

Exercise Session VIII: BGPsec, DoS

Network Security

Matteo Scarlata

November 12th, 2020

ETH Zurich

Context: BGP

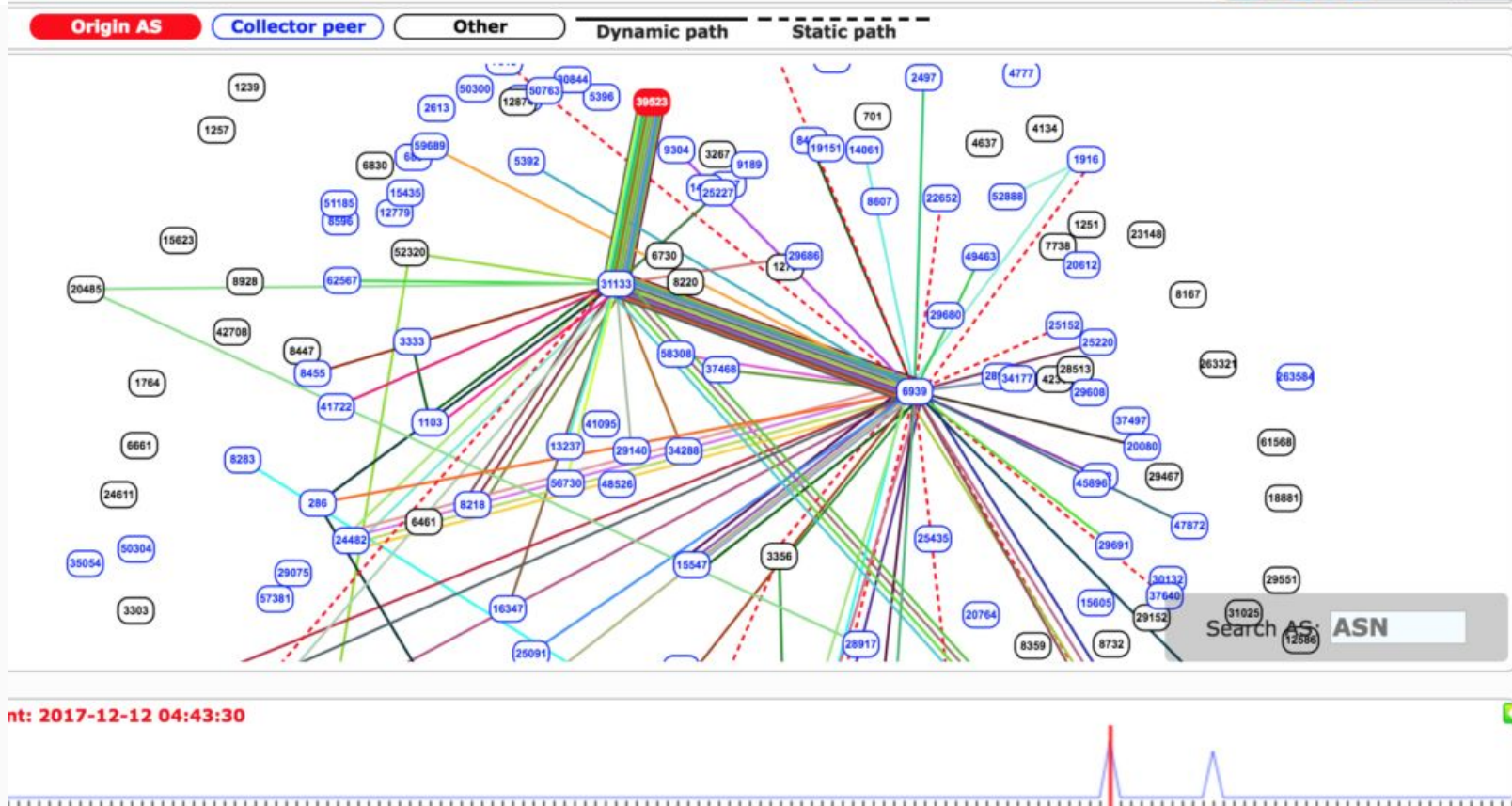
BGP Hijacking: attacks



HOME BLOG ABOUT US PRODUCTS AND SERVICES CLIENT PORTAL

Popular Destinations rerouted to Russia

Posted by Andree Toonk - December 12, 2017 - [Hijack](#) - No Comments

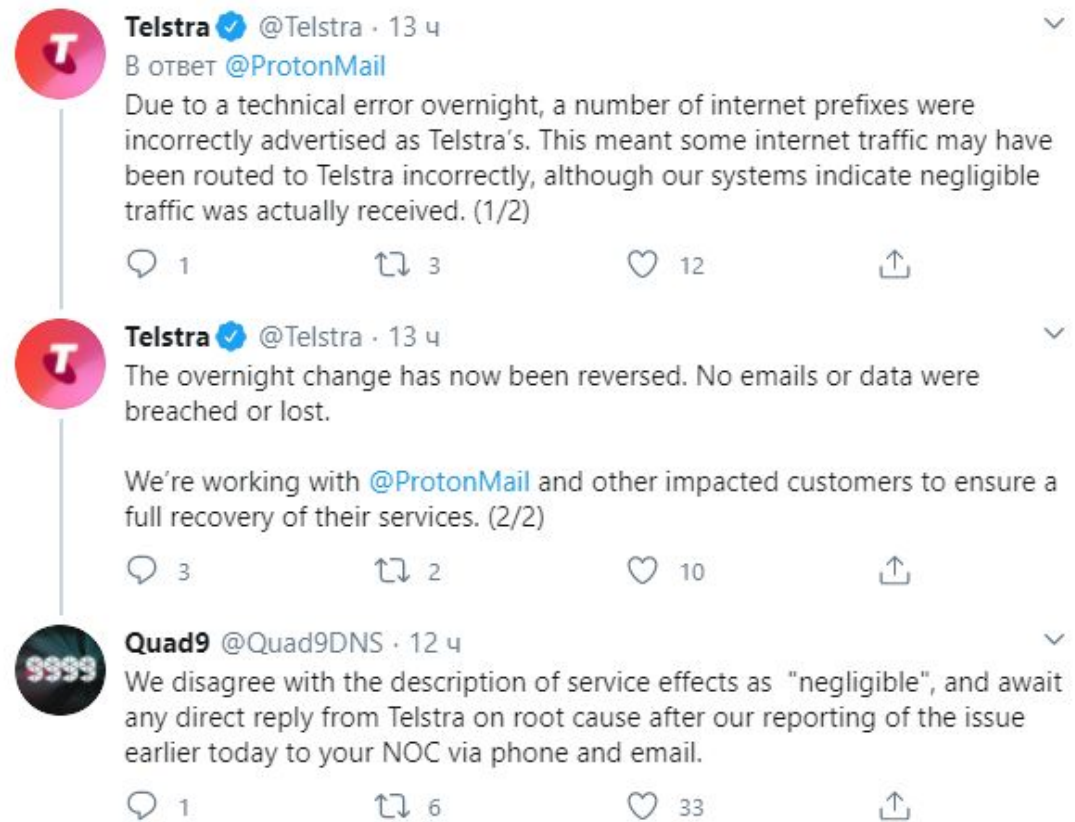


BGP Hijacking: mistakes?


📅 September 30th, 2020


AS1221 hijacking 266 ASNs in 51 countries


On Tuesday, September 29, 2020 AS1221 - Telstra announced 472 prefixes in a BGP hijack event that affected 266 other ASNs in 50 countries, with the most damage rendered



The screenshot shows a Twitter thread with three tweets. The first two are from Telstra (@Telstra), and the third is from Quad9 (@Quad9DNS). The tweets discuss a BGP hijacking event where Telstra incorrectly advertised internet prefixes, affecting 266 other ASNs in 50 countries. Telstra states that the change has been reversed and that no emails or data were breached or lost. Quad9 disagrees with the description of the service effects as "negligible" and awaits a direct reply from Telstra on the root cause.

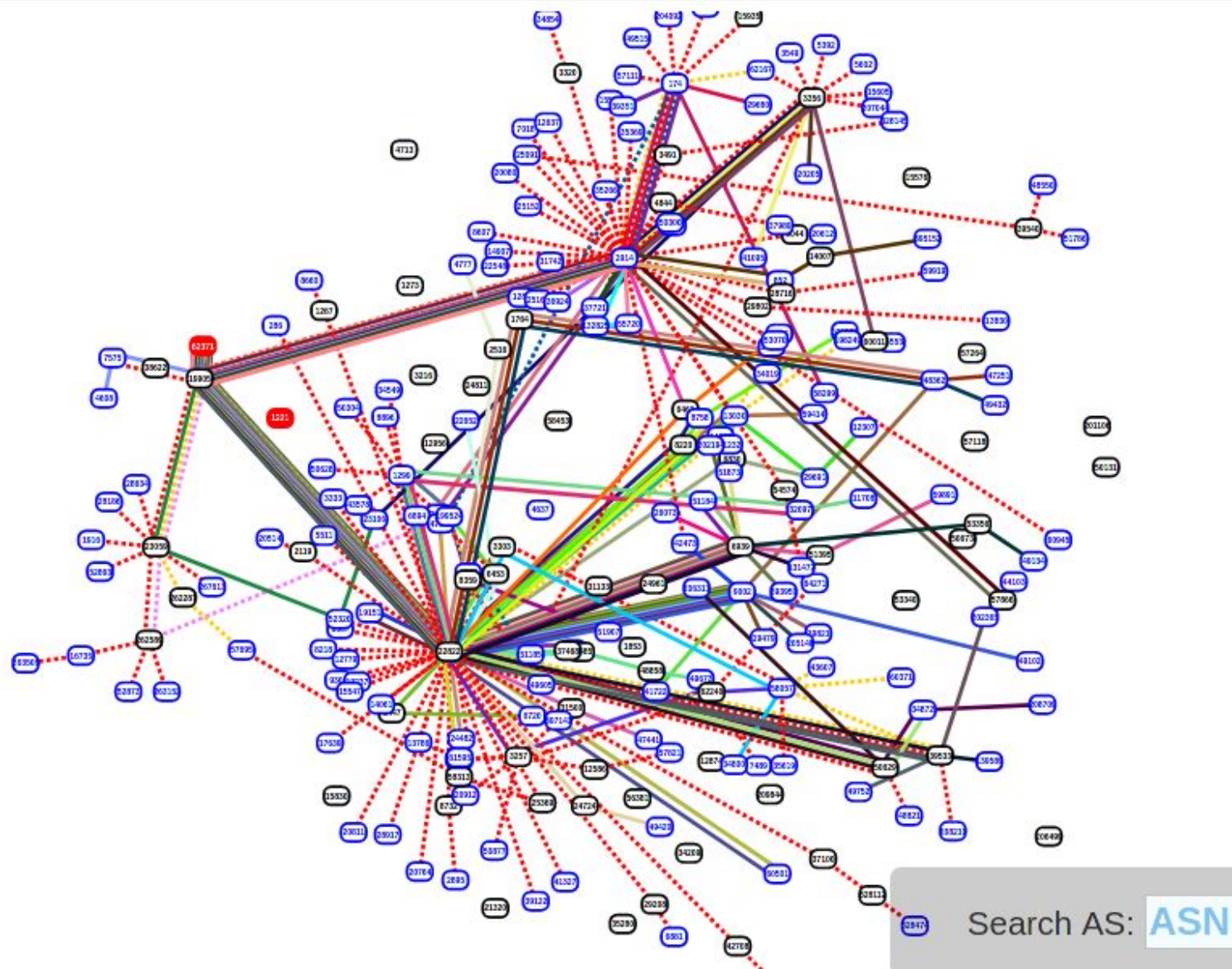
Telstra  @Telstra · 13 4
В ответ [@ProtonMail](#)
Due to a technical error overnight, a number of internet prefixes were incorrectly advertised as Telstra's. This meant some internet traffic may have been routed to Telstra incorrectly, although our systems indicate negligible traffic was actually received. (1/2)
1 3 12

Telstra  @Telstra · 13 4
The overnight change has now been reversed. No emails or data were breached or lost.
We're working with [@ProtonMail](#) and other impacted customers to ensure a full recovery of their services. (2/2)
3 2 10

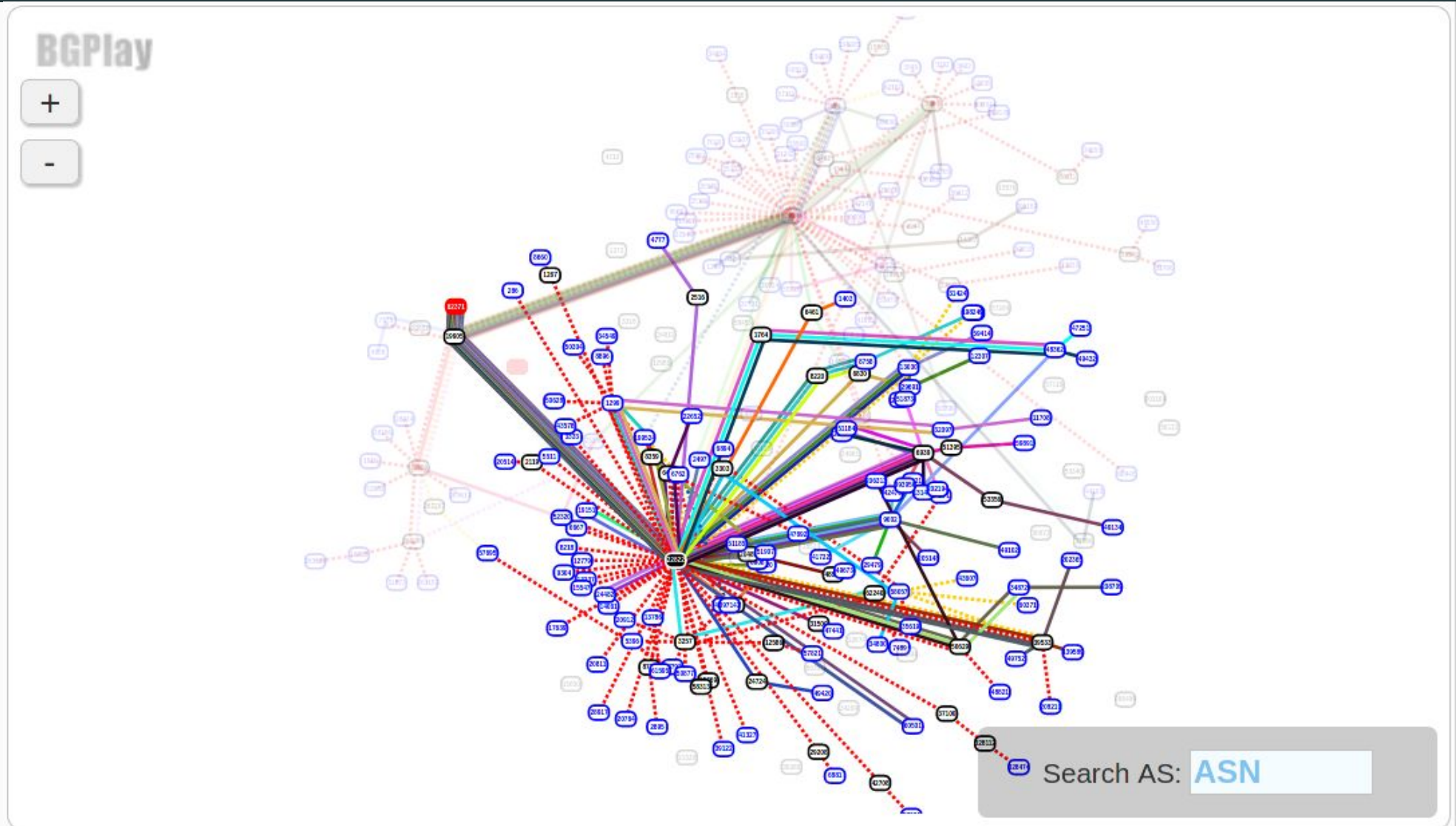
Quad9  @Quad9DNS · 12 4
We disagree with the description of service effects as "negligible", and await any direct reply from Telstra on root cause after our reporting of the issue earlier today to your NOC via phone and email.
1 6 33



Protonmail BGP hijacking, Sept 29th



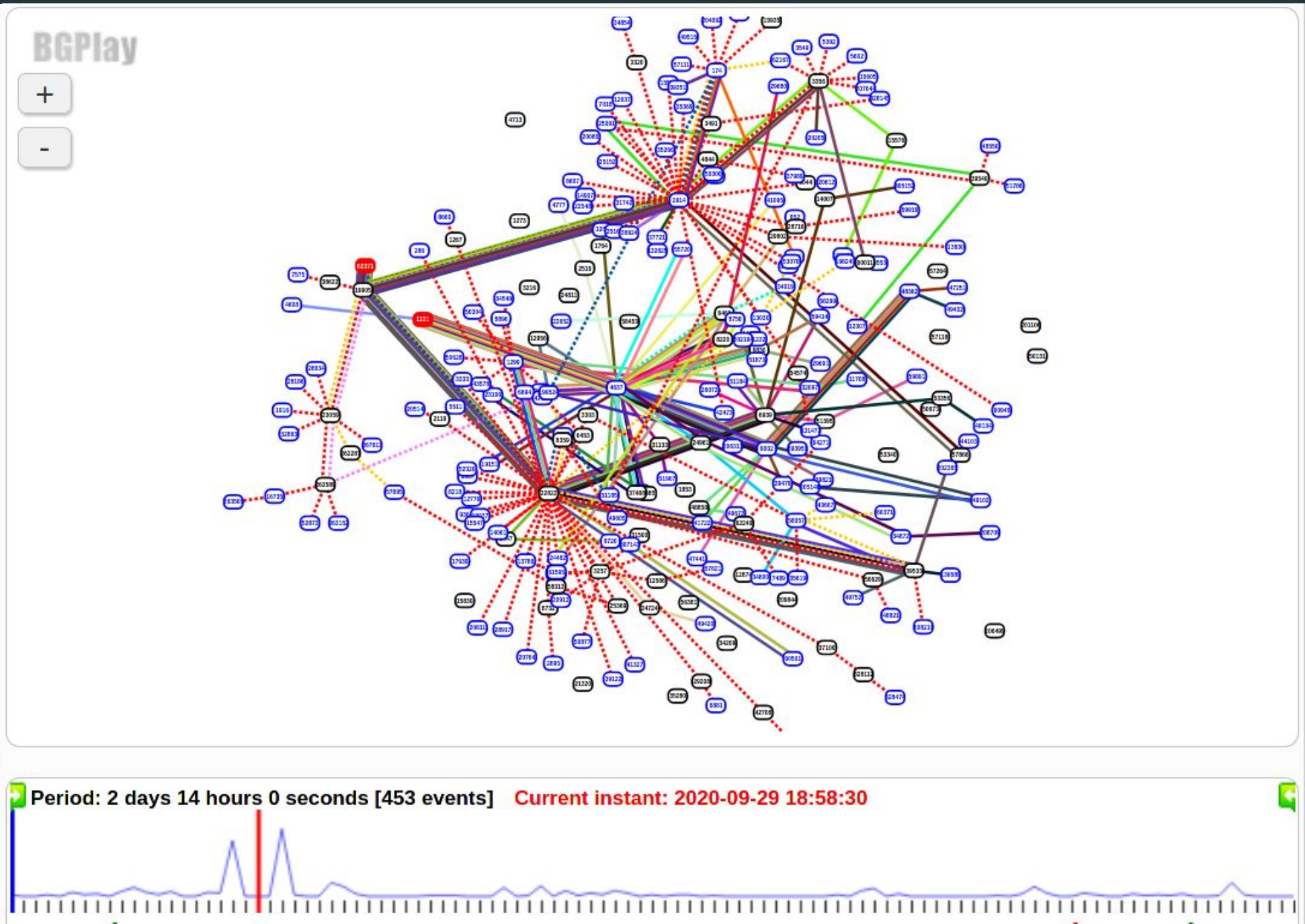
Protonmail: Legitimate route, AS22822, Limelight Networks



Period: 2 days 0 seconds [398 events] Current instant: 2020-09-29 06:59:58



Protonmail: Before

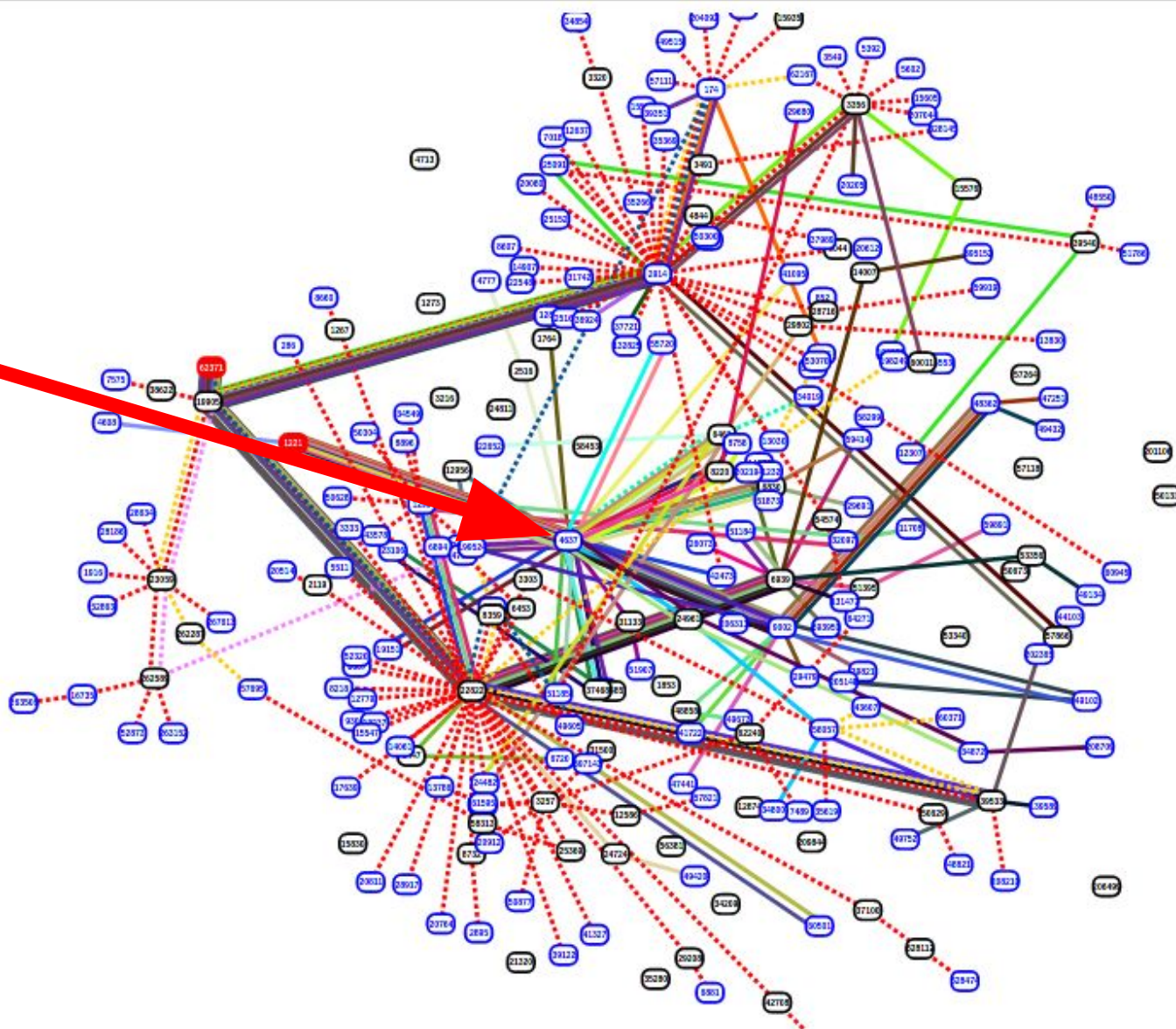


BGPlay

+

-

a random
Australian AS



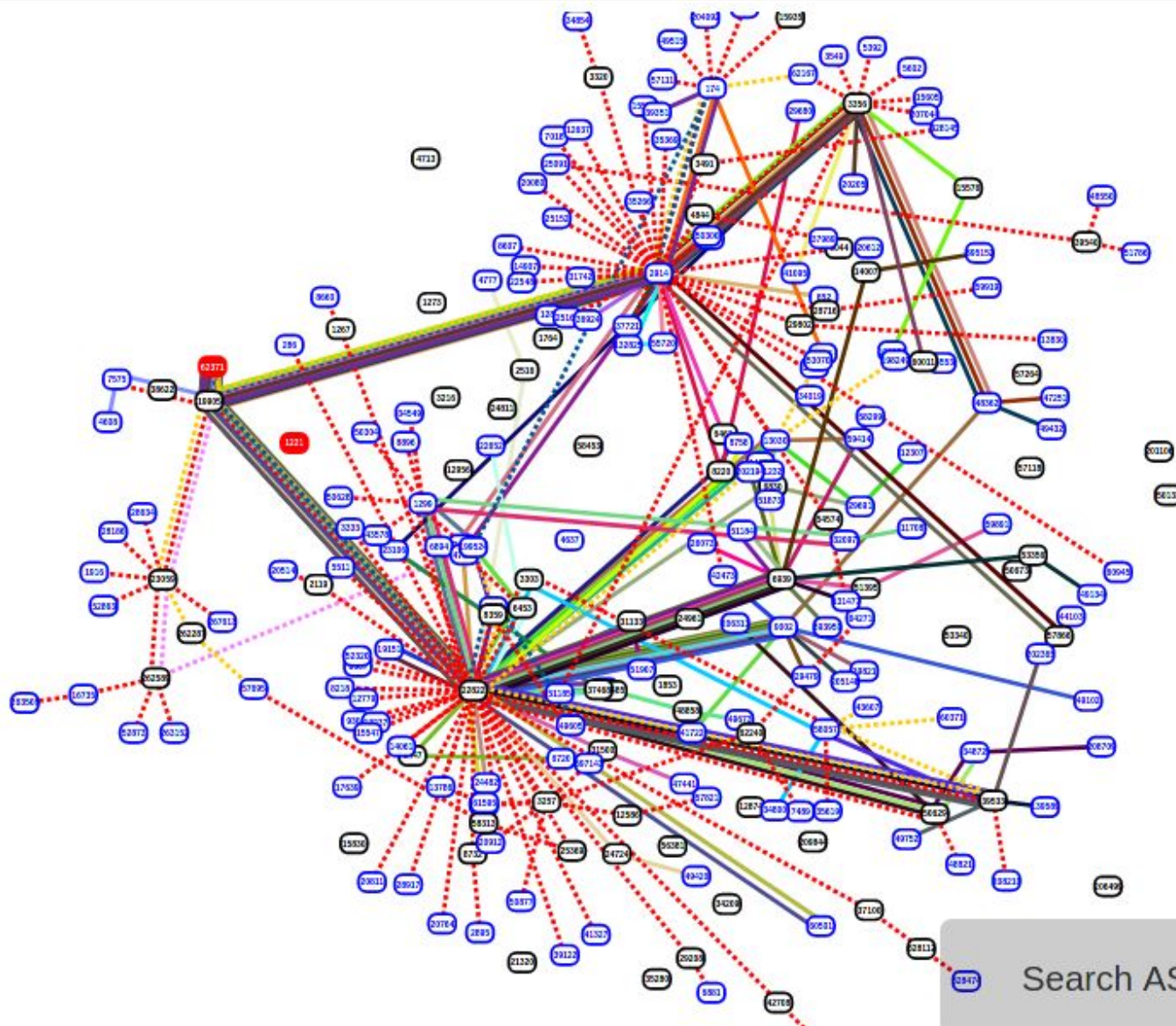
Period: 2 days 14 hours 0 seconds [453 events] Current instant: 2020-09-29 18:58:30



BGPlay

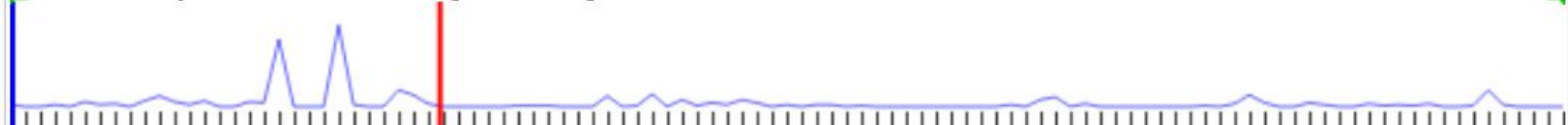
+

-



Search AS:

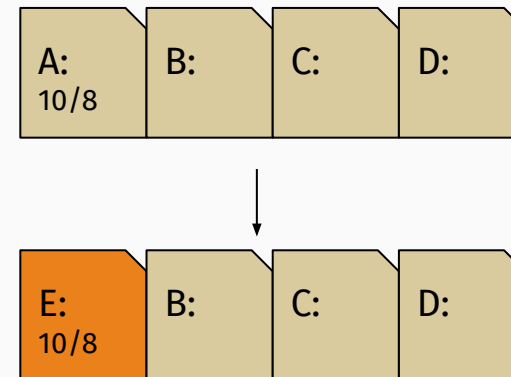
Period: 2 days 14 hours 0 seconds [453 events] Current instant: 2020-09-30 00:08:00



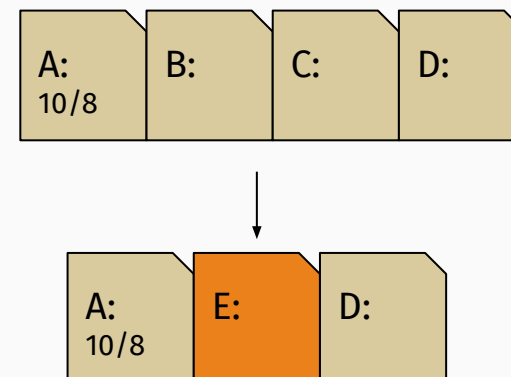
Exercises

Q1, BGP Security: Why?

Lack of origin authentication




Lack of path authentication





Q1, BGP Security: Resource Public Key Infrastructure (RPKI)

Regional Internet Registers issue resource certificates:

 **RPKI Dashboard**

 **41** BGP Announcements

 **4** Valid

 **1** Invalid

 **36** Unknown

BGP Announcements

Route Origin Authorisations (ROAs)


History

↓

Create ROAs for selected BGP Announcements

<input type="checkbox"/>	Origin AS	Prefix	Current Status
<input type="checkbox"/>	AS12654	2001:7fb:fe01::/48	UNKNOWN

9 CERTIFIED RESOURCES

 **Certified Resources**

84.205.64.0/19

93.175.144.0/20

193.30.30.0/23

2001:67c:e0::/48

2001:67c:2e8::/48

2001:67c:2888::/47

2001:67c:2900::/43

2001:7fb::/32

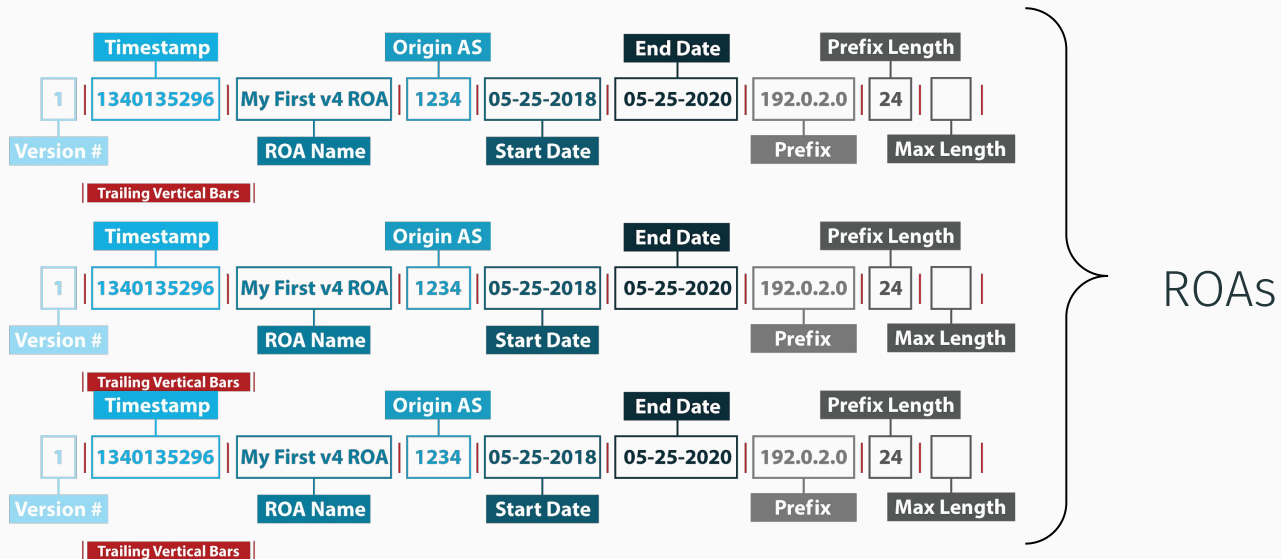
Q1, BGP Security: Resource Public Key Infrastructure (RPKI)

You use your certificate to create Route Origin Authorizations (ROAs):

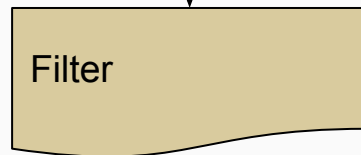


https://www.arin.net/resources/manage/rpki/roa_request/

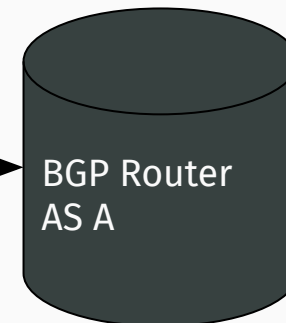
Q1, BGP Security: Resource Public Key Infrastructure (RPKI)



Verify &
Compile Filter

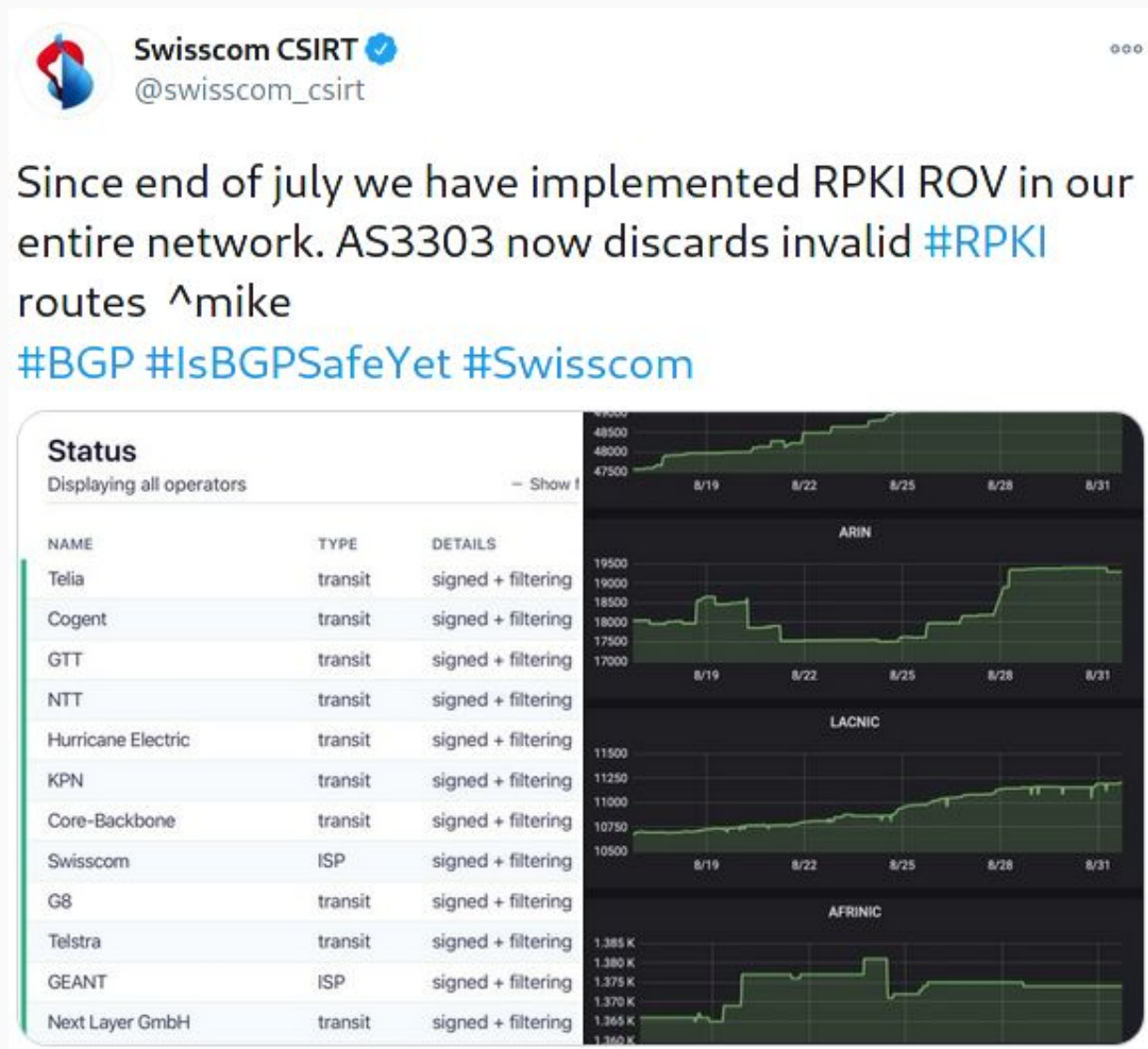


Install Filter



Q1, BGP Security: Resource Public Key Infrastructure (RPKI)

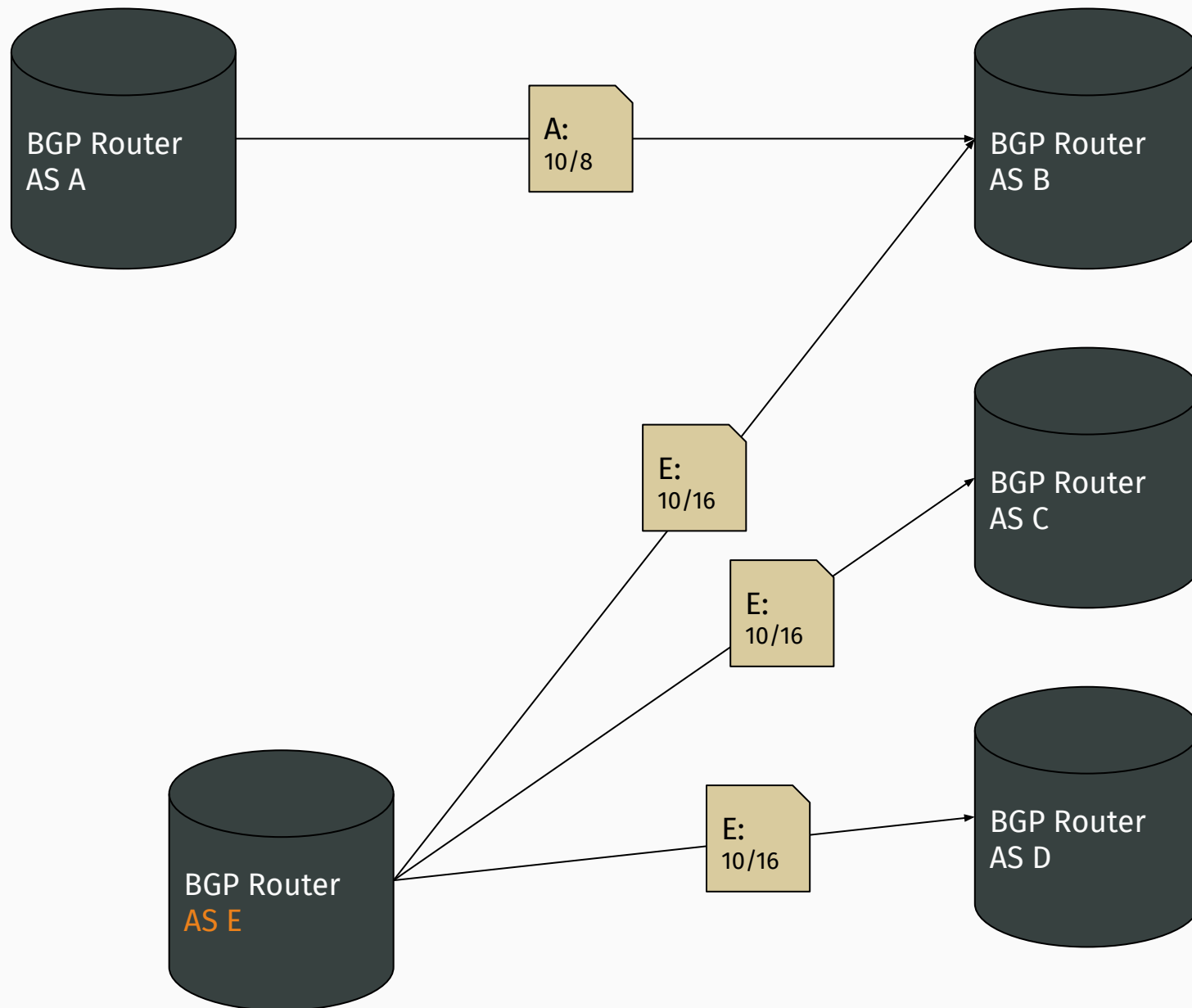
ASs check for ROAs in the RPKI before accepting an announcement:



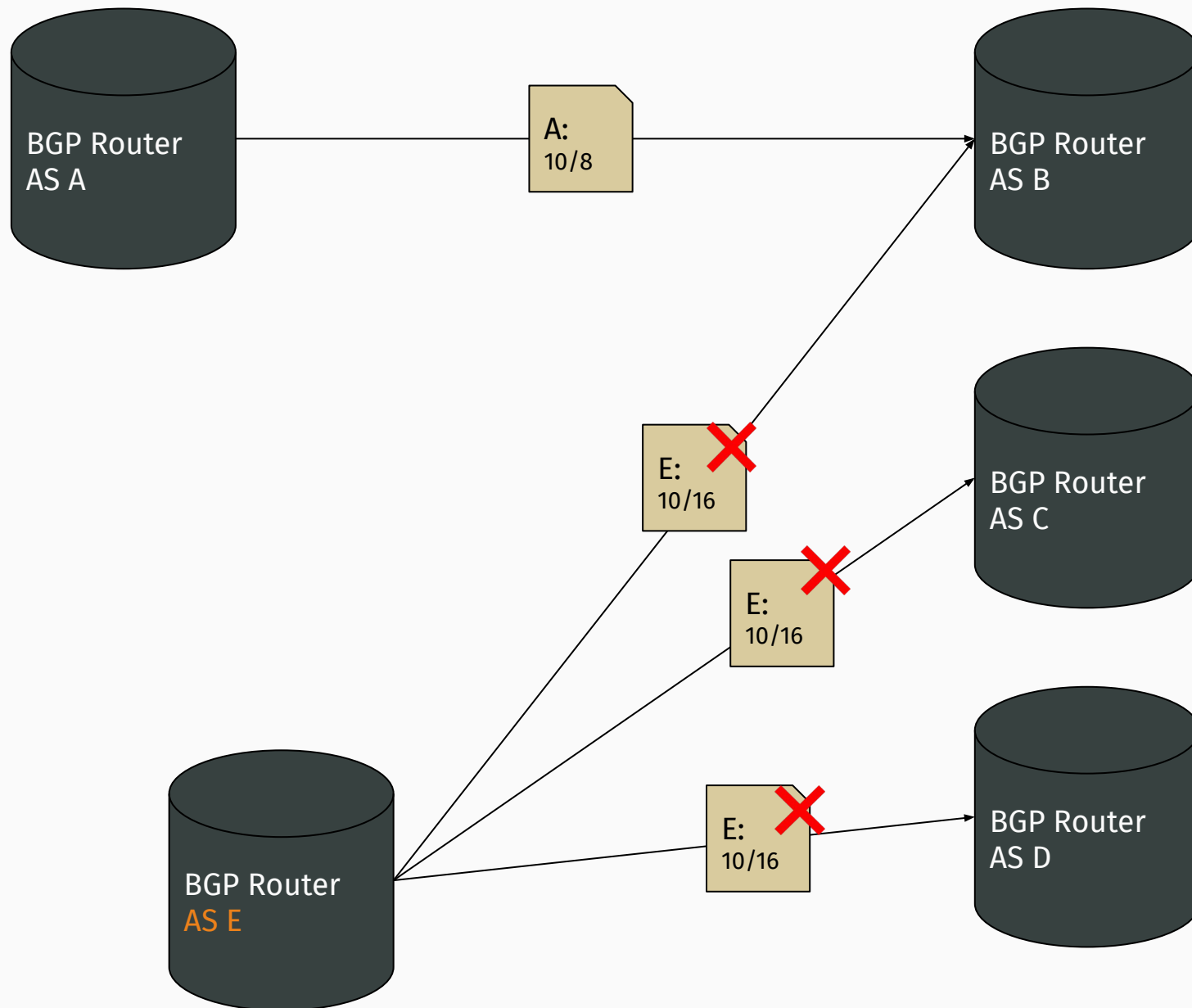
RPKI + BGP Origin Validation answers the question:

“Is this particular route announcement authorised by the legitimate holder of the address space?”

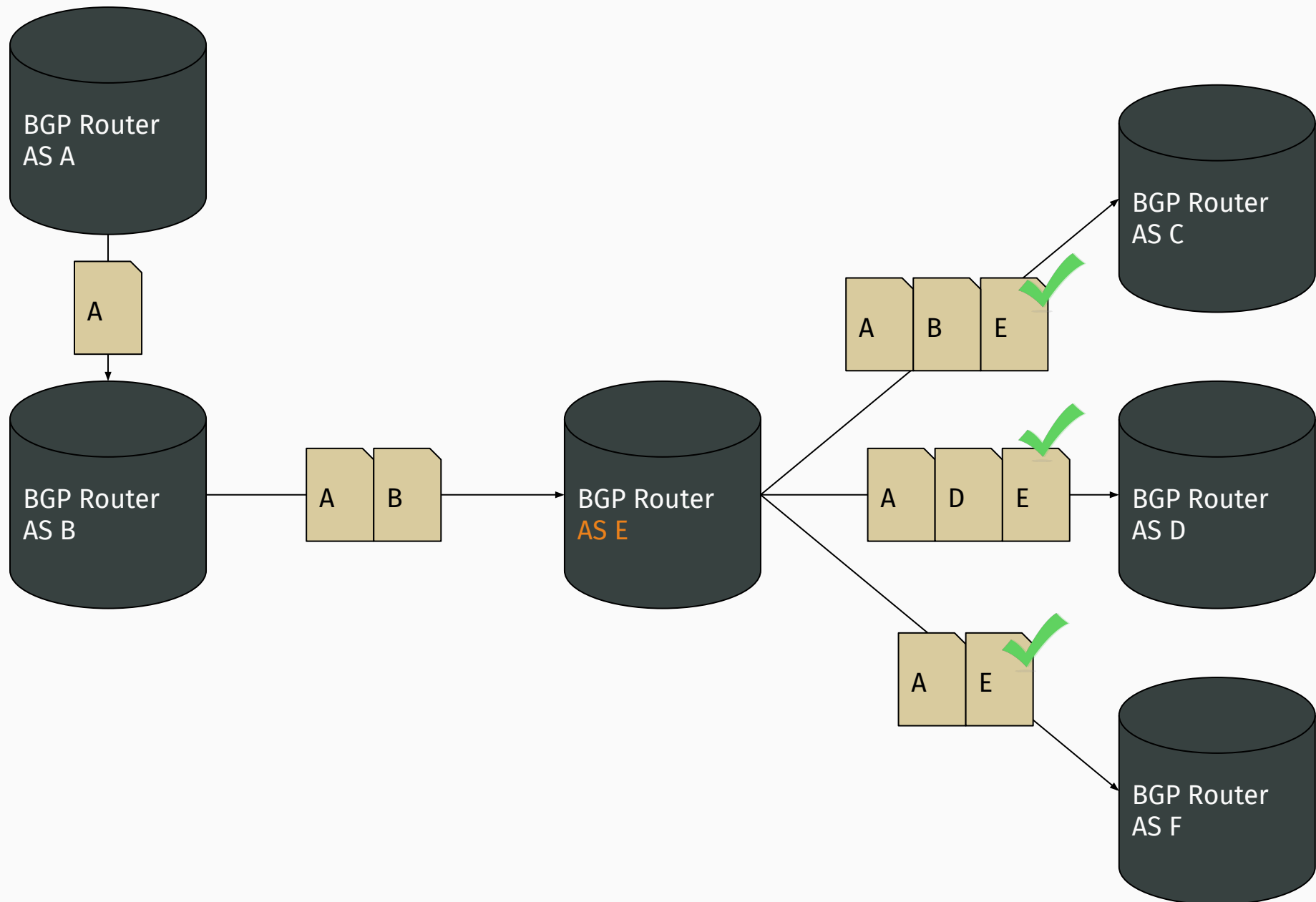
Q1, BGP Security: RPKI



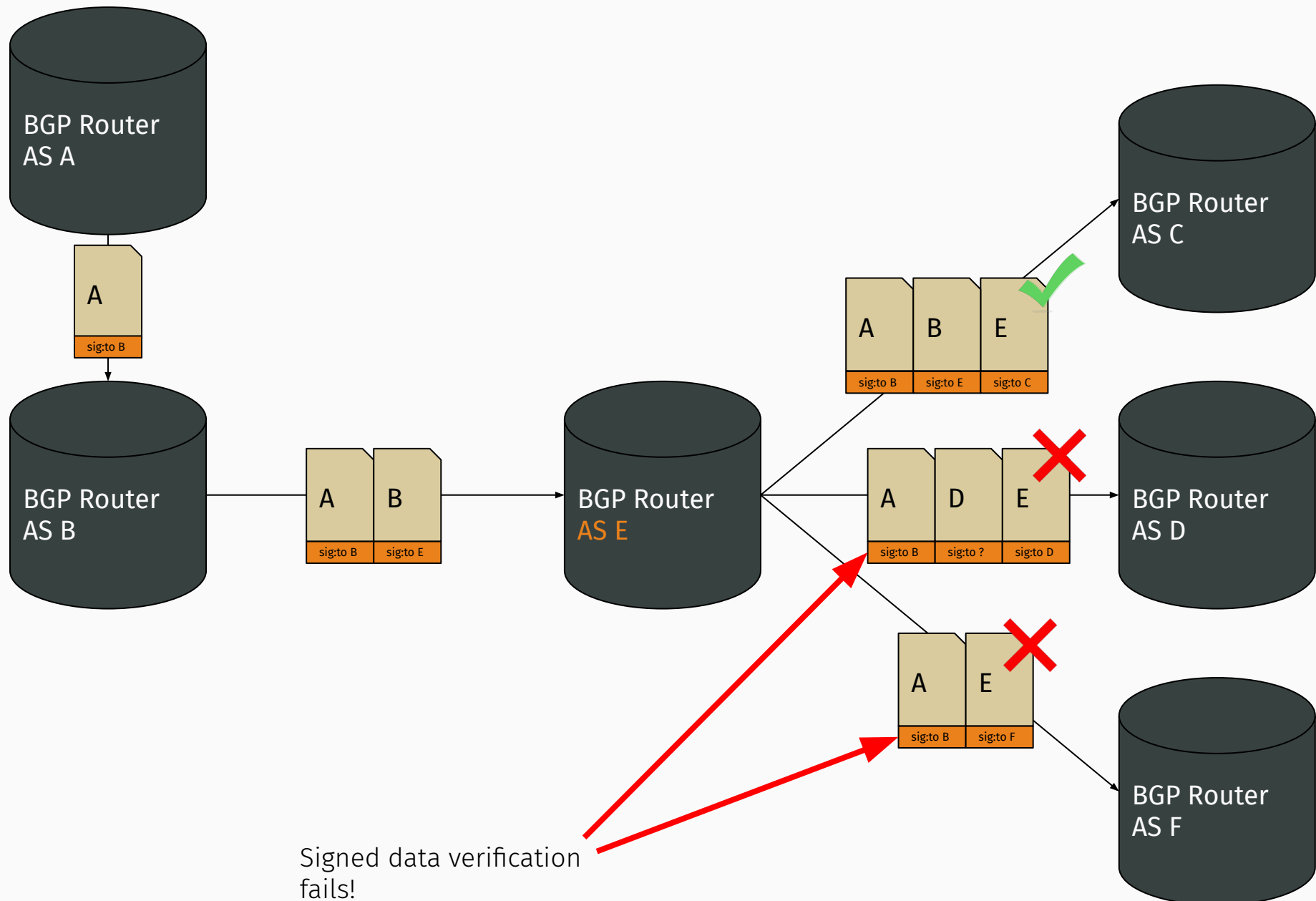
Q1, BGP Security: RPKI



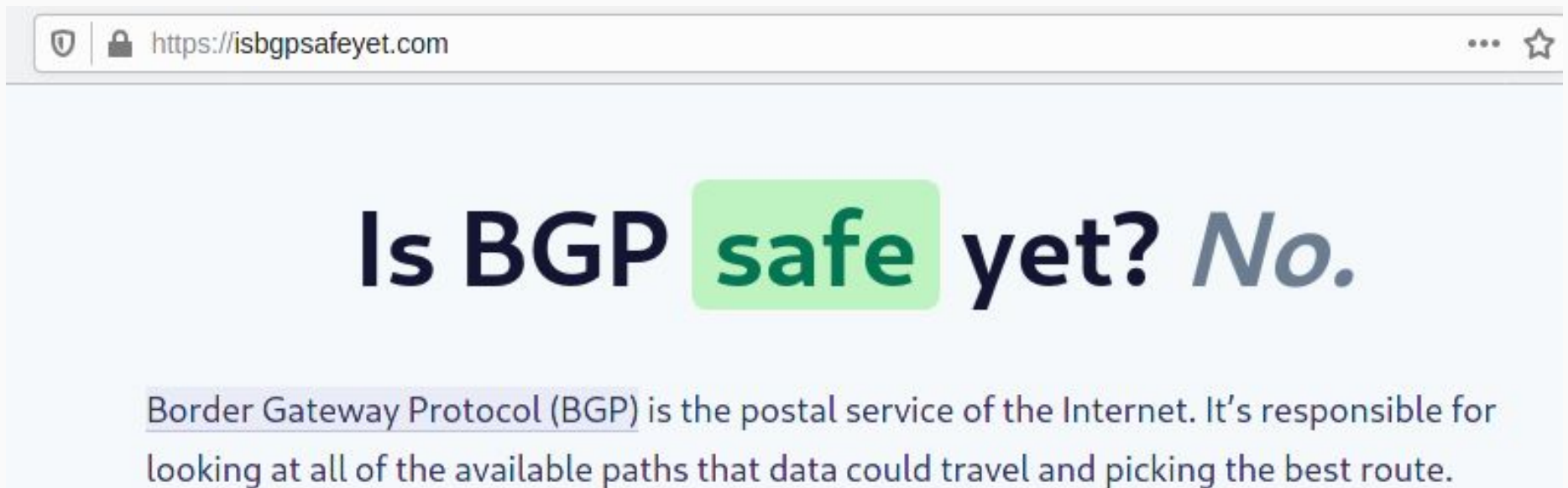
Q1, BGP Security: RPKI



Q1, BGP Security: BGPsec to the rescue



Is BGP safe yet?



Is BGP safe yet?

Status

Displaying 29 major operators

+ Show all

+ Show ASN column

NAME	TYPE	DETAILS	STATUS 
Telia	transit	signed + filtering	safe
Cogent	transit	signed + filtering	safe
GTT	transit	signed + filtering	safe
NTT	transit	signed + filtering	safe
Hurricane Electric	transit	signed + filtering	safe
Cloudflare	cloud	signed + filtering	safe
Netflix	cloud	signed + filtering	safe
Wikimedia Foundation	cloud	signed + filtering	safe
Scaleway	cloud	signed + filtering	safe
TATA	transit	filtering peers only	partially safe
PCCW	transit	filtering peers only	partially safe
Telstra International	transit	signed	partially safe
AT&T	ISP	signed + filtering peers only	partially safe
Google	cloud	signed	partially safe
Amazon	cloud	signed	partially safe
Level3/CenturyLink	transit	started	unsafe
Sparkle	transit	started	unsafe
Zayo	transit		unsafe
Vodafone	transit		unsafe
RETN	transit		unsafe
Orange	transit	started	unsafe
Telefonica/Telxius	transit		unsafe
SingTel	transit		unsafe
PJSC RosTelecom	transit		unsafe
Deutsche Telekom	ISP	started	unsafe
Verizon	ISP		unsafe
Comcast	ISP	started	unsafe
TransTelecom	transit		unsafe
M247	cloud		unsafe

BGPsec deployment



[Main page](#)
[Contents](#)
[Current events](#)
[Random article](#)
[About Wikipedia](#)
[Contact us](#)
[Donate](#)

[Contribute](#)

[Help](#)
[Learn to edit](#)
[Community portal](#)
[Recent changes](#)
[Upload file](#)

[Tools](#)

[What links here](#)
[Related changes](#)
[Special pages](#)
[Permanent link](#)
[Page information](#)
[Cite this page](#)
[Wikidata item](#)

[Print/export](#)

[Download as PDF](#)
[Printable version](#)

Not logged in [Talk](#) [Contributions](#) [Create account](#) [Log out](#)

Article [Talk](#)

[Read](#) [Edit](#) [View history](#)

BGPsec

From Wikipedia, the free encyclopedia

Border Gateway Protocol Security (BGPsec) is a security extension of the [Border Gateway Protocol](#) defined in [RFC 8205](#)^[a], published in September 2017. BGPsec provides to receivers of valid BGPsec UPDATE messages cryptographic verification of the routes they advertise.^[1] BGPsec replaces the BGP AS_PATH attribute with a new BGPsec_Path attribute.^[2]

BGPsec RFCs [\[edit \]](#)

- [RFC 8205](#)^[a] - BGPsec Protocol Specification
- [RFC 8206](#)^[a] - BGPsec Considerations for Autonomous System (AS) Migration
- [RFC 8207](#)^[a] - BGPsec Operational Considerations
- [RFC 8208](#)^[a] - BGPsec Algorithms, Key Formats, and Signature Formats
- [RFC 8209](#)^[a] - A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests

See also [\[edit \]](#)

- [Autonomous system \(Internet\)](#)
- [Border Gateway Protocol](#)

References [\[edit \]](#)

- ↑ Lepinski, Matthew; Sriram, Kotikalapudi (September 2017). "BGPsec Protocol Specification". [RFC 8205](#)^[a]. Missing or empty |url= (help)
- ↑ "BGP security: the BGPsec protocol"^[a]. 30 April 2015.

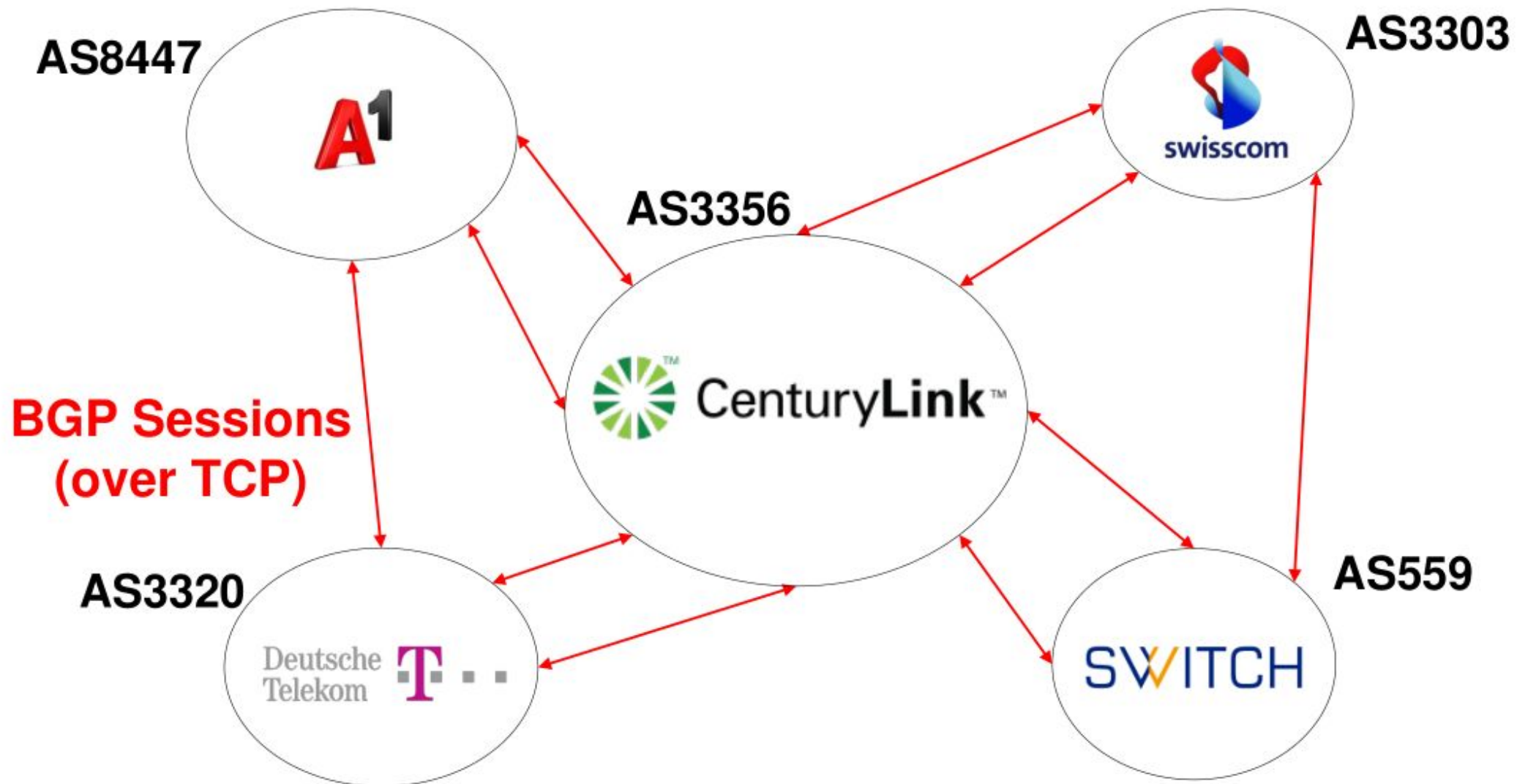


*This Internet-related article is a **stub**. You can help Wikipedia by [expanding it](#).*

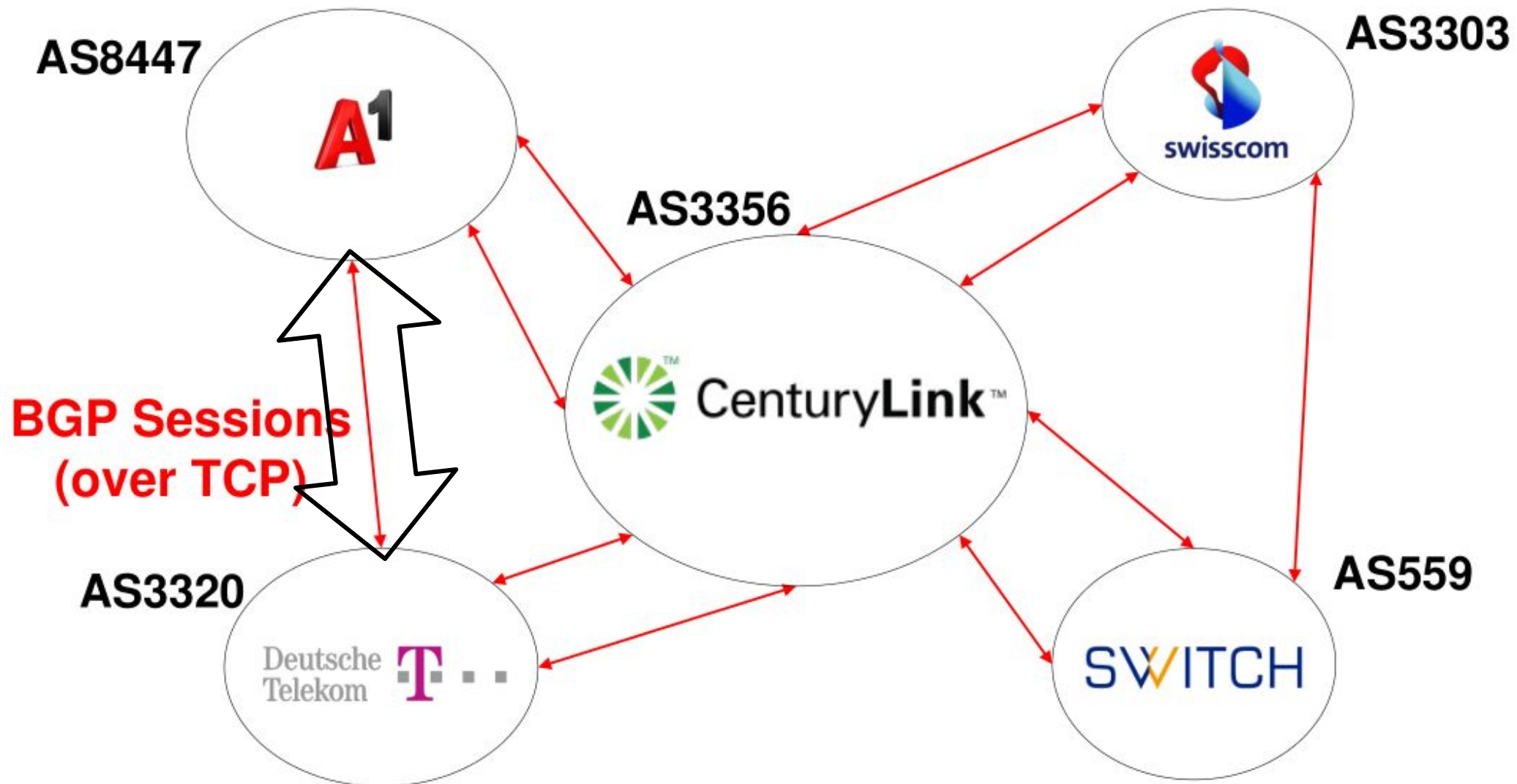
*“Perhaps we were seduced by the prospect of a highly automated secure system and it was only later that it became obvious that BGPSEC has too many deployment impediments and **universal deployment** (a **prerequisite** for **BGPSEC**) is **simply unachievable**.”*

<https://labs.ripe.net/Members/gih/an-update-on-securing-bgp>

Q2, BGP Attacks: TCP



Q2, BGP Attacks: TCP



Q2, BGP Attacks: Gotta catch 'em all

340,282,366,920,938,463,463,374,607,431,768,211,456

IPv6 addresses (4.2×10^{37} usable)

4,294,967,296

IPv4 addresses

Context: DoS

(Distributed) Denial of Service

DDoS extortionists target NZX, Moneygram, Braintree, and other financial services

One of the victims, the New Zealand stock exchange (NZX), has halted trading for the third day in a row following attacks.



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



20 -- 02:45 GMT

MORE FROM CATALIN CIMPANU

Security
Facebook link p
feature and

Alerts and Tips

Resources

Industrial Control Systems

[National Cyber Awareness System](#) > [Current Activity](#) > [DoS and DDoS Attacks against Multiple Sectors](#)

DoS and DDoS Attacks against Multiple Sectors

Original release date: September 04, 2020

Maybe.

dark.fail
@DarkDotFail

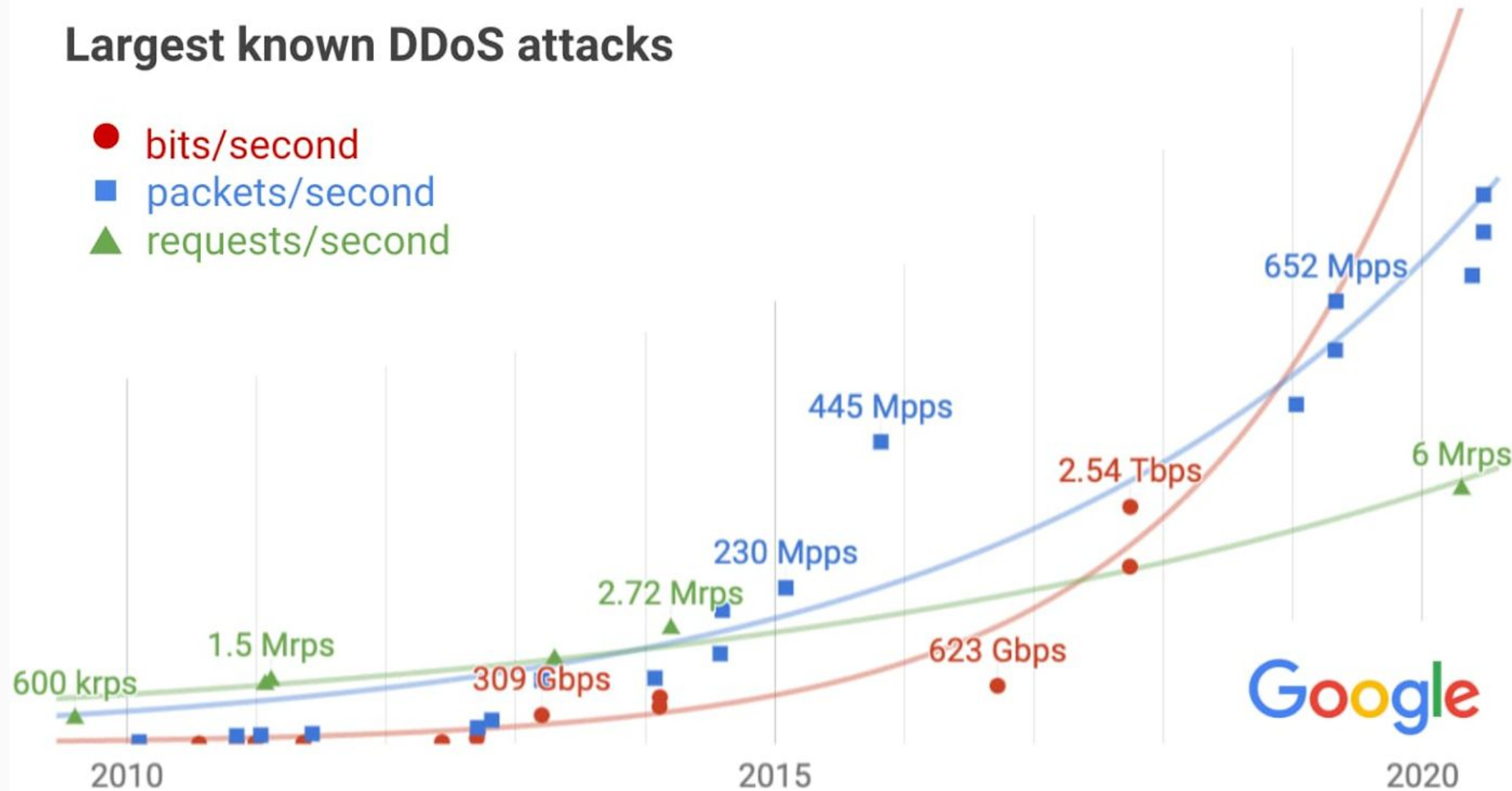
Empire Market remains under a large DDoS attack making it very slow to access. Monero functionality appears broken, Bitcoin is functioning according to multiple trusted sources. Always PGP verify URLs, many phishing links are circulating. dark.fail/pgp

5:55 PM · Aug 21, 2020 · [Twitter Web App](#)

DDoS Trends

Largest known DDoS attacks

- bits/second
- packets/second
- ▲ requests/second

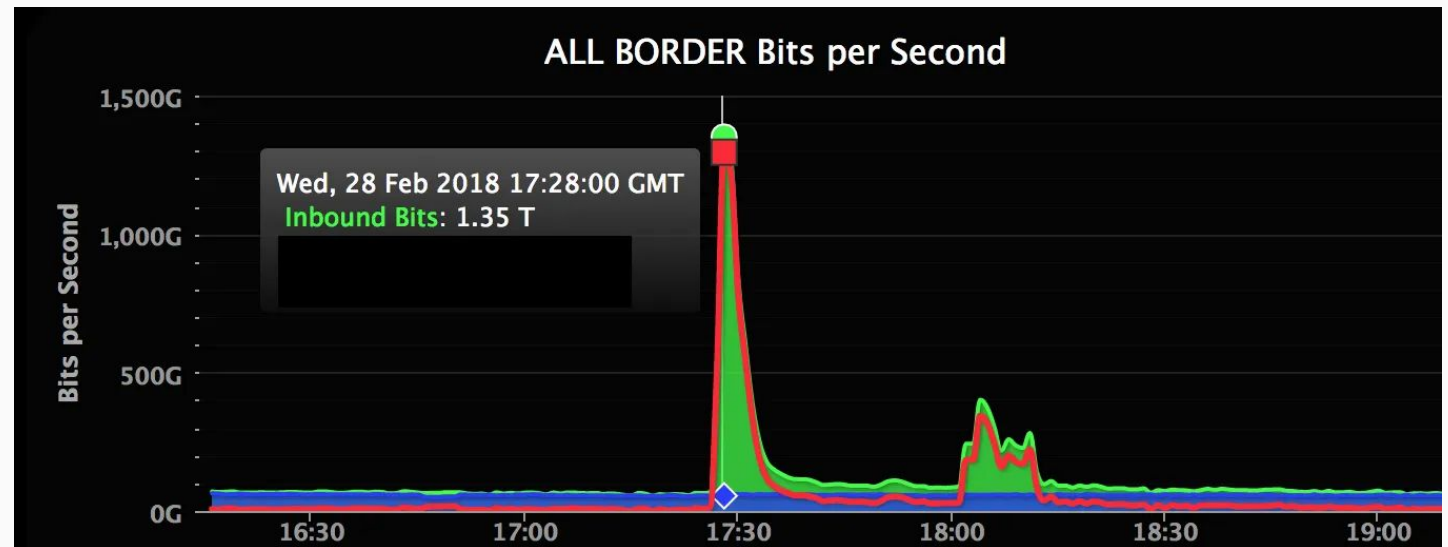


<https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks>

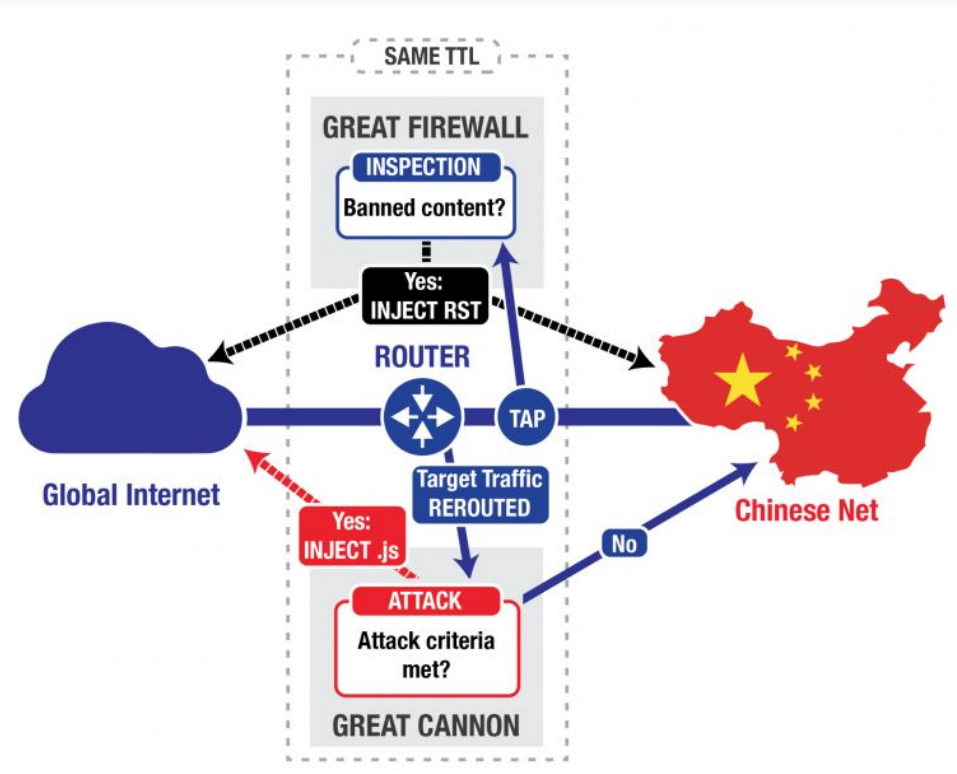
Exercises

Q3, GitHub DDoS

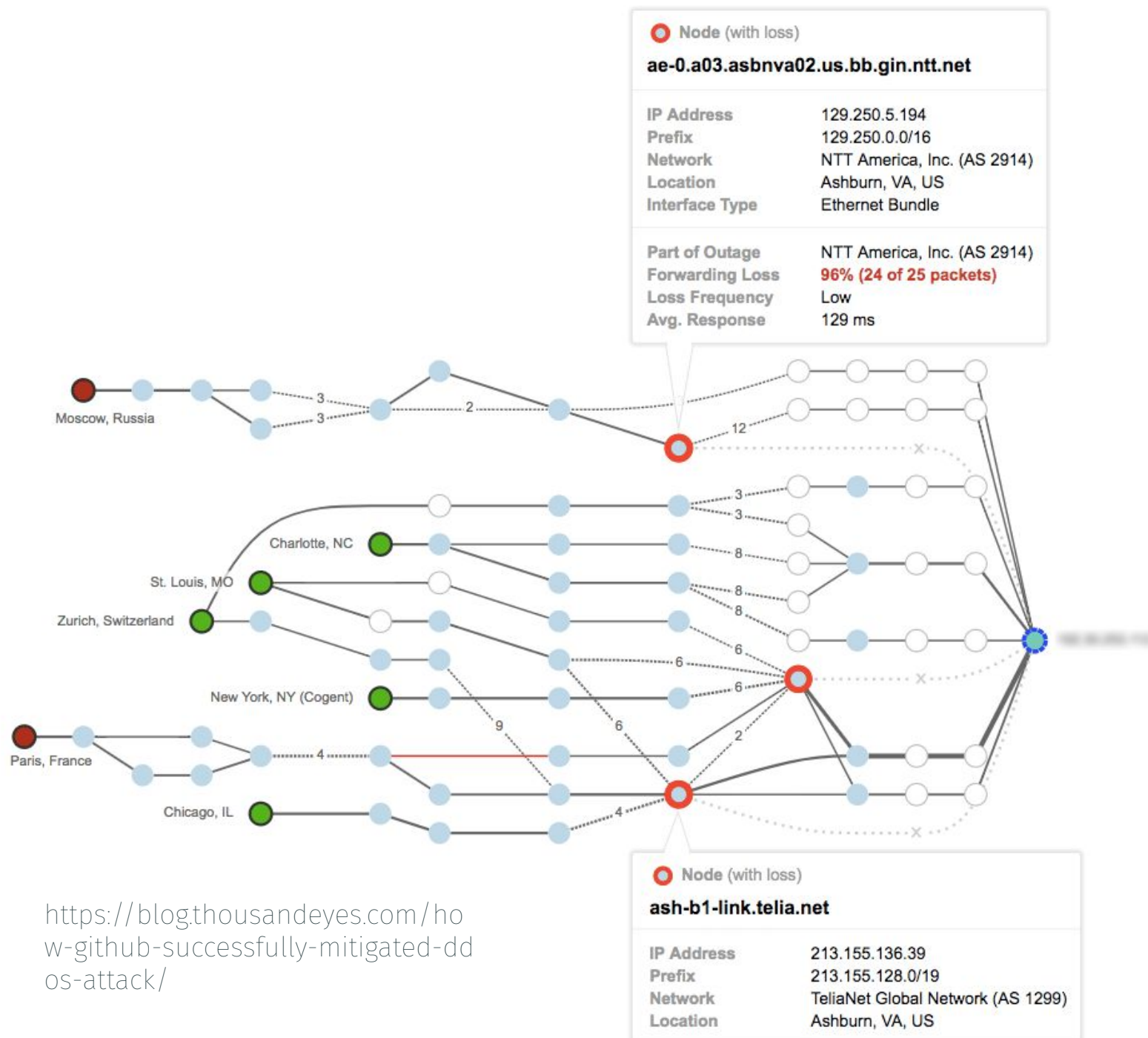
Volumetric:
botnets



Application Layer:
botnets, malicious js

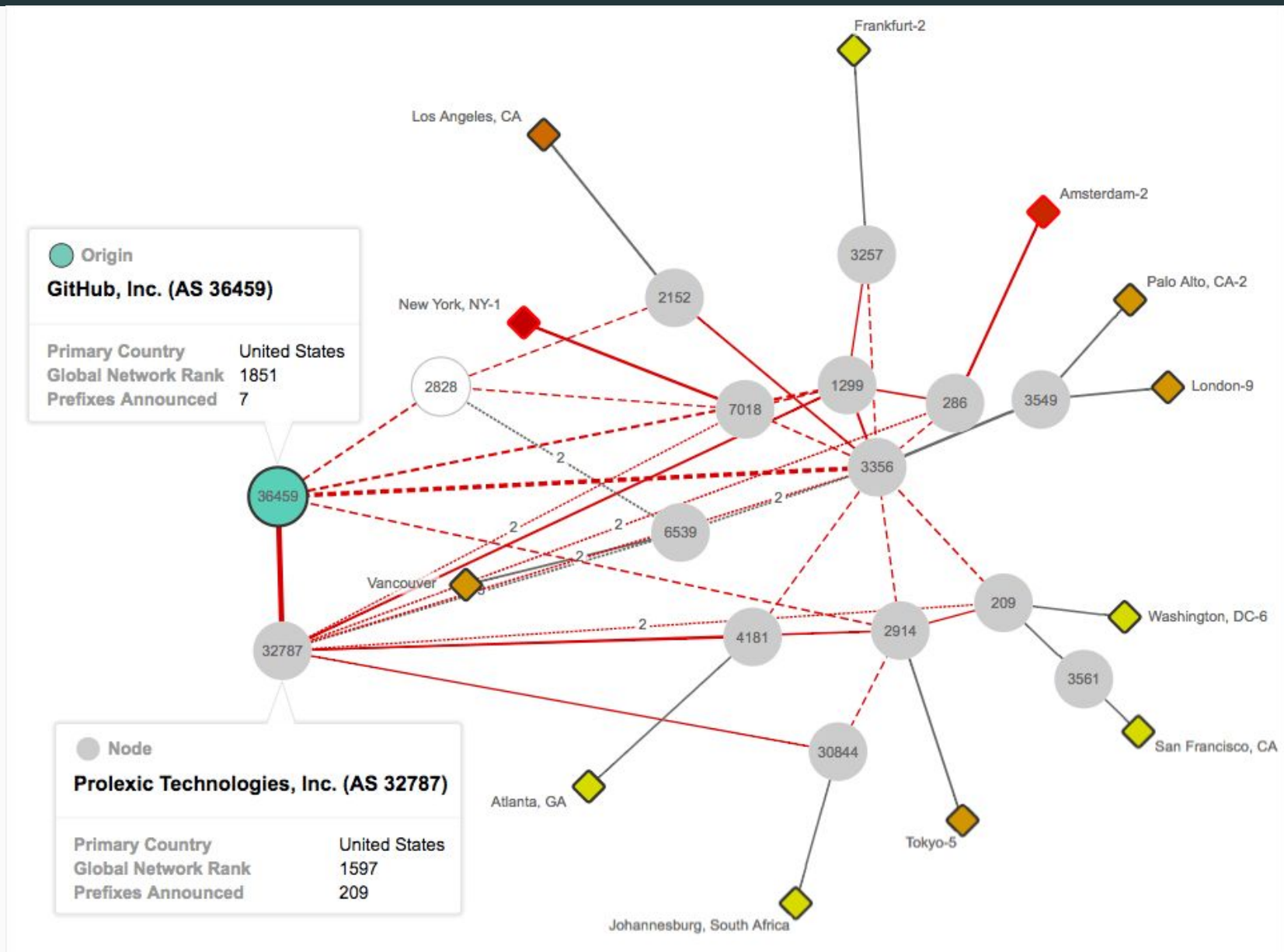


Q3, GitHub DDoS



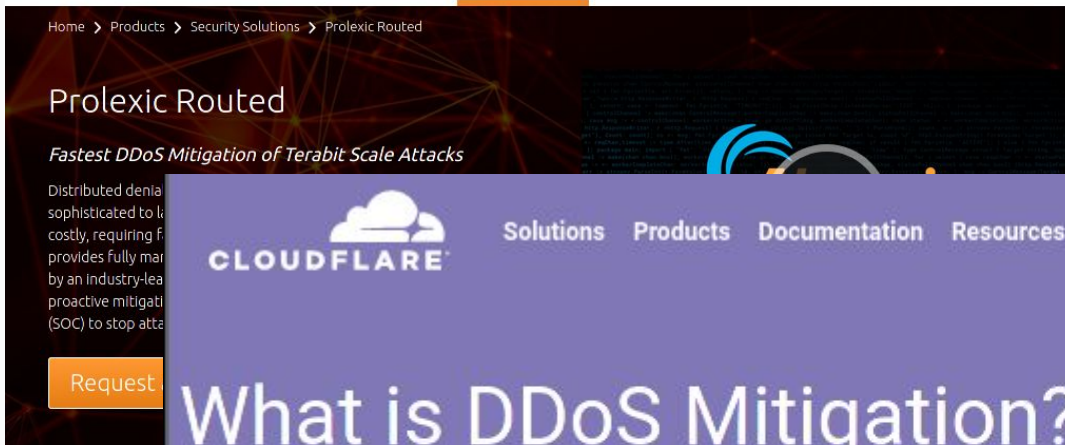
<https://blog.thousandeyes.com/how-github-successfully-mitigated-ddos-attack/>


Q3, GitHub DDoS: BGP



<https://blog.thousandeyes.com/how-github-successfully-mitigated-ddos-attack/>

Defending from DDoS?



[Solutions](#)[Products](#)[Documentation](#)[Resources](#)[Partners](#)[For Enterprise](#)[Pricing](#)

What is DDoS Mitigation?

Properly implemented DDoS mitigation is what keeps websites online during an attack. Explore the process of

Google Cloud Armor

Help protect your applications and websites against denial of service and web attacks.

[Try Google Cloud free](#)

- ✓ Benefit from DDoS protection and WAF at Google scale
- ✓ Detect and mitigate attacks against your [Cloud Load Balancing](#) workloads
- ✓ Mitigate OWASP Top 10 risks and help protect workloads on-premises or in the cloud
- ✓ Introducing a monthly subscription for Cloud Armor Managed Protection Plus: [sign-](#)

Google Cloud Armor



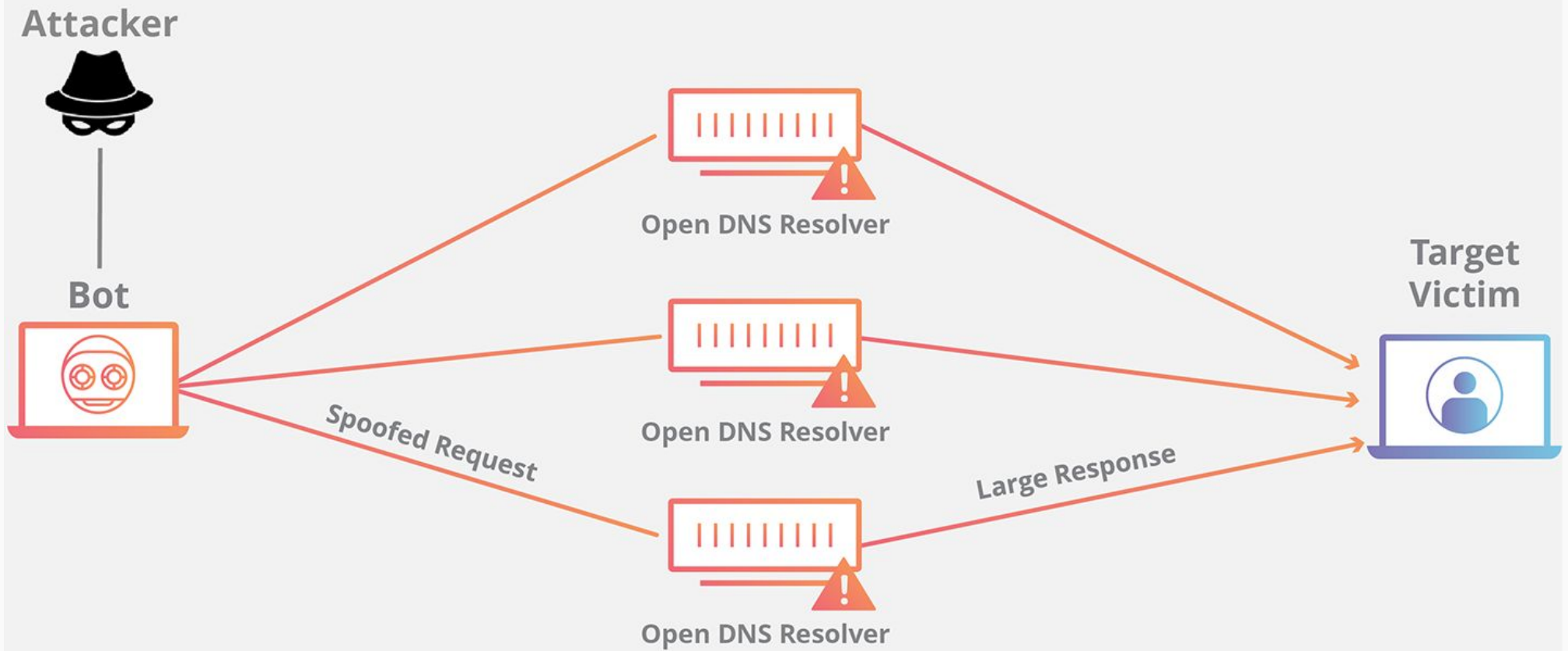
- ! Mitigate volumetric DDoS attacks across all global load balancers
- Application Firewall to help defend against application layer attacks
- Filter traffic based on IP, Geo, and custom match parameters (SQLi, L7 etc)
- Telemetry: Cloud Logging, Cloud Monitoring, and Security Command Center

30:00

VIDEO

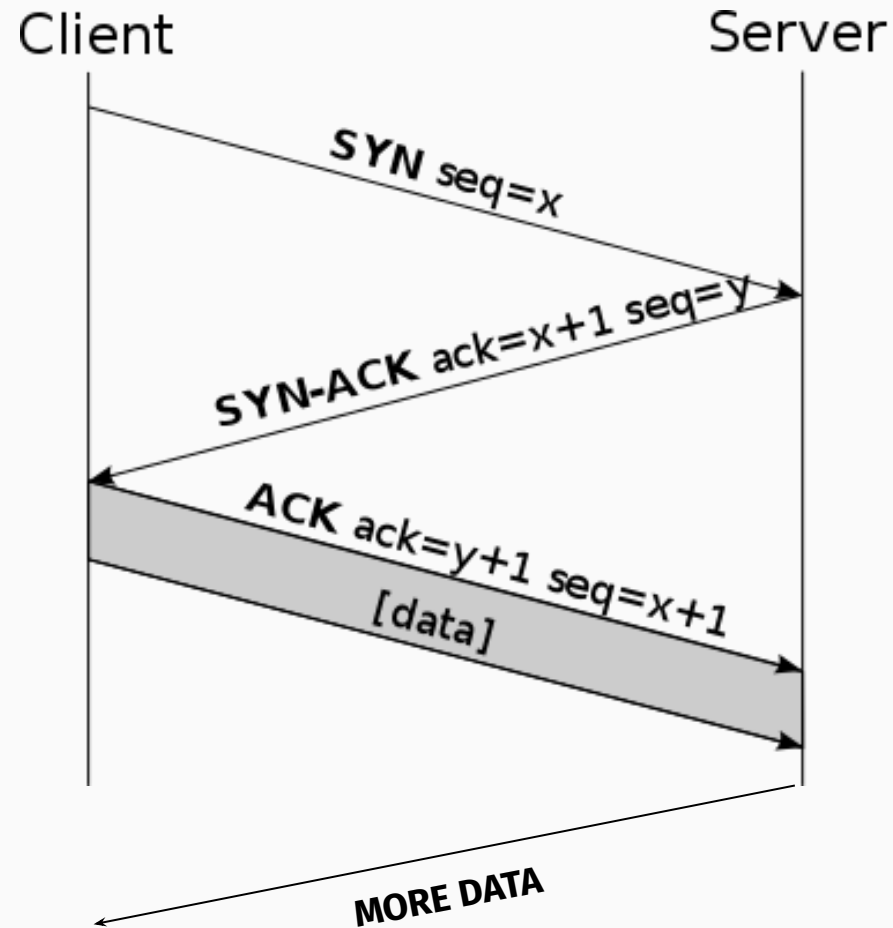
Protect Your Web Sites and Applications with Google Cloud Armor

Q4, DNS Amplification



<https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/>

Q4, DNS Amplification: TCP



Q4, DNS Amplification

```
$ dig @1.1.1.1 cloudflare.com +dnssec DNSKEY
```

```
; <<>> DiG 9.16.8 <<>> @1.1.1.1 cloudflare.com +dnssec DNSKEY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; —>HEADER<— opcode: QUERY, status: NOERROR, id: 57595
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;cloudflare.com.                IN      DNSKEY

;; ANSWER SECTION:
cloudflare.com.                1016    IN      DNSKEY  256 3 13
oJMRsSz5E4gYzS/q6XDrvU1qMPYIjCWzJaOau8XNEZeqCYKD5ar0IRd8
KqXXFJkqmVfRvMGPmM1x8fGAa2XhSA=
cloudflare.com.                1016    IN      DNSKEY  257 3 13
mdsswUyr3DPW132mOi8V9xESWE8jTo0dxCjjnopKl+GqJxpVXckHAeF+
KkxLbxILfDLUT0rAK9iUzy1L53eKGQ=
cloudflare.com.                1016    IN      RRSIG   DNSKEY 13 2 3600 20201209040839
20201010040839 2371 cloudflare.com.
r8W0+3HPFyhFnkCArdjroYPN0fw3K23Si17IVLb3fFQIuHvnVn2GGB+H
X5TMQD508JsYzZgC9k4zwzH92qVJyw=

;; Query time: 23 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Wed Nov 11 18:32:52 CET 2020
;; MSG SIZE rcvd: 313
```


Q4, DNS Amplification

```
$ dig @198.41.0.4 google.com +dnssec
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;google.com.                IN      A

;; AUTHORITY SECTION:
com.                172800   IN      NS      e.gtld-servers.net.
[ ... ]
E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C41A5766
com.                86400    IN      RRSIG    DS 8 1 86400 20201124160000 20201111150000 26116 .
yFIa8zhqrKZDrZYx7keZZ9zholceNwyjgwM0Kiqjo5GQ+Rg0ZWDnwos/
FkPCamK047MTwsZRK94G0ncXtZ+BvłKGuyDdbBvDT9+GRd8YhajhV6uJ
[ ... ]

;; Query time: 26 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Wed Nov 11 19:16:13 CET 2020
;; MSG SIZE rcvd: 1170
```

Q4, DNS Amplification

```
$ dig @1.1.1.1 ANY cloudflare.com +dnssec +edns=0 +bufsize=4096
```

```
; <<>> DiG 9.16.8 <<>> @1.1.1.1 ANY cloudflare.com +dnssec +edns=0 +bufsize=4096
; (1 server found)
;; global options: +cmd
;; Got answer:
;; —>>HEADER<<— opcode: QUERY, status: NOTIMP, id: 2598
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;cloudflare.com.                IN      ANY

;; Query time: 23 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Wed Nov 11 18:35:32 CET 2020
;; MSG SIZE rcvd: 43
```