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

March 2025

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

This report is the third 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.

We also hope that future editions of the report will provide an opportunity to recognise good practice and highlight areas for improvement within the industry. Through these reports, we aim to identify effective factors, policies and processes, and provide the industry with evidence.

While we expect to provide much greater granularity and detail in future reports, this third edition of the topDNS Report focuses on higher-level, aggregated data from June2024 to February 2025. This higher-level approach has been taken for the third report to allow for further data collection and to gather feedback on what would be most helpful in future reports.

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

- **A further marginal increase in malware, PUA and other malicious URLs following a general decrease from June to December 2024.**
  February 2025 recorded a modest month-on-month rise in malicious URLs, with malware (+5.20%), PUA (+3.90%), and other harmful samples (+10.68%) all increasing slightly from January. February's totals – 559,089 for malware, 31,846 for potentially unwanted applications (PUAs), and 46,639 for other malicious URLs – all remained below the nine-month average for each category (641,427, 35,395 and 53,345 respectively). While the figures show some stabilisation after the sharp December to January recovery, July 2024 remained the peak month on record across all three categories.
- **A significant increase in the number of unique URLs being used for potential phishing.**
  The dataset reveals that potential phishing URLs updated by +23.38% compared to January 2025, from 397,214 to 490,080. This was the highest level recorded to date and is well above the nine-month average of 328,090 unique URLs. This figure is also well above the nine-month average of 328,090 unique URLs. The upward trend follows the sharp rebound in January after a low of 140,303 in December 2024, confirming renewed volatility in phishing activity.

- **A further rise in the number of unique URLs used for verified phishing attacks.**
  Verified phishing URLs rose by +16.02%, from 12,043 in January 2025 to 13,972 in February 2025. This remains below the record high of 35,421 in July 2024, but continues the upward trajectory observed since December 2024, when figures reached a low of 6,403. The February figure is closer to the nine-month average of 16,615 but does not yet surpass it, suggesting some ongoing fluctuation in verified phishing activity.
- **The aggregated Share of Top50 ASNs.**
  In February 2025, a total of 531,453 URLs were analysed. Of these, 462,960 were confirmed as malware (87.11%), 28,352 as potentially unwanted applications (5.33%), and 40,141 categorised as 'other' (7.55%). The proportions remained largely stable compared to January, with malware still accounting for nearly nine out of ten URLs. This consistency shows that while absolute volumes fluctuate month to month, the category distribution remains stable.

As these data collection efforts are just beginning, we are not attempting to draw any conclusions from the data at this time. We look forward to reviewing the data as patterns emerge over time. However, we can offer some initial insights into how the methodology captures the data, which will provide a basis for understanding this complex issue in the future.

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 **6,571,507 malicious URLs with ASNs** were identified in the period June 2024 to February 2025, **of which:**

- **5,772,847 URLs** could be **verified as malware**,
- **318,556 URLs** have been **classified as PUA**, and
- **480,105 URLs** as **other**.

Between June 2024 and February 2025, the **most malicious URLs for all three categories** were identified in **July 2024**. The **lowest number of malicious URLs in all three categories** was identified in **December 2024**.

Malicious URLs

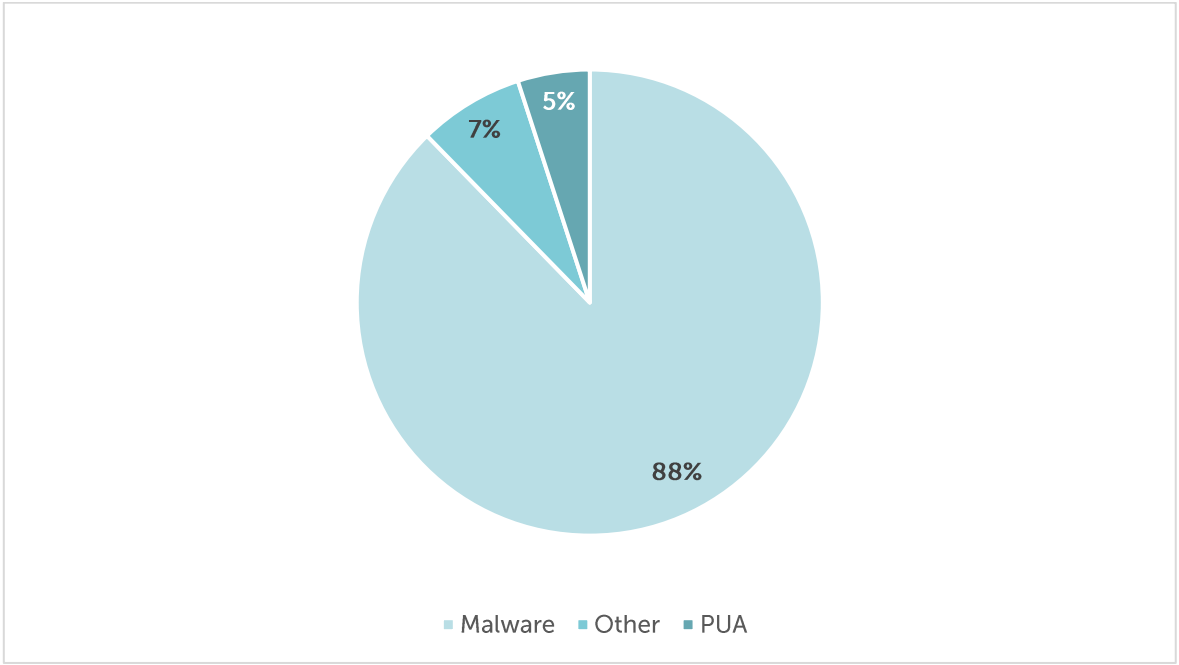

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **February 2025***

History of Malicious URLs

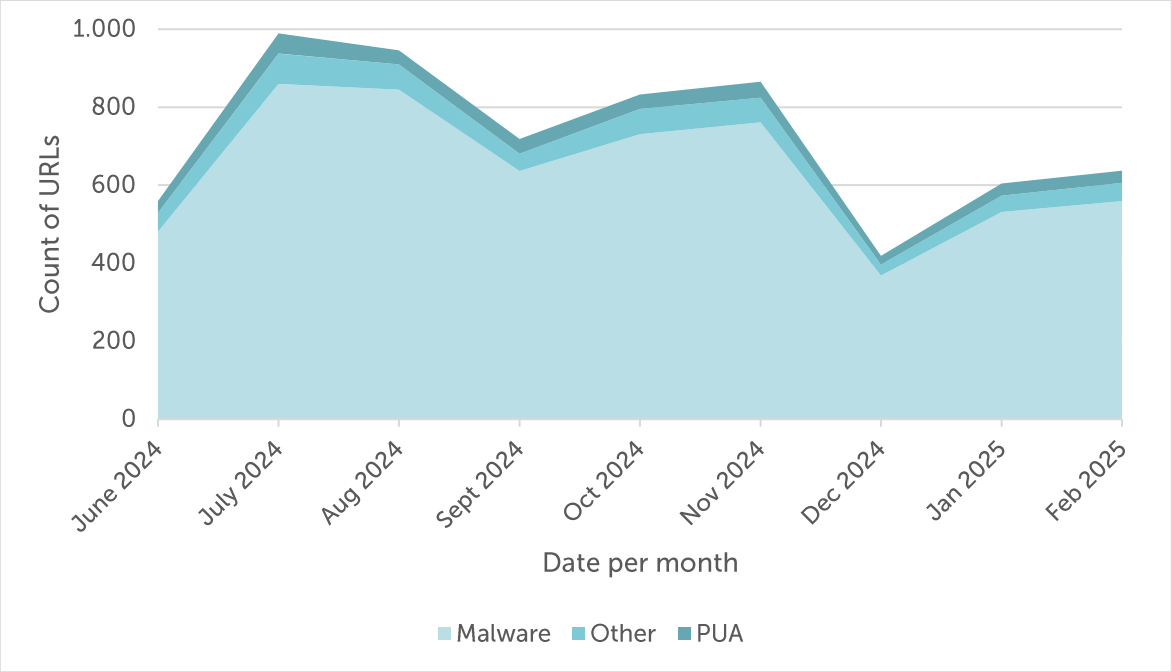

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **June 2024 to February 2025***

History of Malicious URLs

	Malware	Change	PUA	Change	Other	Change
June 2024	480,257		30,108		48,588	
July 2024	859,658	+79.00%	52,043	+72.85%	77,712	+59.94%
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%
Total	**5,772,847**		**318,556**		**480,105**	

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

Key Figures of Malicious URLs

	Malware	Month	PUA	Month	Other	Change
High	859,658	July 2024	52,043	July 2024	77,712	July 2024
Low	368,246	Dec 2024	22,345	Dec 2024	28,432	Dec 2024
Average	**641,427**		**35,395**		**53,345**	

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

Commentary

Following the sharp rebound in January 2025, February recorded a **modest increase in malicious distribution activity.** Compared to January, the number of unique URLs rose by 5.20% for malware, 3.90% for potentially unwanted applications (PUAs), and 10.68% for other harmful samples. Despite these month-on-month gains, February's totals remained below the nine-month averages for all three categories, indicating a period of relative stabilisation rather than continued acceleration.

As in earlier months, **July 2024 still stands out as the peak month on record**, with 859,658 URLs linked to malware, 52,043 to potentially unwanted applications (PUAs), and 77,712 to other threats. By contrast, **December 2024 saw the lowest levels**, with 368,246 URLs linked to malware, 22,345 to PUAs, and 28,432 to other threats. This reinforces the view that, while January and February show recovery from December's trough, **levels remain far from the record highs** observed mid-2024.

The broader dataset now spans nine months, offering a clearer picture of fluctuation. Malware distribution continues to show the greatest volatility, with sharper surges and drops compared to PUAs and other harmful URLs. February's figures suggest a post-rebound plateau, where overall malicious activity has stabilised but not yet returned to the peak intensities of the past year.

However. it's important to note that the dataset currently only covers nine months. This is not sufficient to establish a trend over time.

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 **2,952,809 phishing URLs with ASNs** were identified in the period from June 2024 to January 2025, **of which 149,541 URLs** could be **verified**.

There was a further increase in January and February, with **February marking a new peak** for potential phishing URLs.

Between June 2024 and February 2025, the **highest number of phishing URLs** (**both potential and verified)** were recorded in **July 2024**. The **fewest of all (potential) phishing URLs** were identified in **December 2024**, while the **fewest** of **verified phishing URLs** were identified in **September 2024.**

History of Phishing URLs

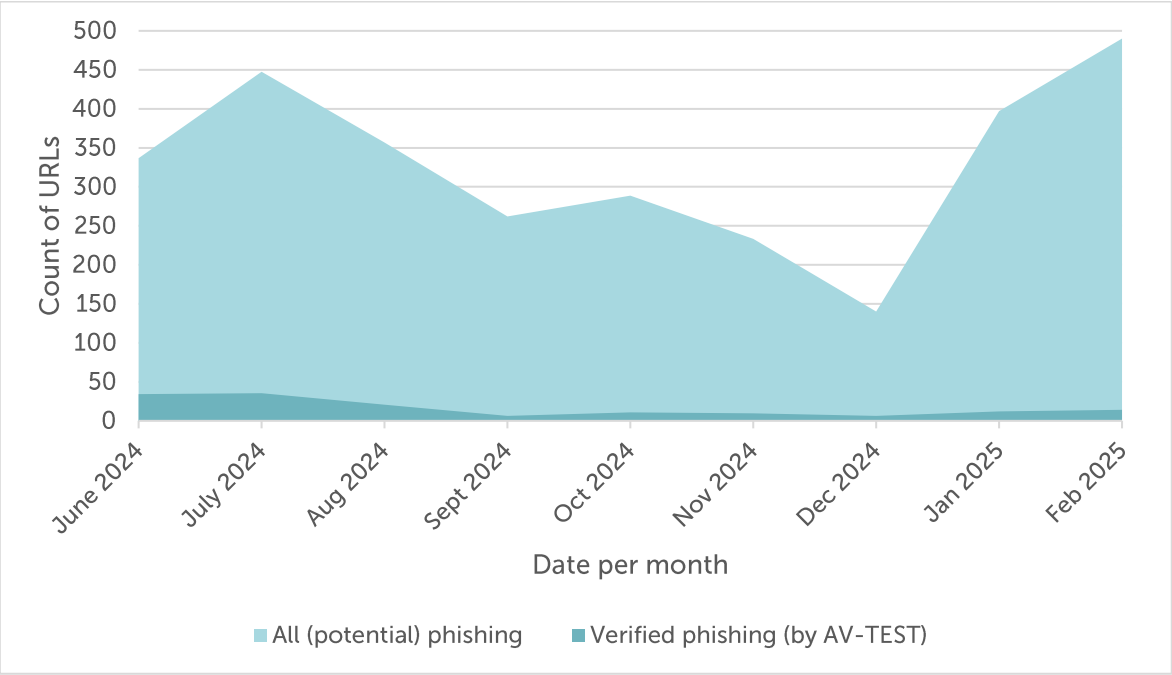

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **June 2024 to February 2025***

History of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Change	Share	Verified phishing	Change
June 2024	336,532		10.17%	34,225	
July 2024	447,619	+33.01%	7.91%	35,421	+3.49%
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%
Total	**2,952,809**			**149,541**	

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

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month		Verified phishing	Month
High	490,080	Feb 2025		35,421	July 2024
Low	140,303	Dec 2024		6,342	Sep 2024
Average	**328,090**			**16,616**	

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

Commentary

Following January's sharp rebound, February 2025 recorded a **further increase in potential phishing activity**, **setting a new high** for the dataset. The number of potential phishing-related URLs rose by 23.38%, climbing from 397,214 in January to 490,080 in February. This not only

extends the recovery from December's low of 140,303 but also surpasses the nine-month average of 328,090.

Despite this new peak, **July 2024 remains the highest month** on record for **verified phishing URLs** (35,421), while **February 2025 now represents the peak for potential phishing URLs** (490,080). The lowest activity continues to be observed in December 2024 for potential phishing (140,303) and in September 2024 for verified phishing (6,342). These figures highlight the volatility of phishing campaigns, which can drop to historic lows before surging rapidly above average levels.

Verified phishing activity also rose in February, with unique URLs increasing by 16.02%, from 12,043 in January to 13,972 in February 2025. While this continues the upward trajectory observed since December, the figure **remains below the nine-month average** of 16,615. Overall, the data suggests that phishing activity is in a phase of renewed expansion in early 2025, led by potential phishing URLs at unprecedented levels and supported by the gradual recovery of verified phishing URLs.

However. it's important to note that the dataset currently only covers nine months. This is not sufficient to establish a trend over time.

Chart: Aggregated Share of Top50 ASNs

This table provides an anonymized high-level overview of the 50 largest autonomous systems identified by their assigned autonomous system number (ASN).

A **total** of **5,255,886 URLs with ASNs** were identified among the Top50 ASNs in February 2025, **of which:**

- **4,575,020 URLs** could be **verified as malware**,
- **272,935 URLs** have been **classified as PUA**, and
- **407,931 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
Total	**4,575,020**		**272,935**		**407,931**		**5,255,886**

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

Commentary

In February 2025, a total of 531,453 URLs were analysed across the Top 50 ASNs. Of these, 462,960 were verified as malware, 28,352 as potentially unwanted applications (PUAs), and 40,141 were categorised as 'other'.

The **distribution of these categories remained consistent** with February 2025 and earlier periods: around 87% malware, 5% PUAs, and 8% other, underscoring the persistent dominance of malware across the top autonomous systems.

However, it is important to note that the dataset currently only covers nine months, which is not yet sufficient to establish a longer-term trend.

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.