AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

topDNS Report: Monthly Analysis for ISPs

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

February 2026

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

This report is the second 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 January 2026 include:

- **Malicious URL volumes contracted sharply following December's historic spike – but elevated baselines persist.**
  Total malicious URLs fell to approximately 920,355 in January 2026, a decline of nearly 69% month-over-month from December's unprecedented peak of 2,912,675. This contraction was driven almost entirely by malware, which dropped to 894,644 (-69.00%) after the December surge of 2,885,933. Despite the steep decline, malware accounted for approximately 97% of all malicious URLs, only marginally below December's record 99% concentration. Notably, January's malware total remains well above pre-October 2025 levels – which typically ranged between 400,000 and 650,000. This indicates that while the December anomaly has unwound, baseline malware activity has not returned to mid-2025 norms. Elevated post-spike baselines warrant continued monitoring.

  Potentially unwanted applications (PUAs) declined further to 12,101 (-5.52%), marking the lowest monthly value of the reporting period and continuing a sustained downward trajectory since the July 2025 peak (105,835). 'Other' malicious content fell similarly to 13,610 (-5.86%), remaining at roughly 1–2% of total malicious URLs. Both categories are now at historically low levels within the current window. Historical highs for PUAs (July 2025: 105,835) and 'other' (February 2025: 46,639) remain unchanged.

- **Phishing activity showed partial rebound in volume but declining verification rates.**
  Potential phishing URLs increased to 86,266 (+36.73%) in January, reversing the three-month downward trend that had run from October through December. Despite this rebound, volumes remain substantially below the April 2025 peak of 542,081 and well below the reporting-period average of 263,558, indicating that the late-2025 structural decline in phishing volume remains intact. Verified phishing fell sharply to 6,081 (-34.89%), the lowest level recorded in the entire reporting period. The verification share dropped to 7.05%, down significantly from December's 14.80%. This marks a clear break from the three-month upward trend in verification rates (October: 5.37%, November: 10.98%, December: 14.80%).

- **The January phishing data indicate re-expansion in volume without a corresponding rise in confirmed threats.**
  The combined pattern – rising volume alongside falling verified cases – signals a shift back toward higher-volume, lower-confirmation activity. The quality-over-quantity dynamic that defined the final quarter of 2025, characterised by declining overall volumes but rising verification ratios, has not carried into January. Whether this represents a tactical shift by threat actors, a loosening of detection thresholds, or normal monthly variation remains to be seen. Current data provide no indication of structural escalation in confirmed phishing activity.

- **The Top 50 ASNs remained highly concentrated in malware activity despite overall volume contraction.**
  The Top 50 ASNs accounted for 879,595 malicious URLs in January 2026, down sharply from December's 2,858,272. The January total comprised 856,332 malware (97.36%), 11,664 PUAs (1.33%) and 11,599 'other' malicious URLs (1.32%). The absolute volume decline mirrors the overall trend, but the concentration profile has not meaningfully changed: malware's 97.36% share within the Top 50 ASNs remains materially above the 12-month aggregate average of 91.43%, confirming that major autonomous systems continue to host a disproportionate share of malware-related infrastructure.

  Across the full February 2025–January 2026 reporting window, the Top 50 ASNs were associated with a cumulative 10,136,360 malicious URLs, comprising 9,583,474 malware (91.43%), 342,924 PUAs (5.19%) and 209,962 'other' content (3.39%). The elevated malware concentration in recent months – particularly November through January – has pushed the cumulative malware share above the mid-year average. The centralisation of malicious activity within a small number of large hosting networks continues to reinforce the case for targeted, ASN-level mitigation as an efficient lever for reducing overall malware distribution.

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 multi-scanner 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 **10,988,729 malicious URLs with ASNs** were identified in the period February 2025 to January 2026, **of which:**

- **10,399,579 URLs** could be **verified as malware**,
- **342,804 URLs** have been **classified as PUA**, and
- **246,346 URLs** as **other**.

The **highest number of malicious URLs for malware** was identified in **December 2025**, representing the **all-time record within the current reporting window, which dramatically surpassed the previous peak of November 2025**. In January 2026, **malware contracted sharply**, though it remains well above the levels observed prior to **October 2025**. Furthermore, **PUAs peaked in July 2025**, before **declining sharply in August 2025** and **reaching their lowest point in January 2026.** 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 remains the low point in the current 12-month reporting window following the rotation of earlier 2024 data.

In the latest month, January 2026, **overall volumes contracted significantly from December's historic spike.** Malware fell significantly but continued to dominate the distribution, accounting for approximately 97% of all malicious URLs, while PUAs and 'other' content each represented only around 1–2%. Although this marks a moderation from December's unprecedented 99% malware concentration, the overall distribution remains heavily skewed toward malware, confirming that the extreme concentration observed in late 2025 has eased but not fundamentally reversed.

Malicious URLs

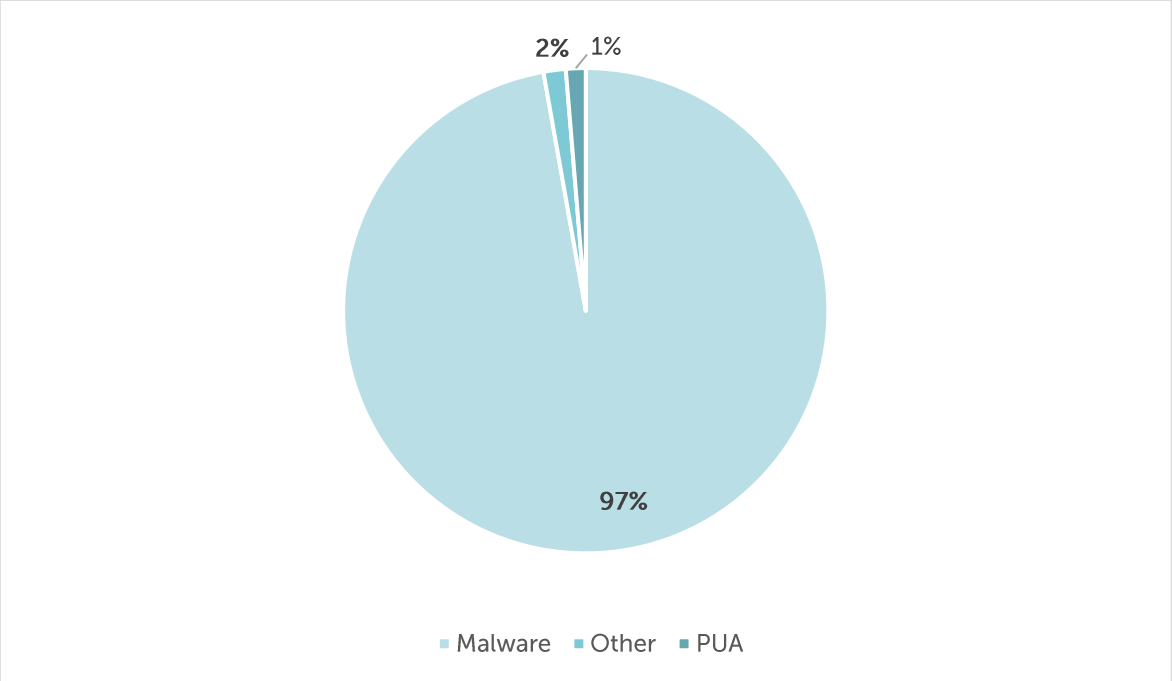

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **January 2026***

History of Malicious URLs

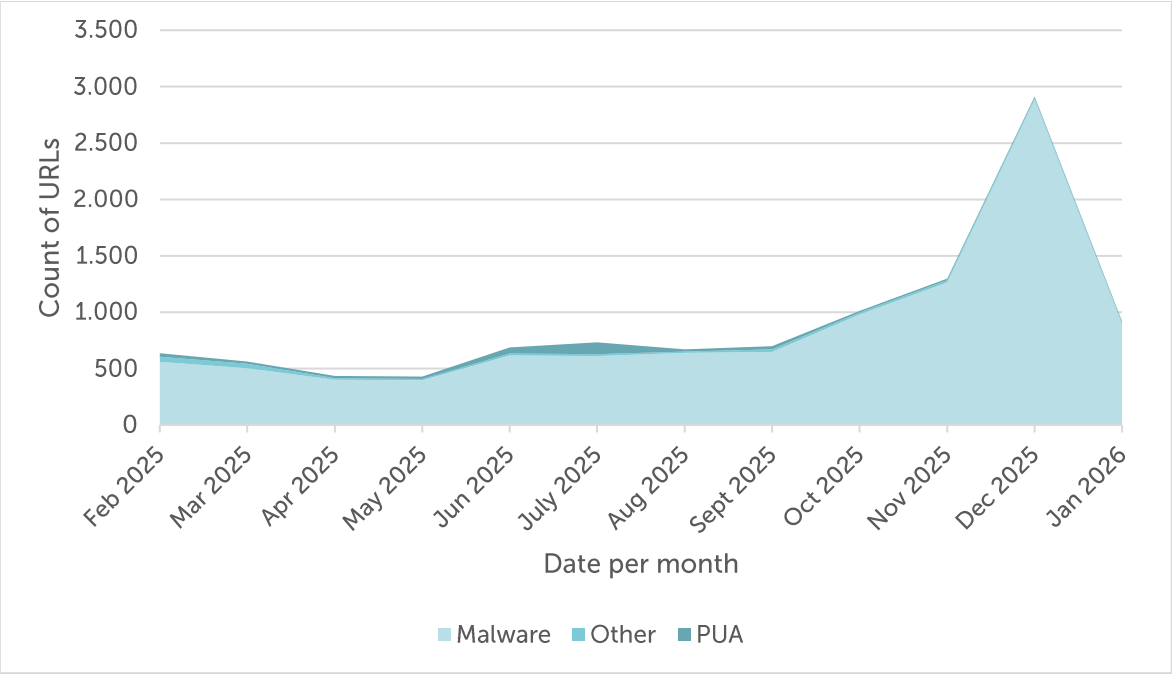

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **February 2025 to January 2026***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
Feb 2025	559,089		31,846		46,639	
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%
Jan 2026	894,644	-69.00%	12,101	-5.52%	13,610	-5.86%
Total	**10,399,579**		**342,804**		**246,346**	

*Table 1: Aggregate Malware Trends - **History of Malicious URLs** - **February 2025 to January 2026***

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	12,101	Jan 2026	12,011	May 2025
Average	**866,632**		**28,567**		**20,529**	

*Table 2: Aggregate Trends - **Key Figures of Malicious URLs** - **February 2025 to January 2026***

Commentary

The aggregate dataset covering February 2025 to January 2026 identified a total of 10,988,729 malicious URLs, of which 10,399,579 were classified as malware, 342,804 as potentially unwanted applications (PUAs), and 246,346 as 'other' malicious content. The **total number of malicious URLs increased substantially compared to the previous reporting period**, driven primarily by the unprecedented malware surge recorded in December 2025, which more than doubled November's already record-breaking levels before a significant correction occurred in January 2026.

The **highest number of malware URLs was recorded in December 2025 at 2,885,933**, representing the **all-time peak** within the current reporting window and **surpassing the previous high of 1,264,566 in November 2025 by 128.22% month-over-month**. In contrast, PUA activity peaked in July 2025 at 105,835 URLs, before declining sharply in August 2025 to 19,551 and subsequently falling to a **new reporting-period low of 12,101 in January 2026**. At the lower end, minimum values occurred in May 2025 for malware (396,207) – which remains the low point in the current 12-month reporting window following the rotation of earlier 2024 data – in January 2026 for PUAs (12,101), and in May 2025 for 'other' content (12,011). On average across the reporting period, monthly figures amounted to approximately 866,632 malware URLs, 28,567 PUAs, and 20,529 'other' URLs.

Following December's historic spike, January 2026 saw malware contract sharply to 894,644 (-69.00%), the **steepest single-month decline in the reporting period**. Despite this correction, malware continued to account for approximately **97% of all malicious URLs** – only marginally below December's unprecedented 99% concentration. PUAs continued their downward trajectory, falling to a **new reporting-period minimum of 12,101** (-5.52%), while 'other' content similarly declined to 13,610 (-5.86%). January's distribution thus remains heavily skewed toward malware, confirming that while December’s extreme concentration has partially eased, the **structural dominance of malware within total malicious URL activity has not meaningfully reversed**.

As shown in Table 2, malware activity ranged from an **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 from a new low of 12,101 in January 2026 to their peak of 105,835 in July 2025, while 'other' content reached a high of 46,639 in February 2025 before falling across subsequent months. These figures **confirm malware's overwhelming dominance in absolute terms** throughout the reporting period, and indicate that the sustained malware surges from October through December 2025 – even as they partially unwound in January – have established a structurally elevated baseline that departs materially from mid-2025 norms.

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 3,162,698 phishing URLs with ASNs** were identified in the period from February 2025 to January 2026, **of which 137,090 URLs** could be **verified**.

There was a continued increase in potential phishing from January through April 2025, followed by a sharp decline beginning in May and extending through June and July 2025. August saw a modest rebound, while September 2025 recorded a substantial increase in potential phishing activity. **October 2025 reversed this pattern**, with potential phishing declining significantly, and November saw a further sharp drop to one of the lowest levels in the reporting period. December 2025 extended this downward trajectory, reaching a new historic low. In January 2026, potential phishing rebounded moderately, while verified phishing declined sharply to its lowest level in the reporting window.

Across the reporting period, the **highest number of all (potential) phishing URLs** was recorded in April 2025, while **verified phishing peaked in May 2025**. The **lowest level of potential phishing occurred in December 2025**, marking the **historic minimum**, whereas **verified phishing reached the second lowest point in January 2026 (6,081)**.

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 October's 5.37%, before declining to 7.05% in January 2026. This reversal indicates that the late-2025 pattern of declining volume combined with rising verification rates did not persist into January, suggesting a return to broader, less targeted detection activity rather than a continued concentration of confirmed phishing threats.

History of Phishing URLs

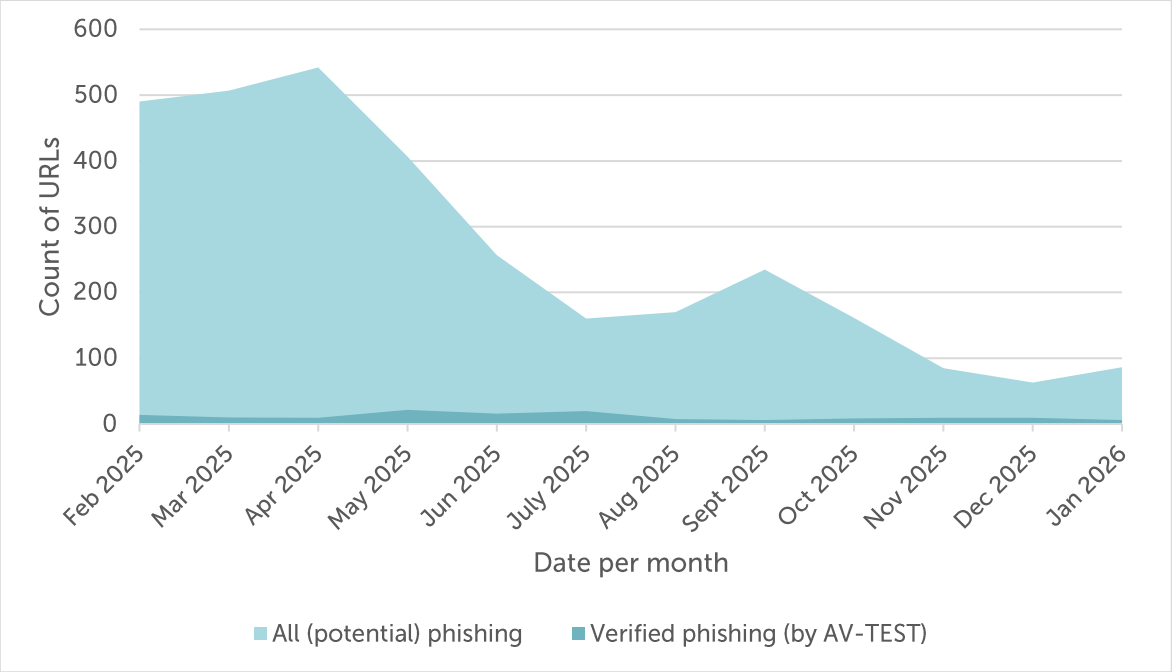

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **February 2025 to January 2026***

Over the past year, AV-TEST has further expanded its phishing analysis in order to obtain more reliable URLs that actually distinct phishing from the potential phishing URLs.

In this report, 'verified phishing' means that AV-TEST has performed a visual similarity comparison with phishing sites that have already been manually validated. If websites are visually similar and/or identical to the 'verified phishing' data, they will be automatically 'verified'. The downside of this approach is that new phishing URLs have to be validated manually on an ongoing basis. To address this issue, additional indicators will be introduced in future editions of this report:

- **Phishing URLs verified by Machine Learning**

  URLs and website content are classified by a self-trained machine learning model. We cannot determine the exact parameters for what constitutes phishing (as is usual with machine learning). This was based on AV-TEST's dataset of verified phishing URLs.

  This method identified 70,757 phishing URLs with ASNs in January 2026. These were included in the total of 86,266 potential phishing URLs with ASNs. Regarding the 6,081 verified phishing URLs, those verified by machine learning represent a separate category.

- **Phishing URLs verified by Visual AI**

  Additionally, AV-TEST uses local Large Language Models (LLMs) with image processing capabilities to analyse URLs, website content, and screenshots, extracting features that are typical of phishing sites. Additionally, several parameters are extracted in this process, including:

  - Is it a domain parking page
  - Is it an error code page
  - Which company is being imitated
  - Which industry sector does the company belong to

  This method identified 41,243 phishing URLs with ASNs in January 2026. These were included in the total of 86,266 potential phishing URLs with ASNs. Regarding the 6,081 verified phishing URLs, those verified by visual AI represent also a separate category.

- **Phishing URLs verified by Machine Learning & Visual AI**

  This category represents a combination of both methods to classify URLs and website content as phishing.

  In this category 32,241 phishing URLs with ASNs have been identified in January 2026. These were included in the total of 86,266 potential phishing URLs with ASNs. There is also a Regarding the 137,090 verified phishing URLs, those verified by visual AI represent also a separate category. There is an overlap with the ‘verified by Machine Learning’ and ‘verified by Visual AI’ categories.

  As soon as data from more months is available, this report will include a visualisation of the data.

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
Feb 2025	490,080		2.85%	13,972	
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%
Jan 2026	86,266	+36.73%	7.05%	6,081	-34.89%
Total	**3,162,698**		4.33%	**137,090**	

*Table 3: Aggregate Trends - **History of All (Potential) and Verified Phishing URLs** - **February 2025 to January 2026***

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	**263,558**			**11,424**	

*Table 4: Aggregate Trends - **Key Figures of All (Potential) and Verified Phishing URLs** - **February 2025 to January 2026***

Commentary

The aggregated dataset covering February 2025 to January 2026 identified a total of 3,162,698 all (potential) phishing URLs and 137,090 verified phishing URLs. Monthly volumes of all (potential) phishing URLs **exhibited pronounced volatility throughout the reporting period**. After rising through March and peaking at 542,081 URLs in April 2025, volumes declined sharply in May (-24.96%) and continued falling through June and July, before fluctuating in August and rebounding in September. October and November saw renewed declines, with December 2025 recording a **historic low of 63,090 URLs**, representing an **88% decline from the April peak**. In January 2026, potential phishing increased to 86,266 (+36.73%), marking a partial rebound from December's minimum but remaining well below mid-2025 levels.

Verified phishing followed a different trajectory. It **peaked in May 2025 at 21,492 URLs**, before declining through the summer months to a low in September 2025 (6,036 URLs). October saw a moderate recovery, followed by incremental increases in November and December. However, **January 2026 recorded 6,081 verified phishing URLs (-34.89%), the second-lowest level in the reporting period**, reversing the late-2025 stabilisation trend and approaching, though not surpassing, September's minimum.

The share of verified phishing within all (potential) phishing URLs varied substantially across the reporting period, ranging from a low of 1.72% in April 2025 to a peak of **14.80% in December 2025**, significantly above the reporting-period average of approximately 4.33%. **January 2026 saw the verification rate decline sharply to 7.05%**, interrupting the three-month upward trajectory observed in October (5.37%), November (10.98%) and December (14.80%). While December had reinforced a pronounced quality-over-quantity dynamic – combining historically low volume with an unprecedented verification share – January's rebound in potential phishing alongside a decline in verified cases suggests a re-expansion in detection volume without a corresponding rise in confirmed threat density.

Overall, the reporting period highlights both the sustained volatility of phishing activity and a late-2025 structural shift toward higher verification rates, culminating in December's peak concentration. **January 2026 marks a partial normalisation of that pattern, with increased volume but reduced verification intensity**, indicating that the quality-driven concentration observed at year-end has not carried into the new reporting cycle.

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 **10,136,360 URLs with ASNs** were identified among the Top50 ASNs in February 2026, **of which:**

- **9,583,474 URLs** could be **verified as malware**,
- **342,924 URLs** have been **classified as PUA**, and
- **209,962 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
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
Jan 2026	856,332	97.36%	11,664	1.33%	11,599	1.32%	879,595
Total	**9,583,474**		**342,924**		**209,962**		**10,136,360**

*Table 5: Aggregate Trends - **Aggregated Share of Top 50 ASNs** - **February 2025 to January 2026***

Commentary

The aggregate dataset for the Top 50 ASNs covering February 2025 to January 2026 identified a total of 10,136,360 malicious URLs. Of these, 9,583,474 (91.43%) were linked to malware, 342,924 (5.19%) to potentially unwanted applications (PUAs), and 209,962 (3.39%) to 'other' content. This twelve-month window fully reflects the late-2025 malware surge and its impact on ASN-level concentration patterns.

Malware dominance remained structurally consistent throughout the reporting period, intensifying markedly in the final quarter of 2025. December 2025 recorded an extraordinary peak of **2,833,805 malware URLs (99.14% of the monthly total)**, far exceeding November's already elevated 1,199,728 (97.51%). The December total of 2,858,272 malicious URLs represented a **132.32% month-over-month increase**, driven almost entirely by malware. **In January 2026, volumes contracted sharply** to 879,595 URLs. Malware nonetheless accounted for 97.36% of activity within the Top 50 ASNs, confirming that while the extreme December concentration moderated, it did not fundamentally reverse.

PUA activity exhibited significant volatility across the reporting period. After peaking at 104,899 URLs (16.46%) in July 2025, PUAs declined sharply in August and continued trending downward through the final quarter, reaching 12,093 (0.42%) in December and **11,664 (1.33%) in January 2026** – the lowest absolute levels recorded within the current window. 'Other' content remained comparatively suppressed throughout the year, peaking at 40,141 in February 2025 before declining to marginal levels in subsequent months.

In summary, malware remains the overwhelming driver of ASN-based malicious activity, with late-2025 dynamics materially reshaping the distribution profile within major hosting networks. Although January 2026 reflects a substantial correction in absolute volume, the **concentration of malware within the Top 50 ASNs remains structurally elevated relative to mid-year norms**. The December surge – heavily concentrated within a small subset of providers – underscores the continued importance of targeted, ASN-level mitigation efforts. Network operators should closely monitor shifts in category distribution, particularly given the demonstrated capacity for rapid, high-volume malware escalation within large autonomous systems.

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.