topDNS Report: Monthly Analysis for ISPs

An initiative by eco – Association of the Internet Industry in collaboration with AV-TEST

November 2025

Contents

Report Summary

This report is the eleventh 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 October 2025 include:

- **Overall malicious URL trends showed dramatic escalation across all categories in October 2025.**
  Malware URLs surged to 979,973 (+51.29% vs. September), reaching a new peak – the highest level in the entire reporting period – and representing 97% of all malicious URLs. Potentially unwanted applications (PUAs) fell to 15,734 (-42.24% compared to September's 27,242), marking the lowest point in the reporting period and representing just 2% of total malicious URLs. 'Other' malicious content decreased to 15,728 (-32.41%), dropping to 1% of the total. The distribution shifted dramatically toward malware dominance at 97%, while PUAs and 'other' content each accounted for only 1-2%, representing the most concentrated malware focus observed during the reporting period. October 2025 now holds the peak record for malware (979,973), while historical peaks for PUAs (July 2025: 105,835) and 'other' content (November 2024: 62,622) remain from earlier periods.

- **Phishing activity in October 2025 showed a divergence between potential phishing and verified phishing.**
  Potential phishing URLs decreased to 161,406 (-31.32% compared to September's 235,013), falling below the 'all (potential) phishing' average of 308,307. Verified phishing URLs, however, rose to 8,662 (+43.51% compared to September's 6,036), re-bounding from September’s historic low, but remaining well below the verified phish-ing average of 11,693. The share of verified phishing within potential phishing in-creased to 5.37%, up from 2.57% in September, suggesting improved detection or a shift in threat actor tactics. April 2025 continues to represent the peak for potential phishing URLs (542,081), while May 2025 holds the peak for verified phishing (21,492).

- **This October surge in verified phishing, following two months of historic lows, suggests renewed threat actor activity or changing attack patterns.**
  Despite remaining approximately 27% below the reporting-period average, the 43.51% month-over-month increase marks a notable reversal of the downward trend observed in August and September. The fluctuation between May 2025's peak (21,492) and

September 2025's trough (6,036) highlights the volatility of phishing campaigns during this reporting period.

- **In October 2025, the Top 50 ASNs accounted for 936,206 malicious URLs, a significant increase compared to September 2025's 709,958.** This included 907,850 malware (96.97%), 15,095 PUAs (1.61%), and 13,261 'other' content (1.42%). The increase was almost entirely driven by malware, which rose by more than 249,000 URLs month-over-month, while PUAs dropped to their lowest level in the reporting period. Across the entire reporting period from June 2024 to October 2025, the Top 50 ASNs generated 9,892,617 URLs in total, including 8,805,669 malware (89.01%), 548,982 PUAs (5.55%), and 537,966 'other' content (5.44%). Malware's share within the Top 50 ASNs reached an unprecedented 96.97% in October, reflecting the broader trend of extreme malware concentration observed across all metrics this month.

This is our sixth 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 **6,761,964 malicious URLs with ASNs** were identified in the period November 2024 to October 2025, **of which:**

- **6,035,732 URLs** could be **verified as malware**,
- **393,061 URLs** have been **classified as PUA**, and
- **333,171 URLs** as **other**.

The **highest number of malicious URLs for malware** was identified in **October 2025**, representing a **new record that surpassed the previous peak of November 2024**. Furthermore, **PUAs peaked in July 2025,** before **collapsing dramatically in August 2025** and **reaching their lowest point in October 2025**. In addition, **'other' content peaked in November 2024** and **reached its lowest level in May 2025**. The **lowest level for malware was recorded in December 2024**.

In the latest month, October 2025, the **distribution shifted to unprecedented malware dominance**, with malware accounting for 97% of all malicious URLs, while PUAs represented just 2% and 'other' content only 1%. Unfortunately, this marks the most concentrated malware focus observed throughout the entire reporting period, departing significantly from the typical distribution seen in previous months.

Malicious URLs

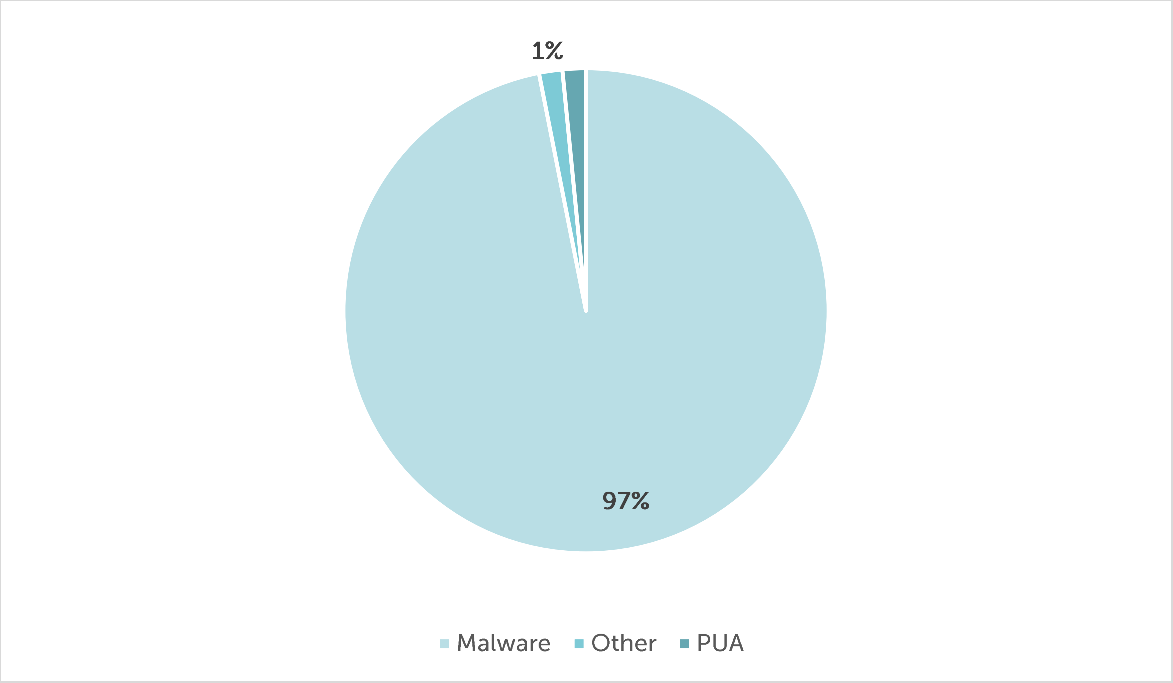

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **October 2025***

History of Malicious URLs

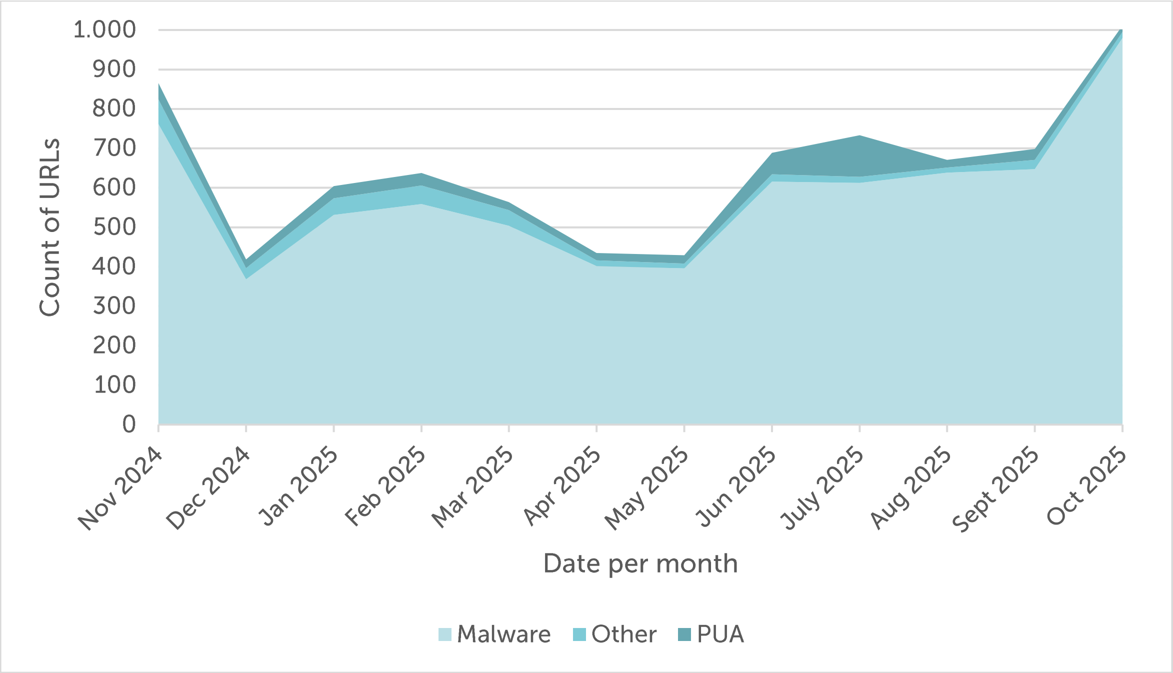

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **October 2024 to October 2025***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
Nov 2024	761,550		41,235		62,622	
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%
Oct 2025	979,973	+51.29%	15,734	-42.24%	15,728	-32.41%
Total	6,035,732		393,061		333,171	

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

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Change
High	979,973	Oct 2025	105,835	Jul 2025	62,622	Nov 2024
Low	368,246	Dec 2024	15,734	Oct 2025	12,011	May 2025
Average	502,978		32,755		27,643	

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

Commentary

The aggregate dataset covering November 2024 to October 2025 identified a total of 6,761,964 malicious URLs with ASNs, of which 6,035,732 were verified as malware, 393,061 classified as potentially unwanted applications (PUAs), and 333,171 as 'other' content. Despite October 2025's record-breaking monthly figures, the **total number of malicious URLs decreased** from 9,892,617 in the previous reporting period due to the rotation of months as the reporting window shifted forward.

The **highest number of malware URLs was recorded in October 2025 at 979,973,** representing **a new peak** that surpassed the previous high of 761,550 in November 2024. PUAs peaked in July 2025 at 105,835 URLs, before collapsing in August 2025 to just 19,551 and **reaching a new low in October 2025 at 15,734**. At the lower end, the minimum values occurred in December 2024 for malware (368,246), October 2025 for PUAs (15,734), and May 2025 for 'other' content (12,011). On average across the reporting period, monthly figures amounted to approximately 502,978 malware URLs, 32,755 PUAs, and 27,643 'other' URLs.

The dramatic surge in malware during October 2025 represents the **most significant monthly increase** observed throughout the entire reporting period, rising 51.29% from September's already elevated levels. Meanwhile, PUAs continued their downward trajectory, falling below their April 2025 low to establish a new minimum at 15,734 – a 42.24% decline from September. In October 2025, the distribution **shifted dramatically toward malware dominance**, with **malware accounting for 97% of all malicious URLs**, while PUAs represented just 2% and 'other' content only 1% – the **most concentrated malware focus** observed throughout the entire reporting period.

As Table 2 highlights, malware activity ranged from a **new high of 979,973 URLs in October 2025** to a **low of 368,246 in December 2024** – a span of over 611,000 URLs. PUAs fluctuated dramatically, from a **new low of 15,734 in October 2025** to their **peak of 105,835 in July 2025**, while 'other' content reached 62,622 in November 2024 but fell to 12,011 in May 2025. These figures **confirm malware's overwhelming dominance in absolute terms**, while PUAs and 'other' categories continue to show volatility, though both declined significantly in October. Notably, the October 2025 malware surge appears to have absorbed activity that might otherwise have been distributed across other categories, resulting in an **unprecedented concentration of threat activity** within the malware classification.

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 **3,699,687 phishing URLs with ASNs** were identified in the period from November 2024 to October 2025, **of which 140,314 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. **October 2025 reversed this pattern**, with potential phishing declining significantly while verified phishing rebounded moderately.

Between November 2024 and October 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 **fewer verified phishing URLs** were identified in **September 2025**, before **rising again in October 2025.**

History of Phishing URLs

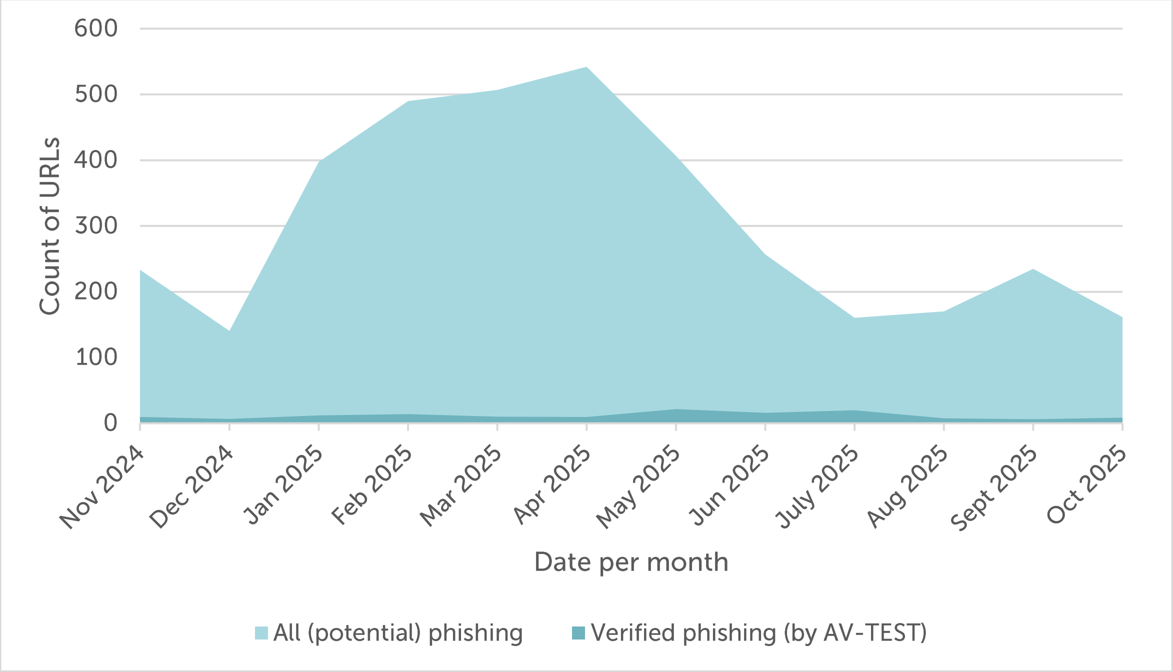

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **November 2024 to October 2025***

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
Nov 2024	233,486		4.07%	9,493	
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%
Oct 2025	161,406	-31.32%	5.37%	8,662	+43.51%
Total	3,699,687		3.79%	140,314	

*Table 3: Aggregate Trends - **History of All (Potential) and Verified Phishing URLs** - **November 2024 to October 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	308,307			11,693	

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

Commentary

The aggregated dataset covering November 2024 to October 2025 identified a total of 3,699,687 all (potential) phishing URLs and 140,314 verified phishing URLs. The volume of all (potential) phishing URLs showed considerable volatility throughout the period. A **dramatic spike in January 2025** (+183.11%), following December 2024's sharp decline, continued increases through February, March, and April 2025, peaking at 542,081 URLs in April, before declining.

July 2025 saw a further drop to 160,240 URLs, followed by modest increases in August and September 2025, before declining again by 31.32% in October 2025 to 161,406 URLs. Verified phishing URLs demonstrated even greater fluctuation, peaking in May 2025 at 21,492 URLs, then declining substantially through June and August 2025, reaching a **reporting-period low in September 2025** at 6,036 URLs, before **rebounding sharply by 43.51% in October 2025 to 8,662 URLs**.

The share of verified phishing within all (potential) phishing URLs varied significantly across the reporting period. It ranged from a low of 1.72% in April 2025 to a high of 12.27% in July 2025. **October 2025** recorded a share of 5.37%, reflecting **improved detection rates** compared to September's 2.57%, though remaining above the reporting-period average of 3.79%. On average across the reporting period, monthly figures amounted to approximately 308,307 all (potential) phishing URLs and 11,693 verified phishing URLs.

The contrasting trends in October 2025 – declining potential phishing alongside rising verified phishing – suggest either improved detection capabilities or a shift in threat-actor tactics toward more sophisticated phishing campaigns that are more readily identified by verification systems.

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 **9,892,617 URLs with ASNs** were identified among the Top50 ASNs in October 2025, **of which:**

- **8,805,669 URLs** could be **verified as malware**,
- **548,982 URLs** have been **classified as PUA**, and
- **537,966 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
Oct 2025	907,850	96.97%	15,095	1.61%	13,261	1.42%	936,206
Total	8,805,669	89.01%	548,982	5.55%	537,966	5.44%	9,892,617

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

Commentary

The aggregate dataset for the Top 50 ASNs covering June 2024 to October 2025 identified a total of 9,892,617 malicious URLs. Of these, 8,805,669 were linked to malware, 548,982 to potentially unwanted applications (PUAs), and 537,966 to 'other' content. Malware remained the overwhelming majority at 89.01%, while PUAs and 'other' content accounted for 5.55% and 5.44%, respectively.

While malware dominance has been consistent, the **volatility of PUAs in mid-to-late 2025 was particularly striking**. After surging to a record 104,899 entries in July 2025 (16.46% of the monthly total), PUAs fell sharply in August to 19,470 (3.37%), recovered modestly to 28,218 (3.97%) in September, before collapsing to just 15,095 (1.61%) in October – the lowest share recorded in the entire dataset. This pattern illustrates the highly dynamic nature of PUA campaigns, which can spike dramatically for short periods before subsiding just as rapidly.

Malware activity remained strong throughout the period, with **October 2025 showing a peak of 907,850 entries** (96.97% of the monthly total) – the highest malware concentration in the dataset. The overall total for October reached 936,206 malicious URLs. This near-total malware dominance in October, combined with the collapse of PUAs to historic lows, suggests that attackers have consolidated around traditional, reliable malware distribution strategies following the experimental PUA surge in mid-2025. 'Other' content showed some diversification in September (23,672, 3.33%), but declined sharply to 13,261 (1.42%) in October, indicating that such diversification tactics remain limited and inconsistent.

In summary, while malware continues to be the primary driver of ASN-based threats, the **pronounced swings in PUAs** – particularly the July 2025 spike followed by October's historic low – underscore **how rapidly attacker strategies can shift**. Network operators are encouraged to closely monitor both PUA and 'other' activity within their ASNs to anticipate potential surges and implement timely mitigation measures.

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.