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

January 2025

topDNS
An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

Report Summary

This report is the first 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 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 first edition of the topDNS Report focuses on higher-level, aggregated data from June to December 2024. This higher-level approach has been taken for the first 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 January 2025 include:

- **A general decrease in malware, PUA and other malware distribution, with a lower number of unique URLs associated with this activity.**
  Although the methodology identified spikes in the number of malicious URLs involved in distributing malware (+79.00%), potentially unwanted applications (+72.85%), and other harmful samples (+59.94%) in July compared to June, all three figures were lower in December. The figures for December were also lower than the seven-month average for each category. July 2024 was the highest month on record for all three categories, with 859,658 unique URLs identified for malware, 52,043 for potentially unwanted applications (PUAs) and 77,712 for other URLs. The lowest number of unique URLs identified for all three categories was in December 2024: 368,246 for malware, 22,345 for PUAs, and 28,432 for other URLs. The observed data shows that aggregate malware trends tend to be more volatile than aggregate phishing trends.
- **A general downward trend in the number of unique URLs being used for potential phishing, with a spike in July 2024.**
  Data identified a 58.31% decrease in the number of unique URLs involved in potential phishing attacks, from 336,532 in June 2024 to 140,303 in December 2024. The seven-month average was 295,074 unique URLs. July 2024 saw the highest number of unique URLs to date, at 447,619. The lowest was 140,303 in December 2024.

- **A general decrease in the number of unique URLs used for verified phishing was observed.**
  Data analysis revealed an 81.29% reduction in the number of unique URLs involved in verified phishing attacks, dropping from 34,225 in June 2024 to 6,403 in December 2024. The seven-month average was 16,042 unique URLs. July 2024 had the highest number of unique URLs on record to date (35,421). September 2024 had the fewest unique URLs (6,342).
- **The aggregated Share of Top50 ASNs.**
  Between June and December 2024, the data shows that a total of 4,233,784 URLs were recorded, of which 3,684,553 were verified as malware, 217,343 were classified as potentially unwanted applications (PUAs), and 331,888 were categorised as 'other'. This dataset will evolve over time, reflecting changes within these three categories.

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 malware and phishing 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 an overview of the number of malicious URLs identified by the methodology, and illustrates how abuse on the Internet is changing over time. It shows the total number of unique URLs identified by the methodology as being involved in phishing, malware and potentially unwanted applications (PUAs), broken down by category:

- **Malware URLs**
- **PUA URLs**
- **Other URLs**

A **total** of **5,329,669 malicious URLs with ASNs** were identified in the period from June 2024 to December 2024, **of which:**

- **4,682,285 URLs** could be **verified as malware**,
- **256,058 URLs** have been **classified as PUA**, and
- **391,327 URLs** as **other**.

Between June and December, 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

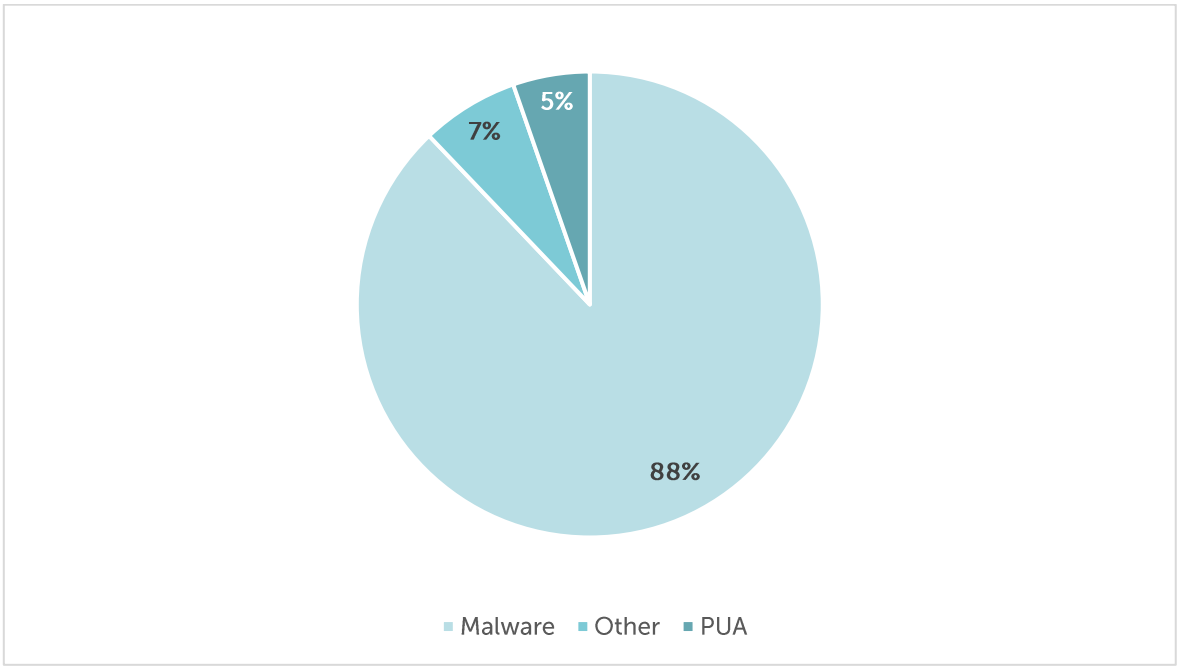

*Figure 1: Aggregate Malware Trends - **Malicious URLs** - **December 2024***

History of Malicious URLs

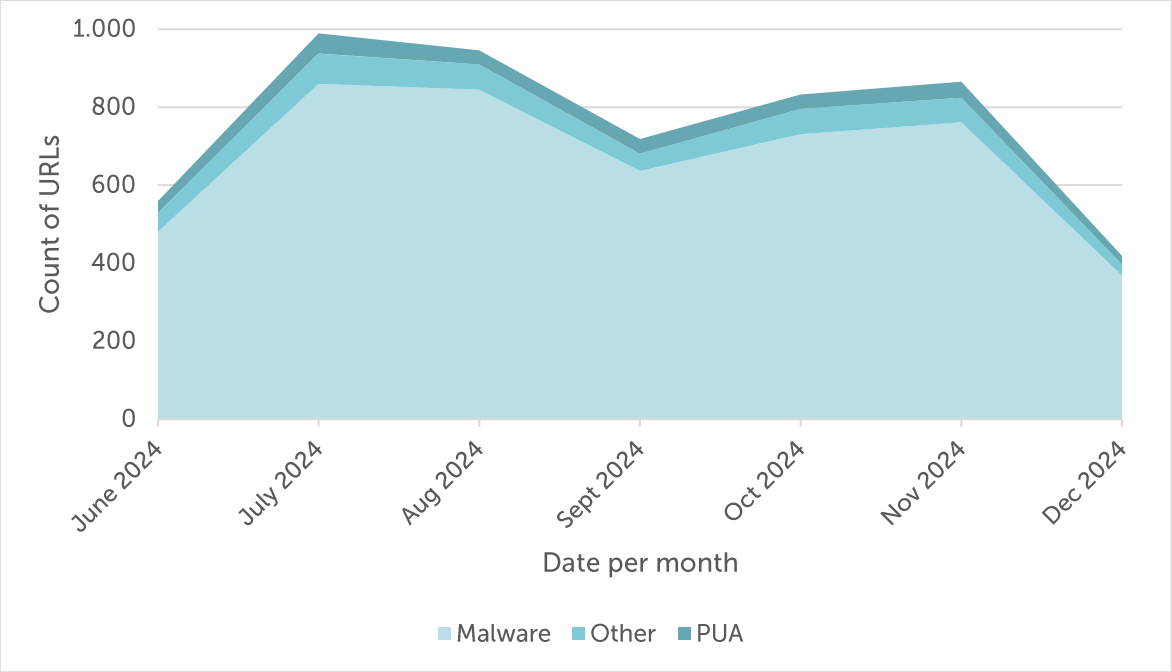

*Figure 2: Aggregate Malware Trends - **History of Malicious URLs** - **June 2024 to December 2024***

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%
Total	**4,682,285**		**256,058**		**391,327**	

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

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	**668,898**		**36,580**		**55,904**	

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

Commentary

Overall, there was a **decline in malware, potentially unwanted applications (PUAs) and other harmful distribution activity**, as reflected in a reduction in the number of unique URLs linked to these threats. Although July 2024 saw sharp increases in malicious URLs distributing malware (+79.00%), PUAs (+72.85%), and other harmful samples (+59.94%) compared to June, all three categories showed significantly lower figures by December.

December's figures also fell below the seven-month averages. July 2024 marked the peak across all categories, with 859,658 unique URLs tied to malware, 52,043 to potentially unwanted applications (PUAs), and 77,712 to other malicious URLs. By contrast, December 2024 recorded the lowest levels: 368,246 for malware, 22,345 for PUAs and 28,432 for other URLs. Overall, the data indicates that malware distribution trends are more volatile than phishing activity.

However. it's important to note that the dataset currently only covers seven 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 **2,065,515 phishing URLs with ASNs** were identified between June and December 2024, **of which 123,526 URLs** could be **verified**.

Between June 2024 and December 2024, the **highest number of phishing URLs** (**both potential and verified)** was identified in **July 2024**. 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

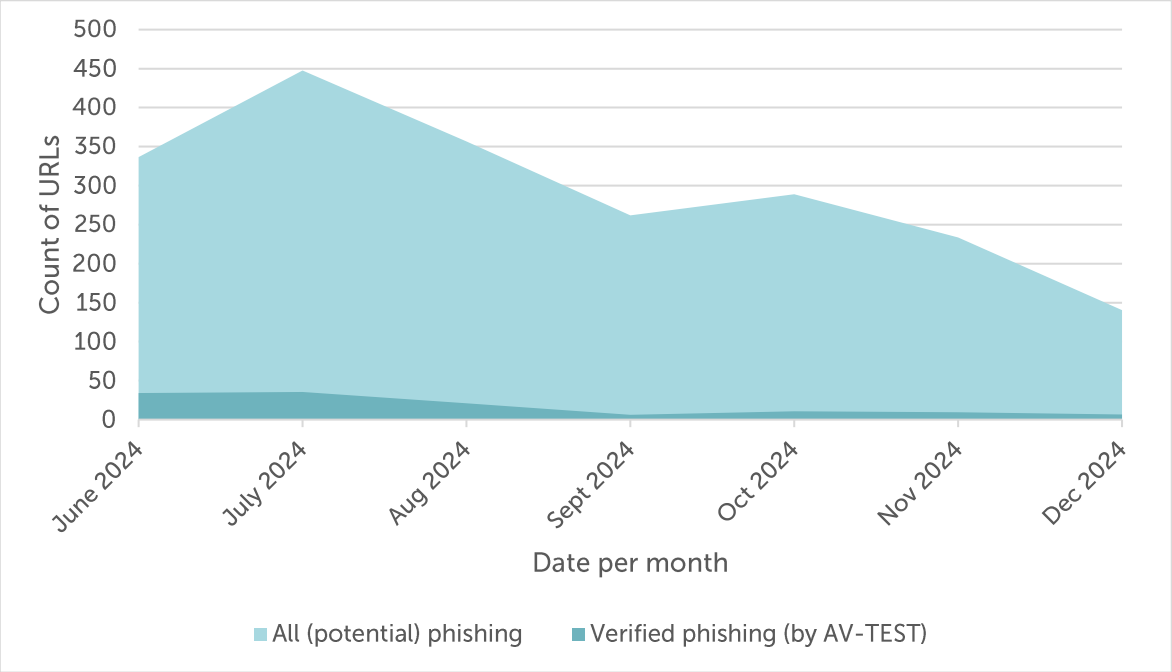

*Figure 3: Aggregate Trends - **History of Phishing URLs** - **June 2024 to December 2024***

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%
Total	**2,065,515**			**123,526**	

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

Key Figures of All (Potential) and Verified Phishing URLs

	All (potential) phishing	Month		Verified phishing	Month
High	447,619	July 2024		35,421	July 2024
Low	140,303	Dec 2024		6,342	Sep 2024
Average	**295,074**			**17,647**	

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

Commentary

Analysis of phishing-related activity reveals an **overall downward trend in the number of unique URLs**, punctuated by a significant increase in July 2024. Between June and December 2024, the volume of phishing URLs fell by 58.31%, dropping from 336,532 to 140,303. The December figure represents not only the lowest point in the reporting period but also sits well below the seven-month average of 295,074, highlighting the sustained contraction in activity towards the end of the year. Conversely, July 2024 saw an all-time high of 447,619 unique phishing URLs, over 50% higher than average, underlining the volatility of phishing

distribution. Overall, these trends suggest that, although phishing campaigns can surge rapidly, their prevalence declined in the latter half of 2024.

A clear **downward trend was observed** in the number of unique URLs linked **to verified phishing** attempts. Between June and December 2024, volumes fell sharply by 81.29%, dropping from 34,225 to just 6,403 URLs. The seven-month average was 17,647, meaning that the figure for December was substantially below the overall baseline. July 2024 saw the highest number of unique URLs (35,421), while September 2024 saw the lowest (6,342). This suggests that, while capable of spiking significantly, verified phishing activity contracted heavily in the latter half of the year.

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

Chart: Aggregated Share of Top50 ASNs

This table provides a high-level, anonymised overview of the 50 largest autonomous systems, as identified by their assigned autonomous system number (ASN).

A **total** of **4,233,784 URLs with ASNs** were identified among the Top50 ASNs between June and December 2024, **of which:**

- **3,684,553 URLs** could be **verified as malware**,
- **217,343 URLs** have been **classified as PUA**, and
- **331,888 URLs** as **other**.

If you are a network operator, please contact us for further details on 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

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

Commentary

Between June and December 2024, a total of 4,233,784 URLs were recorded across the Top 50 ASNs. Of these, 3,684,553 were verified as malware (≈87%), 217,343 were classified as potentially unwanted applications (PUAs, ≈5%), and 331,888 fell into the 'other' category (≈8%). This distribution underscores the **dominance of malware** within the dataset, representing the overwhelming majority of observed URLs. Over time, the balance among these categories is expected to shift, reflecting evolving threat activity and distribution patterns.

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

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.