Spam Wars

Chronicles of Our Fight for Network Integrity

IPXO

IGNAS ANFALOVAS

Engineering Manager,
Platform Team at IPXO

Customer Support Team Lead within a Hosting company:
Over 70,000 tenants across B2B and B2C sectors, spanning 80+ industries

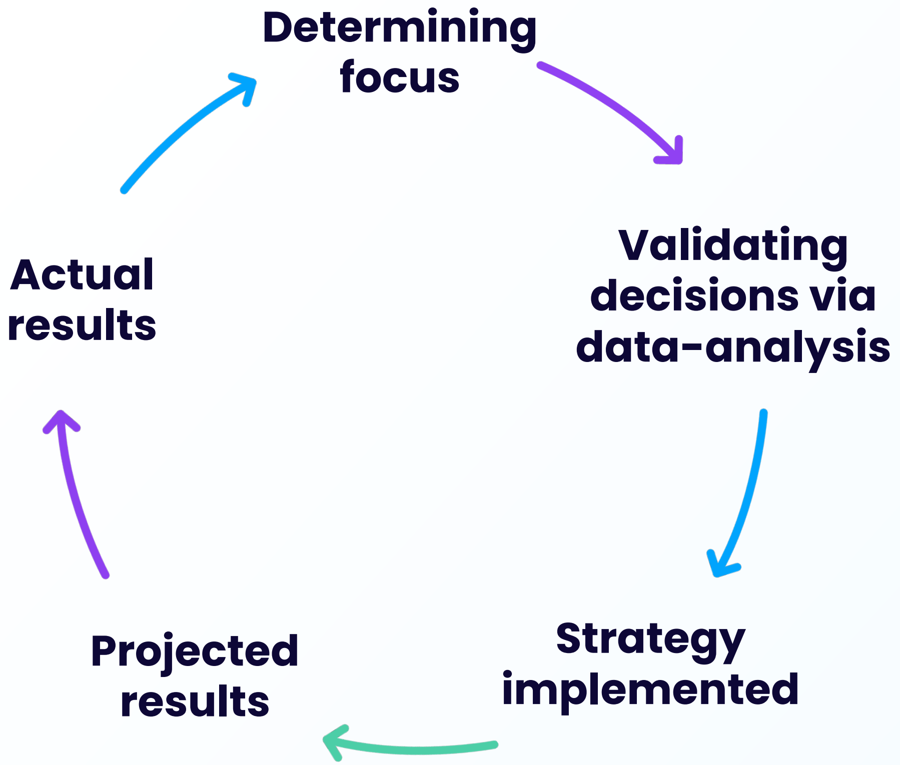
Engineering Manager of the IPXO Platform team:
Planning and implementation of changes of Network Infrastructure

IPXO primarily focuses on IP leasing

PROBLEM

- We monitor IP reputation both during and after leases to ensure clean resources
- Increased IP leases led to a rise in abuse reports
- Most abuse reports were related to SPAM
- Resolving SPAM cases was time-intensive and often ineffective
- Our reputation suffered as SBL (Spamhaus Blocklist) listings increased faster than resolutions

Our Journey in Defending the Network from SPAM



Determining focus

Validating decisions via data-analysis

Strategy implemented

Projected results

Actual results

Our Journey in Defending the Network from SPAM

2023-04

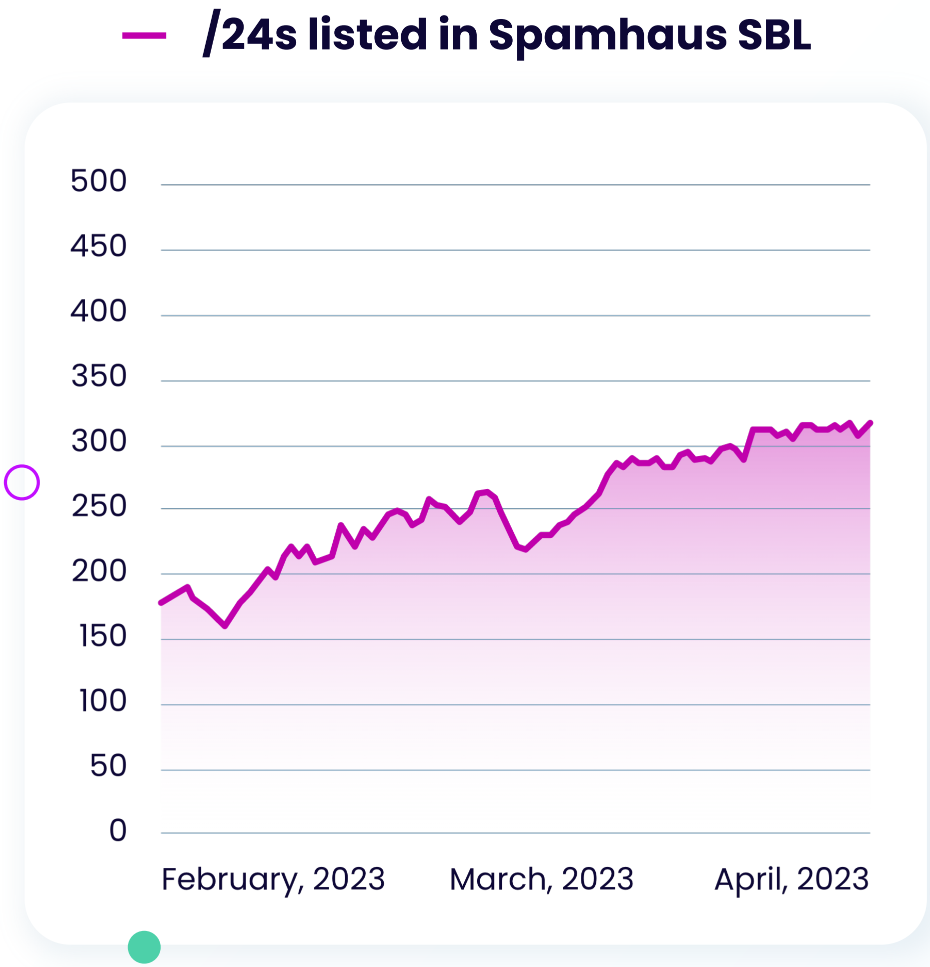
Pointer Record (PTR) & Reverse Domain Name Service (rDNS)

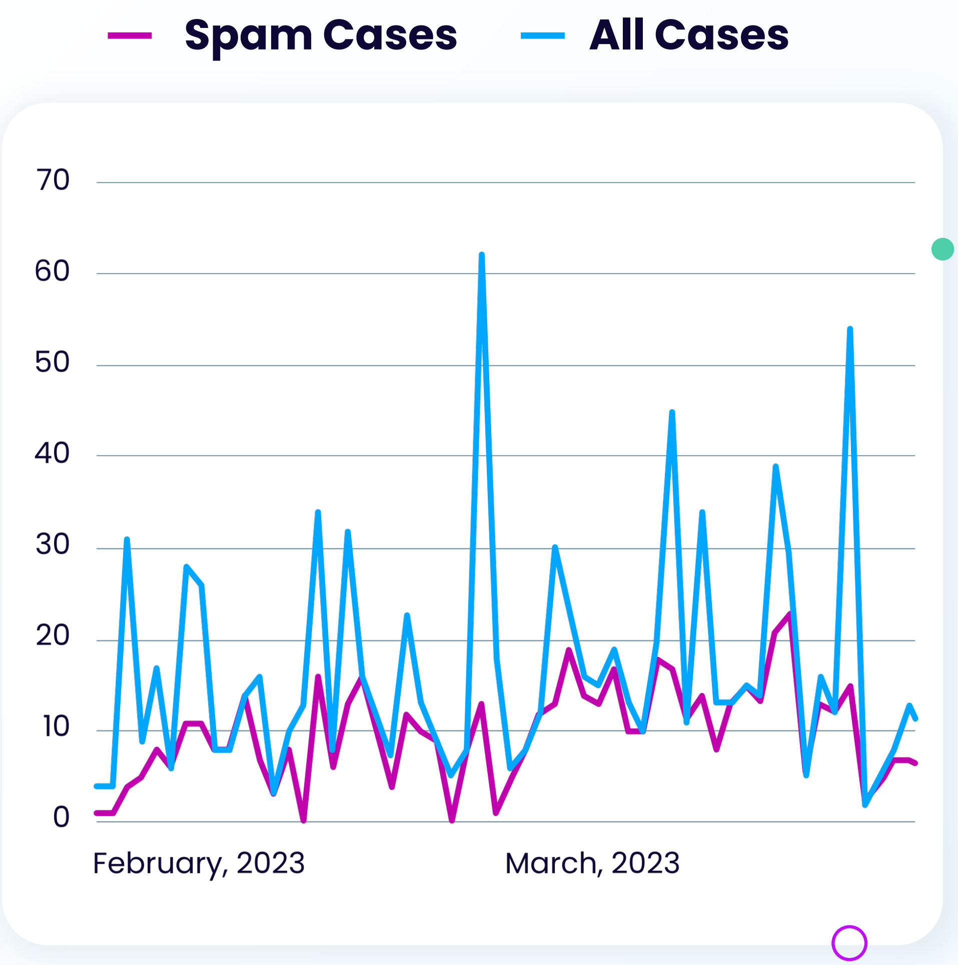
2023-05

Know Your Customer (KYC)

2023-09

Resource Public Key Infrastructure (RPKI)


/24s listed in Spamhaus SBL
500
450
400
350
300
250
200
150
100
50
0
February, 2023
March, 2023
April, 2023


Spam Cases
All Cases
70
60
50
40
30
20
10
0
February, 2023
March, 2023

First Focus:

PTR & rDNS

PTRs primarily serve to enhance email deliverability

Noticed a pattern of abusive behavior using PTRs

○ Some PTRs would lead to obviously fake domains (e.g. Microsoft.com)

○ The PTRs would get changed once a week or sometimes even more frequently

The changes we made

- Introduced automatic PTR scanning
- Improved monitoring to detect clients who frequently modify PTRs
- Developed a feature to disable rDNS and PTR control/configuration in the event of detected anomalies
- Disabled rDNS control by default

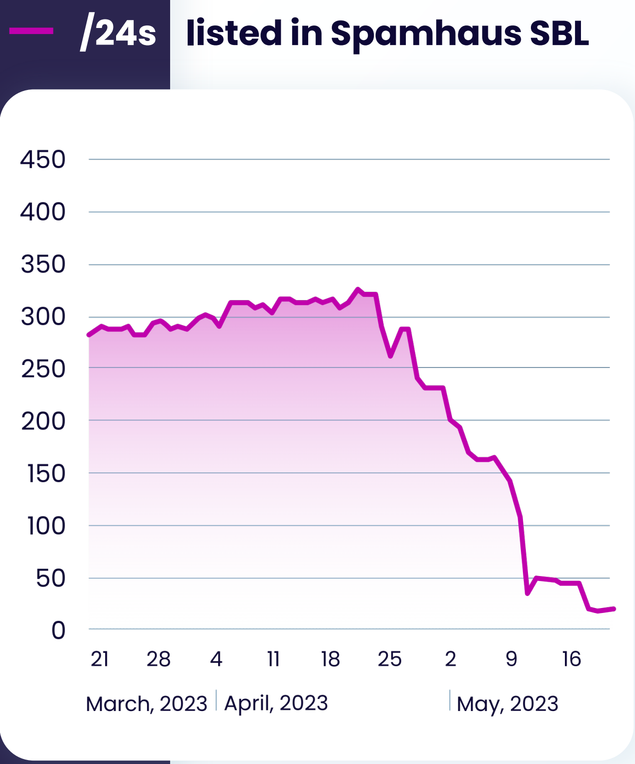
First Focus: **PTR & rDNS**

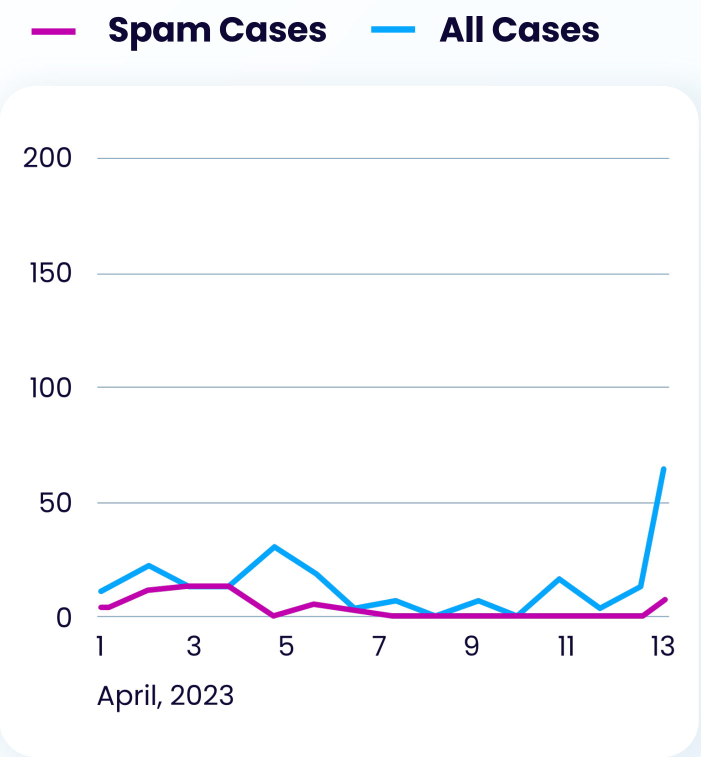
Expected results

- Reduced number of subnets listed in Spamhaus blocklists
- Negative customer feedback
- Chargebacks and temporary decline in sales followed by a return to previous

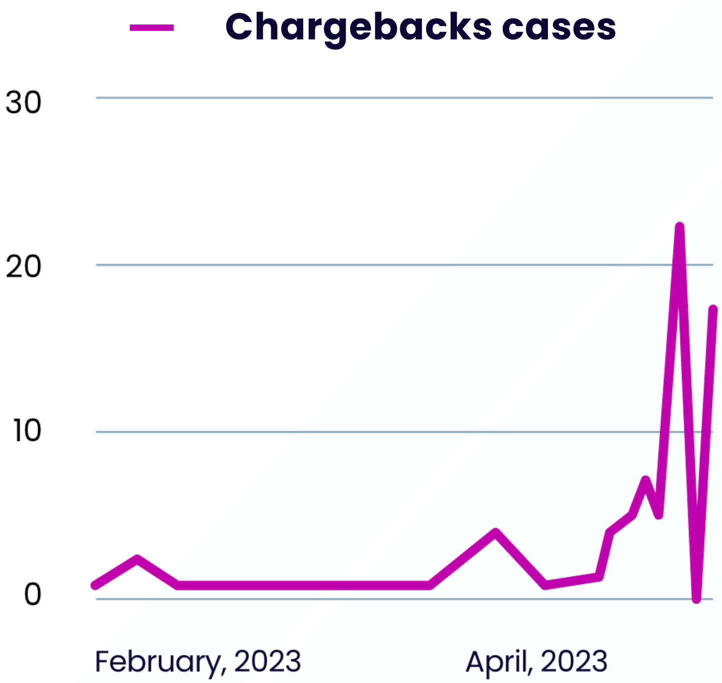
Positive Outcome

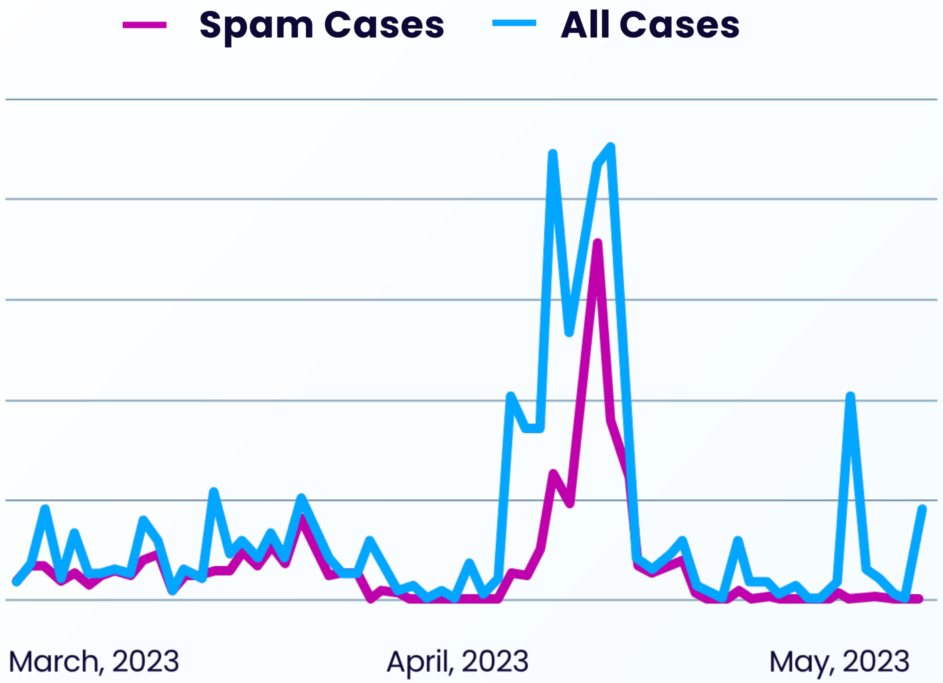
- ✓ Received less SPAM reports
- ✓ Overall decrease in SBL listings
- ✓ Overall better report statistics





Not all rainbows and sunshine





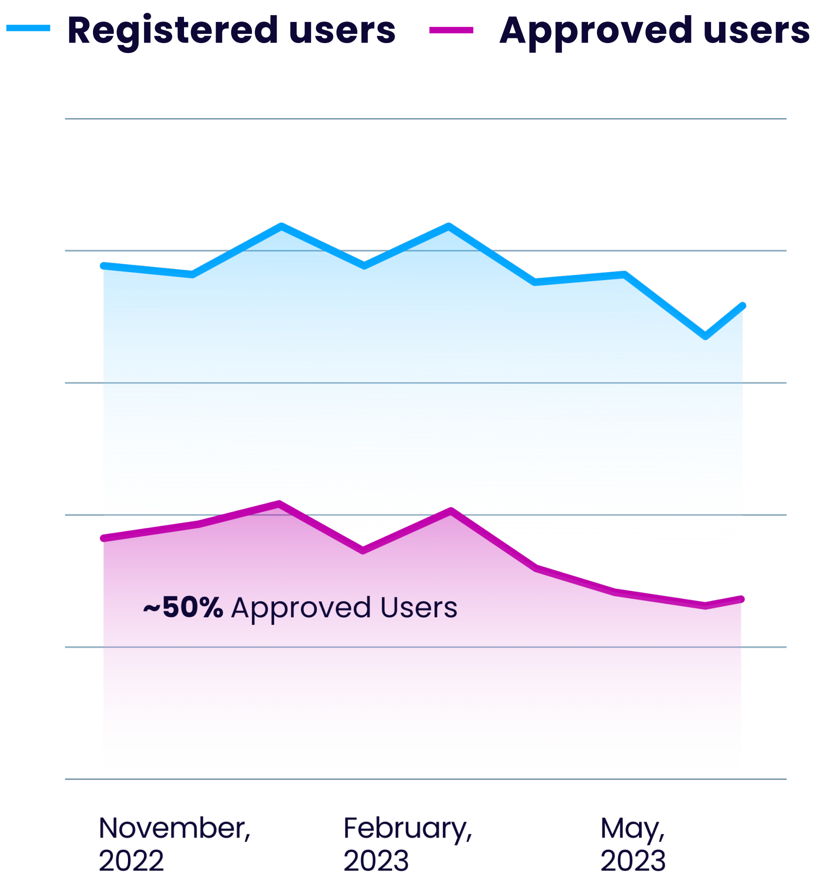
Customer backlash & Chargebacks increased after policy changes

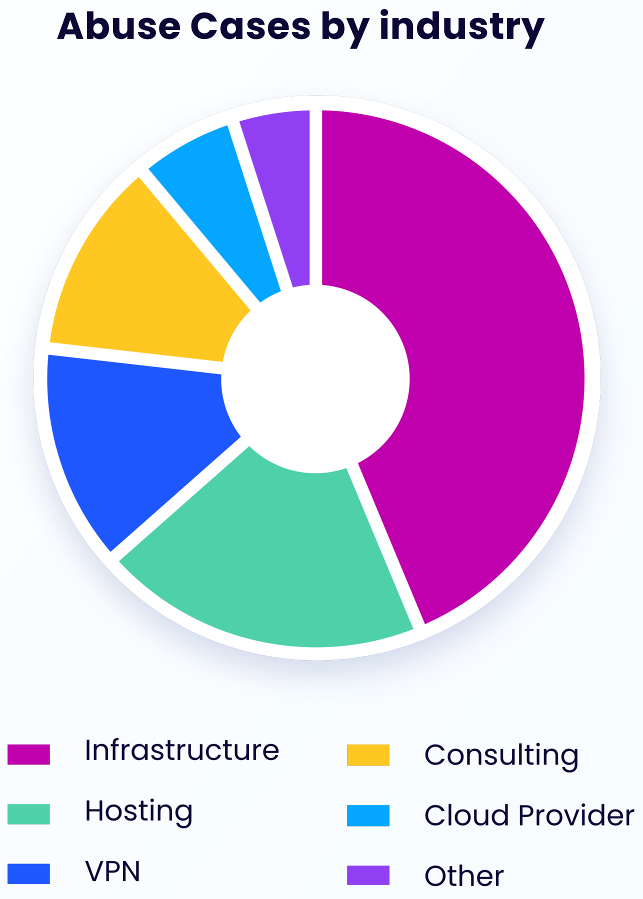
The changes proved to be affective, but more issues resurfaced

Next Focus:

KYC

- Initially, SPAM reports decreased but then surged to levels higher than before
- Malicious clients began using alternative entities to access our services
- A strategic decision was made to prioritize enhancing our KYC procedures





Next Focus: **KYC**

KYC improvements

- Only allow companies with working email, website, and in some cases, legal documents
- Conduct lookups in international USA and EU sanction lists
- Review client abuse handling policies
- Perform client domain reputation scans
- Implement additional procedures for high-risk countries

Next Focus: **KYC**

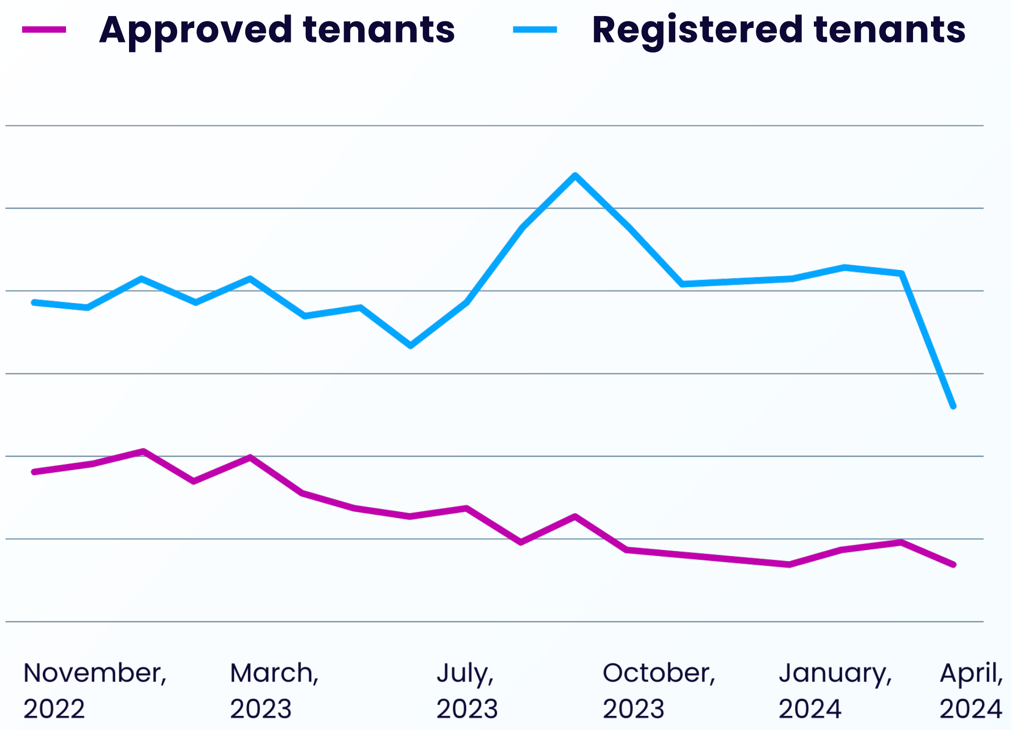
Next Focus: **KYC**

Projected challenges and downsides

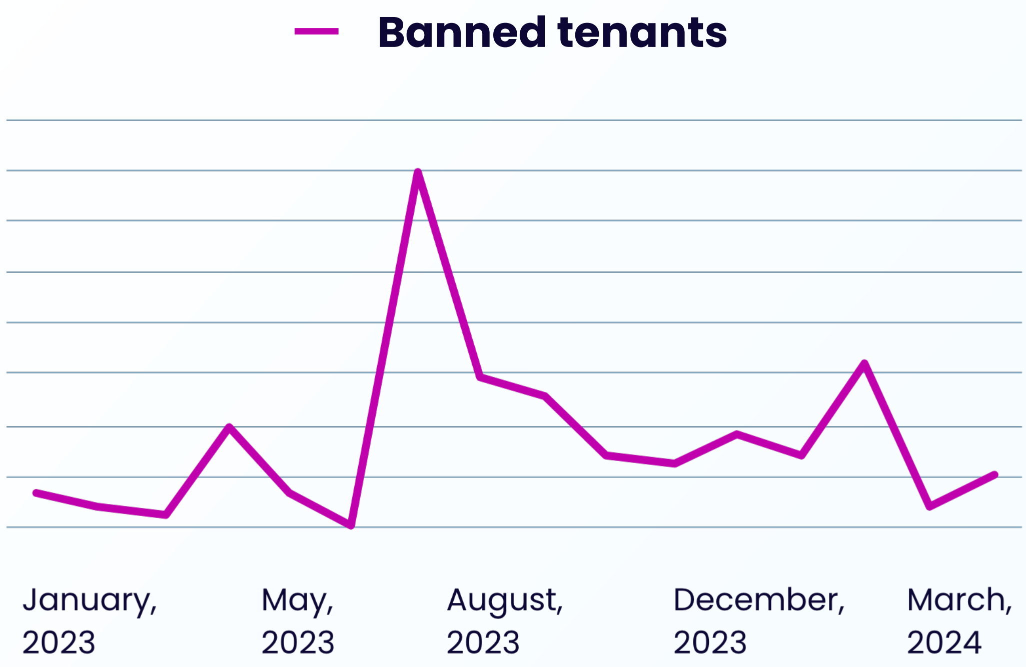
- Banning clients who do not comply with the updated KYC policy
- Addressing negative customer feedback
- Managing even more chargebacks

Outcome

- Initial approve rate fell from 50% to 25%
- Improved KYC processes lead to higher risk indicators in 12 industries

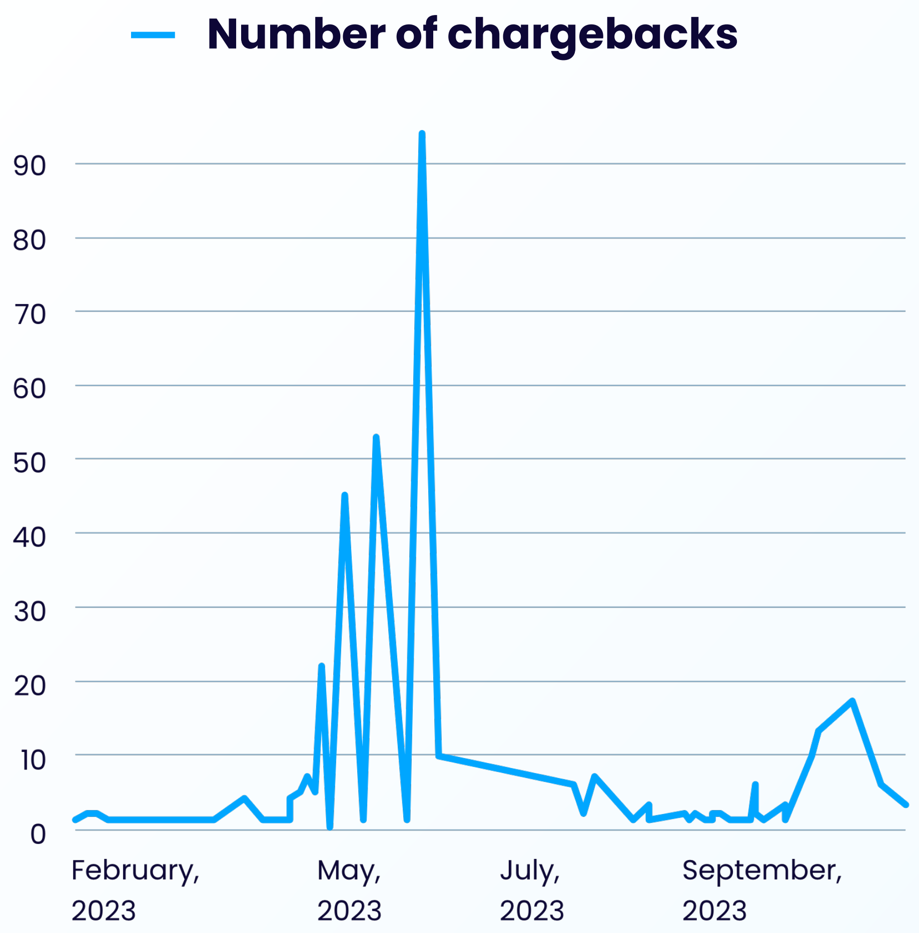


- Banned over 10% of customers in two phases
- 7 countries received the highest risk assessment scores, resulting in bans
- Experienced Distributed Denial-of-Service (DDoS) attacks for approximately two weeks



It seemed great, but...

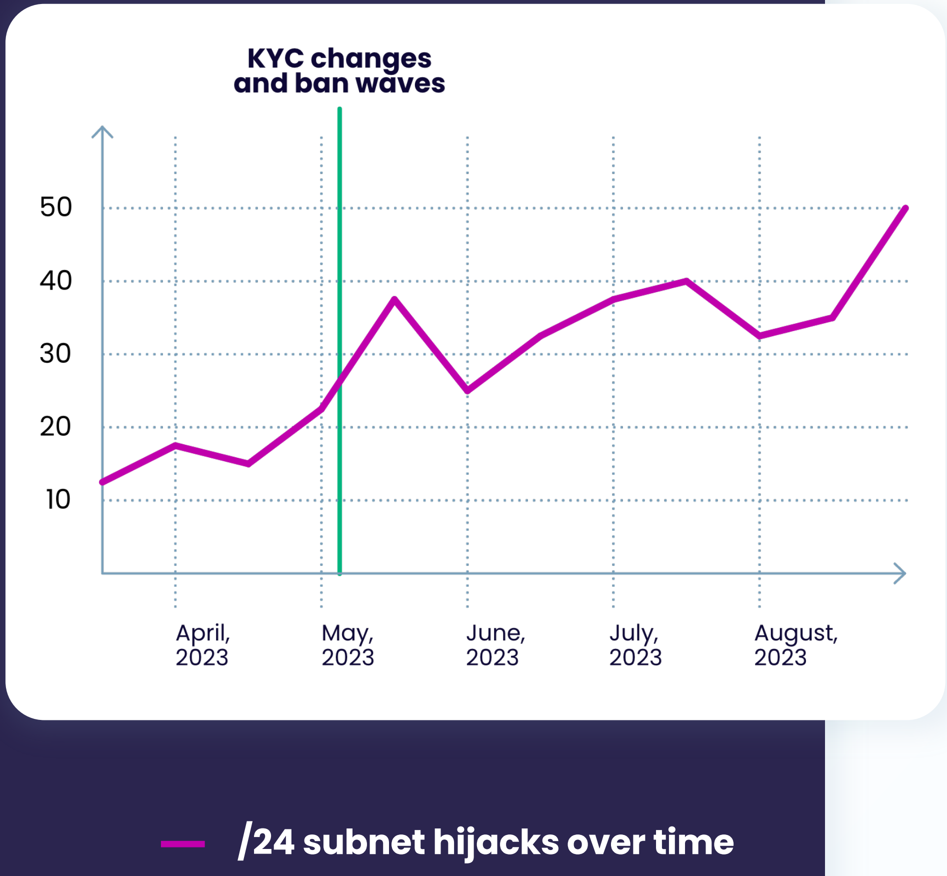
- More chargeback & DDoS attacks
- SPAM reports indicated unused IPs were mostly involved
- Focus shifted to new abuse type: Route Hijacking



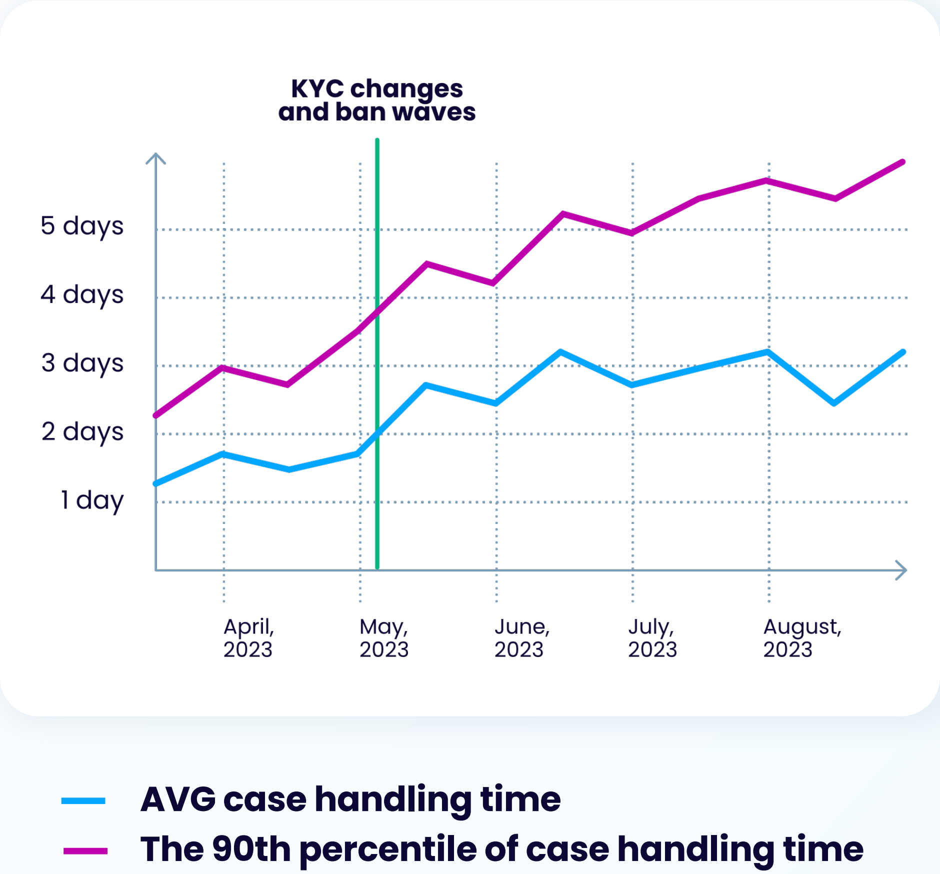
Focus:

RPKI

- Hijacks significantly damage our reputation and finances
- Resolving hijack cases required extensive manual intervention
- After the PTR and KYC policy changes, the majority of SPAM cases originated from hijacked resources
- Abuse reports (like SPAM) from hijacked IPs may wrongly implicate our legitimate users



Hijack case handling time



Next Focus: **RPKI**

Implement changes

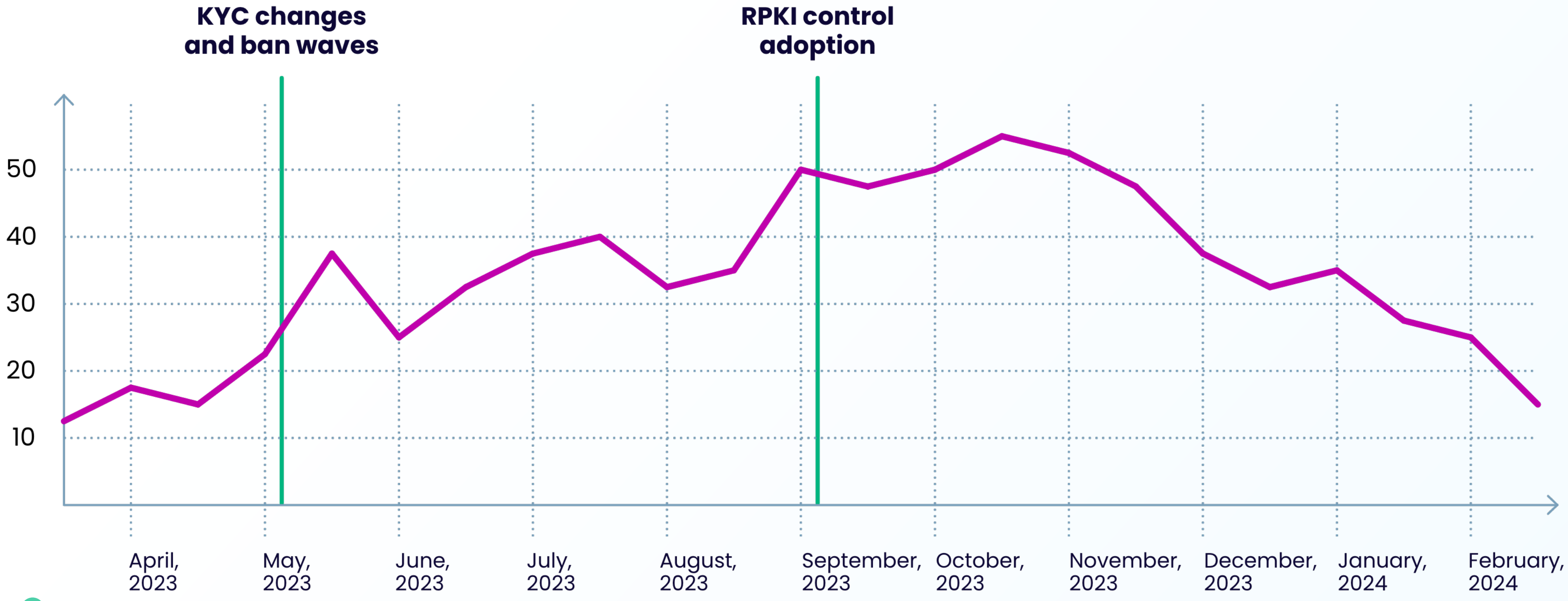
- Prepare infrastructure for RPKI control
- Introduce Border Gateway Protocol (BGP) parking for route security
- Automate RPKI control for handling hijack cases
- Establish subnet quarantine and associated handling fees
- Introduce Autonomous System Number (ASN) control (bans)

Next Focus: **RPKI**

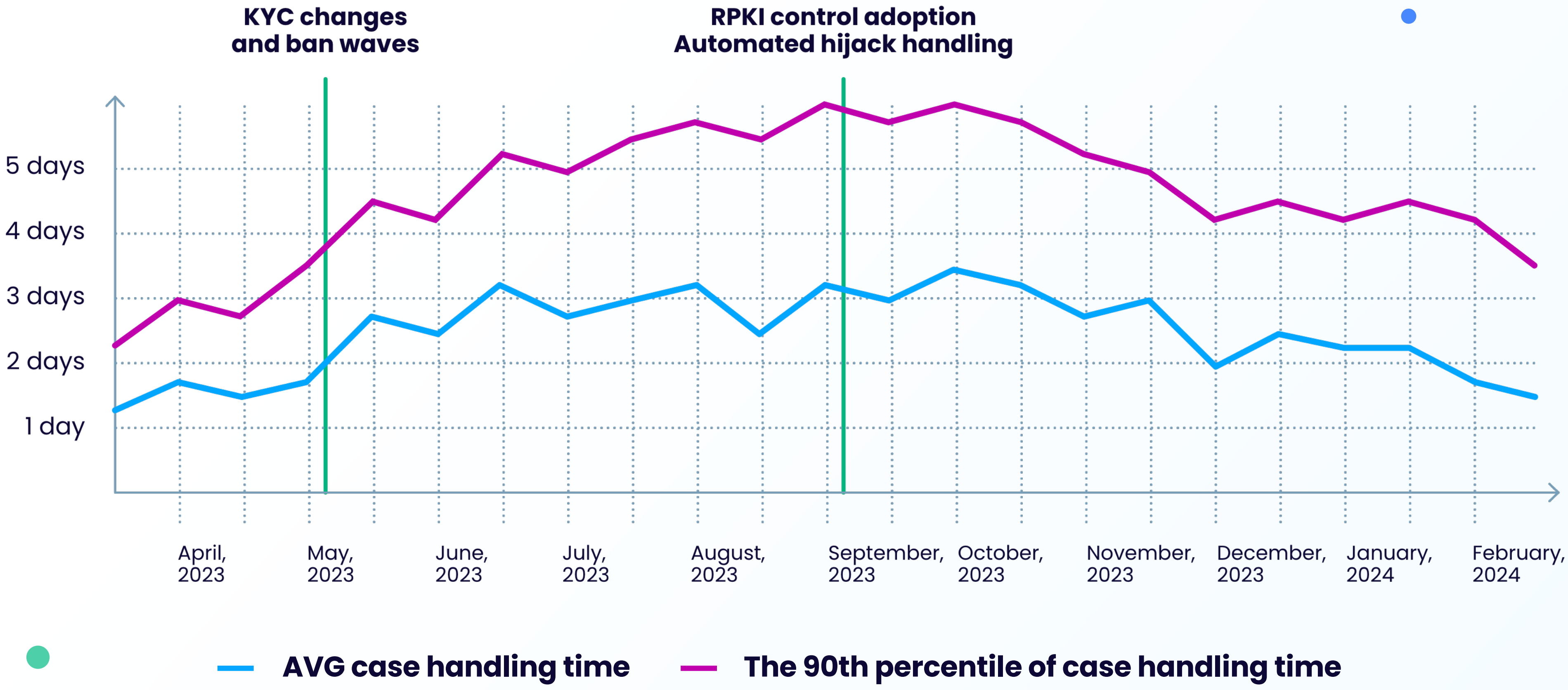
Expected challenges

- Persuade clients to grant us control of RPKI
- Clients unwilling to pay fees for handling abuse cases

– /24 subnet hijacks over time

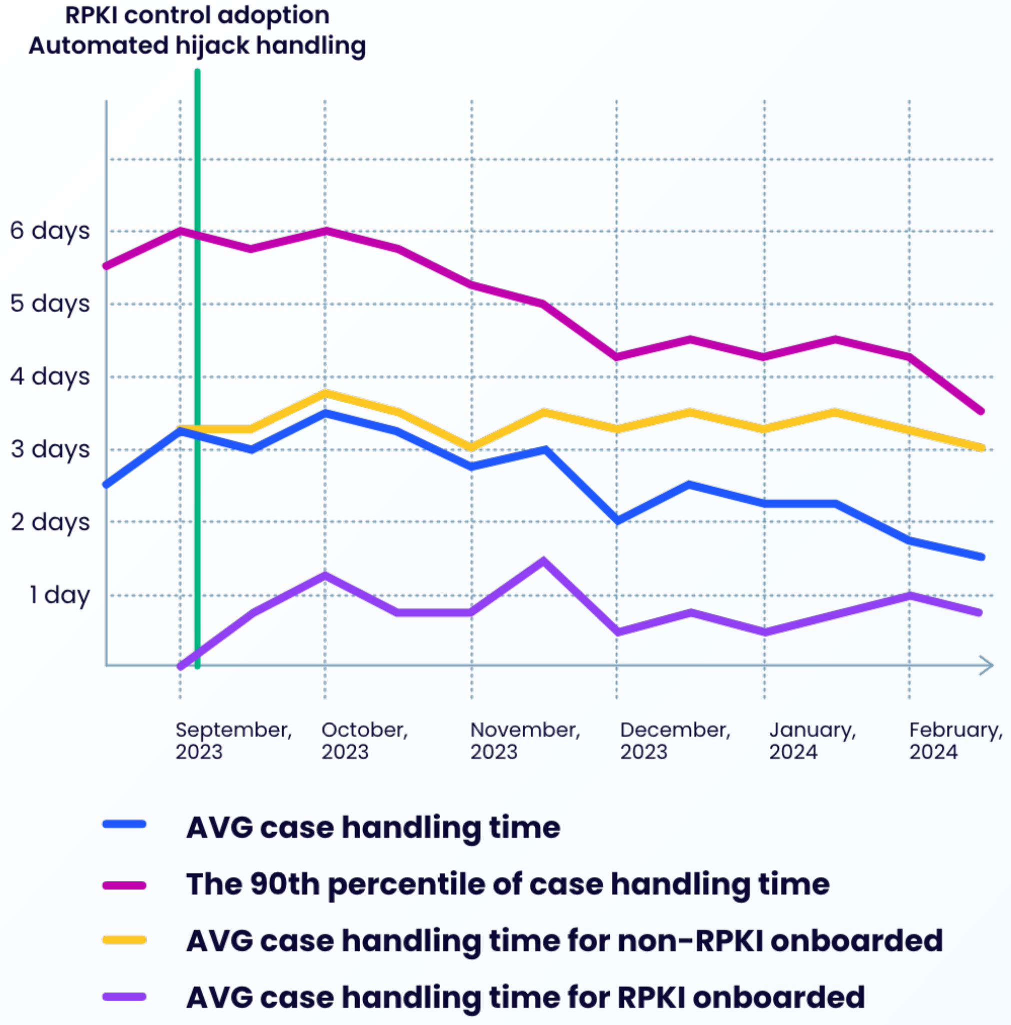


Hijack case handling time

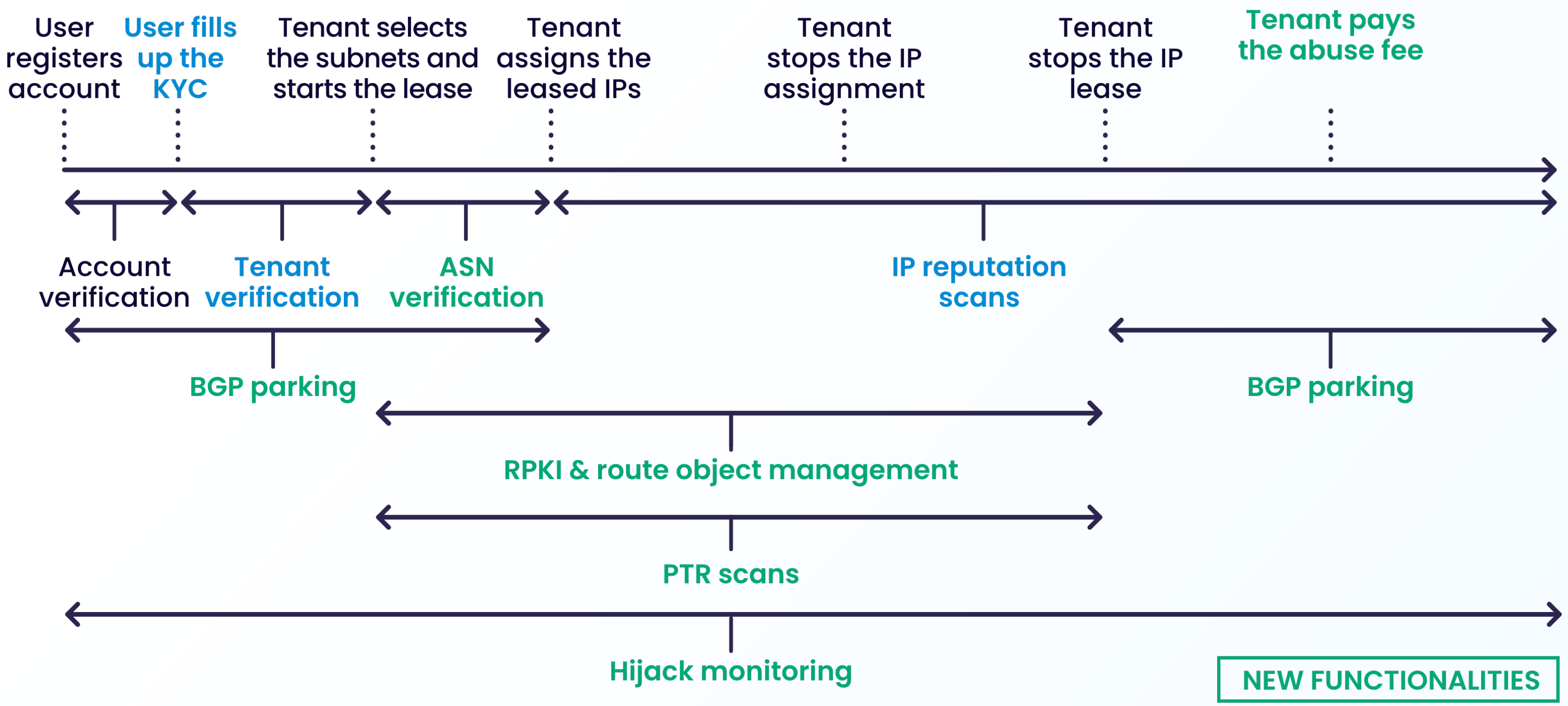


Hijack case handling time

(with RPKI controlled comparison)



All Customer Journey Improvements



User registers account

User fills up the KYC

Tenant selects the subnets and starts the lease

Tenant assigns the leased IPs

Tenant stops the IP assignment

Tenant stops the IP lease

Tenant pays the abuse fee

Account verification

Tenant verification

ASN verification

IP reputation scans

BGP parking

BGP parking

RPKI & route object management

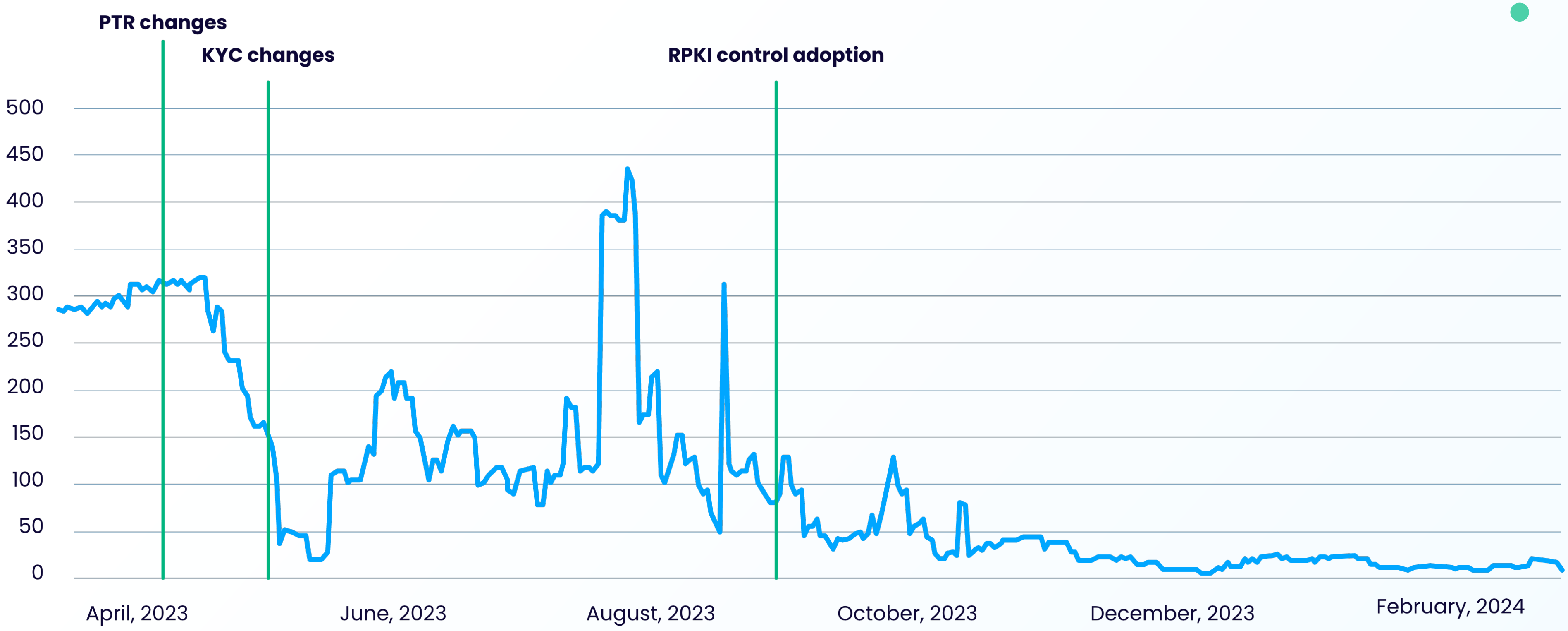
PTR scans

Hijack monitoring

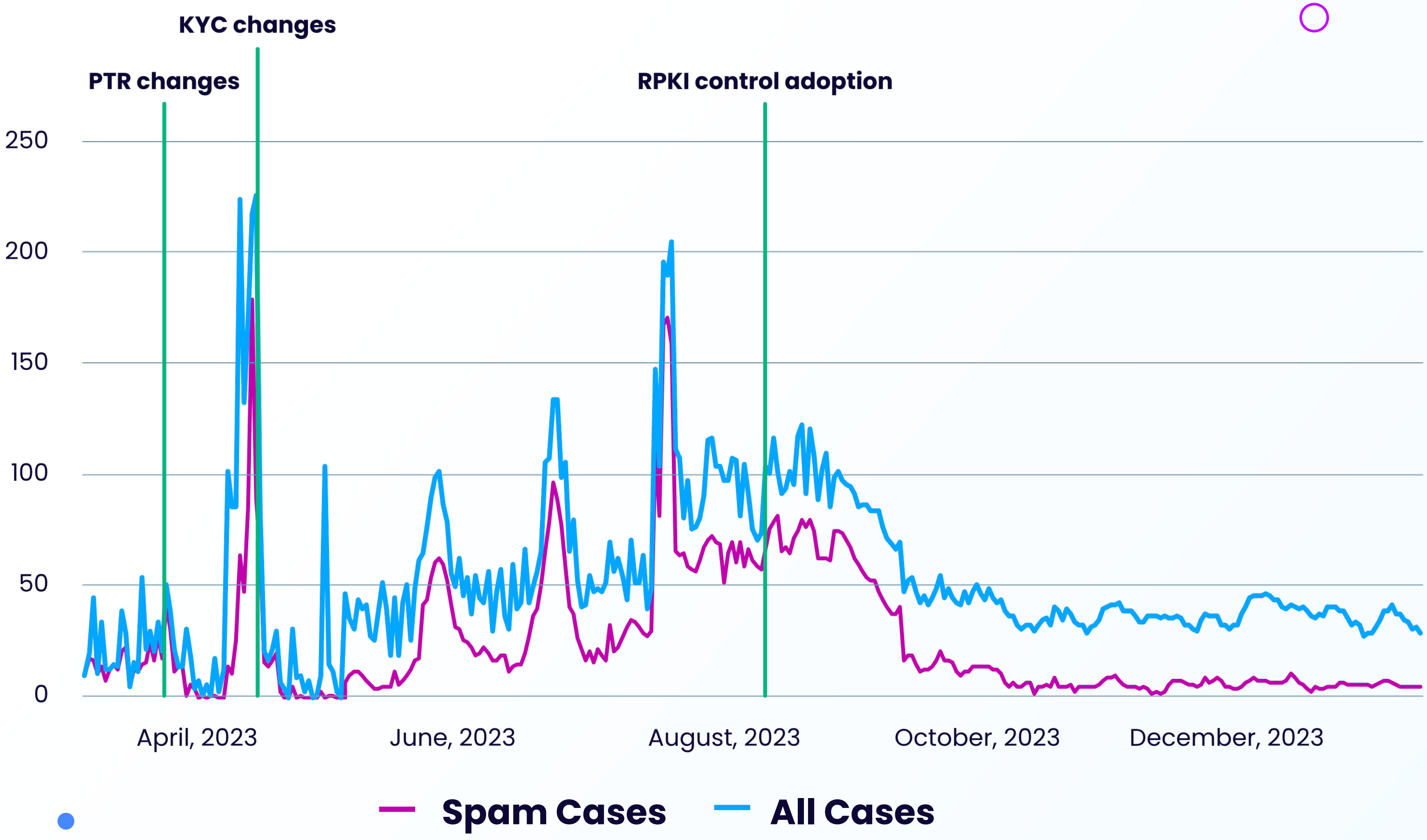
NEW FUNCTIONALITIES

MAJOR IMPROVEMENTS

Before and after implementations



— /24s listed in Spamhaus SBL


KYC changes
PTR changes
RPKI control adoption
250
200
150
100
50
0
April, 2023
June, 2023
August, 2023
October, 2023
December, 2023
Spam Cases
All Cases

Our iterative approach

- Began with changes on the PTR use policy, monitoring and automation
- Updated our TOS and KYC, which helped us get rid of malicious clients
- Deployed infrastructure for BGP parking, hijack monitoring, RPKI control
- Introduced service quarantine and fees for abuse case handling

Key learnings

- No single solution exists; it's best to combine complementary approaches
- Data collection is key for validating decisions
- Achieving significant results demands bold actions
- Do not expect immediate results
- Be prepared to lose some customers and revenue

Thanks

Feel free to reach out

in **Ignas Anfalovas**