# topDNS Report: Monthly Analysis for ISPs

## An initiative by eco – Association of the Internet Industry in collaboration with AV-TEST

January 2026

# Contents

## Report Summary

This report is the first publication in its second year from the topDNS Initiative's measurement initiative, topDNS Report: Monthly Analysis for ISPs. The purpose of this report is to provide a credible and consistent source of metrics for addressing abuse among Internet Service Providers (ISPs). We hope that it will facilitate targeted discussions and pinpoint opportunities to re-duce abuse throughout the entire Internet ecosystem.

Key highlights from the overall data in the month of December 2025 include:

- **Malicious URL trends reached an extraordinary new peak in December 2025.**
  Total malicious URLs climbed to approximately 2,912,675 across all categories. This surge was overwhelmingly driven by malware, which rose to 2,885,933 (+128.22% vs. November), more than doubling November’s already elevated levels. This represents an increase of over 1.6 million malware URLs in a single month, the largest month-over-month rise observed across the entire reporting period. Malware accounted for 99% of all malicious URLs, the highest concentration ever recorded and a notable increase from November's already high 97%.

  In contrast, potentially unwanted applications (PUAs) declined sharply to 12,808 (-17.01%), reaching the lowest level observed within the current reporting period and less than 1% of total malicious URLs. 'Other' malicious content similarly decreased to 14,457 (-21%), dropping to approximately 0.5% of the total. December 2025 now represents the all-time peak record for malware (2,885,933), while May 2025 reflects the lowest malware point (396,207) within the current 12-month reporting window as earlier 2024 data has rotated out. Historical peaks for PUAs (July 2025: 105,835) and 'other' content (February 2025: 46,639) remain from earlier periods in 2025.

- **Phishing activity in December 2025 continued its sustained decline.**
  Potential phishing URLs decreased further to 63,090 (-25.48% compared to November's 84,658), reaching the lowest level ever recorded in the reporting period and remaining well below the overall average of 284,213. This represents an 88% decline from the April 2025 peak of 542,081. Verified phishing URLs remained largely stable at 9,339 (+0.47% vs. November's 9,295), approximately 22% below the reporting-period average of 11,921. Notably, the share of verified phishing within potential phishing increased to 14.80%, up from 10.98% in November, marking the highest verification rate observed to date. This continues a three-month upward trend (October: 5.37%, November: 10.98%, December: 14.80%). May 2025 remains the peak month for verified phishing in absolute terms (21,492).

- **Taken together, the December phishing data reinforces a clear quality-over-quantity paradigm.**
  While the absolute volume of potential phishing URLs has declined sharply – falling 88% from the April peak – the proportion of confirmed phishing has nearly tripled since October. This indicates that an increasing share of detected activity represents genuine threats. The data are consistent with either improved precision in detection systems, a shift by threat actors toward more targeted and sophisticated campaigns designed to evade initial filters, or a combination of both. The sustained three-month pattern of declining volume alongside rising verification rates points to a structural change in phishing tactics rather than short-term fluctuation.

- **The Top 50 ASNs accounted for 2,858,272 malicious URLs in December 2025.**
  This marks a dramatic increase from 1,230,309 in November, more than doubling in a single month. The December total comprised 2,833,805 malware URLs (99.14%), 12,093 PUAs (0.42%), and 12,374 'other' malicious URLs (0.43%). The increase was driven almost entirely by malware, which rose by more than 1.6 million URLs month-over-month (+136.25%), pushing malware's share to an unprecedented level within the Top 50 ASNs. PUAs declined further to their lowest level of the reporting period, falling 18.11% from already low November values.

  Across the full reporting period from January to December 2025, the Top 50 ASNs were associated with 6,913,609 malicious URLs in total, including 6,320,844 malware (91.43%), 358,500 PUAs (5.19%), and 234,265 'other' content (3.39%). Malware's 99.14% share in December represents the most extreme concentration observed among the Top 50 ASNs, substantially exceeding November's 97.51% and underscoring the increasing dominance of malware-hosting infrastructure within major autonomous systems. The concentration observed at a single provider in December further highlights the potential effectiveness of targeted intervention efforts.

This is our eighth report to cover a full 12-month period, with the reporting years rotating to make comparisons easier and patterns clearer. This is an important step towards identifying longer-term trends.

We encourage all readers to review this report and its methodology, as well as the data, and to contact us with any questions, ideas or suggestions that could help us improve and expand it. After all, our goal is to help the Internet industry and the wider community become better equipped to fight online abuse. The topDNS Initiative will publish this and future reports on the topDNS website.

For more information on the topDNS Initiative's mission and the data and sources used, please refer to the 'Background' section at the end of this document.

# Methodology

Understanding general trends in online abuse is useful for grasping phishing and malware across the ISP ecosystem, as well as identifying high-level trends over time. This report presents aggregated data for all months recorded at the time of publication.

### The malware methodology includes the following labels:

- **Malware**: The majority of AV-TEST's scan results conclude that the sample belongs to the 'malware' category. This includes classic viruses and Trojans, but is also subdivided internally into malware families and names.
- **PUA**: This stands for 'Potentially Unwanted Application'. Such applications/samples do not directly exhibit malware behaviour, but they can disrupt the user experience through aggressive advertising, hidden functions, or impaired system performance.
- **Other**: This includes samples that cannot be attributed automatically to malware or potentially unwanted applications (PUAs).

Each URL is followed by a downloadable file (either directly or as a web page in the form of an HTML file). These files are downloaded and analysed by AV-TEST tools (VTEST -> AV multiscanner system). These downloaded files are referred to as 'samples'.

### The phishing methodology includes the following labels:

- **Potential Phishing**: URLs/websites that AV-TEST receives from phishing blocklists or whose source code generates a 'phishing' detection in VTEST's static analysis are declared as 'potential phishing'. (Potential) Phishing URLs are not only downloaded, but also visualised via a browser screenshot, which is used for AV-TEST's visual phishing analysis (Phinder).

- **Verified Phishing**: All 'Potential Phishing' URLs are checked with an automated visual comparison of the screenshots. This is based on manual pre-work, where screenshots are classified as 'Phishing' or 'No Phishing' by AV-TEST staff. If a 'Potential Phishing' URL is found to be similar to a 'Verified Phishing' URL, it is automatically classified as such.

This report uses the following definitions for Uniform Resource Locator (URL), Internet Service Provider (ISP), and Autonomous System Number (ASN):

- **Uniform Resource Locator (URL)**: A URL is the address of a specific resource on the Internet. It consists of several components, including the protocol (e.g., HTTP or HTTPS), the domain name (e.g., example.com), and the path to the resource (e.g., /page). URLs are used to locate and access websites, images, videos, and other online content.

- **Internet Service Provider (ISP)**: An ISP is a company or organisation that provides Internet access to individuals and businesses. ISPs offer various connection types, including broadband, fibre, DSL and mobile data. ISPs are responsible for transferring data between users and the Internet, and they often offer additional services such as email hosting and web hosting, and security features.
- **Autonomous System Number (ASN)**: An ASN is a unique identifier assigned to an Autonomous System (AS), which is a network or group of Internet Protocol (IP) prefixes under the control of a single administrative entity, such as an Internet Service Provider (ISP), cloud provider, or large enterprise.

# Chart: Aggregate Malware Trends

This chart provides a high-level view of how many malicious URLs with ASNs have been identified by the methodology and how abuse on the Internet is changing over time. It shows the absolute volume of unique URLs the methodology has identified that are engaged in phishing, malware, PUA and other malware, broken down by category:

- **Malware URLs**
- **PUA URLs**
- **Other URLs**

A **total** of **10,684,739 malicious URLs with ASNs** were identified in the period January 2025 to December 2025, **of which:**

- **10,036,408 URLs** could be **verified as malware**,
- **373,456 URLs** have been **classified as PUA**, and
- **274,875 URLs** as **other**.

The **highest number of malicious URLs for malware** was identified in **December 2025**, representing a **new all-time record that dramatically surpassed the previous peak of November 2025**. Furthermore, **PUAs peaked in July 2025**, before **collapsing dramatically in August 2025** and **reaching their lowest point in December 2025**. In addition, **'other' content peaked in February 2025** and reached its **lowest level in May 2025**. The **lowest level for malware was recorded in May 2025,** which became the new low point in the current 12-month reporting window due to the rotation of months as earlier 2024 data cycled out.

In the latest month, December 2025, the **distribution shifted to an unprecedented extreme of malware dominance**, with malware accounting for 99% of all malicious URLs, while PUAs and 'other' content each represented less than 1%. This marks the most concentrated malware focus observed throughout the entire reporting period, departing significantly from the typical distribution seen in previous months and even exceeding November's already extreme 97% concentration.

## Malicious URLs

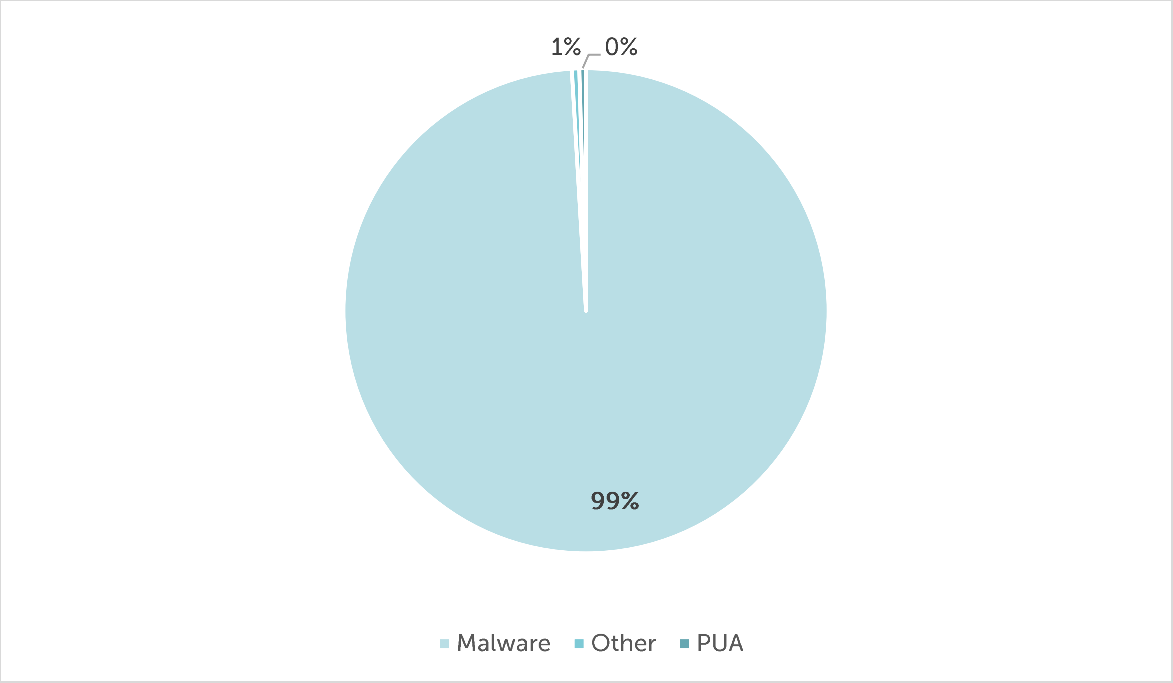

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **December 2025***

## History of Malicious URLs

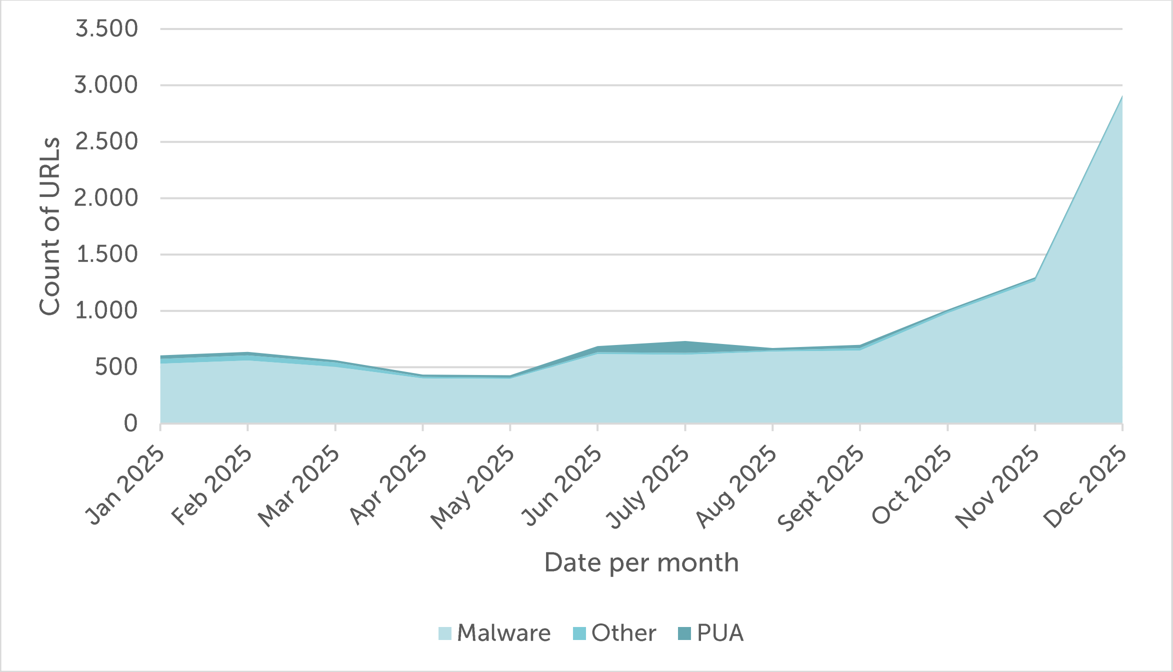

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **January 2025 to December 2025***

## History of Malicious URLs

| | Malware | Change | PUA | Change | Other | Change |
|---|---|---|---|---|---|---|
| Jan 2025 | 531,473 | | 30,652 | | 42,139 | |
| Feb 2025 | 559,089 | +5.20% | 31,846 | +3.90% | 46,639 | +10.68% |
| Mar 2025 | 504,027 | -9.85% | 20,104 | -36.87% | 39,830 | -14.60% |
| Apr 2025 | 401,518 | -20.34% | 18,739 | -6.79% | 14,600 | -63.34% |
| May 2025 | 396,207 | -1.32% | 21,305 | +13.69% | 12,011 | -17.73% |
| Jun 2025 | 615,448 | +55.33% | 54,207 | +154.43% | 18,942 | +57.71% |
| July 2025 | 612,196 | -0.53% | 105,835 | +95.24% | 15,686 | -17.19% |
| Aug 2025 | 638,238 | +4.25% | 19,551 | -81.53% | 13,272 | -15.39% |
| Sep 2025 | 647,740 | +1.49% | 27,242 | +39.34% | 23,270 | +75.33% |
| Oct 2025 | 979,973 | +51.29% | 15,734 | -42.24% | 15,728 | -32.41% |
| Nov 2025 | 1,264,566 | +29.04% | 15,433 | -1.91% | 18,301 | +16.36% |
| Dec 2025 | 2,885,933 | +128.22% | 12,808 | -17.01% | 14,457 | -21.00% |
| **Total** | **10,036,408** | | **373,456** | | **274,875** | |

*Table 1: Aggregate Malware Trends - **History of Malicious URLs** - **January 2025 to December 2025***

## Key Figures of Malicious URLs

| | Malware | Month | PUA | Month | Other | Change |
|---|---|---|---|---|---|---|
| **High** | 2,885,933 | Dec 2025 | 105,835 | Jul 2025 | 46,639 | Feb 2025 |
| **Low** | 396,207 | May 2025 | 12,808 | Dec 2025 | 12,011 | May 2025 |
| **Average** | **836,367** | | **31,121** | | **22,906** | |

*Table 2: Aggregate Trends - **Key Figures of Malicious URLs** - **January 2025 to December 2025***

## Commentary

The aggregate dataset covering January 2025 to December 2025 identified a total of 10,684,739 malicious URLs with ASNs, of which 10,036,408 were classified as malware, 373,456 as potentially unwanted applications (PUAs), and 274,875 as 'other' malicious content. The **total number of malicious URLs increased extraordinarily** from the previous reporting period, driven primarily by the unprecedented malware explosion observed in December 2025, which more than doubled the previous month's already-record levels as it entered the 12-month reporting window.

The **highest number of malware URLs was recorded in December 2025 at 2,885,933**, representing an **extraordinary new all-time peak** that dramatically surpassed the previous high of 1,264,566 in November 2025 – a 128.22% month-over-month increase. In contrast, PUA activity peaked in July 2025 at 105,835 URLs, before collapsing sharply in August 2025 to 19,551 and subsequently declining to **a new low of 12,808 in December 2025**. At the lower end, the minimum values occurred in May 2025 for malware (396,207) – which became the new low point in the current 12-month reporting window due to the rotation of months as earlier 2024 data cycled out – December 2025 for PUAs (12,808), and May 2025 for 'other' content (12,011). On average across the reporting period, monthly figures amounted to approximately 562,856 malware URLs, 30,054 PUAs, and 22,906 'other' URLs.

The dramatic surge in malware during December 2025 represents the most **dramatic escalation in the entire reporting period**, rising 128.22% from November's already record-breaking levels and adding over 1.6 million malware URLs in a single month. Meanwhile, PUAs continued their downward trajectory, falling to a new minimum at 12,808 – a 17.01% decline from November. In December 2025, the distribution **reached an unprecedented extreme of malware dominance**, with **malware accounting for 99% of all malicious URLs**, while PUAs and 'other' content each represented less than 1% – marking **the most concentrated malware focus** observed throughout the entire reporting period and significantly exceeding even November's extreme 97% concentration.

As shown in Table 2, malware activity ranged from a **new all-time high of 2,885,933 URLs in December 2025** to a **low of 396,207 in May 2025** – a span of nearly 2.5 million URLs representing more than a sevenfold increase. PUAs fluctuated dramatically, from a **new low of 12,808 in December 2025** to their **peak of 105,835 in July 2025**, while 'other' content reached a high of 46,639 in February 2025 before falling sharply in subsequent months. These figures **confirm malware's overwhelming dominance in absolute terms** and suggest that the sustained malware surges from October through December 2025 may have absorbed activity that might otherwise have been distributed across other threat categories, culminating in December’s extreme 99% malware share.

# Chart: Aggregate Phishing Trends

This chart provides an overview of how many phishing URLs with ASNs have been identified by the methodology, and illustrates how phishing on the Internet is changing over time. It shows the absolute volume of unique URLs identified by the methodology as being involved in the distribution of phishing, broken down by category:

- **(Potential) Phishing URLs**
- **Verified Phishing URLs**

A **total of 3,473,646 phishing URLs with ASNs** were identified in the period from January 2025 to December 2025, **of which 143,052 URLs** could be **verified**.

There was a further increase in January, February, March and April 2025, followed by a sharp decline in May 2025 and continued drops in June and July 2025, before a modest rise in August 2025. September 2025 saw a substantial rebound in potential phishing, but verified phishing reached a new low. **October 2025 reversed this pattern**, with potential phishing declining significantly while verified phishing rebounded moderately. November 2025 continued these divergent trends, with potential phishing plummeting to a historic low, while verified phishing increased modestly. December 2025 extended both trends, with potential phishing falling to an even lower historic minimum, while verified phishing remained relatively stable with minimal growth.

Between December 2024 and December 2025, the **highest number of all (potential) phishing URLs** was identified in April 2025, while **verified phishing URLs** peaked in **May 2025**. The **fewest of all (potential) phishing URLs** were identified in **December 2025**, marking a **new historic low for the reporting period**, while the **fewest verified phishing URLs** were identified in **September 2025**, before **rising again in October, November and December 2025.**

Notably, the verification rate (verified phishing as a share of potential phishing) reached its **highest point in December 2025 at 14.80%**, significantly exceeding November's 10.98% and nearly tripling October's 5.37%. This unprecedented verification rate suggests either substantially improved detection precision or a decisive shift toward more sophisticated, targeted phishing campaigns that are more likely to bypass initial filters.

## History of Phishing URLs

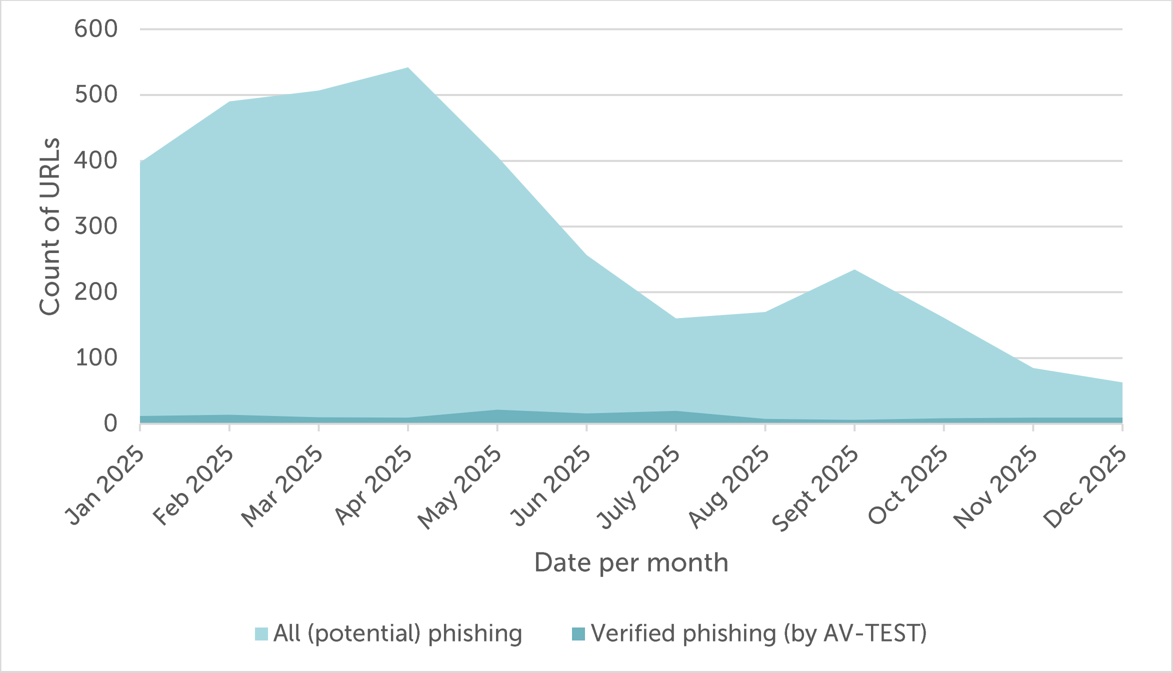

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **January 2025 to December 2025***

## History of All (Potential) and verified Phishing URLs

| | All (potential) phishing | Change | Share | Verified phishing | Change |
|---|---:|---:|---:|---:|---:|
| **Jan 2025** | 397,214 | | 3.03% | 12,043 | |
| **Feb 2025** | 490,080 | +23.38% | 2.85% | 13,972 | +16.02% |
| **Mar 2025** | 506,671 | +3.39% | 1.96% | 9,939 | -28.86% |
| **Apr 2025** | 542,081 | +6.99% | 1.72% | 9,297 | -6.46% |
| **May 2025** | 406,756 | -24.96% | 5.28% | 21,492 | +131.17% |
| **Jun 2025** | 256,529 | -36.93% | 6.20% | 15,907 | -25.99% |
| **July 2025** | 160,240 | -37.54% | 12.27% | 19,656 | +23.57% |
| **Aug 2025** | 169,908 | +6.03% | 4.36% | 7,414 | -62.28% |
| **Sept 2025** | 235,013 | +38.32% | 2.57% | 6,036 | -18.59% |
| **Oct 2025** | 161,406 | -31.32% | 5.37% | 8,662 | +43.51% |
| **Nov 2025** | 84,658 | -47.55% | 10.98% | 9,295 | +7.31% |
| **Dec 2025** | 63,090 | -25.48% | 14.80% | 9,339 | +0.47% |
| **Total** | **3,473,646** | | | **143,052** | |

*Table 3: Aggregate Trends - **History of All (Potential) and Verified Phishing URLs - January 2025 to December 2025***

## Key Figures of All (Potential) and Verified Phishing URLs

| | All (potential) phishing | Month | | Verified phishing | Month |
|---|---:|---:|---|---:|---:|
| **High** | 542,081 | Apr 2025 | | 21,492 | May 2025 |
| **Low** | 63,090 | Dec 2025 | | 6,036 | Sept 2025 |
| **Average** | **289,471** | | | **11,921** | |

*Table 4: Aggregate Trends - **Key Figures of All (Potential) and Verified Phishing URLs - January 2025 to December 2025***

## Commentary

The aggregated dataset covering January 2025 to December 2025 identified a total of 3,473,646 all (potential) phishing URLs and 143,052 verified phishing URLs. Monthly volumes of all (potential) phishing URLs exhibited **significant volatility throughout the reporting period**. After an initial rise from January 2025, which recorded 397,214 URLs, substantial increases were observed through April 2025, **peaking at 542,081 URLs**. This was followed by a sharp decline in May 2025 (-24.96%) and continued drops in June (-36.93%) and July 2025 (-37.54%), before modest fluctuations in August and September. October and November 2025 saw continued declines, with December 2025 recording a **historic low of 63,090** all (potential) phishing URLs, reflecting a 25.48% decline from November and representing an 88% decline from the April peak.

Verified phishing URLs displayed a **different pattern, peaking in May 2025 at 21,492 URLs**, before declining through June and August to a **reporting-period low in September 2025 (6,036 URLs)**. October 2025 marked a moderate recovery (8,662 URLs), followed by slight increases in November (9,295 URLs) and December (9,339 URLs).

The share of verified phishing within all (potential) phishing URLs varied significantly across the reporting period. It ranged from a low of 1.72% in April 2025 to a peak of 14.80% in December 2025. December 2025 recorded a remarkable share of **14.80%**, up from November's 10.98% and nearly tripling October's 5.37%, representing the **highest verification rate** in the entire reporting period and **well above the average of 4.19%**. On average across the reporting period, monthly figures amounted to approximately 289,471 all (potential) phishing URLs and 11,921 verified phishing URLs.

The **contrasting trends** observed over the October-November-December 2025 period – sustained declines in potential phishing alongside stable or slightly increasing verified phishing and dramatically elevated verification rates – suggest either significant enhancements in detection and verification capabilities or a fundamental shift in threat-actor tactics toward higher-quality, more targeted phishing campaigns. The 14.80% verification rate in December, combined with the historic low in potential phishing volume, strongly reinforces the **quality-over-quantity evolution** in the phishing threat landscape. This three-month progression (October: 5.37%, November: 10.98%, December: 14.80%) indicates not a temporary fluctuation but rather a sustained transformation in phishing tactics.

Overall, the reporting period highlights not only the **persistent volatility** of phishing activity, but also a decisive **shift toward more sophisticated, detectable campaigns** in the latter months, with December marking the culmination of this trend.

# Chart: Aggregated Share of Top50 ASNs

This table provides an anonymised high-level overview of the 50 largest autonomous systems identified by their assigned autonomous system number (ASN).

A **total** of **9,747,414 URLs with ASNs** were identified among the Top50 ASNs in December 2025, **of which:**

- **9,154,649 URLs** could be **verified as malware**,
- **358,500 URLs** have been **classified as PUA**, and
- **234,265 URLs** as **other**.

If you are a network operator, please contact us for further details which of the URLs mentioned above are assigned to your autonomous system number (ASN): topdns@eco.de

### Aggregated Share of Top 50 ASNs

| | Malware | Share | PUA | Share | Other | Share | Total |
|---|---|---|---|---|---|---|---|
| **Jan 2025** | 427,507 | 87.13% | 27,240 | 5.55% | 35,902 | 7.32% | 490,649 |
| **Feb 2025** | 462,960 | 87.11% | 28,352 | 5.33% | 40,141 | 7.55% | 531,453 |
| **Mar 2025** | 422,319 | 88.96% | 18,240 | 3.84% | 34,148 | 7.19% | 474,707 |
| **Apr 2025** | 343,056 | 91.93% | 18,154 | 4.86% | 11,971 | 3.21% | 373,181 |
| **May 2025** | 337,196 | 92.09% | 19,209 | 5.25% | 9,767 | 2.67% | 366,172 |
| **Jun 2025** | 494,633 | 88.07% | 52,762 | 9.39% | 14,233 | 2.53% | 561,628 |
| **July 2025** | 520,073 | 81.60% | 104,899 | 16.46% | 12,383 | 1.94% | 637,355 |
| **Aug 2025** | 547,454 | 94.97% | 19,470 | 3.37% | 10,600 | 1.84% | 577,524 |
| **Sept 2025** | 658,068 | 92.69% | 28,218 | 3.97% | 23,672 | 3.33% | 709,958 |
| **Oct 2025** | 907,850 | 96.97% | 15,095 | 1.61% | 13,261 | 1.42% | 936,206 |
| **Nov 2025** | 1,199,728 | 97.51% | 14,768 | 1.20% | 15,813 | 1.29% | 1,230,309 |
| **Dec 2025** | 2,833,805 | 99.14% | 12,093 | 0.42% | 12,374 | 0.43% | 2,858,272 |
| **Total** | **9,154,649** | | **358,500** | | **234,265** | | **9,747,414** |

*Table 5: Aggregate Trends -* ***Aggregated Share of Top 50 ASNs - January 2025 to December 2025***

## Commentary

The aggregate dataset for the Top 50 ASNs covering January 2025 to December 2025 identified a total of 9,747,414 malicious URLs. This represents the first twelve-month reporting period without the aggregated June-December 2024 block that appeared in previous reports. Of the total URLs, 9,154,649 (93.92%) were linked to malware, 358,500 (3.68%) to potentially unwanted applications (PUAs), and 234,265 (2.40%) to 'other' content.

While malware dominance remained consistent throughout 2025, the **PUA activity exhibited remarkable volatility during mid-to-late year**. After surging to a record 104,899 entries in July 2025 (16.46% of the monthly total), PUAs declined sharply to 19,470 (3.37%) in August, recovered modestly to 28,218 (3.97%) in September, then collapsed consecutively to 15,095 (1.61%) in October, 14,768 (1.20%) in November, and reached a new historic low of 12,093 (0.42%) in December – the lowest share and absolute count recorded in the entire dataset. This pattern illustrates the highly dynamic nature of PUA campaigns, which can spike dramatically for short periods before subsiding just as rapidly.

Malware activity intensified substantially in the final quarter, with **December 2025 recording an extraordinary peak of 2,833,805 entries** (99.14% of the monthly total) – the highest concentration and absolute volume in the dataset, far exceeding November's already unprecedented 1,199,728 (97.51%). December’s total of 2,858,272 malicious URLs represented a 132.32% increase over November's 1,230,309. Critically, this December surge was primarily driven by significant increases at a single provider, suggesting either a major infrastructure compromise or a concentrated shift in threat actor hosting preferences at that specific autonomous system. This near-total malware dominance, combined with PUAs collapsing to historic lows, indicates that attackers have decisively consolidated around traditional, reliable malware distribution strategies. Meanwhile, other content remained heavily suppressed at 12,374 (0.43%) in December, confirming that threat diversification tactics remain extremely limited.

In summary, while malware continues to be the overwhelming driver of ASN-based threats, the **pronounced swings in PUAs** – particularly the July 2025 spike followed by consecutive October-November-December historic lows – underscore **how rapidly attacker strategies can shift.** The December 2025 surge represents the most concentrated malware activity observed throughout the entire reporting period, with the Top 50 ASNs accounting for an unprecedented 99.14% malware share. The concentration of the December surge at a single provider further emphasizes the critical importance of targeted intervention efforts at specific autonomous systems. Network operators are encouraged to closely monitor both PUA and 'other' activity within their ASNs to anticipate potential surges and implement timely mitigation measures, while remaining particularly vigilant against the accelerating escalation of malware-based threats.

# Background

## Mission

The topDNS Initiative (https://topdns.eco) was founded in 2021 by members of eco – Association of the Internet Industry. The stable, safe and secure operation of the DNS has proven to be the foundation for the global expansion of the Internet as a universal public resource. However, like any other innovation and every technology, the Internet and the DNS are vulnerable to abuse, such as malware, botnets, phishing, pharming or spam. The topDNS Initiative and its members are committed to reducing online abuse and strengthening the Internet industry.

This report aims to measure malicious URLs at ISPs to improve the community's understanding of online abuse and ultimately enhance industry practices. We hope it will provide insight into how online abuse is changing over time, enabling concrete, specific conversations about the impact of abuse on not only the domain registration industry, but the Internet industry as a whole.

We intend to use this evidence to drive change within the Internet industry, improving understanding of where online abuse is concentrated and discussing effective ways to prevent and mitigate it. Our aim is to highlight good and best practices, as well as identifying areas for improvement and issues that require attention.

Online abuse affects everyone. We aim to leverage this insight to enhance the overall health of the Internet ecosystem. Our goal is to prevent or swiftly mitigate any harm to end users, businesses, governments, civil society organisations, public services and the general public, while safeguarding the advantages and principles of an open Internet.

Although the ultimate goal is to reduce abuse, mitigation should still take place at the appropriate level. The aim is to provide transparent resources for discussions about the prevalence and mitigation of phishing and malware on the open Internet.

## Data & Sources

This report is a collaboration with AV-TEST, a member of the Anti-Malware Testing Standards Organization, analysing samples from various sources with AV-TEST's AV Multiscanner system as well as static and dynamic analysis tools. The report aims to provide the industry with evidence and information on the distribution of phishing and malware across the ecosystem. The project will begin by examining the harm caused by malware and phishing. Phishing and malware have been chosen as the focus because there is generally sufficient verifiable evidence of the security threat they pose.

In future reports, we may include other types of abuse and additional metrics, or combine various data points, provided they are consistent with the mission of topDNS and the priorities chosen for this report. The topDNS Initiative also works very closely with other initiatives, such as the NetBeacon Institute, to work together on data and to reduce online abuse. As a result, we view this report as a complement to the NetBeacon MAP: Monthly Analysis which provides detailed statistics and data for domain name registries and registrars.

It is important to recognise the limitations of this work. The universal challenge of understanding malicious activity in society means that we can only measure identified and verified harm.

Phishing and malware that has been identified and verified will always be a subset of all existing phishing and malware. There will also be 'false positives', i.e. URLs categorised as phishing or malware when they actually aren't, due to classification errors and differences in standards. Additionally, there is a possibility that reported abuse is biased towards particular geographic regions or activities that are more likely to be reported.

We are committed to refining this project as we go along, and we welcome insights from across the industry to help us improve and iterate. If you would like to get in touch with the topDNS Initiative, please contact: topdns@eco.de

# About

## eco – Association of the Internet Industry

With approximately 1,000 member companies, eco (https://international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.

## topDNS Initiative

The stable, safe and secure operation of the DNS has proven to be the foundation for the global expansion of the Internet as a universal public resource. However, like any other innovation and every technology, the Internet and the DNS are vulnerable to abuse, such as malware, botnets, phishing, pharming or spam. The topDNS Initiative (https://topdns.eco) and its members are committed to fighting DNS abuse.

## AV-TEST Institute

AV-TEST (https://www.av-test.org/en) is an independent supplier of services in the fields of IT Security and Antivirus Research, focusing on the detection and analysis of the latest malicious software and its use in comprehensive comparative testing of security products.

Due to the timeliness of the testing data, malware can instantly be analysed and categorised, trends within virus development can be detected early, and IT-security solutions can be tested and certified. The AV-TEST Institute's results provide an exclusive basis of information helping vendors to optimize their products, special interest magazines to publish research data, and end users to make good product choices.

AV-TEST has operated out of Magdeburg (Germany) since 2004 and employs more than 30 team members, professionals with extensive practical experience. The AV-TEST laboratories include 500 client and server systems, where more than 3,500 terabytes of independently collected test data, containing both malicious and harmless sample information, are stored and processed.