



THREAT INTELLIGENCE REPORT

Threat landscape 2026

IPv4 threat metrics for the same period in 2025 and 2026, and the live feed as of 5 October 2026.

Period: 1 January to 5 October, UTC, in 2025 and 2026. Prepared from OneFirewall Alliance IPv4 rules and STIX 2 indicators, exported 5 October 2026. All IPv4 addresses are masked, and no member, user or token data is included.

Executive summary

What the data says

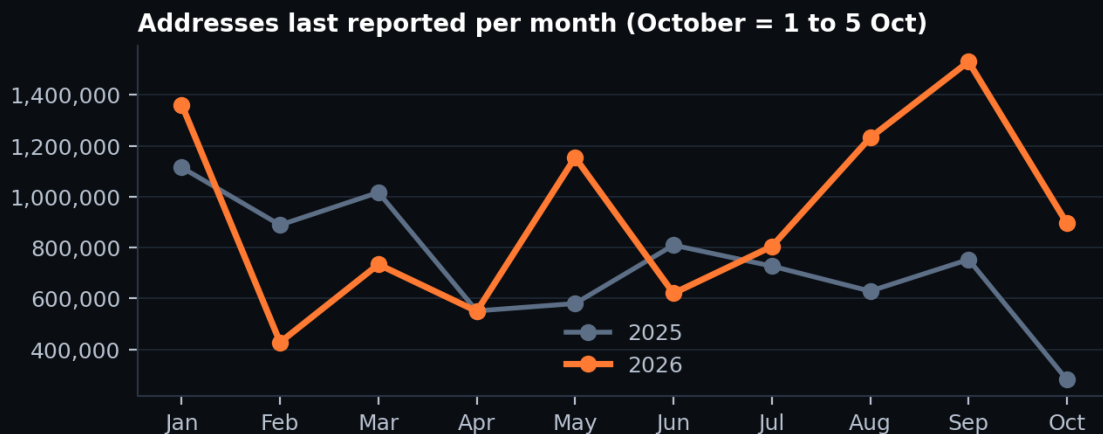
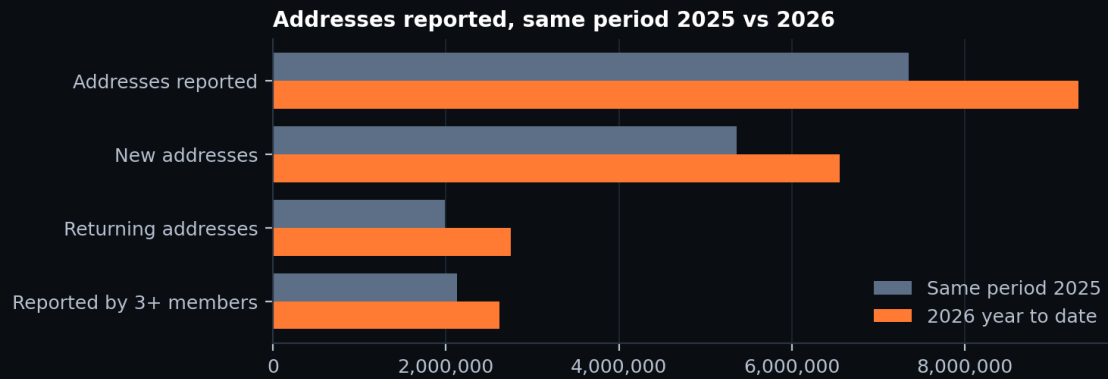
9,308,265 IPv4 addresses reported, 2026 year to date (+26.6% vs 2025)	2,755,500 Returning addresses (+38.7% vs 2025)	2,615,790 Reported by three or more members (+22.8%)
79,496 Stored score of 150 or more (+68.0% vs 2025)	2,032,103 Active addresses in the live feed today	41.4% Of active addresses are reported by three or more members

- **More addresses, and more returning.** 9.31 million IPv4 addresses were reported in 2026 so far, up 26.6%. Returning addresses grew faster than new ones (+38.7% against +22.2%).
- **More addresses are reaching the enforcement threshold.** Addresses with a stored score of 150 or more rose 68%, from 47,326 to 79,496. The 95th percentile eased slightly, from 93 to 88.
- **Port scanning and SSH brute force lead the tagged activity.** SSH brute force rose from 5,323 to 106,562 tagged rows. Many 2026 tags had no 2025 baseline, so their change reflects coverage as well as attacks.
- **Origins are shifting.** China (15.3% of 2026 rows) and the United States (13.0%) are the largest. US rows rose 77.4%, while India fell 44.4% and Iran fell 82.2%.
- **Cloud-hosted sources now make up almost half of the feed.** They account for 45.1% of 2026 rows, up from 116,522 to 4,199,580 rows. This partly reflects tagging coverage, so read it as a shift in who reports.
- **Indicators are consolidating.** STIX 2 objects fell 28.0%, while distinct indicators rose 8.5%: fewer duplicates and more unique indicators.

1 • Volume

More addresses, and more of them are returning

Addresses last reported in the same period grew 26.6% year on year. Returning addresses, first seen before the year and still reported, grew 38.7%, which means a growing share of the feed is infrastructure that was already known.



October covers 1 to 5 October in both years.

2 · Severity

More addresses reach the enforcement threshold

The TAXII threshold of 150 is crossed by more addresses in 2026. The median stored score moved from 13 to 16, while the 95th percentile eased from 93 to 88, so the most extreme scores have not grown.

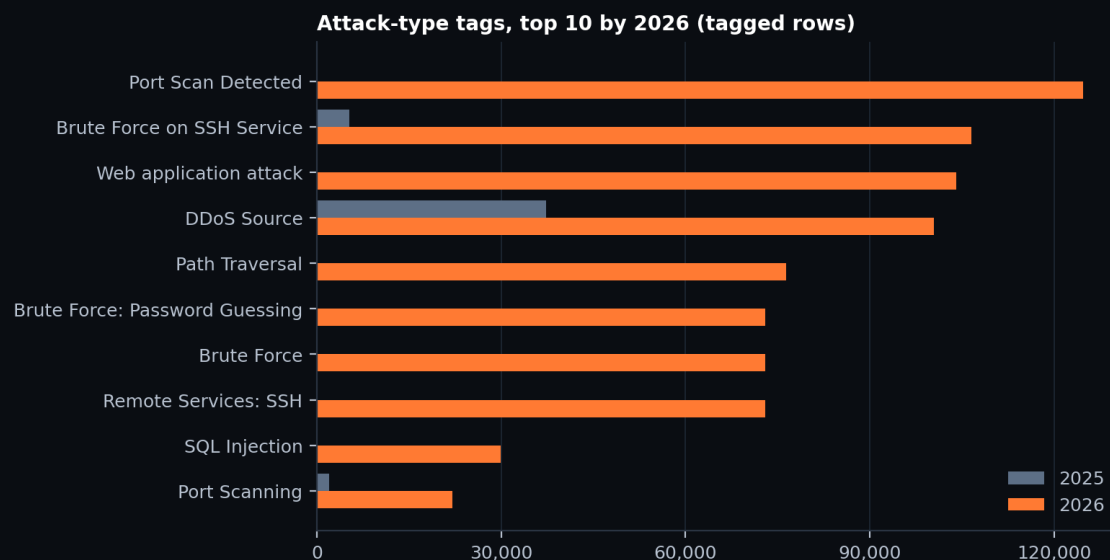
Metric	2025	2026	Change
Addresses with stored score at or above 150	47,326	79,496	+68.0%
Median stored score	13	16	+23.1%
95th percentile stored score	93	88	-5.4%

Scores are compared on the stored value for both years.

3 · Attack types

Port scanning and SSH brute force lead the tagged activity

The most common tags in 2026 are port scans (124,644 rows), SSH brute force (106,562) and web application attacks (104,015). Tags absent from the 2025 export have no baseline, so their change is shown as n/a.



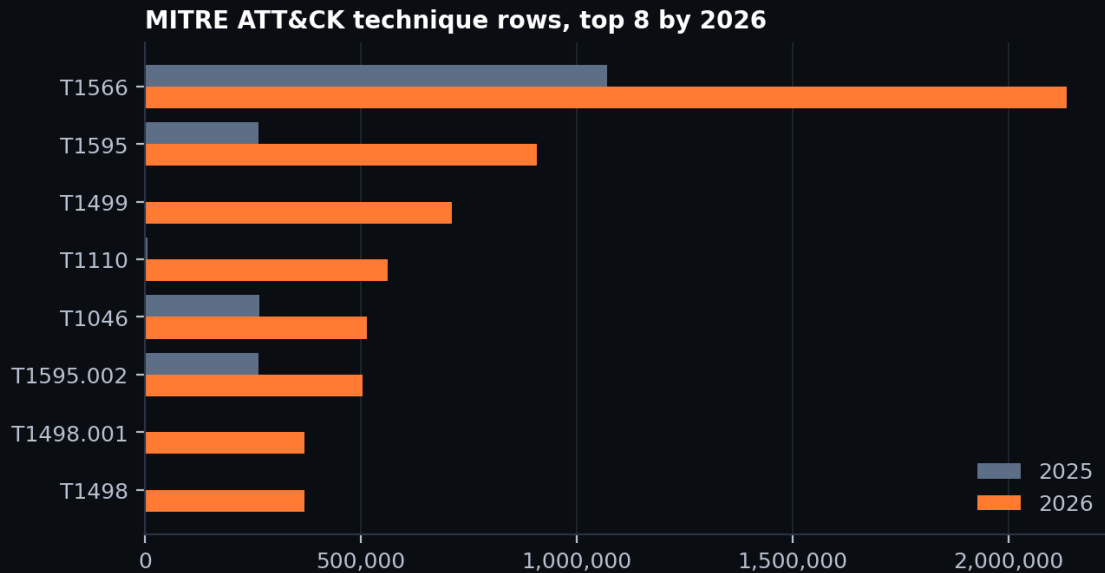
Attack-type tag	2025	2026	Change
Port Scan Detected	0	124,644	n/a (new tag)
Brute Force on SSH Service	5,323	106,562	+1901.9%
Web application attack	0	104,015	n/a (new tag)
DDoS Source	37,310	100,410	+169.1%
Path Traversal	0	76,354	n/a (new tag)
Brute Force: Password Guessing	0	73,009	n/a (new tag)
Brute Force	0	73,009	n/a (new tag)
Remote Services: SSH	0	72,986	n/a (new tag)
SQL Injection	0	29,909	n/a (new tag)
Port Scanning	1,998	22,053	+1003.8%

A row can carry several tags. Many 2026 tags were absent from the 2025 export, so their change reflects tagging coverage, not attacks alone.

4 • MITRE ATT&CK;

Brute-force grew fastest of the techniques with a 2025 baseline

Brute-force techniques (T1110) went from 6,557 rows in 2025 to 562,826 in 2026. Phishing (T1566) doubled to 2.1 million rows; T1566 also counts spam sources, so it is a broad measure.



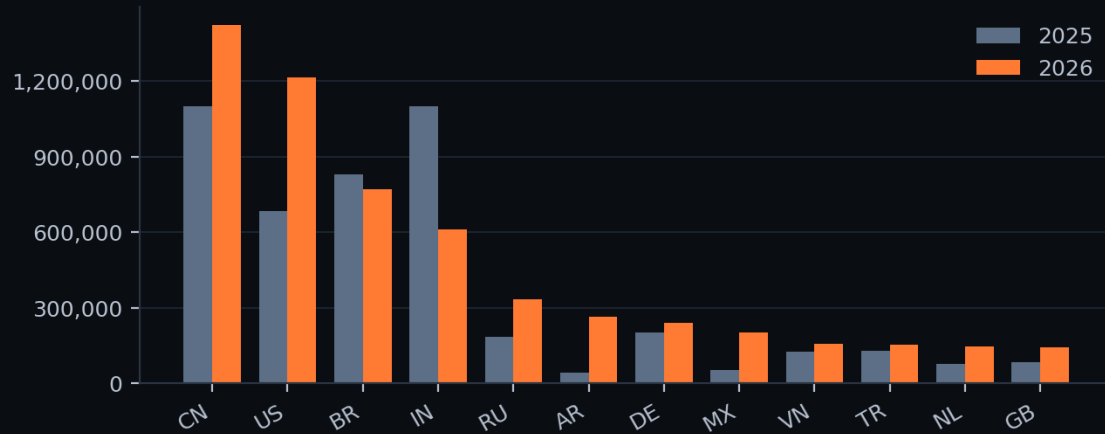
Technique	2025	2026	Change
T1566	1,070,471	2,135,415	+99.5%
T1595	263,728	907,142	+244.0%
T1499	0	710,369	n/a (new)
T1110	6,557	562,826	+8483.6%
T1046	265,721	513,710	+93.3%
T1595.002	263,728	504,045	+91.1%
T1498.001	0	370,168	n/a (new)
T1498	0	370,168	n/a (new)

5 • Origins

Origins are shifting towards the US and cloud networks

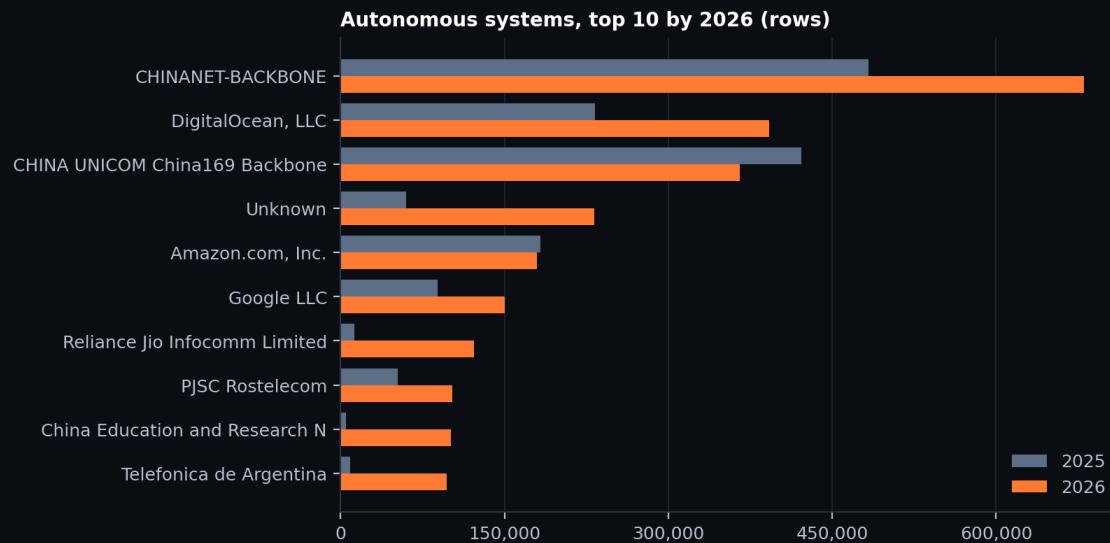
China and the United States are the largest countries of origin in 2026, at 15.3% and 13.0% of rows. Hosting and cloud networks grew strongly: DigitalOcean rose from 232,913 to 392,451 rows, and Google from 88,881 to 150,220.

Country of origin, top 12 by 2026 (rows)



Country	2025	2026	Change
CN	1,098,984	1,423,455	+29.5%
US	684,623	1,214,208	+77.4%
BR	830,886	770,807	-7.2%
IN	1,100,195	611,167	-44.4%
RU	185,043	332,917	+79.9%
AR	44,457	264,749	+495.5%
DE	201,338	239,485	+18.9%
MX	54,369	200,697	+269.1%
VN	126,955	158,319	+24.7%
TR	129,090	152,439	+18.1%

Autonomous systems with the most rows in 2026

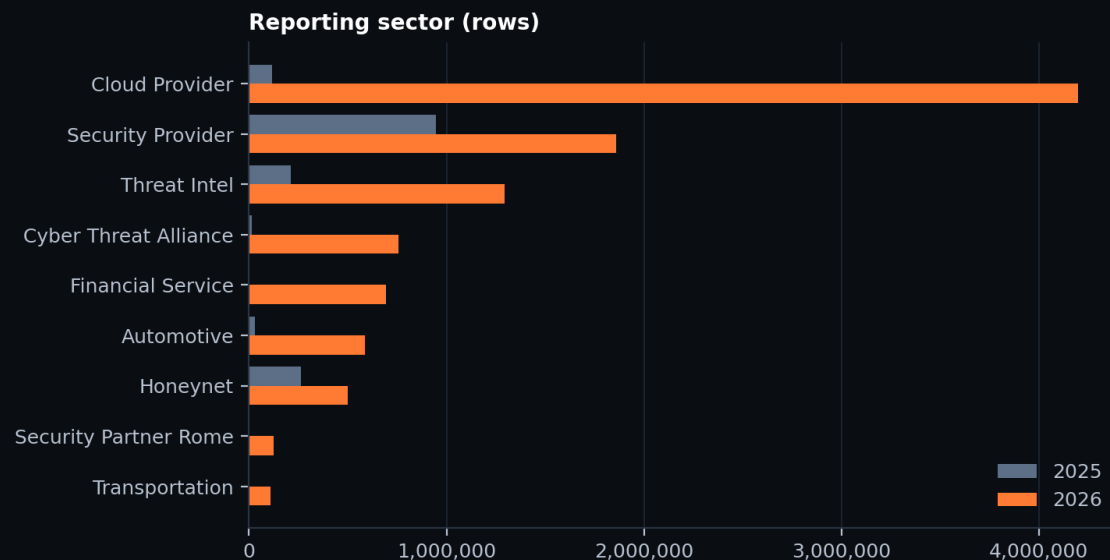


Geography uses IPinfo lite. Addresses with no autonomous system entry are shown as Unknown.

6 • Reporting sources

Cloud-hosted sources now make up almost half of the feed

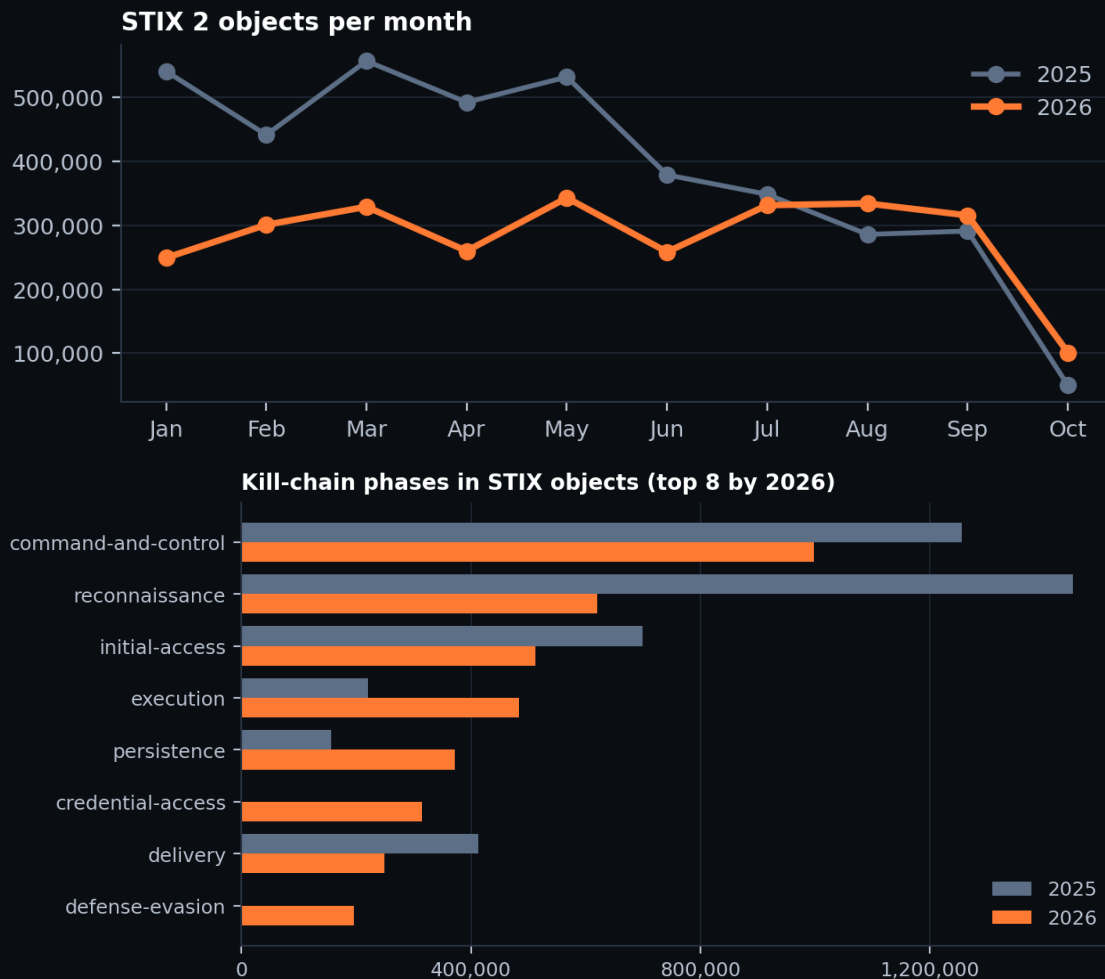
Rows reported by cloud providers rose from 116,522 to 4,199,580, which is 45.1% of 2026 rows. This is the largest change in the dataset and partly reflects which sources were tagged in each year, so read it as a shift in who reports, not in attacks alone.



7 · Indicators

Indicators are consolidating: fewer objects, more unique ones

STIX 2 objects fell 28.0%, from 3.92 million to 2.82 million, while distinct indicators rose 8.5%, from 615,234 to 667,727. Command-and-control is still the leading kill-chain phase, persistence rose from 156,386 to 371,324 objects, and credential access appeared at scale.

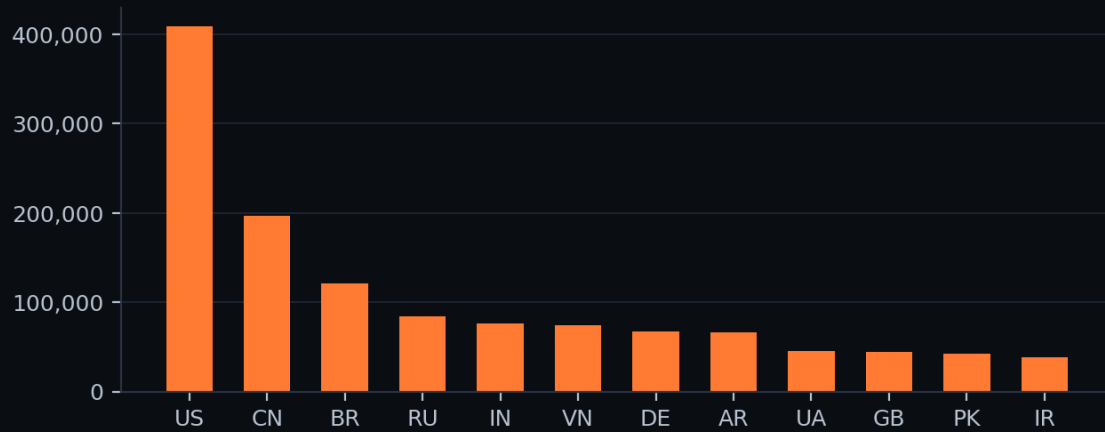


8 • Right now

The live feed as of 5 October 2026

2,032,103 addresses are active in the live feed. 840,527 of them (41.4%) are reported by three or more members. 52,605 have a displayed score of at least 150, and 1,038 score 500 or more.

Active addresses by country of origin (live feed, 5 Oct 2026)



Active attack-type tag	Rows
Port Scan Detected	82,109
Brute Force on SSH Service	64,338
Brute Force	33,047
Brute Force: Password Guessing	33,047
Remote Services: SSH	33,040
DDoS Source	26,758
Web application attack	19,310
Port Scanning	11,965

Method and caveats

How these numbers were produced

- Source: exports of OneFirewall IPv4 rules (live_rules) and STIX 2 indicators from the OneFirewall Elasticsearch, 5 October 2026.
- Periods: 1 January to 5 October, UTC, in 2025 and 2026. Change is the percentage change from 2025 to 2026.
- Tag-based metrics depend on which reporting sources and tags existed in each year. Many 2026 tags have no 2025 baseline, so their change is a coverage effect, not only a change in attacks.
- Scores are compared on the stored value for both years.
- Geography uses IPinfo lite. Some addresses have no autonomous system entry and are reported as Unknown. Sector labels have their trailing country code removed.
- Every IPv4 address is masked, with the last octet removed. No member, user or token data is included.