



The Hidden Risk of Spam: IP Denylist



Presented by

Samarjit Biswas

(VP Global – Emerging Cybersecurity Technologies –Telecom

Mob - +91 9971448176 ,

Email samarjit@xelelabs.net

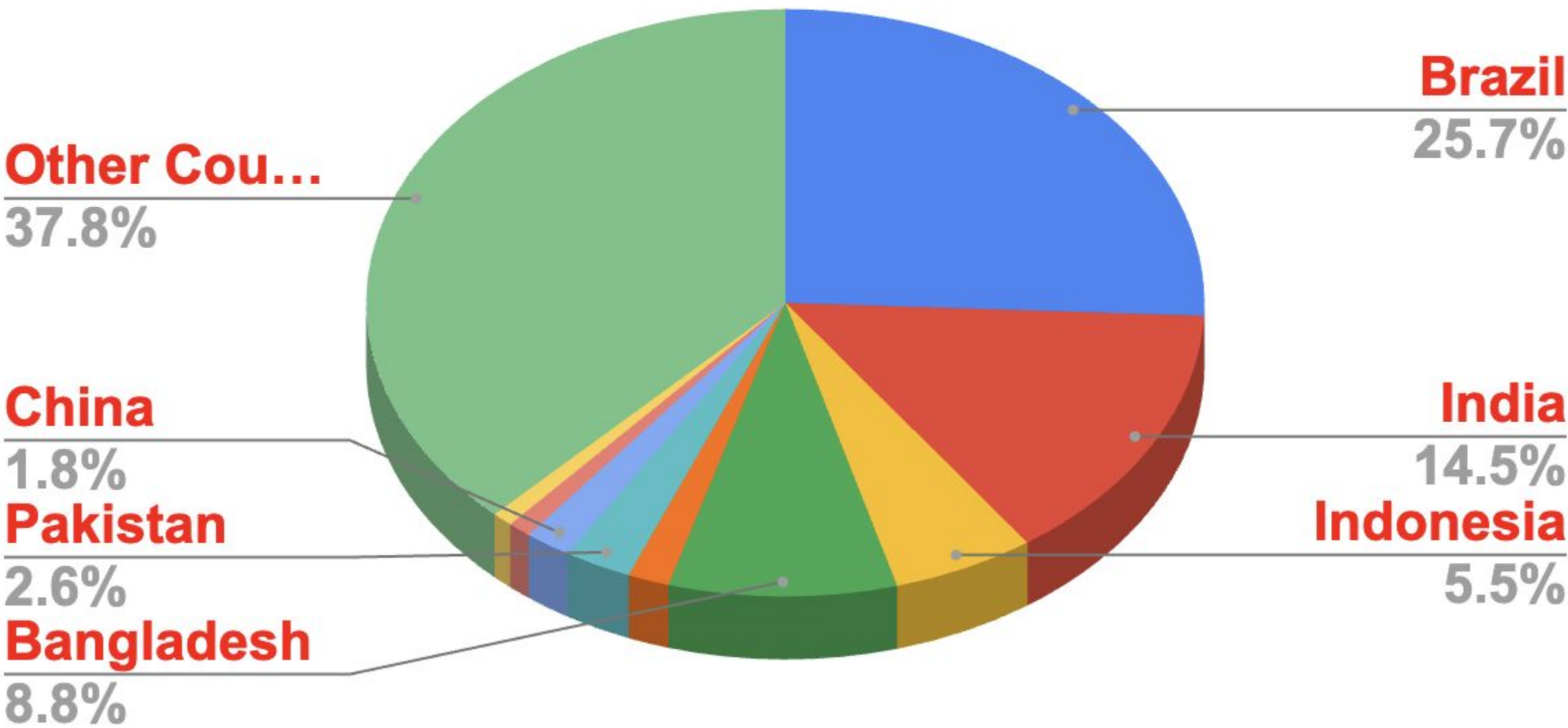
- 1 Why **IP Denylist** happens?
- 2 How banks and governments use it?
- 3 Steps to prevent or resolve **Deny list** issues?



Spam Generated Globally listed level3

source : UCEPROTECT Level 3 Charts - 8th July 2026

ASN Listed in Global Spam



Country	ASN listed %
Brazil	25.7
India	14.5
Bangladesh	8.8
Indonesia	5.5
Pakistan	2.6
China	1.8
Combodia	1.6
Taiwan	0.9
Hongkong	0.8
Other Countries	37.8

Why Are IP Addresses **Denylisted**?



Impact of RBL **Denylisting**

IPs listed on multiple RBLs (Realtime Blackhole Lists) signal that the ISP's network is a source of abuse.

Unable to access many websites protected against poor-reputation IPs

Customer complaints and service disruption

Frequent CAPTCHAs, access denials

Email delivery failures & spam folder placement

Damage to ISP organization IP reputation

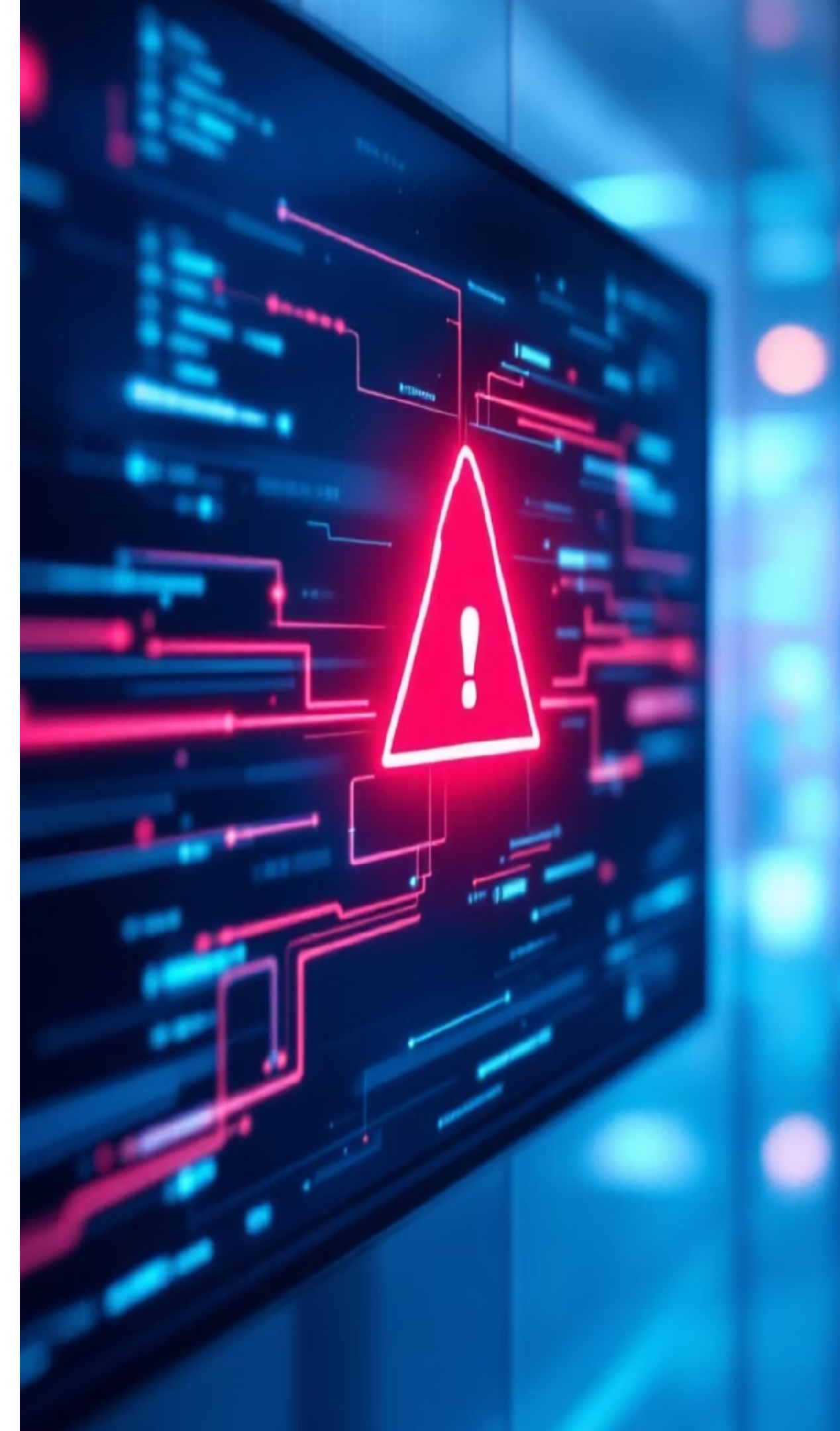
Loss of trust with service provider

Entire IP ranges or subnets getting blocked

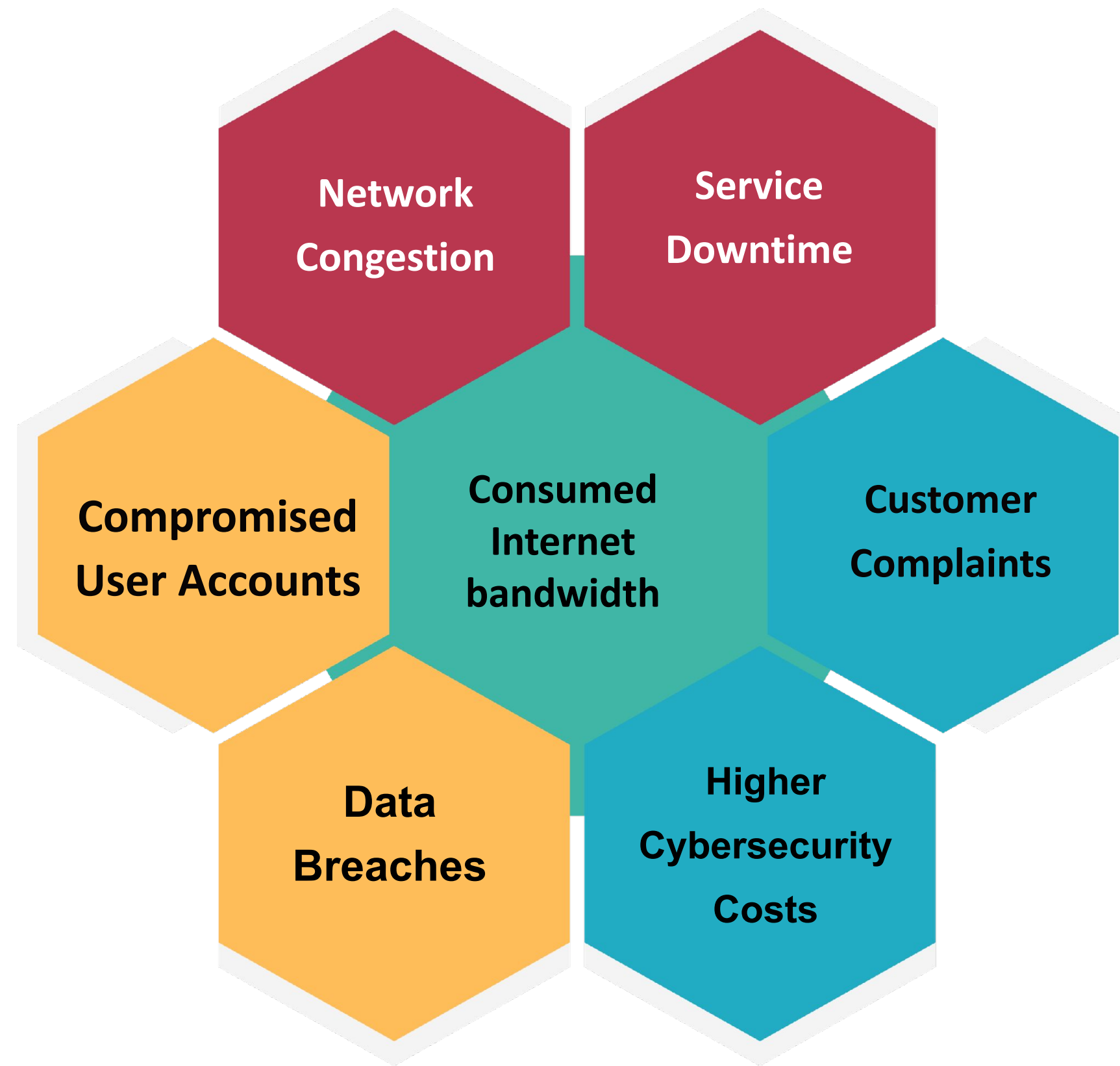
Increased delisting effort, delays, and manual intervention

Websites blocking or challenging traffic from listed IPs (e.g. Cloudflare WAF, AWS WAF, Akamai WAF , Banking portal & Govt web portal)

One infected host can impact thousands of legitimate users.



Impact of Brute-Force Attacks on Telecom & ISPs



Role of RBL (Real Time Blackhole list)



More than 50 RBLs are active Globally

How Do RBLs Denylist IP Addresses?

IPs are added to RBL Denylist when they are observed sending spam, malicious traffic, or violating network policies.

These lists are then shared with mail servers and security systems to block or filter risky IPs.



Why Do Banks & Governments Block Denylisted IPs?

Banks and governments block Deny list IPs to protect money, accounts, data, and systems from hackers, fraud, and cyberattacks.

- **Prevent Fraud** — Block IPs associated with suspicious activities.
- **Protect Data** — Reduce the risk of unauthorized access to sensitive information.
- **Block Malware** — Prevent communication with malware-infected or compromised systems.
- **Stop Cyber Attacks** — Reduce threats such as DDoS, brute-force attacks, and scanning.
- **Prevent Phishing** — Block traffic from IPs linked to phishing and malicious websites.
- **Protect Users** — Safeguard customers and citizens from online threats.
- **Meet Compliance** — Support cybersecurity policies, regulatory requirements, and risk-management practices.



Sources of Denylisted IP Data for Banks & Governments

Global Deny list Databases

They regularly pull data from public & commercial blocklists:

- ❖ Spamhaus
- ❖ Barracuda
- ❖ UCE Protect
- ❖ SORBS etc .

These lists detect spam, malware, botnets, DDoS sources, and hacking activity

Internal Security Logs

Banks and Gov systems generate their own data based on:

- ❖ Failed login attempts
- ❖ Fraudulent transactions
- ❖ Suspicious account access



List of RBLs



Major & Widely Used RBLs

- 1 Spamhaus SBL
- 2 Spamhaus XBL
- 3 Spamhaus PBL
- 4 Spamhaus ZEN
- 5 SpamCop
6. Barracuda BRBL
7. Invaluent ivmSIP / ivmSIP/24 / ivmURI
8. SORBS (multiple zones)
9. UCEPROTECT Level 1/2/3
10. PSBL (Passive Spam Block List)

General DNSBLs

11. Abuseat CBL
12. Mailspike BL / Z
13. SEM-BACKSCATTER
14. SpamRATS (RATS-DNS, RATS-NoPtr, RATS-Spam)
15. Trend Micro Email Reputation Services
16. Hostkarma (Black/White/Yellow Lists)
17. NiX Spam
18. NoSolicitado
19. SpamEatingMonkey (SEM-BL, SEM-URI)
20. LashBack UBL
21. NotJustAnotherBlacklist (NJABL) (legacy)

Country-Specific or Regional RBLs

22. DNSBL Chile
23. Brasil RB
24. China Anti-Spam Alliance
25. Korea KRBL
- 26 Russia RBLplus

Open Relay / Open Proxy / Dynamic IP Lists

27. SORBS DUHL
28. ORDB (legacy)
29. DSBL (legacy)
30. Dynablock / Dyn RBLs
31. DroneBL
32. TOR Exit Node DNSBL
33. Spamhaus DROP / EDROP
34. OpenBL.org

List of RBLs



Backscatter & Forgery Lists

35.Backscatterer.org

36.SWL (Sender Whitelist) / BSL (Blacklist)

37. NBL (NoBounce List)

Domain / URL-Based RBLs (SURBL-style)

38.SURBL multi-zone (WS, AB, JP, PH, MW, OB)

39.URIBL Black / Grey / Red

40.Spamhaus DBL (Domain Block List)

41.Invaluement ivmURI

42.PhishTank (URL-based)

43.Google Safe Browsing (domain/malware)

44.MalwareDomains.com

Commercial / Enterprise RBLs

45.Proofpoint TRAP

46.Cisco Talos Reputation Lists

47.Symantec/Broadcom Email Security Cloud

48.McAfee TrustedSource

49.Cloudmark CSI

50.FortiGuard AntiSpam Lists

51.Trend Micro Email Reputation

52.Sophos Linode DNSBL

Other RBLs & Legacy Lists

53.SpamCannibal (defunct)

54.Blackholes.five-ten-sg.com

55.AHBL (defunct)

56.SpamBusted

57.Manitu DNSBL

58.RBLKr

59.Habl RFC Ignorant

60.0spam DNSBL



Policies & Best Practices for ISPs / Telcos to Reduce IP- Denylist

Filter port 25
587, 465, 2525

Maintain proper
Reverse DNS (PTR)
records

Protect network
from Brute force
attack
Port 21 , 22, 23

Monitor IP Reputation — Continuously monitor RBLs and global reputation databases - UCEprotect .

Thanks



Samarjit Biswas

(VP Global – Emerging Cybersecurity Technologies –Telecom)

Mob - +91 9971448176 (WhatsApp)

Email samarjit@xelelabs.net