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

July 2026

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Contents 2

Report Summary 3

Methodology 5

Chart: Aggregate Malware Trends 7

Chart: Aggregate Phishing Trends 11

Chart: Aggregated Share of Top50 ASNs 18

Background 20

- Mission 20
- Data & Sources 20

About 22

- eco – Association of the Internet Industry 22
- topDNS Initiative 22
- AV-TEST Institute 22

Report Summary

This report is the seventh 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 June 2026 include:

- **Malicious URL volumes fell to a new reporting-period low in June, while 'other' malicious content reached a new high.**
  Total malicious URLs fell to **589,548** in June 2026, representing a **26.20% month-on-month decrease** from May (798,874). This decline was driven primarily by malware, which fell to **546,822 (-28.38%)** and accounted for approximately **93% of all malicious URLs**. June therefore marks the lowest malware volume in the current 12-month reporting window, indicating that the elevated levels seen during late 2025 and the spring 2026 recovery have continued to unwind.

  Potentially unwanted applications (PUAs) increased slightly to **8,519 (+5.73%)**, recovering from the May low of 8,057 but **remaining close to the bottom of the reporting range** and well below the July 2025 peak. In contrast, **'other' malicious URLs rose to 34,207 (+25.22%)**, establishing a **new reporting-period high** and increasing their share of total malicious URLs to approximately 6%. Despite this rise, 'other' content remains a secondary category compared with malware.

- **Potential phishing activity declined, while verified phishing rebounded.**
  All (potential) phishing URLs fell to **51,937 (-28.98%)** in June 2026, reversing May's increase. Volumes remain above the February low of 39,489 but are roughly half the reporting-period **average (103,657)**, confirming that overall phishing activity remains subdued relative to late 2025.

  Verified phishing increased to **2,663 (+33.82%)**, reversing the decline observed in May but remaining well below the reporting-period average of 6,619. The **verification rate rose from 2.72% in May to 5.13% in June**. This remains above the reporting-period low of 2.57% recorded in September 2025 and below the aggregate verification share of 6.39%.

- **Detection metrics declined sharply across all additional detection methods.**
  Machine learning detections **fell to 13,983 (-65.68%)**, visual **AI detections to 17,000 (-47.32%)**, and **detections identified by both methods to 8,509 (-72.16%)**. This reverses the broad May increase and places machine learning detections close to their

February low. As these categories overlap, the decline should be interpreted as a broad reduction in detections across the additional methods rather than as a direct measure of verified phishing.

- **Malicious activity remains highly concentrated within the Top 50 ASNs.** The Top 50 ASNs accounted for **547,743 malicious URLs** in June 2026, down 27.21% from May, comprising **510,834 malware URLs (93.26%), 7,693 PUAs (1.40%)**, and **29,216 URLs classified as 'other' malicious content (5.33%)**. This is the lowest monthly total in the current 12-month Top 50 dataset. While malware remains dominant, its share declined from 95.93% in May as 'other' content reached its highest monthly volume and share in the current window. The continued concentration of activity within the Top 50 ASNs supports targeted ASN-level mitigation as an effective mechanism for reducing large-scale abuse.

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 malware, PUA and other malware, broken down by category:

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

A **total** of **12,070,858 malicious URLs with ASNs** were identified in the period July 2025 to June 2026, **of which:**

- **11,550,286 URLs** could be **verified as malware**,
- **278,267 URLs** have been **classified as PUA**, and
- **242,305 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. Following this spike, volumes declined sharply in January and February 2026, recovered partially in March and April, and then **fell for a second consecutive month to 546,822 URLs in June 2026 (-28.38%)**. June therefore represents the lowest malware volume in the current reporting period, falling below the previous February 2026 low of 587,312 URLs and fully reversing the spring recovery.

PUA activity continued to exhibit substantial volatility over the reporting period. It **peaked in July 2025 (105,835 URLs)** before declining sharply through the second half of the year. After reaching a new low of 8,057 URLs **in May 2026, PUA volumes edged up to 8,519 URLs in June (+5.73%)**. This modest increase does not materially alter the longer-term downward trend, with current volumes remaining close to the reporting-period minimum.

In contrast, 'other' malicious content followed a different trajectory. In **June 2026**, this category **increased to 34,207 URLs (+25.22%)**, establishing **a new reporting-period high** and extending the rise recorded in May. Despite this increase, it continues to represent only a small proportion of total malicious activity. Across the full period, monthly averages amounted to **approximately 962,524 malware URLs, 23,189 PUAs**, and **20,192 'other' malicious URLs**, highlighting the persistent imbalance between categories.

Overall, the data indicate that the extreme spike observed in late 2025 has largely unwound and that **malware continues to dominate the threat landscape structurally**. At the same time, June recorded the lowest malware volume in the current 12-month window, while

'other' malicious content reached a new high. The resulting June distribution remains heavily skewed towards malware, but the rise in 'other' content to approximately 6% represents a modest broadening of the monthly composition.

Malicious URLs

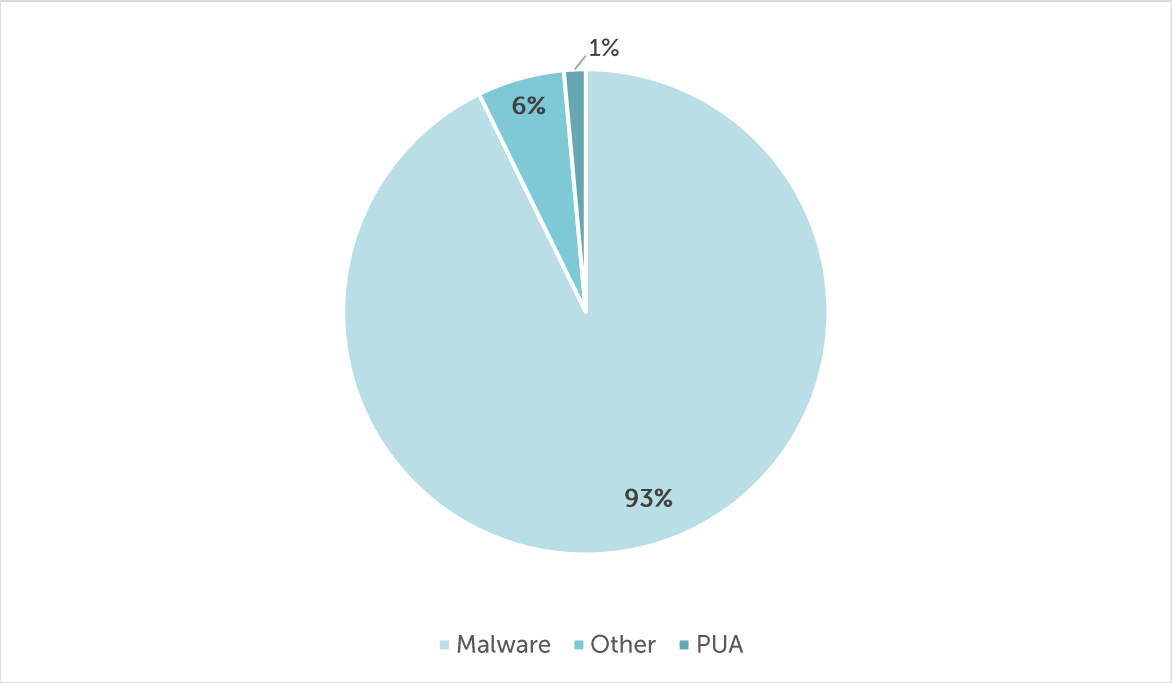

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **June 2026***

History of Malicious URLs

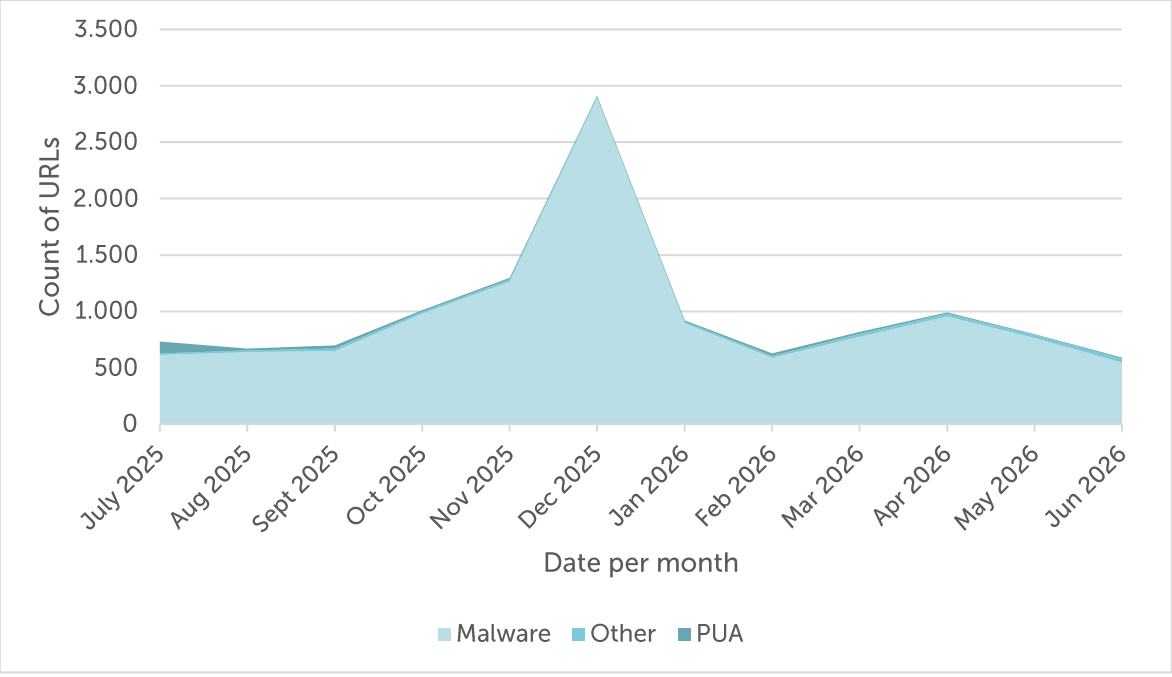

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **July 2025 to June 2026***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
July 2025	612,196		105,835		15,686	
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%
Jun 2026	546,822	-28.38%	8,519	+5.73%	34,207	+25.22%
Total	**11,550,286**		**278,267**		**242,305**	

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

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Month
High	2,885,933	Dec 2025	105,835	Jul 2025	34,207	Jun 2026
Low	546,822	Jun 2026	8,057	May 2026	13,272	Aug 2025
Average	**962,524**		**23,189**		**20,192**	

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

Commentary

The aggregate dataset covering **July 2025 to June 2026** identified a total of **12,070,858 malicious URLs** associated with ASNs, of which **11,550,286 URLs** were classified as malware, **278,267 URLs** were classified as PUA, and **242,305 URLs** as other malicious content. The June data extend the moderation observed after April, with total malicious URL volumes falling to the lowest level in the current reporting window.

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 in both May and June, reaching **546,822 URLs in June (-28.38%)**. This is the **lowest malware volume of the reporting period** and places current activity below the levels observed throughout the remainder of the 12-month window.

PUA activity remained close to its reporting-period low. After reaching a peak of **105,835 URLs in July 2025**, volumes declined substantially through the remainder of the reporting period. Following the May 2026 low of **8,057 URLs**, June recorded a slight increase to **8,519 (+5.73%)**. The limited rebound confirms that PUA activity remains structurally subdued compared with mid-2025 levels.

'Other' malicious content continued to move in the opposite direction. The category increased to **34,207 URLs in June 2026 (+25.22%)**, establishing a **new reporting-period high** after the previous May record of 27,317 URLs. Although its share increased to around 6% of all malicious URLs in June, the category remains comparatively small relative to malware.

As reflected in Table 2, malware activity ranged from **546,822 URLs (June 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 **34,207 URLs (June 2026)**.

Overall, the data confirms the **continued structural dominance of malware within the malicious URL landscape**. However, June marks a further normalisation in absolute malware volumes and a modest shift in composition, with **'other' malicious content reaching its highest level in the current window**. PUA activity remains near its low, while the overall malicious URL total is now below all other months in the reporting period.

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 1,243,883 (potential) phishing URLs** and **79,424 verified phishing URLs** were identified in the period from **July 2025 to June 2026**. The data show pronounced volatility in overall volumes, while phishing activity during 2026 remains substantially below the levels recorded in the second half of 2025.

All (potential) phishing activity **peaked in September 2025 (235,013 URLs)** before declining sharply during the final quarter of the year. Following a reporting-period low of 39,489 URLs in February 2026, **volumes recovered intermittently through May**, reaching 73,130 URLs, before falling again to 51,937 URLs in June 2026 (-28.98%). June therefore sits only modestly above the February low and at approximately half the reporting-period average of 103,657 URLs.

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 minimum of 1,691 URLs in February 2026**, confirmed phishing remained low in March, April and May before **increasing to 2,663 URLs in June (+33.82%)**. Despite this rebound, the June figure remains well below the reporting-period average of 6,619 URLs.

The verification rate, meaning verified phishing as a share of potential phishing, varied significantly over time. The **verification rate reached a reporting-period low of 2.57% in September 2025** and subsequently peaked at 14.80% in December. After falling to 2.72% in May 2026, it **recovered to 5.13% in June**. This **remains below the 6.39% aggregate verification share** across the current reporting window, indicating that confirmed phishing remains a relatively small share of overall potential phishing activity.

Additional detection metrics **moved sharply lower in June**. Machine learning detections fell to 13,983 (-65.68%), visual AI detections to 17,000 (-47.32%), and URLs identified by both methods to 8,509 (-72.16%). These declines reverse the broad increase recorded in May. As the three categories are not mutually exclusive, they indicate a contraction across the additional detection methods rather than a direct one-to-one change in verified phishing.

Overall, the data indicates that phishing activity remains structurally subdued relative to late 2025. **June combined a renewed decline in potential phishing with a modest rebound in**

verified cases and the verification rate. The mixed movement does not indicate a broad-based escalation; instead, it reflects continued volatility at comparatively low absolute levels

History of Phishing URLs

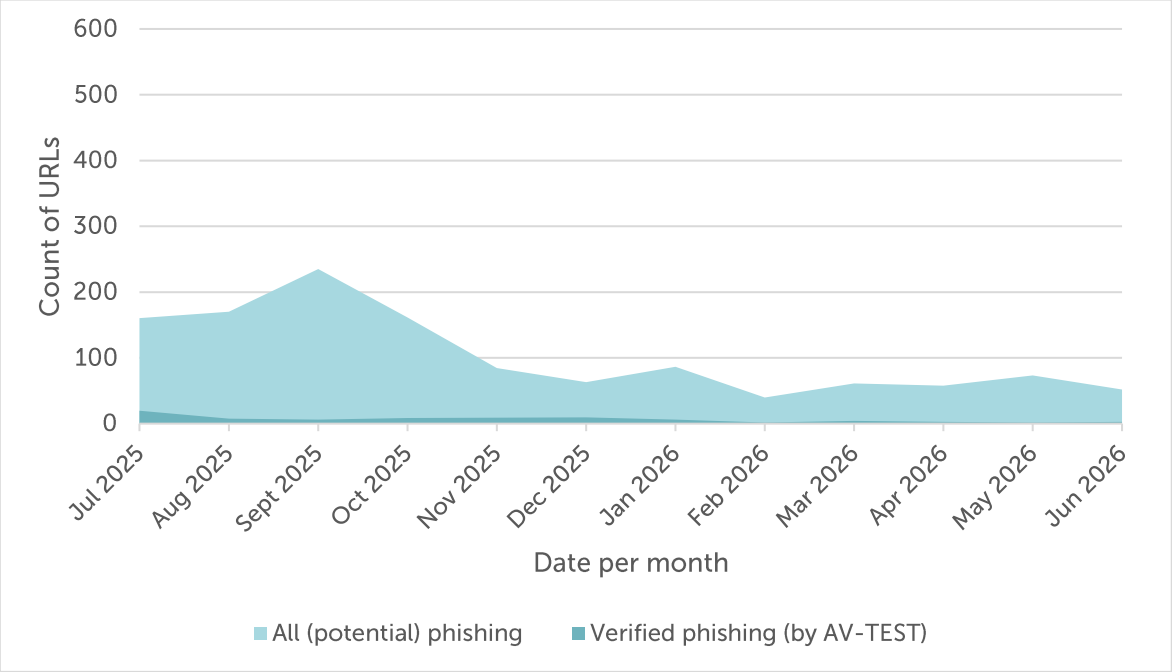

*Figure 3: Aggregate Trends - **History of Phishing URLs - July 2025 to June 2026***

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 **June 2026**, this approach identified **13,983 phishing URLs with ASNs via machine learning, 17,000 via visual AI**, with **8,509 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 **51,937 potential phishing URLs with ASNs**.

History of Phishing URLs verified by Machine Learning & Visual AI

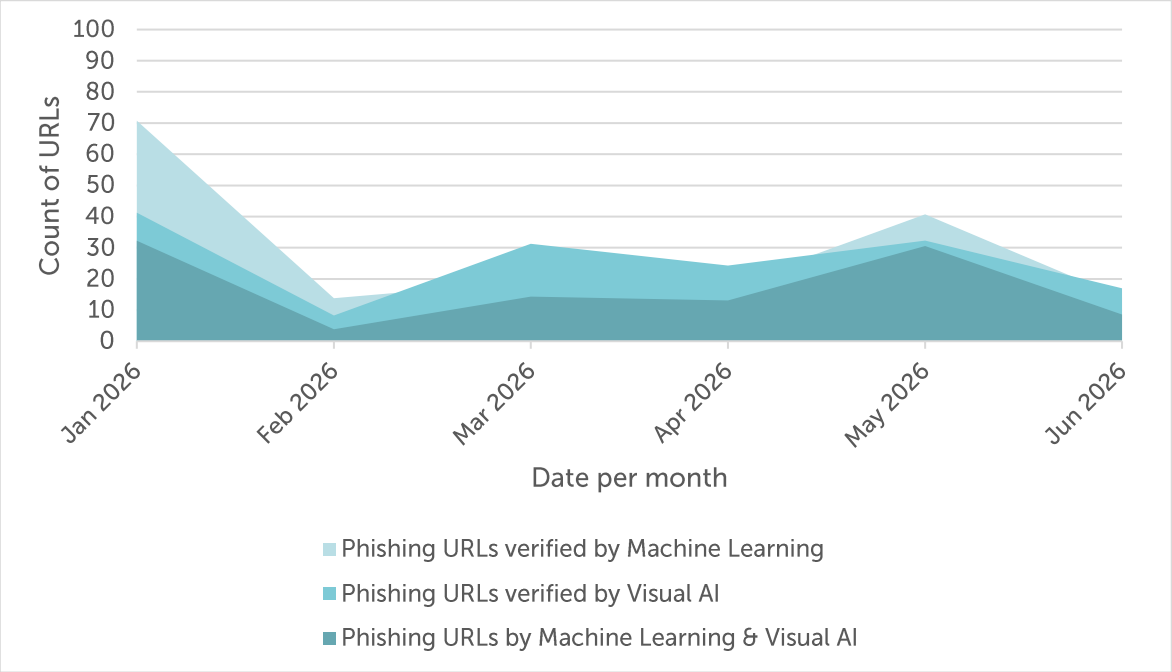

*Figure 4: Aggregate Trends - **History of Phishing URLs verified by Machine Learning & Visual AI** - **January 2026 to June 2026***

- **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 **17,000 phishing URLs with ASNs in June 2026**. These were included in the total of **51,937 potential phishing URLs with ASNs**. Regarding the **2,663 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, **8,509 phishing URLs with ASNs were identified in June 2026**. These were included in the total of **51,937 potential phishing URLs with ASNs**. Regarding the **2,663 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%
June 2026	13,983	-65.68%	17,000	-47.32%	8,509	-72.16%
Total	**176,244**		**154,225**		**102,500**	

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

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

	Verified by Machine Learning	Month	Verified by Visual AI	Month	Verified by Machine Learning & Visual AI	Month
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	**29,374**		**25,704**		**17,083**	

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

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
July 2025	160,240		12.27%	19,656	
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%
Jun 2026	51,937	-28.98%	5.13%	2,663	+33.82%
Total	**1,243,883**		6.39%	**79,424**	

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

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month		Verified phishing	Month
High	235,013	Sep 2025		19,656	Jul 2025
Low	39,489	Feb 2026		1,691	Feb 2026
Average	**103,657**			**6,619**	

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

Commentary

The aggregated dataset covering **July 2025 to June 2026** identified a total of **1,243,883 (potential) phishing URLs** and **79,424 verified phishing URLs** associated with ASNs. Overall phishing activity remains substantially below the levels observed during the second half of 2025, with June reversing the temporary increase recorded in May.

All (potential) phishing activity peaked in **September 2025 at 235,013 URLs** before declining sharply during the following months. After reaching a reporting-period low of **39,489 URLs in February 2026**, volumes recovered intermittently through May before falling to **51,937 in June 2026 (-28.98%)**. This leaves June at around half the reporting-period average of **103,657 URLs** and confirms that overall phishing volumes remain subdued.

Verified phishing followed a more persistent downward trajectory after peaking in **July 2025 at 19,656 URLs**. Confirmed phishing activity reached a minimum of **1,691 URLs in February 2026** and remained comparatively low through May. June recorded a rebound to **2,663 (+33.82%)**, but the figure remains well below the reporting-period average of **6,619** and does not materially alter the broader low-volume pattern.

The share of verified phishing within total (potential) phishing URLs remains volatile. The **verification rate reached a reporting-period low of 2.57% in September 2025** and subsequently peaked at 14.80% in December. After falling to 2.72% in May 2026, it **recovered to 5.13% in June**. This rebound brings the rate closer to, but still below, the **6.39% aggregate verification share** for the 12-month window.

Detection metrics provide additional context. In June 2026, machine learning detections fell to **13,983 (-65.68%)**, visual AI detections to **17,000 (-47.32%)**, and URLs identified by both methods to **8,509 (-72.16%)**. The broad decline reverses the strong increase observed in May and places all three metrics well below their May levels. Because the categories overlap,

these figures should be read as complementary detection indicators rather than as separate counts of verified phishing.

Overall, the data suggest that phishing activity remains **structurally subdued relative to earlier phases of the reporting period**. June saw a decline in potential phishing alongside a modest recovery in verified phishing and the verification rate. This mixed pattern indicates continued volatility at low absolute levels rather than a renewed escalation in 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 11,446,802 URLs** with ASNs were identified among the Top 50 ASNs during the period July 2025 to June 2026, of which:

- **10,965,420 URLs** could be **verified as malware**,
- **278,796 URLs** have been **classified as PUA**, and
- **202,586 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
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
Jun 2026	510,834	93.26%	7,693	1.40%	29,216	5.33%	547,743
Total	**10,965,420**	**95.79%**	**278,796**	**2.44%**	**202,586**	**1.77%**	**11,446,802**

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

Commentary

The aggregate dataset for the Top 50 ASNs covering **July 2025 to June 2026** identified a total of **11,446,802 malicious URLs**. Of these, **10,965,420 URLs (95.79%)** were linked to malware, **278,796 URLs (2.44%)** to PUA, and **202,586 URLs (1.77%)** 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 in both May and June. June recorded **547,743 total malicious URLs**, the **lowest monthly total in the current 12-month Top 50 dataset**, with malware accounting for **93.26%** of activity.

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 remained low in 2026. June recorded **7,693 PUA URLs (1.40%)**, slightly below May and representing the **lowest PUA volume in the current 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 **29,216 URLs (5.33%) in June 2026**, establishing the **highest monthly volume and share in the current Top 50 window**. The increase reduced malware's monthly share from 95.93% in May to 93.26% in June, but did not displace malware as the dominant category.

Overall, the data underscore the continued centralisation of malicious infrastructure within major autonomous systems, with **malware remaining the primary driver of abuse**. Absolute volumes fell to a new 12-month low in June, while the composition broadened modestly as **'other' malicious content increased**. Even so, the **structural concentration remains pronounced**, continuing 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.