topDNS Report:
Monthly Analysis for ISPs

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

July 2025

Contents

Report Summary

This report is the seventh 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.

This is our second report to cover a full 12-month period. From now on, future editions will rotate across reporting months, always covering the previous 12 months. This will facilitate comparisons and highlight patterns more clearly in the future. This is an important next step for this report, as it will help to identify longer-term trends while this edition continues to demonstrate how the methodology captures the data.

Key highlights from the overall data in the month of June 2025 include:

- **Overall, an increase in malware, PUA and other malicious content was recorded in comparison to the previous month.**
  In June 2025, malware URLs rose sharply to 615,448 (+55.33% compared to May), recovering from the lows of April and May. Potentially unwanted applications (PUAs) surged to 54,207 (+154.43%), setting a new high for the reporting period, while 'other' content also increased to 18,942 (+57.71%). Malware continued to dominate, making up 89% of malicious URLs, with PUAs at 8% and 'other' content at 3%. July 2024 remains the peak month for malware and 'other' content, while June 2025 now represents the highest point for PUAs.

- **A general decline in the number of unique URLs being used for potential phishing was observed.**
  Potential phishing URLs dropped to 256,529 in June 2025 (–36.93% compared to May), continuing the downward trend after April's high of 542,081. Despite this decline, the June figure remained close to the reporting-period average of 360,693. The highest value continues to be April 2025, while the lowest was recorded in December 2024 with 140,303.

- **A decline in the number of unique URLs used for verified phishing was also observed.**
  Verified phishing URLs decreased to 15,907 in June 2025 (–25.99% compared to May), remaining just above the reporting-period average of 14,329. July 2024 still marks the highest value at 35,421, while the lowest continues to be September 2024, with 6,342. Despite the June downturn, verified phishing activity remains volatile, with significant spikes earlier in 2025.
- **The aggregated Share of Top50 ASNs.**
  In June 2025, the Top 50 ASNs accounted for 561,628 malicious URLs: 494,633 malware (88.07%), 52,762 PUAs (9.39%), and 14,233 'other' content (2.53%). This total represents a sharp increase compared to May's 366,172. Across the full reporting period from June 2024 to June 2025, the Top 50 ASNs contributed 7,031,574 URLs in total, including 6,172,224 malware, 381,300 PUAs, and 478,050 as 'other' content. Malware continues to account for the overwhelming majority of malicious activity on these networks.

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 **8,129,493 malicious URLs with ASNs** were identified in the period July 2024 to June 2025, **of which:**

- **7,209,790 URLs** could be **verified as malware**,
- **402,803 URLs** have been **classified as PUA**, and
- **516,900 URLs** as **other**.

The **most malicious URLs for malware and 'other' content** were identified in **July 2024**, while PUAs peaked more recently in June 2025. The **lowest numbers were recorded in December 2024 for malware,** in **April 2025 for PUAs**, and in **May 2025 for 'other' content**.

Malicious URLs

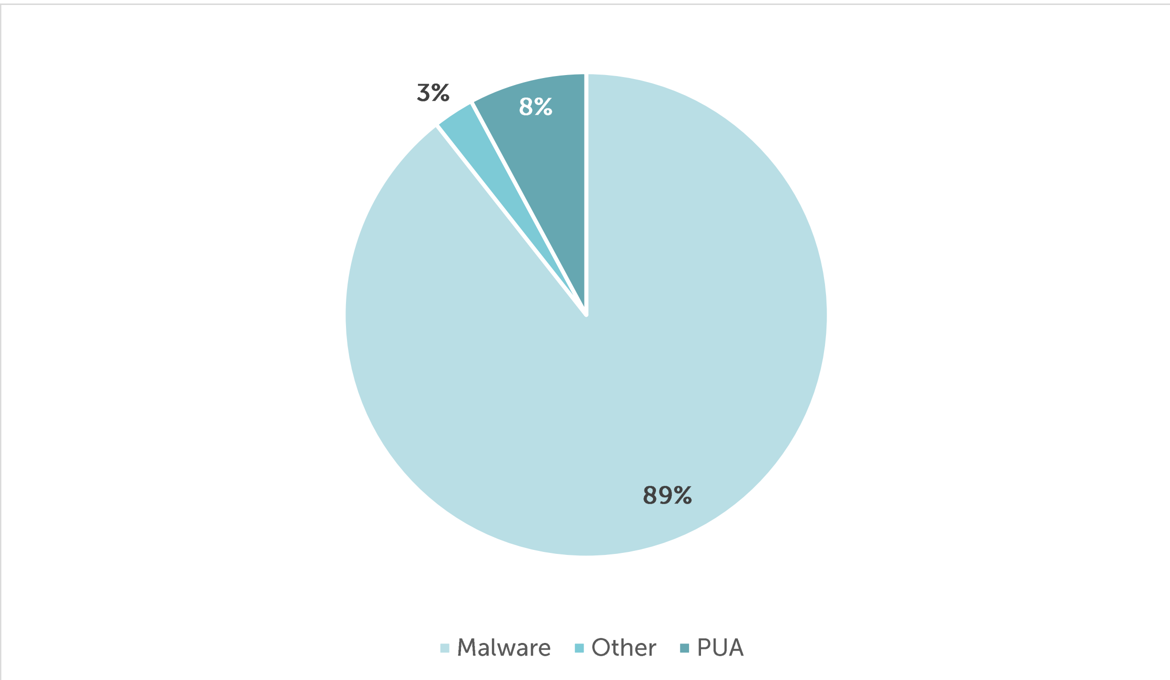

*Figure 1: Aggregate Malware Trends - **Malicious URLs - June 2025***

History of Malicious URLs

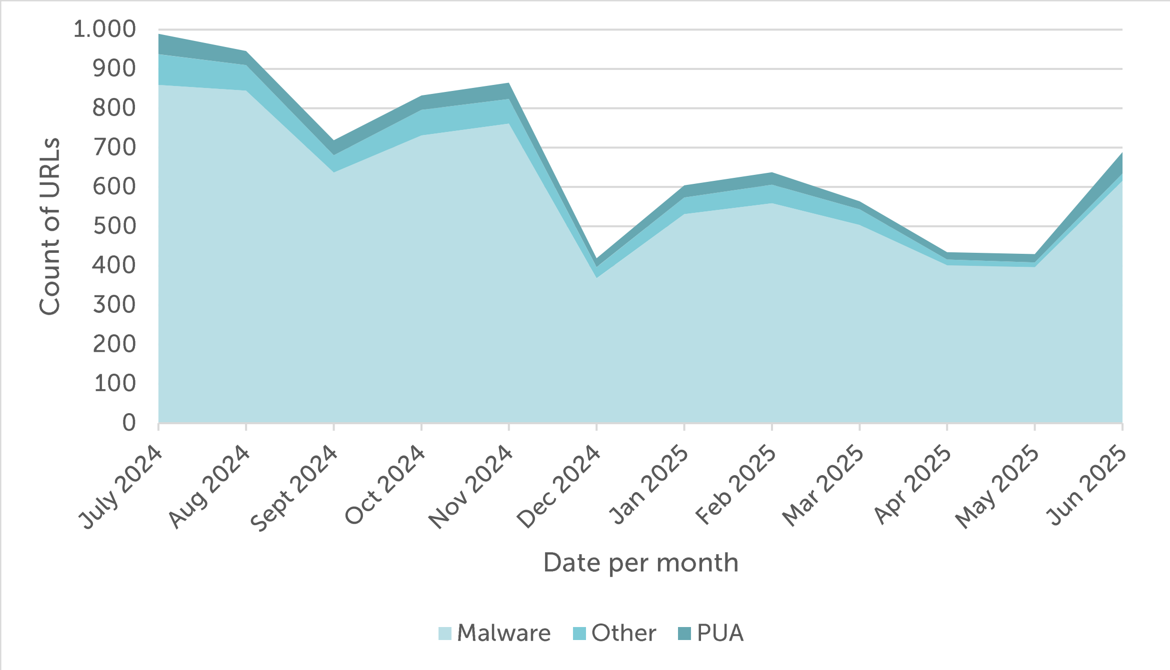

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **July 2024 to June 2025***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
July 2024	859,658		52,043		77,712	
Aug 2024	844,986	-1.71%	35,701	-31.40%	64,877	-16.52%
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%
Total	**7,209,790**		**402,803**		**516,900**	

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

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Change
High	859,658	July 2024	54,207	Jun 2025	77,712	July 2024
Low	368,246	Dec 2024	18,739	Apr 2025	12,011	May 2025
Average	**600,816**		**33,567**		**43,075**	

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

Commentary

The aggregate dataset covering July 2024 to June 2025 shows that malware continues to dominate malicious activity, with 7,209,790 URLs identified during the period, compared to 402,803 potentially unwanted applications (PUAs) and 516,900 'other' URLs. On average, this equates to 600,816 malware URLs, 33,567 PUAs, and 43,075 'other' URLs per month.

June 2025 was particularly significant, marking a **strong rebound across all categories** after the lows of April and May. Malware URLs rose sharply to 615,448 (+55.33%), while PUAs surged to 54,207 (+154.43%), reaching a new peak for the reporting period. 'Other' content also increased by 57.71% to 18,942 URLs. In proportional terms, malware continued to dominate with 89% of all malicious URLs, while PUAs accounted for 8% and 'other' URLs for 3%.

Looking at the **broader trends**, the highest levels of malicious URLs were recorded in July 2024 for malware and 'other' content, and in June 2025 for PUAs. The lowest volumes occurred in December 2024 for malware, April 2025 for PUAs, and May 2025 for 'other' content. These shifts underline not only the consistently high prevalence of malware, but also the relative growth of PUAs in 2025, which – while smaller in absolute terms – show the strongest upward trajectory.

Overall, the malware trend shows **high volatility**, suggesting periodic surges in malicious activity followed by steep declines. Despite occasional growth spurts, the overall PUA trend remains **less volatile than malware** but highly sensitive to isolated spikes. The dataset suggests **cyclical surges followed by sharp contractions**, likely tied to **campaign-based attacks** or seasonal factors.

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 **4,328,314 phishing URLs with ASNs** were identified in the period from July 2024 to June 2025, **of which 171,951 URLs** could be **verified**.

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

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**, and the **fewest of verified phishing URLs** were identified in **September 2024.**

History of Phishing URLs

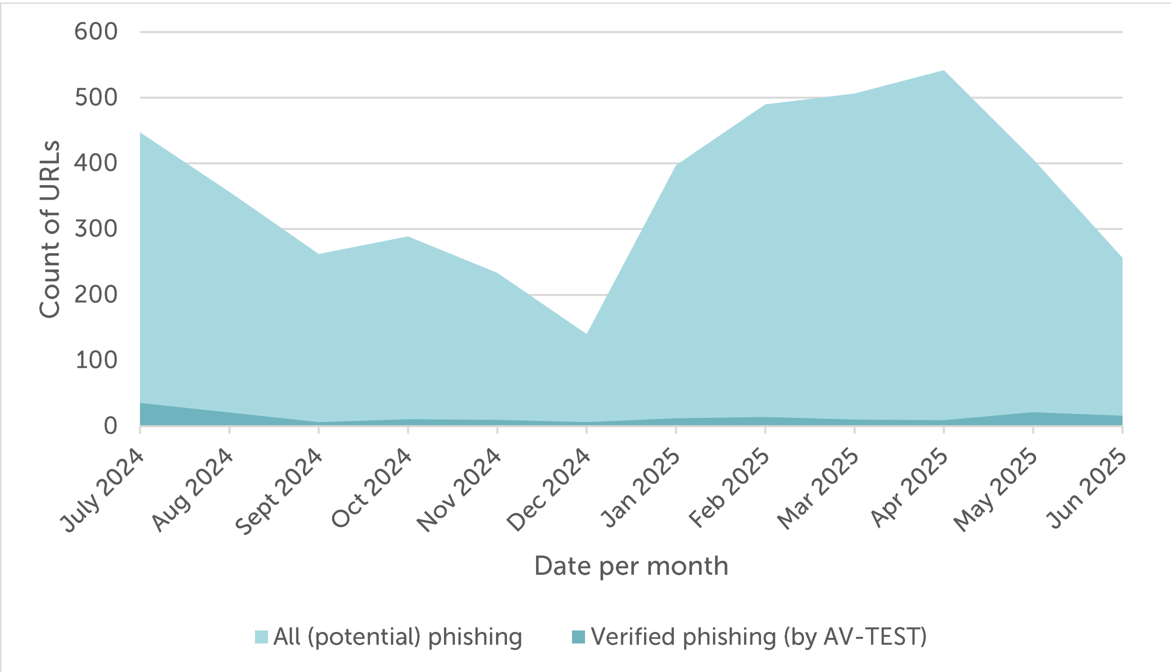

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **July 2024 to June 2025***

History of All (Potential) and verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
July 2024	447,619		7.91%	35,421	
Aug 2024	356,659	-20.32%	5.84%	20,826	-41.20%
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%
June 2025	256,529	-36.93%	6.20%	15,907	-25.99%
Total	**4,328,314**			**171,951**	

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

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month		Verified phishing	Month
High	542,081	Apr 2025		35,421	July 2024
Low	140,303	Dec 2024		6,342	Sep 2024
Average	**360,693**			**14,329**	

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

Commentary

The aggregate dataset covering July 2024 to June 2025 identified 4,328,314 phishing URLs with ASNs, of which 171,951 were verified. There was a **steady increase in potential phishing URLs from January to April 2025**, culminating in a peak of 542,081 URLs in April, followed by a **small dip in May and a sharper decline in June** to 256,529 (-36.93% compared to May). Despite this drop, the **June figure remained close to the reporting-period average** of 360,693 potential phishing URLs. These swings suggest that phishing activity is **campaign-driven**, with sudden spikes of large-scale distribution followed by quieter periods.

Verified phishing URLs peaked in July 2024 (35,421), with a more recent high in May 2025 (21,492). At the lower end, potential phishing URLs reached their minimum in December 2024 (140,303), while verified phishing URLs were lowest in September 2024 (6,342). On average across the reporting period, monthly values equated to around 360,693 potential phishing URLs and 14,329 verified phishing URLs. In June 2025, verified phishing also declined to 15,907 (-25.99% compared to May), remaining just above the reporting-period average. Overall, verified phishing exhibits **similar volatility** to total phishing but with **sharper fluctuations**.

This highlights the consistently greater scale of potential phishing compared to verified campaigns, but also the **volatility of attacker behaviour**, with sharp spikes in confirmed phishing activity. Interestingly, spikes in verified phishing (e.g., May 2025) did not always align with peaks in total phishing, indicating **targeted campaigns that generated fewer but more sophisticated attacks**. The sharp drop in late 2024 (Sept–Dec) followed by surges in early 2025 suggests **phishing campaigns may be timed around specific periods** (e.g., year-end shopping, tax season).

The dataset reflects **episodic, campaign-driven phishing activity** with inconsistent verification shares, highlighting challenges in detection and the adaptability of phishing tactics.

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 June 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
Total	**6,172,224**		**381,300**		**478,050**		**7,031,574**

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

Commentary

The aggregate data for the Top 50 ASNs between June 2024 and June 2025 shows a total of 7,031,574 malicious URLs, underscoring the concentration of malicious activity within a relatively small set of networks. Of these, 6,172,224 URLs (almost 88%) were linked to malware, while 381,300 were classified as potentially unwanted applications (PUAs) and 478,050 as 'other' content. Monthly distributions fluctuated, with malware consistently making up the overwhelming majority of malicious activity, followed by smaller shares of PUAs and 'other' content. Notably, June 2025 saw malware volumes recover from the April–May lows, while PUAs nearly doubled compared to the previous month, marking their highest share of the reporting period.

In June 2025 alone, the Top 50 ASNs accounted for 561,628 malicious URLs, including 494,633 malware (88.07%), 52,762 PUAs (9.39%), and 14,233 'other' content (2.53%). This represented a sharp increase compared to May's 366,172 URLs, underlining the scale and volatility of activity within these networks.

Across the full reporting period, malware continued to dominate, confirming its position as the most significant threat within the ASN landscape.

PUAs generally remains low but experienced **episodic surges**, likely tied to campaign-specific distribution. 'Other' content shows a **clear downward trend**, indicating either reduced attacker activity in this segment or improved blocking/filtering mechanisms. Peaks in total detections (e.g., June–Dec 2024 and June 2025) suggest that **attacker activity clusters around certain timeframes**, possibly linked to global events, campaigns, or exploit cycles.

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.