The State of DNSSEC in Switzerland

SWITCH

Michael Hausding

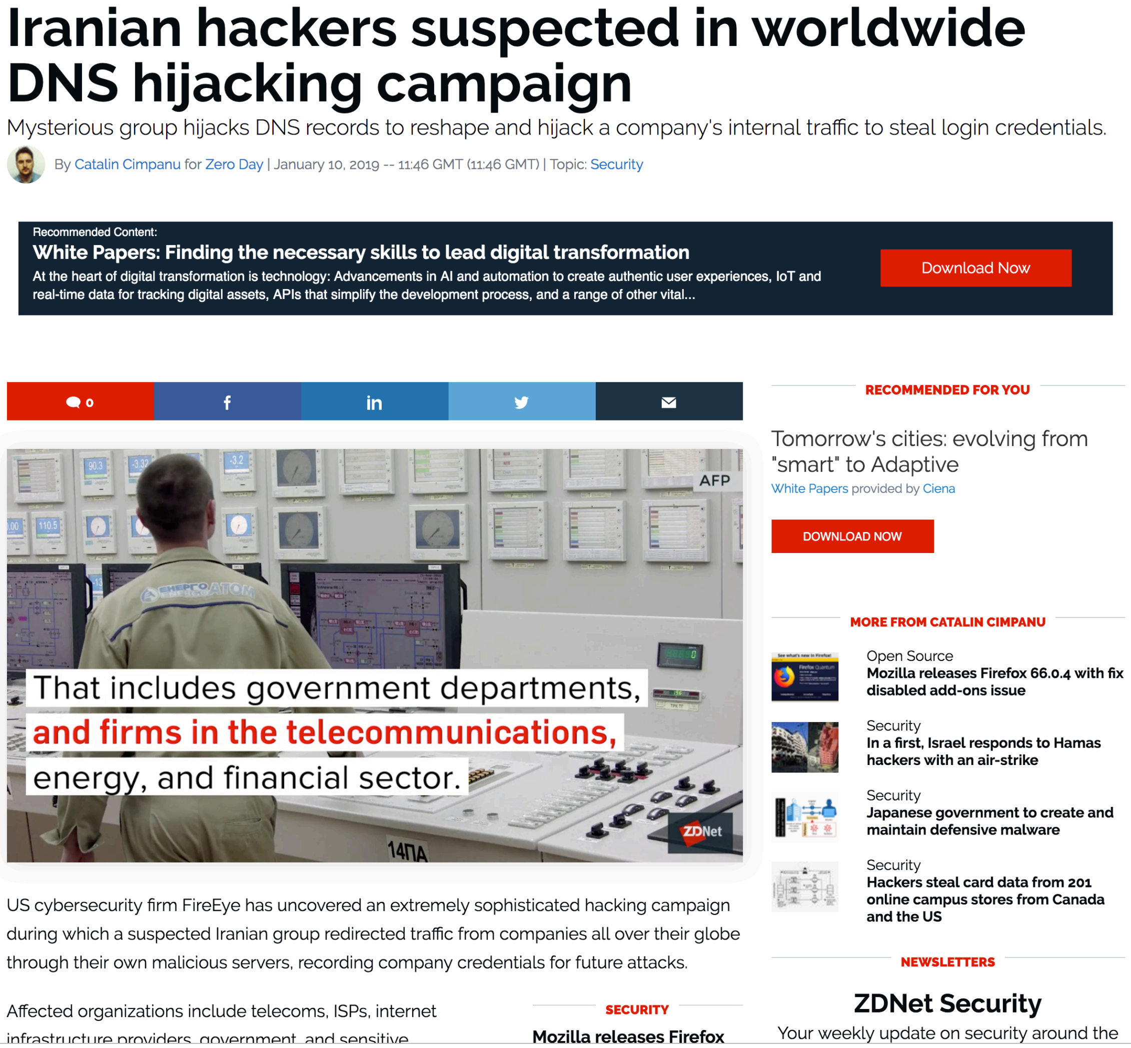
michael.hausding@switch.ch
@mhausding

SWINOG, Bern 8.5.2019

LOS ANGELES – 22 February 2019

The Internet Corporation for Assigned Names and Numbers (ICANN) believes that there is an ongoing and significant risk to key parts of the Domain Name System (DNS) infrastructure.

In the context of increasing reports of malicious activity targeting the DNS infrastructure, ICANN is calling for full deployment of the Domain Name System Security Extensions (DNSSEC) across all unsecured domain names.



Iranian hackers suspected in worldwide DNS hijacking campaign

Mysterious group hijacks DNS records to reshape and hijack a company's internal traffic to steal login credentials.

By Catalin Cimpanu for Zero Day | January 10, 2019 -- 11:46 GMT (11:46 GMT) | Topic: Security

0
AFP
That includes government departments,
and firms in the telecommunications,
energy, and financial sector.
ZDNet

US cybersecurity firm FireEye has uncovered an extremely sophisticated hacking campaign during which a suspected Iranian group redirected traffic from companies all over their globe through their own malicious servers, recording company credentials for future attacks.

Affected organizations include telecoms, ISPs, internet infrastructure providers, government, and sensitive

SECURITY

Mozilla releases Firefox

MORE FROM CATALIN CIMPANU

Open Source
Mozilla releases Firefox 66.0.4 with fix disabled add-ons issue

Security
In a first, Israel responds to Hamas hackers with an air-strike

Security
Japanese government to create and maintain defensive malware

Security
Hackers steal card data from 201 online campus stores from Canada and the US

NEWSLETTERS

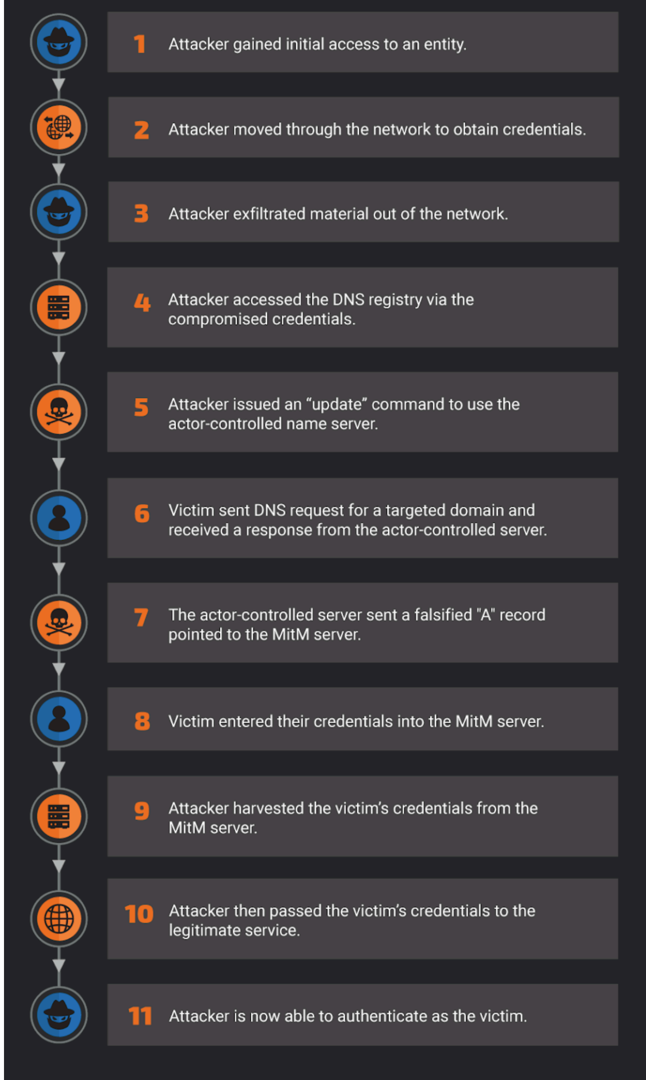
ZDNet Security

Your weekly update on security around the

- Attacks on the DNS are real
- No detection for months
- DNSSEC is a means to secure the integrity of the DNS
- TLS, 2FA do not protect you if attackers control your DNS!

https://www.icann.org/news/announcement-2019-02-22-en

https://blog.talosintelligence.com/2019/04/seaturtle.html



1 Attacker gained initial access to an entity.

2 Attacker moved through the network to obtain credentials.

3 Attacker exfiltrated material out of the network.

4 Attacker accessed the DNS registry via the compromised credentials.

5 Attacker issued an “update” command to use the actor-controlled name server.

6 Victim sent DNS request for a targeted domain and received a response from the actor-controlled server.

7 The actor-controlled server sent a falsified "A" record pointed to the MitM server.

8 Victim entered their credentials into the MitM server.

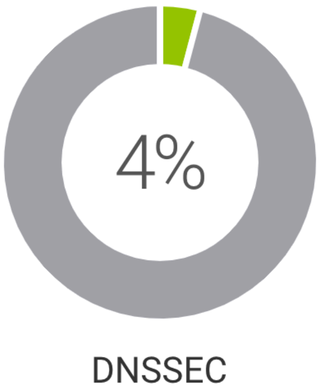
9 Attacker harvested the victim’s credentials from the MitM server.

10 Attacker then passed the victim’s credentials to the legitimate service.

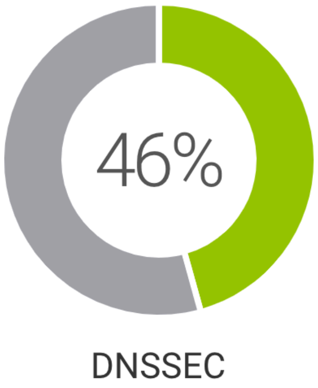
11 Attacker is now able to authenticate as the victim.

DNSSEC signed domain names (Top 1000)

.ch

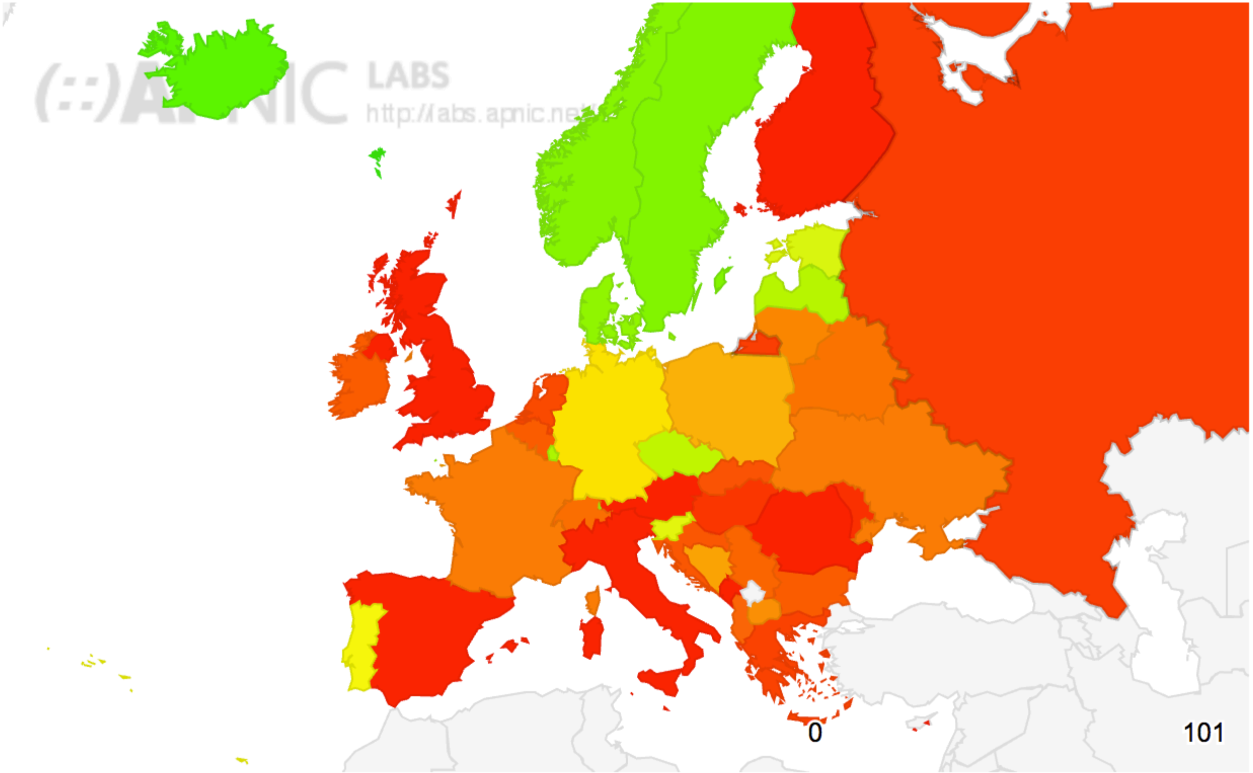


.se



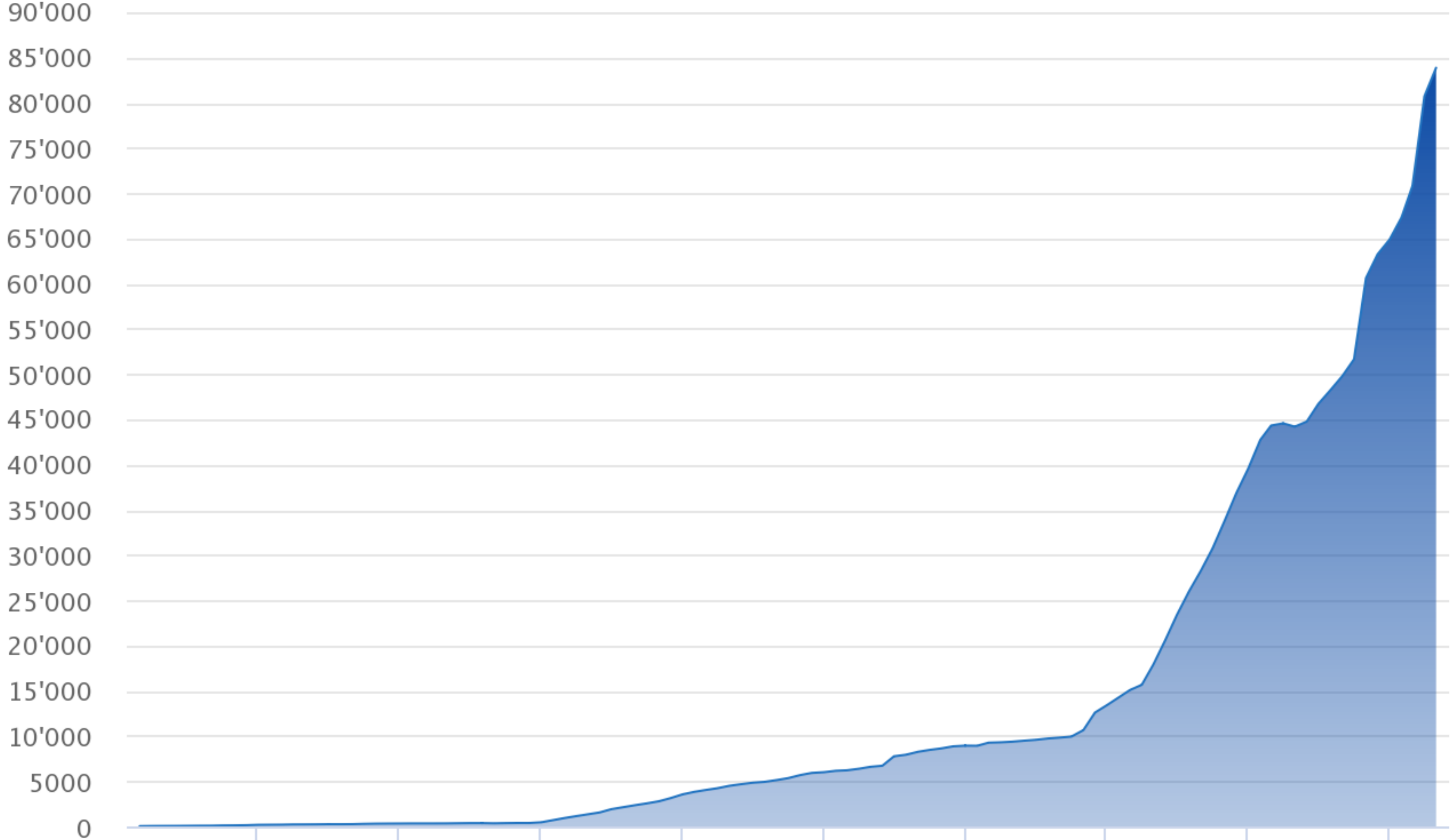
DNSSEC Validation

Region Map for Europe (150)



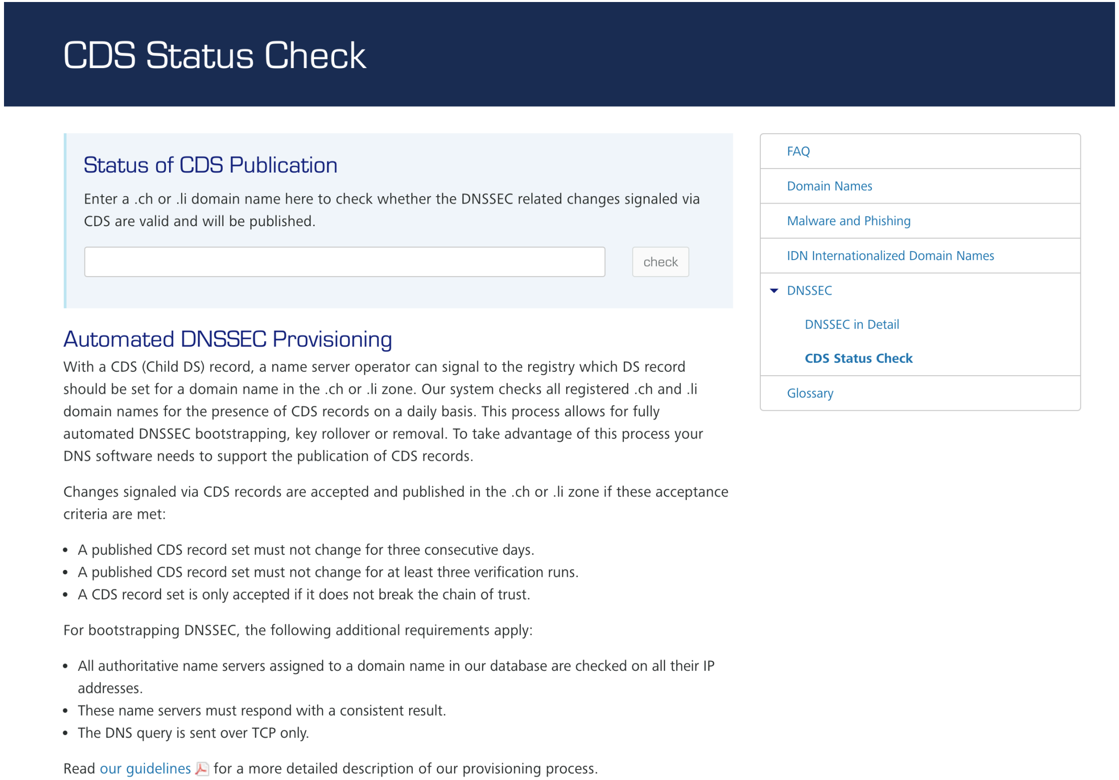
Signed .ch domains

Anzahl .ch-Domain-Namen mit DNSSEC



© SWITCH

Child DS (CDS)



CDS Status Check

Status of CDS Publication

Enter a .ch or .li domain name here to check whether the DNSSEC related changes signaled via CDS are valid and will be published.

Automated DNSSEC Provisioning

With a CDS (Child DS) record, a name server operator can signal to the registry which DS record should be set for a domain name in the .ch or .li zone. Our system checks all registered .ch and .li domain names for the presence of CDS records on a daily basis. This process allows for fully automated DNSSEC bootstrapping, key rollover or removal. To take advantage of this process your DNS software needs to support the publication of CDS records.

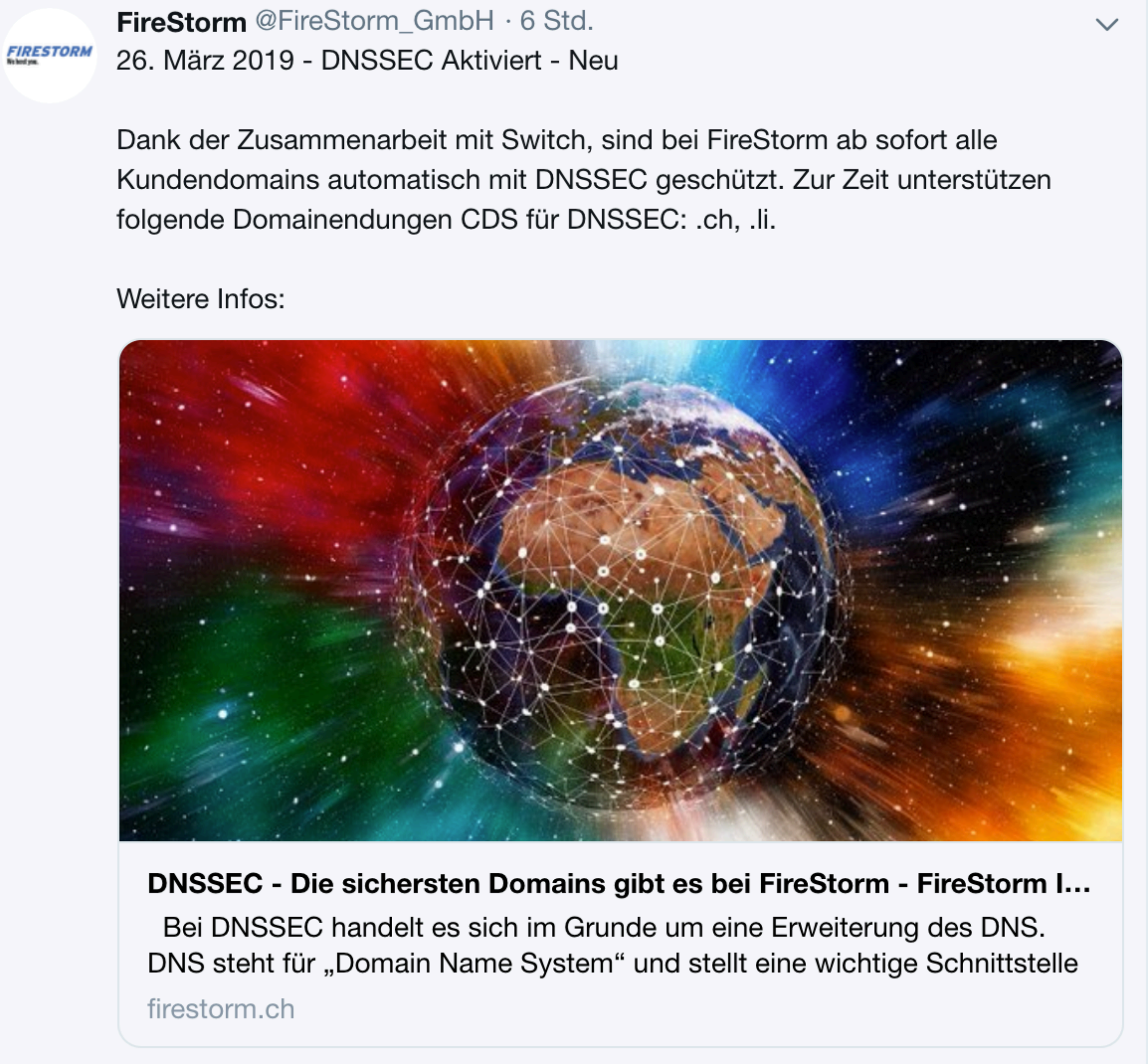
Changes signaled via CDS records are accepted and published in the .ch or .li zone if these acceptance criteria are met:

- A published CDS record set must not change for three consecutive days.
- A published CDS record set must not change for at least three verification runs.
- A CDS record set is only accepted if it does not break the chain of trust.

For bootstrapping DNSSEC, the following additional requirements apply:

- All authoritative name servers assigned to a domain name in our database are checked on all their IP addresses.
- These name servers must respond with a consistent result.
- The DNS query is sent over TCP only.

Read our guidelines for a more detailed description of our provisioning process.



FireStorm @FireStorm_GmbH · 6 Std.

26. März 2019 - DNSSEC Aktiviert - Neu

Dank der Zusammenarbeit mit Switch, sind bei FireStorm ab sofort alle Kundendomains automatisch mit DNSSEC geschützt. Zur Zeit unterstützen folgende Domainendungen CDS für DNSSEC: .ch, .li.

Weitere Infos:

DNSSEC - Die sichersten Domains gibt es bei FireStorm - FireStorm I...

Bei DNSSEC handelt es sich im Grunde um eine Erweiterung des DNS. DNS steht für „Domain Name System“ und stellt eine wichtige Schnittstelle

firestorm.ch

Signed .ch Domain Namen

admin.ch

search.ch

switch.ch

teletext.ch

open.ch, oetiker.ch

gmx.ch, protonmail.ch, posteo-dns.ch

iway.ch, interway.ch, internezohosting.ch, netzone.ch, csti.ch

unibe.ch, hefr.ch, heia-fr.ch

evoting.ch

gkb.ch

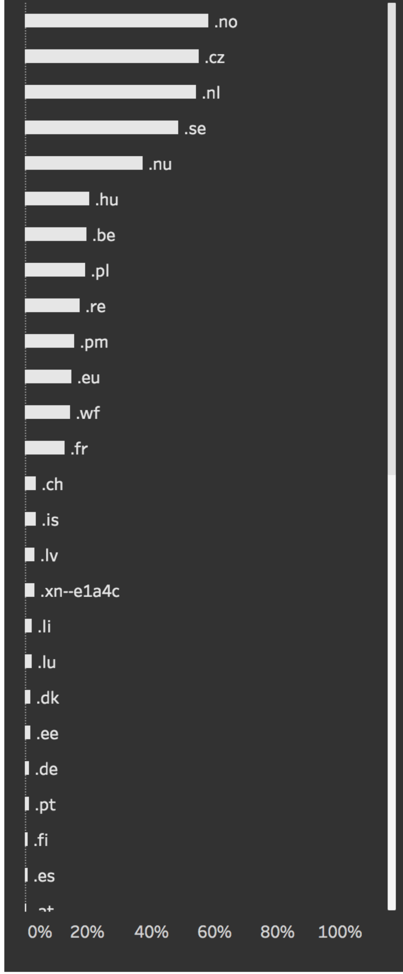
DNSSEC signing in Switzerland

- Total number of DNSSEC signed .ch domain names rises
- Tool support is available and mature
- CDS helps to automate signing
- Signing all new registrations by default (Infomaniak)
- Signing complete portfolio (FireStorm)

- We need more hosters signing their domain names!

RANKS

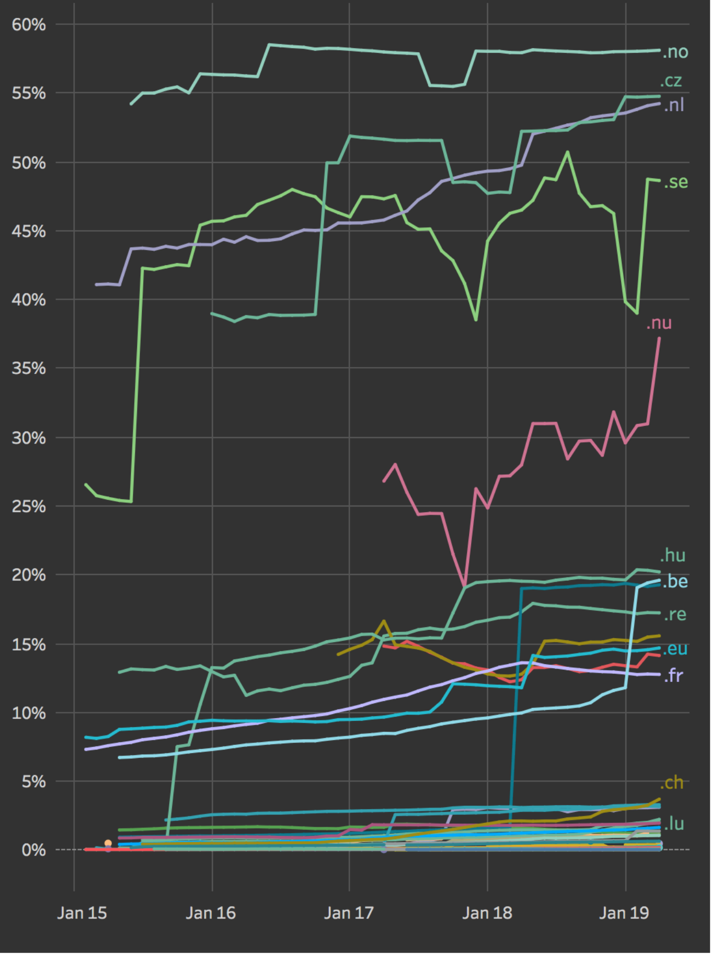
DNSSEC (% domains) Apr 19



TRENDS

DNSSEC (% domains)

Feb 15 to Apr 19

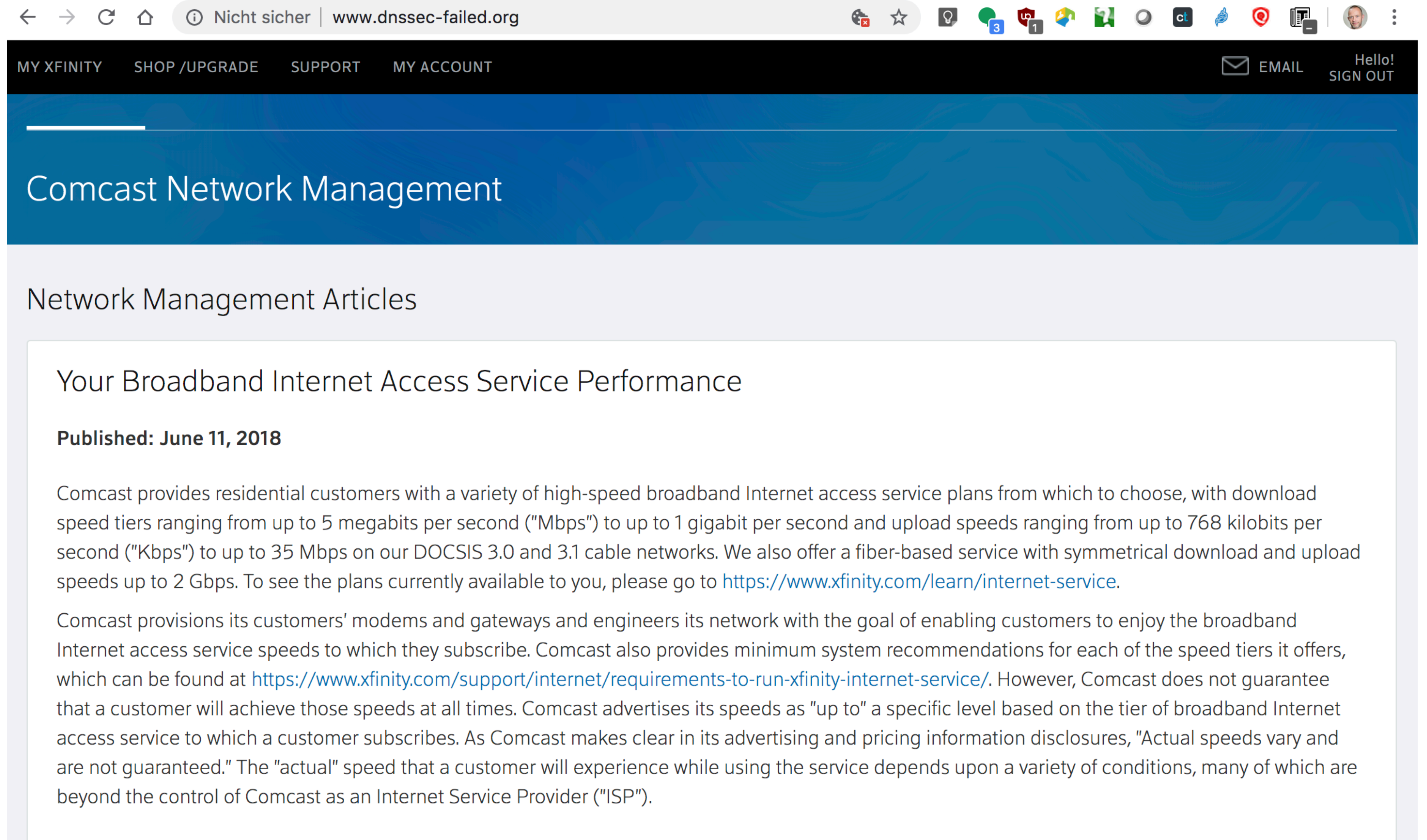


Validation Rate in Switzerland

How to measure DNSSEC Validation?

- Browse to dnssec-failed.org
- Browser based measurements with ads
- RIPE Atlas
- DS requests on authoritative DNS server
- dig

dnssec-failed.org



Comcast Network Management

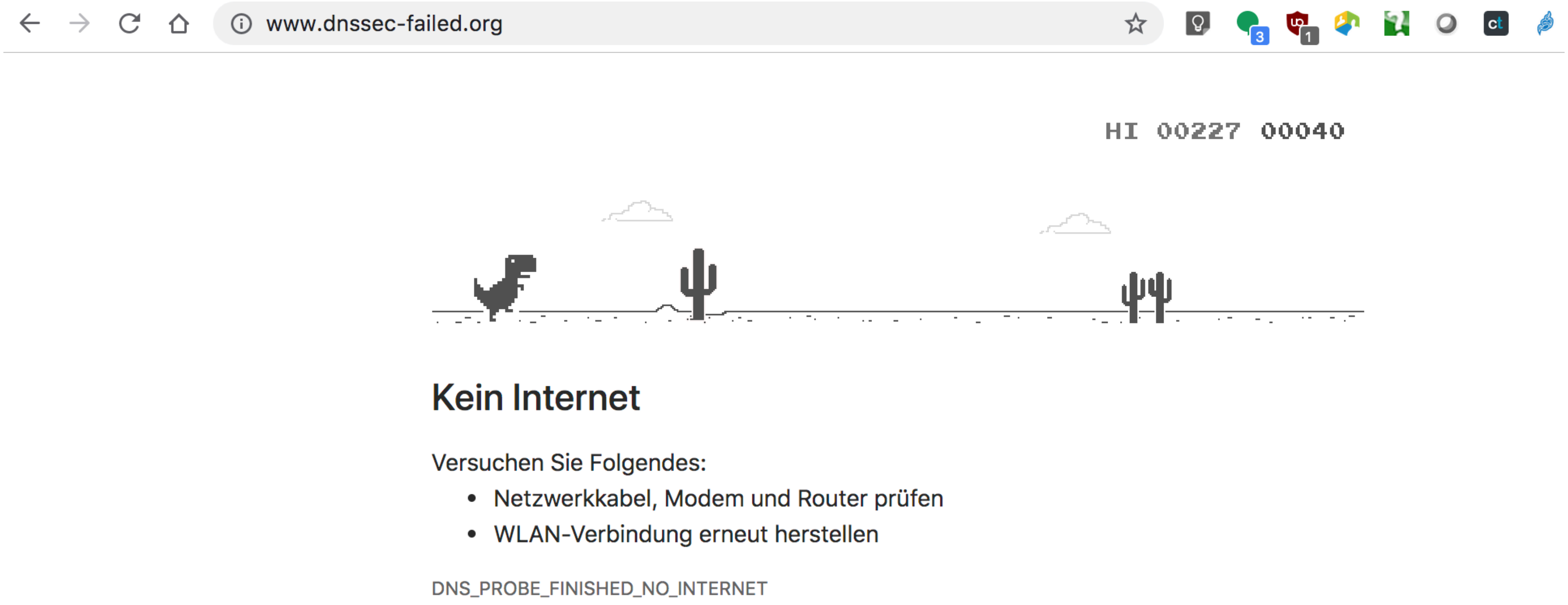
Network Management Articles

Your Broadband Internet Access Service Performance

Published: June 11, 2018

Comcast provides residential customers with a variety of high-speed broadband Internet access service plans from which to choose, with download speed tiers ranging from up to 5 megabits per second ("Mbps") to up to 1 gigabit per second and upload speeds ranging from up to 768 kilobits per second ("Kbps") to up to 35 Mbps on our DOCSIS 3.0 and 3.1 cable networks. We also offer a fiber-based service with symmetrical download and upload speeds up to 2 Gbps. To see the plans currently available to you, please go to https://www.xfinity.com/learn/internet-service.

Comcast provisions its customers' modems and gateways and engineers its network with the goal of enabling customers to enjoy the broadband Internet access service speeds to which they subscribe. Comcast also provides minimum system recommendations for each of the speed tiers it offers, which can be found at https://www.xfinity.com/support/internet/requirements-to-run-xfinity-internet-service/. However, Comcast does not guarantee that a customer will achieve those speeds at all times. Comcast advertises its speeds as "up to" a specific level based on the tier of broadband Internet access service to which a customer subscribes. As Comcast makes clear in its advertising and pricing information disclosures, "Actual speeds vary and are not guaranteed." The "actual" speed that a customer will experience while using the service depends upon a variety of conditions, many of which are beyond the control of Comcast as an Internet Service Provider ("ISP").



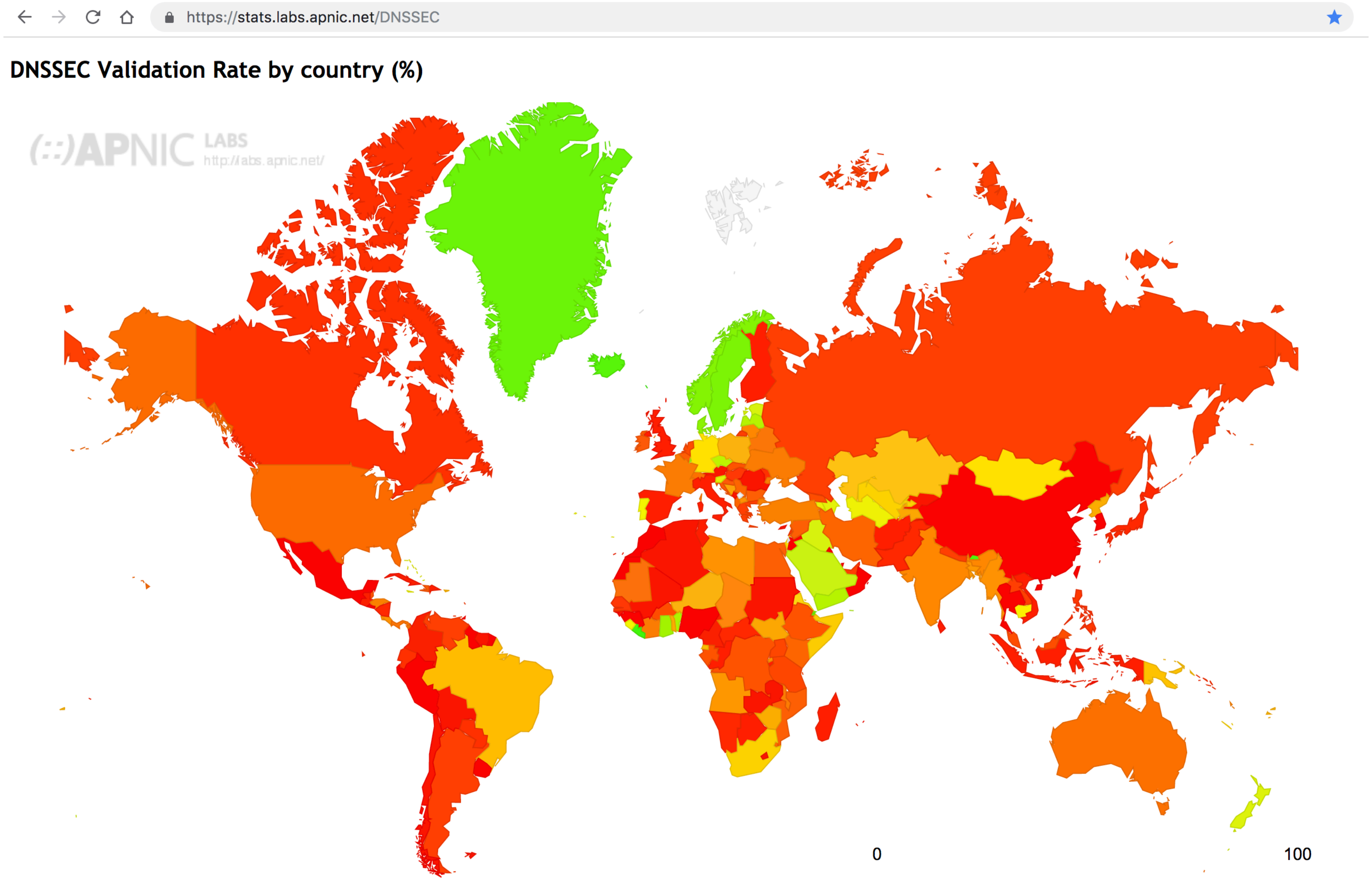
Kein Internet

Versuchen Sie Folgendes:

- Netzwerkkabel, Modem und Router prüfen
- WLAN-Verbindung erneut herstellen

DNS_PROBE_FINISHED_NO_INTERNET

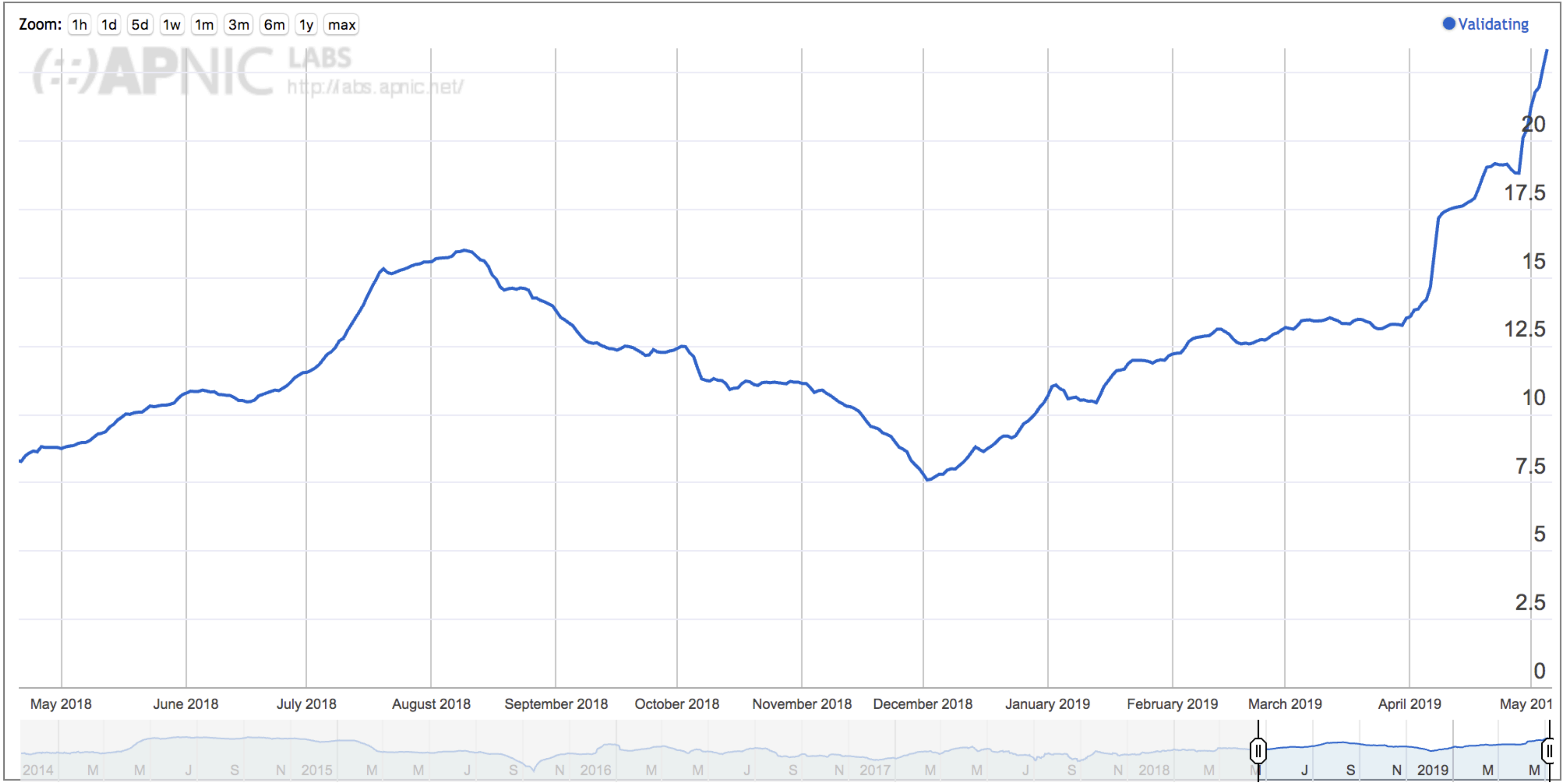
Browser based measurements from APNIC



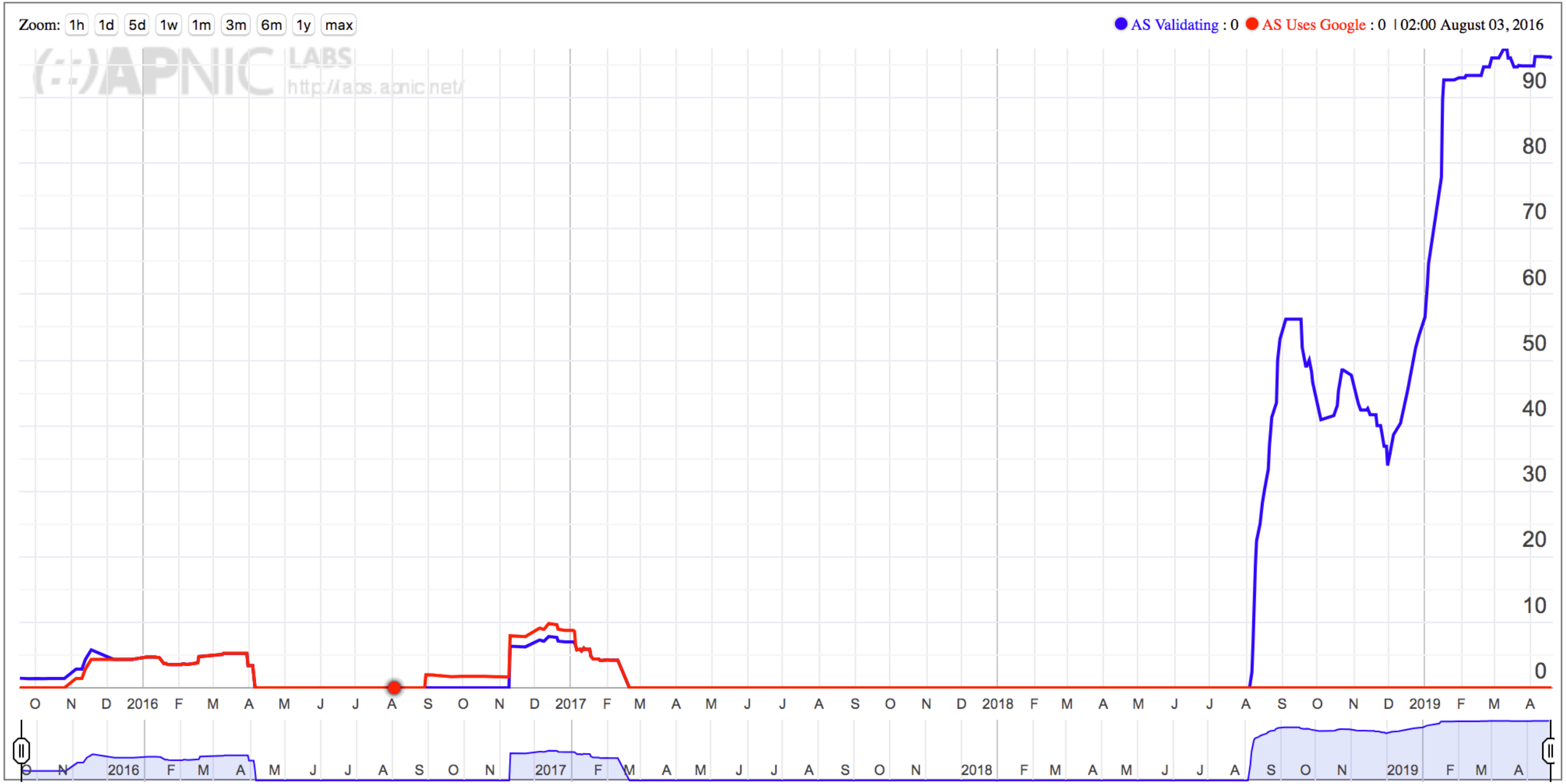
https://stats.labs.apnic.net/DNSSEC

DNSSEC Validation Rate by country (%)

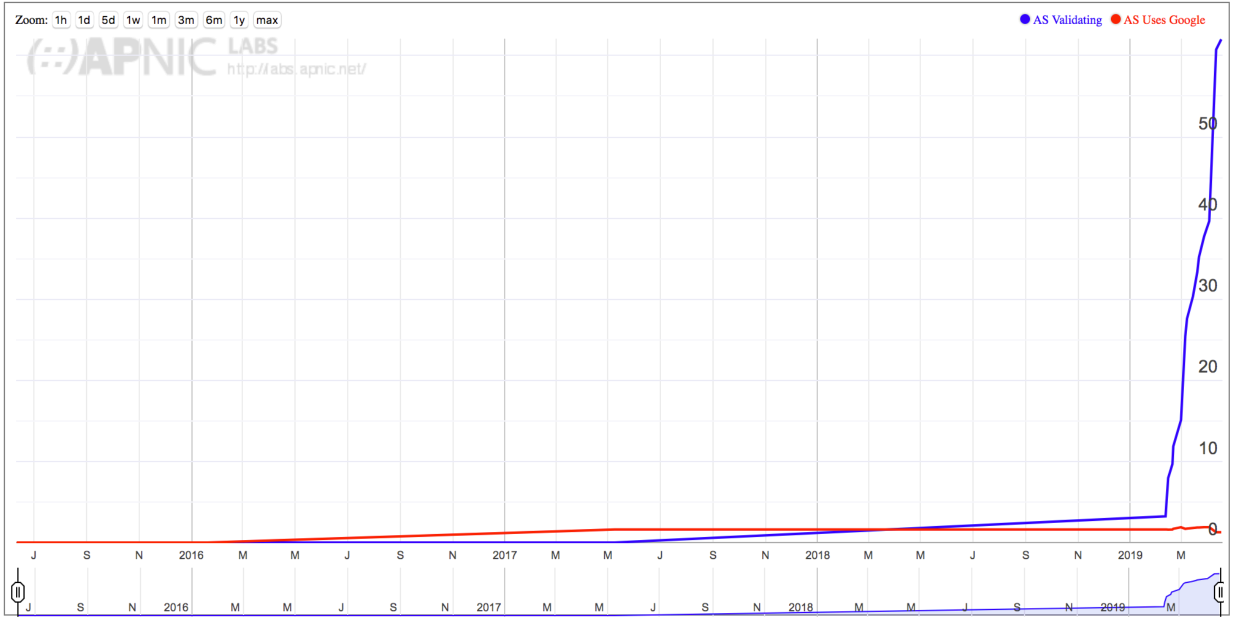
Use of DNSSEC Validation for Switzerland (CH)



DNSSEC Per-Country Deployment for AS33845: SWISSGOV, Switzerland (CH)


Zoom: 1h 1d 5d 1w 1m 3m 6m 1y max
● AS Validating : 0 ● AS Uses Google : 0 | 02:00 August 03, 2016
APNIC LABS http://labs.apnic.net/
90
80
70
60
50
40
30
20
10
0
O N D 2016 F M A M J J A S O N D 2017 F M A M J J A S O N D 2018 F M A M J J A S O N D 2019 F M A
O N 2016 F M A M J J A S O N 2017 F M A M J J A S O N 2018 F M A M J J A S O N 2019 F M A

DNSSEC Per-Country Deployment for AS12511: CH-POSTNETZ Post CH AG, Switzerland (CH)



Average Interval (days) 10

□ Show country ASN List

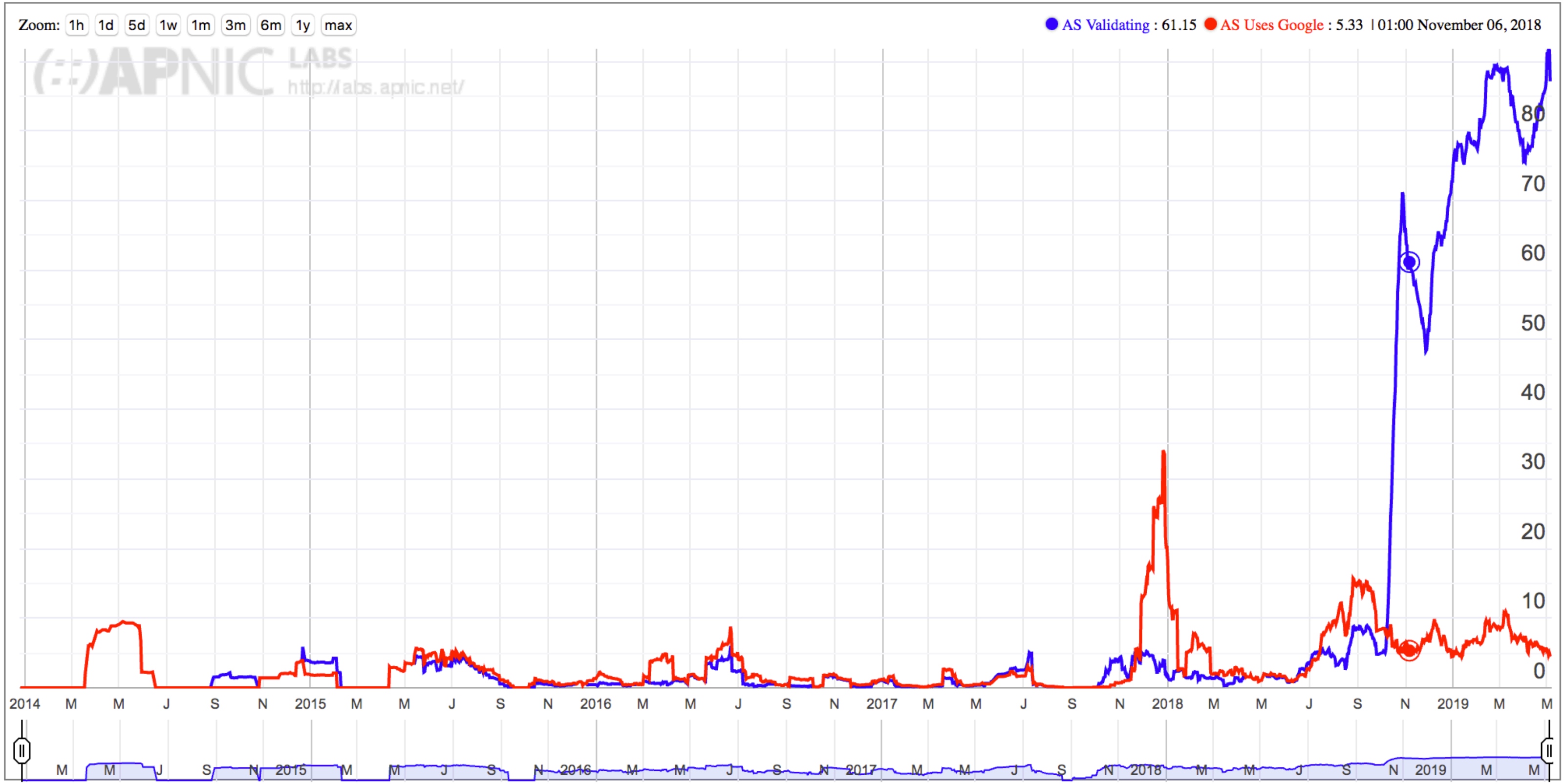
□ Hide Google PDNS Use

□ Show Country Totals

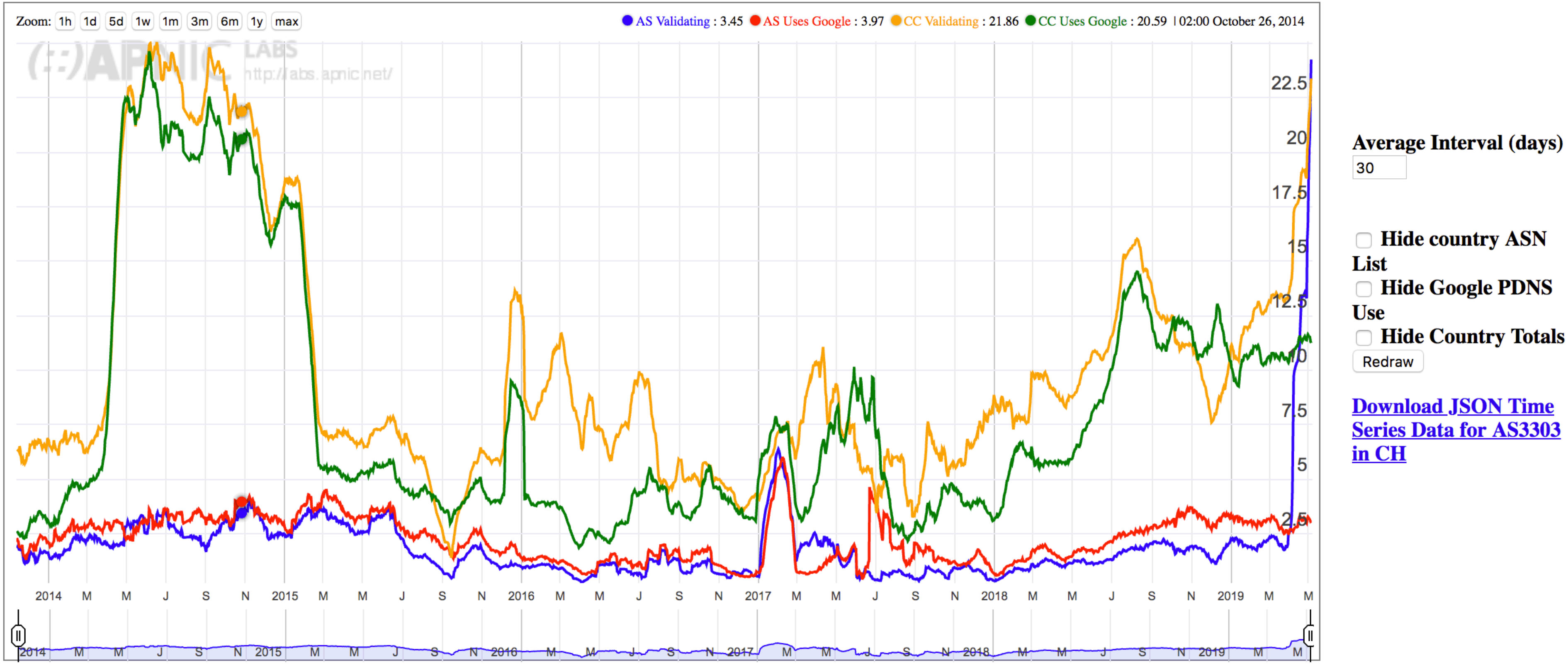
Redraw

Download JSON Time Series Data for AS12511 in CH

DNSSEC Per-Country Deployment for AS21232: GGAMAUR, Switzerland (CH)



DNSSEC Per-Country Deployment for AS3303: SWISSCOM Swisscom (Switzerland) Ltd, Switzerland (CH)


Zoom: 1h 1d 5d 1w 1m 3m 6m 1y max
● AS Validating : 3.45 ● AS Uses Google : 3.97 ● CC Validating : 21.86 ● CC Uses Google : 20.59 | 02:00 October 26, 2014
APNIC LABS http://labs.apnic.net/
22.5
20
17.5
15
12.5
10
7.5
5
2.5
2014 M M J S N 2015 M M J S N 2016 M M J S N 2017 M M J S N 2018 M M J S N 2019 M M
2014 M M J S N 2015 M M J S N 2016 M M J S N 2017 M M J S N 2018 M M J S N 2019 M M

Average Interval (days)

30

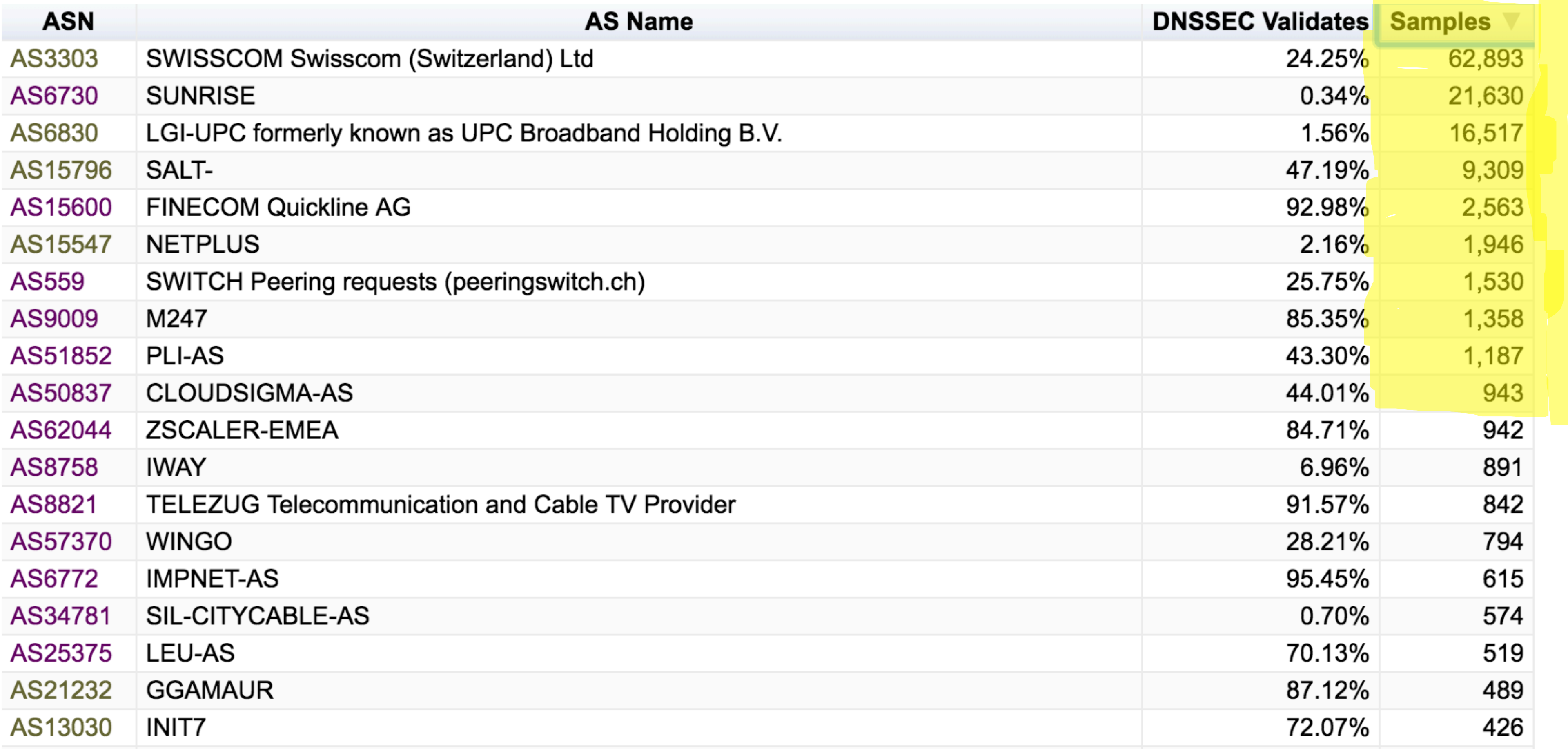
□ **Hide country ASN List**

□ **Hide Google PDNS Use**

□ **Hide Country Totals**

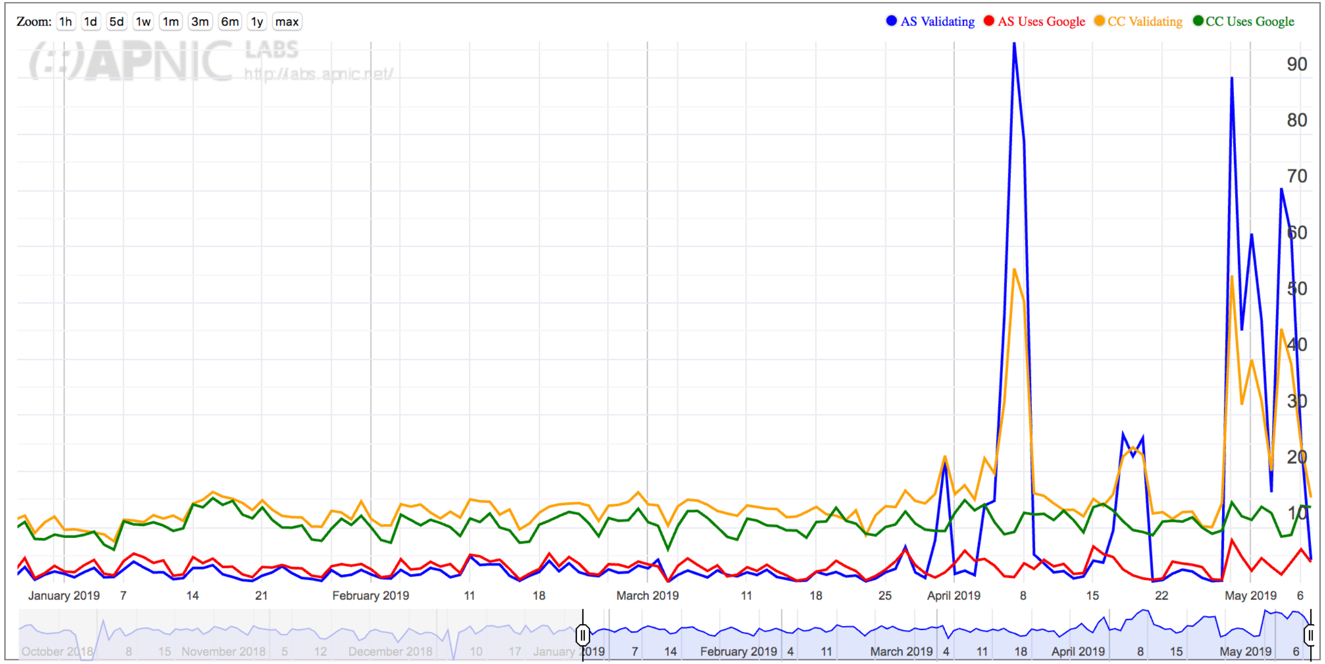
Redraw

Download JSON Time Series Data for AS3303 in CH



ASN	AS Name	DNSSEC Validates	Samples ▼
AS3303	SWISSCOM Swisscom (Switzerland) Ltd	24.25%	62,893
AS6730	SUNRISE	0.34%	21,630
AS6830	LGI-UPC formerly known as UPC Broadband Holding B.V.	1.56%	16,517
AS15796	SALT-	47.19%	9,309
AS15600	FINECOM Quickline AG	92.98%	2,563
AS15547	NETPLUS	2.16%	1,946
AS559	SWITCH Peering requests (peeringswitch.ch)	25.75%	1,530
AS9009	M247	85.35%	1,358
AS51852	PLI-AS	43.30%	1,187
AS50837	CLOUDSIGMA-AS	44.01%	943
AS62044	ZSCALER-EMEA	84.71%	942
AS8758	IWAY	6.96%	891
AS8821	TELEZUG Telecommunication and Cable TV Provider	91.57%	842
AS57370	WINGO	28.21%	794
AS6772	IMPNET-AS	95.45%	615
AS34781	SIL-CITYCABLE-AS	0.70%	574
AS25375	LEU-AS	70.13%	519
AS21232	GGAMAUR	87.12%	489
AS13030	INIT7	72.07%	426

DNSSEC Per-Country Deployment for AS3303: SWISSCOM Swisscom (Switzerland) Ltd, Switzerland (CH)



Average Interval (days) 1

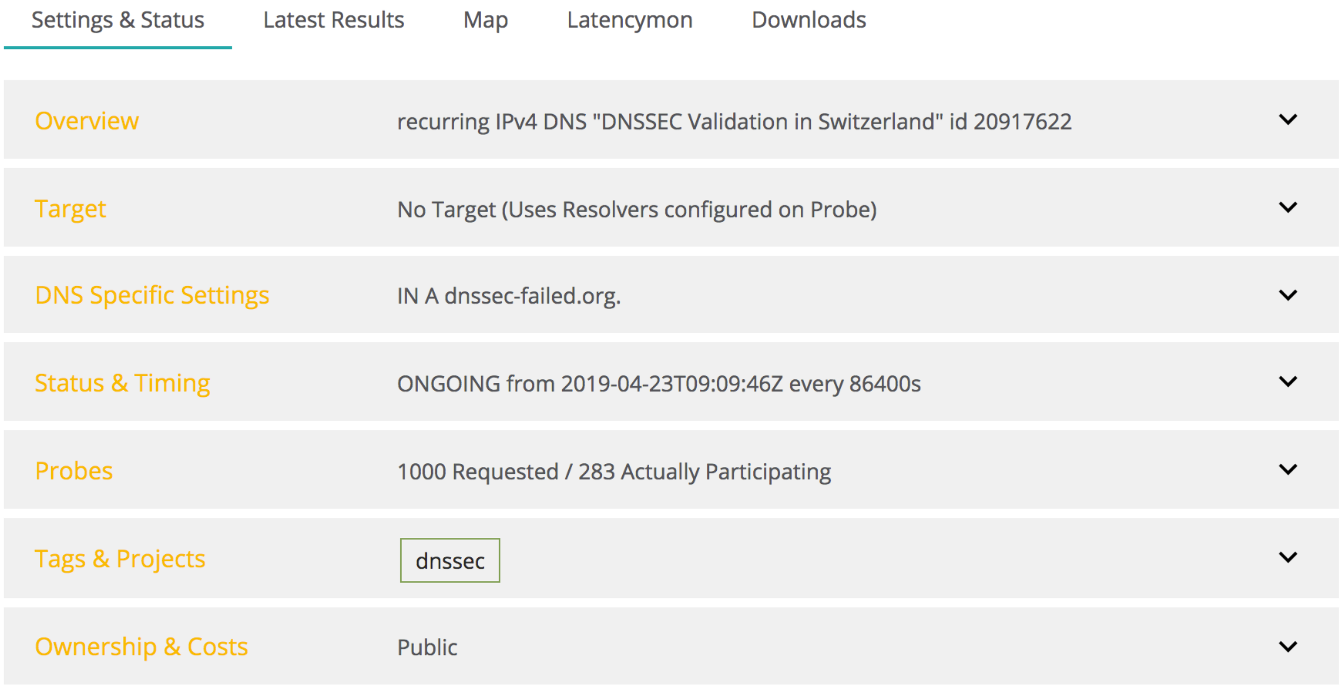
□ Hide country ASN List
□ Hide Google PDNS Use
□ Hide Country Totals

Redraw

Download JSON Time Series Data for AS3303 in CH

RIPE atlas

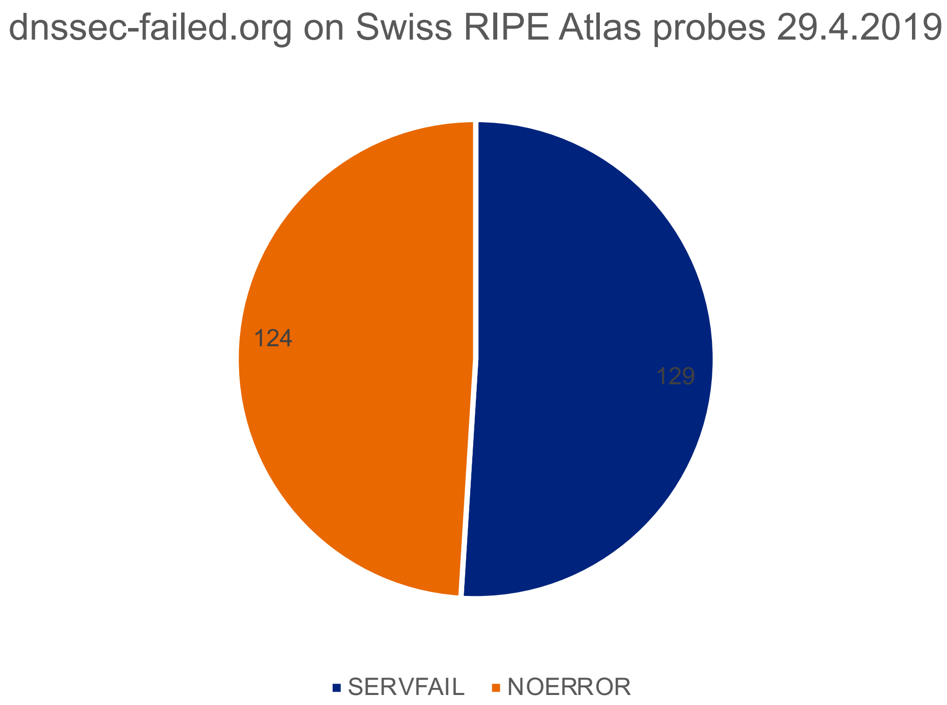
RIPE Atlas DNSSEC validation measurement



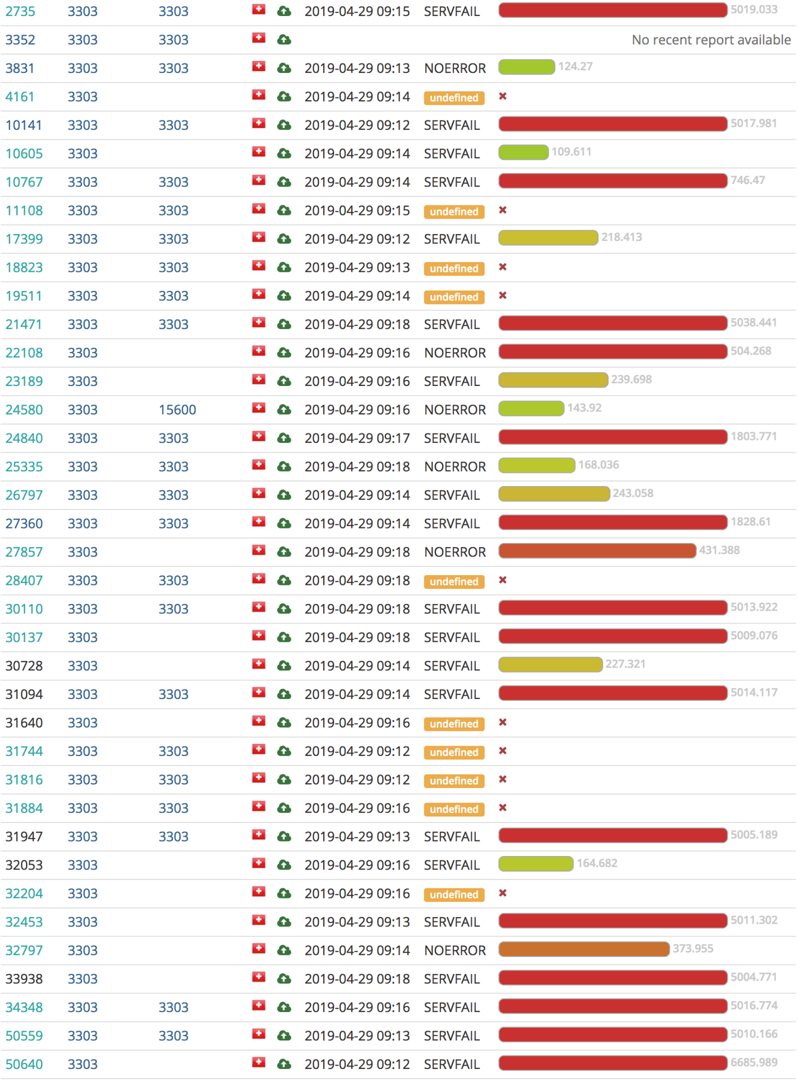
Overview	recurring IPv4 DNS "DNSSEC Validation in Switzerland" id 20917622
Target	No Target (Uses Resolvers configured on Probe)
DNS Specific Settings	IN A dnssec-failed.org.
Status & Timing	ONGOING from 2019-04-23T09:09:46Z every 86400s
Probes	1000 Requested / 283 Actually Participating
Tags & Projects	dnssec
Ownership & Costs	Public

https://atlas.ripe.net/measurements/20917622/#!probes

dnssec-failed.org



On 29.4. probes in AS 3303 showed more than 50% SERVFAIL when queried for dnssec-failed.org



2735	3303	3303	🇨🇭	☁	2019-04-29 09:15	SERVFAIL	5019.033
3352	3303	3303	🇨🇭	☁			No recent report available
3831	3303	3303	🇨🇭	☁	2019-04-29 09:13	NOERROR	124.27
4161	3303		🇨🇭	☁	2019-04-29 09:14	undefined	✖
10141	3303	3303	🇨🇭	☁	2019-04-29 09:12	SERVFAIL	5017.981
10605	3303		🇨🇭	☁	2019-04-29 09:14	SERVFAIL	109.611
10767	3303	3303	🇨🇭	☁	2019-04-29 09:14	SERVFAIL	746.47
11108	3303	3303	🇨🇭	☁	2019-04-29 09:15	undefined	✖
17399	3303	3303	🇨🇭	☁	2019-04-29 09:12	SERVFAIL	218.413
18823	3303	3303	🇨🇭	☁	2019-04-29 09:13	undefined	✖
19511	3303	3303	🇨🇭	☁	2019-04-29 09:14	undefined	✖
21471	3303	3303	🇨🇭	☁	2019-04-29 09:18	SERVFAIL	5038.441
22108	3303		🇨🇭	☁	2019-04-29 09:16	NOERROR	504.268
23189	3303		🇨🇭	☁	2019-04-29 09:16	SERVFAIL	239.698
24580	3303	15600	🇨🇭	☁	2019-04-29 09:16	NOERROR	143.92
24840	3303	3303	🇨🇭	☁	2019-04-29 09:17	SERVFAIL	1803.771
25335	3303	3303	🇨🇭	☁	2019-04-29 09:18	NOERROR	168.036
26797	3303	3303	🇨🇭	☁	2019-04-29 09:14	SERVFAIL	243.058
27360	3303	3303	🇨🇭	☁	2019-04-29 09:14	SERVFAIL	1828.61
27857	3303		🇨🇭	☁	2019-04-29 09:18	NOERROR	431.388
28407	3303	3303	🇨🇭	☁	2019-04-29 09:18	undefined	✖
30110	3303	3303	🇨🇭	☁	2019-04-29 09:18	SERVFAIL	5013.922
30137	3303		🇨🇭	☁	2019-04-29 09:18	SERVFAIL	5009.076
30728	3303		🇨🇭	☁	2019-04-29 09:14	SERVFAIL	227.321
31094	3303	3303	🇨🇭	☁	2019-04-29 09:14	SERVFAIL	5014.117
31640	3303		🇨🇭	☁	2019-04-29 09:16	undefined	✖
31744	3303	3303	🇨🇭	☁	2019-04-29 09:12	undefined	✖
31816	3303	3303	🇨🇭	☁	2019-04-29 09:12	undefined	✖
31884	3303	3303	🇨🇭	☁	2019-04-29 09:16	undefined	✖
31947	3303	3303	🇨🇭	☁	2019-04-29 09:13	SERVFAIL	5005.189
32053	3303		🇨🇭	☁	2019-04-29 09:16	SERVFAIL	164.682
32204	3303		🇨🇭	☁	2019-04-29 09:16	undefined	✖
32453	3303		🇨🇭	☁	2019-04-29 09:13	SERVFAIL	5011.302
32797	3303		🇨🇭	☁	2019-04-29 09:14	NOERROR	373.955
33938	3303		🇨🇭	☁	2019-04-29 09:18	SERVFAIL	5004.771
34348	3303	3303	🇨🇭	☁	2019-04-29 09:16	SERVFAIL	5016.774
50559	3303	3303	🇨🇭	☁	2019-04-29 09:13	SERVFAIL	5010.166
50640	3303		🇨🇭	☁	2019-04-29 09:12	SERVFAIL	6685.989

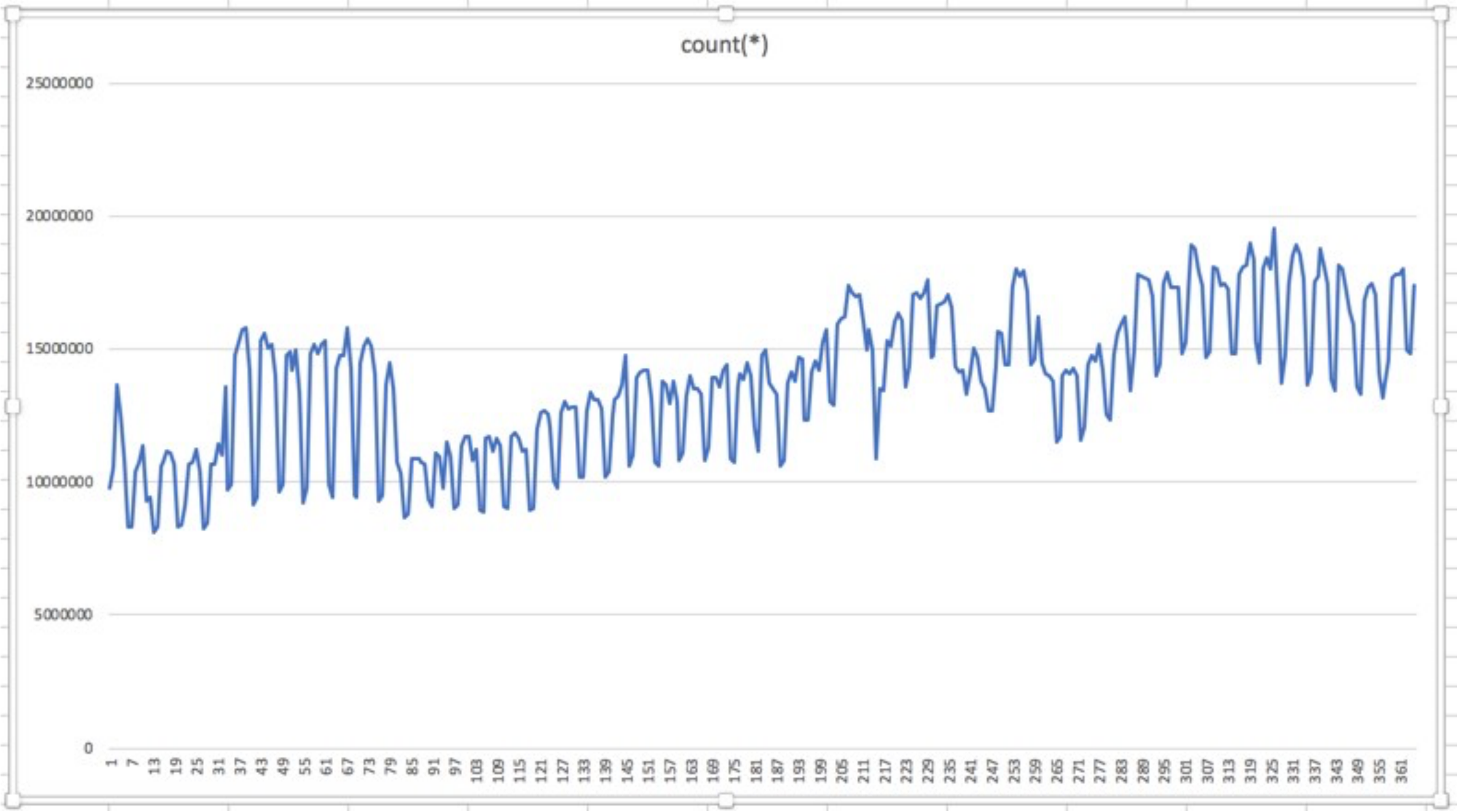
RIPE Atlas DNSSEC validation measurement

- Using the default resolver of the probe
- May be biased depending on the recursive DNS
- Lots of public DNS resolvers (1.1.1.1, 8.8.8.8, quad9)
- Destination doesn‘t help 192.168.1.1
- Resolver can also identified with a request to whoami.lua.powerdns.org

https://atlas.ripe.net/measurements/20788254/

DS requests on a.nic.ch

DS requests on a.nic.ch



Summary

DNSSEC

- Is an essential part of Internet security
- Is a mature protocol
- Improves the security for all services
- Tool support available and easy
- Growing usage of DNSSEC in Switzerland, both Signing and Validation ☺

dns-operation@switch.ch

logo: Cloudflare