DNSFilter

THREAT TRENDS:

DNSFILTER Q2 SECURITY REPORT

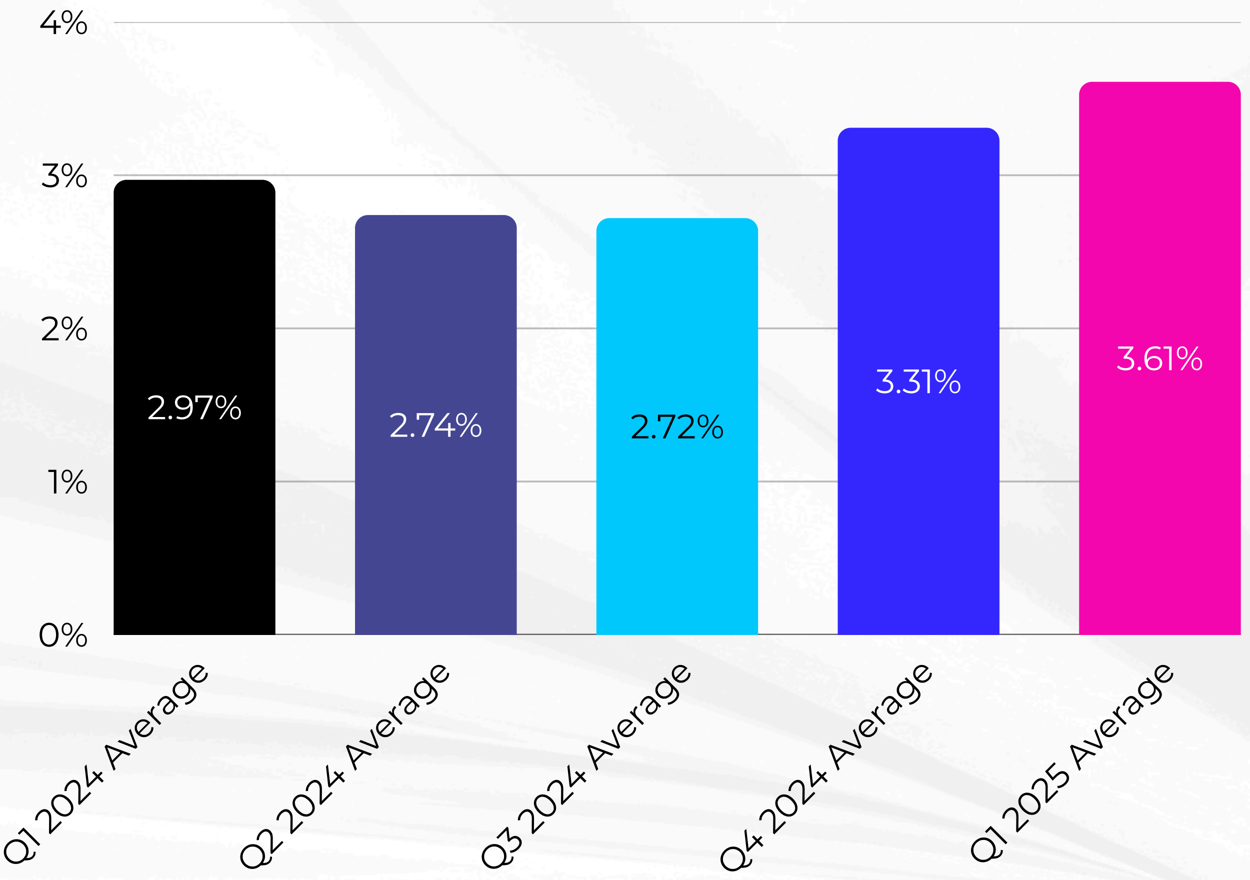
EXECUTIVE SUMMARY

In Q1 2025 on the DNSFilter network, the top threat type by query volume was the new domains category. Previously, malware has held the top spot as the most-trafficked threat category at DNSFilter. This Q1 Security Report will go over threat traffic, query growth, and investigate why new domains have grown during the January 1, 2025 - March 31, 2025 timeframe.

A GROWING NETWORK

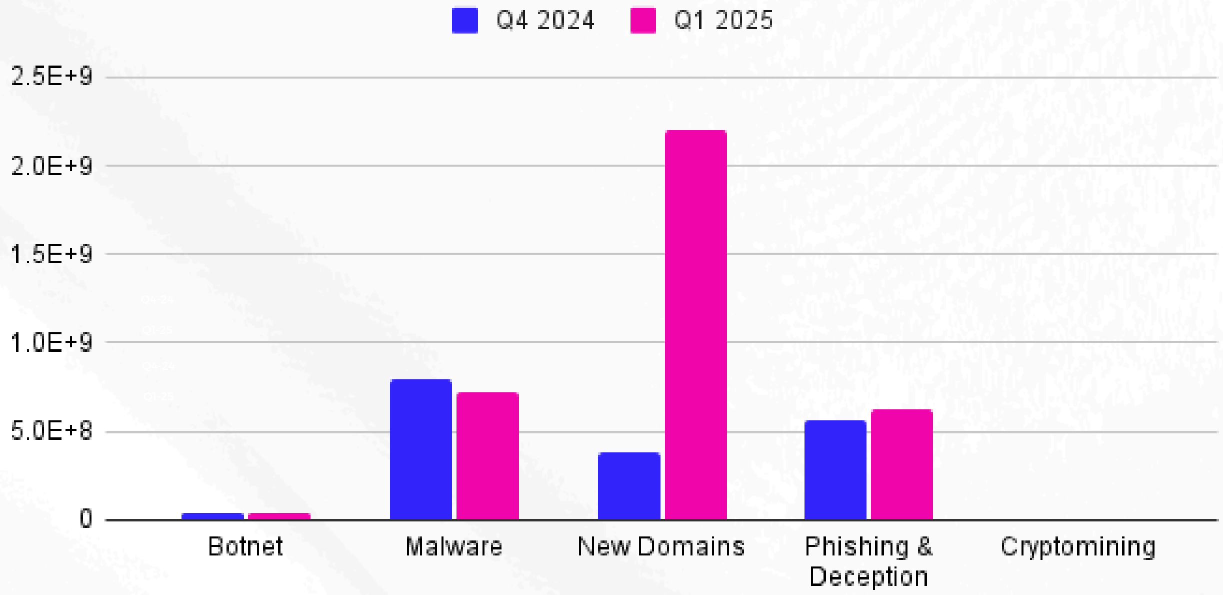
Q1 2025 was a landmark quarter for DNSFilter's network. January recorded the highest DNS traffic volume of all time, followed closely by March. Across the quarter, 3.61% of total DNS traffic was blocked — the highest quarterly block rate on record. Traffic can be blocked for a variety of reasons; not all blocked traffic is malicious. All sites are blocked at the discretion of our end-users, who may choose to block domains associated with time-wasting or inappropriate sites in addition to cyber threats.

January, again, was a standout with 3.73% of all traffic blocked on the network. Between Q1 2024 and Q1 2025, blocked traffic on our network grew by over 21% and queries as a whole grew by 45%.

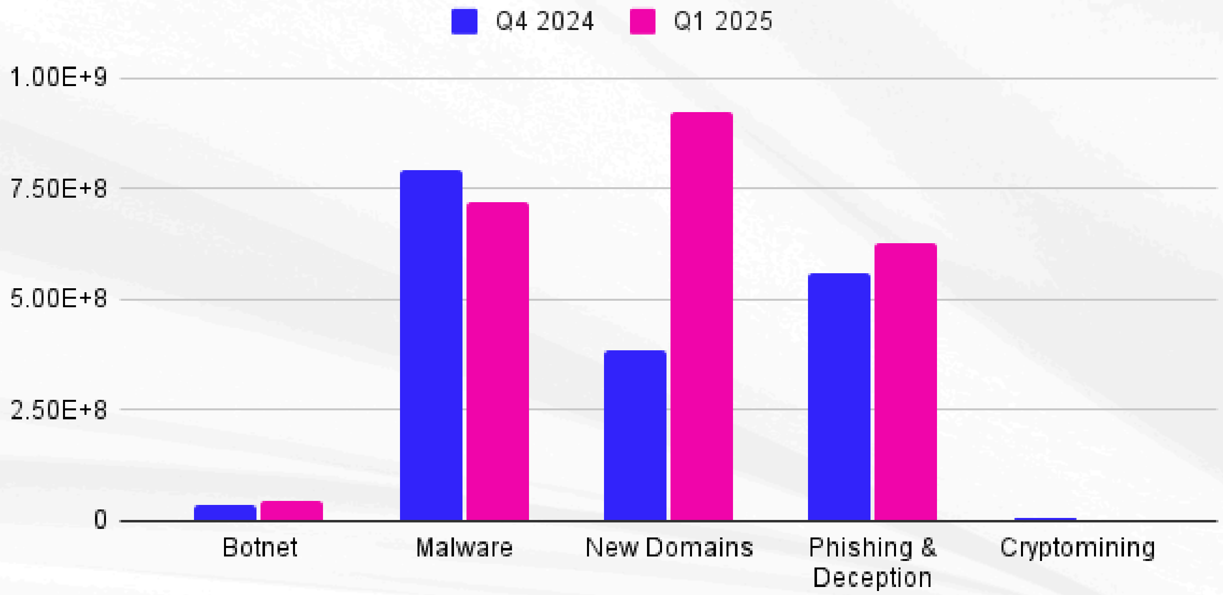


Depending on the purpose of a new domain, we can see large unexpected jumps in traffic. This was the case when we noticed a new Content Server set up by a popular social media platform in Q1. This caused a request surge of 473% compared to Q4. This traffic is, by all intents and purposes, harmless and legitimate, but can skew the data. Removing this outlier, we are left with a modest 140% increase by comparison, though this still retains the highest amount of traffic compared to any other threat category on our network.

TOTAL THREAT REQUESTS Q4 2024 VS. Q1 2025 (INCLUDING CONTENT SERVER DOMAINS)



TOTAL THREAT REQUESTS Q4 2024 VS. Q1 2025 (EXCLUDING CONTENT SERVER DOMAINS)



Malicious traffic was also on the rise, with January experiencing the largest amount of malicious traffic. Out of all identified traffic in January, over 1% of requests were malicious. In February and March, over .71% of all traffic was categorized as malicious.

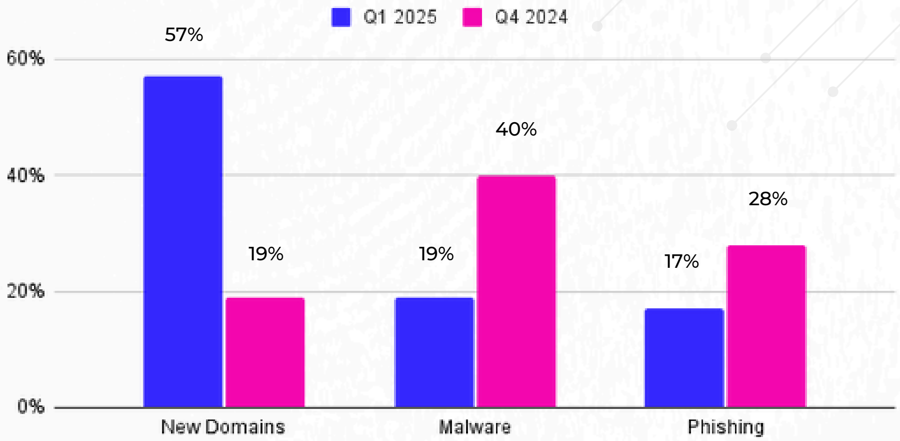
TOP THREAT CATEGORIES

While our new domains category overtook both phishing and malware in Q1 2025, it’s important to note that DNSFilter made changes to its phishing category at the end of 2024. We split the category known as phishing and deceptive into two distinct categories:

- Phishing
- Suspicious and deceptive

However, for the purposes of this report, we combined those two categories in order to have an accurate comparison looking back at Q4.

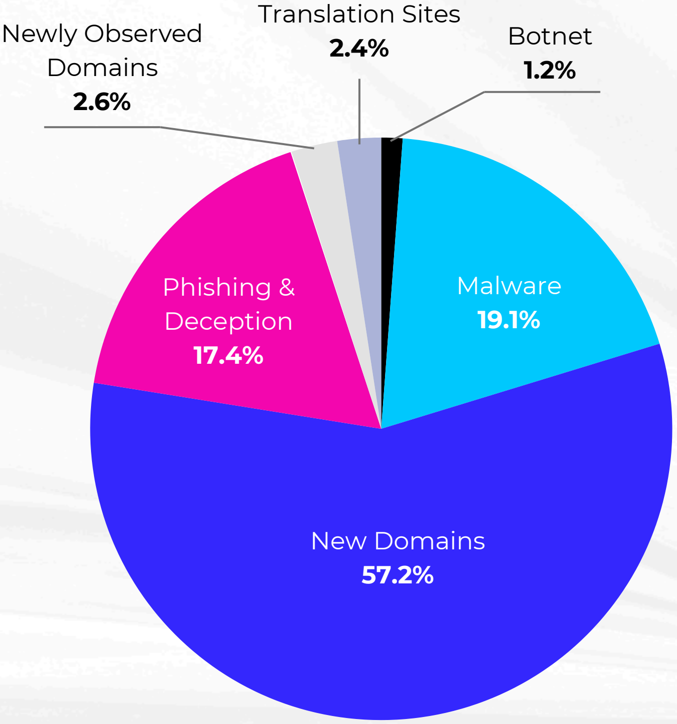
PERCENT MAKEUP OF MALICIOUS CATEGORIES ON THE DNSFILTER NETWORK



Even without the inclusion of the suspicious and detective queries, phishing would still be at No. 3 in this list, with no other threat category coming within range of the number of queries phishing produces.

What is surprising here is that malware, which has remained a top threat through 2023 and 2024, has dropped significantly in Q1 2025, both in raw query count and when compared to the overall makeup of the threat landscape on the DNSFilter network.

Total requests (excluding proxy and avoidance):



What this data tells us is not necessarily that there were more active new domains than usual in Q1, but there was more traffic than usual. This means, the new domains that were created were more popular with users on our network for some reason. This could mean successful threat campaigns leveraging these new domains, resulting in greater traffic.

New domains can be considered suspicious and possibly malicious, but sometimes are simply just new. Blocking this category can protect you from emerging threats and domains that have the potential to become malicious, since new domains are used frequently in phishing and malware campaigns.

The DNSFilter network is processing upwards of 170 billion queries everyday, and many of these are domains that we are processing for the first time. We examined queries to the top 100 domains within this category and found that over 19% of new domains identified in Q1 are still malicious or potentially malicious, meaning that roughly **one in every five clicks** to a site categorized as a new domain is still a potential risk.

TOP THREAT CATEGORIES

The Top Level Domains that are used in threat domains shift quarter over quarter as threat actors adopt new TLDs for use in their campaigns. Threat actors will often choose TLDs and registries that are less expensive and even free in some cases, meaning they can move on front domains and register new ones quickly without cost concerns.

TOP BLOCKED TLDS

	TLD	% Blocked
1.	.pw	99.38%
2.	.cn	97.37%
3.	.eu	96.28%
4.	.me	96.07%
5.	.ru	95.64%

In our Annual Security Report, our list was exceptionally different with only .me present in the previous list, moving from No. 5 to No. 4 in Q1 2025 and increasing over 10 percentage points. These changes might be indicative of IT administrators and cybersecurity professionals using DNSFilter's wildcard feature to block particular domains, regardless of how a site is categorized. The Top Level Domains for both China and Russia appear on this list, indicating that our users are more likely to block these ccTLDs.

Users often choose to block TLDs when they gain a reputation for unsafe, harmful, or malicious content. The most-blocked TLD on our network is also the second-most malicious domain, indicating that the high volume of malicious domains has led our customers to block this domain without question more often than not.

COUNTRY CODE TOP LEVEL DOMAINS (CCTLDS) MOST LIKELY TO BE MALICIOUS

While the previous TLDs were likely to be blocked, the content itself is not inherently malicious.
When we look at the percent of threat requests that belong to ccTLDs, these are the top five most-malicious ccTLDs in Q1 2025:

	ccTLD	% Malicious
1. French and Southern Atlantic Lands	**.tf**	**88% of traffic**
2. Palau	**.pw**	**68% of traffic**
3. Sint Maarten	**.sx**	**64% of traffic**
4. Aland	**.ax**	**46% of traffic**
5. Lichtenstein	**.li**	**41% of traffic**

Palau’s ccTLD (.pw) has become known as a ccTLD often leveraged in attacks. This explains why it is the most-blocked TLD on our network, and for good reason. Nearly 70% of all .pw queries on our network are malicious.

Aland and Lichtenstein are new to this top 5 list, and in total this list represents higher malicious activity per ccTLD than what we reported in our Annual Security Report. Previously, the French and Southern Atlantic Lands were found to be 39% malicious but have since *more than doubled*.

The top 3 listed here were also the top 3 in our Annual Security Report, though in a different order. When zeroing in on .tf, .pw, and .sx, 60% of the top 100 domains of each ccTLD are categorized as proxy and filter avoidance. Sites categorized as proxy and filter avoidance are sites that provide information or a means to circumvent DNS based content filtering, including VPN and anonymous surfing services. This means using these sites enables the evasion of security controls, opening end users up to increased risk. These proxy and filter avoidance sites are also potentially malicious on their own, linking to malware or other threats.

DNSFilter

WHY DO THREAT ACTORS TARGET NEW DOMAINS?

Cybersecurity professionals and IT administrators must prioritize real-time detection of suspicious domains, especially those lacking age or reputation signals. DNSFilter customers are already adapting as they are blocking new domains (and threats as a whole) at a higher volume than ever before.

Threat actors increasingly register brand-new domains because:

- They can capitalize on trends with catchy domain names, customizing their threat campaign.
- New domains often don't appear on blocklists yet, buying attackers a window of time for exploitation.
- Many of these are used in “fast flux” attacks, where domains are cycled quickly to avoid detection.

DNSFilter customers can leverage our new domains category and implement rules to block questionable TLDs. These actions, taken together, can mitigate risk for both end users and organizations as a whole. As our network grows and we process and block more threat queries, we expect new domains to continue to grow as a category as this is a regular technique used by threat actors in phishing and fast flux attacks.

ABOUT DNSFILTER

DNSFilter protects every click, leveraging AI-driven content filtering and threat protection to block threats 10 days earlier than competitors and secure users everywhere they work. Our solutions help boost worker productivity, minimize compliance risk, and protect corporate brands on public Wi-Fi networks. Our intuitive, granular policy controls and flexible deployment options safeguard hybrid work laptops, IoT devices, and legacy technology. Unlike traditional filtering solutions, we deploy in minutes instead of days and are trusted by more than 40,000 organizations worldwide.

BOOK YOUR DNSFILTER DEMO TODAY