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

May 2026

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

This report is the fifth 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 April 2026 include:

- **Malicious URL volumes increased again in April, driven by renewed mal-ware growth, while remaining well below late-2025 peak levels.** Total **malicious URLs increased to 990,988**, representing a +21.27% month-on-month rise from March (817,161). This increase was driven pre-dominantly by malware, which rose to 954,994 (+23.33%) and accounted for approximately 96% of total malicious activity. Despite the increase, overall volumes remained substantially below the December 2025 peak (2,885,933), indicating a sustained elevated baseline rather than a return to peak conditions.

  PUAs declined to 12,452 (-26.38%), bringing volumes close to the January 2026 low (12,101) and reinforcing the broader downward trend following February's temporary rebound. **'Other' malicious URLs also decreased to 23,542 (-9.03%)** after the March high (25,879), but remained above most monthly levels in the reporting window. Overall, the distribution shifted further towards malware dominance, with PUAs and 'other' categories together accounting for less than 4% of total activity.

- **Phishing activity weakened again after March's short rebound and remains structurally subdued relative to earlier in the reporting period.** All (potential) phishing URLs decreased to **57,703 (-5.47%)**, reversing part of March's rebound and remaining far below the May 2025 high (**406,756**) and the reporting-period average (**148,508**). Verified phishing also declined to **2,615 (-34.33%)**, the second-lowest value in the current window after February **2026 (1,691)**.

- **Detection metrics declined across all verification methods, indicating that the March recovery did not extend into April.** Machine learning detections fell to **17,720 (-7.72%)**, visual AI detections declined to **24,277 (-22.28%)**, and combined-method detections de-creased to **13,060 (-8.70%)**. The decreases were moderate compared with the sharp February contraction, but the consistency across methods points to a renewed weakening in observable phishing activity rather than a method-specific artefact. All detection volumes remained substantially below January 2026 levels.

- **Malicious activity remained highly concentrated within the Top 50 ASNs, with malware continuing to dominate.**
  The Top 50 ASNs accounted for **945,285** malicious URLs in April, of which **913,564 (96.64%)** were malware. PUAs and 'other' categories comprised only **1.23%** and **2.12%** respectively. The increase from March (778,453) was driven primarily by malware, confirming that the post-February recovery remains concentrated within a small number of large hosting networks.

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 **11,800,556 malicious URLs with ASNs** were identified in the period May 2025 to April 2026, **of which:**

- **11,251,619 URLs** could be **verified as malware**,
- **337,203 URLs** have been **classified as PUA**, and
- **211,734 URLs** as **other**.

The highest level of malware activity was recorded in **December 2025 (2,885,933 URLs)**, representing the peak of the late-2025 surge and significantly exceeding all other months in the current reporting window. Following this spike, volumes declined sharply in January and February 2026, before rising in March and again in April 2026 to **954,994 (+23.33%)**. This confirms a recovery from the February low, but not a return to peak conditions. Furthermore, **PUA activity remained volatile**. It peaked in **July 2025 (105,835 URLs)**, declined sharply in the second half of the year, reached its low in **January 2026 (12,101)**, rebounded briefly in February and then declined again to **12,452 (-26.38%)** in April, close to the period low. In addition, **'Other' malicious content** reached its high in **March 2026 (25,879)**, before decreasing to **23,542 (-9.03%)** in April, still remaining above most months in the reporting window. Across the full period, monthly averages amounted to approximately **937,635 malware URLs, 28,100 PUAs**, and **17,645 'other' malicious URLs**, highlighting the persistent imbalance between categories.

Overall, the data indicate that the extreme late-2025 spike has largely unwound, while malware continues to dominate the threat landscape structurally. The April increase extends the post-February recovery, but current levels remain far below the December peak. This points to stabilisation at an elevated baseline relative to early and mid-2025, with limited and inconsistent diversification into PUA and 'other' categories.

Malicious URLs

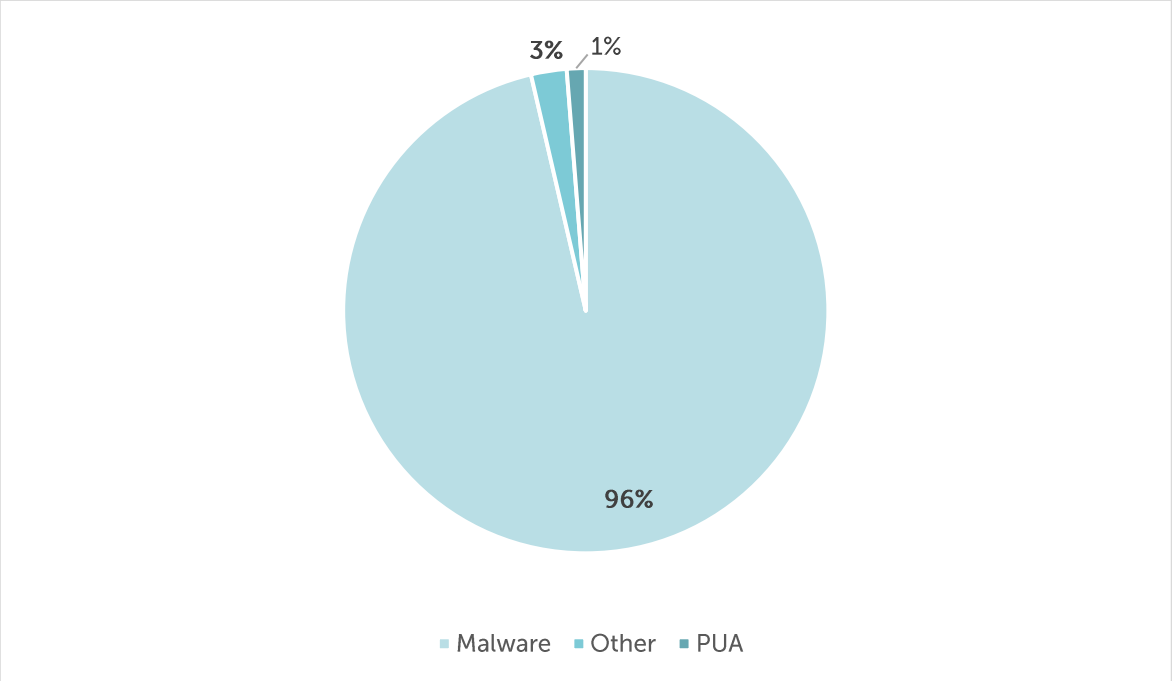

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **April 2026***

History of Malicious URLs

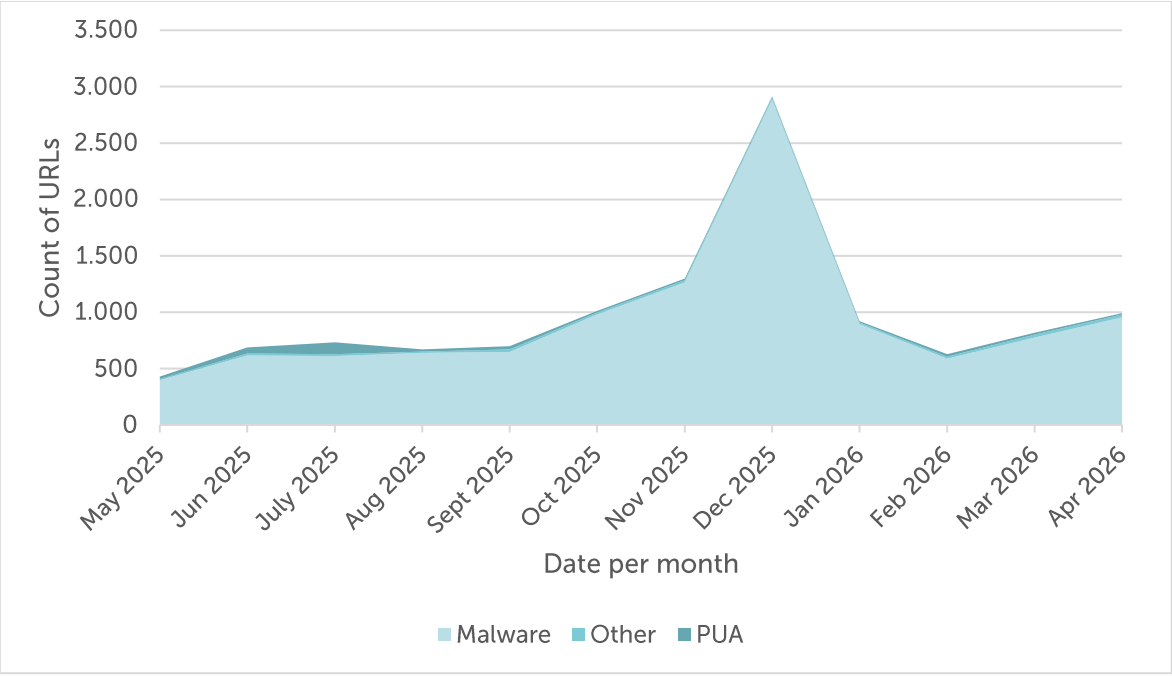

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **May 2025 to April 2026***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
May 2025	396,207		21,305		12,011	
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%
Mar 2026	774,368	+31.85%	16,914	-28.39%	25,879	+51.91%
Apr 2026	954,994	+23.33%	12,452	-26.38%	23,542	-9.03%
Total	**11,251,619**		**337,203**		**211,734**	

*Table 1: Aggregate Malware Trends - **History of Malicious URLs** - **May 2025 to April 2026***

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Change
High	2,885,933	Dec 2025	105,835	Jul 2025	25,879	Mar 2026
Low	396,207	May 2025	12,101	Jan 2026	12,011	May 2025
Average	**937,635**		**28,100**		**17,645**	

*Table 2: Aggregate Trends - **Key Figures of Malicious URLs** - **May 2025 to April 2026***

Commentary

The aggregate dataset covering May 2025 to April 2026 identified a total of **11,800,556 malicious URLs** associated with ASNs, of which **11,251,619 URLs were classified as malware**, **337,203 URLs as PUA**, and **211,734 URLs as other malicious content**. Compared with the previous reporting window, total volumes increased slightly due to the inclusion of April 2026, with the latest month extending the post-February recovery in malware activity.

Malware activity continued to define the overall trend. **December 2025 remained the peak (2,885,933 URLs)**, followed by sharp declines in January (-69.00%) and February (-34.35%). Activity then increased in March (+31.85%) and April (+23.33%), reaching **954,994** in April. This two-month recovery indicates renewed activity after the correction phase, but volumes remain around two thirds below the December peak.

PUA activity followed a more volatile but generally downward trajectory. After peaking in **July 2025 (105,835 URLs)**, volumes declined sharply through the second half of 2025. Following a temporary rebound in February 2026 (23,621), PUAs declined in March and again in April to **12,452 (-26.38%)**, just above the January 2026 low of 12,101.

'Other' malicious content remained comparatively low through most of the reporting period but increased materially in early 2026. After reaching the reporting-period high in **March 2026 (25,879)**, the category declined to **23,542 (-9.03%)** in April. This suggests continued short-term variability without a structural shift away from malware dominance.

As reflected in Table 2, malware activity ranged from a low of **396,207 URLs (May 2025)** to a peak of **2,885,933 (December 2025)**, representing more than a sevenfold increase across the reporting period. PUAs ranged from 12,101 to 105,835, while 'other' content ranged from 12,011 to 25,879. The April data kept these ranges unchanged while reinforcing the contrast between high malware volumes and much smaller secondary categories.

Overall, the data confirm the continued structural dominance of malware within the malicious URL landscape. The April increase suggests that activity has stabilised above the February low, but the absence of comparable growth in PUA and 'other' categories indicates that the recovery remains concentrated in malware rather than a broader diversification of malicious content.

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 1,782,101 (potential) phishing URLs** and **112,170 verified phishing URLs** were identified in the period from May 2025 to April 2026.

The data show pronounced volatility in overall volumes, alongside sustained weakness in verified activity through early 2026.

All (potential) phishing activity peaked in **May 2025 (406,756 URLs)** and declined sharply through June and July before fluctuating in the second half of 2025. After reaching a low point in **February 2026 (39,489)**, volumes rebounded in March to 61,043, before decreasing again in April to **57,703 (-5.47%)**. This leaves April as the second-lowest month in the reporting window and confirms that the March rebound was limited.

Verified phishing followed a more compressed trajectory. After peaking in **May 2025 (21,492 URLs)**, volumes declined through mid-2025, stabilised briefly in late 2025, and then fell sharply in early 2026 to a minimum of **1,691 in February**. March saw a temporary recovery to 3,982, but April declined again to **2,615 (-34.33%)**, remaining close to the reporting period low.

The verification rate, meaning verified phishing as a share of potential phishing, varied significantly over time, peaking in **December 2025 (14.80%)** before declining steadily into early 2026. After a brief increase to 6.52% in March, the rate fell again to **4.53%** in April. This places the April rate below the reporting-period average of **6.29%** and indicates that the late-2025 shift towards a higher confirmed share has not resumed.

Additional detection metrics further support these trends. In April 2026, **17,720 URLs** were identified via machine learning, **24,277 via visual AI**, and **13,060 through combined methods**. Each method declined compared with March, indicating that the April weakening was visible across detection approaches rather than confined to one method.

Overall, the data indicate that phishing activity remained structurally subdued in April 2026. The March rebound did not develop into sustained escalation, and both potential and verified phishing volumes stayed near the lower end of the reporting-period range.

History of Phishing URLs

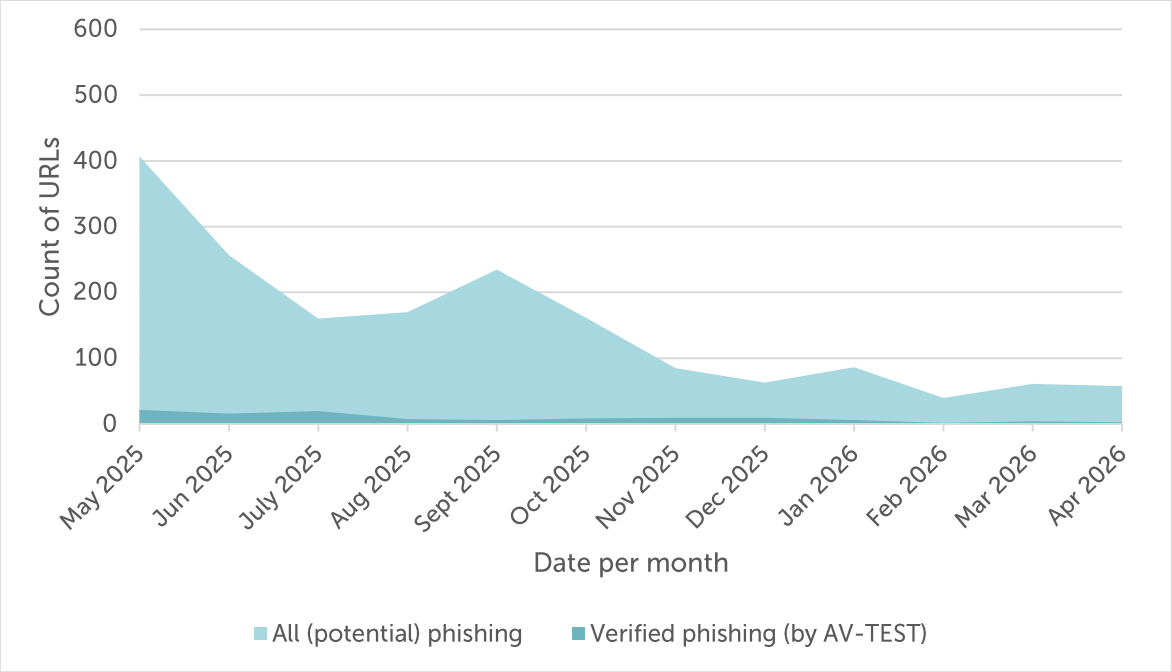

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **May 2025 to April 2026***

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 April 2026, this approach identified 17,720 phishing URLs with ASNs via machine learning, 24,277 via visual AI, and 13,060 URLs via 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 **57,703 potential phishing URLs with ASNs**.

History of Phishing URLs verified by Machine Learning & Visual AI

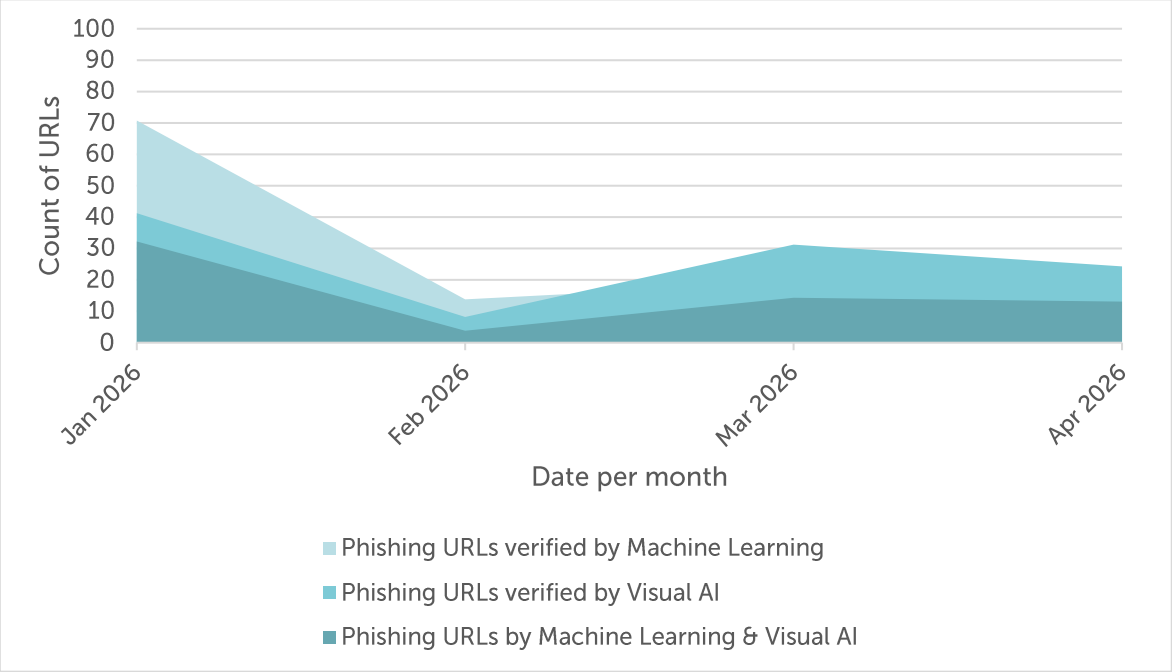

*Figure 4: Aggregate Trends - **History of Phishing URLs verified by Machine Learning & Visual AI - January 2026 to April 2026***

- **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 24,277 phishing URLs with ASNs in April 2026. These were included in the total of **57,703 potential phishing URLs with ASNs**. Regarding the **2,615 verified phishing URLs**, those verified by visual AI represent 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, 13,060 phishing URLs with ASNs were identified in April 2026. These were included in the total of **57,703 potential phishing URLs with ASNs**. Regarding the **2,615 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%
Mar 2026	19,202	+38.78%	31,234	+280.81%	14,304	+273.96%
Apr 2026	17,720	-7.72%	24,277	-22.28%	13,060	-8.70%
Total	**121,515**		**104,956**		**63,430**	

*Table 3: Aggregate Trends - **History of Phishing URLs verified by Machine Learning & Visual AI** - **January 2026 to April 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	**30,379**		**26,239**		**15,858**	

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

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
May 2025	406,756		5.28%	21,492	
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%
Mar 2026	61,043	+54.58%	6.52%	3,982	+135.48%
Apr 2026	57,703	-5.47%	4.53%	2,615	-34.33%
Total	**1,782,101**		6.29%	**112,170**	

*Table 5: Aggregate Trends - **History of All (Potential) and Verified Phishing URLs** - **May 2025 to April 2026***

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month		Verified phishing	Month
High	406,756	May 2025		21,492	May 2025
Low	39,489	Feb 2026		1,691	Feb 2026
Average	**148,508**			**9,348**	

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

Commentary

The aggregated dataset covering **May 2025 to April 2026** identified a total of **1,782,101 (potential) phishing URLs** and **112,170 verified phishing URLs** associated with ASNs. Compared with the previous reporting window, overall volumes declined markedly, reflecting the rotation out of the April 2025 potential-phishing peak and the continued suppression of phishing activity in early 2026.

All (potential) phishing activity reached its highest point in **May 2025 (406,756 URLs)** within the current reporting window before declining sharply in June and July. This downward trend continued with intermittent fluctuations, culminating in a low point in **February 2026 (39,489)**. After a short rebound in March, volumes decreased again to **57,703 (-5.47%)** in April, leaving the month well below the reporting-period average of **148,508**.

Verified phishing followed a broadly similar but more compressed trajectory. After peaking in **May 2025 (21,492 URLs)**, confirmed cases declined through mid-2025 and stabilised briefly towards the end of the year. This stability did not persist into 2026, with verified phishing falling to **1,691 in February**. April 2026 recorded **2,615 verified phishing URLs (-34.33% compared with March)**, making it the second-lowest month in the current window.

The share of verified phishing within total (potential) phishing URLs exhibited considerable variation over time. It peaked in **December 2025 (14.80%)**, reflecting a period characterised by lower overall volumes but a higher concentration of confirmed threats. This pattern reversed in early 2026, with the verification rate declining to 4.28% in February, recovering to 6.52% in March and then falling again to **4.53% in April**. The April rate remains below late-2025 levels and below the period average, indicating that the structural shift towards higher confirmation intensity has not resumed.

Detection metrics provide further context for these trends. After the broad-based rebound in March, all detection methods decreased in April: machine learning to **17,720 (-7.72%)**, visual AI to **24,277 (-22.28%)**, and combined methods to **13,060 (-8.70%)**. The consistency of these decreases across methodologies suggests that the April decline reflects a reduction in observable phishing activity rather than a method-specific effect.

Overall, the data highlight a continued structural suppression of phishing activity relative to mid-2025. The March rebound was not sustained in April, and both potential and verified phishing remained near the lower end of the reporting range. The current pattern therefore suggests stabilisation at low activity levels, rather than renewed escalation in phishing threats.

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 **11,074,341 URLs with ASNs** were identified among the Top50 ASNs in April 2026, **of which:**

- **10,564,549 URLs** could be **verified as malware**,
- **335,334 URLs** have been **classified as PUA**, and
- **174,458 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
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	94.79%	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
Mar 2026	739,897	95.05%	22,648	2.91%	15,908	2.04%	778,453
Apr 2026	913,564	96.64%	11,652	1.23%	20,069	2.12%	945,285
Total	**10,564,549**		**335,334**		**174,458**		**11,074,341**

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

Commentary

The aggregate dataset for the Top 50 ASNs covering May 2025 to April 2026 identified a total of **11,074,341 malicious URLs**. Of these, **10,564,549 URLs (95.39%) were linked to malware**, **335,334 URLs (3.03%) to PUA**, and **174,458 URLs (1.58%) to other malicious content**. This confirms a persistent and pronounced concentration of malicious activity within a relatively small number of large hosting networks.

Malware dominance remained structurally consistent throughout the reporting period, intensifying markedly in late 2025. **December 2025 recorded the peak at 2,833,805 malware URLs (99.14% share)**, far exceeding prior months. Following this surge, total volumes declined sharply in January and February 2026, before increasing in March and again in April to **945,285 total URLs**. This indicates a sustained recovery from the February low, though still well below the December peak. Malware accounted for **913,564 URLs in April, or 96.64% of Top 50 ASN activity**, one of the highest levels observed outside the late-2025 surge.

PUA activity exhibited significant variability. After reaching a high in **July 2025 (104,899; 16.46%)**, volumes declined substantially through the second half of the year, reaching 11,664 in January 2026. After a temporary increase in February and March, PUA activity declined to **11,652 (1.23%)** in April, the lowest value in the current Top 50 ASN window and a marginal share of overall activity.

'Other' malicious content followed a similar pattern of early higher values followed by sustained lower levels. In April 2026, this category increased to **20,069 URLs (2.12%)**, up from 15,908 in March. While this represents a month-on-month rise, its share remains limited and does not materially alter the malware-dominated profile of the Top 50 ASNs.

Overall, the data underscore the continued centralisation of malicious infrastructure within major autonomous systems, with malware as the primary driver. Although absolute volumes remain far below the late-2025 spike, April confirms a renewed increase after the February low. These dynamics continue to support targeted, ASN-level mitigation strategies as an effective approach to reducing large-scale malware distribution.

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.