



October 2026 Risky IP Insights

Over Half of New Risky IPs Vanish Within a Week — Week-Old Blocklists Miss a Third of Active Threats

More than half of newly observed risky IPs stop showing malicious activity within a week, and a blocklist updated just seven days late misses roughly one-third of active threats. Across ~49 million risky IPv4 addresses tracked between September 27 and October 25, 2026 (77% on residential broadband), threat activity splits into a persistent 14% driving 63% of volume and a 32% single-day flash tier — while 89% of risky IPs in China are hijacked shared residential proxies.

32% / ~5d

NEW RISKY IPS LAST 1 DAY;
HALF VANISH IN ~5 DAYS

84.2% → 67.1%

BLOCKLIST COVERAGE:
SAME-DAY
VS. 1-WEEK UPDATE LAG

14% → 63%

PERSISTENT IPS (15+ DAYS)
DRIVE 63% OF RISK
VOLUME

89%

OF RISKY IPS IN CHINA
ARE HIJACKED SHARED
PROXIES

KEY FINDINGS

Four operational takeaways from 29 days of IP telemetry

Between September 27 and October 25, 2026, Threat Hunter observed approximately 49 million IPv4 addresses exhibiting risky behavior (1.3% of routable IPv4, 77% on residential broadband). That residential proxies dominate is already industry consensus; what breaks static defenses is how fast those addresses turn over and how sharply they split between persistent repeat offenders, one-day flash exits, and hijacked household routers.

32% / 42.3%

Half of a 30-day blocklist is dead weight

32% of new risky IPs last one day, half vanish in ~5 days, and only 42.3% remain active on Day 7. Bans need a 7–14 day TTL.

84.2% → 67.1%

Every day of lag leaks ~5%

A same-day 7-day rolling blocklist covers 84.2% of active risky IPs; a 1-day lag drops to 79.5%, 1 week to 67.1%, and 15.8% each day are first-time 7-day appearances.

14% → 63%

Two completely different adversaries

IPs active 15+ days are just 14% of risky IPs but drive 63% of activity (24% datacenter, 95% still active); 1-day flash IPs (32%, 81% outside China) need real-time scoring.

89%

Hijacked shared proxies in China

In China (25.1% of risky IPs), 89% are hijacked shared residential proxies (93% home broadband). Hard blocks hit real households; use step-up auth.

+29%

Non-China risky IPs rose 29%

Outside China (75% of risky IPs, <0.1% hijacked shared), weekly active risky IPs climbed 29% in October to 20.66M, led by Brazil, India, and the US.

~49M

Global baseline (1 in 75 IPv4)

80% operated as proxy exits and 22% as hijacked shared residential proxies across 77% residential, 10% mobile, and 6% datacenter networks.

Methodological note on the two "32%" figures: In the 14-day new-IP retention analysis (FIG. 2, tracking new risky IPs first seen Oct 4–11), 32% appeared only on Day 0 (68.1% remained by Day 1). Separately, across the full 29-day window (FIG. 4, Sep 27 – Oct 25), 32% of all observed risky IPs were active on only 1 day in total, accounting for 3% of total risky activity volume.

01 · SCALE & NETWORK DISTRIBUTION

~49M risky IPv4 addresses — 77% on residential broadband

During the 29-day window, roughly 49 million IPv4 addresses exhibited risky activity (1.3% of routable IPv4, or 1 in every 75 public addresses). Eighty percent (80%) operated as proxy exits, while 22% were hijacked shared residential proxies — consumer devices infected with proxy malware whose home bandwidth is resold by proxy platforms, putting legitimate households and threat actors on the same IP. Fast-flux dial-up and other categories accounted for under 1% (categories overlap slightly).

NETWORK TYPE	SHARE OF RISKY IPS	POLICY IMPLICATION
Residential broadband	77%	Dynamic ISP reassignment means bans must carry a 7–14 day TTL to avoid blocking reassigned households.
Mobile networks	10%	Carrier-grade NAT and tower handoffs require real-time scoring paired with device/session telemetry.
Datacenter	6%	Accounts for 24% of persistent (15+ day) risky IPs; ideal for direct static blocklisting.
Enterprise leased lines	5%	Fixed-exit proxies or compromised corporate egress.
Campus networks	0.3%	Shared institutional NAT gateways.

Geographically, 75% of risky IPs are located outside China across 116 countries and regions, led by Brazil (7.9%), India (7.3%), and the United States (6.7%), with Latin America, Europe, and South Asia ranking highest by region. China accounts for 25.1%.

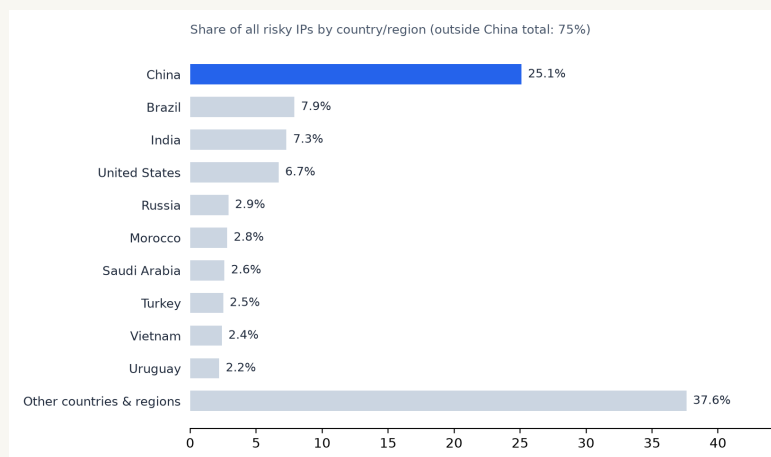


FIG. 1 Distribution of risky IPv4 addresses by country and region (Sep 27 – Oct 25, 2026; outside China total: 75%).

02 · CHURN & BLOCKLIST DECAY

Why half of a 30-day blocklist is dead weight

Newly observed risky IPs have a short shelf life. Tracking the cohort of risky IPs first seen between October 4 and October 11 over the following 14 days shows that 32% appear for only one day (68.1% remain active on Day 1), dropping to 55.2% on Day 3, 50% at roughly Day 5, 42.3% on Day 7, and 24.8% on Day 14. Across the entire 29-day dataset, nearly half of all risky IPs were no longer active in the final week.

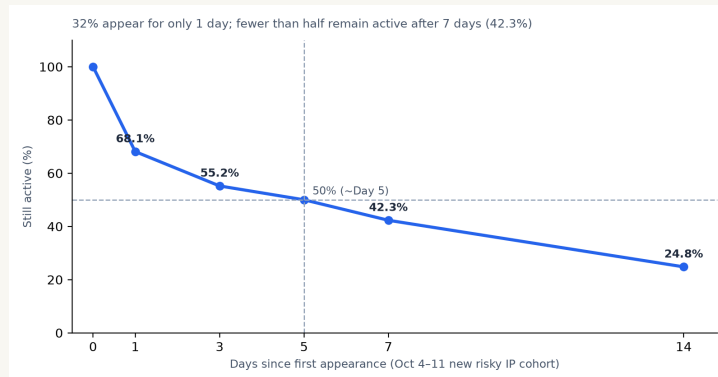


FIG. 2 14-day survival curve of newly observed risky IPs (Oct 4–11 cohort).

Operational takeaway A ban on a newly seen risky IP has an effective shelf life of about one week. Because ISPs reassign residential addresses to new subscribers, permanent bans create false positives, while a 30-day historical blocklist is nearly half inactive.

03 Every day of blocklist delay leaks another slice of risk

Using a rolling 7-day lookback blocklist ("all risky IPs seen in the prior 7 days"), interception coverage drops sharply as updates lag: a same-day update covers 84.2% of that day's active risky IPs, falling to 79.5% with a 1-day delay (nearly 5 percentage points lost), 73.4% at 3 days, 67.1% at 7 days (one-third missed), and 61.3% at 14 days. Even with a same-day refresh, 15.8% (~16%) of daily active risky IPs have never appeared in the preceding 7 days.

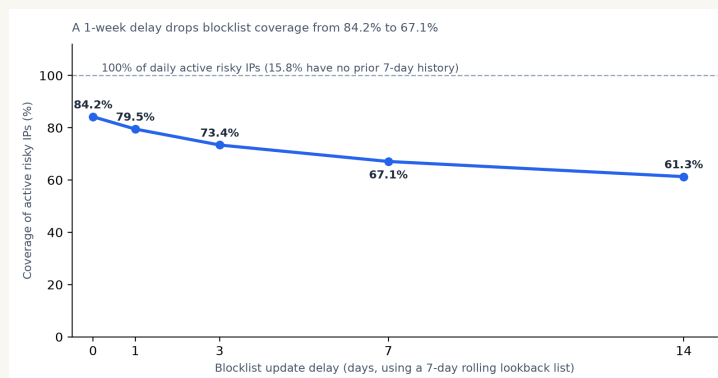


FIG. 3 Share of daily active risky IPs covered by a 7-day rolling blocklist vs. update delay in days (Oct 4–25 composite).

Operational takeaway Blocklists should update in real time — or at least daily. And because 15.8% of daily risky IPs have no prior 7-day history, no static feed can pre-list them; catching first-day threats requires real-time risk evaluation.

04 · CONCENTRATION & PROXY ARCHITECTURE

Two distinct adversaries: 14% persistent vs. 32% one-day flash

Risky IPs split into two distinct populations: a persistent minority and a transient majority. Across the 29-day window, IPs active for 15 or more days make up just 14% of distinct risky IPs but generate 63% of all risky activity (the top 10% alone drive 62%). Conversely, the 32% of IPs active on only a single day generate just 3% of risky activity.

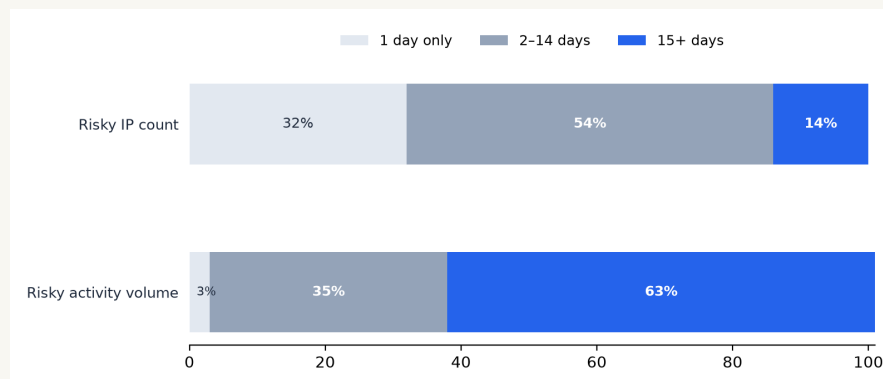


FIG. 4 Share of distinct risky IPs vs. share of total risky activity by active duration across the 29-day window.

ACTIVE DURATION (29-DAY WINDOW)	SHARE OF RISKY IPS	SHARE OF RISKY ACTIVITY	DATACENTER SHARE	STILL ACTIVE IN FINAL WEEK
1 day only	32%	3%	2%	33%
2-14 days	54%	35%	4%	56%
15+ days	14%	63%	24%	95%

Among single-day risky IPs, 81% are located outside China (only 2% in datacenters), predominantly on residential broadband and mobile networks. Persistent 15+ day IPs (where datacenter representation jumps to 24% and 95% remain active in the final week) belong on hard blocklists; single-day flash IPs must be handled by real-time scoring.

05 In China, 89% of risky IPs are hijacked shared residential proxies

Addresses in China represent 25.1% of global risky IPs, and 89% of them are hijacked shared residential proxies: 93% sit on home broadband, spread across major carriers (China Telecom 38%, China Mobile 28%, China Unicom 27%), with 45% still active in the final week (vs. 57% for other risky IPs). The remaining ~11% in China are primarily cloud-datacenter and enterprise proxy exits. Outside China, risky IPs are predominantly dedicated proxy exits, with hijacked shared proxies under 0.1% in Threat Hunter's telemetry.

Operational takeaway When traffic arrives from a risky IP in China, the connection is usually shared with an uncompromised household unaware its router or device is relaying proxy traffic. Hard IP blocks punish legitimate users; step-up verification combined with device and account signals is far safer.

06 · OCTOBER TREND & DEFENSE PLAYBOOK

Risky IPs outside China climbed 29% in October

By late October (week of Oct 19–25), weekly active risky IPs outside China reached 20.66 million — up 29% (~30%) from the late-September baseline (Sep 28 – Oct 4) and rising every week. Weekly active risky IPs in China rose and then eased to 5.98 million in the final week (up ~10% vs. week one). Whether the non-China surge continues will be tracked through November telemetry.

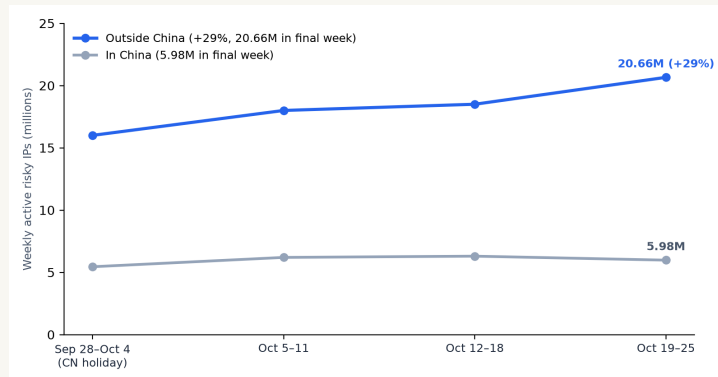


FIG. 5 Weekly active risky IPv4 addresses outside China vs. in China (millions, Monday–Sunday weeks).

07 Defense recommendations: match controls to IP churn

CONTROL LAYER	OPERATIONAL RECOMMENDATION & TELEMETRY BASIS
1. Set 7–14 day TTLs on IP bans	Over half of new risky IPs vanish within a week (42.3% active on Day 7) and nearly half of a 30-day list is inactive. Expire bans to avoid hitting reassigned home users.
2. Refresh daily + score first-seen IPs live	A 1-day lag drops coverage from 84.2% to 79.5% (67.1% at 1 week), and 15.8% of daily active risky IPs have no prior 7-day history.
3. Split persistent vs. transient tiers	Hard-block the persistent 14% (15+ days, driving 63% of activity, 24% datacenter, 95% still active); route 1-day flash IPs (32%, 81% outside China) to real-time scoring.
4. Step-up auth in China; real-time scoring globally	89% of risky IPs in China are hijacked shared proxies (93% residential) — use step-up verification. Outside China (75% of total, up 29% in Oct across Brazil, India, US), score residential/mobile sign-ups and logins in real time.

Threat Hunter continuously tracks the emergence and decay of risky IPs worldwide, providing real-time IP risk intelligence (threathunter.com/en/products/ip-risk-intelligence) so risk teams can act on an address's live state rather than an expired list.

Source: Threat Hunter IP Risk Intelligence (Sep 27 – Oct 25, 2026) · threathunter.com · Contact: tim@threathunter.com