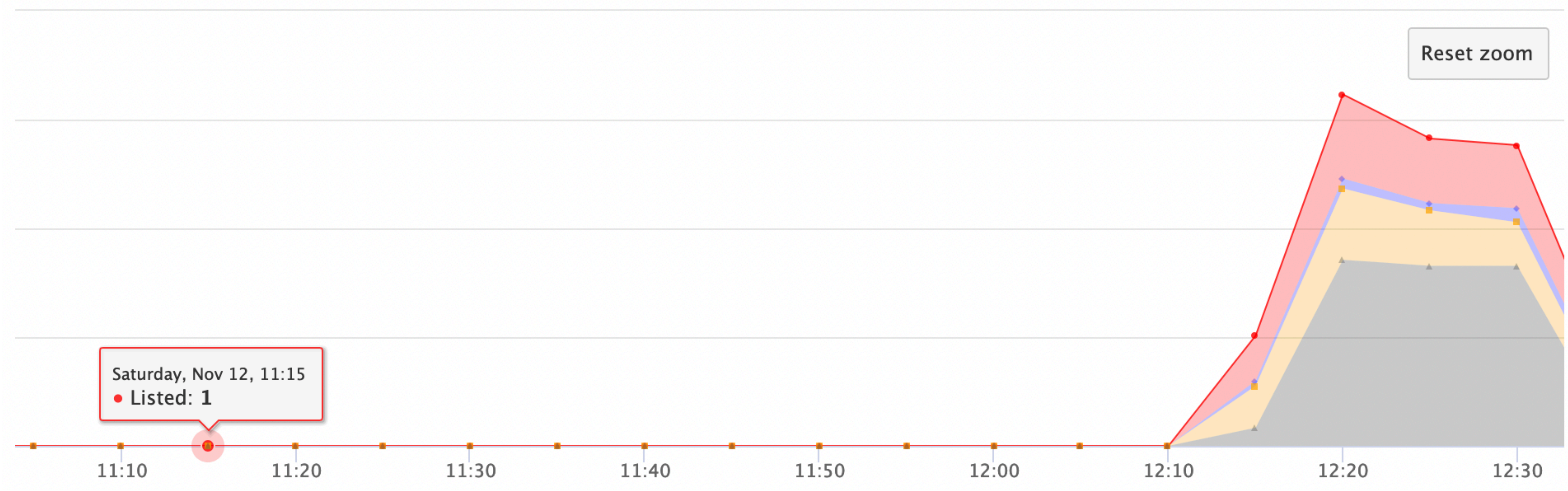
Newsletter - klm-mail.com



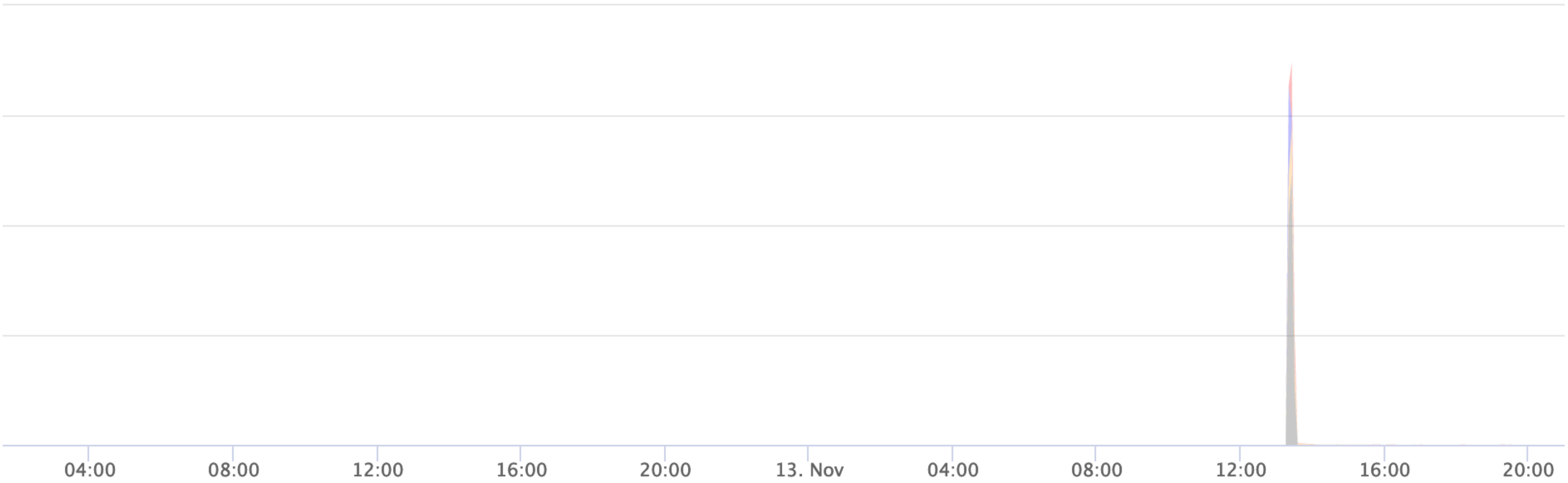
Regular spam run - airfountains.biz



Zooming in - airfountains.biz



'Hailstorm' spam run - womenrevital.co



Notice something?

Even though these can protect you.In reality, when a crisis happens so quickly.

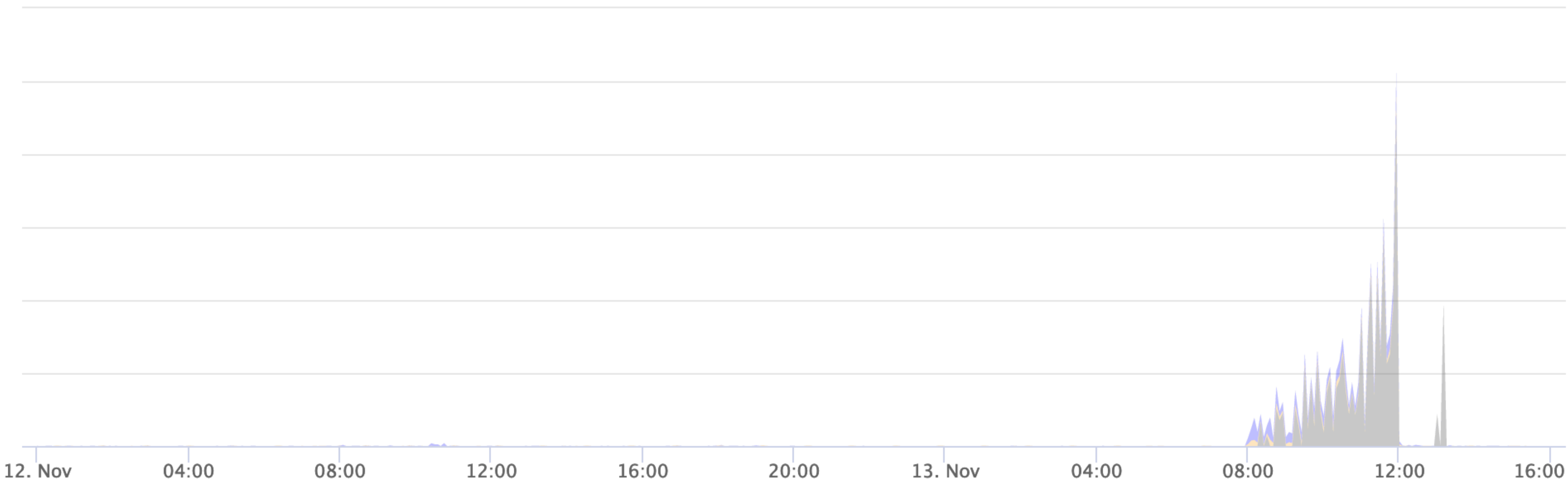
Just fill out the brief questionnaire that follows.It is that easy!

Notice something?

Even though these can protect you.In reality, when a crisis happens so quickly.

Just fill out the brief questionnaire that follows.It is that easy!

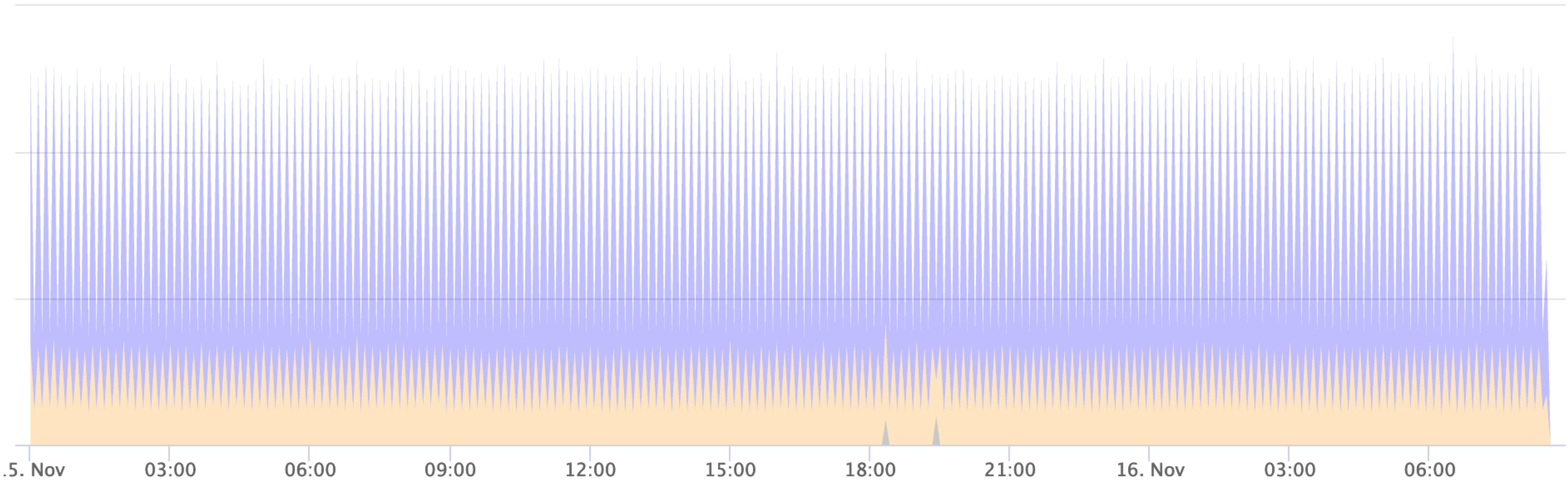
Liberal parsing - coin.it



Liberal parsing - shellscripts

ubuntu-webpagesourcecheck.sh
vtigercron.sh
mysqlthreads.sh
restart_httpd_new.sh
smtp-ipset-wl.sh

Cronjobs visualized - update.sh



Liberal parsing - config files

mysql-virtual_client.cf

updates_spamassassin_org.cf

database_virtual_mailbox_domains.cf

database_virtual_mailbox_maps.cf

More WAT (1)

_.to

_.com.br

org

net

More WAT (2)

obheyun8_vejlglxy6

dlb5o4fqz_q05ermqx8mfccgh8

uphgpipnyc7qxt_ludqhtlbh8mzb79n

hwuo87aaus_pnpdjqvryekhzg

8vmx_w03dvy5eaxmj1yfmpp

Closing up thoughts

Public sources attract all sorts of data - wanted and unwanted (but possibly interesting).

Can you predict the shape of the graph? Before it happens?

Thank you!

carel@spamhaus.org

www.spamhaus.org