ARIN 47

12-14 APRIL 2021

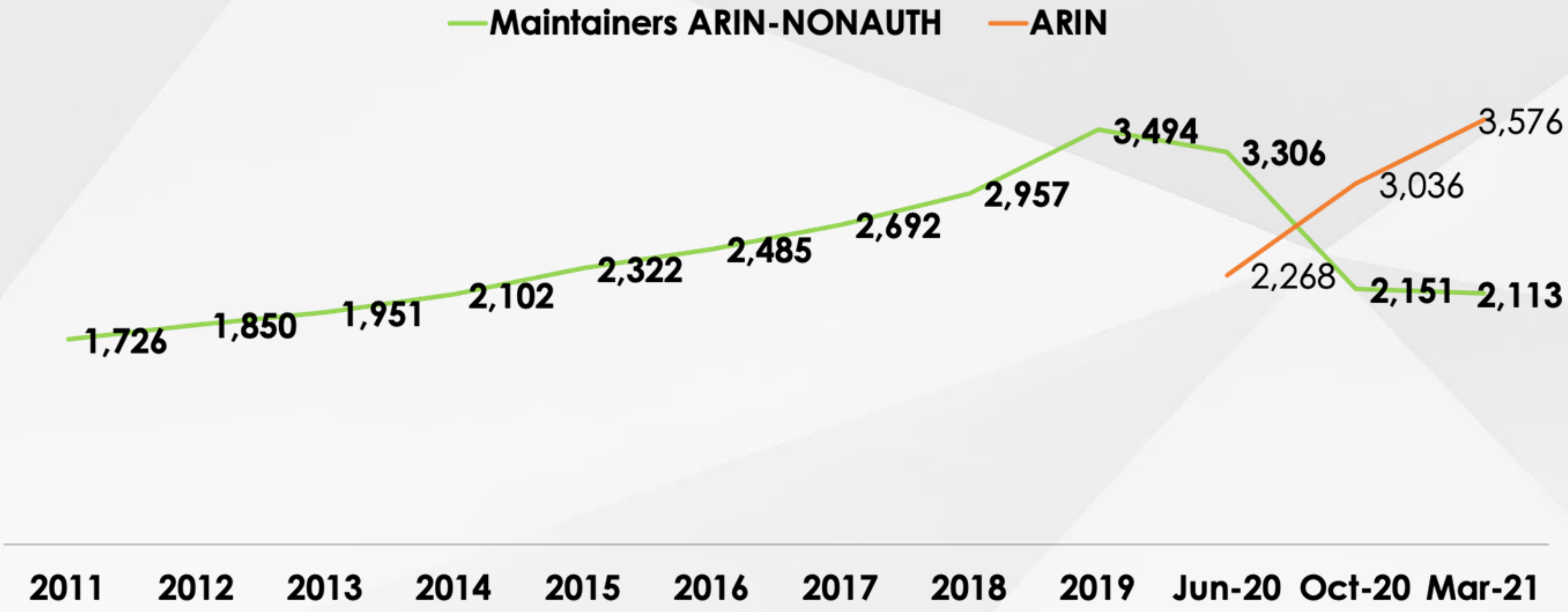
IRR, RPKI, and Password Security Update

Mark Kosters, Chief Technology Officer

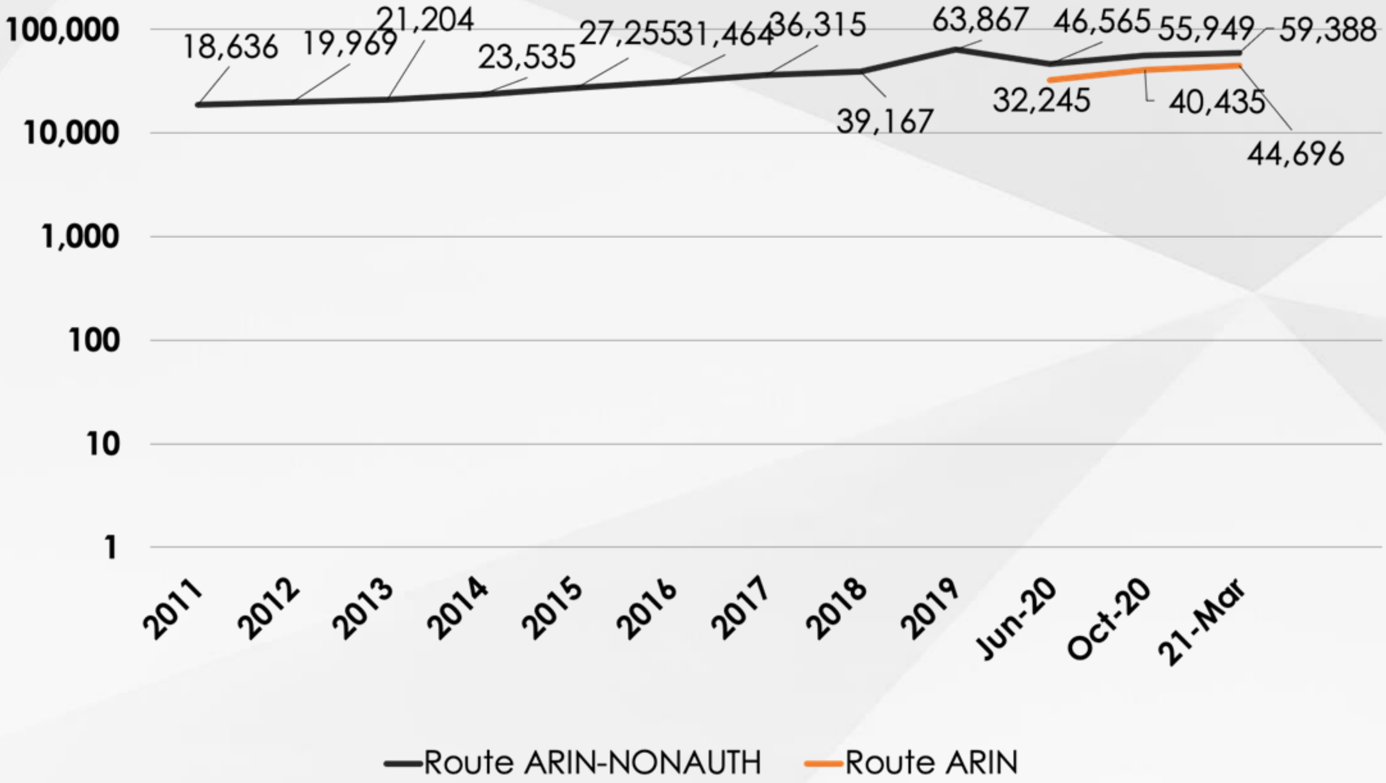
IRR Update

12-14 APRIL 2021

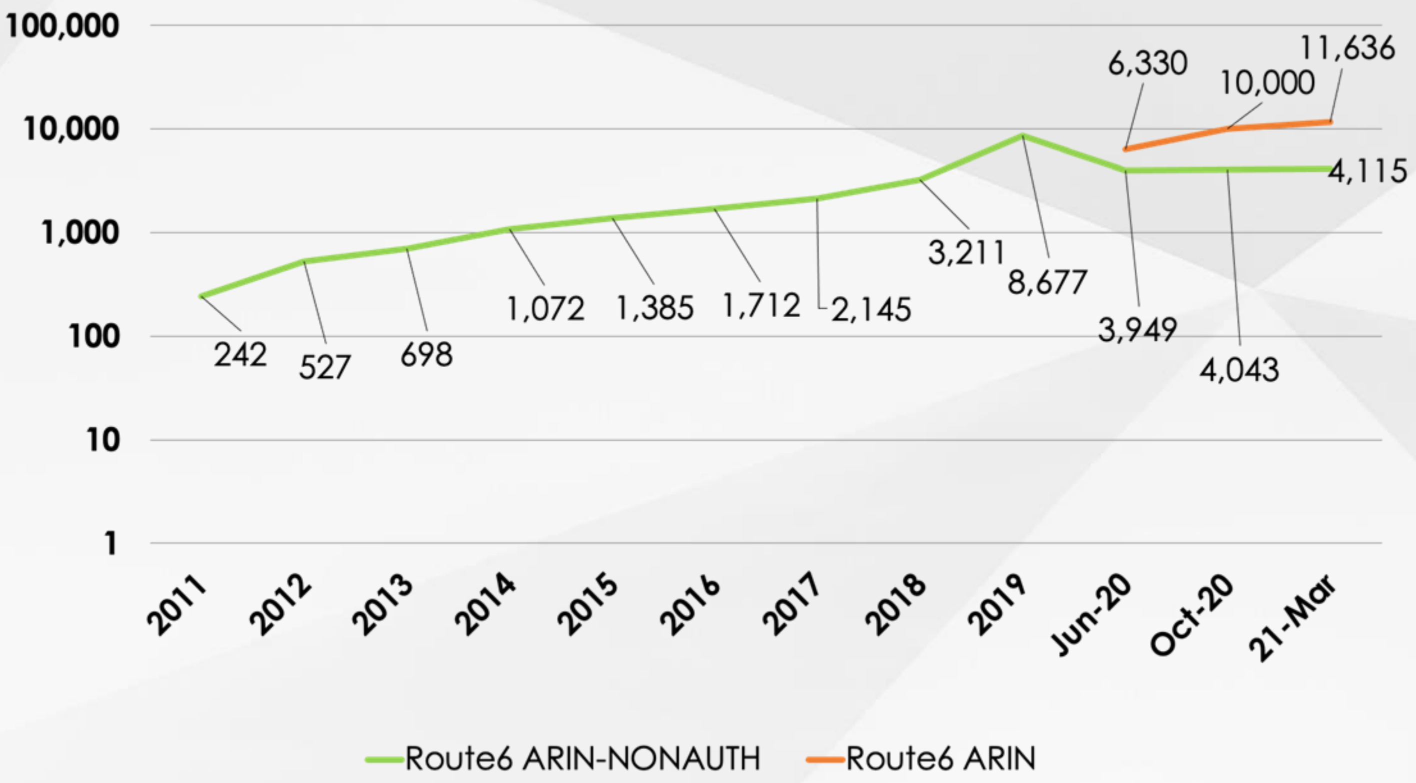
Maintainers/Orgs



Route Objects



Route6 Objects



Interesting Observations

Expected to see a drop in ARIN-NONAUTH - but that is not reality

- Maintainers (pre June 2020) have come to life
- Number of route objects is roughly the same for both ARIN and ARIN-NONAUTH
- Growth in Orgs participating in ARIN

Should we have expected a significant drop in ARIN-NONAUTH?

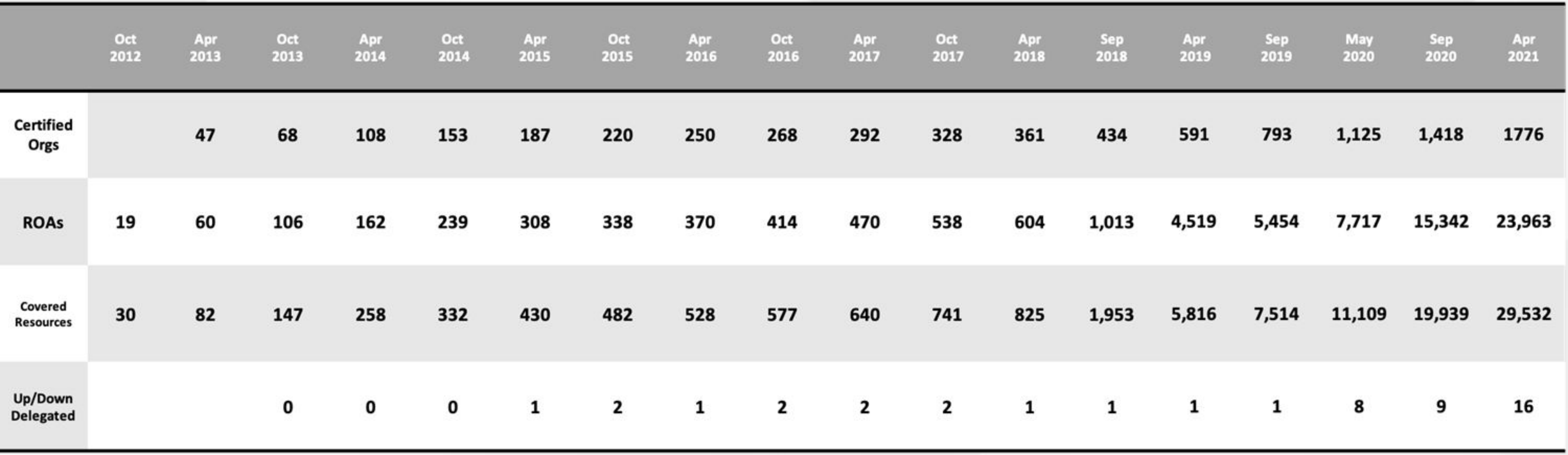
RPKI Update

RPKI Challenges

We had two outages in 2020

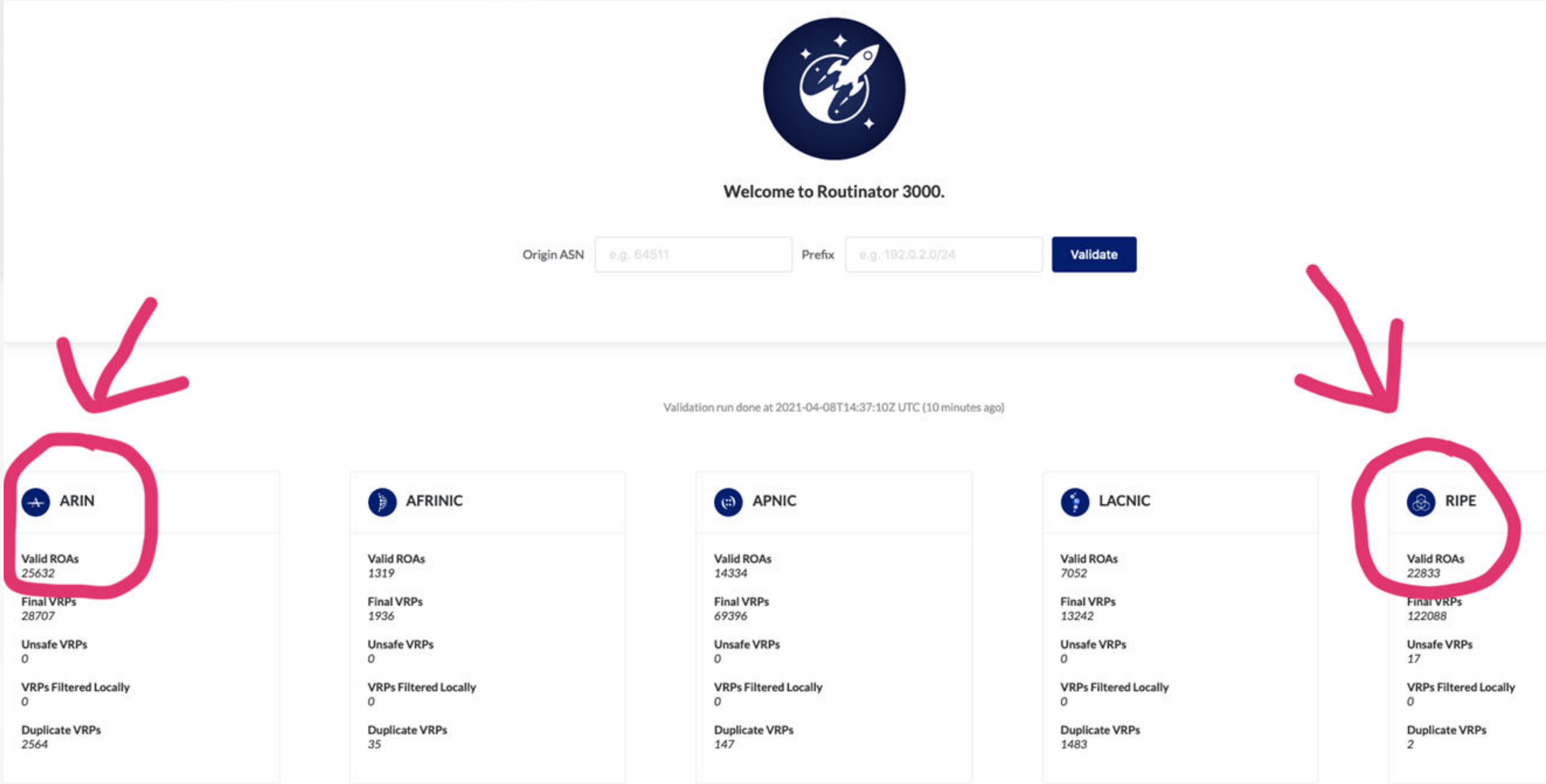
- August 12, 2020 - Encoding issue that was seen by a subset of validators
  - Resolution: Test against additional validators (See "**Supported/Tested RPKI Validators**" under https://www.arin.net/resources/manage/rpki/)
  - Resolution: Set up monitoring that matches Verified Routing Prefixes (VRPs) emitted from the various validators
- Nov 20, 2020 - Omission of delegated RPKI users after a software upgrade
  - Resolution: Performed an audit of our implementation against RPKI RFCs and test coverage
  - Resolution: Hired a Senior Product Manager (Brad Gorman)

RPKI Statistics



	Oct 2012	Apr 2013	Oct 2013	Apr 2014	Oct 2014	Apr 2015	Oct 2015	Apr 2016	Oct 2016	Apr 2017	Oct 2017	Apr 2018	Sep 2018	Apr 2019	Sep 2019	May 2020	Sep 2020	Apr 2021
Certified Orgs		47	68	108	153	187	220	250	268	292	328	361	434	591	793	1,125	1,418	1776
ROAs	19	60	106	162	239	308	338	370	414	470	538	604	1,013	4,519	5,454	7,717	15,342	23,963
Covered Resources	30	82	147	258	332	430	482	528	577	640	741	825	1,953	5,816	7,514	11,109	19,939	29,532
Up/Down Delegated			0	0	0	1	2	1	2	2	2	1	1	1	1	8	9	16

ARIN is #1 on ROAs!



Welcome to Routinator 3000.

Validation run done at 2021-04-08T14:37:10Z UTC (10 minutes ago)

	ARIN	AFRINIC	APNIC	LACNIC	RIPE
Valid ROAs	*25632*	*1319*	*14334*	*7052*	*22833*
Final VRPs	*28707*	*1936*	*69396*	*13242*	*122088*
Unsafe VRPs	*0*	*0*	*0*	*0*	*17*
VRPs Filtered Locally	*0*	*0*	*0*	*0*	*0*
Duplicate VRPs	*2564*	*35*	*147*	*1483*	*2*

Password Security Update

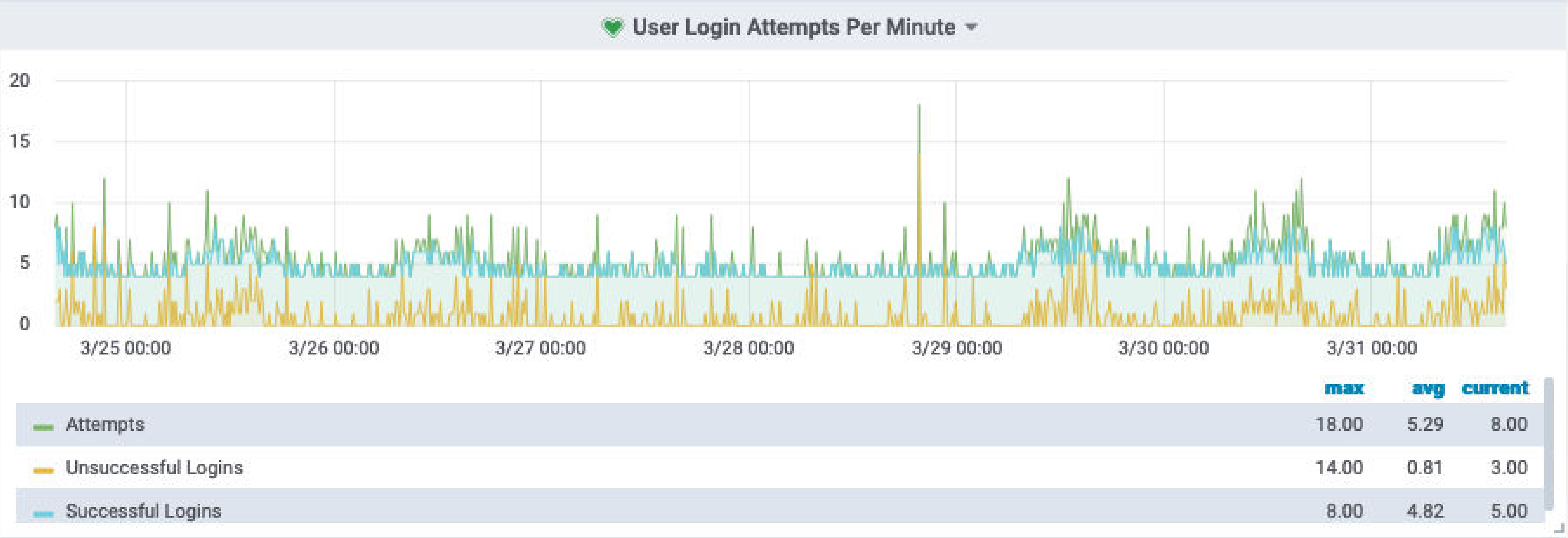
Brute Force Password Hijacking

Noticed a flurry of brute force hacking attempts that locked people’s accounts

- Pre Oct 29, 2020 account login behavior: Allows for 6 login attempts, then locked account
- Pivoted to insert a captcha after x failed login attempts
- Post Oct 29, 2020 account behavior: Allow for x failed login attempts, then captcha, then y failed login attempts where x+y = 6

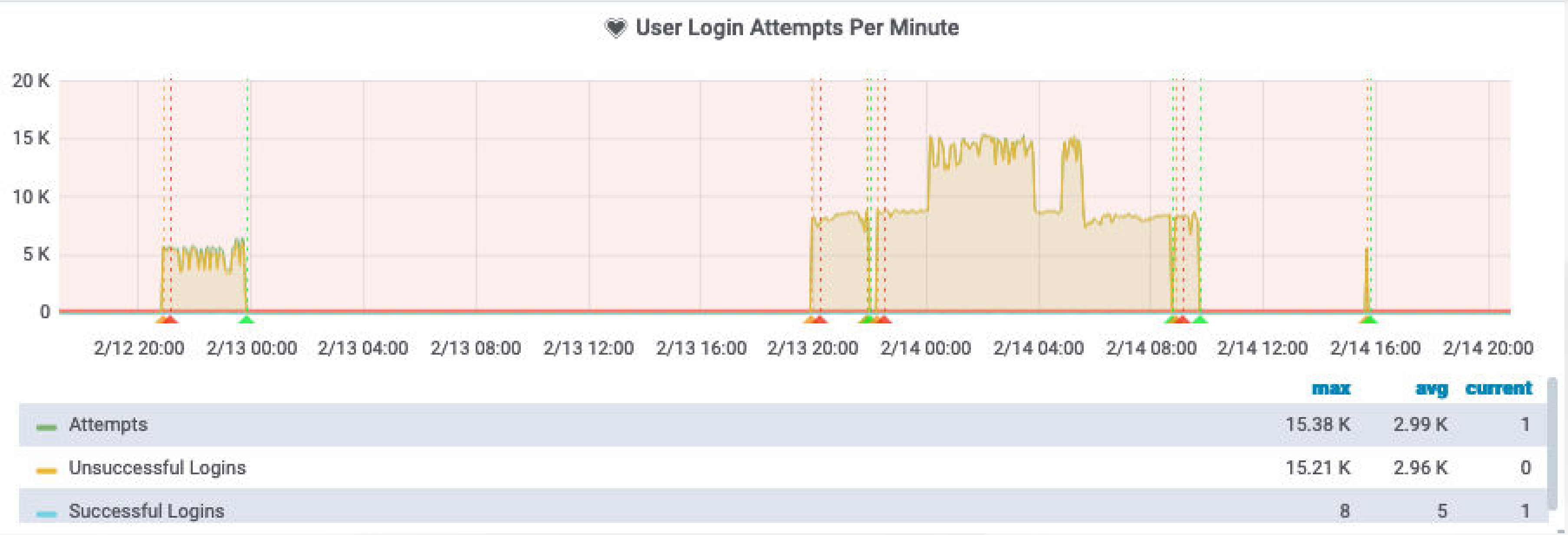
This stopped the brute force activity from locking accounts.

Normal Login Activity



	max	avg	current
🟩 Attempts	18.00	5.29	8.00
🟨 Unsuccessful Logins	14.00	0.81	3.00
🟦 Successful Logins	8.00	4.82	5.00

Brute Force Attack Example



	max	avg	current
🟩 Attempts	15.38 K	2.99 K	1
🟨 Unsuccessful Logins	15.21 K	2.96 K	0
🟦 Successful Logins	8	5	1

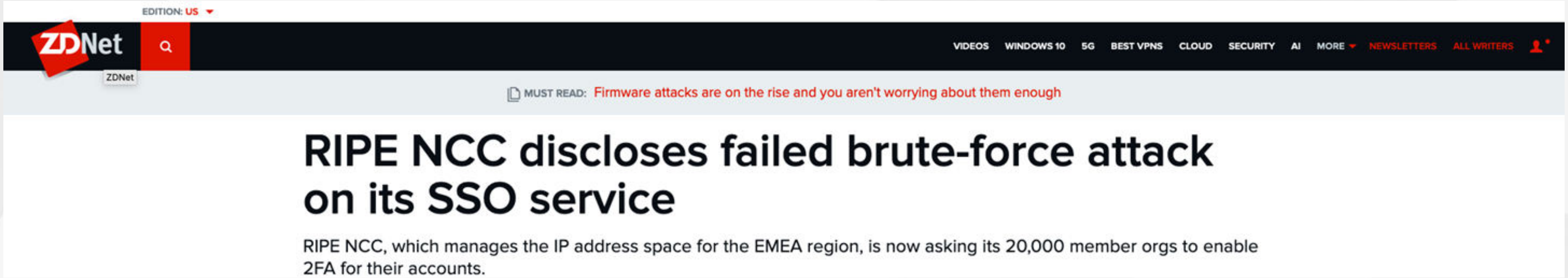
Net total for that week

Invalid Password: 9,711 attempts

Invalid Captcha: 249,205 attempts

Invalid Username: 10,999,044 attempts

We Were Not Alone



MUST READ: Firmware attacks are on the rise and you aren't worrying about them enough

RIPE NCC discloses failed brute-force attack on its SSO service

RIPE NCC, which manages the IP address space for the EMEA region, is now asking its 20,000 member orgs to enable 2FA for their accounts.

Resultant Activity

Consultation on Login Security

Result:

- Align with NIST SP800-63b password guidelines
- Check against a list that contains values known to be compromised
- Not impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters)
- Rate limit by using a captcha and incrementing timeout periods before allowing further attempts

This code will be released in June 2021.

Thanks!

Any
Questions?