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

June 2026

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

This report is the sixth 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 May 2026 include:

- **Malicious URL volumes declined following April's recovery, though malware continues to dominate the threat landscape.**
  Total malicious URLs fell to **798,874** in May 2026, representing a **19.39% month-on-month decrease** from April (990,988). This decline was driven primarily by malware, which fell to **763,500 (-20.05%)** and continued to account for approximately **96% of all malicious URLs**. Despite the reduction, malware volumes remain substantially above the levels observed during the first half of 2025, indicating that activity has stabilised at an elevated baseline following the late-2025 surge.

  Potentially unwanted applications (PUAs) declined further to **8,057 (-35.30%)**, establishing **a new low for the reporting period** and continuing the longer-term contraction observed since mid-2025. In contrast, 'other' malicious URLs increased to **27,317 (+16.04%)**, exceeding the previous peak recorded in March 2026 and becoming **the highest value in the current reporting window**. Nevertheless, this category continues to represent only a small proportion of overall malicious activity.

- **Potential phishing activity increased, while verified phishing continued to decline.**
  All (potential) phishing URLs rose to **73,130 (+26.74%)** in May 2026, extending the recovery that began after the February low. However, volumes remain significantly below both the reporting-period average (**120,706**) and the June 2025 peak (**256,529**), indicating that the broader structural decline in phishing activity remains intact.

  Verified phishing fell further to **1,990 (-23.90%)**, remaining only slightly above the reporting-period minimum recorded in February 2026 (**1,691**). The verification rate consequently declined to **2.72%**, representing **the lowest value observed during the reporting period**.

- **Detection metrics increased substantially across all verification methods.**
  Machine learning detections increased to **40,746 (+129.94%)**, visual AI detections rose to **32,269 (+32.92%)**, and detections identified by both methods increased to **30,561 (+134.00%)**. The consistency of these increases across methodologies suggests **a broad rise in detectable phishing-related activity**. However, the continued

decline in verified phishing indicates that this increase has not translated into a corresponding rise in confirmed phishing cases.

- **Malicious activity remains highly concentrated within the Top 50 ASNs.** The Top 50 ASNs accounted for **752,518 malicious URLs** in May 2026, comprising **721,866 malware URLs (95.93%)**, **7,740 PUAs (1.03%)**, and **22,912 URLs classified as 'other' malicious content (3.04%)**. Although overall volumes declined compared with April, **the concentration profile remains largely unchanged**, with malware continuing to account for **the overwhelming majority of activity hosted within major autonomous systems**. These findings continue to support targeted ASN-level mitigation as an effective mechanism for reducing large-scale 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 **12,169,907 malicious URLs with ASNs** were identified in the period June 2025 to May 2026, **of which:**

- **11,618,912 URLs** could be **verified as malware**,
- **323,955 URLs** have been **classified as PUA**, and
- **227,040 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 prior months. Following this spike, volumes declined sharply in January and February 2026, recovered partially in March and April, and then fell again to **763,500 URLs in May 2026 (-20.05%)**. While this represents a moderation of activity, malware volumes remain elevated relative to much of the first half of the reporting period.

Furthermore, PUA activity exhibited substantial volatility over the reporting period. It peaked in **July 2025 (105,835 URLs)** before declining sharply through the second half of the year. In **May 2026**, PUA volumes fell to **8,057 URLs**, establishing **a new low for the reporting period** and confirming the continuation of the longer-term downward trend.

In contrast, 'other' malicious content followed a different trajectory. In **May 2026**, this category increased to **27,317 URLs (+16.04%)**, establishing **a new reporting-period high** and exceeding the previous peak recorded in March 2026. Despite this increase, it continues to represent only a small proportion of total malicious activity. Across the full period, monthly averages amounted to approximately **968,243 malware URLs**, **26,996 PUAs**, and **18,920 'other' malicious URLs**, highlighting the persistent imbalance between categories.

Overall, the data indicate that while the extreme spike observed in late 2025 has largely unwound, **malware continues to dominate the threat landscape structurally**. Activity levels have moderated since the late-2025 peak but remain elevated relative to much of 2025. The distribution across categories remains heavily skewed towards malware, with only limited diversification into PUA and 'other' classifications.

Malicious URLs

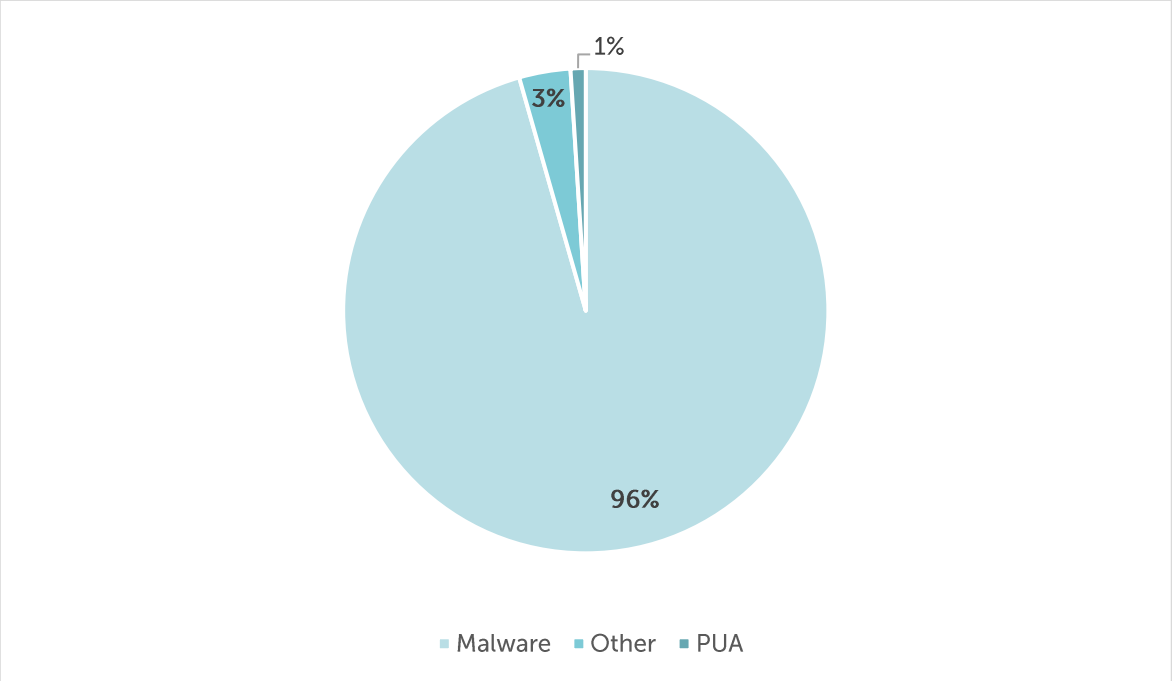

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **May 2026***

History of Malicious URLs

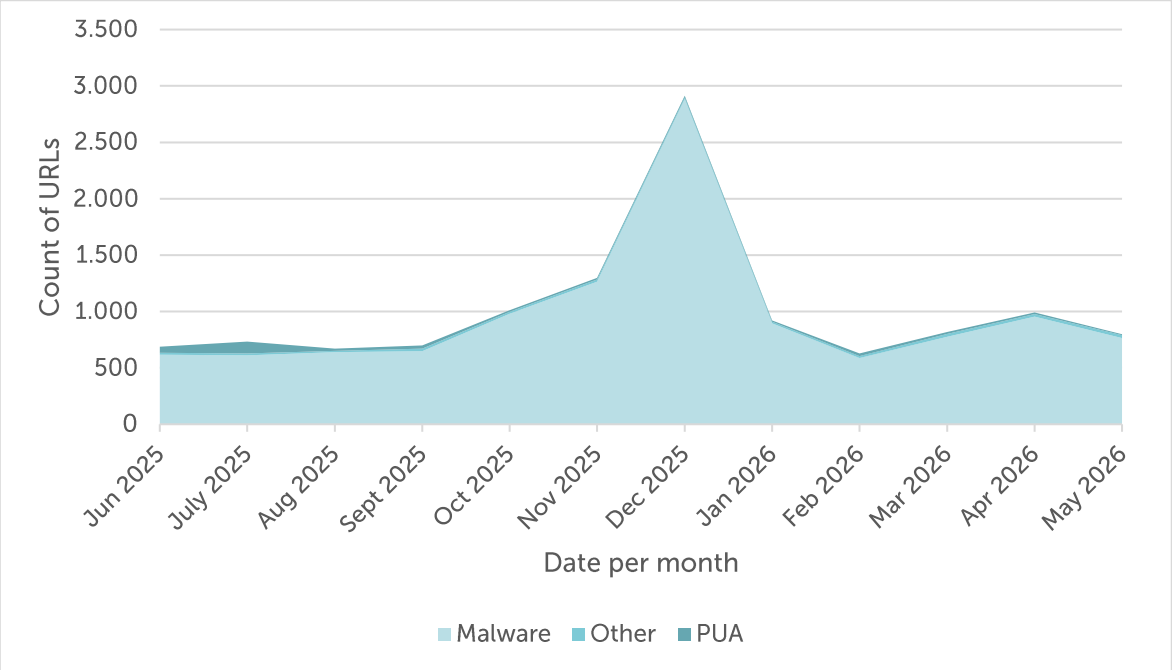

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **June 2025 to May 2026***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
Jun 2025	615,448		54,207		18,942	
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%
May 2026	763,500	-20.05%	8,057	-35.30%	27,317	+16.04%
Total	**11,618,912**		**323,955**		**227,040**	

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

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Change
High	2,885,933	Dec 2025	105,835	Jul 2025	27,317	May 2026
Low	587,312	Feb 2026	8,057	May 2026	13,272	Aug 2025
Average	**968,243**		**26,996**		**18,920**	

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

Commentary

The aggregate dataset covering June 2025 to May 2026 identified a total of **12,169,907 malicious URLs** associated with ASNs, of which **11,618,912 URLs** were classified as malware, **323,955 URLs** were classified as PUA, and **227,040 URLs** as other malicious content. Compared with the previous reporting window, overall malicious URL volumes moderated following the recovery observed during March and April 2026.

The highest level of malware activity was recorded in **December 2025 (2,885,933 URLs)**, representing **the peak within the reporting window** and substantially exceeding all other months. Following the sharp correction in January and February 2026 and the partial recovery observed in March and April, malware declined again in May 2026 to **763,500 (-20.05%)**. While this represents a significant reduction compared with April, volumes remain above those observed throughout much of the first half of the reporting period.

PUA activity continued its longer-term contraction. After reaching a peak of **105,835 URLs in July 2025**, volumes declined substantially through the remainder of the reporting period, reaching **a new low of 8,057 URLs in May 2026**. This confirms that the temporary rebound observed in February 2026 did not develop into a sustained recovery.

'Other' malicious content followed a different trajectory. Unlike malware and PUAs, this category increased to **27,317 URLs in May 2026 (+16.04%)**, establishing **a new reporting-period high** and exceeding the previous peak recorded in March 2026. Despite this increase, the category remains comparatively small and does not materially alter the overall composition of malicious activity.

As reflected in Table 2, malware activity ranged from **587,312 URLs (February 2026)** to **2,885,933 URLs (December 2025)**. PUA activity ranged from **8,057 URLs (May 2026)** to **105,835 URLs (July 2025)**, while 'other' malicious content ranged from **13,272 URLs (August 2025)** to **27,317 URLs (May 2026)**.

Overall, the data confirms **the continued structural dominance of malware within the malicious URL landscape**. While activity has moderated considerably since the late-2025 peak, current levels remain elevated relative to much of 2025. Diversification into PUA and 'other' categories remains limited, despite the recent increase observed in the latter.

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 1,448,475 (potential) phishing URLs** and **92,668 verified phishing URLs** were identified in the period from **June 2025 to May 2026**. The data show pronounced volatility in overall volumes, alongside a sustained decline in verified phishing activity throughout late 2025 and 2026.

All (potential) phishing activity peaked in **June 2025 (256,529 URLs)** before declining sharply through July and fluctuating during the second half of the year. Following a prolonged downward trend, activity reached **a reporting-period low of 39,489 URLs in February 2026**. Volumes subsequently recovered to 61,043 in March and 57,703 in April before increasing further to **73,130 URLs in May 2026 (+26.74%)**. Despite this recovery, activity remains substantially below both the reporting-period average and the levels observed during the first half of the reporting period.

Verified phishing followed a partially similar but more compressed trajectory. After peaking in **July 2025 (19,656 URLs)**, volumes declined substantially through the remainder of the reporting period. Following a temporary stabilisation in late 2025, verified phishing fell sharply during early 2026, reaching **a minimum of 1,691 URLs in February 2026**. In **May 2026**, verified phishing declined further to **1,990 URLs (-23.90%)**, remaining only marginally above the reporting-period low and indicating continued weakness in confirmed phishing activity.

The verification rate, meaning verified phishing as a share of potential phishing, varied significantly over time, peaking at **14.80% in December 2025** before declining throughout 2026. After recovering temporarily to 6.52% in March, the verification rate fell to **4.53% in April** and **2.72% in May 2026**, representing **the lowest level observed during the reporting period**. This suggests that recent increases in potential phishing activity have been concentrated primarily among lower-confidence detections rather than confirmed phishing cases.

Additional detection metrics further support these trends. In **May 2026**, **40,746 URLs** were identified via machine learning, **32,269** via visual AI, and **30,561** through combined methods. While these results are not mutually exclusive, all three detection categories recorded substantial month-on-month increases, indicating a broad-based rise in detectable phishing-

related activity. However, the continued decline in verified phishing demonstrates that this increase has not translated into a corresponding rise in confirmed phishing threats.

Overall, the data indicate that while potential phishing activity has recovered from the February 2026 low, **phishing activity remains structurally lower than earlier in the reporting period**. The increase observed in recent months is therefore best interpreted as a partial recovery in overall detection activity rather than evidence of a renewed escalation in confirmed phishing threats.

History of Phishing URLs

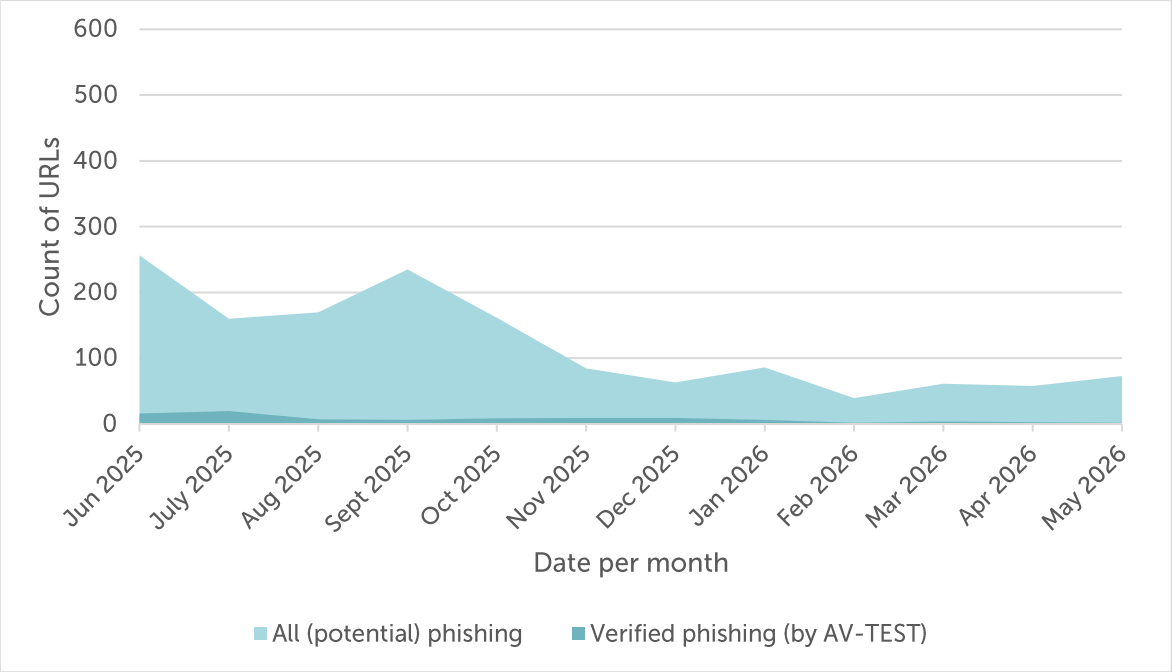

*Figure 3: Aggregate Trends - **History of Phishing URLs - June 2025 to May 2026***

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 **May 2026**, this approach identified **40,746 phishing URLs with ASNs via machine learning**, **32,269 via visual AI**, with **30,561 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 **73,130 potential phishing URLs with ASNs**.

History of Phishing URLs verified by Machine Learning & Visual AI

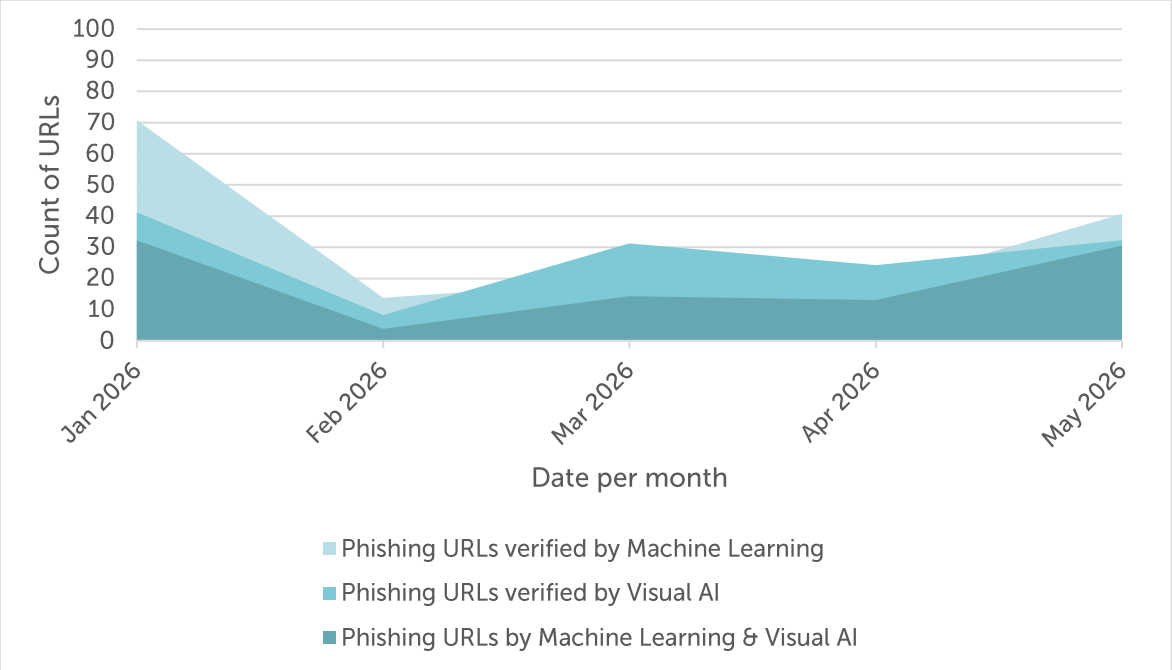

*Figure 4: Aggregate Trends - **History of Phishing URLs verified by Machine Learning & Visual AI - January 2026 to May 2026***

- **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 **32,269 phishing URLs with ASNs in May 2026**. These were included in the total of **73,130 potential phishing URLs with ASNs**. Regarding the **1,990 verified phishing URLs**, those verified by visual AI also 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, **30,561 phishing URLs with ASNs were identified in May 2026**. These were included in the total of **73,130 potential phishing URLs with ASNs**. Regarding the **1,990 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	-22.27%	13,060	-8.70%
May 2026	40,746	+129.94%	32,269	+32.92%	30,561	+134.00%
Total	**162,261**		**137,225**		**93,991**	

*Table 3: Aggregate Trends - **History of Phishing URLs verified by Machine Learning & Visual AI** - **January 2026 to May 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	**32,452**		**27,445**		**18,798**	

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

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
Jun 2025	256,529		6.20%	15,907	
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%
May 2026	73,130	+26.74%	2.72%	1,990	-23.90%
Total	**1,448,475**		6.40%	**92,668**	

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

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month		Verified phishing	Month
High	256,529	Jun 2025		19,656	Jul 2025
Low	39,489	Feb 2026		1,691	Feb 2026
Average	**120,706**			**7,722**	

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

Commentary

The aggregated dataset covering **June 2025 to May 2026** identified a total of **1,448,475 (potential) phishing URLs** and **92,668 verified phishing URLs** associated with ASNs. Overall phishing activity remains substantially below the levels observed during the first half of the reporting period, despite the increase recorded in May 2026.

All (potential) phishing activity peaked in **June 2025 at 256,529 URLs** before declining sharply during the following months. After reaching a **reporting-period low of 39,489 URLs in February 2026**, volumes recovered gradually to 57,703 in April and increased further to **73,130 in May 2026 (+26.74%)**. Despite this recovery, activity remains well below both the reporting-period average and the levels observed throughout most of 2025.

Verified phishing followed a more persistent downward trajectory. After peaking in **July 2025 at 19,656 URLs**, confirmed phishing activity declined substantially over the reporting period. Following a temporary stabilisation in late 2025, verified phishing fell sharply in early 2026, reaching **a minimum of 1,691 URLs in February 2026**. May 2026 recorded a further decline to **1,990 (-23.90%)**, indicating that the modest recovery observed in potential phishing volumes has not been accompanied by an increase in confirmed phishing activity.

The share of verified phishing within total (potential) phishing URLs continued to weaken throughout 2026. After reaching **a peak of 14.80% in December 2025**, the verification rate declined to **7.05% in January**, **4.28% in February**, **6.52% in March**, **4.53% in April**, and **2.72% in May**. This represents **the lowest verification rate within the reporting period** and suggests that the increase in potential phishing activity has been concentrated primarily among lower-confidence detections.

Detection metrics provide additional context. In May 2026, machine learning detections increased to **40,746 (+129.94%)**, visual AI detections rose to **32,269 (+32.92%)**, and URLs identified by both methods increased to **30,561 (+134.00%)**. The consistency of these increases across methodologies indicates **a significant rise in detectable phishing-related activity**. However, the continued decline in verified phishing demonstrates that this increase has not translated into a corresponding rise in confirmed phishing threats.

Overall, the data suggest that phishing activity remains **structurally subdued relative to earlier phases of the reporting period**. While potential phishing volumes have recovered from the February low, verification rates continue to decline, indicating that the current environment is characterised by increased detection activity but relatively low levels of confirmed phishing.

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 11,460,687 URLs** with ASNs were identified among the Top 50 ASNs during the period June 2025 to May 2026, of which:

- **10,949,219 URLs** could be **verified as malware**,
- **323,865 URLs** have been **classified as PUA**, and
- **187,603 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
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
May 2026	721,866	95.93%	7,740	1.03%	22,912	3.04%	752,518
Total	**10,949,219**		**323,865**		**187,603**		**11,460,687**

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

Commentary

The aggregate dataset for the Top 50 ASNs covering **June 2025 to May 2026** identified a total of **11,460,687 malicious URLs**. Of these, **10,949,219 URLs (95.54%)** were linked to malware, **323,865 URLs (2.83%)** to PUA, and **187,603 URLs (1.64%)** 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, recovered partially in March and April, and then declined again in May 2026 to **752,518 total URLs**. Despite these fluctuations, malware continued to account for the overwhelming majority of activity, representing **95.93% of all malicious URLs in May 2026**.

PUA activity exhibited significant variability. After reaching a high in **July 2025 (104,899 URLs; 16.46%)**, volumes declined substantially through the second half of the year and continued falling throughout 2026, reaching **7,740 URLs (1.03%) in May 2026**, the lowest level observed during the reporting period. This confirms the longer-term contraction in PUA-related activity within major autonomous systems.

'Other' malicious content followed a different trajectory. While remaining comparatively small throughout the reporting period, this category increased to **22,912 URLs (3.04%) in May 2026**, representing one of the highest levels observed during the reporting window. Despite this increase, its contribution to overall malicious activity remains limited compared with malware.

Overall, the data underscores the continued centralisation of malicious infrastructure within major autonomous systems, with **malware remaining the primary driver of abuse**. Although absolute volumes have moderated since the late-2025 peak, **the structural concentration remains largely unchanged**. 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.