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 2025

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

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

- **Overall, a stabilisation in malware and 'other' malicious content was recorded, while PUAs showed a major increase compared to the previous month.**
  In July 2025, malware URLs edged down slightly to 612,196 (-0.53% compared to June), while potentially unwanted applications (PUAs) almost doubled to 105,835 (+95.24%), setting a new reporting-period high. 'Other' content decreased to 15,686 (-17.19%). In addition, malware continued to dominate overall, representing 84% of malicious URLs, with PUAs increasing their share to 14% and 'other' content making up 2%. August 2024 remains the peak month for malware and 'other' content, while July 2025 now represents the highest point for PUAs.

- **A general decline in the number of unique URLs being used for potential phishing was also recorded.**
  Potential phishing URLs fell sharply to 160,240 in July 2025 (-37.54% compared to June), marking the lowest value of the reporting period and significantly below the average of 336,745. The highest number of potential phishing URLs continues to be April 2025 (542,081), while the lowest remains in December 2024 (140,303).

- **An increase in the number of unique URLs used for verified phishing was observed.**
  Verified phishing URLs rose to 19,656 in July 2025 (+23.57% compared to June), remaining above the reporting-period average of 13,016. The highest level of verified phishing URLs continues to be August 2024 (20,826), while the lowest was September 2024 (6,342). The July increase highlights once again the volatility of verified phishing activity, with periodic spikes despite the overall decline in potential phishing URLs.

  At the same time, the share of verified phishing within total phishing activity shifted noticeably, underlining the changing composition and unpredictability of attacker behavior.

- **The aggregated Share of Top50 ASNs.**
  In July 2025, the Top 50 ASNs accounted for 637,355 malicious URLs: 520,073 malware (81.60%), 104,899 PUAs (16.46%), and 12,383 'other' content (1.94%). This total represents a further increase compared to June's 561,628, with PUAs reaching their highest monthly volume in the ASN dataset. Across June 2024 to July 2025, the Top 50 ASNs contributed 7,668,929 URLs in total, including 6,692,297 malware, 486,199 PUAs, and 490,433 as 'other' content. Malware remains the dominant category, but the rising share of PUAs in mid-2025 indicates an important shift in the composition of malicious activity.

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 **7,873,797 malicious URLs with ASNs** were identified in the period August 2024 to July 2025, **of which:**

- **6,962,328 URLs** could be **verified as malware**,
- **456,595 URLs** have been **classified as PUA**, and
- **454,874 URLs** as **other**.

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

Malicious URLs

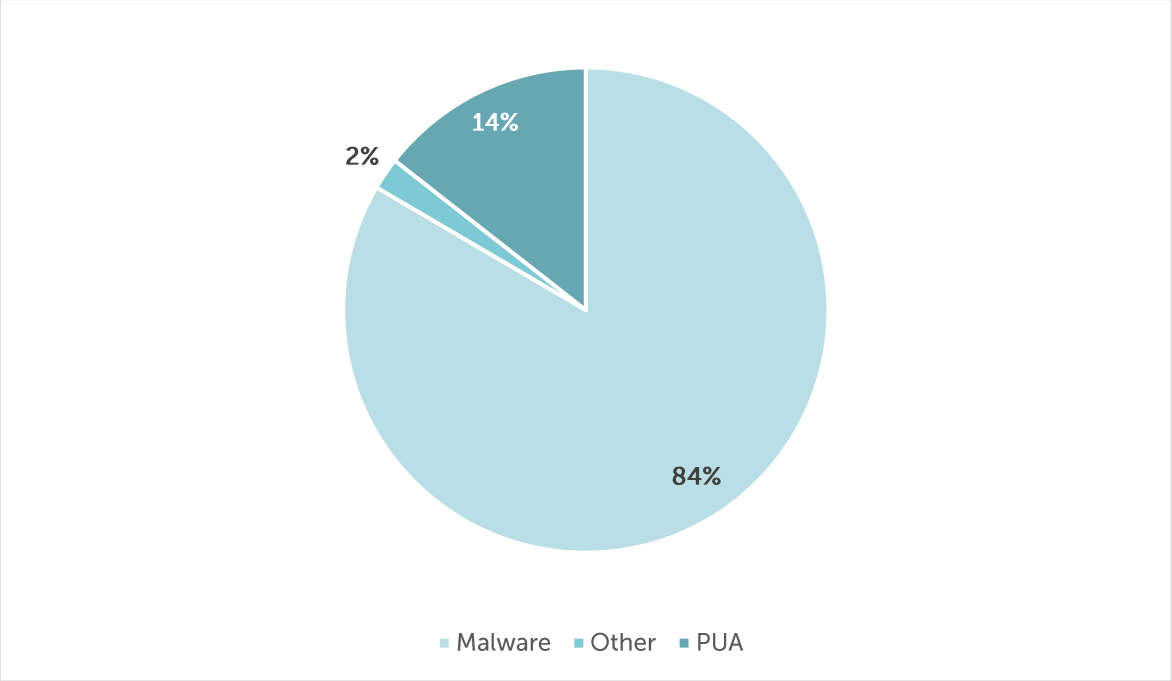

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **July 2025***

History of Malicious URLs

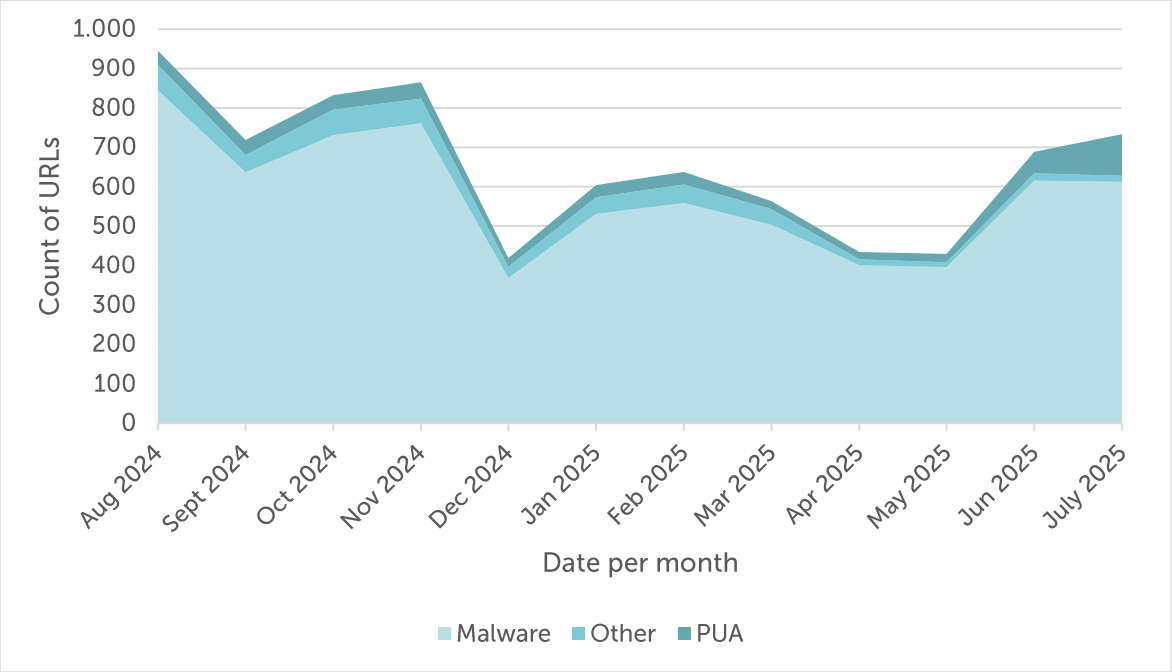

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **August 2024 to July 2025***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
Aug 2024	844,986		35,701		64,877	
Sept 2024	636,693	-24.65%	37,805	+5.89%	44,214	-31.58%
Oct 2024	730,895	+14.80%	36,821	-2.60%	64,882	+46.75%
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%
Total	**6,962,328**		**456,595**		**454,874**	

*Table 1: Aggregate Malware Trends - **History of Malicious URLs** - **August 2024 to July 2025***

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Change
High	844,986	Aug 2024	105,835	Jul 2025	64,877	Aug 2024
Low	368,246	Dec 2024	18,739	Apr 2025	12,011	May 2025
Average	**580,194**		**38,050**		**37,906**	

*Table 2: Aggregate Trends - **Key Figures of Malicious URLs** - **August 2024 to July 2025***

Commentary

The aggregate dataset covering August 2024 to July 2025 identified a total of 7,873,797 malicious URLs with ASNs, of which 6,962,328 were verified as malware, 456,595 classified as potentially unwanted applications (PUAs), and 454,874 as 'other' content. **The highest numbers of malware and 'other' URLs** were recorded in August 2024, while **PUAs peaked more recently in July 2025**, reaching 105,835 URLs, which is almost double the June figure of 54,207. 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 580,200 malware URLs, 38,100 PUAs, and 37,900 'other' URLs.

The highs for malware and 'other' content remain unchanged compared to earlier reports, but the lows have shifted again, reflecting the volatility of the smaller categories. While malware remains by far the dominant category, the **sharp rise in PUAs in mid-2025** – reaching 14% of all malicious URLs in July, a much larger share than in earlier months – **signals a change in the composition of malicious activity** and warrants closer monitoring going forward. By July 2025, PUAs had overtaken 'other' threats significantly, which may suggest a **strategic attacker shift toward distributing potentially unwanted applications** rather than miscellaneous threats.

Malware URL activity is **cyclical with deep troughs followed by strong rebounds**, suggesting campaign-driven bursts. 'Other' threats are **inconsistent and unstable**, with large spikes and sudden declines, pointing to irregular attack campaigns, improved filtering or attacker focus shifting elsewhere.

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 **4,040,935 phishing URLs with ASNs** were identified in the period from August 2024 to July 2025, **of which 156,186 URLs** could be **verified**.

There was a further increase in January, February, March and April 2025, with a small dip appearing in May 2025 and a sharper decline in June and July 2025.

Between June 2024 and April 2025, the **highest number of phishing URLs** was identified in **April 2025**, while **verified phishing URLs** peaked in **July 2024**, with a **more recent high in May 2025**. The **fewest of all (potential) phishing URLs** were identified in **December 2024**, while the **fewest of verified phishing URLs** were identified in **July 2025**, and the **fewest of verified phishing URLs** were identified in **September 2024**.

History of Phishing URLs

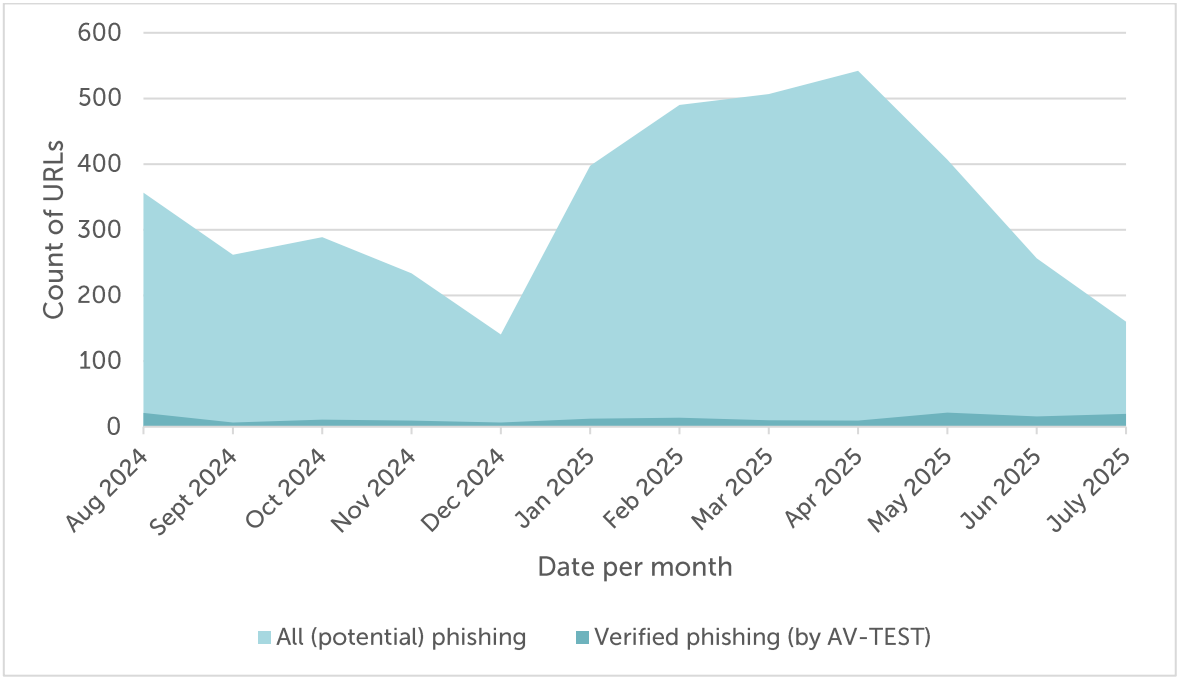

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **August 2024 to July 2025***

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
Aug 2024	356,659		5.84%	20,826	
Sept 2024	262,016	-26.54%	2.42%	6,342	-69.55%
Oct 2024	288,900	+10.26%	3.74%	10,816	+70.55%
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%
Total	**4,040,935**			**156,186**	

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

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month	Share	Verified phishing	Month
High	542,081	Apr 2025		20,826	Aug 2024
Low	140,303	Dec 2024		6,342	Sep 2024
Average	**336,745**			**13,016**	

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

Commentary

The aggregate dataset covering August 2024 to July 2025 identified a total of 4,040,935 phishing URLs with ASNs, of which 156,186 were verified. Potential phishing URLs increased steadily from January through April 2025, before dipping in May and then falling more sharply in June and July 2025. The highest number of potential phishing URLs was recorded in April 2025, while verified phishing URLs peaked earlier in July 2024, with a more recent high in May 2025. At the lower end, potential phishing reached its minimum in July 2025, as well as verified phishing URLs in September 2024. On average across the reporting period, monthly values equated to around 324,800 potential phishing URLs and 13,000 verified phishing URLs.

The **highs for phishing activity remain unchanged** compared to earlier reports, but **the lows have shifted** again, confirming volatility in both categories. While potential phishing volumes are consistently far larger, verified phishing continues to show sudden spikes, indicating the presence of focused campaigns. Notably, in July 2025, verified phishing made up 12.27% of all potential phishing URLs, which was the **highest share of the reporting period**. This highlights that even during declines in overall activity, a larger proportion of cases may still be confirmed.

As analysed in previous reports, potential phishing is **campaign-driven**, showing large seasonal swings. **Peaks** often **cluster around the first quarter**, which may reflect attackers exploiting post-holiday or tax-related activities. **Verified phishing** shows **sharper swings than total phishing**, suggesting that **some campaigns were more effectively validated as true phishing attacks** (e.g., May–July 2025).

Interestingly, the **share of verified phishing increased in periods of overall phishing decline** (e.g., Dec 2024, May–July 2025). This pattern suggests that during low-volume months, a **larger proportion of suspected phishing URLs were confirmed as real**, possibly indicating atackers may be shifting strategy towards more targeted, higher-quality phishing campaigns.

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 **7,031,574 URLs with ASNs** were identified among the Top50 ASNs in July 2025, **of which:**

- **6,172,224 URLs** could be **verified as malware**,
- **381,300 URLs** have been **classified as PUA**, and
- **478,050 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
Total	**6,692,297**		**486,199**		**490,433**		**7,668,929**

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

Commentary

The aggregate dataset for the Top 50 ASNs covering August 2024 to July 2025 identified a total of 7,668,929 malicious URLs. Of these, 6,692,297 were linked to malware, 486,199 to potentially unwanted applications (PUAs), and 490,433 to 'other' content. Malware continued to represent the overwhelming majority of malicious activity at around 87%, but PUAs showed a notable rise in mid-2025, reaching their highest monthly value in July with 104,899 entries. The consecutive increases in June and July – with PUAs nearly doubling month-on-month – lifted their share of the Top 50 ASN dataset from single digits to more than 16%, underlining a shift in the balance of threats.

While malware remains the dominant threat, the **growing share of PUAs** highlights how threat patterns are shifting and diversifying. July 2025 marks a **strategic shift**, with attackers focusing heavily on PUAs. This **could reflect changes in distribution tactics** (e.g., bundling with popular downloads or large-scale adware campaigns). 'Other' categories are being **phased out or effectively mitigated**, as attackers appear to favor malware and PUAs instead. This trend needs to be monitored in future reports.

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.