ARIN 49

POWERED BY PARTICIPATION

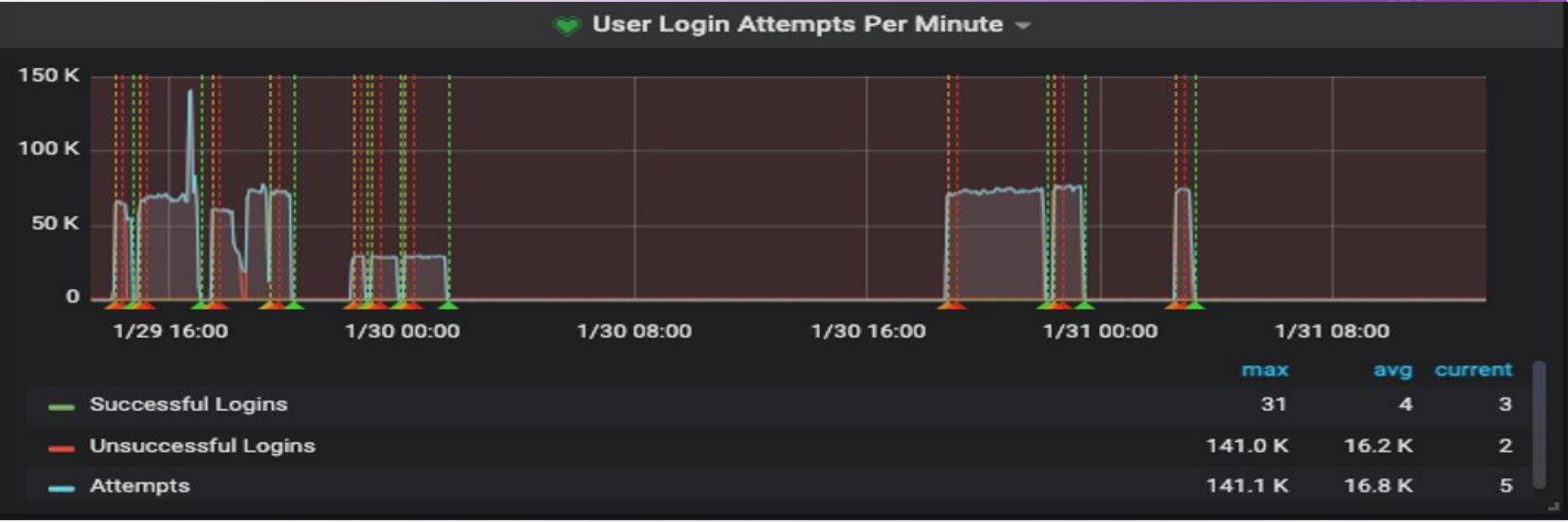
Brute Force Login Attacks

Mark Kosters
Garth Dubin

Agenda

- Effects of the Attacks (aka “The Problem”)
- Engineering and Customer Costs
- Operational and Customer Mitigation Strategies

The Problem



	max	avg	current
🟩 Successful Logins	31	4	3
🟥 Unsuccessful Logins	141.0 K	16.2 K	2
🟦 Attempts	141.1 K	16.8 K	5

Latest: Around 65,000 login attempts per minute

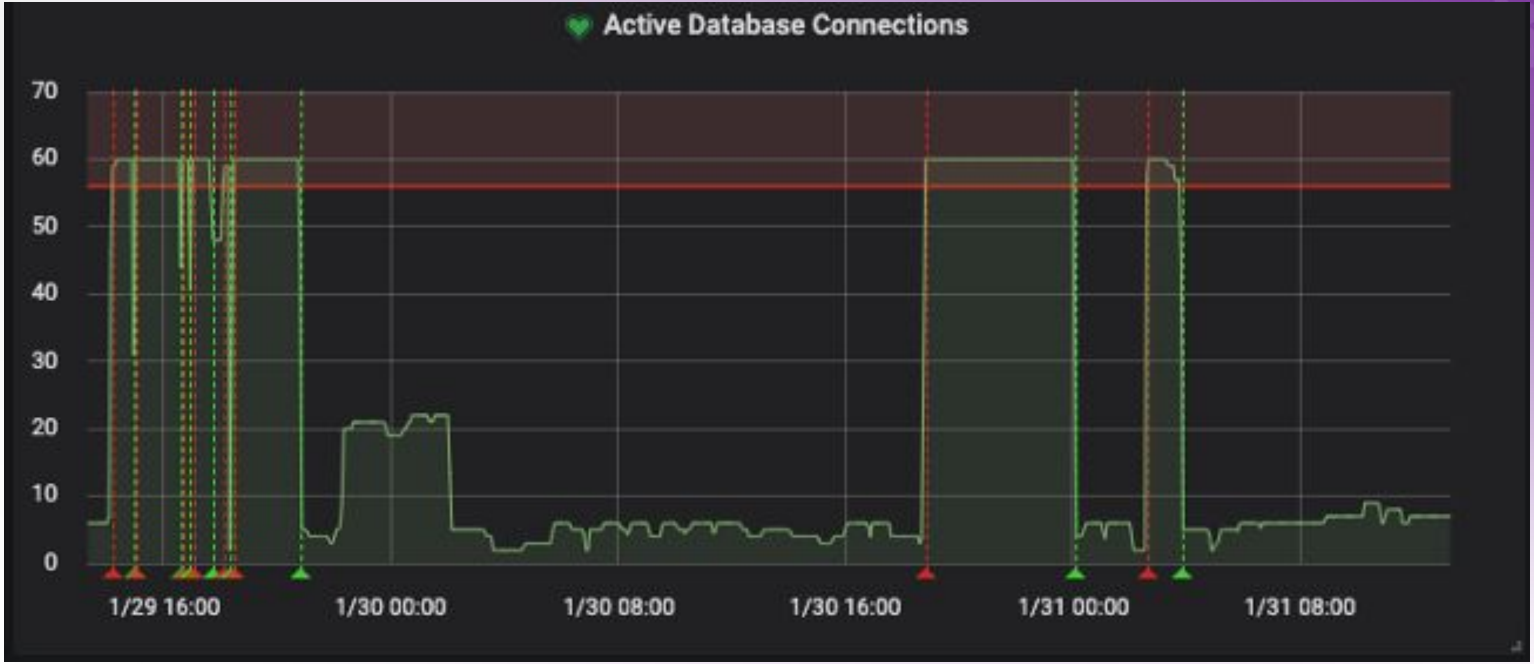
The Problem

The attacks are almost always highly distributed.

In one specific attack, we saw sources came from:

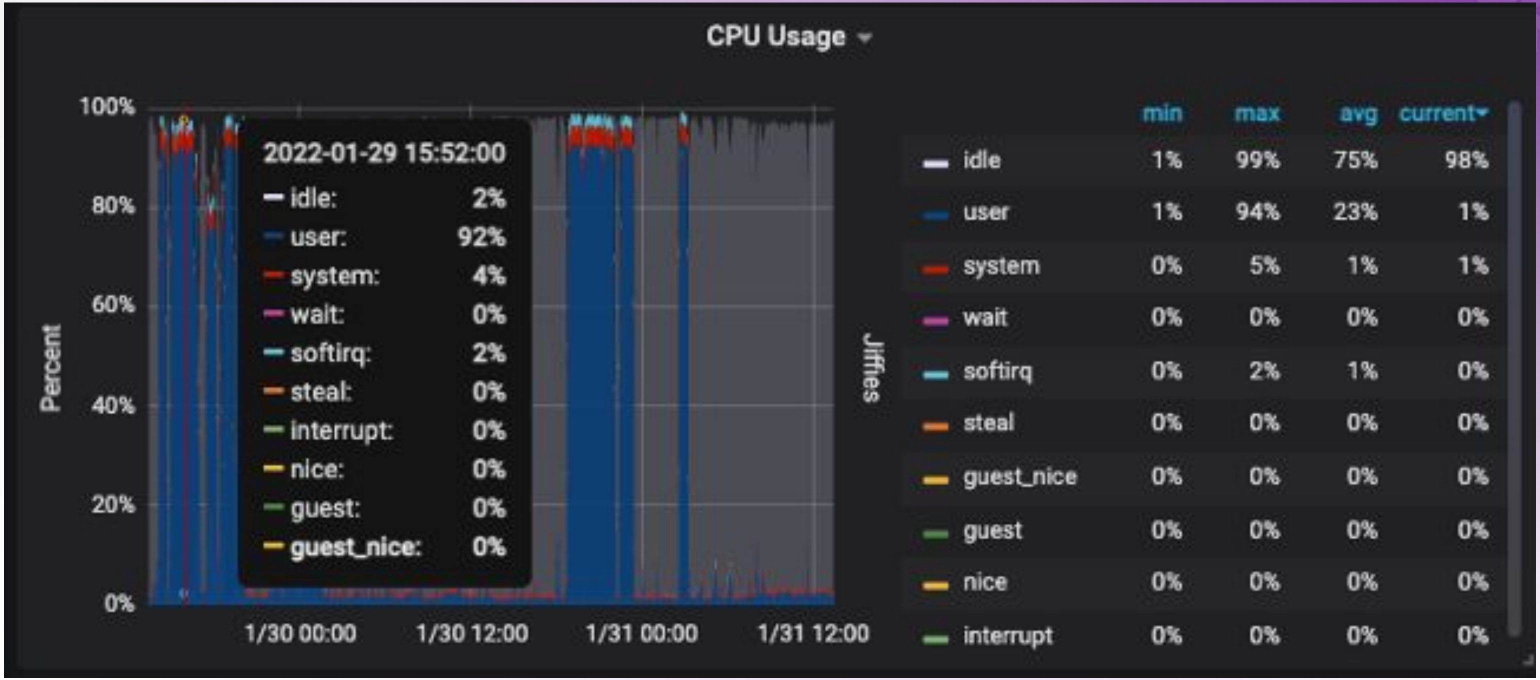
- 22,959 unique IP addresses
    - 3,791 (16%) were only used a single time.
    - 10,696 (46%) were used less than 10 times.
    - 12,637 (55%) were used less than 100 times.
- The attack came from many disparate blocks, from both IPv4 and IPv6 space.

The Problem



These attacks overwhelming our checks/monitoring for database connections.

The Problem



2022-01-29 15:52:00

- idle: 2%
- user: 92%
- system: 4%
- wait: 0%
- softirq: 2%
- steal: 0%
- interrupt: 0%
- nice: 0%
- guest: 0%
- guest_nice: 0%

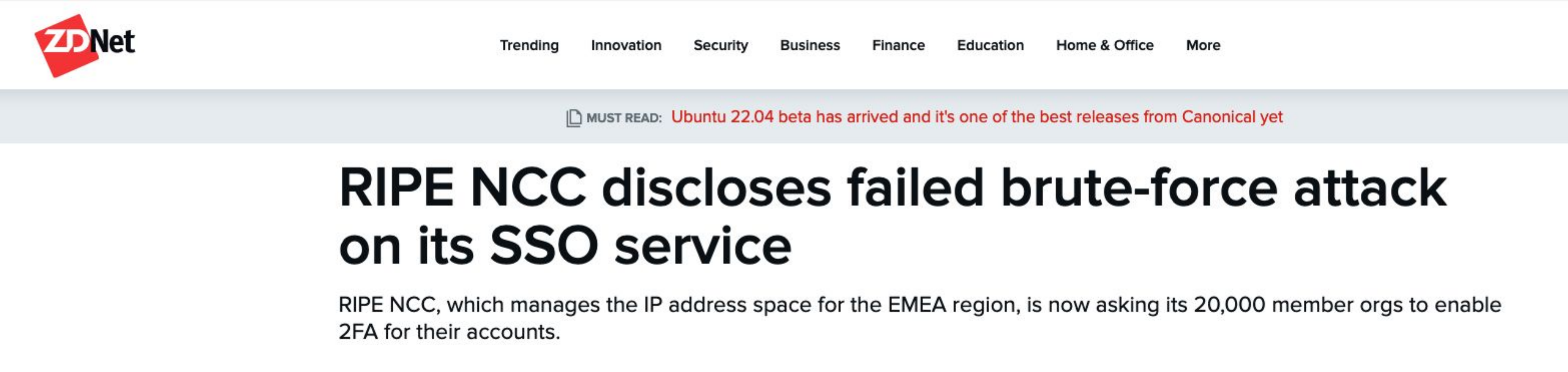
	min	max	avg	current
— idle	1%	99%	75%	98%
— user	1%	94%	23%	1%
— system	0%	5%	1%	1%
— wait	0%	0%	0%	0%
— softirq	0%	2%	1%	0%
— steal	0%	0%	0%	0%
— guest_nice	0%	0%	0%	0%
— guest	0%	0%	0%	0%
— nice	0%	0%	0%	0%
— interrupt	0%	0%	0%	0%

These attacks drive up CPU utilization.

The Problem

- Logging invalid login attempts filled logs at 1.8 gigabytes/hour.
- Drives filled quickly; this created a Java problem since Java has trouble writing to files of that size.
- Adding more boxes to serve the login process actually increased the login attempt rate.

We are not alone



MUST READ: Ubuntu 22.04 beta has arrived and it's one of the best releases from Canonical yet

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.

https://www.zdnet.com/article/ripe-discloses-failed-brute-force-attack-on-its-sso-service/
Posted Feb 18, 2021

Engineering and Customer Costs

- Each incident has opportunity costs
  - Pulls focus away from current tasks
  - Happens 24/7
- Estimated cost
  - Each attack hour requires 5 person-hours:
    - Analyzing the source
    - Analyzing compromised accounts
    - Analyzing existing login code
    - Reporting results
- Customer cost
  - Each incident result compromised web-user accounts, averaging 13 per event (most web-user accounts are not associated with resource holdings).
  - There is always a risk that not all compromised accounts are discovered.

Operational Mitigation Strategies

- Caching all usernames to prevent round trips to the database.
- Evaluating the login process to optimize the workflow and study its impact on system resources.
- Re-evaluating logging and metrics gathering.
- Automatically monitoring successful logins during surges and report to RSD/Engineering.
- Presenting a CAPTCHA to all users before they can submit their login information while under a login harvesting attack.

None of these should be customer impacting.

Customer Mitigation Strategies

- 3.2% of all users (192K) have 2FA enabled.
- Of users who have logged in more than once (109K), 5.3% have 2FA enabled.
- Improve our 2FA functionality:
    - Add support for SMS 2FA. While less secure than TOTP, it may encourage adoption in users who are unwilling to download an authenticator application.
    - A community consultation will be released soon to discuss the possibility of enforcing 2FA on all customer accounts that are associated with resources.

Thanks!

Any Questions?