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

August 2026

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

This report is the eighth 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 July 2026 include:

- **Malicious URL volumes declined for a third consecutive month, with malware reaching a new reporting-period low while 'other' content reached a new high.**
  Total malicious URLs fell to **420,968** in July 2026, representing a **28.59% month-on-month decrease** from June (589,548). This decline was driven primarily by malware, which fell to **378,129 (-30.85%)** and accounted for approximately **90% of all malicious URLs**. July 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 **8,616 (+1.14%)**, extending the modest recovery from the May low of 8,057 but remaining close to the bottom of the reporting range. In contrast, **'other' malicious URLs rose marginally to 34,223 (+0.05%)**, establishing a **new reporting-period high** and increasing their share of total malicious URLs to **approximately 8%**. Despite this rise, 'other' content remains a secondary category compared with malware.

- **Potential phishing activity nearly doubled, while verified phishing also increased but remained comparatively low.**
  All (potential) phishing URLs rose to **102,368 (+97.10%)** in July 2026, almost doubling from June and moving slightly above the 12-month average of **98,834**. Despite this sharp increase, volumes remained well below the reporting-period peak of **235,013** recorded in September 2025.

  Verified phishing increased to **3,392 (+27.38%)**, reversing part of the decline observed earlier in 2026 but remaining well below both the reporting-period average of **5,263** and the December 2025 high of **9,339**. Because potential phishing grew substantially faster than verified phishing, the verification rate fell from 5.13% in June to 3.31% in July.

- **Detection metrics remained broadly stable across the automated verification methods.**
  Machine learning detections decreased marginally to **13,857 (-0.90%)**, visual AI detections fell to **16,772 (-1.34%)**, while detections identified by both methods

increased to **9,114 (+7.11%)**. The relative stability of these metrics contrasts with the near doubling of potential phishing URLs, indicating that the July increase in potential activity was not accompanied by a comparable rise across the automated verification indicators.

- **Malicious activity remained highly concentrated within the Top 50 ASNs, although July showed a marked shift in category composition.** The Top 50 ASNs accounted for **370,371 malicious URLs** in July 2026, down **32.38% from June**. This total comprised **334,669 malware URLs (90.36%)**, **7,868 PUAs (2.12%)**, and **27,834 URLs classified as 'other' malicious content (7.52%)**. Malware's share was the lowest in the current 12-month window, while the share of 'other' content was the highest. The Top 50 ASNs still accounted for approximately 88% of all malicious URLs identified in July, supporting continued targeted ASN-level mitigation while also indicating a modest reduction in concentration compared with June.

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 **11,758,109 malicious URLs with ASNs** were identified in the period August 2025 to July 2026, **of which:**

- **11,316,219 URLs** could be **verified as malware**,
- **181,048 URLs** have been **classified as PUA**, and
- **260,842 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. Following the partial recovery observed in March and April 2026, malware declined for three consecutive months, falling to 378,129 URLs in July (-30.85%). **July therefore represents the lowest malware volume in the current reporting window** and sits approximately 60% below the 12-month average of 943,018.

PUA activity remained at comparatively low levels. Within the current reporting window, it **peaked at 27,242 URLs in September 2025** before declining through late 2025 and early 2026. **After reaching a low of 8,057 URLs in May, volumes increased slightly to 8,519 in June and 8,616 in July (+1.14%)**, indicating stabilisation close to the lower end of the reporting range rather than a material recovery.

In contrast, 'other' malicious content remained elevated. **July** recorded 34,223 URLs (+0.05%), only marginally above June's 34,207 but sufficient to establish **a new reporting-period high**. The near-flat month-on-month movement suggests a plateau at elevated levels rather than a further acceleration. Across the full period, monthly averages amounted to approximately **943,018 malware URLs, 15,087 PUAs**, and **21,737 'other' malicious URLs**.

Overall, the July data show a continued contraction in total malicious URL volumes, driven overwhelmingly by the decline in malware. **Malware remains the dominant category**, but its July share fell to approximately 90%, while 'other' content rose to just over 8%. This represents a notable diversification in category composition compared with the extreme malware concentration observed in late 2025 and early 2026.

Malicious URLs

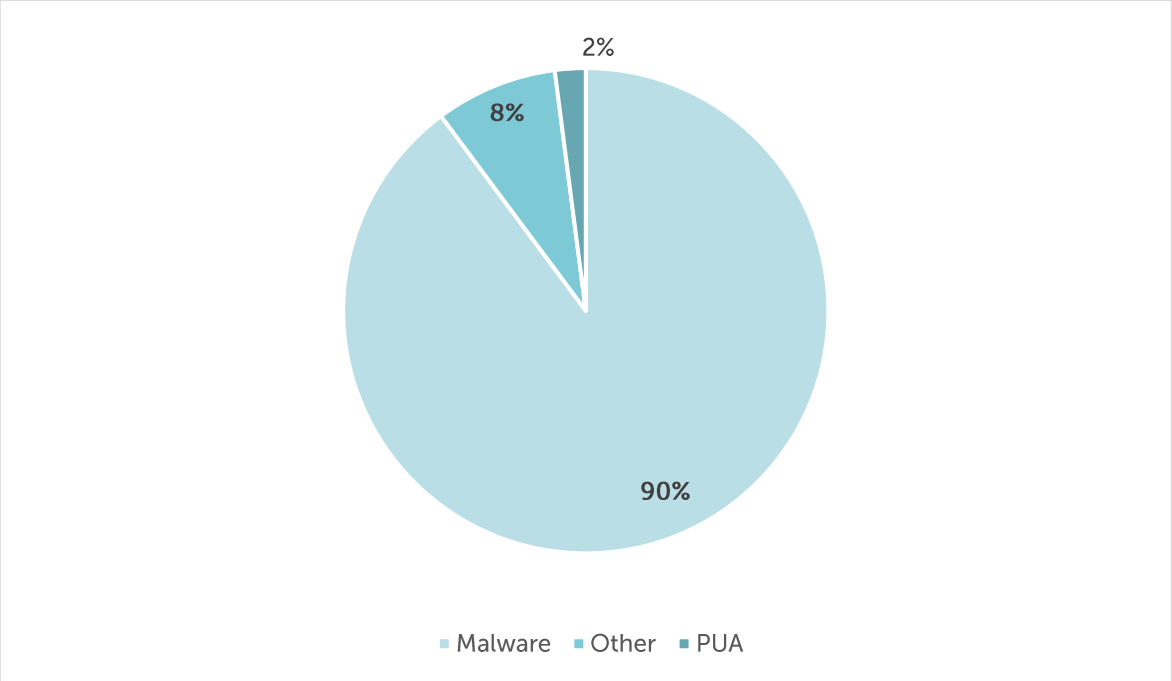

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **July 2026***

History of Malicious URLs

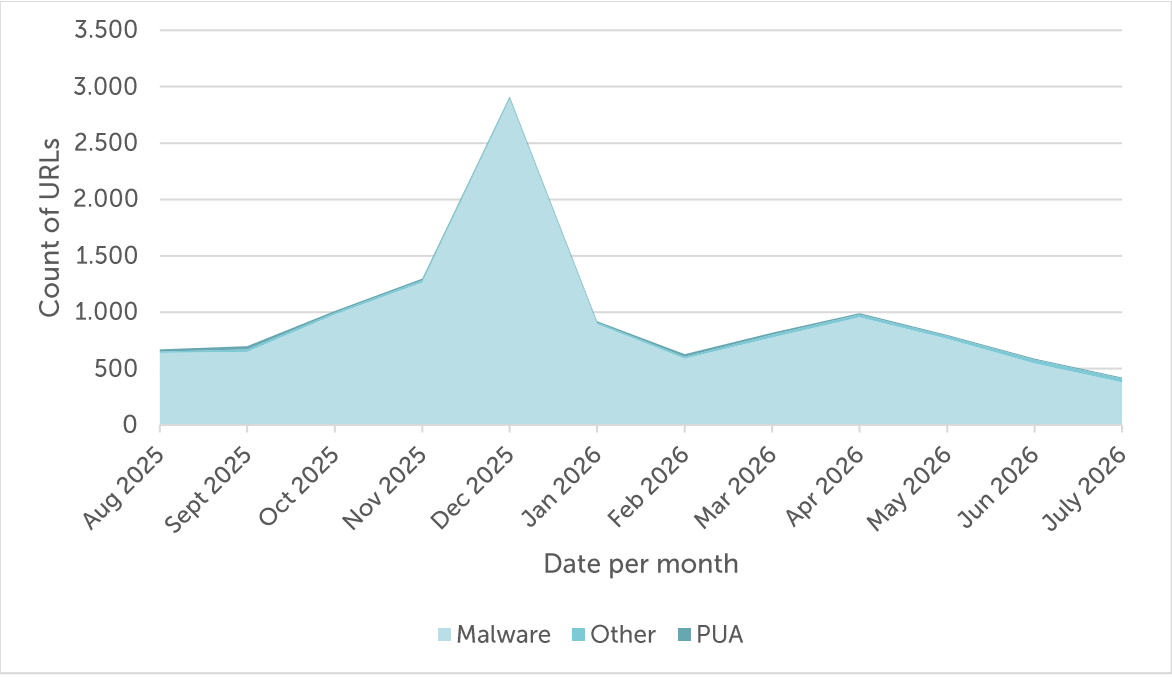

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **August 2025 to July 2026***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
Aug 2025	638,238		19,551		13,272	
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%
July 2026	378,129	-30.85%	8,616	+1.14%	34,223	+0.05%
Total	**11,316,219**		**181,048**		**260,842**	

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

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Month
High	2,885,933	Dec 2025	27,242	Sep 2025	34,223	Jul 2026
Low	378,129	Jul 2026	8,057	May 2026	13,272	Aug 2025
Average	**943,018**		**15,087**		**21,737**	

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

Commentary

The aggregate dataset covering August 2025 to July 2026 identified a total of **11,758,109 malicious URLs** associated with ASNs, of which **11,316,219 URLs were classified as malware**, **181,048 URLs as PUA**, and **260,842 URLs as other malicious content**. The latest data extend the decline in overall malicious activity observed since April 2026.

The highest level of malware activity was recorded in **December 2025 (2,885,933 URLs)**, substantially **exceeding all other months in the reporting window**. Following the partial recovery in March and April, malware declined in May, June and July, reaching **378,129 URLs in July (-30.85%)**. This is the lowest malware volume in the current 12-month period and marks a clear reversal from the elevated levels seen during late 2025 and early 2026.

PUA activity remained subdued. After reaching its current-window **high of 27,242 URLs in September 2025**, volumes declined substantially and reached a **low of 8,057 in May 2026**. The small increases recorded in June and July, to 8,519 and 8,616 respectively, suggest stabilisation at a low level rather than a sustained rebound.

'Other' malicious content followed a different trajectory. It rose sharply in June and then remained virtually unchanged in July at **34,223 URLs (+0.05%)**, establishing **a new reporting-period high**. Although the absolute increase in July was negligible, the category's share of total malicious URLs rose to approximately 8% because malware volumes contracted much more strongly.

As reflected in Table 2, malware activity ranged from **378,129 URLs in July 2026 to 2,885,933 in December 2025**. PUA activity ranged from **8,057 URLs in May 2026 to 27,242 in September 2025**, while 'other' malicious content ranged from **13,272 URLs in August 2025 to 34,223 in July 2026**.

Overall, the data confirm that **malware remains the dominant component of the malicious URL landscape**, but the degree of concentration has eased. July combines the lowest malware volume in the current reporting window with the highest absolute level of 'other' malicious content, producing the most diversified category mix seen in recent months.

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 1,186,011 (potential) phishing URLs** and **63,160 verified phishing URLs** were identified in the period from **August 2025 to July 2026**. The data continue to show pronounced volatility in overall phishing volumes, while verified phishing remains comparatively subdued in 2026.

All (potential) phishing activity peaked at **235,013 URLs in September 2025 before declining sharply through the final quarter** of the year. After reaching a **reporting-period low of 39,489 URLs in February 2026**, activity fluctuated at lower levels through June before **rising sharply to 102,368 URLs in July (+97.10%)**. This places July slightly above the reporting-period average of 98,834, although volumes remain 56% below the September peak.

Verified phishing reached its current-window **high of 9,339 URLs in December 2025 and fell to a low of 1,691 in February 2026**. July recorded 3,392 verified phishing URLs (+27.38%), an increase from June but still substantially below both the reporting-**period average of 5,263 and the late-2025 high**.

The verification rate, meaning verified phishing as a share of potential phishing, peaked at **14.80% in December 2025**. **In July, the rate fell to 3.31% from 5.13% in June**. The decline occurred despite an increase in verified phishing because the volume of potential phishing almost doubled, indicating that the July expansion was concentrated primarily in the broader pool of suspected activity.

Additional detection **metrics were comparatively stable in July**. Machine learning identified **13,857 URLs (-0.90%)**, **visual AI identified 16,772 (-1.34%)**, and **9,114 URLs were identified by both methods (+7.11%)**. These results are not mutually exclusive. The limited movement across these metrics contrasts with the 97.10% increase in potential phishing and suggests that the broader rise in July was not mirrored proportionately across the automated verification methods.

Overall, the July data indicate a strong rebound in potential phishing activity from June's low level, but not a corresponding escalation in confirmed or automatically verified phishing. **Verified phishing remains well below late-2025 levels**, while the verification share has declined, supporting a cautious interpretation of the increase in headline potential-phishing volumes.

History of Phishing URLs

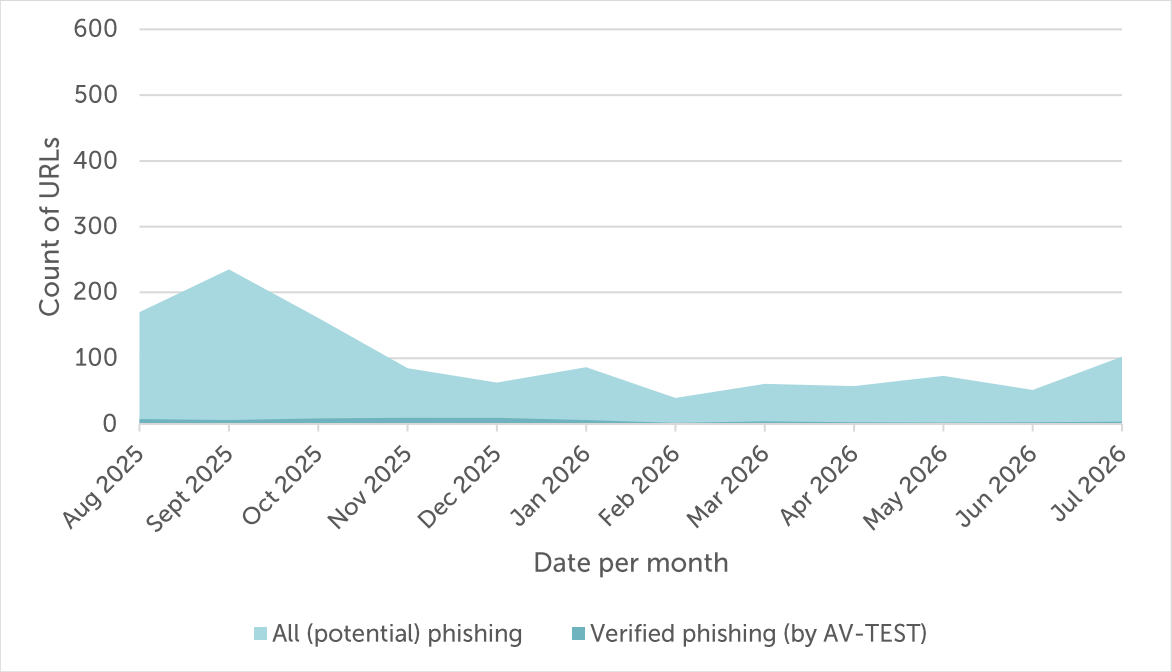

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **August 2025 to July 2026***

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 **July 2026**, this approach identified **13,857 phishing URLs with ASNs via machine learning**, **16,772 via visual AI**, with **9,114 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 **102,368 potential phishing URLs with ASNs**.

History of Phishing URLs verified by Machine Learning & Visual AI

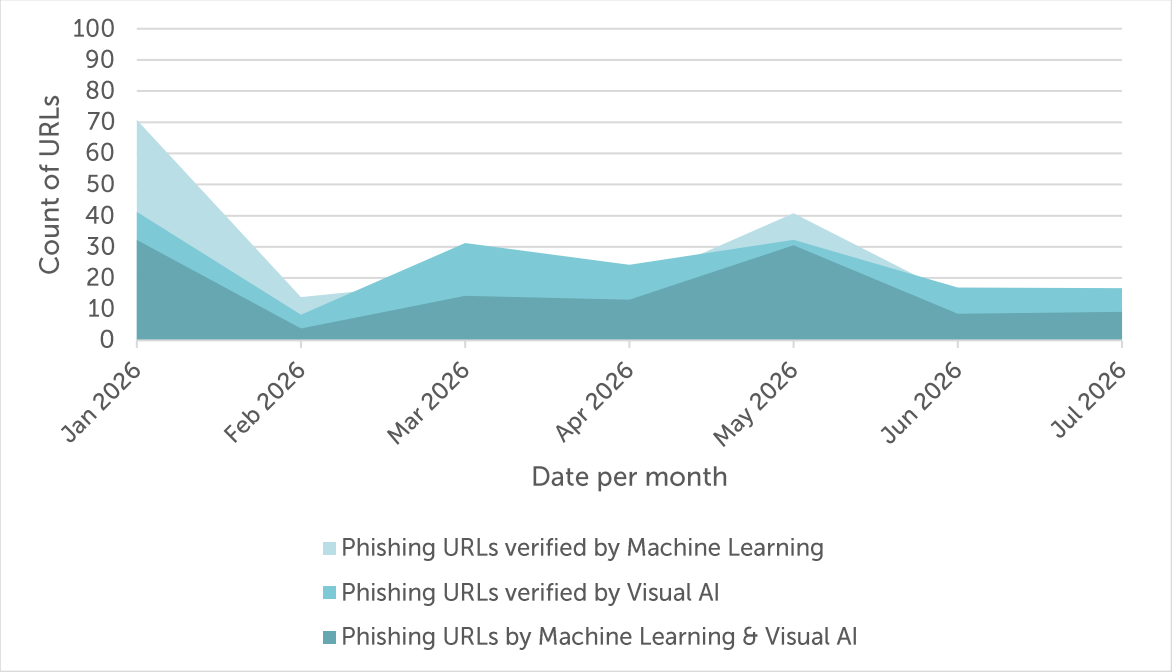

*Figure 4: Aggregate Trends - **History of Phishing URLs verified by Machine Learning & Visual AI - January 2026 to July 2026***

- **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 **16,772 phishing URLs with ASNs in July 2026**. These were included in the total of 102,368 potential phishing URLs with ASNs. Regarding the **3,392 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, **9,114 phishing URLs with ASNs were identified in July 2026**. These were included in the total of **102,368 potential phishing URLs with ASNs**. Regarding the **3,392 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%
July 2026	13,857	-0.90%	16,772	-1.34%	9,114	+7.11%
Total	**190,101**		**170,997**		**111,614**	

*Table 3: Aggregate Trends - **History of Phishing URLs verified by Machine Learning & Visual AI** - **January 2026 to July 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	**27,157**		**24,428**		**15,945**	

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

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
Aug 2025	169,908		4.36%	7,414	
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%
July 2026	102,368	+97.10%	3.31%	3,392	+27.38%
Total	**1,186,011**		5.33%	**63,160**	

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

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month		Verified phishing	Month
High	235,013	Sep 2025		9,339	Dec 2025
Low	39,489	Feb 2026		1,691	Feb 2026
Average	**98,834**			**5,263**	

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

Commentary

The aggregated dataset covering **August 2025 to July 2026** identified a total of **1,186,011 (potential) phishing URLs** and **63,160 verified phishing URLs** associated with ASNs. July produced a sharp increase in potential phishing activity, while confirmed phishing increased more moderately and remained at comparatively low levels.

All (potential) phishing activity reached its reporting-period high of **235,013 URLs in September 2025** before declining markedly through late 2025. Following the **February 2026 low of 39,489**, volumes fluctuated through the spring and fell to 51,937 in June. **July then recorded a 97.10% increase to 102,368 URLs**, bringing activity **slightly above the 12-month average** of 98,834 but still well below the September peak.

Verified phishing followed a more subdued trajectory. After reaching 9,339 URLs in December 2025, **volumes fell sharply in early 2026 and bottomed out at 1,691 in February**. **July recorded 3,392 verified phishing URLs (+27.38%)**, continuing the increase from the May level of 1,990 but remaining approximately 36% below the reporting-period average.

The share of verified phishing within total (potential) phishing URLs **fell from 5.13% in June to 3.31% in July**. This decline occurred despite the increase in verified phishing because potential phishing expanded much more rapidly. The result indicates that the **July rebound was driven primarily by a larger pool of potential cases** rather than a proportionate increase in confirmed phishing.

Detection metrics provide further context. Machine learning **detections were broadly stable at 13,857 (-0.90%)**, **visual AI detections at 16,772 (-1.34%)**, and **URLs identified by both methods increased moderately to 9,114 (+7.11%)**. The absence of a comparable surge in these metrics reinforces the distinction between the sharp increase in potential phishing and the more limited movement in stronger verification signals.

Overall, the data suggest that **July represents a rebound in potential phishing volume rather than a return to the higher confirmed-threat levels observed in late 2025**. The combination of rising potential activity, more moderate growth in verified phishing, and a lower verification share points to renewed volume without equivalent strengthening in confirmation metrics.

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 11,179,818 URLs** with ASNs were identified among the Top 50 ASNs during the period August 2025 to July 2026, of which:

- **10,780,016 URLs** could be **verified as malware**,
- **181,765 URLs** have been **classified as PUA**, and
- **218,037 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
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
July 2026	334,669	90.36%	7,868	2.12%	27,834	7.52%	370,371
Total	**10,780,016**	**96.42%**	**181,765**	**1.63%**	**218,037**	**1.95%**	**11,179,818**

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

Commentary

The aggregate dataset for the Top 50 ASNs covering **August 2025 to July 2026** identified a total of **11,179,818 malicious URLs**. Of these, **10,780,016 URLs (96.42%)** were linked to malware, **181,765 URLs (1.63%)** to PUA, and **218,037 URLs (1.95%)** to other malicious content. The data therefore continue to show a pronounced concentration of malicious activity within the largest autonomous systems identified by the methodology.

Malware dominance intensified markedly in late 2025, peaking in December at 2,833,805 URLs and a 99.14% share. Following the partial recovery observed in March and April 2026, Top 50 volumes declined for three consecutive months. **July recorded 370,371 malicious URLs in total (-32.38% from June), the lowest monthly total** in the current reporting window. Malware fell to 334,669 URLs (-34.49%), and its share declined to 90.36%, also the lowest share in the 12-month period.

PUA activity remained close to the lower end of the reporting range. After peaking at 28,218 URLs in September 2025, **volumes declined substantially and reached 7,693 in June 2026**. July recorded a small increase to 7,868 (+2.27%), corresponding to a 2.12% share of the Top 50 total.

'Other' malicious content decreased slightly **from its June high of 29,216 URLs to 27,834 in July (-4.73%)**. However, because malware declined much more sharply, the category's share rose to 7.52%, the highest proportion observed in the current reporting window. The July composition therefore represents a notable shift away from the extreme malware concentration seen during late 2025 and early 2026.

Overall, malicious activity remains highly concentrated within the Top 50 ASNs, which accounted for approximately 88% of all malicious URLs identified in July. However, this was lower than the approximately 93% recorded in June, and **the category mix became more diversified**. These dynamics continue to support targeted ASN-level mitigation while indicating that both **absolute concentration and malware's internal share eased in July**.

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.