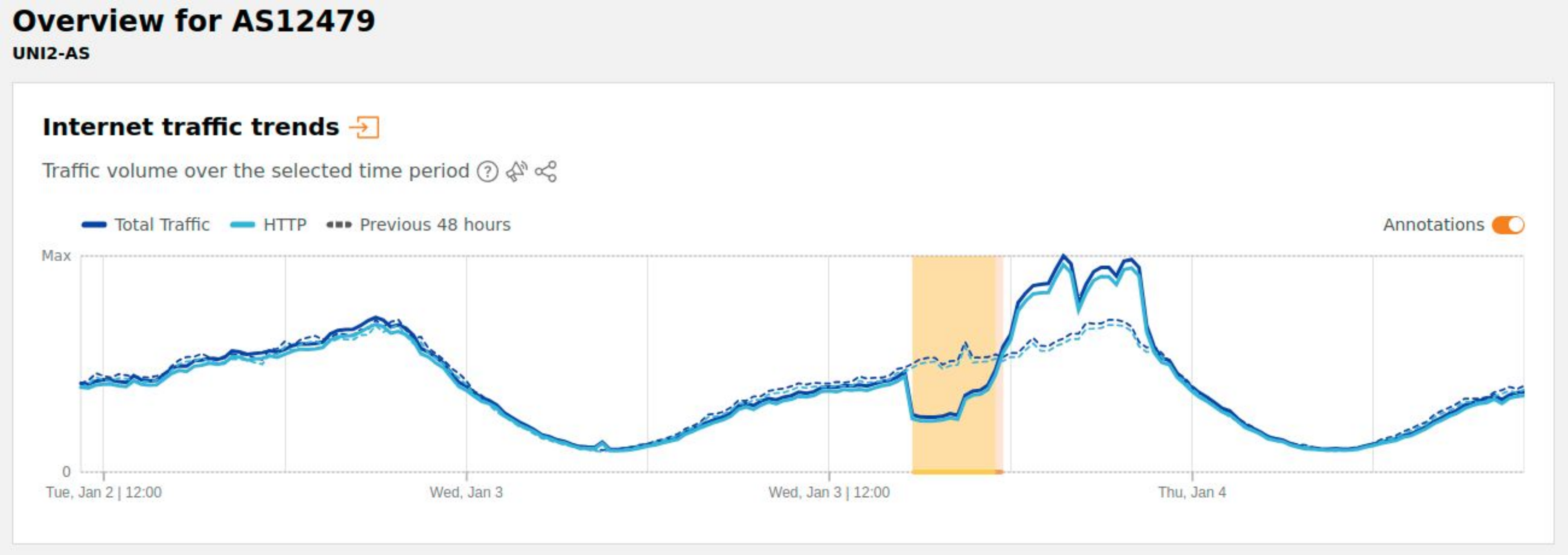
Signed but not secure

Ben Cartwright-Cox @ PeeringDays 2024

The Orange Spain incident timeline

- Rough timeline is
  - [???] Orange Spain employee has a compromised computer, and logs into their RIPE NCC Account with the password of "`ripeadmin`"
  - [???] This password is eventually leaked to a publicly searchable engine of compromised credentials
  - [Jan 3] Person finds these creds, and logs into Orange Spain's RIPE NCC account, there is no 2FA enabled on the account
  - [09:38] First RPKI Changes are seen
  - [13:50~] Person signs ROAs that points 2 Million IP's to a non orange ASN
  - [14:30] Orange Spain's traffic is greatly impacted
  - [17:30~] Malicious ROA is removed
  - [19:00] Reachability mostly restored

The Orange Spain incident timeline



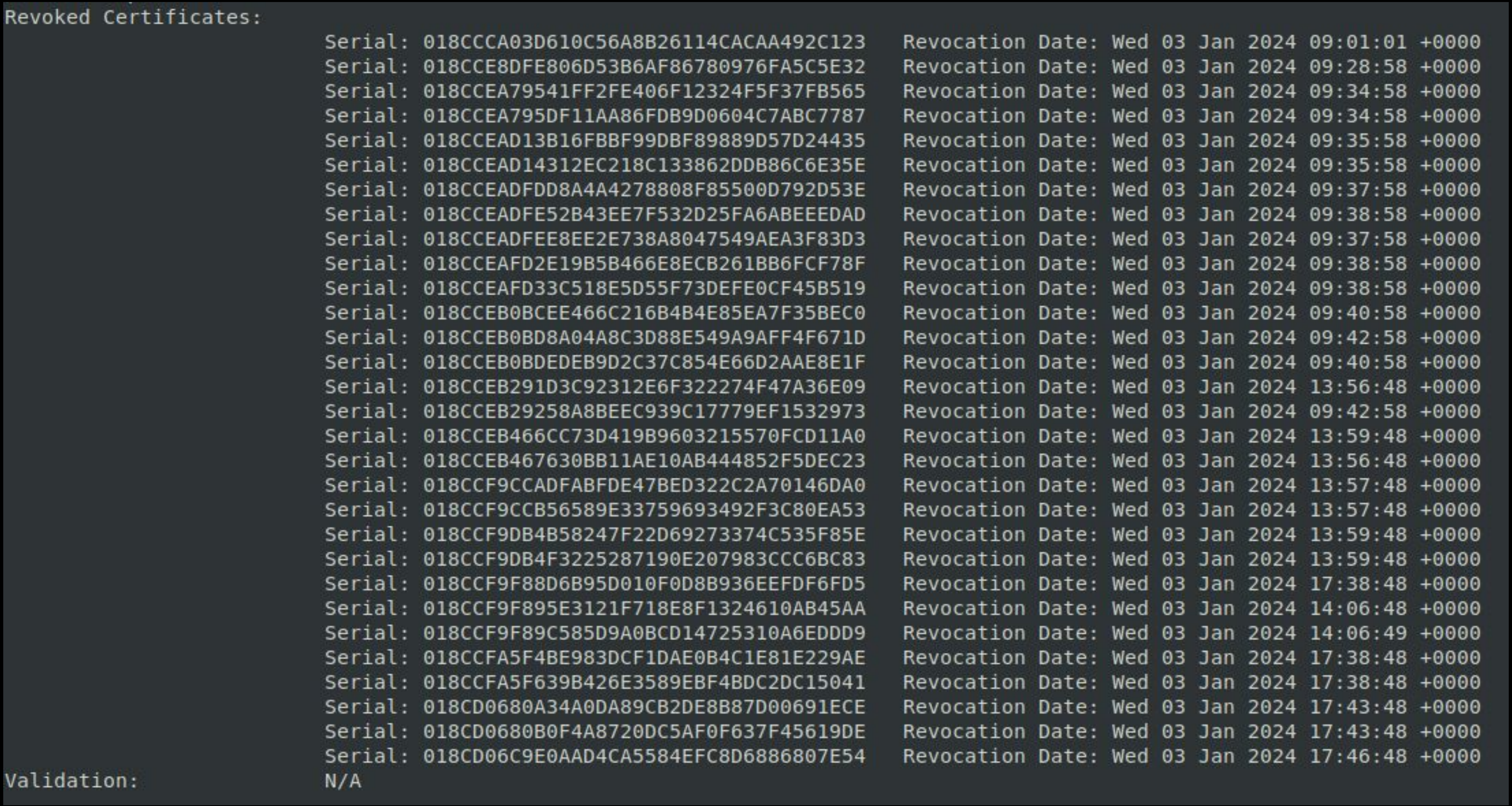
Overview for AS12479

UNI2-AS

Internet traffic trends

Traffic volume over the selected time period

[illegible] Orange Spain's traffic is greatly impacted

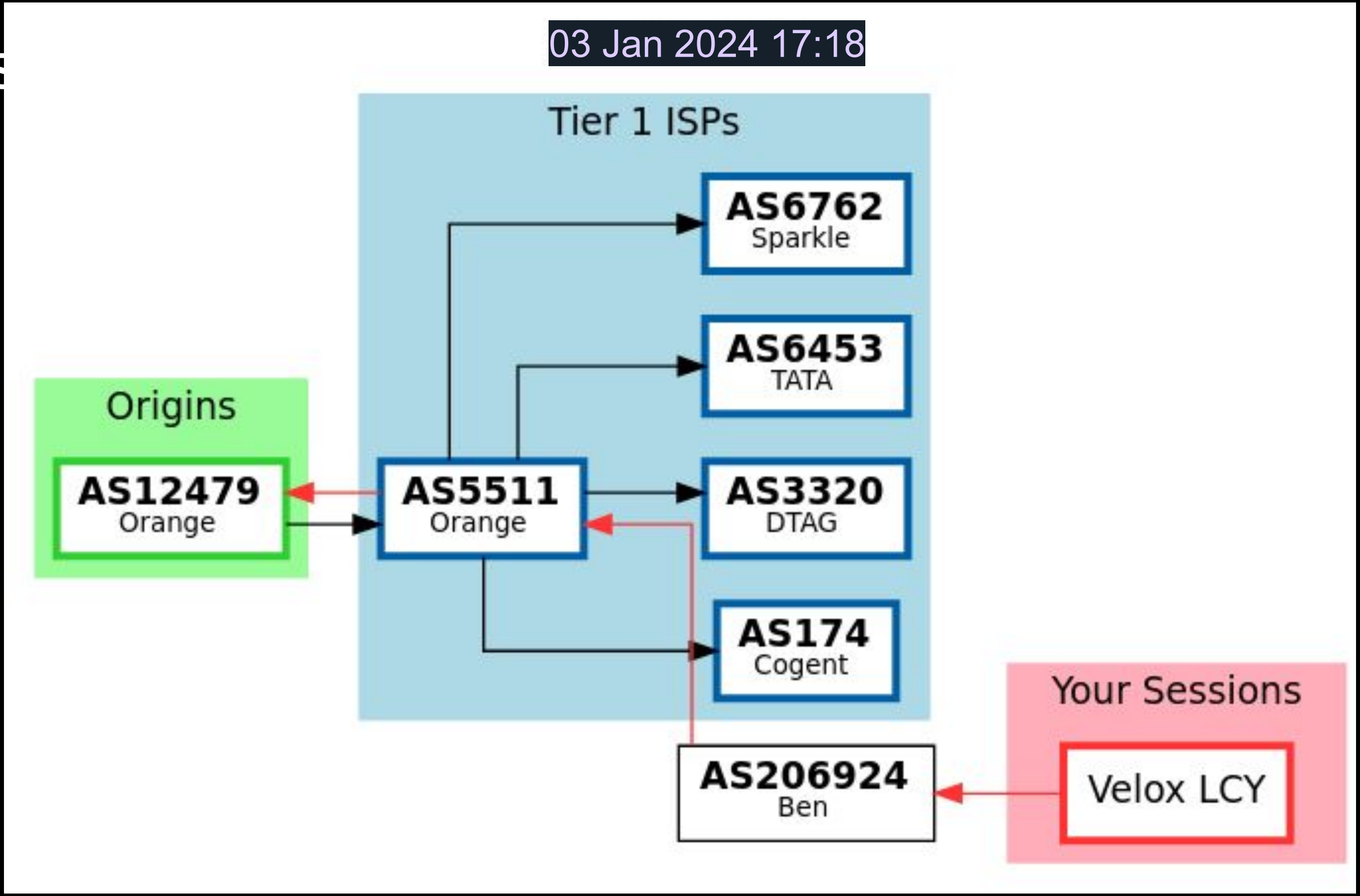


```
Revoked Certificates:
                          Serial: 018CCCA03D610C56A8B26114CACAA492C123   Revocation Date: Wed 03 Jan 2024 09:01:01 +0000
                          Serial: 018CCE8DFE806D53B6AF86780976FA5C5E32   Revocation Date: Wed 03 Jan 2024 09:28:58 +0000
                          Serial: 018CCEA79541FF2FE406F12324F5F37FB565   Revocation Date: Wed 03 Jan 2024 09:34:58 +0000
                          Serial: 018CCEA795DF11AA86FDB9D0604C7ABC7787   Revocation Date: Wed 03 Jan 2024 09:34:58 +0000
                          Serial: 018CCEAD13B16FBBF99DBF89889D57D24435   Revocation Date: Wed 03 Jan 2024 09:35:58 +0000
                          Serial: 018CCEAD14312EC218C133862DDB86C6E35E   Revocation Date: Wed 03 Jan 2024 09:35:58 +0000
                          Serial: 018CCEADFDD8A4A4278808F85500D792D53E   Revocation Date: Wed 03 Jan 2024 09:37:58 +0000
                          Serial: 018CCEADFE52B43EE7F532D25FA6ABEEEDAD   Revocation Date: Wed 03 Jan 2024 09:38:58 +0000
                          Serial: 018CCEADFEE8EE2E738A8047549AEA3F83D3   Revocation Date: Wed 03 Jan 2024 09:37:58 +0000
                          Serial: 018CCEAFD2E19B5B466E8ECB261BB6FCF78F   Revocation Date: Wed 03 Jan 2024 09:38:58 +0000
                          Serial: 018CCEAFD33C518E5D55F73DEFE0CF45B519   Revocation Date: Wed 03 Jan 2024 09:38:58 +0000
                          Serial: 018CCEB0BCEE466C216B4B4E85EA7F35BEC0   Revocation Date: Wed 03 Jan 2024 09:40:58 +0000
                          Serial: 018CCEB0BD8A04A8C3D88E549A9AFF4F671D   Revocation Date: Wed 03 Jan 2024 09:42:58 +0000
                          Serial: 018CCEB0BDEDEB9D2C37C854E66D2AAE8E1F   Revocation Date: Wed 03 Jan 2024 09:40:58 +0000
                          Serial: 018CCEB291D3C92312E6F322274F47A36E09   Revocation Date: Wed 03 Jan 2024 13:56:48 +0000
                          Serial: 018CCEB29258A8BEEC939C17779EF1532973   Revocation Date: Wed 03 Jan 2024 09:42:58 +0000
                          Serial: 018CCEB466CC73D419B9603215570FCD11A0   Revocation Date: Wed 03 Jan 2024 13:59:48 +0000
                          Serial: 018CCEB467630BB11AE10AB444852F5DEC23   Revocation Date: Wed 03 Jan 2024 13:56:48 +0000
                          Serial: 018CCF9CCADFABFDE47BED322C2A70146DA0   Revocation Date: Wed 03 Jan 2024 13:57:48 +0000
                          Serial: 018CCF9CCB56589E33759693492F3C80EA53   Revocation Date: Wed 03 Jan 2024 13:57:48 +0000
                          Serial: 018CCF9DB4B58247F22D69273374C535F85E   Revocation Date: Wed 03 Jan 2024 13:59:48 +0000
                          Serial: 018CCF9DB4F3225287190E207983CCC6BC83   Revocation Date: Wed 03 Jan 2024 13:59:48 +0000
                          Serial: 018CCF9F88D6B95D010F0D8B936EEFDF6FD5   Revocation Date: Wed 03 Jan 2024 17:38:48 +0000
                          Serial: 018CCF9F895E3121F718E8F1324610AB45AA   Revocation Date: Wed 03 Jan 2024 14:06:48 +0000
                          Serial: 018CCF9F89C585D9A0BCD14725310A6EDDD9   Revocation Date: Wed 03 Jan 2024 14:06:49 +0000
                          Serial: 018CCFA5F4BE983DCF1DAE0B4C1E81E229AE   Revocation Date: Wed 03 Jan 2024 17:38:48 +0000
                          Serial: 018CCFA5F639B426E3589EBF4BDC2DC15041   Revocation Date: Wed 03 Jan 2024 17:38:48 +0000
                          Serial: 018CD0680A34A0DA89CB2DE8B87D00691ECE   Revocation Date: Wed 03 Jan 2024 17:43:48 +0000
                          Serial: 018CD0680B0F4A8720DC5AF0F637F45619DE   Revocation Date: Wed 03 Jan 2024 17:43:48 +0000
                          Serial: 018CD06C9E0AAD4CA5584EFC8D6886807E54   Revocation Date: Wed 03 Jan 2024 17:46:48 +0000
Validation:               N/A
```

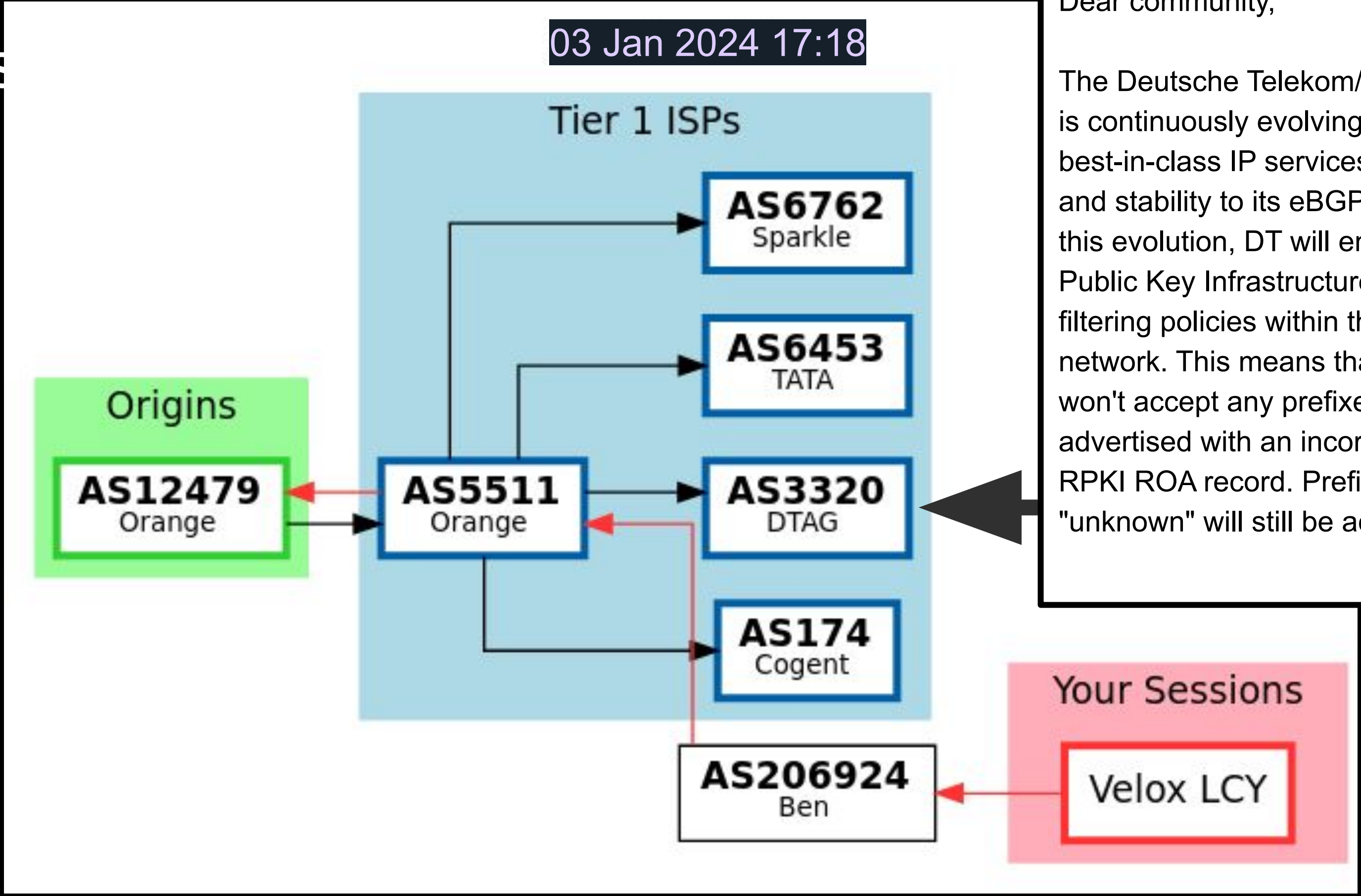
Woops!

- RIPE NCC does not enforce 2FA for users with assets
- RIPE NCC does not have a way to force all members of an account to use 2FA
- It seems to have taken a long time for RIPE and/or Orange to react to this incident
- Their NCC account should not have also been compromised by malware (easier said than done) and certainly shouldn't have had the password of "`ripeadmin`"
- This also exposed who is not RPKI filtering towards Orange

Woops


03 Jan 2024 17:18

Woops



03 Jan 2024 17:18

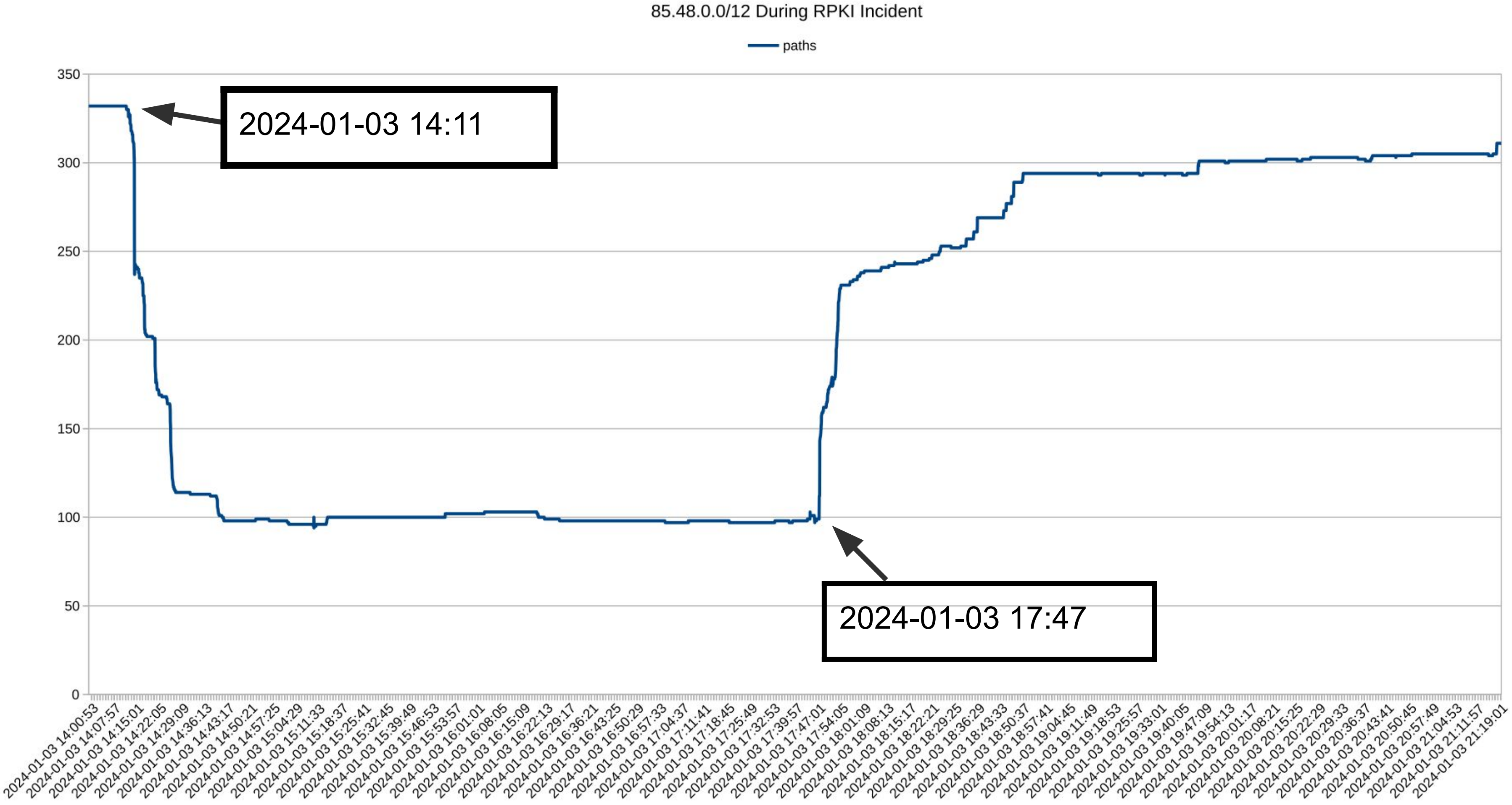
Dear community,

The Deutsche Telekom/AS3320 network is continuously evolving to provide best-in-class IP services, connectivity, and stability to its eBGP peers. As part of this evolution, DT will enable Resource Public Key Infrastructure (RPKI) based filtering policies within the AS3320 network. This means that in the future we won't accept any prefixes that are advertised with an incorrect matching RPKI ROA record. Prefixes validated as "unknown" will still be accepted.

Two possible takeaways

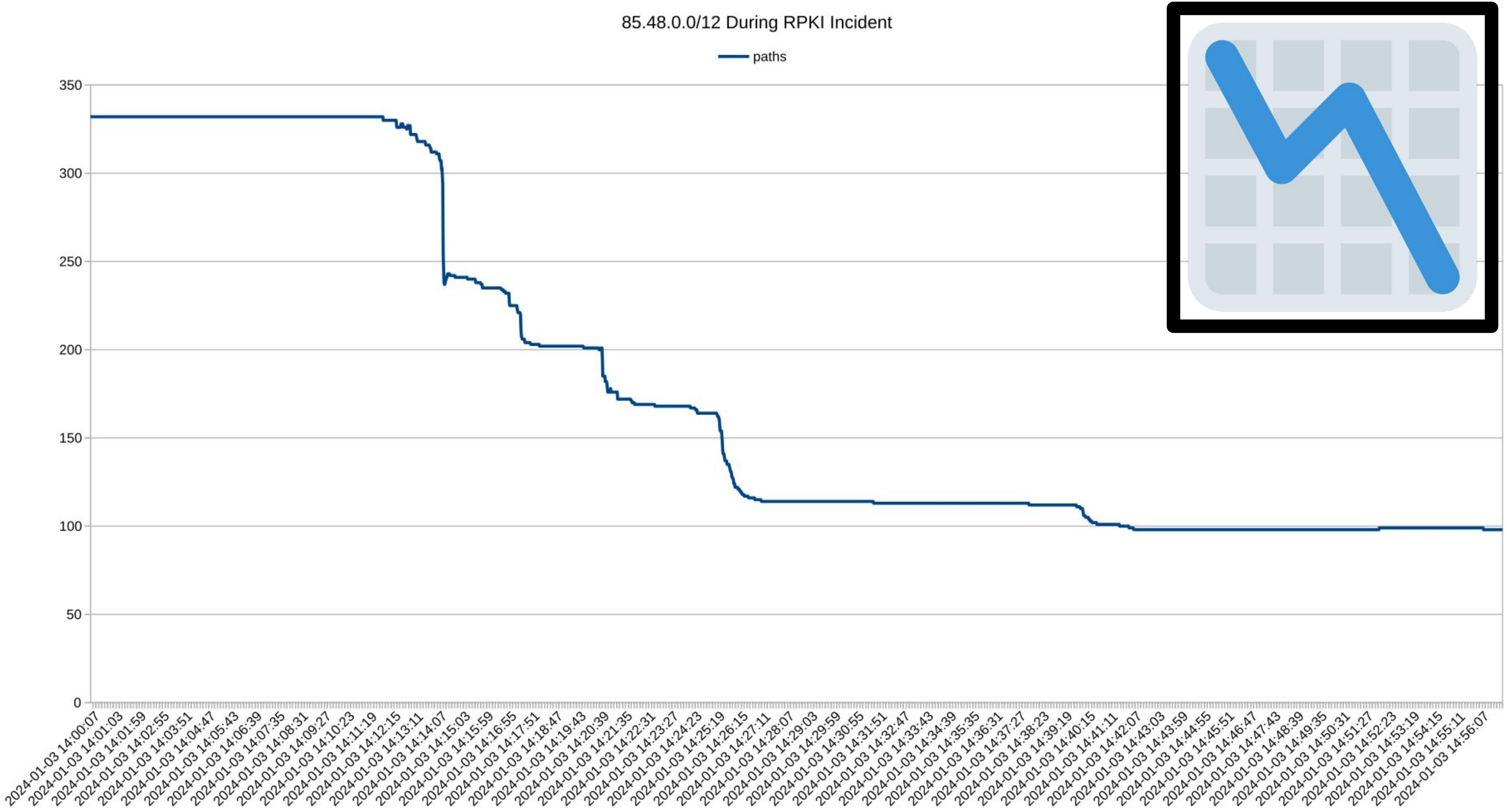
- How fast did networks drop/restore?
- How do you fix stuff like this in a emergency?

How fast did networks drop/restore?

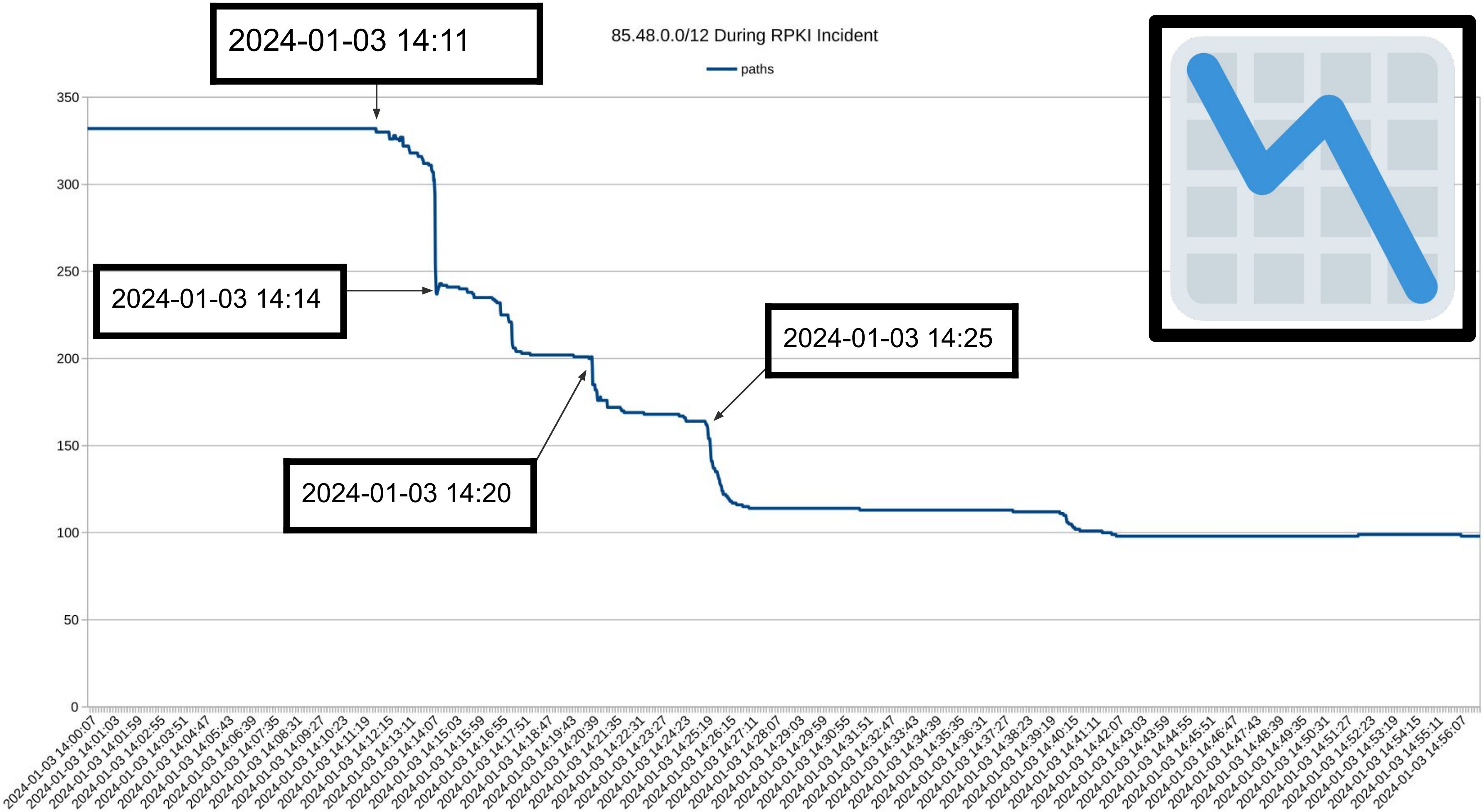


2024-01-03 14:11

2024-01-03 17:47



85.48.0.0/12 During RPKI Incident



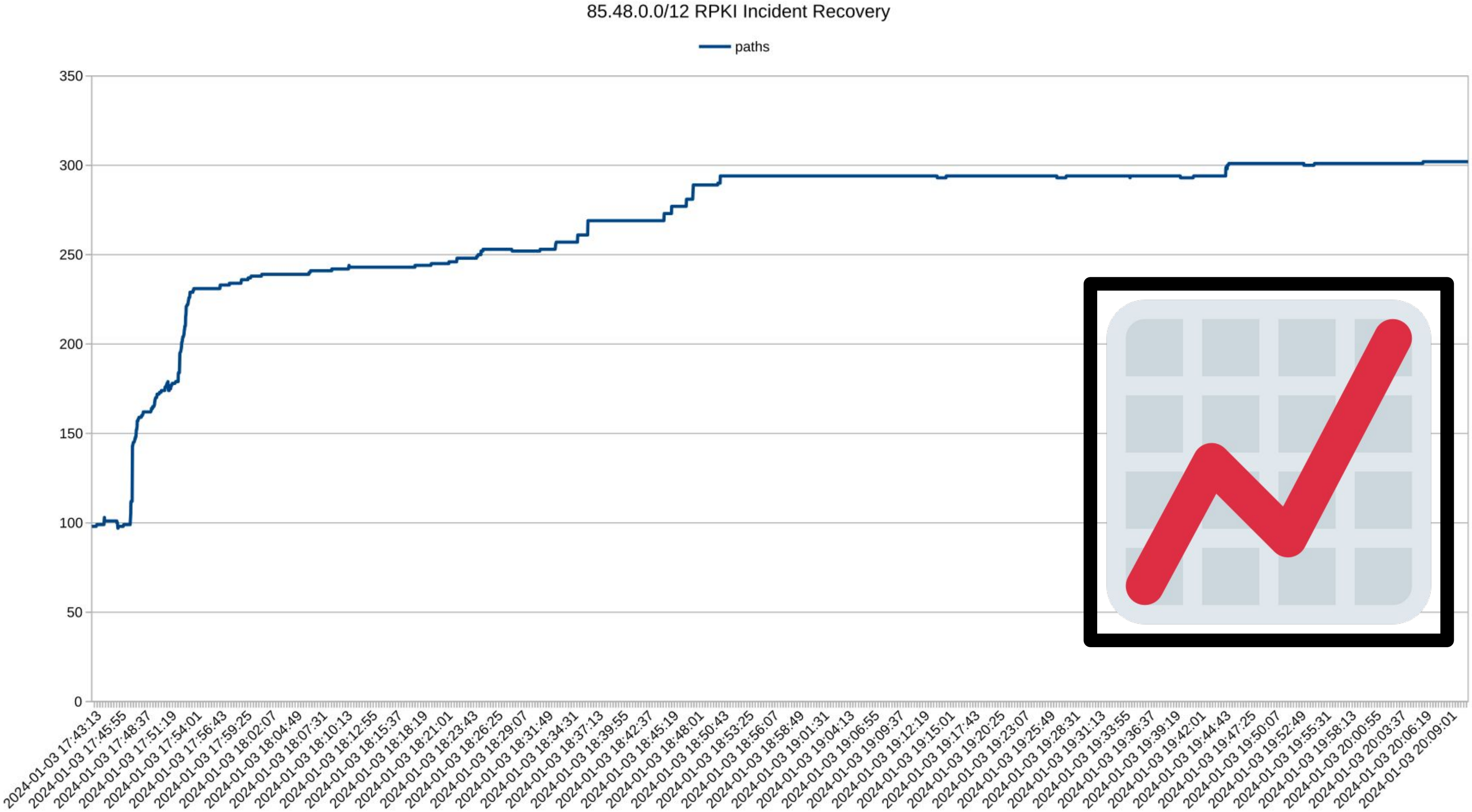
85.48.0.0/12 During RPKI Incident

2024-01-03 14:11

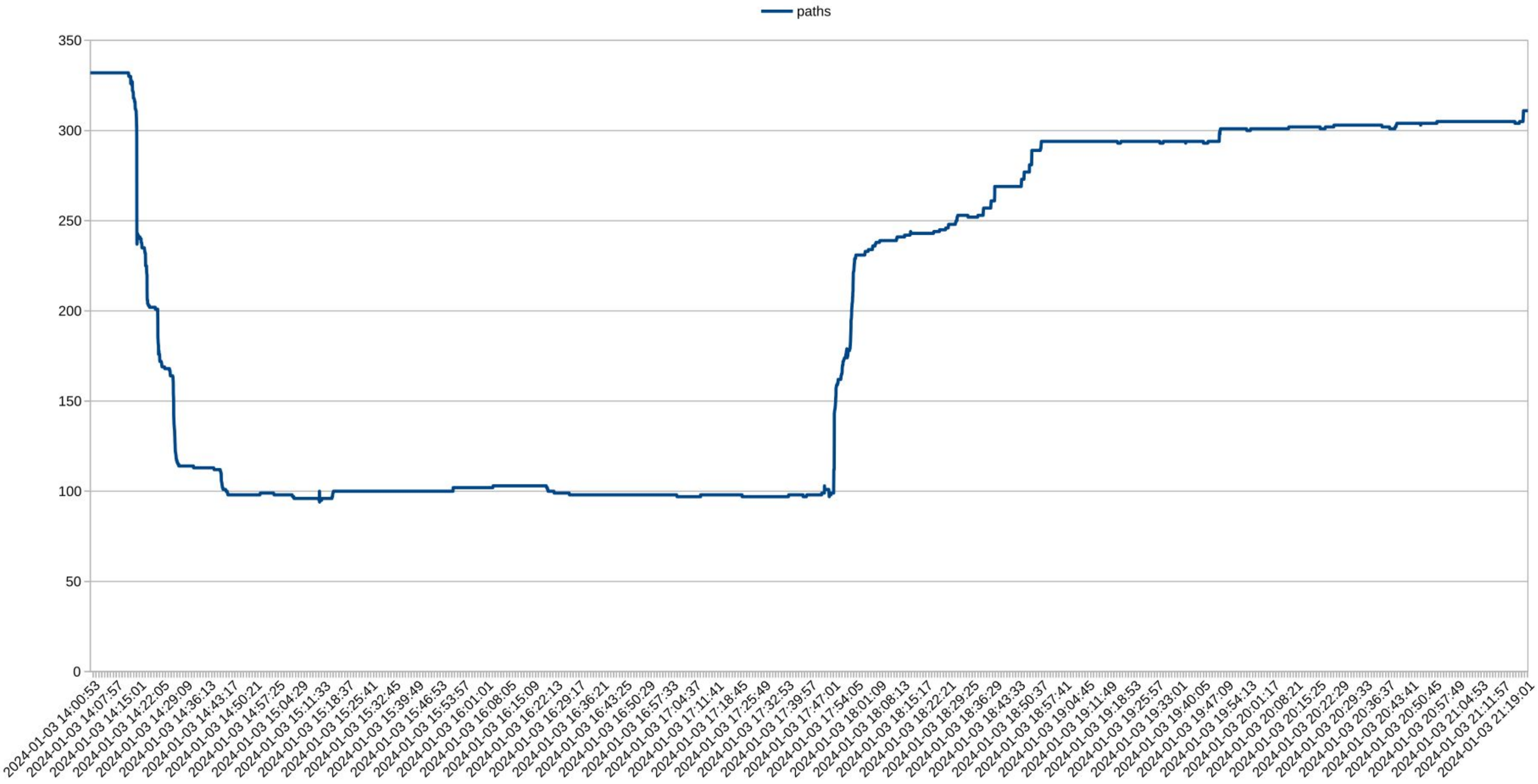
2024-01-03 14:14

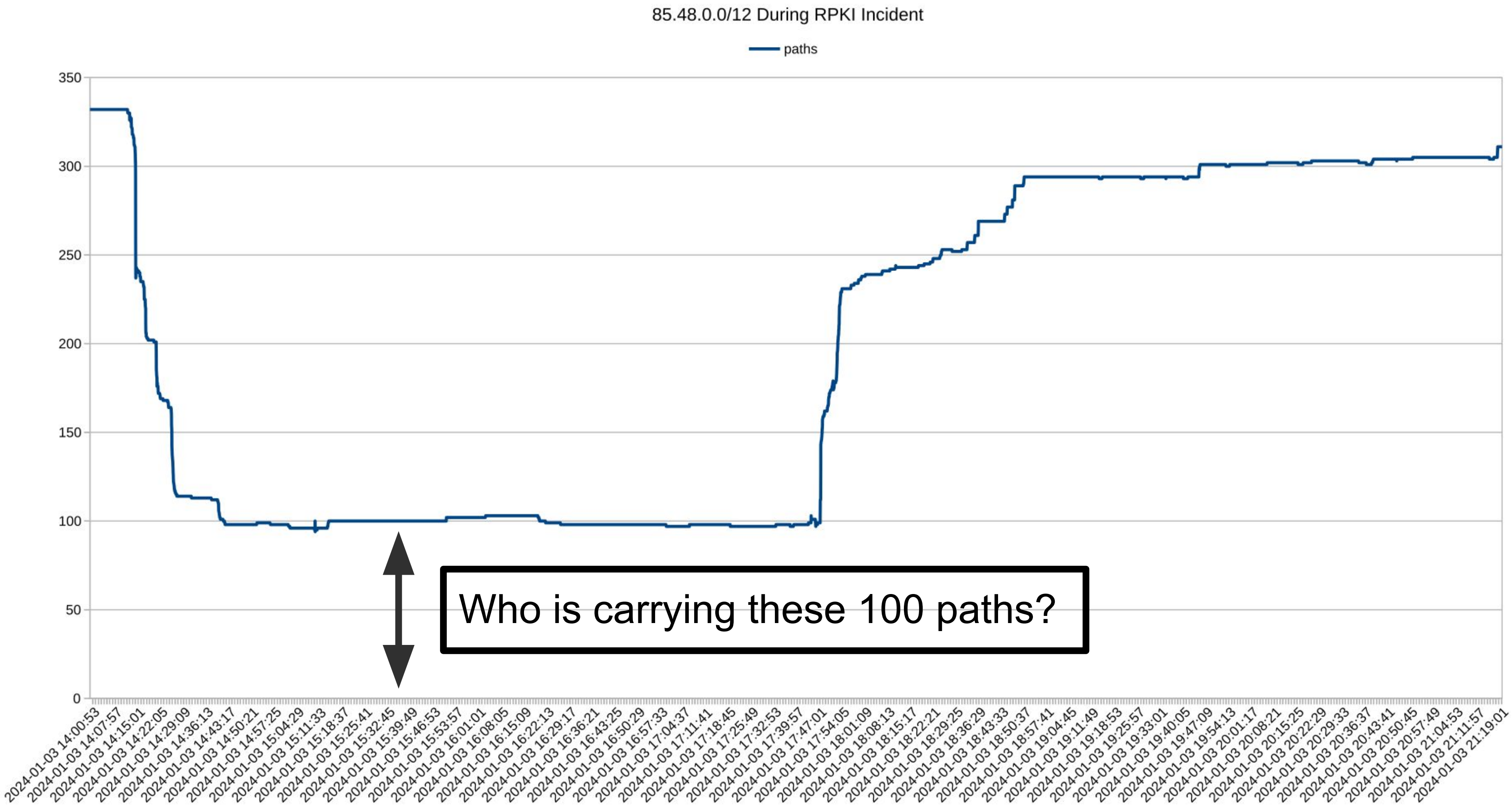
2024-01-03 14:20

2024-01-03 14:25


85.48.0.0/12 RPKI Incident Recovery
paths
350
300
250
200
150
100
50
0
2024-01-03 17:43:13
2024-01-03 17:45:55
2024-01-03 17:48:37
2024-01-03 17:51:19
2024-01-03 17:54:01
2024-01-03 17:56:43
2024-01-03 17:59:25
2024-01-03 18:02:07
2024-01-03 18:04:49
2024-01-03 18:07:31
2024-01-03 18:10:13
2024-01-03 18:12:55
2024-01-03 18:15:37
2024-01-03 18:18:19
2024-01-03 18:21:01
2024-01-03 18:23:43
2024-01-03 18:26:25
2024-01-03 18:29:07
2024-01-03 18:31:49
2024-01-03 18:34:31
2024-01-03 18:37:13
2024-01-03 18:39:55
2024-01-03 18:42:37
2024-01-03 18:45:19
2024-01-03 18:48:01
2024-01-03 18:50:43
2024-01-03 18:53:25
2024-01-03 18:56:07
2024-01-03 18:58:49
2024-01-03 19:01:31
2024-01-03 19:04:13
2024-01-03 19:06:55
2024-01-03 19:09:37
2024-01-03 19:12:19
2024-01-03 19:15:01
2024-01-03 19:17:43
2024-01-03 19:20:25
2024-01-03 19:23:07
2024-01-03 19:25:49
2024-01-03 19:28:31
2024-01-03 19:31:13
2024-01-03 19:33:55
2024-01-03 19:36:37
2024-01-03 19:39:19
2024-01-03 19:42:01
2024-01-03 19:44:43
2024-01-03 19:47:25
2024-01-03 19:50:07
2024-01-03 19:52:49
2024-01-03 19:55:31
2024-01-03 19:58:13
2024-01-03 20:00:55
2024-01-03 20:03:37
2024-01-03 20:06:19
2024-01-03 20:09:01

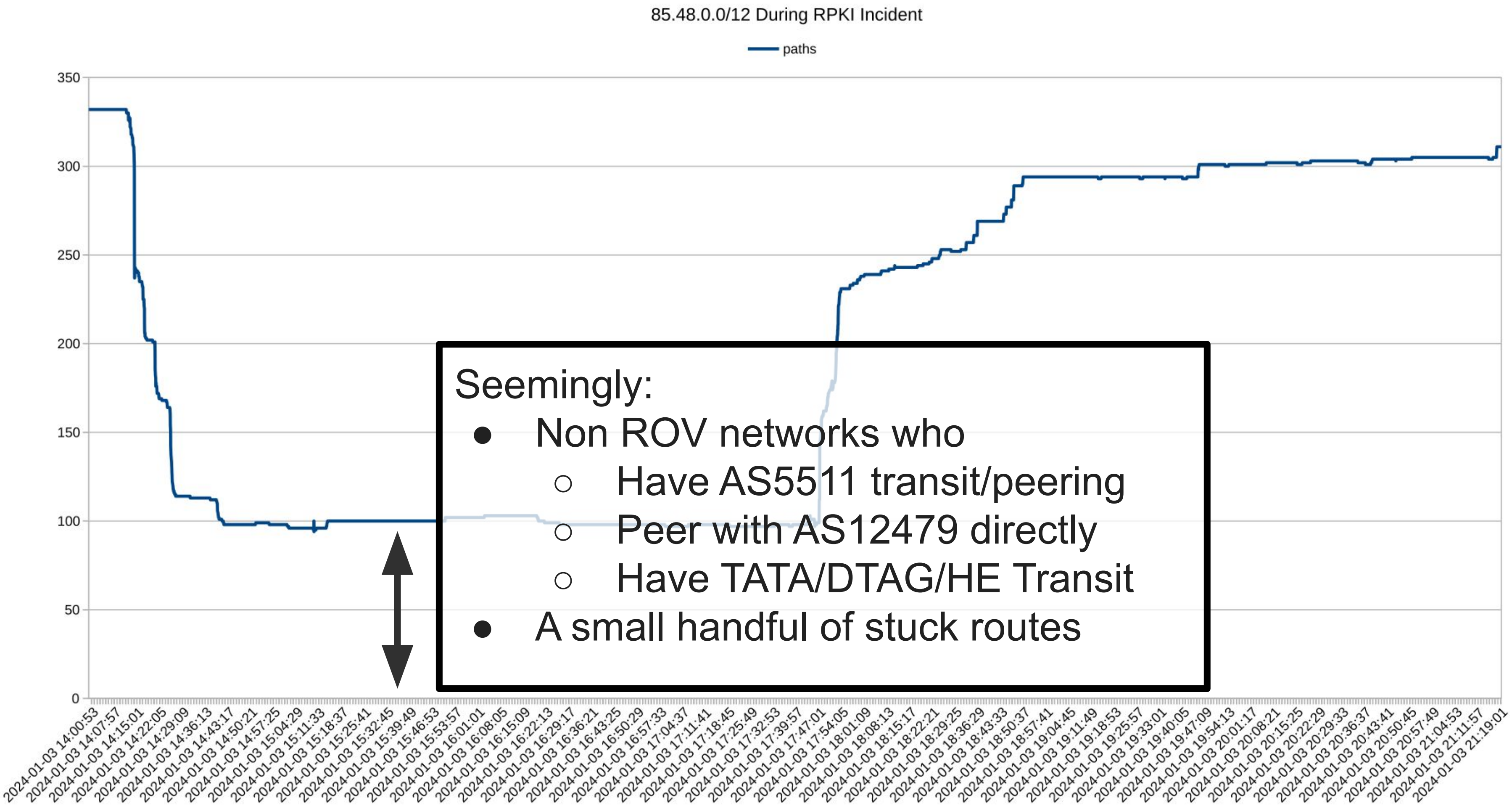
85.48.0.0/12 During RPKI Incident





85.48.0.0/12 During RPKI Incident

Who is carrying these 100 paths?



Seemingly:

- Non ROV networks who
  - Have AS5511 transit/peering
  - Peer with AS12479 directly
  - Have TATA/DTAG/HE Transit
- A small handful of stuck routes

How *could* you fix this problem in production?

S.L.U.R.M

Simplified

Local

Internet…

Number Resource Management

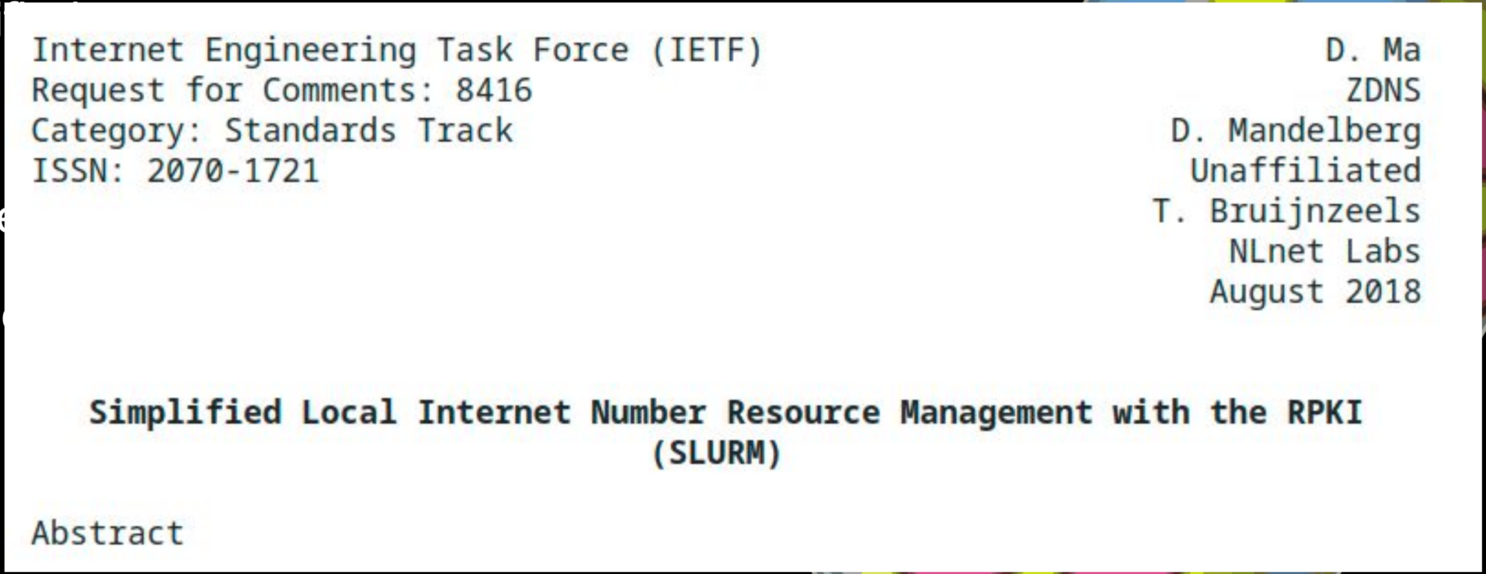
S.L.U.R.M

Simplif

Local

Interne

Numb



```
Internet Engineering Task Force (IETF)                             D. Ma
Request for Comments: 8416                                          ZDNS
Category: Standards Track                                  D. Mandelberg
ISSN: 2070-1721                                             Unaffiliated
                                                           T. Bruijnzeels
                                                              NLnet Labs
                                                             August 2018


   Simplified Local Internet Number Resource Management with the RPKI
                                (SLURM)

Abstract
```

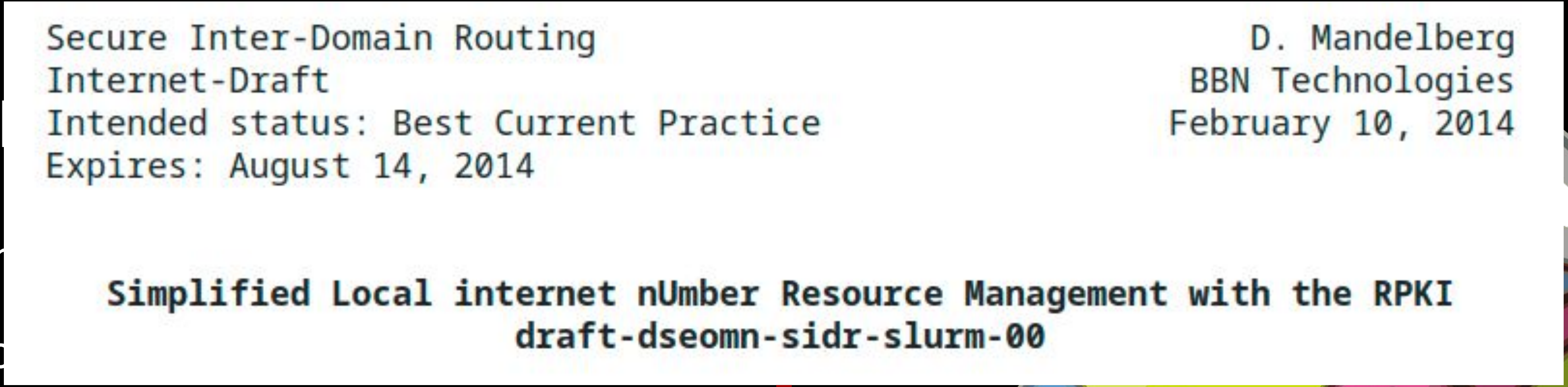
S.l

Sim

Loc

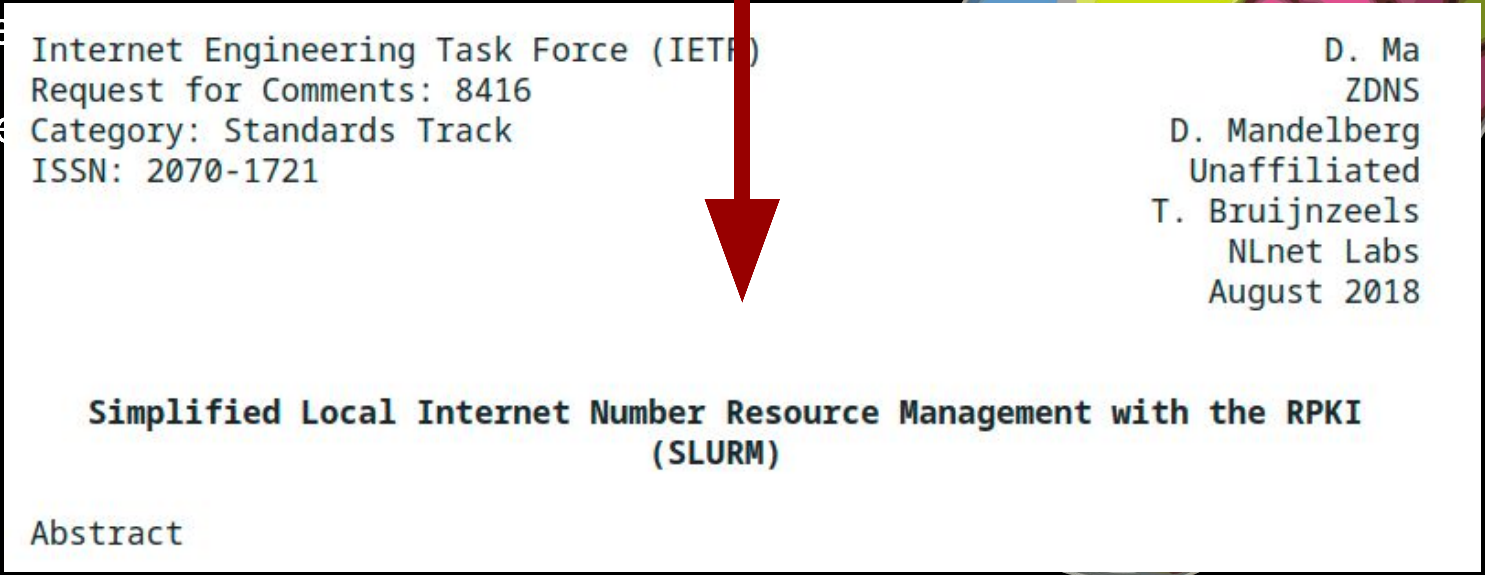
Interne

Numbe



```
Secure Inter-Domain Routing                                D. Mandelberg
Internet-Draft                                          BBN Technologies
Intended status: Best Current Practice                 February 10, 2014
Expires: August 14, 2014
```

Simplified Local internet nUmber Resource Management with the RPKI
draft-dseomn-sidr-slurm-00



```
Internet Engineering Task Force (IETF)                             D. Ma
Request for Comments: 8416                                          ZDNS
Category: Standards Track                                  D. Mandelberg
ISSN: 2070-1721                                              Unaffiliated
                                                            T. Bruijnzeels
                                                                NLnet Labs
                                                               August 2018
```

Simplified Local Internet Number Resource Management with the RPKI
(SLURM)

Abstract

SLURM lets you inject/filter RPKI data

- Filtering is useful for:
  - A customer who is calling you up urgently asking you to ignore RPKI for their prefixes because it's wrong (and the update may take up to 30 mins to properagte)
  - Handling known bad RPKI data from someone else (Like this Orange Incident)
- Injection is useful for:
  - Forcing your own routes to always be RPKI Valid,
  - Allowing your /32 blackhole routes to be RPKI valid (or other workaround/hacks)

SLURM Examples

ROAs for 10.0.0.0/24+AS65000 will be removed from the validator input

A ROA for

10.2.0.0/25{to 26}+AS65002

will always exist

```
{
 "slurmVersion": 1,
 "validationOutputFilters": {
   "prefixFilters": [
     {
       "asn": 65000,
       "prefix": "10.0.0.0/24"
     }
   ],
   "bgpsecFilters": []
 },
 "locallyAddedAssertions": {
   "prefixAssertions": [
     {
       "asn": 65002,
       "prefix": "10.2.0.0/25",
       "maxPrefixLength": 26
     }
   ]
 }
}
```

SLURM Support

- Routinator https://routinator.docs.nlnetlabs.nl/en/stable/local-exceptions.html
- StayRTR , add -slurm ./slurm.json to the process
- GoRTR, use StayRTR
- FORT, Ensure you are on a recent version, then check your docs

I cannot in good faith recommend other RPKI Validators/RTR Implementations right now

Takeaways

- Bad passwords are everywhere, **Use 2FA and enforce it with policy**
- Even if you don't validate ROV, your upstreams likely do
- You can mitigate incidents like this for yourself or customers with SLURM
- HE does not do ROV validation in the way you would expect
    - Either that or it's busted
- It takes longer for your prefixes to come back from a RPKI incident than it does for it to disappear

Takeaways

- Bad passwords are everywhere, **Use 2FA and enforce it with policy**
- Even if you don't validate ROV, your upstreams likely do
- You can mitigate incidents like this for yourself or customers with SLURM
- HE does not do ROV validation in the way you would expect
    - Either that or it's busted
- It takes longer for your prefixes to come back from a RPKI incident than it does for it to disappear
- And finally…

Feed more collectors!

More people should feed route collectors to help future research of incidents like this!

https://bgp.tools/kb/setup-sessions

https://github.com/routeviews/issues/issues

I legitimately could not figure out where RIS/Catchpoint/1000Eyes

bgp.tools's IX collector footprint

- 🇵🇱 THINX Warsaw
- 🇬🇧 LINX + LONAP
- 🇩🇪 DE-CIX - All Germany, New York, Chicago, Madrid, etc
- 🇧🇬 BIX
- 🇷🇸 SOX Serbia
- 🇩🇪 BCIX
- 🇸🇪 NETNOD Stockholm and Copenhagen
- 🇷🇴 InterLAN
- 🇳🇱 FrysIX + INTERIX
- 🇧🇷 IX.BR Sao Paulo
- 🇨🇿 NIX.CZ

More on:
https://bgp.tools/as/212232#ix

Thanks, Questions?

Private comments also accepted at admin+pd@bgp.tools