Four Years of Breaking HTTPS with BGP Hijacking

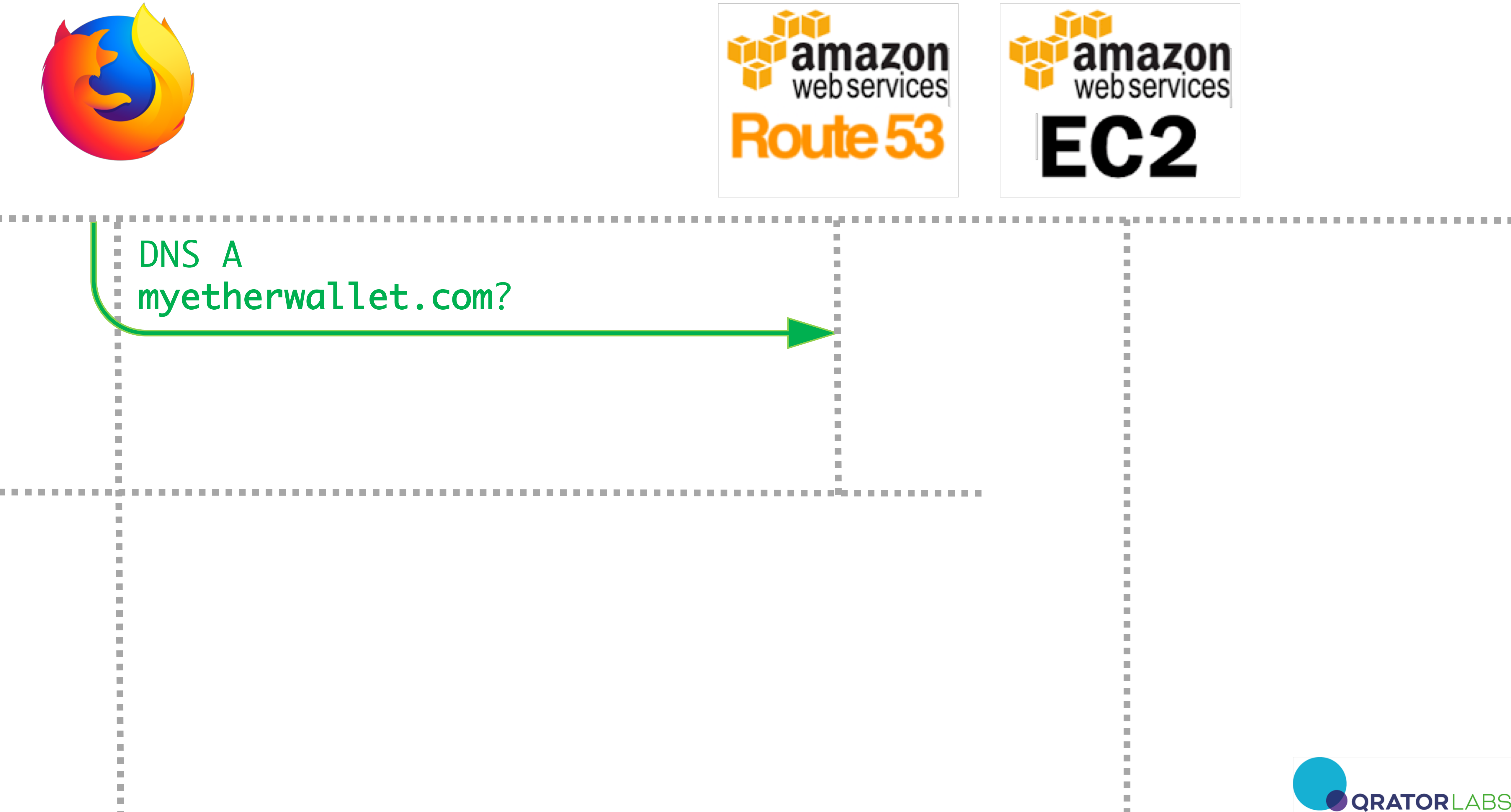
Töma Gavrichenkov <ag@qrator.net>
GPG: 2deb 97b1 0a3c 151d b67f
1ee5 00e7 94bc 4d08 9191

QRATOR LABS

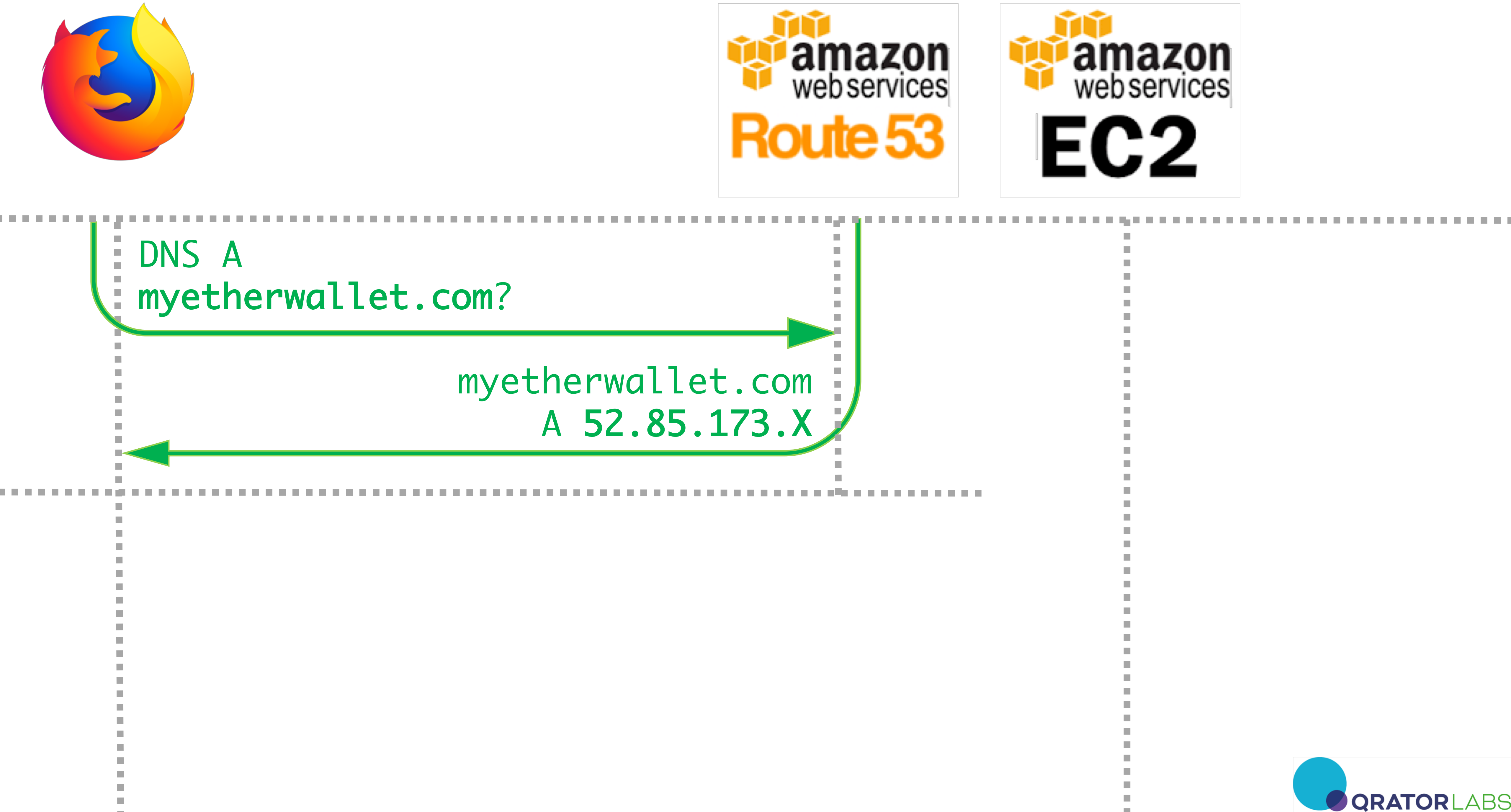
MyEtherWallet

April 24, 2018: myetherwallet.com gets BGP hijacked

- Went for 2 hours unnoticed
- Was using rogue HTTPS certificate
  so users clicked through certificate errors
- https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/

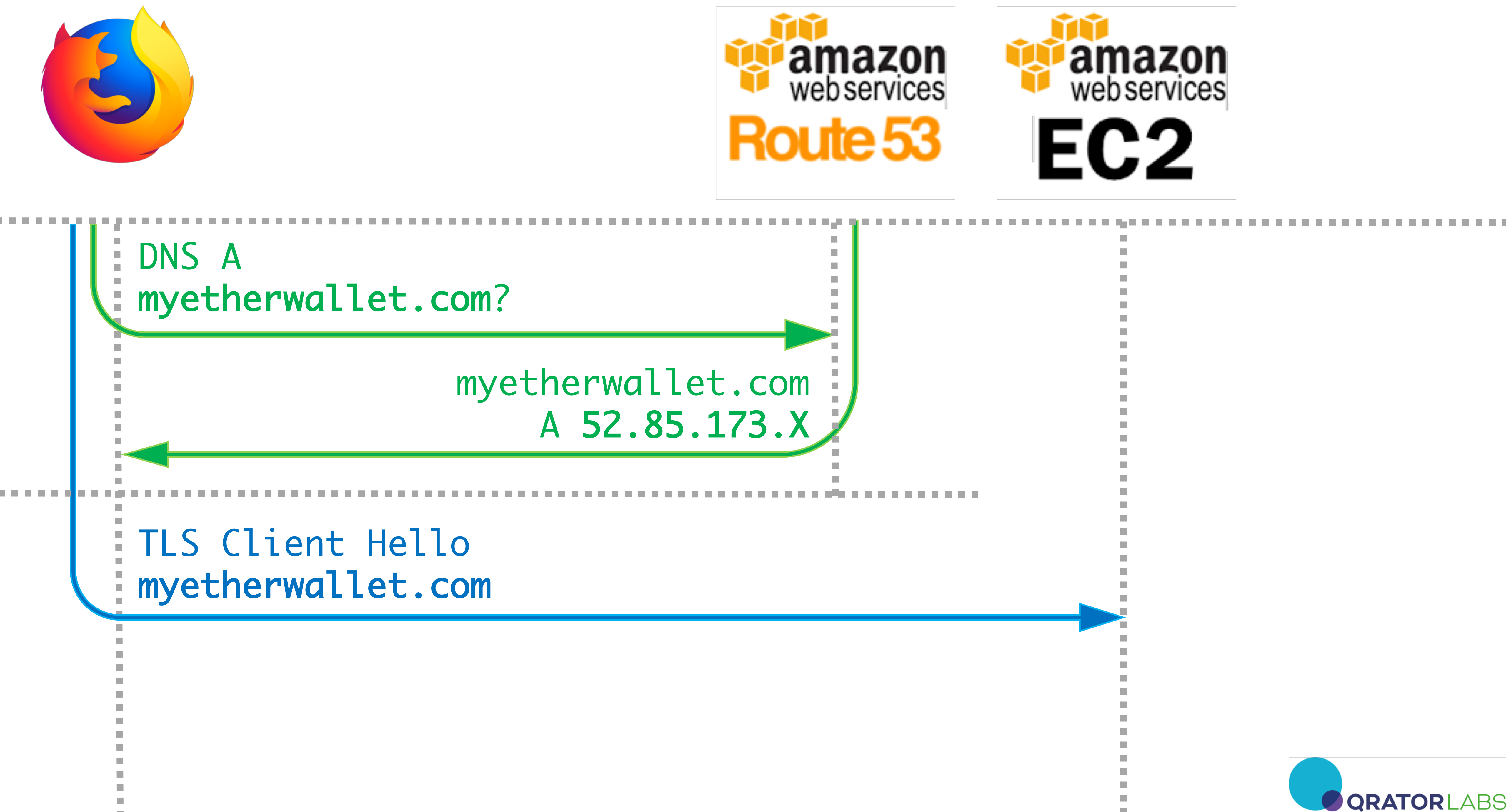


DNS A
myetherwallet.com?



DNS A
myetherwallet.com?

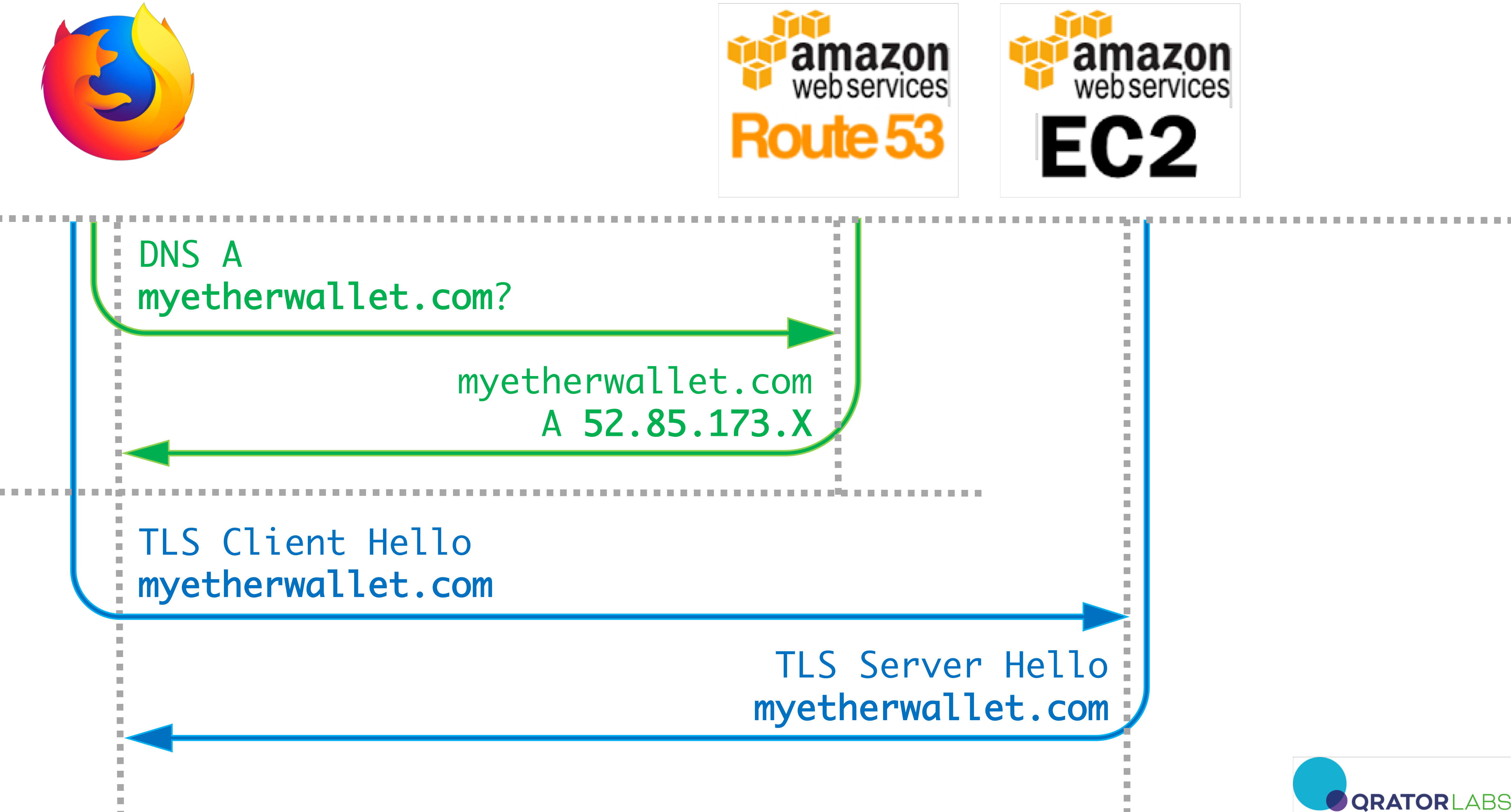
myetherwallet.com
A 52.85.173.X



DNS A
myetherwallet.com?

myetherwallet.com
A 52.85.173.X

TLS Client Hello
myetherwallet.com

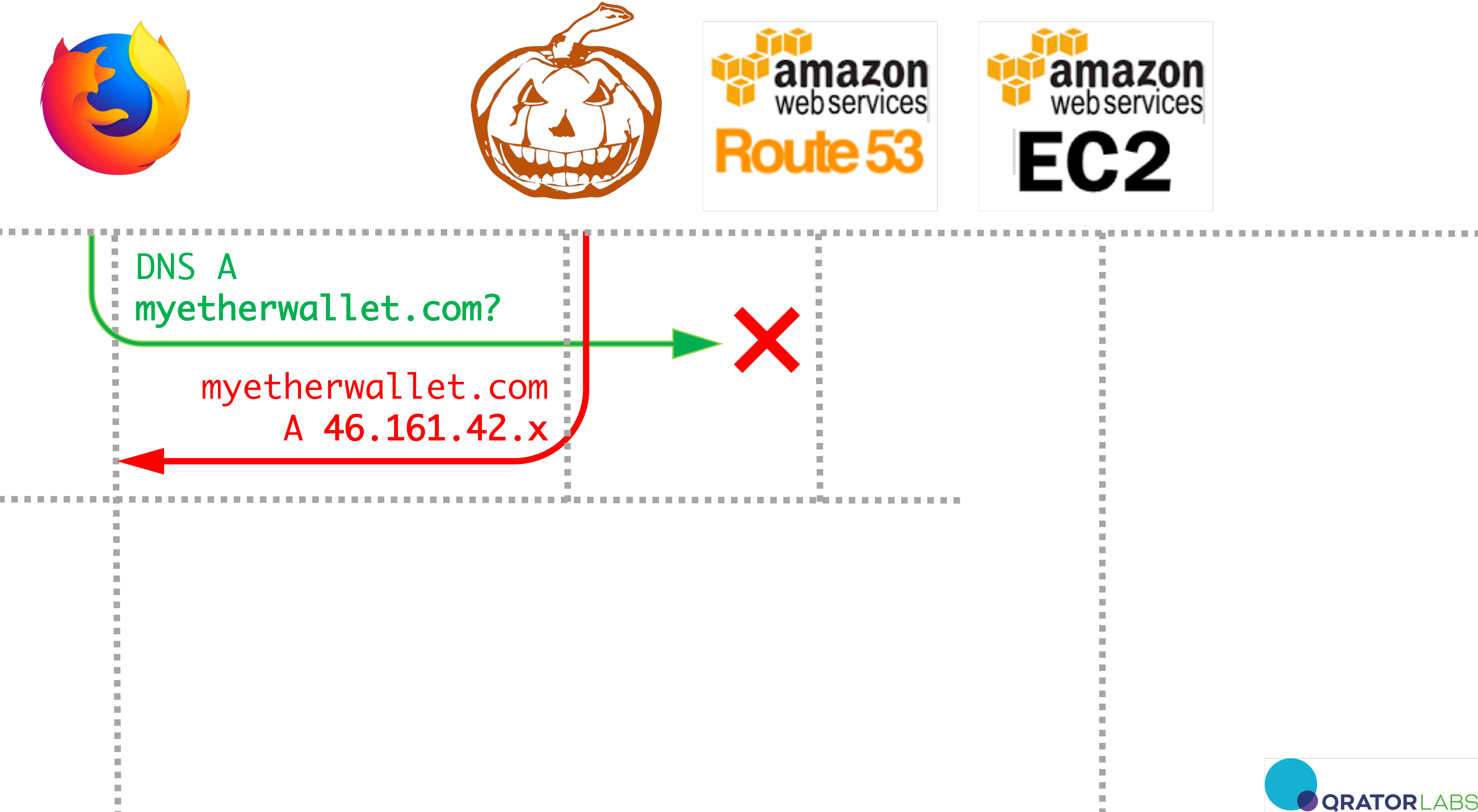


DNS A
myetherwallet.com?

myetherwallet.com
A 52.85.173.X

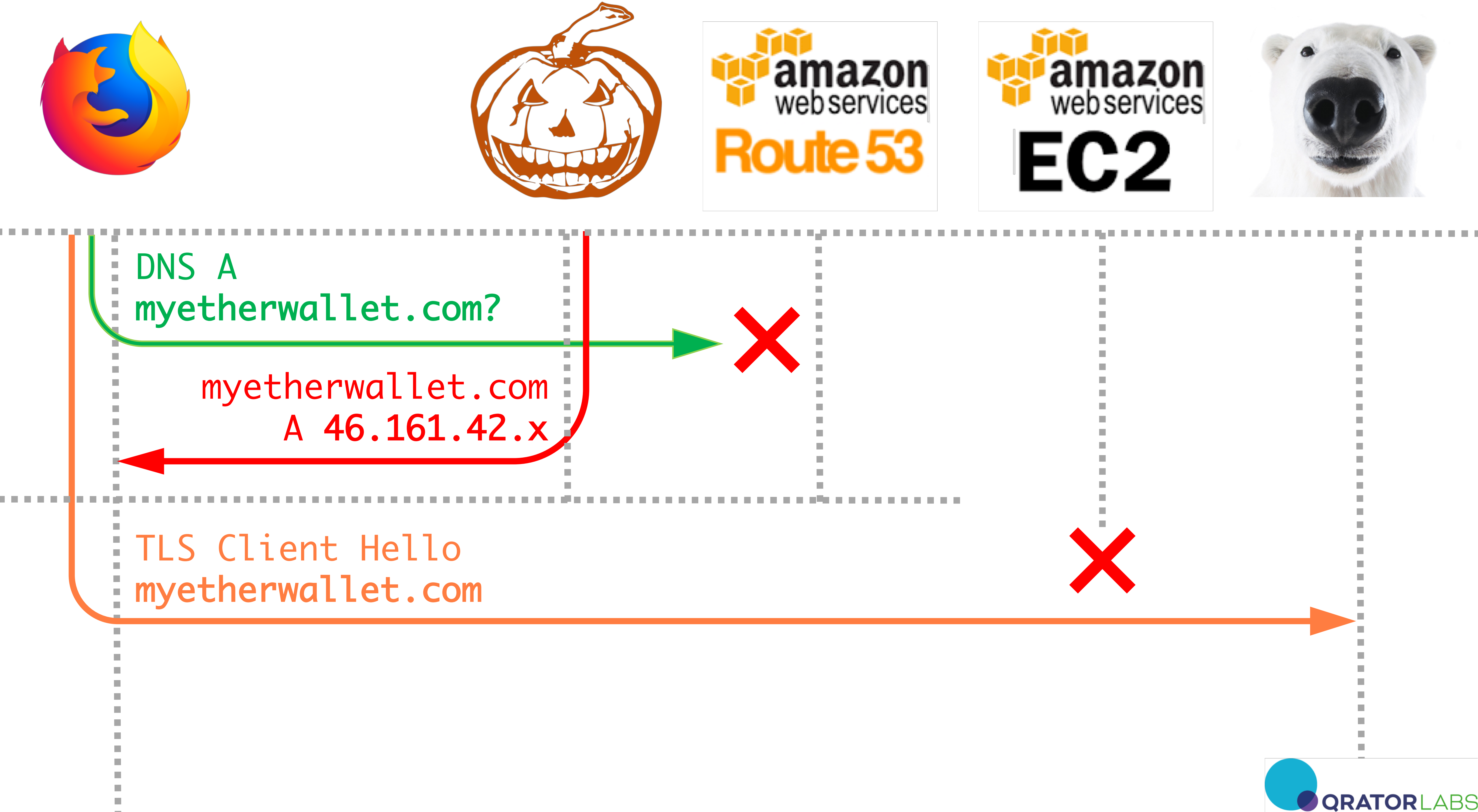
TLS Client Hello
myetherwallet.com

TLS Server Hello
myetherwallet.com



DNS A
myetherwallet.com?

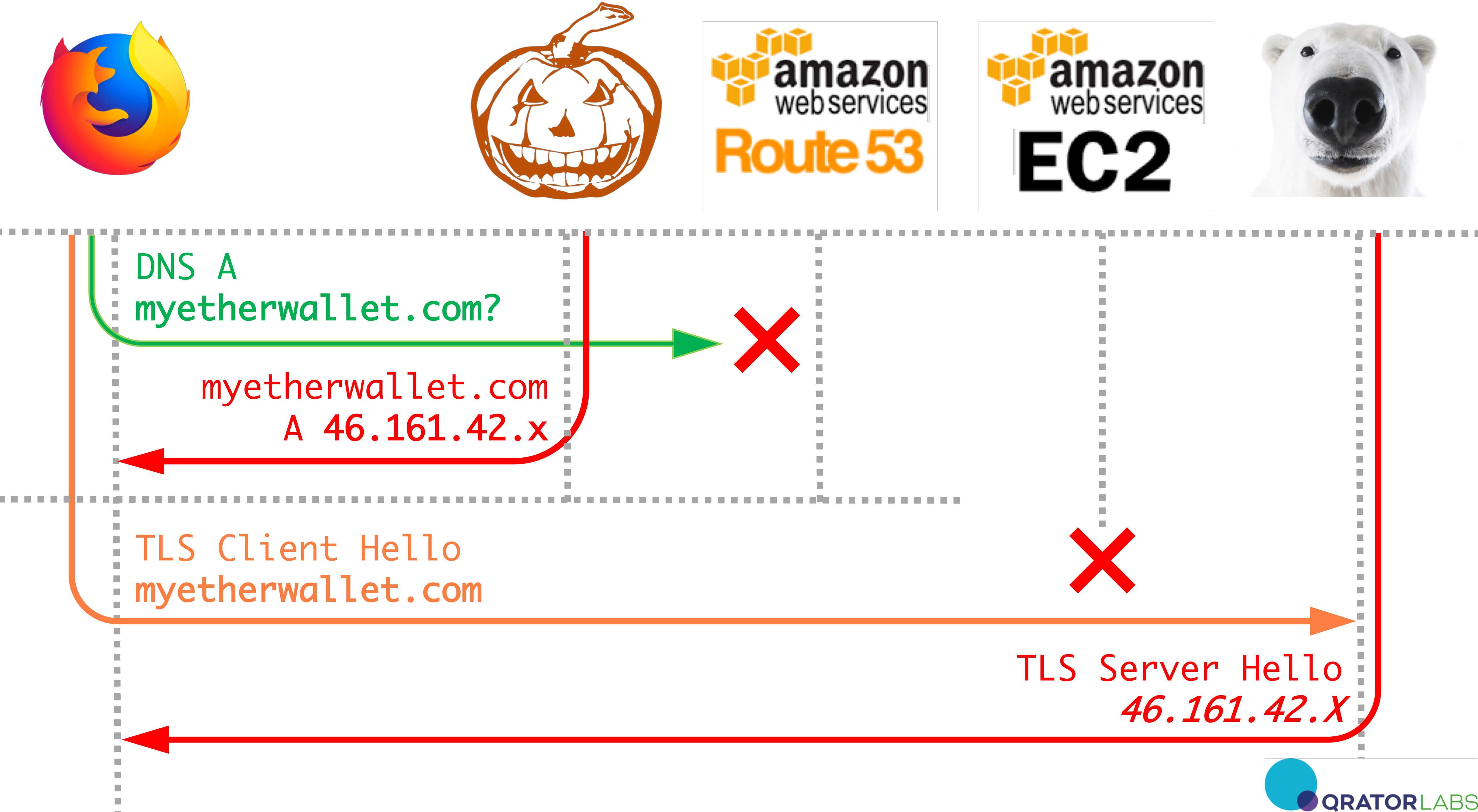
myetherwallet.com
A 46.161.42.x



DNS A
myetherwallet.com?

myetherwallet.com
A 46.161.42.x

TLS Client Hello
myetherwallet.com



DNS A
myetherwallet.com?

myetherwallet.com
A 46.161.42.x

TLS Client Hello
myetherwallet.com

TLS Server Hello
46.161.42.X

MyEtherWallet

- **The attacker was using a self-signed TLS certificate**
- It’s not that easy to get through HTTPS certificate errors with a contemporary browser

- Yet, some users still ignored the warnings
- **Which made some of the experts blame the users**
- ”We should make HTTPS warnings harder to click through”

MyEtherWallet

”We should make HTTPS warnings harder to click through”

— Whoops. **Nope.** It wouldn’t help here — because of BGP.

“Breaking HTTPS with BGP hijacking”

http://www.blackhat.com/us-15/briefings.html#breaking-https-with-bgp-hijacking

- TL;DR: companies issuing certificates are using the same techniques to verify the remote side
- Hence after BGP hijacking an attacker can obtain a valid HTTPS certificate for the target site

“Breaking HTTPS with BGP hijacking”

http://www.blackhat.com/us-15/briefings.html#breaking-https-with-bgp-hijacking

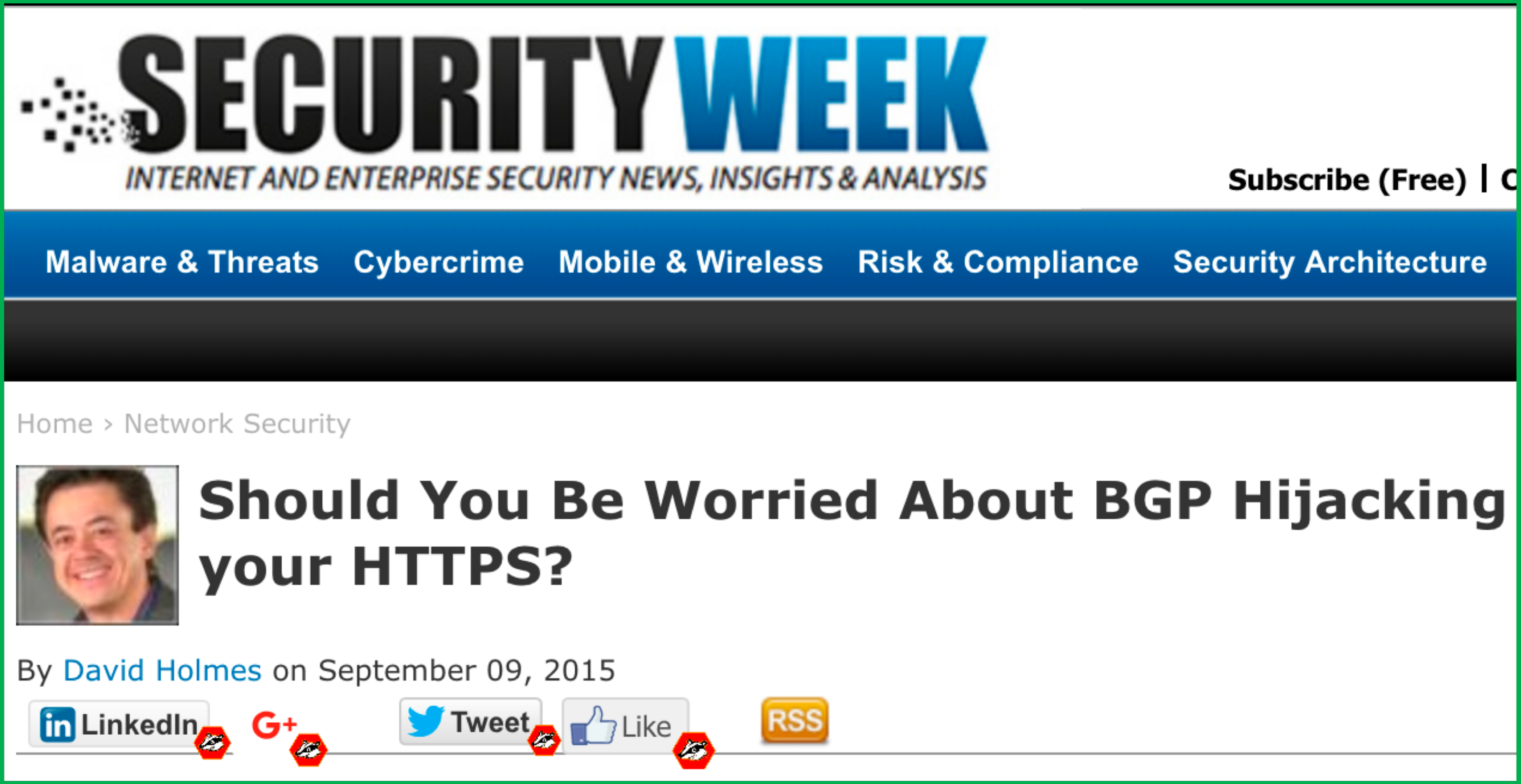
- 2 basic types:
  - Global Hijacking
  - Local Hijacking
- With both types, it’s possible to feed a CA’s verifying script with false data:
  - HTTP
  - DNS
  - WHOIS

“Breaking HTTPS with BGP hijacking”

http://www.blackhat.com/us-15/briefings.html#breaking-https-with-bgp-hijacking

- 2 basic types:
  - Global Hijacking
  - Local Hijacking
- With both types, it’s possible to feed a CA’s verifying script with false data, **which in turn would lead to a valid certificate issued and sent to an attacker**
- After that, (nearly) impossible to reliably investigate the incident

An immediate feedback from PKIX industry experts:



Should You Be Worried About BGP Hijacking your HTTPS?

By David Holmes on September 09, 2015

A feedback from PKIX industry experts:

- No reports of the attack happening in the wild
- Extended Validation addresses the issue
- RFC 7469 “HTTP Public Key Pinning” sees more and more adoption
- Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus

Ergo: **not something to really worry about**

https://www.securityweek.com/should-you-be-worried-about-bgp-hijacking-your-https

1. *“No reports of the attack happening in the wild”*
2. *“Extended Validation addresses the issue”*
3. *“RFC 7469 “HTTP Public Key Pinning” sees more and more adoption”*
4. *“Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus”*

It’s now almost 4 years ago.

How did that go?

1. *“No reports of the attack happening in the wild”*

> *“That’s a conference type attack. Those won’t happen in practice.”*
>
> — Someone in a private conversation

1. *“No reports of the attack happening in the wild”*

> *“That’s a conference type attack. Those won’t happen in practice.”*
>
> — Someone in a private conversation

Yet it turns out they do.

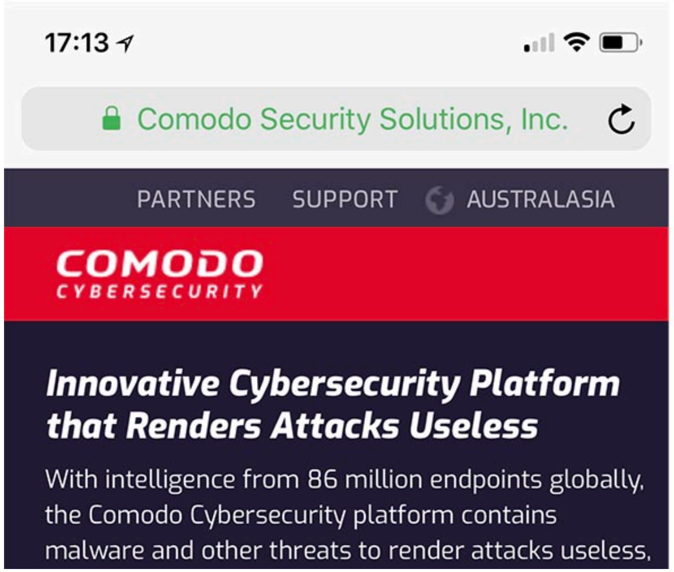
- You only need a cryptocurrency exchange large enough — or a **motivated attacker**
- MyEtherWallet attackers could’ve done that **easily**
  - Probably they don’t attend conferences
- Actually, **2 other** (suspected) cases were reported directly to the authors during 2018

2. *“Extended Validation addresses the issue”*

Except it’s dead.

- Not shown on mobile devices
- Web sites ditching EV
- No way to automate

iOS 11



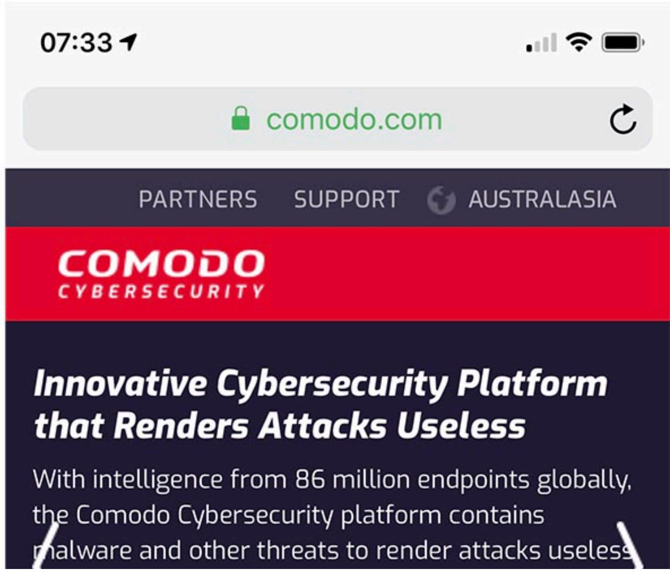
17:13

Comodo Security Solutions, Inc.

Innovative Cybersecurity Platform that Renders Attacks Useless

With intelligence from 86 million endpoints globally, the Comodo Cybersecurity platform contains malware and other threats to render attacks useless.

iOS 12



07:33

comodo.com

Innovative Cybersecurity Platform that Renders Attacks Useless

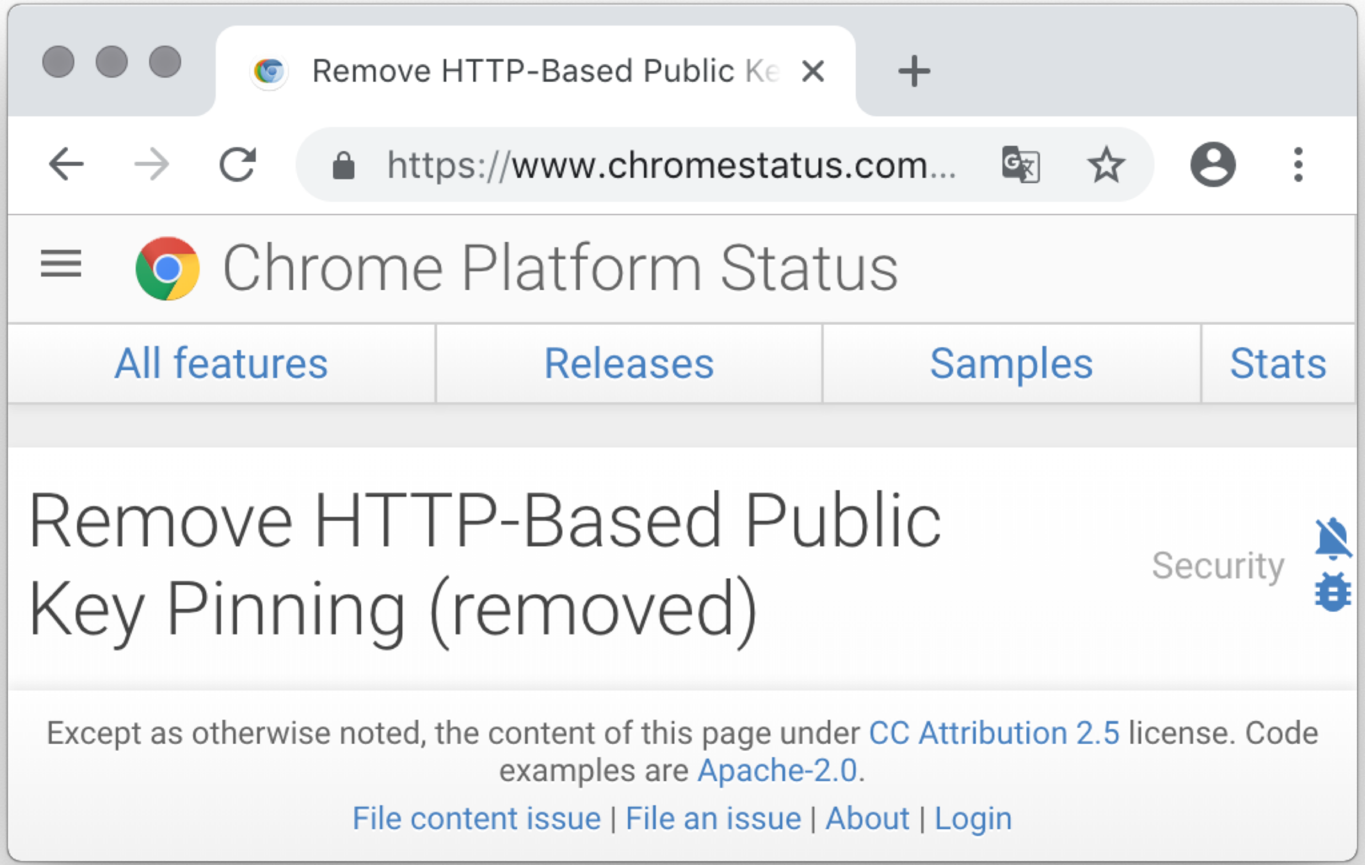
With intelligence from 86 million endpoints globally, the Comodo Cybersecurity platform contains malware and other threats to render attacks useless

https://www.troyhunt.com/extended-validation-certificates-are-dead/

3. “RFC 7469 “HTTP Public Key Pinning” sees more and more adoption”

Except it’s dead, either.

- Hard to automate
- Got low adoption
- Risks of hostile pinning



Remove HTTP-Based Public Key Pinning (removed)

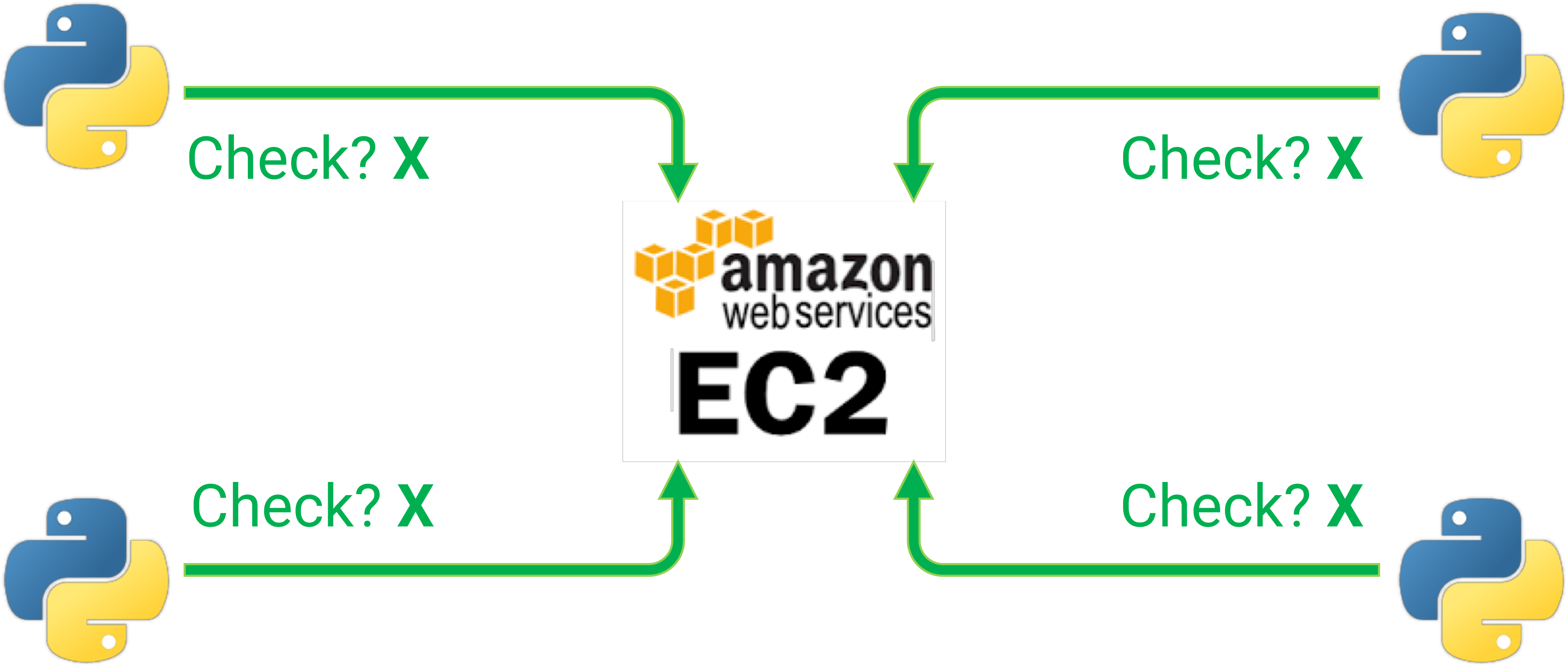
Except as otherwise noted, the content of this page under CC Attribution 2.5 license. Code examples are Apache-2.0.

File content issue | File an issue | About | Login

https://www.chromestatus.com/feature/5903385005916160

4. *“Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus”*

4. *“Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus”*



Check? **X**

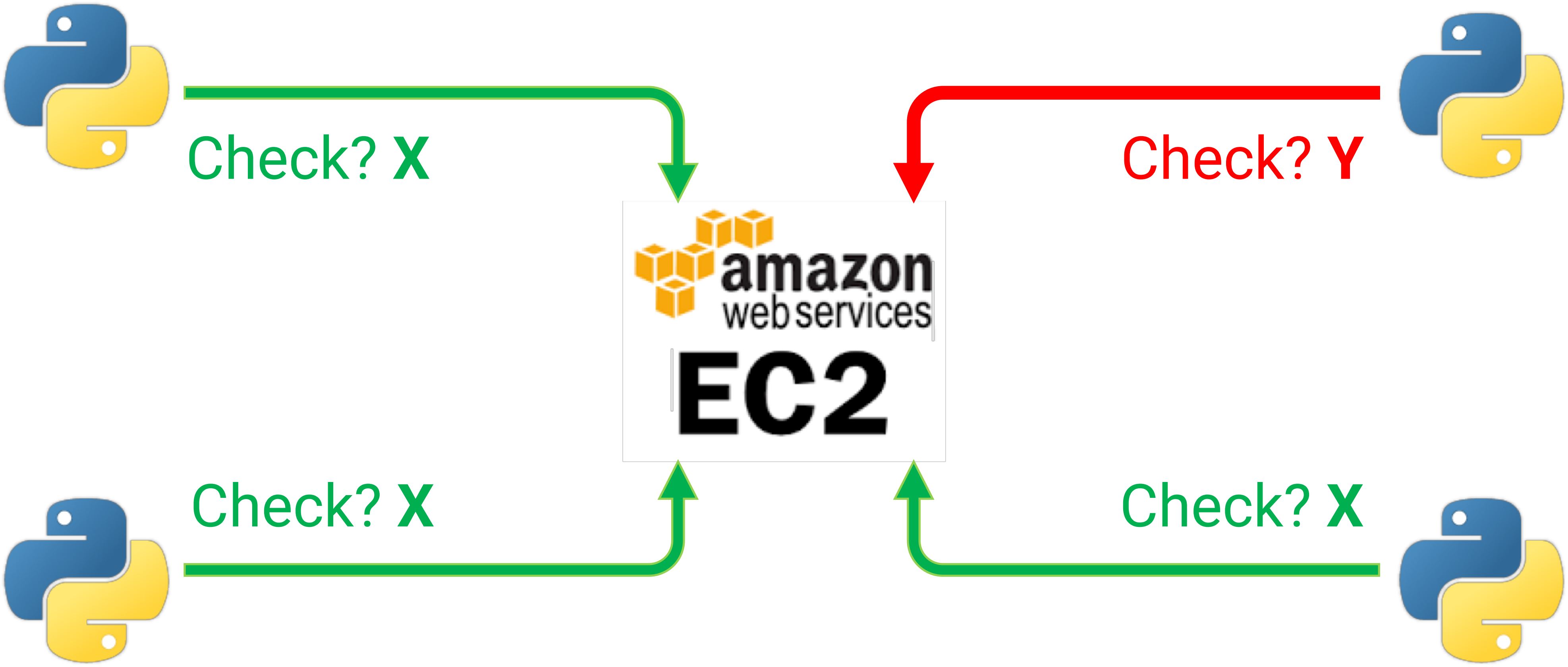
Check? **X**

Check? **X**

Check? **X**

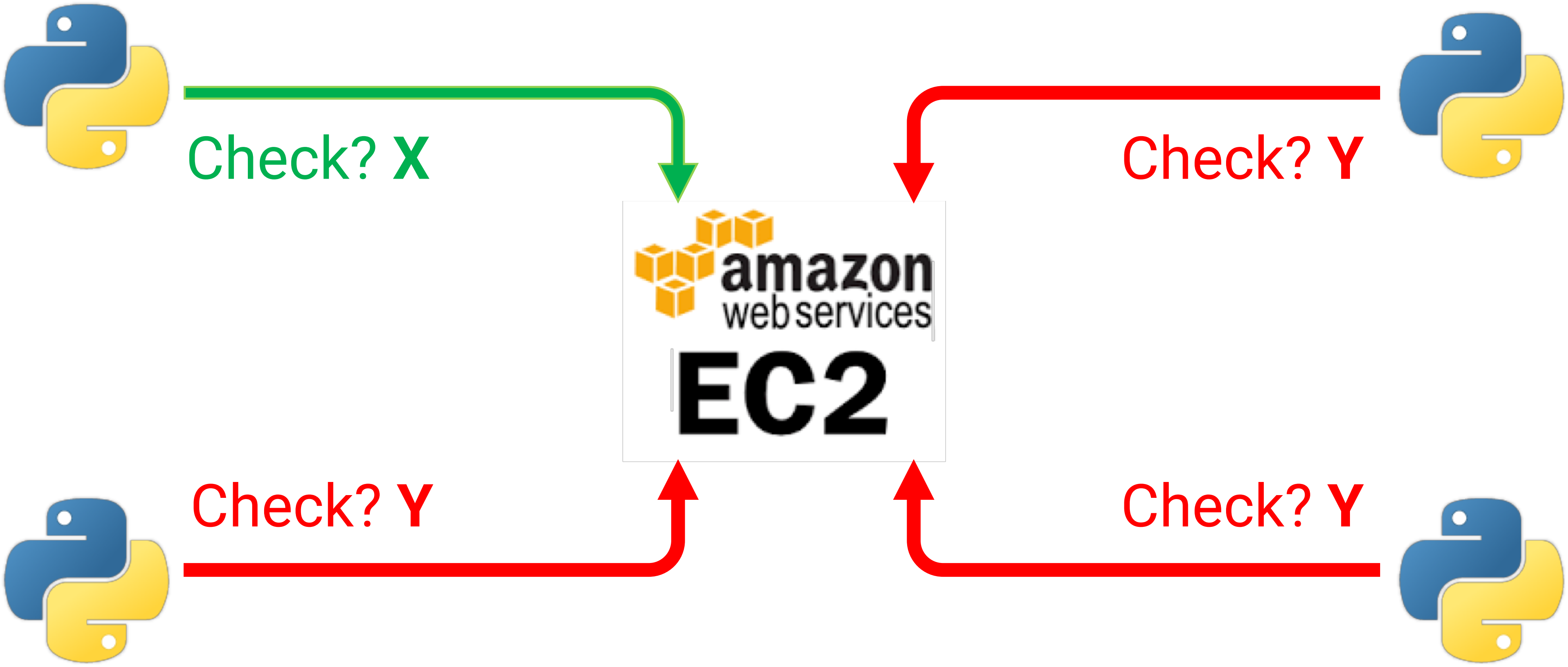
= O.K.!

4. “Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus”



= O.K.!

4. *“Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus”*



Check? **X**

Check? **Y**

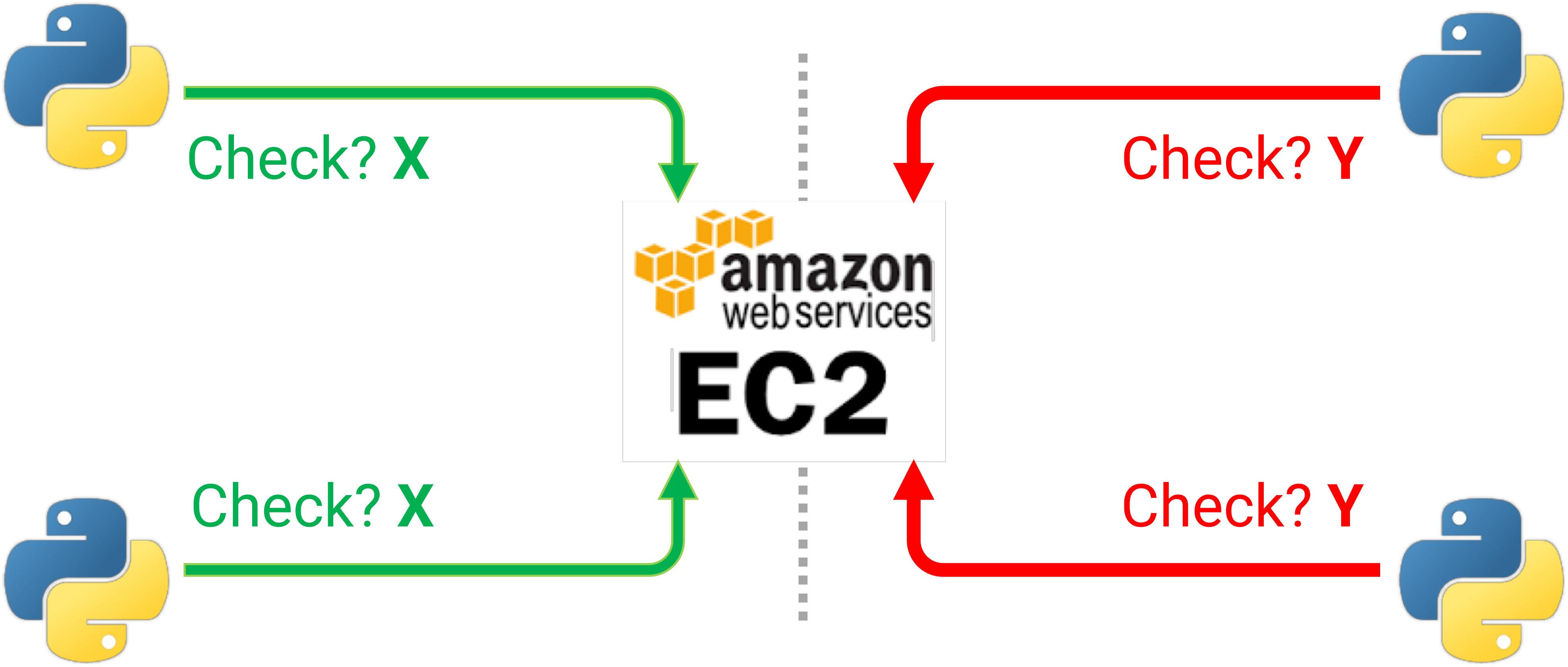
amazon web services EC2

Check? **Y**

Check? **Y**

= O.K.!

4. *“Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus”*



= FAIL (the only case)

4. “Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus”

- …yes, the *“majority”* part is just broken, but, nevertheless, we’ve got the idea.
  So what?

- It turns out someone finally got interested with the issue
  (before the malicious ones did).

Guess who cared?

4. “Conscientious CA uses multiple clients to do validation and only issues if the majority reports consensus”

- …yes, the *“majority”* part is just broken, but, nevertheless, we’ve got the idea.
  So what?

- It turns out someone finally got interested with the issue (before the malicious ones did).

Guess who cared?

Scientists.

“Using BGP to Acquire Bogus TLS Certificates”

https://www.petsymposium.org/2017/papers/hotpets/bgp-bogus-tls.pdf

Jennifer Rexford et al., **Princeton University, 2017**

“Using BGP to Acquire Bogus TLS Certificates”

https://www.petsymposium.org/2017/papers/hotpets/bgp-bogus-tls.pdf
Jennifer Rexford et al., **Princeton University, 2017**

- Confirmed the observations
- Got real certificates issued by:
  - **Symantec**
  - **Comodo**
  - **Let’s Encrypt**
  - **GoDaddy**

“Bamboozling Certificate Authorities with BGP”

http://www.cs.princeton.edu/~jrex/papers/bamboozle18.pdf

Jennifer Rexford et al., **Princeton University, 2018**

“Bamboozling Certificate Authorities with BGP”

http://www.cs.princeton.edu/~jrex/papers/bamboozle18.pdf

Jennifer Rexford et al., **Princeton University, 2018**

- Topic development: **5** different cases
  - ”Global Hijacking” -> **Traditional sub-prefix attack**
  - “Local Hijacking” -> Traditional **equally-specific-prefix** attack
  - **Prepended** sub-prefix attack
  - Prepended equally-specific-prefix attack
  - **AS-path poisoning attack**

Further Research

- *“Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates”*, Borgolte et al., UC Santa Barbara
  http://www.utdallas.edu/~shao/papers/borgolte_ndss18.pdf

- *“RiPKI: The tragic story of RPKI deployment in the Web ecosystem”*, Wählisch et al., FU Berlin
  http://conferences.sigcomm.org/hotnets/2015/papers/wahlisch.pdf

- *“Secure Entity Authentication”*, Dou, Zuochao, New Jersey Institute of Technology

- etc. (Google Scholar keeps pinging me from time to time)

So what did CAs do?

- Certificate transparency

- DNS Certificate Authority Authorization RR: RFC 6844

So what did CAs do?

- Certificate transparency
  - Leaves an attack window before the issuance and first OCSP actions: the MyEtherWallet attack, for instance, lasted only for 2 hours

- DNS Certificate Authority Authorization RR: RFC 6844
  - Doesn’t prevent the case of a fraudulent issuance by the same CA
  - Doesn’t cover hijacking of the DNS server itself

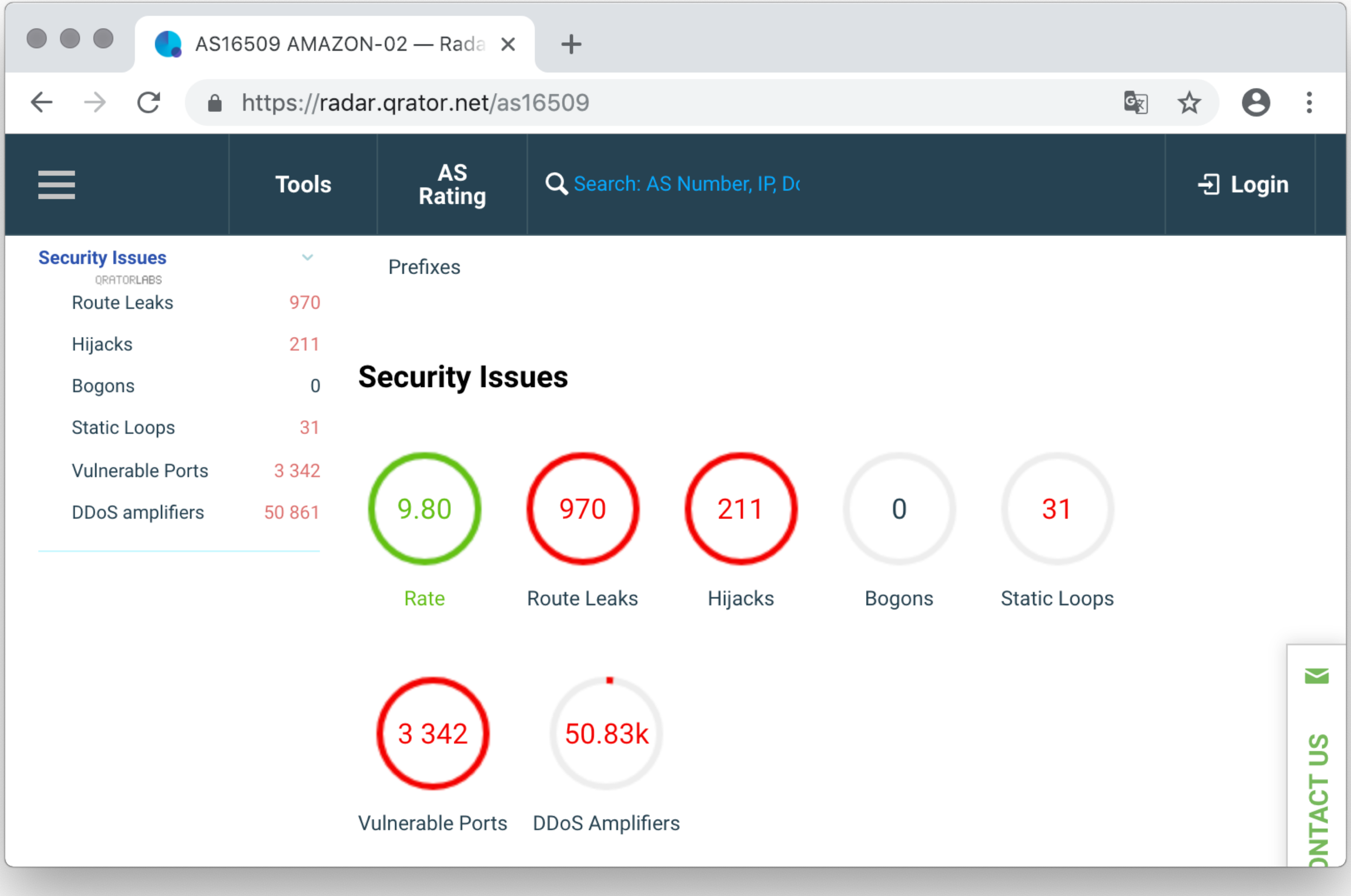
By the way

Why did the folks attacking MyEtherWallet hijack the **whole Amazon DNS** instead of just the MyEtherWallet Web server?

Why to hijack DNS instead of HTTP?

Well, we don’t know **for sure** (maybe they were just drunk),
but we have a clue.

- An average authoritative DNS server gets roughly 0,1% of traffic the corresponding Web server does.
  <Do I need to explain?>
- Hijacking DNS allows us to forward precisely the HTTP traffic we want and not to see the rest of HTTP going through the network
- So it’s **more cost-effective** this way!
- That makes DNS the most likely target for future BGP attacks



Security Issues

QRATORLABS

Route Leaks	970
Hijacks	211
Bogons	0
Static Loops	31
Vulnerable Ports	3 342
DDoS amplifiers	50 861

Prefixes

Security Issues

9.80	970	211	0	31
Rate	Route Leaks	Hijacks	Bogons	Static Loops

3 342	50.83k
Vulnerable Ports	DDoS Amplifiers

What has been done by ICANN and the DNS community?

- Nothing, because everything (i.e. DNSSEC) is already there!
- **Low adoption**, however

What has been done by the ISP community?

- ROA
- BGPSec

What has been done by the ISP community?

- ROA: validates only the source, doesn’t cover AS Path
- BGPSec

What has been done by the ISP community?

- ROA: validates only the source, doesn’t cover AS Path

- BGPSec, guess what,

What has been done by the ISP community?

- ROA: validates only the source, doesn’t cover AS Path

- BGPSec, guess what, **low adoption so far**

What has been done by the ISP community?

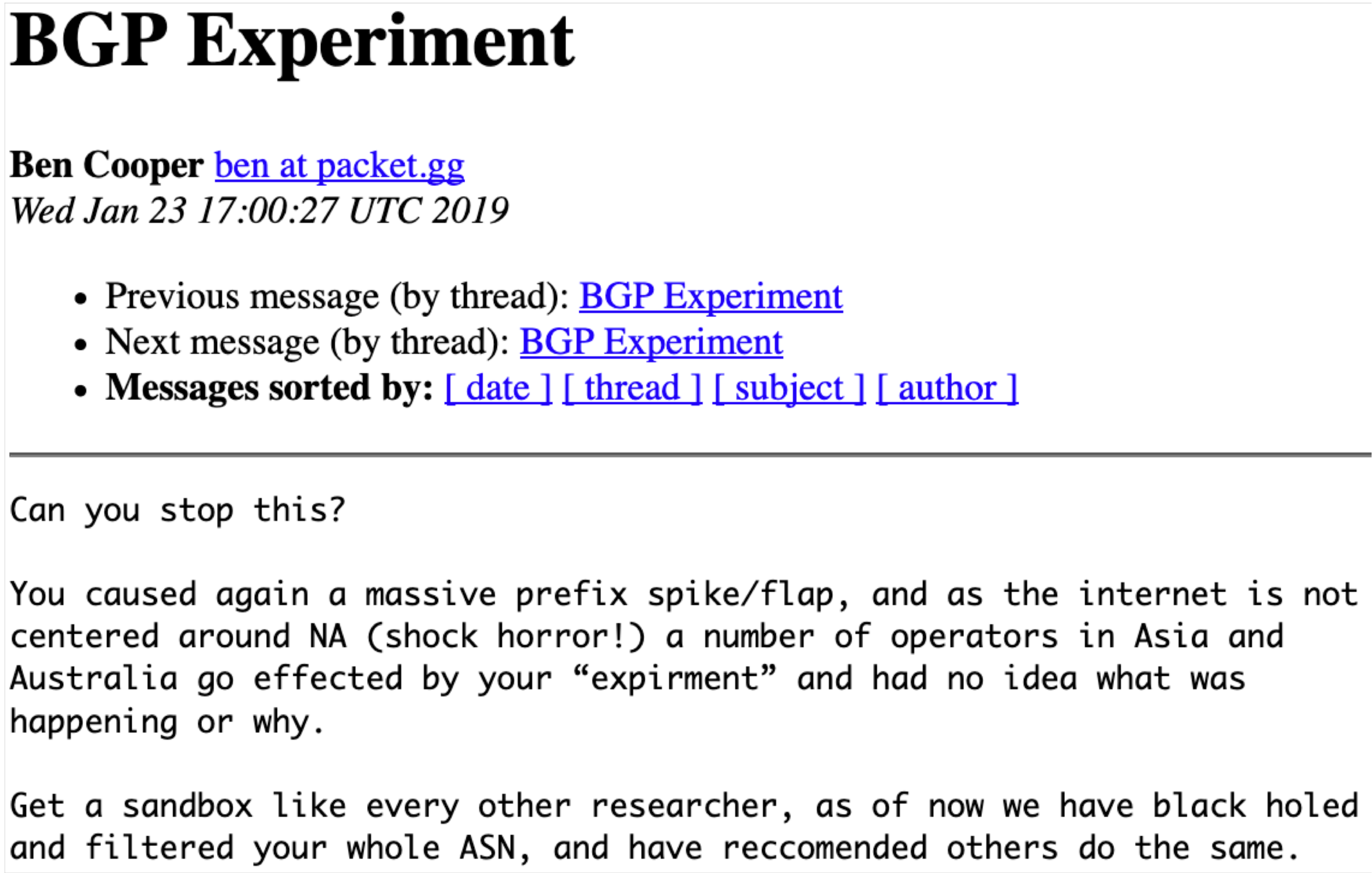
- ROA: validates only the source, doesn’t cover AS Path
- BGPSec, guess what, **low adoption so far**
- ASPA
  - **https://tools.ietf.org/html/draft-azimov-sidrops-aspa-verification**
  - **?**
  - Please ~~donate~~ pay attention

QRATORLABS

What has been done by the ISP community?

It turns out we cannot even test new approaches in the wild!

- Broken BGP software
- Obsolete BGP s/w
- Months or years between s/w updates



BGP Experiment

Ben Cooper ben at packet.gg
Wed Jan 23 17:00:27 UTC 2019

- Previous message (by thread): BGP Experiment
- Next message (by thread): BGP Experiment
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Can you stop this?

You caused again a massive prefix spike/flap, and as the internet is not
centered around NA (shock horror!) a number of operators in Asia and
Australia go effected by your “expirment” and had no idea what was
happening or why.

Get a sandbox like every other researcher, as of now we have black holed
and filtered your whole ASN, and have reccomended others do the same.
```

Bottom line.

- I’m being frequently criticized for delivering pessimistic talks.

Bottom line.

- I’m being frequently criticized for delivering pessimistic talks.

Okay, it’s 4 years after,
and we aren’t even close to a solution.
Let’s be optimistic about it!

Bottom line.

- I'm being frequently criticized for delivering pessimistic talks.

Okay, it's 4 years after,
and we aren't even close to a solution.
Let's be optimistic about it!

Or, maybe, it's time to stop feeding the users with soothing words that don't really change anything in the end.

Bottom line.

- I’m being frequently criticized for delivering pessimistic talks.
- I’m also (sometimes) being criticized for just speaking of problems, not offering a solution.

Bottom line.

- I’m being frequently criticized for delivering pessimistic talks.
- I’m also (sometimes) being criticized for just speaking of problems, not offering a solution.

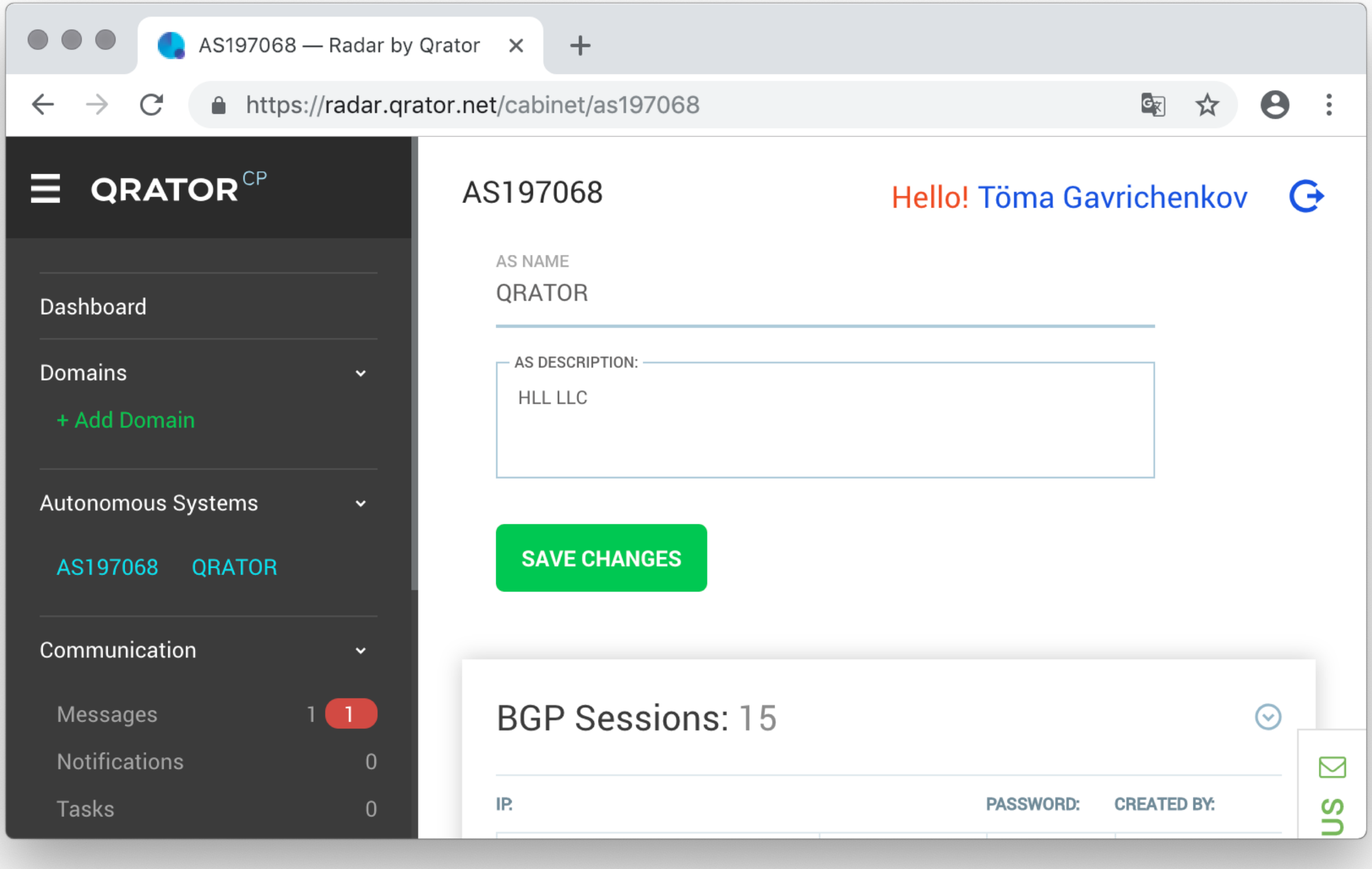
But some solutions are already there!

- We ditched HPKP, EV
  (okay, the last one was predictable)
- We don’t adopt DNSSEC/BGPSec

Adopt a multihop BGP session!

It’s cool and free!

https://radar.qrator.net/



AS197068

AS197068 QRATOR

AS NAME

QRATOR

AS DESCRIPTION:

HLL LLC

BGP Sessions: 15

IP:	PASSWORD:	CREATED BY:

Bottom line.

- I’m being frequently criticized for delivering pessimistic talks.
- I’m also (sometimes) being criticized for just speaking of problems, not offering a solution.
- The combined technical debt in the Internet doesn’t appear to shrink, it only grows further.
  It only takes some time to contribute into paying off that debt,
  so **why not to start now?**

Bottom line.

- I’m being frequently criticized for delivering pessimistic talks.
- I’m also (sometimes) being criticized for just speaking of problems, not offering a solution.
- The combined technical debt in the Internet doesn’t appear to shrink, it only grows further.
  It only takes some time to contribute into paying off that debt, so **why not to start now?**

Please.

Q&A

mailto:

Töma Gavrichenkov <ag@qrator.net>