DNSFilter

ANNUAL SECURITY REPORT

JANUARY 2025

TABLE OF CONTENTS

FOREWORD

Every year, our annual security report serves as a reminder of the critical role DNSFilter plays as a frontline defender on the DNS layer. At the scale of the internet, threats are relentless, but so is our commitment to stopping them. Every malicious request we block isn't just a statistic—it's a real attack prevented, real harm avoided, and real people protected.

Today, our network processes an average of 170 billion DNS queries every day, and more than **200 million** of those daily queries are active threats that we catch and stop. Behind those numbers are phishing campaigns that never reached their targets, ransomware that never took hold, and malware that never had the chance to spread. That's the impact of our work—and it's what drives us forward.

The challenges are only getting bigger. Threats on our network grew by 36% over the period covered in this report, reflecting not just the volume of malicious activity but also the creativity of those behind it. We meet this challenge by staying ahead: advancing our AI-driven models to detect subtle, early indicators of attack behavior before threats can escalate. The result is a security approach that doesn't just react but anticipates—uncovering emerging risks and neutralizing them before they become real-world problems.

What sets DNSFilter apart is our proactive stance and our relentless pursuit of stopping threats before they cause harm. While others may wait for known threats to appear on public feeds, we're identifying and blocking them earlier, disrupting attackers' efforts at every turn. For our customers, this means greater peace of mind, greater resilience, and fewer bad days caused by a successful attack.

As we move into 2025, our mission remains clear: to protect people, businesses, and organizations from the worst the internet has to offer. We'll keep innovating, keep improving, and keep standing between threat actors and the real-world harm they aim to cause.

Here's to another year of staying ahead of the curve—and keeping those we serve safe.

KEN **CARNESI**

CEO, DNSFILTER

2024 INDUSTRY NEWS IN REVIEW

Over the past year, the cybersecurity landscape has been shaped by intensifying ransomware campaigns, evolving business email compromise (BEC) tactics[1], significant law enforcement successes against cybercriminal networks[2], and of course AI-driven threats[3]. Notably, ransomware has continued to dominate as a critical threat, with groups like ALPHV/BlackCat and Royal (Blacksuit) ransomware[4] syndicates leading high-profile attacks. The healthcare sector[5] was especially targeted, with ALPHV affiliates encouraged to victimize hospitals following enforcement actions against the group in December 2023. This deliberate pivot underscores how ransomware operators adapt their strategies to exploit vulnerabilities in high-value, critical infrastructure sectors.

BEC attacks have reinforced their position as a top-tier identity-centric threat, with adversaries leveraging increasingly sophisticated methods to compromise organizational email systems. Key tactics such as email forwarding and hiding rules have emerged as pervasive techniques, emphasizing the attackers' focus on evasion and persistence. These methods allow threat actors to silently exfiltrate data or monitor communications for extended periods, enhancing their ability to exploit compromised accounts effectively. BEC's persistence signals the need for organizations to double down on email security and user awareness programs.

Amid this evolving threat environment, law enforcement and collaborative cybersecurity efforts have achieved notable victories. Operations like "Endgame" have demonstrated the global reach and effectiveness of coordinated actions against cybercriminal networks. These successes highlight that while the cybercrime ecosystem continues to innovate, the combined efforts of law enforcement, industry stakeholders, and government agencies are achieving meaningful results. High-profile takedowns have disrupted criminal operations and reaffirmed the value of information sharing and public-private partnerships in combatting cyber threats.

The emergence of novel nation-state operations, such as the Muddling Meerkat DNS mystery[6], further illustrates the complex interplay of espionage and cybercrime. These sophisticated campaigns blur the lines between geopolitical motives and traditional hacking, often leveraging stealthy techniques to compromise infrastructure and conduct reconnaissance. Such developments challenge defenders to adopt more proactive, intelligence-driven approaches to anticipate and mitigate threats from well-resourced adversaries.

Despite the growing ease with which malicious actors can deploy advanced tools through the use of Artificial Intelligence, the cybersecurity community has shown resilience and adaptability. Continued innovation in detection capabilities, a focus on threat intelligence, and law enforcement engagement are providing critical momentum in the fight against cybercrime.

[1] https://redcanary.com/threat-detection-report/midyear-update/trends/

[2] https://www.fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals

[3] https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

[4] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

[5] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

[6] https://www.darkreading.com/threat-intelligence/muddling-meerkat-poses-nation-state-dns-mystery

TRENDS AND ANALYSIS:
DATA IN MOTION

THE BIG PICTURE

While the trends change year-over-year, our passive DNS data is constant and provides a lens for us to examine the last 12 months.

The percent of threats on our network increased significantly in 2024. While still under 1% of all network traffic, identified threats on our network grew by 36% between October 2023 and September 2024. The relative distribution of threats remained consistent over time, though the percent of malware queries increased by 14% and phishing increased by 203%. This is in-line with the marked increase in ransomware seen across the industry, with phishing being the most common method for ransomware distribution.

Percent of threats on network

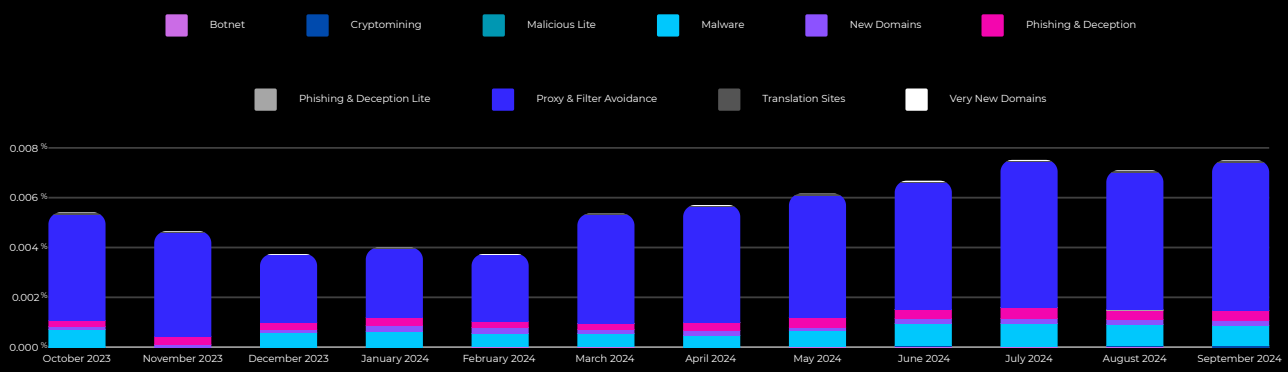


Figure 1. Percent of threat queries out of total queries on the DNSFilter network October 2023- September 2024

While the percent of threats on our network is under 1% of all queries totaled, this represents a daily average of 92 million queries.

Over this time period, August 2024 was the month with the largest amount of threat queries on our network, but July was the month with the highest overall percentage of threats on the DNSFilter network.

When we look at domains, however, we see a different story.

Threat domains as a percent of total unique domains by month

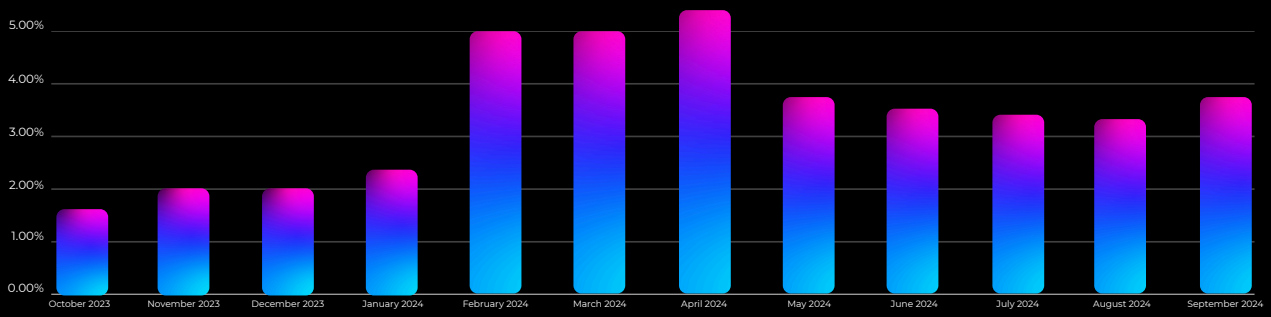


Figure 2. Percent of threat domains out of total unique domains on the DNSFilter network October 2023- September 2024

Out of the total number of unique domains trafficked by month, April had the highest number of unique threat domains. This means that while threats in April only made up .56% of all network traffic, there were a large number of unique domains making up that lower percentage point. In April, 5.26% of all unique domains trafficked on our network were malicious. The average over the time period we examined (October 2023 - September 2024) was 3.5% with only February, March, and April over 5%. This timeline coincides with findings from research firm Egress, who saw a 28% increase in phishing emails between April 1st and June 30 of 2024.[7] The method of attack is no longer malicious attachment, but malicious *hyperlink*.

[7] https://www.makeuseof.com/phishing-attacks-increasing-2024/

Percent of threat category blocks, of all blocks, by category over time

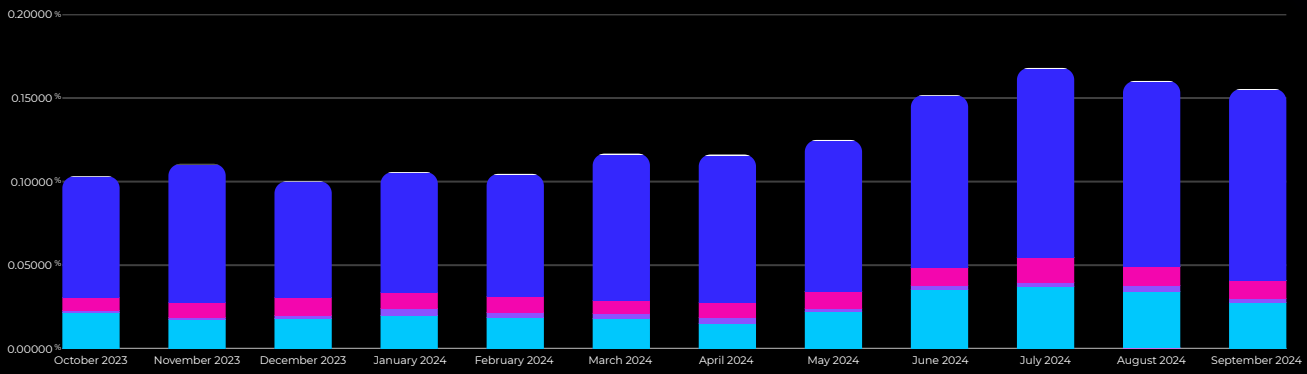


Figure 3. Percent of threat category blocks, of all blocks by category on the DNSFilter network from October 2023- September 2024

When we look at threats blocked compared to all content blocked on the DNSFilter network, between 10% and 16% of all blocked requests were malicious, with that number increasing steadily through September, which aligns with the steady increase of phishing emails seen by Egress. July had the highest instance of malicious blocked content, with 16.6% of all blocked content being malicious. Outside of our proxy & filter avoidance category, the category that made up the largest number of blocked malicious requests was malware. In July, malware made up 3.66% of all blocked content requests on our network. This more than doubled from earlier in this timeframe (1.704% in November 2023). This coincides with an increase of Mac malware in 2024[8] as well as Corvus' report that the number of ransomware victims in Q3 was higher than Q2[9]—and interestingly, 40% of the activity is attributable to only five ransomware groups:

- RansomHub
- PLAY
- LockBit 3.0
- MEOW
- Hunters International

[8] https://appleinsider.com/articles/24/12/04/what-a-new-threat-report-says-about-mac-malware-in-2024
[9] https://www.infosecurity-magazine.com/news/five-ransomware-groups-40-of/?&web_view=true

It is also significant to note that while July had the highest traffic to malware, Thursday, August 15 had the highest single day of malware traffic on the DNSFilter network in 2024. We'll examine the top level domains (TLDs) on that day later in this report. You can see the full distribution of query traffic here:

Total requests by Category (excluding proxy)

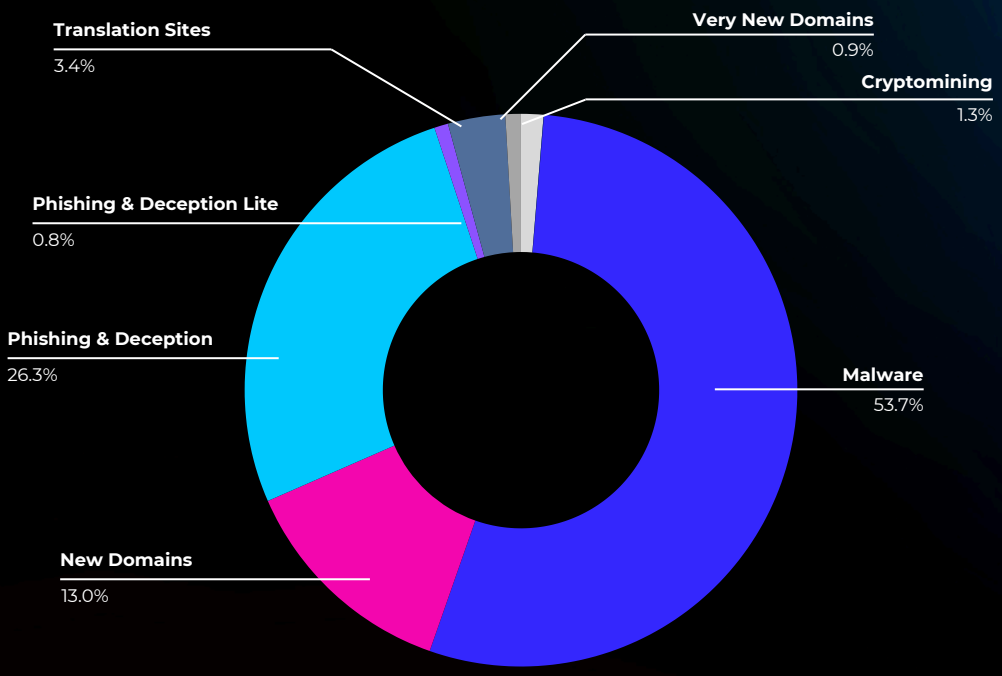


Figure 4. Percent of threat category blocks, of all blocks by category on the DNSFilter network from October 2023- September 2024

However, when we instead look at domain count as opposed to queries, we see a different story:

Domain count by category (excluding Proxy & Filter Avoidance)

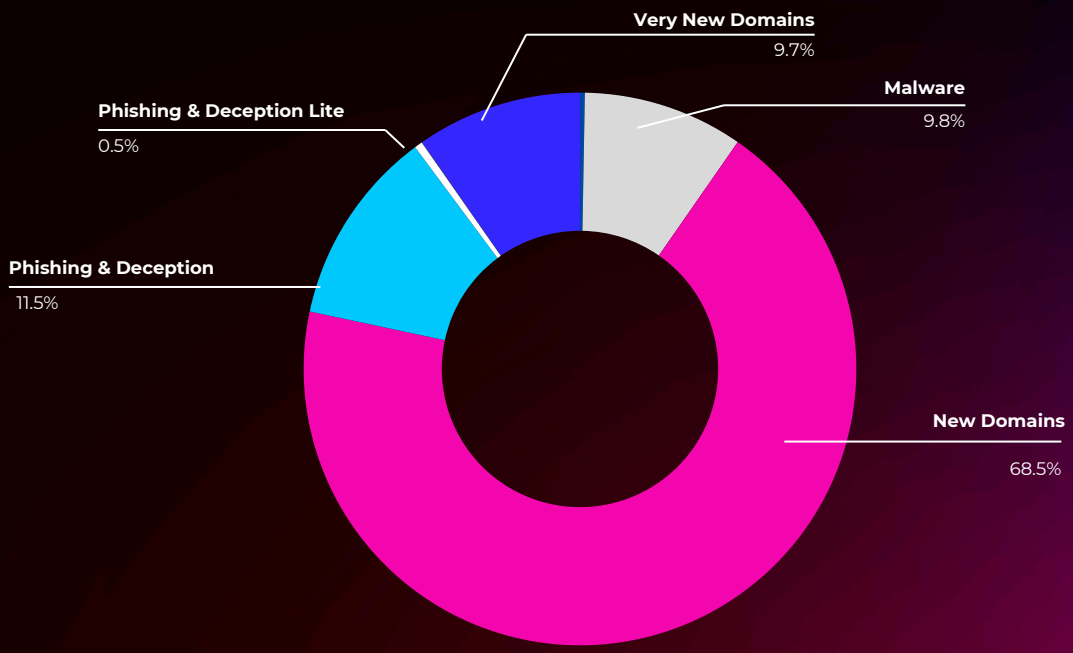


Figure 5. Domain count by category on the DNSFilter network from October 2023- September 2024

New domains make up over 68% of all unique threat domains on the DNSFilter network. So while malware queries are more active, it means that there are fewer malware domains active on our network—which is consistent with having five malware groups responsible for a large portion of all ransomware. These malware domains are likely attempting to “phone home” repeatedly, sometimes as often as 300 times per hour. This is activity we have observed on our network over the last 12 months.

The nature of new domains is that they generally have lower traffic, yet they are frequently used only once and then discarded, leading to a higher overall volume.

One final note on a threat that we often don’t discuss: CSAM (child sexual abuse material) content on the DNSFilter network is always less than 0.00% of daily network traffic. However, despite the low query counts, we still see attempted (and blocked) traffic to these domains on a daily basis. This is the only category that is always blocked on our network, without exception. At DNSFilter, we are blocking more CSAM every single day than we ever have before in our history.

COMPARING TO THE PREVIOUS YEAR

Percent of threats identified out of all queries

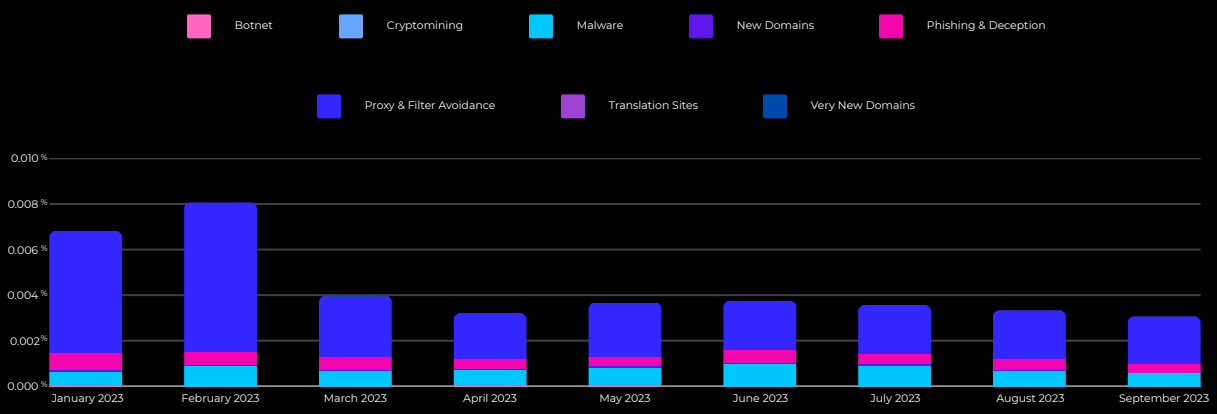


Figure 6. Percent of threats identified out of all queries by category on the DNSFilter network from January 2023- September 2023

Compared to the previous period, threats actually made up a higher percentage of our network by a slight margin in 2023, with the highest periods being January and February. Despite this higher percentage of threats, DNSFilter processed and blocked far more threat queries in 2024 than the previous year because of the growth of its network. The average daily volume of threat queries grew 26.77% between last year and this year.

HOW OFTEN IS THE AVERAGE PERSON ENCOUNTERING A THREAT?

According to our data, one in every 174 requests is malicious. Since the average person makes 5,000 DNS requests per day, that means a single person could encounter as many as 29 threat queries in a single day. This is significantly higher than last year's findings, where one in every 1,000 queries was a threat.

The overall trend is that not only is DNSFilter processing more daily queries than ever before, but we're also processing and blocking a higher volume of threat requests—and the percentage of threats is increasing as well.

AI ON OUR NETWORK

In 2023, DNSFilter released its GenAI category which has allowed us to see trends in AI adoption over time. In 2024, we saw overall traffic increase 786% between October 2023 and September 2024. The number of individual AI domains has increased 15% over this period. While new GenAI domains have been registered, categorized, and visited on the DNSFilter network, it is still a relatively small number of domains making up a large portion of traffic. AI traffic made up .12% of our network in September 2024, which was roughly 14% of all threat traffic on our network over that time period—36% higher than malware alone.

AI Queries over time

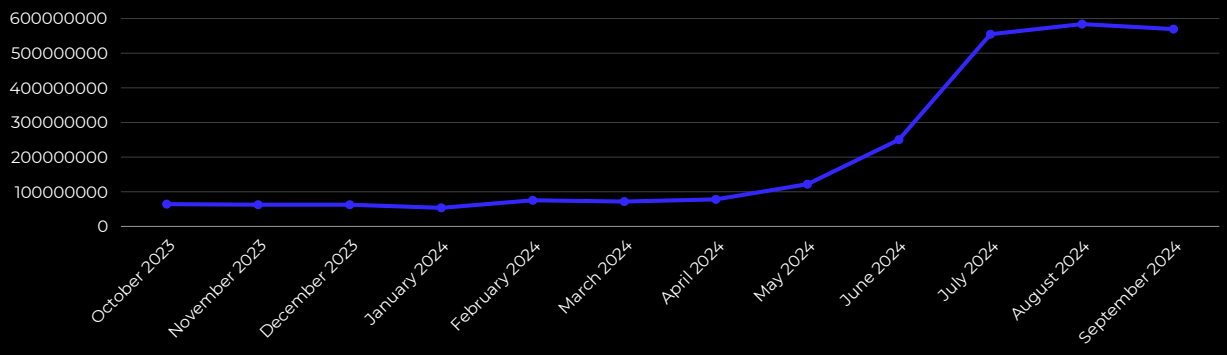


Figure 7. AI query traffic over time

AI domain count over time

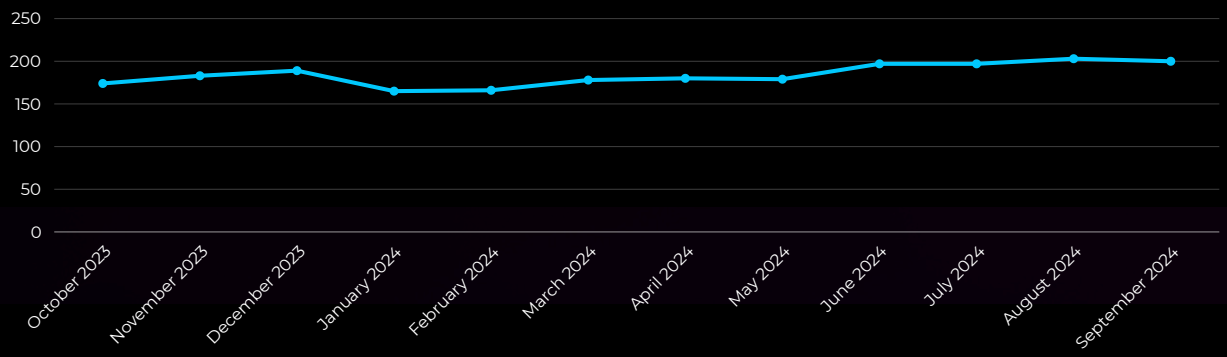


Figure 8. Unique AI domains over time

But the generative AI category is just the start of AI on our network this year. Amid AI's rise, scams using AI[10] or exploiting AI have considerably increased. New domains using variations of the terms "artificial intelligence" and "machine learning" attached to a variety of cheaper TLDs (such as .shop, .today, .life, .site, .fyi, or .zone) appeared consistently on our network throughout the year. Not surprisingly, 56% of domains using these keywords on our network contained a form of "artificial intelligence" in the domain name.

Many of the domains seem to have been created to exploit an interest in learning more about AI, evidenced by the keywords used in this set of domains:

- Courses
- Degrees
- Courses Online
- Online courses for

Other sites were set up to look like AI tool lists or AI compliance software. Because these domains were set up to be used in threats for a brief period of time, a majority of them are no longer active or taken down by the registrar. These scams are usually short-lived, but they can cause a lot of damage in a short amount of time while they are active.

[10] https://www.ic3.gov/PSA/2024/PSA241203

THREATS BY REGION

When we review threats by region on our network, we examine which server on our network (in which location) processed the request.

The data in the following map shows what percentage of requests routed through each region is categorized as malicious.

Percent of Threat Requests by Region

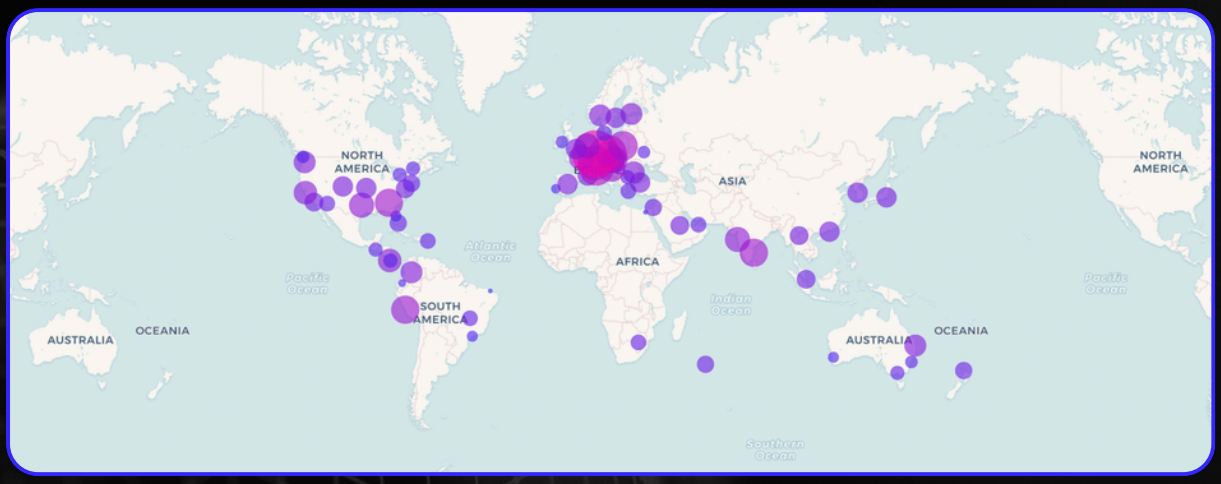


Figure 9. Map showing percent of threat activity October 2023 - September 2024

The top five countries which have the highest percentage of malicious requests on our network are:

1. Germany	**1.14%**
2. Czech Republic	**0.89%**
3. Italy	**0.79%**
4. Switzerland	**0.78%**
5. Poland	**0.67%**

Why these countries? Part of it may be that these countries host a significant number of data centers or Content Delivery Networks (CDNs) that are sometimes leveraged by threat actors to host malicious domains. For example, Germany[11] and Switzerland,[12] in particular, are known for strong data privacy regulations and advanced infrastructure, which can sometimes attract both legitimate businesses and malicious actors looking to exploit these features.

Out of all queries trafficked through our US servers, only .47% of all requests were threats. However, the percentage of threat traffic increased between July and September. Looking at these months alone, in the lead-up to the 2024 US elections, would have placed the US just outside the top five—seventh place to be exact.

[11] https://www.bfdi.bund.de/EN/BfDI/UeberUns/DieBehoerde/diebehoerde_node.html

[12] https://www.digitalguardian.com/blog/what-new-swiss-data-protection-act-and-how-do-you-achieve-compliance

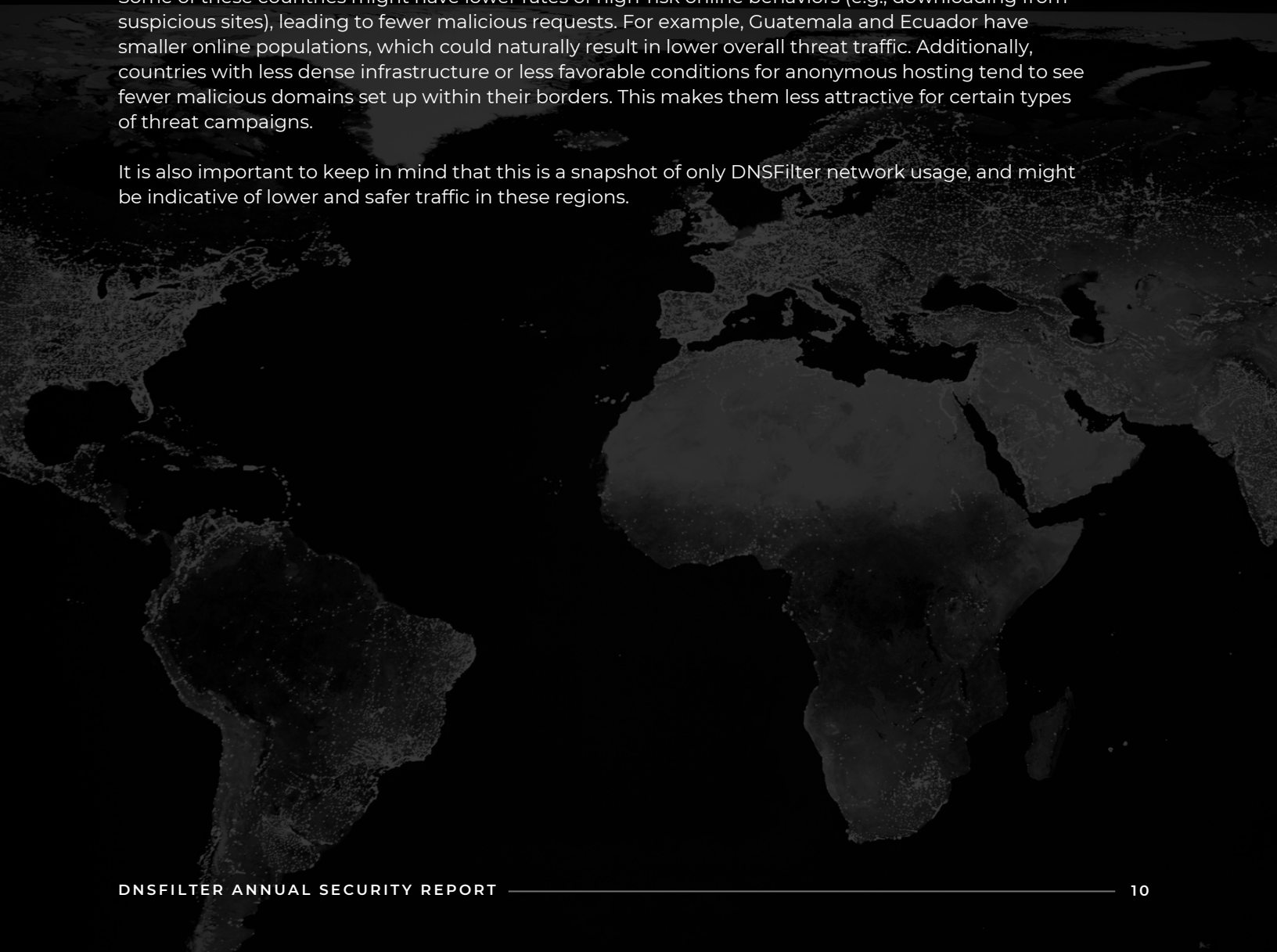
The average of threat query traffic across all countries on the DNSFilter network was 0.41%, making the US generally more susceptible to threats than the average on our network.

Ecuador was the country with the fewest number of threats passing through our servers, with .09%. The top five countries with the least threat traffic were:

1. Ecuador	**.09%**
2. Brazil	**0.16%**
3. Ireland	**0.22%**
4. Australia	**0.23%**
5. Guatemala	**0.24%**

Some of these countries might have lower rates of high-risk online behaviors (e.g., downloading from suspicious sites), leading to fewer malicious requests. For example, Guatemala and Ecuador have smaller online populations, which could naturally result in lower overall threat traffic. Additionally, countries with less dense infrastructure or less favorable conditions for anonymous hosting tend to see fewer malicious domains set up within their borders. This makes them less attractive for certain types of threat campaigns.

It is also important to keep in mind that this is a snapshot of only DNSFilter network usage, and might be indicative of lower and safer traffic in these regions.



TLD ANALYSIS

Analyzing the top level domains (TLDs) that are most-trafficked and most-blocked on our network every year gives us insight into the popularity of certain TLDs on our network—not to mention trends as to which TLD is leveraged by the most threat actors.

Just as .com is generally the most popular TLD in-use on the web, it's also the most popular for threats. .com is a familiar domain, and it might imply safety to those who are targeted in an attack. Because of this, it remains a popular TLD for use in attacks.

Let's compare the top trafficked TLDs to the most blocked TLDs by raw query volume:

	Most Trafficked TLD	Most Blocked TLD
1.	.com	.com
2.	.google	.google
3.	.apple	.apple
4.	.net	.foo
5.	.foo	.net

But when we look at which individual TLDs have the highest amount of traffic blocked, we have a very different top five:

	TLD	% Blocked
1.	.foo	Nearly 100% of Traffic
2.	.co	Over 90% of Traffic
3.	.de	Over 90% of Traffic
4.	.biz	Over 90% of Traffic
5.	.me	Over 90% of Traffic

Percent blocked by TLD

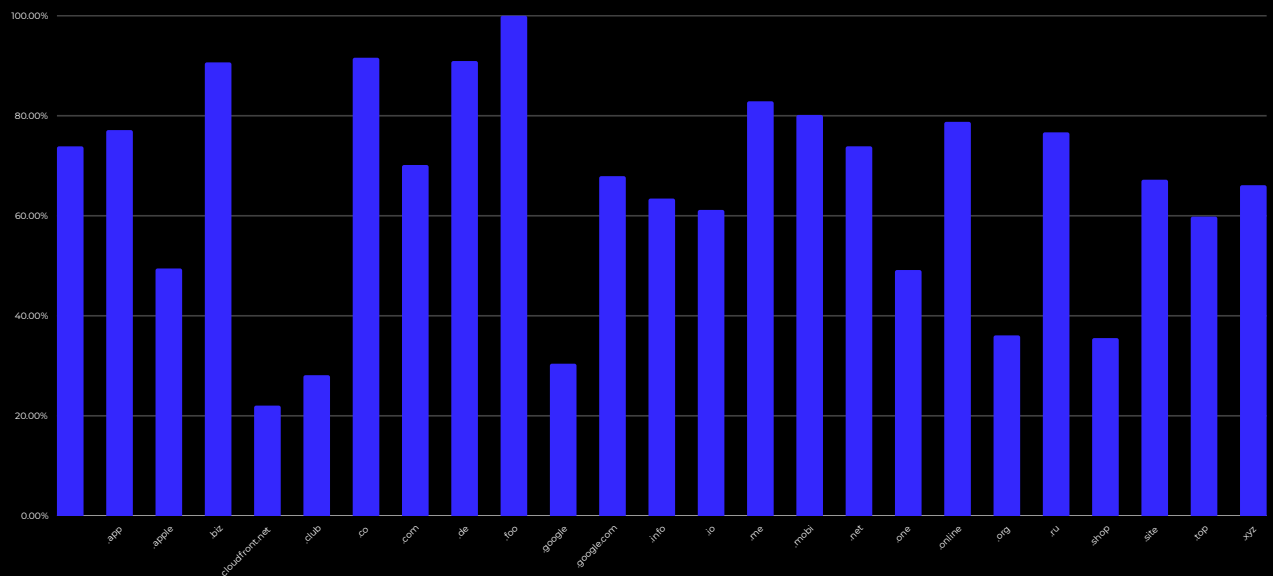


Figure 10: Percent of blocked traffic by TLD October 2023 - September 2024

Finally, let's examine country code top level domains (ccTLDs). Many ccTLDs are used in threats because the domains are low cost or even free to obtain. When we look at the percent of threat requests that belong to ccTLDs, these are the top five most-malicious ccTLDs within the last year:

	ccTLD	% Malicious
1. Sint Maarten	**.sx**	**43% of Traffic**
2. French and Southern Atlantic Lands	**.tf**	**39% of Traffic**
3. Palau	**.pw**	**38% of Traffic**
4. Christmas Island	**.cx**	**30% of Traffic**
5. Faeroe Islands	**.fo**	**25% of Traffic**

Something to note here is that this list is very different from lists we published in 2023 and 2022, as usage trends within domains shift over time. Domain registrars also become better at shutting down domains with abuse as the frequency increases.

In our first year publishing this report, the ccTLD ranked as most-malicious on our network was Equatorial Guinea (.gq). In last year's report, Iceland (.is) was at the top of the list. What this shows us is the lifecycle of a threat domain; having visibility into which threats (via which ccTLDs) are most prominent on your network allows you to block threats appropriately and in a timely manner. Your own network might look very different from the DNSFilter ecosystem as a whole.

MSP SPOTLIGHT: THE CATEGORIES MSPS DO—AND DON'T—BLOCK FOR THEIR CUSTOMERS

Managed Service Providers (MSPs) sit in an interesting position in our industry. They are IT and security experts with access to multiple organizations and their infrastructure, making them a prime target for cybercriminals.[13] Meanwhile, they need to protect their own customers' networks and data.

Because of this unique position, how MSPs approach cybersecurity is different compared to organizations that manage their own IT and cybersecurity infrastructure. This can be seen in what content categories they block within their policies.

No matter what type of organization you are—MSP or not—there is a very consistent top list of categories that our users block on their network:

1. Malware
2. Botnet
3. Phishing
4. Cryptomining
5. Adult Content

What separates MSPs from organizations that manage their own IT and security directly is how often these categories are added to their DNSFilter block policies.

In doing a comparison of MSPs and non-MSPs, MSPs are more security-conscious and more willing to allow users to traffic the web as they please. Non-MSPs are security conscious but they are also much more stringent about what their users are able to access.

Let's compare MSP policies to non-MSP policies. Cryptomining can be found in 93% of all MSP policies, while non-MSP organizations block cryptomining in 88% of policies. Cryptomining is a simple but lesser known threat; it refers to the act of computers mining for cryptocurrency, but the real threat is resource hijacking where someone's device is overtaken to mine for cryptocurrency on behalf of a malicious actor, resulting in poor performance and high electric bills. While it is a lesser known threat, it is still a significant risk to the business. It seems MSPs are more likely to recognize this threat and put policies in place to protect their users from it.

[13] https://www.cshub.com/attacks/articles/managed-service-providers-a-gateway-for-cyber-attacks

Meanwhile, MSP policies block games in 19% of all policies, compared to 25% of non-MSP policies. Other interesting content comparisons that show the difference between what MSPs are likely to block as opposed to other organizations:

	MSPs	Non-MSPs
Blogs & Personal Sites	**8%**	**13%**
Media Sharing	**7%**	**13%**
Streaming Media	**7%**	**11%**
Shopping	**4%**	**7%**
Generative AI Tools	**3%**	**7%**

Another interesting factor are block lists: MSPs are not as likely to leverage a block list (or AppAware) as non-MSPs, possibly because they are less concerned about controlling internet access and more concerned with blocking threats.

When looking at blocked query traffic for MSPs, these are the top 10 most-blocked categories:

1. Advertising
2. Trackers Lite
3. Advertising Lite
4. Trackers
5. Proxy & Filter Avoidance
6. Block Lists & AppAware
7. Parked Sites
8. Search Engines
9. Information Technology
10. Malware

For non-MSP organizations, malware does not make the top 10 and their most-blocked category is block lists and AppAware.

It all comes down to the difference in how they use their systems and approach security. When we look at the most-trafficked categories on our network for MSPs, the majority of traffic belongs to content servers, Information Technology, Business, Social Networking, and Media Sharing (in that order). Those five categories make up nearly 80% of all traffic. The majority of those queries need to be resolved as quickly as possible, with no blocking interference.

SPOTLIGHT ON CURRENT EVENTS

2024 presented a unique set of challenges and opportunities, revealing distinct trends across our network.

MAJOR IT OUTAGES

In July, CrowdStrike suffered a global IT outage that spurred threat actors to create scam sites primarily preying on people looking to fix the problem. **DNSFilter published a list of domains** seen at this time to help those who wanted to block these very new domains that likely had not yet appeared in threat feeds.

Between July 19 and July 22, we blocked over 189,000 requests to domains with “crowdstrike” in the name that were categorized as new domains, phishing & deception, or malware—sometimes multiple categories at the same time. Traffic was low on Friday, presumably because these threat actors were registering and setting up these domains, but traffic steadily rose between July 20 and July 23, with an average of 63,000 block requests to these domains on our network between July 20 - July 22.

Important to note is that prior to July 19 on our network when looking at the entire month of July, there was no malicious traffic to domains that contained “crowdstrike” in the domain name.

Blocked Requests to Fake Crowdstrike Domains

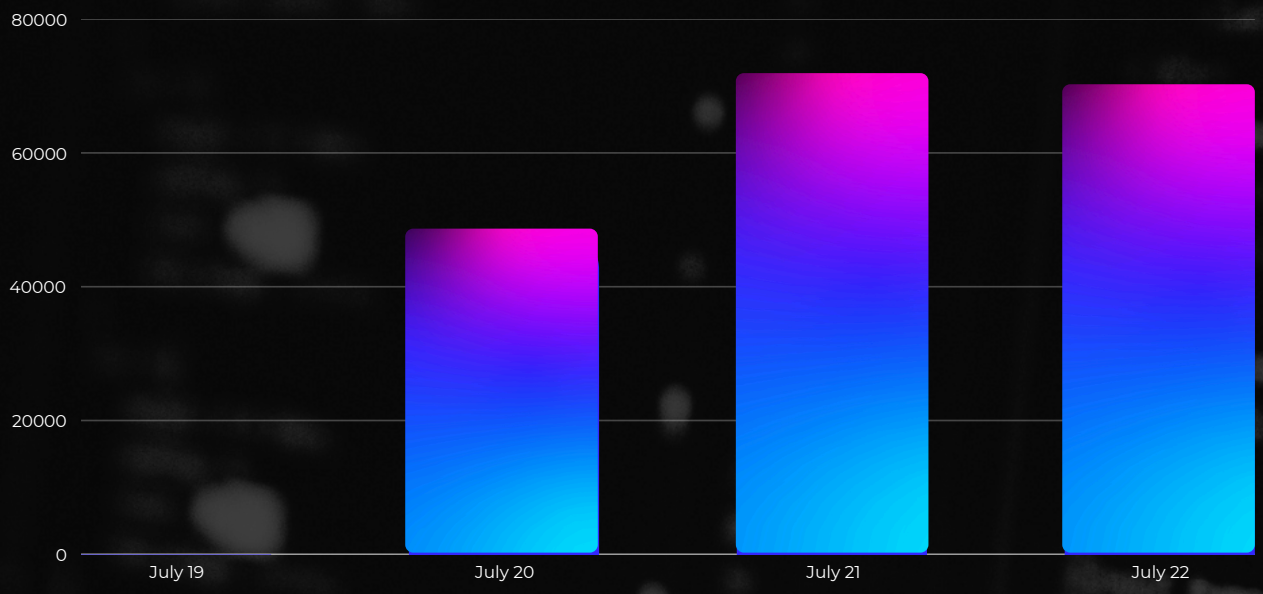


Figure 11: July data showing malicious domains with "Crowdstrike" in the domain name

A DRAMATIC HURRICANE SEASON

The National Oceanic and Atmospheric Administration (NOAA) forecast for the 2024 hurricane season between June 1 and November 10th cited an expectation that there would be an 85% chance that storms would be "above normal".[14] Hurricane Helene became the 5th strongest Atlantic hurricane, striking the southern US with unprecedented fury[15] and leaving behind damage in the range of 30.5 to 47.5 billion dollars.[16] Not two weeks later, Hurricane Milton struck in short order off the coast of Florida.

Unfortunately, malicious actors seek to leverage the emotional state of not only those actively suffering from the event, but also those wishing to contribute to the cause of restoration or reconstruction. In looking at our network:

Traffic to Malicious Domains with "Hurricane" in the Domain Name

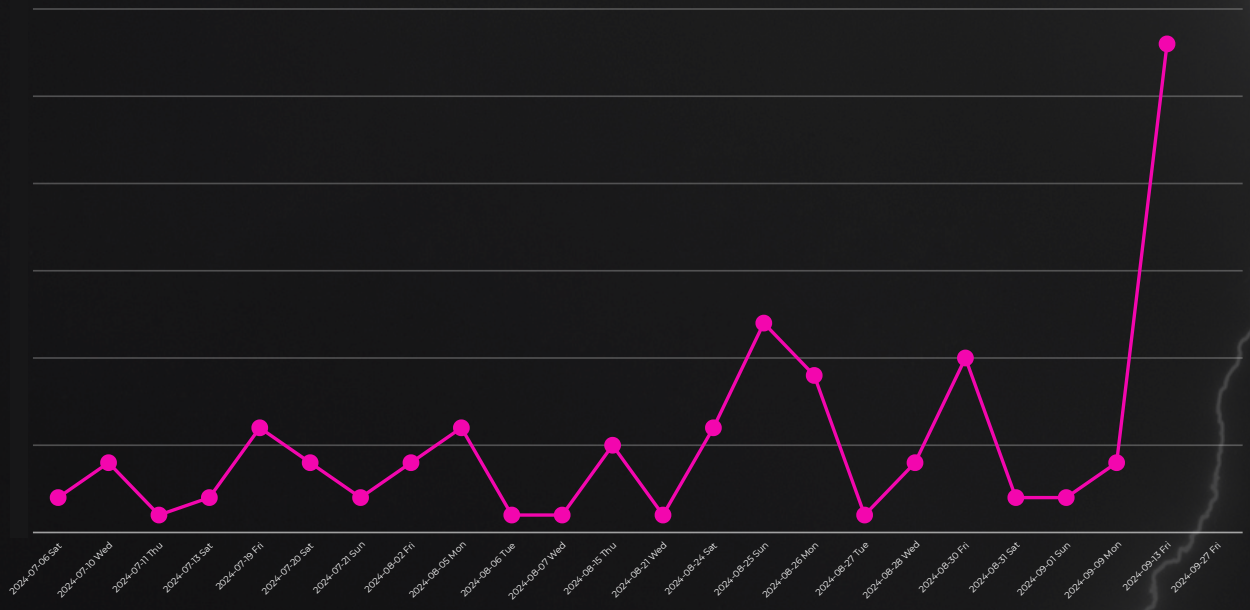


Figure 12: Malicious traffic to domains with "hurricane" in the domain name July - September 2024

We can see a definitive jump in malicious domains as Hurricane Helene was on its way to make landfall, and well after. Looking into these domains, we could see variations on unconfirmed donation requests through new third parties, personal pay links from those claiming to be victims (before Helene even landed), and other permutations on scams used to entice those sympathetic to give inordinate amounts.

[14] https://www.noaa.gov/news-release/noaa-predicts-above-normal-2024-atlantic-hurricane-season

[15] https://disasterphilanthropy.org/disasters/2024-atlantic-hurricane-season

[16] http://www.cnn.com/2024/10/07/business/property-damange-hurricane-helene-47-billion/index.html

ELECTION SEASON

Election cycles present numerous challenges that transcend political affiliation. Similar to tactics employed during wartime or periods of conflict, these deceptive schemes exploit public fatigue and manufacture a sense of urgency due to the looming election deadline. AI-driven scams, from deepfakes to phishing sites, were a huge part of the 2024 election cycle.[17]

The following is an assessment of malicious links over time including the word vote in the domain name:

Malicious domains with "Vote" in the domain name

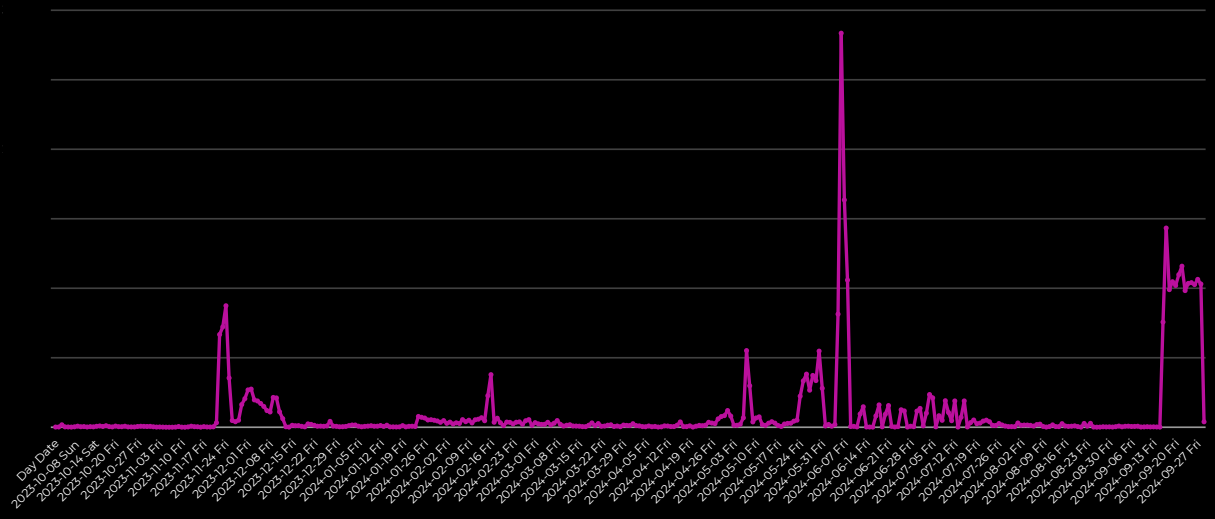


Figure 13: Malicious traffic to domains with "vote" in the domain name between October 2023 and September 2024

The peak was 27x above the daily average of domains with "vote" in the domain name over the last year. This domain was linked to by low-authority backlinks and has since been taken down. Another spike in traffic to this term occurred on September 18, which was 13x the daily average, with sustained traffic between September 17 and September 29 showing steady interest in voting-related domains in the lead up to the election.

On June 16, 2024, malicious domains with "ballot" in the domain name experienced a peak, with requests surging 74x over the daily average. This dramatic increase stands out compared to other categories, suggesting a particularly intense interest or targeted activity around ballot-related domains. The June 2024 spike in ballot-related requests could align with a documented increase in phishing scams targeting voters. According to data from Fortinet,[18] over 1,000 new election-themed, potentially malicious domains were registered in 2024, many of which aimed to deceive voters and donors through phishing schemes impersonating political campaigns and fundraising platforms. These efforts included darknet listings of phishing kits designed to harvest sensitive data from individuals interested in election-related content, a trend that coincides with the significant increase in ballot-related domain traffic observed on June 16.

[17] https://www.trendmicro.com/en_us/research/24/j/ai-election-deepfakes.html

[18] https://www.helpnetsecurity.com/2024/10/22/us-election-phishing-activity/

CONCLUSIONS

DNS, often an overlooked component of security architecture, provides critical visibility into the threat landscape. Integrating DNS data into your security posture unlocks valuable insights for Root Cause Analysis (RCA), reveals user activity patterns, and exposes network trends requiring action.

With the average user encountering 29 malicious queries daily, the need for proactive security measures is clear. Newly registered domains continue to be a significant risk vector, often exploited in conjunction with trending events to bypass traditional defenses and infiltrate our inboxes.

One area we're particularly excited about at DNSFilter is leveraging weakly supervised models to enhance security outcomes. Research from DNSFilter has shown that these AI and ML models, even with little direct supervision, can be trained to recognize subtle, early indicators of threat behaviors that conventional models may miss. Our goal with this approach is not just to respond to known threats, but to uncover potential vulnerabilities early—strengthening our customers' defenses through AI that's both efficient and far-reaching. For those interested in the specifics, our team's findings, which were presented at 2024 CAMLIS, are available in our technical white paper on this research **here**.

As AI becomes increasingly intertwined with both cyber threats and our digital lives, organizations must adopt a proactive and vigilant security posture. Leveraging the insights gleaned from DNS data, coupled with advanced AI-powered security solutions, is paramount in effectively mitigating these evolving threats and safeguarding our digital future.

BOOK YOUR DNSFILTER DEMO TODAY