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

March 2026

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

This report is the third 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 reduce abuse throughout the entire Internet ecosystem.

Key highlights from the overall data in the month of February 2026 include:

- **Malicious URL volumes continued to normalise, though still above mid-2025 baselines.**
  Total malicious URLs declined further to 627,969 in February 2026, representing a 34.35% month-on-month decrease from January (920,355). This reduction was driven primarily by malware, which fell to 587,312, accounting for the bulk of the overall decline. Despite the continued contraction, malware still accounted for approximately 93% of all malicious URLs (Figure 1), confirming its persistent dominance as the primary threat vector. While volumes have moved closer to the mid-2025 range (roughly between 400,000 and 650,000), they remain elevated relative to the lower end of that period, indicating that the post-December spike normalisation is stabilising rather than fully reverting to earlier baselines.

  In contrast, PUAs increased to 23,621 (+95.20%), representing a rebound from January's low and a partial reversal of the sustained decline observed since the July 2025 peak. Similarly, 'other' malicious URLs rose to 17,036 (+25.17%), though they continue to comprise only a marginal share (around 3-4%) of total activity, indicating modest diversification following several months of malware-heavy concentration.

- **Phishing activity contracted sharply across both volume and verification, reaching the lowest levels in the reporting period.**
  All verification methods recorded substantial and proportional declines (Figure 4, Tables 3–4), with machine learning falling to 13,836 (-80.45%), visual AI to 8,202 (-80.11%), and combined methods to 3,825 (-88.14%). The consistency of these reductions suggests that the decline is not attributable to changes in detection methodology or coverage but instead reflects a genuine contraction in confirmed phishing cases. There is no evidence of divergence between detection approaches, reinforcing the interpretation that February represents a low-activity period for verified phishing threats.

- **Detection metrics declined uniformly, indicating reduced confirmed phishing activity rather than changes in detection effectiveness.**
  All verification methods recorded substantial and proportional declines (Figure 4,

Tables 3–4), with machine learning falling to 13,836 (-80.45%), visual AI to 8,202 (-80.11%), and combined methods to 3,825 (-88.14%). The consistency of these reductions suggests that the decline is not attributable to changes in detection methodology or coverage, but instead reflects a genuine contraction in confirmed phishing cases. There is no evidence of divergence between detection approaches, reinforcing the interpretation that February represents a low-activity period for verified phishing threats.

- **Malicious activity remains highly concentrated within the Top 50 ASNs, particularly for malware distribution.**
  The Top 50 ASNs accounted for 593,584 malicious URLs in February (Table 7), of which 93.66% were malware, with PUAs (3.85%) and 'other' (2.49%) comprising only minor shares. Although total volumes declined in line with broader trends, the concentration profile remains largely unchanged, with malware continuing to dominate disproportionately within major hosting networks and exceeding the 12-month average share (around 91%). Across the full reporting period, the Top 50 ASNs were responsible for over 10.19 million malicious URLs, confirming the persistent centralisation of malicious infrastructure. This concentration continues to support the case for targeted, ASN-level mitigation as an effective strategy for reducing overall malware exposure.

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 **9,498,650 malicious URLs with ASNs** were identified in the period March 2025 to February 2026, **of which:**

- **8,947,328 URLs** could be **verified as malware**,
- **334,579 URLs** have been **classified as PUA**, and
- **216,743 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 and significantly surpassing the previous peak in November 2025**. In February 2026, **malware continued to contract following the sharp correction observed in January**, moving closer to the range that characterised activity between **March and September 2025**. Furthermore, **PUAs peaked in July 2025**, before **declining sharply in August 2025** and **reaching their lowest point in January 2026.** This trend partially **reversed in February 2026**, with a notable rebound following **several months of sustained contraction**. In addition, **'other' malicious content peaked in March 2025 and reached its lowest level in May 2025**, remaining at comparatively low levels thereafter. The lowest level for malware was also recorded in May 2025, which remains the low point within the current 12-month reporting window.

In the latest month, February 2026, **overall volumes declined further from January's already reduced levels.** Malware continued to dominate the distribution, although its share decreased compared to the extreme concentration observed in December and January. PUAs and 'other' content increased modestly in relative terms but remained minor components of the overall threat landscape. While the distribution has become slightly more balanced, it remains heavily skewed towards malware, indicating that the structural dominance observed in late 2025 has moderated but not fundamentally changed.

Malicious URLs

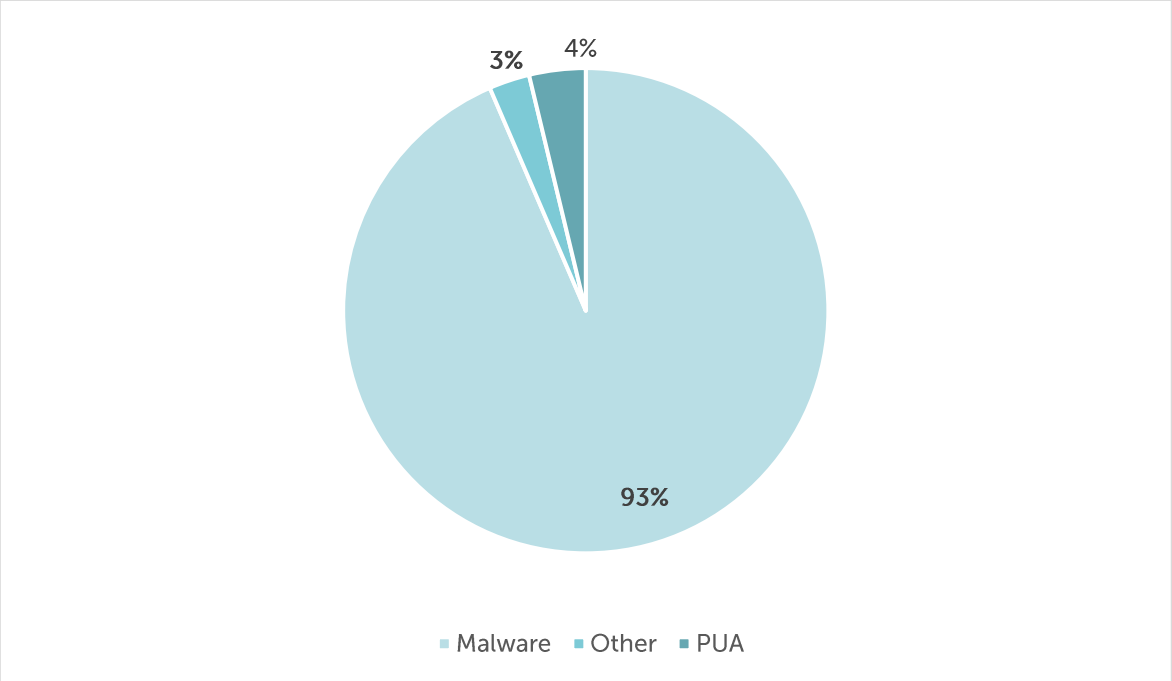

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **February 2026***

History of Malicious URLs

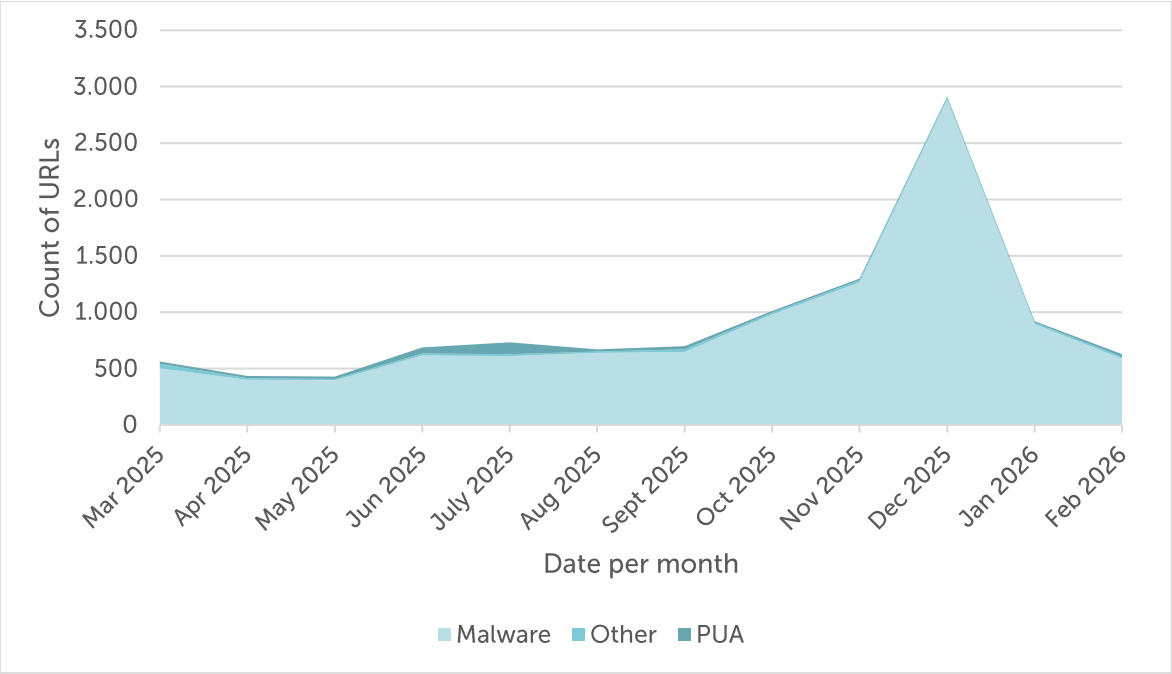

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **March 2025 to February 2026***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
Mar 2025	504,027		20,104		39,830	
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%
Feb 2026	587,312	-34.35%	23,621	+95.20%	17,036	+25.17%
Total	**8,947,328**		**334,579**		**216,743**	

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

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Change
High	2,885,933	Dec 2025	105,835	Jul 2025	39,830	Mar 2025
Low	396,207	May 2025	12,101	Jan 2026	12,011	May 2025
Average	**745,611**		**27,882**		**18,062**	

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

Commentary

The aggregate dataset covering March 2025 to February 2026 identified a total of 9,498,650 malicious URLs associated with ASNs, of which 8,947,328 were classified as malware, 334,579 as potentially unwanted applications (PUAs), and 216,743 as 'other' malicious content. Compared to the previous reporting window, **total volumes declined, reflecting the absence of a comparable large-scale spike** to that observed in December 2025. The earlier surge in malware activity, which drove totals sharply higher in late 2025, continued to unwind through January and February 2026, resulting in a more moderate aggregate profile.

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 **substantially exceeding 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 entering a sustained decline that culminated in a low point in January 2026 (12,101), **followed by a partial rebound (23,621) in February 2026**. 'Other' malicious content reached its highest level **in March 2025 at 39,830 and declined thereafter**, with its lowest point recorded in May 2025. Minimum values across categories were observed in May 2025 for malware, January 2026 for PUAs, and May 2025 for 'other' content, marking the lowest activity levels in the reporting period. On average, monthly volumes amounted to approximately **745,611 malware URLs**, **27,882 PUAs**, and **18,062 'other' malicious URLs**.

Following December's historic spike, malware contracted sharply in **January 2026** and declined further in **February 2026**, indicating a continued correction phase. Despite this reduction, malware remained the dominant category, accounting for approximately **93% of all malicious URLs** in February. This represents a notable decrease from the extreme concentration observed in December (99%) and January (approximately 97%), but still reflects a heavily skewed distribution. PUAs and 'other' content increased modestly in February following prior declines, though both categories remained comparatively small in absolute and relative terms.

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 exhibited a narrower but still pronounced range, declining from their mid-2025 peak to a low in January 2026 **before rebounding in February**. 'Other' content followed a similar pattern of early peak and subsequent stabilisation at lower levels. Overall, the data confirm malware's sustained dominance throughout the reporting period and indicate that, while the late-2025 surge has largely unwound, baseline activity remains structurally elevated relative to mid-2025 conditions.

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 2,712,107 phishing URLs with ASNs** were identified in the period from March 2025 to February 2026, **of which 124,809 URLs** could be **verified**.

There was a continued increase in potential phishing from March 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 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 historic low. In January 2026, potential phishing rebounded moderately, while **February 2026 saw a renewed and more pronounced decline**, bringing volumes to a new minimum within the reporting period. Verified phishing followed a broadly similar trajectory, declining further in February to its lowest level in the dataset.

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 February 2026**, falling below the previous low recorded in December 2025, while **verified phishing also reached its lowest point in February 2026**, following consecutive declines from late 2025 into early 2026.

Notably, the verification rate (verified phishing as a share of potential phishing) reached its **highest point in December 2025 at 14.80%**, significantly exceeding the levels observed in October and November, before declining in January. This downward trend continued in **February 2026**, with the verification rate falling further to its lowest level in the reporting period. This sustained decline indicates that the late-2025 pattern of declining volume combined with rising verification rates has fully reversed, suggesting a shift back towards broader, lower-confirmation activity rather than a continued concentration of confirmed phishing threats.

History of Phishing URLs

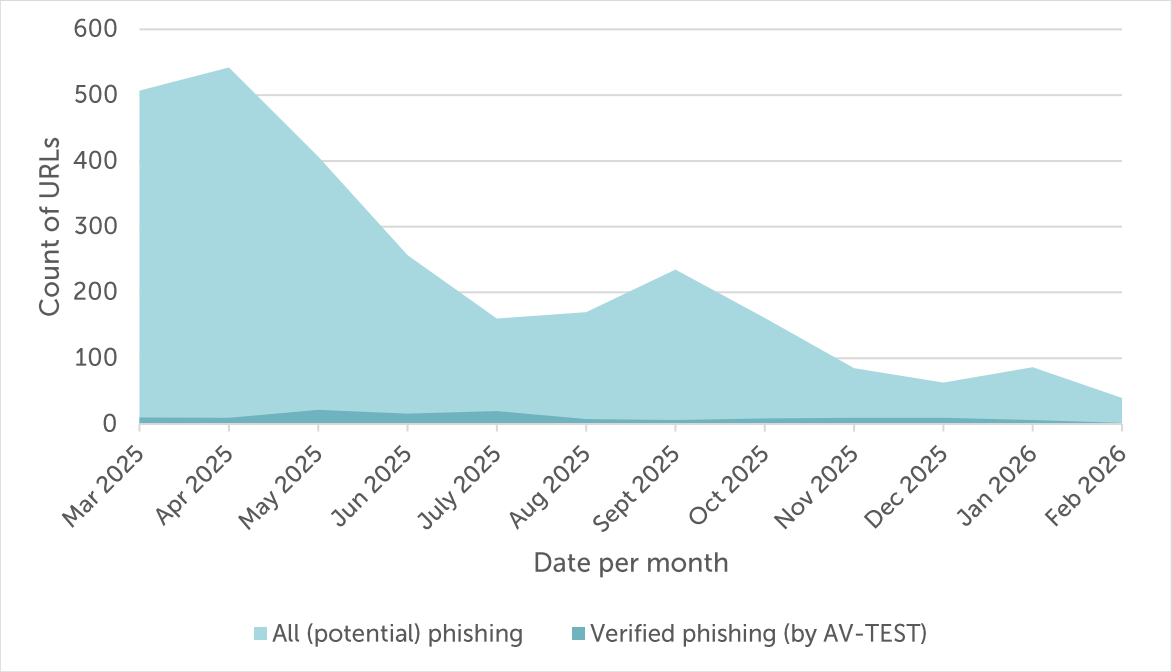

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **March 2025 to February 2026***

Over the past year, AV-TEST has further expanded its phishing analysis in order to distinguish more reliably between verified phishing URLs and the wider set of potential phishing URLs.

In this report, 'verified phishing' refers to URLs that AV-TEST has assessed using visual similarity analysis against phishing websites that have already been manually validated. Where websites are found to be visually highly similar and/or identical to the 'verified phishing' data, they may also be classified automatically as verified phishing. One limitation of this approach is that new phishing URLs must still 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**

  Under this approach, URLs and website content are classified using a self-trained machine learning model and visual AI techniques based on AV-TEST's dataset of verified phishing URLs. As is typical for machine learning, it is not possible to define a fixed set of explicit classification parameters.

  In February 2026, this approach identified 13,836 phishing URLs with ASNs via machine learning and **8,202 via visual AI**, with **3,825 URLs identified by both methods** (Figure 4, Table 3). These results are not mutually exclusive, as there is a measurable

overlap between detection methods. All identified URLs form part of the total of 39,489 potential phishing URLs with ASNs.

History of Phishing URLs verified by Machine Learning & Visual AI

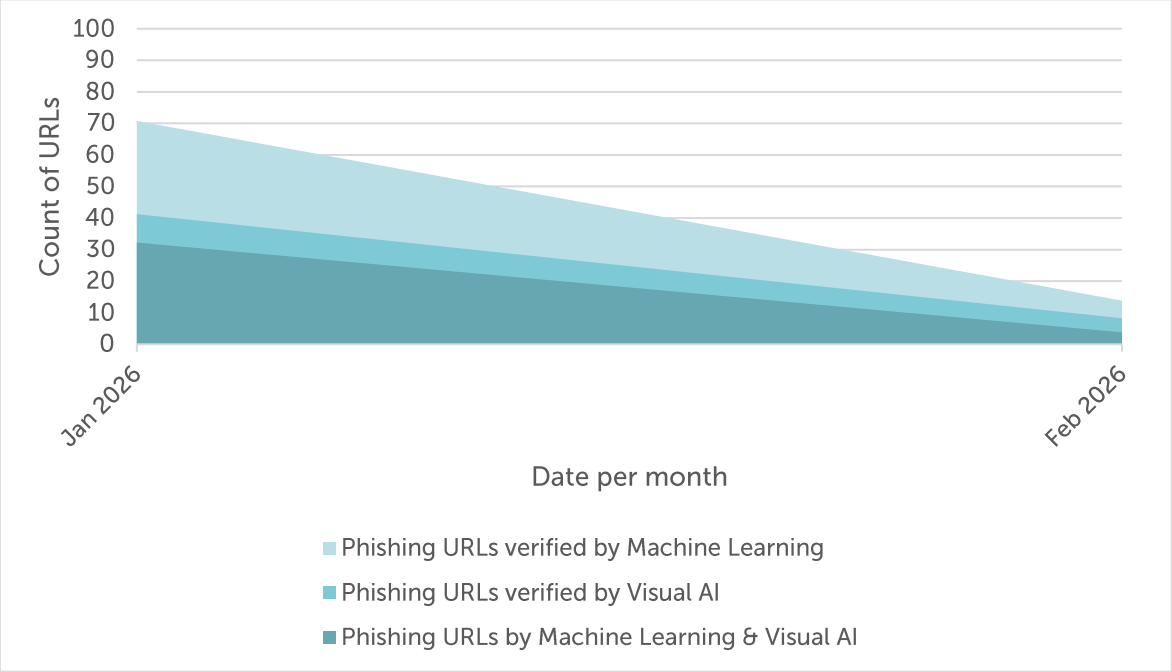

Figure 4: Aggregate Trends - ***History of Phishing URLs verified by Machine Learning & Visual AI - January 2026 to February 2026***

- **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 8,202 phishing URLs with ASNs in February 2026. These were included in the total of 39,489 potential phishing URLs with ASNs. Regarding the 1,691 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 3,825 phishing URLs with ASNs have been identified in February 2026. These were included in the total of 39,489 potential phishing URLs with ASNs. Also, regarding the 1,691 verified phishing URLs, those verified by visual AI represent a separate category. There is an overlap with the 'verified by Machine Learning' and 'verified by Visual AI' categories.

History of Phishing URLs verified by Machine Learning & Visual AI

	Verified by Machine Learning	Change	Verified by Visual AI	Change	Verified by Machine Learning & Visual AI	Change
Jan 2026	70,757		41,243		32,241	
Feb 2026	13,836	-80.45%	8,202	-80.11%	3,825	-88.14%
Total	**84,593**		**49,445**		**36,066**	

*Table 3: Aggregate Trends - **History of Phishing URLs verified by Machine Learning & Visual AI - January 2026 to February 2026***

Key Figures of Phishing URLs verified by Machine Learning & Visual AI

	Verified by Machine Learning	Change	Verified by Visual AI	Change	Verified by Machine Learning & Visual AI	Change
High	70,757	Jan 2026	41,243	Jan 2026	32,241	Jan 2026
Low	13,836	Feb 2026	8,202	Feb 2026	3,825	Feb 2026
Average	**42,297**		**24,723**		**18,033**	

*Table 4: Aggregate Trends - **Key Figures of Phishing URLs verified by Machine Learning & Visual AI - January 2026 to February 2026***

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
Mar 2025	506,671		1.96%	9,939	
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%
Feb 2026	39,489	-54.22%	4.28%	1,691	-72.19%
Total	**2,712,107**		4.60%	**124,809**	

*Table 5: Aggregate Trends - **History of All (Potential) and Verified Phishing URLs** - **March 2025 to February 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	Feb 2026		1,691	Feb 2026
Average	**226,009**			**10,401**	

*Table 6: Aggregate Trends - **Key Figures of All (Potential) and Verified Phishing URLs** - **March 2025 to February 2026***

Commentary

The aggregated dataset covering March 2025 to February 2026 identified a total of 2,712,107 all (potential) phishing URLs and 124,809 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 moderately to 86,266, marking a partial rebound from December's minimum; however, **February 2026 reversed this trend**, with volumes declining sharply again to 39,489, a new low within the reporting period, reinforcing the broader downward trajectory observed since mid-2025.

Verified phishing followed a partially divergent pattern. 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. This stabilisation did not persist into 2026: **verified phishing declined sharply in January and fell further in February 2026 to 1,691, the lowest level in the dataset**, indicating a sustained contraction in confirmed phishing activity rather than short-term fluctuation.

The share of verified phishing within all (potential) phishing URLs varied substantially across the reporting period, **reaching its highest level in December 2025 (14.80%)**, significantly above the reporting-period average of approximately 4.33%. This peak reflected a pronounced quality-over-quantity dynamic, with low overall volumes but a high concentration of confirmed threats. However, this pattern reversed in early 2026. January saw a decline in the verification rate, and **February 2026 extended this trend further, with the verification rate falling to 4.28%**, the lowest level in the reporting period. This indicates a continued shift towards higher volumes of unverified or lower-confidence detections relative to confirmed phishing cases.

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. **The subsequent decline in both volume and verification intensity in January and February 2026 suggests a transition away from that pattern.** Rather than a continuation of quality-driven concentration, current data point to a suppressed threat environment characterised by low volumes and reduced confirmation rates, with no indication of a renewed escalation in verified phishing activity.

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 **10,198,491 URLs with ASNs** were identified among the Top50 ASNs in February 2026, **of which:**

- **9,676,463 URLs** could be **verified as malware**,
- **337,428 URLs** have been **classified as PUA**, and
- **184,600 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
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
Feb 2026	555,949	93.66%	22,856	3.85%	14,779	2.49%	593,584
Total	**9,676,463**		**337,428**		**184,600**		**10,198,491**

*Table 7: Aggregate Trends - **Aggregated Share of Top 50 ASNs** - **March 2025 to February 2026***

Commentary

The aggregate dataset for the Top 50 ASNs covering March 2025 to February 2026 identified a total of 10,198,491 malicious URLs. Of these, 9,676,463 (94.88%) were linked to malware, 337,428 (3.31%) to potentially unwanted applications (PUAs), and 184,600 (1.81%) to 'other' malicious content. This twelve-month window captures both the late-2025 malware surge and the subsequent correction phase, while confirming a sustained increase in malware concentration within major hosting networks compared to earlier periods.

Malware dominance remained structurally consistent throughout the reporting period, intensifying markedly in the final quarter of 2025. December 2025 recorded a peak of **2,833,805 malware URLs (99.14% of the monthly total)**, far exceeding November's already elevated levels. **In January 2026, total volumes contracted sharply** to 879,595 malicious URLs, and declined further in **February 2026 to 593,584**, reflecting a continued correction following the December spike. Despite this reduction, malware remained dominant, accounting for **93.66% of activity in February**, confirming that while the extreme concentration observed in December has moderated, it has not fundamentally reversed.

PUA activity exhibited significant volatility across the reporting period. After peaking at 104,899 URLs (16.46%) in July 2025, PUAs declined sharply in the second half of the year, reaching 11,664 in January 2026, before rebounding to **22,856 (3.85%) in February 2026**. 'Other' malicious content followed a similar pattern, peaking earlier in the reporting period before declining to comparatively low levels, with **14,779 URLs (2.49%) recorded in February 2026**.

In summary, malware remains the dominant driver of ASN-based malicious activity, with late-2025 dynamics reinforcing its concentration within a relatively small number of large hosting networks. Although the post-December correction has reduced absolute volumes, the **structural skew towards malware persists.** The December surge – heavily concentrated within a small subset of providers – continues to underscore the importance of targeted, ASN-level mitigation strategies, particularly given the demonstrated capacity for rapid, large-scale malware expansion within major 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.