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

October 2025

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

This report is the tenth publication from the topDNS Initiative's measurement initiative, topDNS Report: Monthly Analysis for ISPs. The purpose of this report is to establish 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 September 2025 include:

- **Overall, malware maintained its strong dominance, while both PUAs and other malicious content showed modest increases in September 2025.** Malware URLs rose to 647,740 (+1.49% compared to August), maintaining their overwhelming share at 93% of all malicious URLs. Potentially unwanted applications (PUAs) rebounded significantly to 27,242 (+39.34% compared to August's low of 19,551), recovering somewhat from July's dramatic collapse but nonetheless remaining well below the July 2025 peak of 105,835. 'Other' malicious content increased sharply to 23,270 (+75.33%), reversing the declining trend seen in recent months. The distribution returned to previous levels with malware at 93%, PUAs at 4%, and 'other' content at 3%, after August's temporary malware dominance at 95%. Historical peaks remain: November 2024 for malware (761,550), July 2025 for PUAs (105,835), and October 2024 for 'other' content (64,882).
- **Phishing activity showed contrasting trends in September, with po-tential phishing rebounding strongly while verified phishing reached a new low.** Potential phishing URLs increased substantially to 235,013 (+38.32% compared to the small rise of +6.03% in August), though still below the reporting-period average of 318,932. Even more notably, verified phishing URLs declined further to 6,036 (-18.59% vs. August and -62.28% vs. July), marking the lowest point in the entire report-ing period since October 2024. The previous low was September 2025 at 6,342. April 2025 still represents the highest point for potential phishing URLs (542,081), while May 2025 holds the peak for verified phishing (21,492).
- **This continued decline in verified phishing, despite the rise in potential activity, represents a notable departure from earlier 2025 patterns.** The sustained lower levels across August and September suggest a potential shift in threat actor behaviour or improved detection and takedown mechanisms. September's figure sits approximately 49% below the reporting-period average of 11,872, highlighting the stabilization at lower levels compared with earlier spikes in May and July.

- **In September 2025, the Top 50 ASNs accounted for 709,958 malicious URLs, a significant increase compared to August's 577,524.**
  This total included 658,068 malware (92.69%), 28,218 PUAs (3.97%), and 23,672 'other' content (3.33%). The increase was driven primarily by malware, which grew by over 110,000 URLs month-over-month. Across the reporting period from June 2024 to September 2025, the Top 50 ASNs contributed 8,956,411 URLs in total, including 7,897,819 malware (88.18%), 533,887 PUAs (5.96%), and 524,705 'other' content (5.86%). Malware continues to dominate these networks, with PUAs showing significant volatility – particularly the dramatic spike in July 2025 (104,899) followed by a sharp decline in August (19,470) and modest recovery in September (28,218).

This is our fifth report to cover a full 12-month period, with the reporting years rotating to make comparisons easier and patterns clearer. This is an important step towards identifying longer-term trends.

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 **7,578,834 malicious URLs with ASNs** were identified in the period October 2024 to September 2025, **of which:**

- **6,766,627 URLs** could be **verified as malware**,
- **429,882 URLs** have been **classified as PUA**, and
- **382,325 URLs** as **other**.

The **highest number of malicious URLs for malware and 'other' content** was identified in **November 2024** and **October 2024** respectively, while **PUAs peaked more recently in July 2025, before collapsing in August 2025** and **partially recovering in September 2025.** The **lowest levels were recorded** in **December 2024 for malware, April 2025 for PUAs**, and **May 2025 for 'other' content**.

In the latest month, September 2025, the ratio returned to the previous distribution level, with malware accounting for 93% of all malicious URLs, PUAs at 4%, and 'other' content at 3%.

Malicious URLs

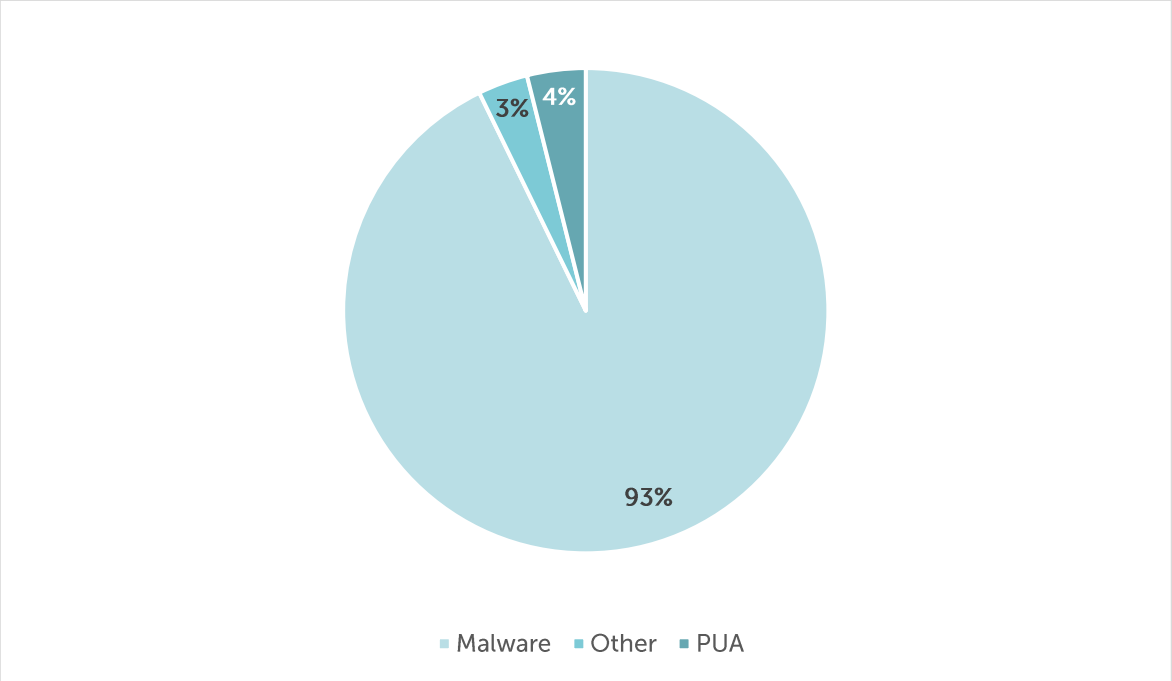

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **September 2025***

History of Malicious URLs

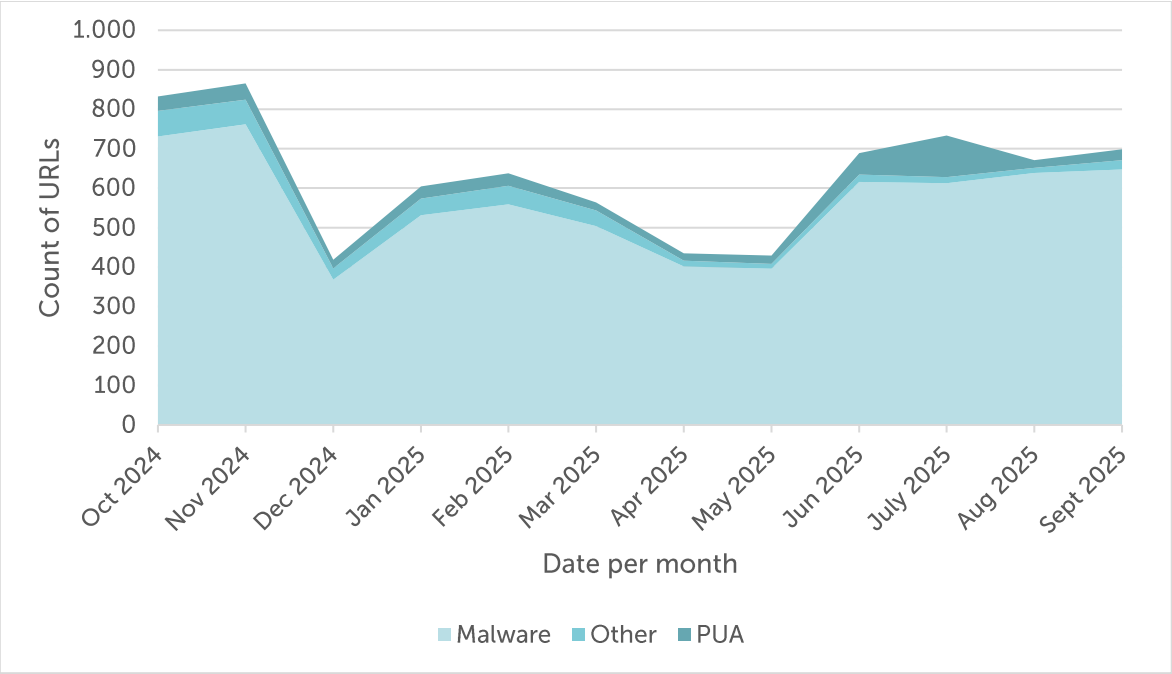

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **October 2024 to September 2025***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
Oct 2024	730,895		36,821		64,882	
Nov 2024	761,550	-4.19%	41,235	+11.99%	62,622	-3.48%
Dec 2024	368,246	-51.65%	22,345	-45.81%	28,432	-54.60%
Jan 2025	531,473	+44.33%	30,652	+37.18%	42,139	+48.21%
Feb 2025	559,089	+5.20%	31,846	+3.90%	46,639	+10.68%
Mar 2025	504,027	-9.85%	20,104	-36.87%	39,830	-14.60%
Apr 2025	401,518	-20.34%	18,739	-6.79%	14,600	-63.34%
May 2025	396,207	-1.32%	21,305	+13.69%	12,011	-17.73%
Jun 2025	615,448	+55.33%	54,207	+154.43%	18,942	+57.71%
July 2025	612,196	-0.53%	105,835	+95.24%	15,686	-17.19%
Aug 2025	638,238	+4.25%	19,551	-81.53%	13,272	-15.39%
Sep 2025	647,740	+1.49%	27,242	+39.34%	23,270	+75.33%
Total	6,766,627		429,882		382,325	

*Table 1: Aggregate Malware Trends - **History of Malicious URLs** - **October 2024 to September 2025***

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Change
High	761,550	Nov 2024	105,835	Jul 2025	64,877	Oct 2024
Low	368,246	Dec 2024	18,739	Apr 2025	12,011	May 2025
Average	563,886		35,824		31,860	

*Table 2: Aggregate Trends - **Key Figures of Malicious URLs** - **October 2024 to September 2025***

Commentary

The aggregate dataset covering October 2024 to September 2025 identified a total of 7,578,834 malicious URLs with ASNs, of which 6,766,627 were verified as malware, 429,882 classified as potentially unwanted applications (PUAs), and 382,325 as 'other' content. The highest numbers of **malware and 'other' URLs** were recorded in November 2024 and October 2024 respectively, while **PUAs peaked more recently in July 2025** at 105,835 URLs, **before collapsing in August 2025 to just 19,551** and partially **recovering to 27,242 in September 2025**. At the lower end, the minimum values occurred in December 2024 for malware (368,246), April 2025 for PUAs (18,739), and May 2025 for 'other' content (12,011). On average across the reporting period, monthly figures amounted to approximately 563,886 malware URLs, 35,824 PUAs, and 31,860 'other' URLs.

The highs for malware and 'other' content remain unchanged compared to earlier reports, but PUAs continue to demonstrate dramatic volatility. After July's extraordinary spike to nearly 14% of all malicious URLs, **PUAs dropped back to 3% in August** before **recovering modestly to 4% in September 2025**. In the latest month, September 2025, the ratio returned to the previous distribution level, with malware accounting for 93% of all malicious URLs, PUAs at 4%, and 'other' content at 3%. This represents a normalisation **after August's unusual distribution where malware reached 95% dominance**. The September figures align more closely with historical patterns observed throughout most of the reporting period.

As Table 2 highlights, malware activity ranged from a high of 761,550 URLs in November 2024 to a low of 368,246 in December 2024. PUAs fluctuated more sharply, from 18,739 in April 2025 to 105,835 in July 2025, while 'other' content reached 64,882 in October 2024 but fell to 12,011 in May 2025. These figures **confirm malware's dominance in absolute terms**, while PUAs and 'other' categories continue to show much greater volatility, reflecting campaign-driven surges and seasonal dips. Notably, 'other' content reversed its **steady downward trajectory** in September 2025, increasing by 75.33% to 23,270 URLs, suggesting a possible resurgence of activity in this category after months of decline.

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 **3,827,181 phishing URLs with ASNs** were identified in the period from October 2024 to September 2025, **of which 142,468 URLs** could be **verified**.

There was a further increase in January, February, March and April 2025, followed by a sharp decline in May 2025 and continued drops in June and July 2025, before a modest rise in August 2025. September 2025 saw a substantial rebound in potential phishing, but verified phishing reached a new low.

Between October 2024 and September 2025, the **highest number of all (potential) phishing URLs** was identified in April 2025, while **verified phishing URLs** peaked in **May 2025**. The **fewest of all (potential) phishing URLs** were identified in **December 2024**, while the **fewest verified phishing URLs** were identified in **September 2025**.

History of Phishing URLs

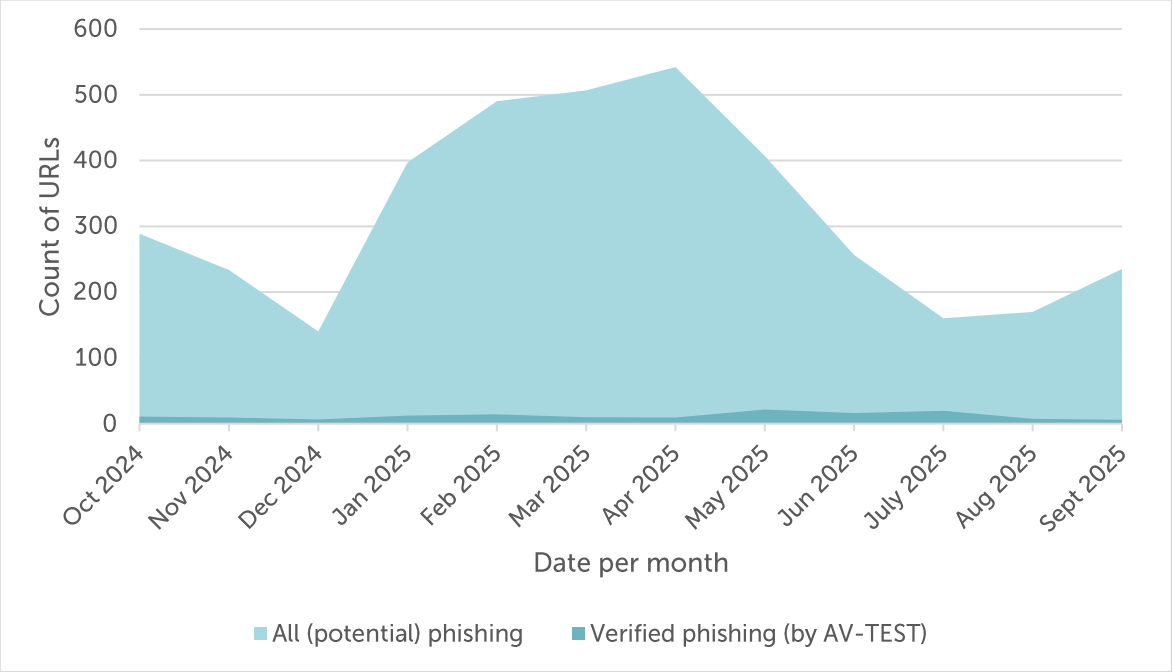

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **October 2024 to September 2025***

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
Oct 2024	288,900		3.74%	10,816	
Nov 2024	233,486	-19.18%	4.07%	9,493	-12.23%
Dec 2024	140,303	-39.91%	4.56%	6,403	-32.55%
Jan 2025	397,214	+183.11%	3.03%	12,043	+88.08%
Feb 2025	490,080	+23.38%	2.85%	13,972	+16.02%
Mar 2025	506,671	+3.39%	1.96%	9,939	-28.86%
Apr 2025	542,081	+6.99%	1.72%	9,297	-6.46%
May 2025	406,756	-24.96%	5.28%	21,492	+131.17%
Jun 2025	256,529	-36.93%	6.20%	15,907	-25.99%
July 2025	160,240	-37.54%	12.27%	19,656	+23.57%
Aug 2025	169,908	+6.03%	4.36%	7,414	-62.28%
Sept 2025	235,013	+38.32%	2.57%	6,036	-18.59%
Total	3,827,181		3.72%	142,468	

*Table 3: Aggregate Trends - **History of All (Potential) and Verified Phishing URLs** - **October 2024 to September 2025***

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month		Verified phishing	Month
High	542,081	Apr 2025		21,492	May 2025
Low	140,303	Dec 2024		6,342	Sept 2025
Average	318,932			11,872	

*Table 4: Aggregate Trends - **Key Figures of All (Potential) and Verified Phishing URLs** - **October 2024 to September 2025***

Commentary

The aggregate dataset covering October 2024 to September 2025 identified a total of 3,827,181 phishing URLs with ASNs, of which 142,468 were verified. Potential phishing URLs increased steadily from January through April 2025, before falling sharply in May and continuing to decline through June and July. August 2025 showed a modest recovery, followed by a substantial rebound in overall phishing activity in September 2025, even as verified phishing reached a new low. Despite this recovery, levels remained below the April peak. The highest number of potential phishing URLs was recorded in April 2025, while verified phishing URLs peaked in May 2025. At the lower end, potential phishing reached its minimum in December 2024, while **verified phishing** was lowest **in September 2025, marking a new record low** for the reporting period. On average across the reporting period, monthly values averaged around 318,932 potential phishing URLs and 11,872 verified phishing URLs.

The **distribution between potential and verified phishing shifted notably** through mid-to-late 2025. On average, verified phishing represented about 3.72% of all suspected phishing URLs, but this share fluctuated dramatically, rising to over 12% in July 2025 before collapsing to just 4.36% in August and falling further to 2.57% in September. This sustained decline highlights how the late summer period reduced not only total verified volumes but also the proportion of cases confirmed as phishing, reaching the lowest verification rate in the entire reporting period.

As in previous months, **potential phishing displays seasonal and campaign-driven dynamics**, with peaks clustering in the first quarter of 2025. Verified phishing remains far more volatile, reflecting the uneven effectiveness of different campaigns and the sharp fluctuations between May's spike and September's record low. Interestingly, in some low-volume months such as December 2024, verified phishing accounted for a larger share of suspected URLs (4.56%), suggesting a shift toward more targeted campaigns during quieter periods.

By contrast**, September 2025** diverged sharply from this pattern, with **potential phishing rebounding substantially while verified cases plummeted to their lowest point**, resulting in the smallest verification share (2.57%) observed. This suggests that while overall phishing activity intensified in September, the campaigns may have been less sophisticated or more rapidly detected and neutralised, leading to lower confirmation rates. The **contrasting trends** – rising potential phishing alongside falling verified phishing – **indicate a possible shift in attacker tactics or improved defensive measures during this period**.

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 **8,956,411 URLs with ASNs** were identified among the Top50 ASNs in September 2025, **of which:**

- **7,897,819 URLs** could be **verified as malware**,
- **533,887 URLs** have been **classified as PUA**, and
- **524,705 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
June - Dec 2024	3,684,553	87.03%	217,343	5.13%	331,888	7.84%	4,233,784
Jan 2025	427,507	87.13%	27,240	5.55%	35,902	7.32%	490,649
Feb 2025	462,960	87.11%	28,352	5.33%	40,141	7.55%	531,453
Mar 2025	422,319	88.96%	18,240	3.84%	34,148	7.19%	474,707
Apr 2025	343,056	91.93%	18,154	4.86%	11,971	3.21%	373,181
May 2025	337,196	92.09%	19,209	5.25%	9,767	2.67%	366,172
Jun 2025	494,633	88.07%	52,762	9.39%	14,233	2.53%	561,628
July 2025	520,073	81.60%	104,899	16.46%	12,383	1.94%	637,355
Aug 2025	547,454	94.97%	19,470	3.37%	10,600	1.84%	577,524
Sept 2025	658,068	92.69%	28,218	3.97%	23,672	3.33%	709,958
Total	7,897,819	88.18%	533,887	5.96%	524,705	5.86%	8,956,411

*Table 5: Aggregate Trends - **Aggregated Share of Top 50 ASNs** - **June 2024 to September 2025***

Commentary

The aggregate dataset for the Top 50 ASNs covering June 2024 to September 2025 identified a total of 8,956,411 malicious URLs. Of these, 7,897,819 were linked to malware, 533,887 to potentially unwanted applications (PUAs), and 524,705 to 'other' content. Malware remained the overwhelming majority at 88.18%, but the volatility of PUAs was again evident. After surging to a record 104,899 entries in July 2025 (16.46% of the monthly total), PUAs collapsed in August to 19,470 (3.37%), before recovering modestly to 28,218 (3.97%) in September 2025. This recovery remained far below the July peak. Malware maintained its dominance at 92.69% in September, down slightly from August's 94.97%, as both PUAs and 'other' content increased their shares.

While malware continues to dominate ASN-related threats, the **sharp mid-2025 swings in PUAs** highlight how attacker strategies can **shift rapidly** and on a large scale. The July spike suggests a period of concentrated PUA distribution, possibly linked to bundling with popular downloads or large-scale adware campaigns, while **the August decline and September's modest recovery show how volatile such campaigns can be**. 'Other' categories showed increased activity in September, rising to 23,672 (3.33%), the highest share since early 2025, suggesting attackers may be diversifying their tactics beyond **malware and PUAs**.

In retrospect, **July 2025 stands out as an anomaly**, showing how a sudden surge in PUAs can temporarily disrupt the distribution of threats. The **return to malware dominance in August 2025 (nearly 95%)** and the stabilisation in September 2025 (92.69%) suggest that the PUA surge was short-lived and attackers have largely reverted to established malware strategies, though with slightly more diversification into 'other' categories than seen in August.

Network operators are encouraged to request further details for their assigned ASNs to better assess exposure and take timely countermeasures.

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.