DNSFilter

2024 ANNUAL SECURITY REPORT

DATA FROM OVER 25 TRILLION DNS REQUESTS

TABLE OF CONTENTS

FOREWORD

In writing the foreword for our third annual security report, I'm reminded that once again our network can be seen as a microcosm of the Internet as a whole. What happens in the real world, from trends to politics, is captured in some form across our network. In 2023, we processed over one million queries every single second. This includes innocuous business queries—the majority of our network—as well as those malicious sites that the DNSFilter system is built to protect against.

In a split second, we can see queries that fall into a variety of different categories. Gambling, malware, education and self-help, social networking, botnet—all of that traffic hits our network the same way, the only difference is what our users choose to block based on their internal, corporate policies.

AI is one theme you'll notice throughout this year's report as it was inescapable. In December of 2023, we even launched a Generative AI category to assist our customers in blocking these types of sites for better protection over PII and plagiarism.

Another feature we launched at the end of 2023 was **Malicious Domain Protection**. This feature takes a look at the domain string and was built by our labs team, which handles research and development, with the intention of discovering Domain Generation Algorithms (DGA), though it finds malicious sites outside of DGAs as well. DGAs are domain strings randomly generated and used in malware attacks, and of increasing importance to block as malware and ransomware continued to grow over the last year.

Looking forward to 2024 at DNSFilter, we will continue to follow the trends and implement changes and additions to our product to adapt to the world around us. We will be launching new filtering capabilities to give our customers tighter controls over the allowed and blocked URLs on their network, among other functionality.

As always, we will keep our ear to the ground and as new threats emerge or new patterns evolve, we will act.

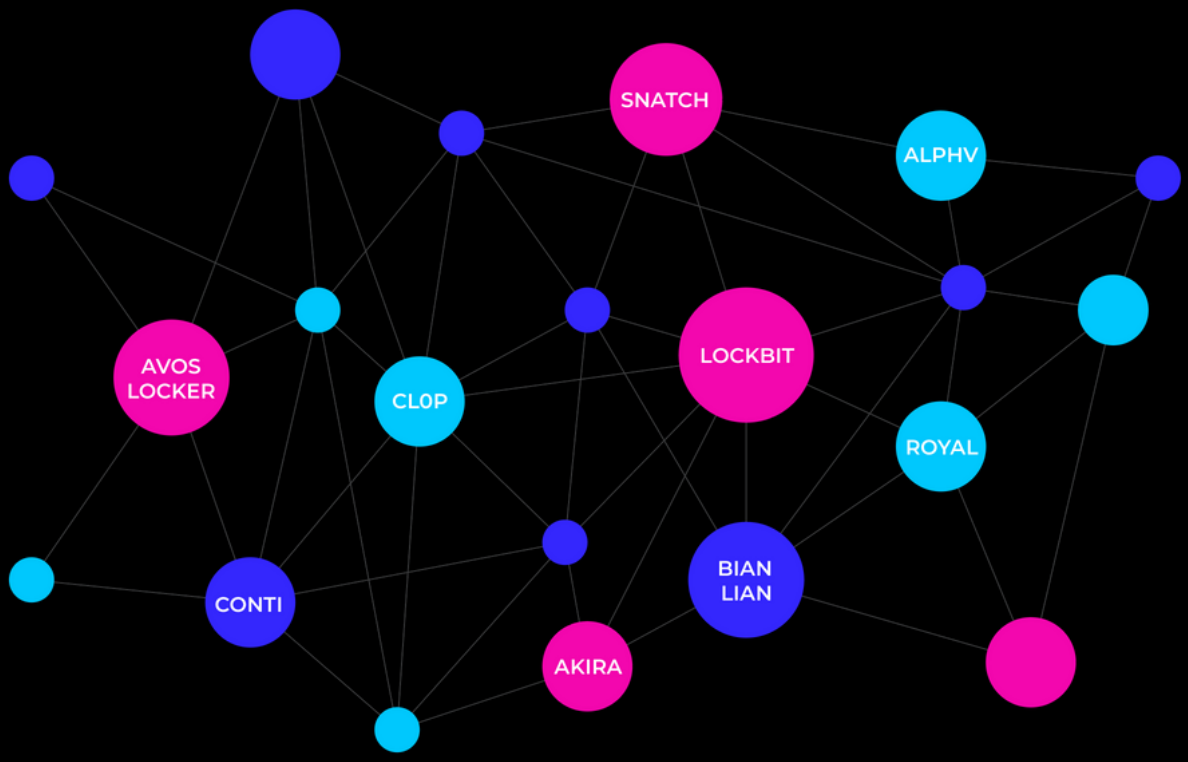
KEN **CARNESI**

CEO, DNSFILTER

2023 INDUSTRY NEWS IN REVIEW

While it is easy for us to frame the data breaches and cybersecurity incidents that occur throughout the year by the organizations they impact, there has been a greater focus by news outlets to identify threats on their own. We can say with certainty which organizations experienced a cyberattack in 2023: **Fidelity, T-Mobile (thrice), 23andMe, MGM Resorts in Las Vegas,** and countless others without the large name to make the news.

However, we can also point to the adversaries on the other side of the fence, the threat actor gangs responsible for attacks on organizations (of any size) in 2023. As of this writing, arguably the top ransomware actors of the moment are:



Roughly **65% of attacks** by these threat actors leveraged domains at some point during the attack. All of these ransomware actors heavily rely on phishing techniques, social engineering, and links to malicious websites. According to CISA, **90% of all cyberattacks start with a phishing attack**. This is why ***protective DNS*** continues to be a critical layer to secure in the modern tech stack.

The FBI and Justice Department assisted in an international takedown of Qakbot malware and botnet this year, an information-stealing malware focused on financial information that has existed since 2007.

Meanwhile, March 2023 broke records with the high number of ransomware attacks that occurred—459 attacks, which was 91% more than the previous month and 62% more than March 2022.

In the end, more focus needs to be placed on the "how" as opposed to the "who" on either side. DNS can be leveraged as a threat vector, but also as a tool for analysis, root cause or otherwise. It can feel like a game of whack-a-mole for both threat hunters and cybersecurity vendors, but by focusing on the "how" these threats are initiated, we can do a better job at protecting online users—no matter where they are.

LET'S DIG IN.

THE YEAR IN REVIEW: REFLECTIONS ON LAST YEAR'S PREDICTIONS

In last year's report, we made a few projections about what we felt the next year would bring. We were spot on with some, we had a couple of pretty close observations, and a few that weren't quite right, but we felt like the spirit of the vision was preserved. The events of this year were a strange intersection of much more of the same in terms of threat actors and much of the threat landscape, but in other ways, particularly the ubiquity of GenAI, the playing field has changed drastically. These are our assessments of how we did with last year's predictions.

MAJOR PLAYERS INCREASE THEIR STAKES

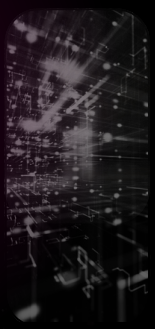
...Attackers are getting more efficient, and more careful as well in the wake of major disruption events such as the Colonial Pipeline attack and the Kaseya attack. They are looking to gain more success over a longer period and across broader targets with the hopes of staying under the radar. This will be the ideal state moving forward for the foreseeable future.

With the exception of some unexpected major disruption activities from international law enforcement this year, it would have been hard to be more accurate here. There was so much "more of the same" that the threat actors who had seemingly gone away resurfaced and rose to the top as if they'd never slowed down. With the exception of a few high profile attacks (such as the MGM hack, or the breaches by USDoD (the threat actor, not the government agency), and the bothersome DDoS outages claimed by Anonymous Sudan, the entire year seemed to be encapsulated by the numbers getting bigger and the threat actors doing everything they could to stay under the radar (except stopping). Threat actors were able to maximize their paydays without drawing too much attention to themselves.

THE DEATH OF ATTRIBUTION (AS A SERVICE)

Outside of targeted Nation-State attacks, which require a certain degree of focus and control, the modern enterprising attacker is looking to outsource their efforts. Specialized services are going to be cheap, reliable ways to achieve the various stages of the attack lifecycle. ...“Attribution” as a concept may end up pointing to several different teams, if they can be uniquely identified at all. Outside of cybersecurity research, law enforcement, geopolitics, and international diplomacy, it’s not going to yield much value anymore. Maybe it’s time to devalue the effort behind “who” and focus more energy on stopping the “how.”

This probably should have been a hope more than a wish—after all, the attribution of who carried out an attack should matter less than the remediation and the “how”. Attribution continues to get more difficult as attackers share more tools and resort to Living-Off-The-Land techniques. However, the desire to have that attribution will not subside. A trend that has been seen this year, presumably in order to feed that desire, has been to report early attribution before it’s really determined, but to hedge the risk as being “suspected” or “alleged” or “preliminary.” Still, as far as predictions go, this would technically be a miss. Yes, attribution is getting harder, and the need for it arguably dwindles, but there are many still clinging to the need to announce who was behind which cybersecurity event.. There’s no reason to believe it’s going to change any time soon.



THE THREAT OF THE YEAR WON’T BE FROM THIS YEAR

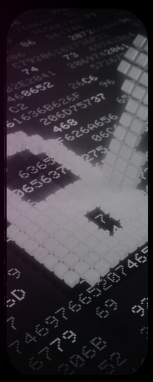
Some of the most memorable, troublesome, and difficult attacks of the last few years have been based in software that has been around for a long time, sometimes decades. Software libraries, log management systems, and ancient network protocols—that were perhaps created when software development was less of a rigorous engineering discipline and security was less of a concern—have all been recently exploited to disastrous effect. ...If widely trusted and widely used applications, protocols, and libraries are exploited, it will result in a panicked scramble to find a solution and distribute it.

This should probably count as a wash—it wasn’t really wrong, but it was right for some of the wrong reasons. Some of the biggest news stories (outside of the clamor for all things Generative AI), were centered around low-tech attacks, and probably most notable among them being social engineering. Ransomware and phishing still stood strong in the world of cyber threats, and plenty of new vulnerabilities were discovered and reported, but it seemed like every time a story started to get really scary, it was a case of more of the same. Social engineering, password reuse, unsecured databases—rinse and repeat.

JUST ANOTHER LINK IN THE CHAIN

Cascading attacks are where it's at. If an attacker can compromise a supply chain provider, a Managed Service Provider (MSP), cloud provider, or other consolidated platform aggregator then it's like hitting the lottery. ...Supply chain businesses will continue to have a huge target on their backs, and the smallest gap in the armor will trigger a frenzy. More of these attacks are almost sure to occur.

MSP-focused attacks are definitely a regular occurrence, but they didn't evolve into a major watershed for the war against cyber attacks. Instead, they just seemed to rise in prominence just far enough to blend in with the greater cyber threat landscape as another aspect of the attack surface. Likewise, software supply chains, and specifically software libraries, similarly failed to achieve notoriety largely simply because they just get lost in their own noise. There's a new story about a compromised npm library, or an imposter application, or some vulnerability found in a shared protocol seemingly every week. This seems to hit the mark as a prediction, especially when we take into account some **findings from Huntress** in 2023 where in 65% of incidents they monitored, "threat actors used RMM software as a method for persistence or remote access mechanisms following initial access."



HOW I LEARNED TO STOP WORRYING AND LOVE ENCRYPTION

Encrypted traffic is bursting to find its stride. It looks to be poised to move as encrypted browser traffic, whether over DoT, DoH, DoQ or some other standard collides with needs for privacy around the world at a time when blockchain technologies are continuing to mature and emerge in markets other than cryptocurrency. Blockchain technologies, for instance, will certainly continue to evolve into several different emerging technologies and provide new solutions to difficult problems moving into the future. ...This arms race will emerge to new levels with increasing innovation into expectant and emergent technological vistas.

This one ended up being a relatively big swing and a miss. Encrypted DNS traffic continues to be a topic of discussion, and privacy is always a critical issue, but 2023 didn't see much in the way of actual change and growth.

Both Firefox and Chrome have established that their default behavior is DoH where the model is supported, and have held that position for a few years now. Firefox moved to automatic DoH in 2018 and Chrome in late 2019. At the time, DoH traffic was around 1% of DNS traffic. Since that time, it certainly hasn't taken over the world, but reports put their estimates at between 8-10% of traffic.

However, there doesn't seem to be a lot of public engagement with the topic anymore. It's almost like the outside world collectively shrugged its shoulders once the browsers embraced default encrypted DNS where applicable, but if there is going to be any major seismic shift, it's going to have to be solely on the efforts of the security community to carry that burden.

TRENDS AND ANALYSIS: DATA IN MOTION

THE BIG PICTURE

The percent of threat queries on our network increased significantly in 2023—**nearly doubling by the end of Q3 2023 with huge spikes in January and February.**

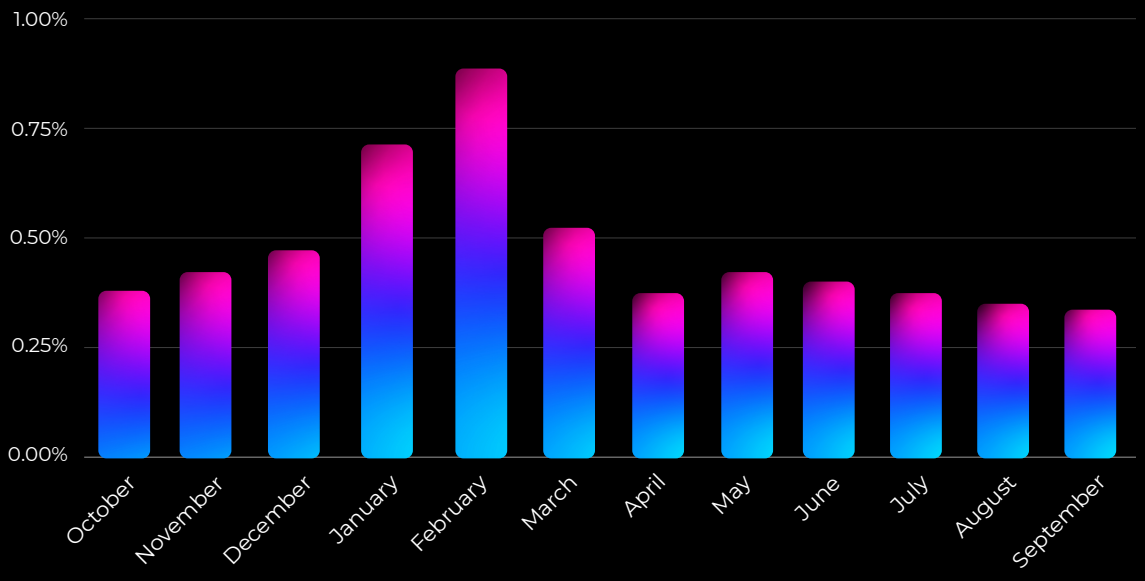


Figure 1. Percent of threat queries out of total queries on the DNSFilter network October 2022 - September 2023

As mentioned in the introduction, March was prolific in terms of the number of ransomware attacks that occurred during those 31 days. However, the spike in malicious traffic on the DNSFilter network occurred in that 60-day period before March. It's possible that this spike shows when these campaigns were active, whereas March is when the ransomware was launched and the footholds were initially made known.

However, the number of domains out of the total on our network per month tells a slightly different story:

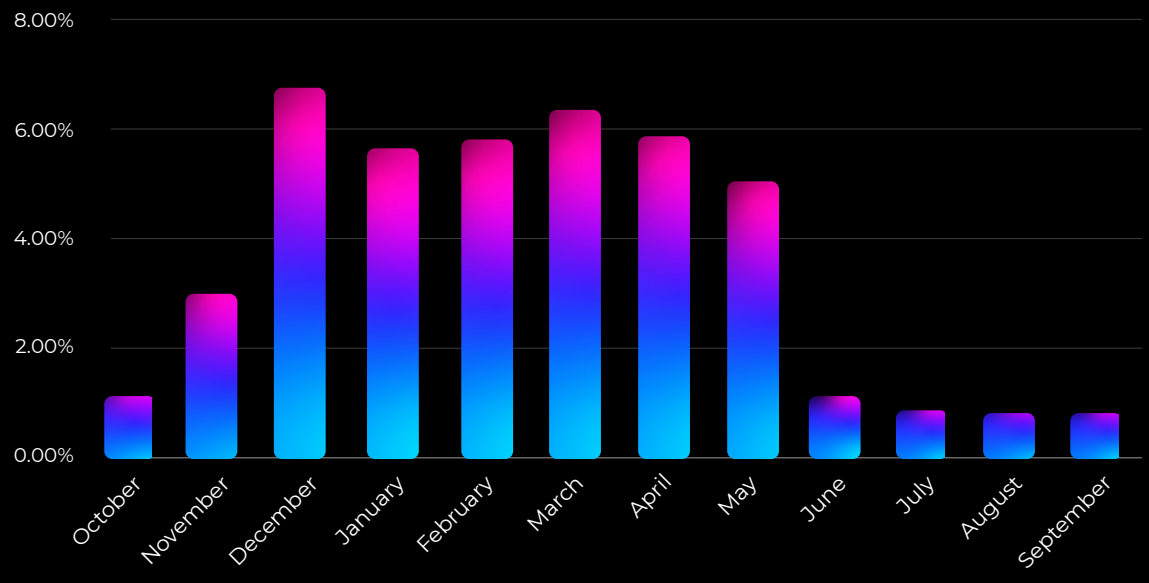


Figure 2. Percent of threat domains out of total domains on the DNSFilter network October 2022 - September 2023

It seems that there was a greater variety of malicious domains on our network peaking in December 2022 and remaining relatively consistent through May before dropping very low in June and holding steady through September 2023.

December 2022 had the highest prevalence of threat queries and it remained relatively constant through May 2023 until there was a massive dropoff beginning in June 2023. This means that a fewer number of domains were doing more of the work in June - September, signaling more organization by the threat actors launching these attacks, and matching a slightly lower total threat count as well.

Across the entire year, the breakdown of threat queries on our network looks like this:

GRAND TOTAL OF THREAT QUERIES (INCLUDING PROXY CATEGORY)

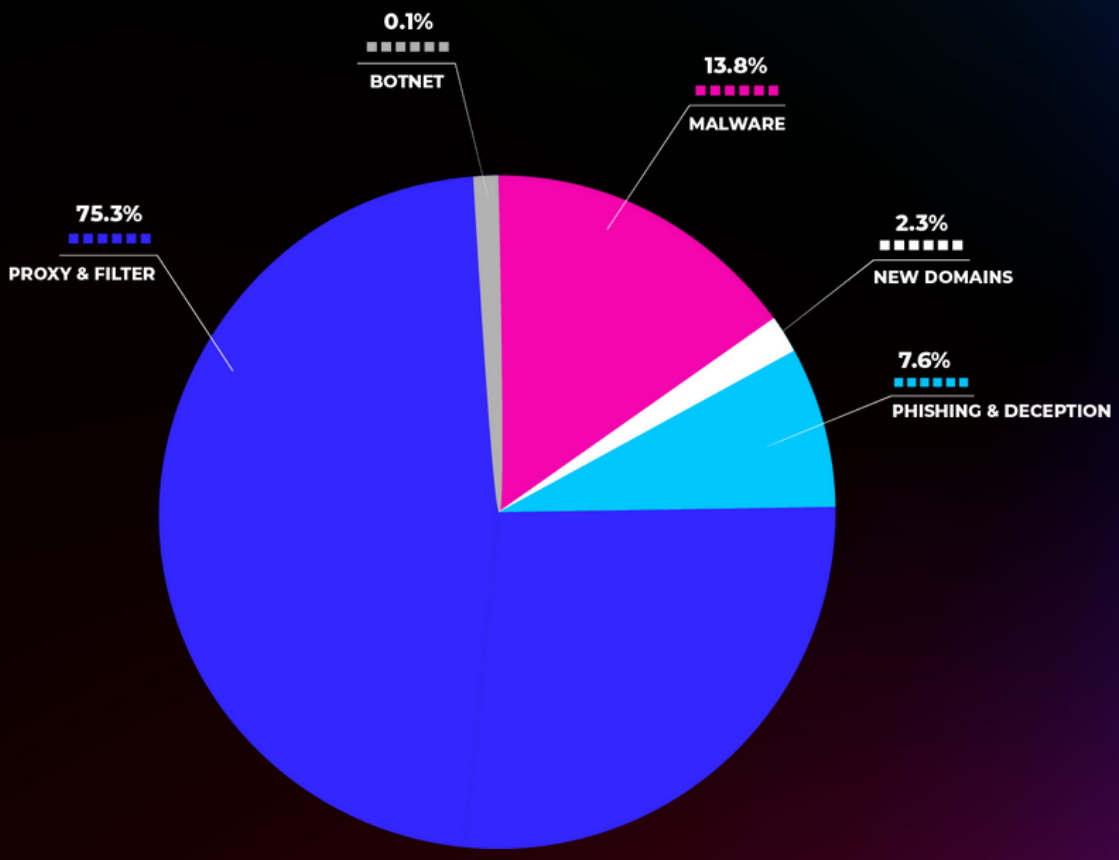


Figure 3

If we remove proxy & filter avoidance, knowing it is the largest threat category and can obscure the other categories, the breakdown looks like this:

GRAND TOTAL OF THREAT QUERIES (EXCLUDING PROXY CATEGORY)

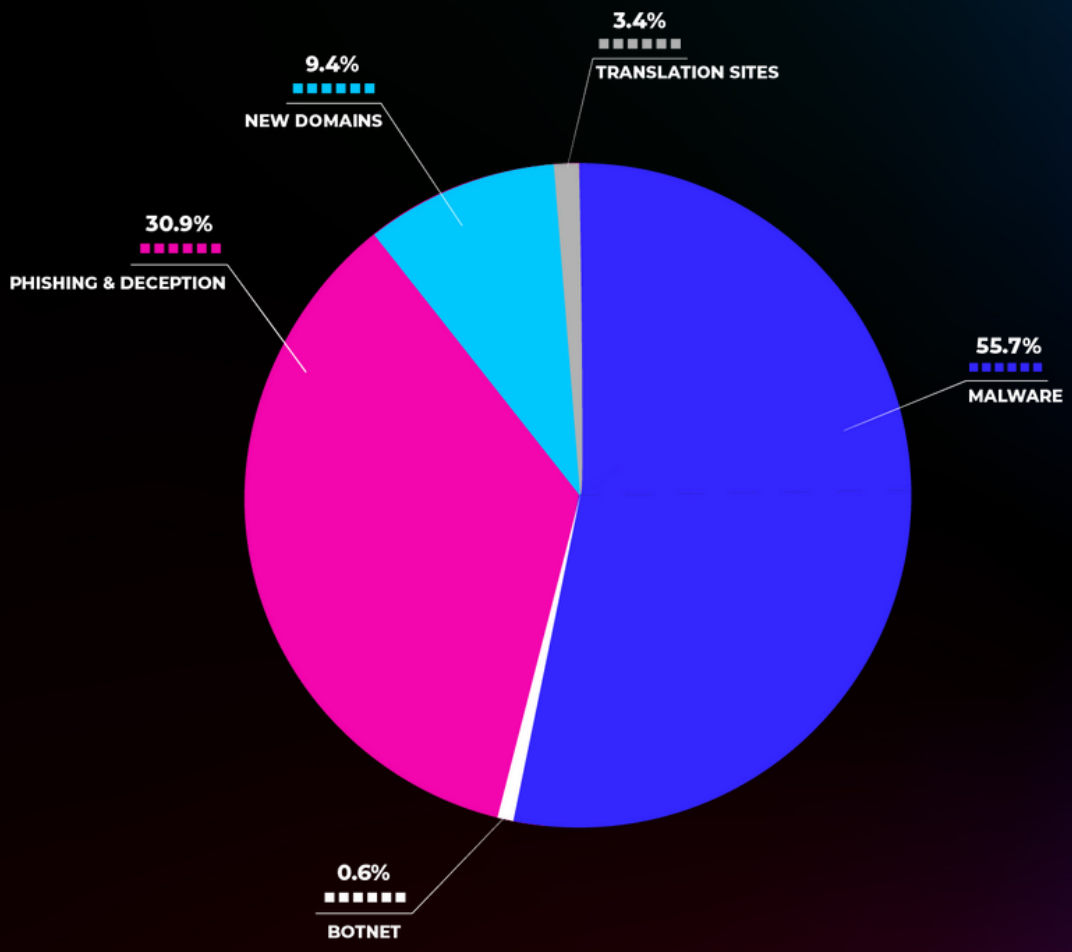


Figure 4

But what if we just look at the unique domain count?

GRAND TOTAL OF DISTINCT DOMAINS (INCLUDING PROXY CATEGORY)

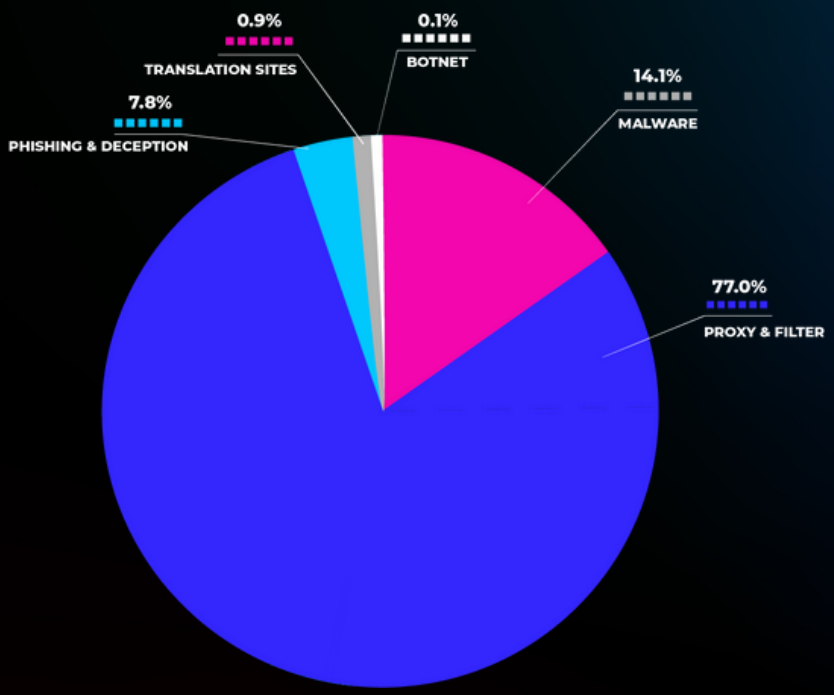


Figure 5

Without it:

GRAND TOTAL OF DISTINCT DOMAINS (EXCLUDING PROXY CATEGORY)

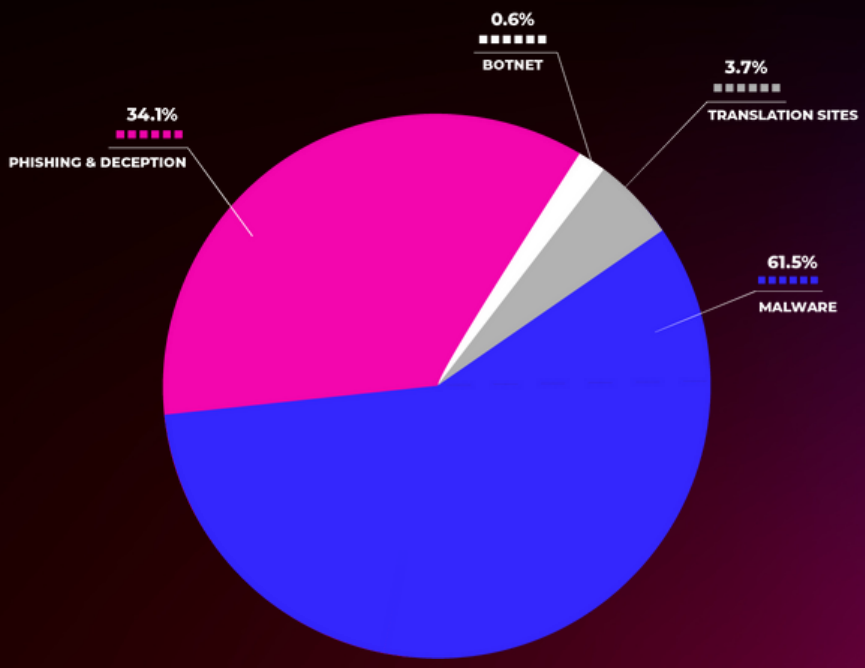


Figure 6

While the query count does not necessarily always correlate to the count of domains within a certain category, these charts show that a large amount of domains were responsible for the large amount of malware threat queries. This is indicative of threat actors leveraging unique malware domains for dedicated tactics, and the breadth of malware that is out there.

New threats are always emerging, but as new threats emerge and old ones disappear, they can be queried thousands or millions of times, infecting a myriad of networks, before transforming and relaunching under a new domain.

COMPARING TO THE PREVIOUS YEAR

A comparison between the detection rates for 2022 versus 2023 are shown below in Figure 7. In each of our primary security categories, we noted a significant increase in activity across the board, except in blocks by the “New Domain" category. Botnets increased detections by 32%, Malware detections increased by 40%, Phishing detections increased by 106%, and blocks for Very New Domains, which are malicious domains registered within the previous 24 hours, increased by a shocking 1250%. This however, when compared to the status for blocks for “New Domains”, which decreased by 10%, indicates that the health for the categories is more in line with reality. The disparity between values for the two categories should be reasonably linear since they observe the same data, except one is for one day (24 hours) and the other is for 30 days. This year, those actual values for blocks exist at almost exactly a 1:10 ratio, which would indicate that much of the malicious activity is detected by the block on the first day of registration, but also that the same threat is being carried for longer and is still active at the 30-day mark.

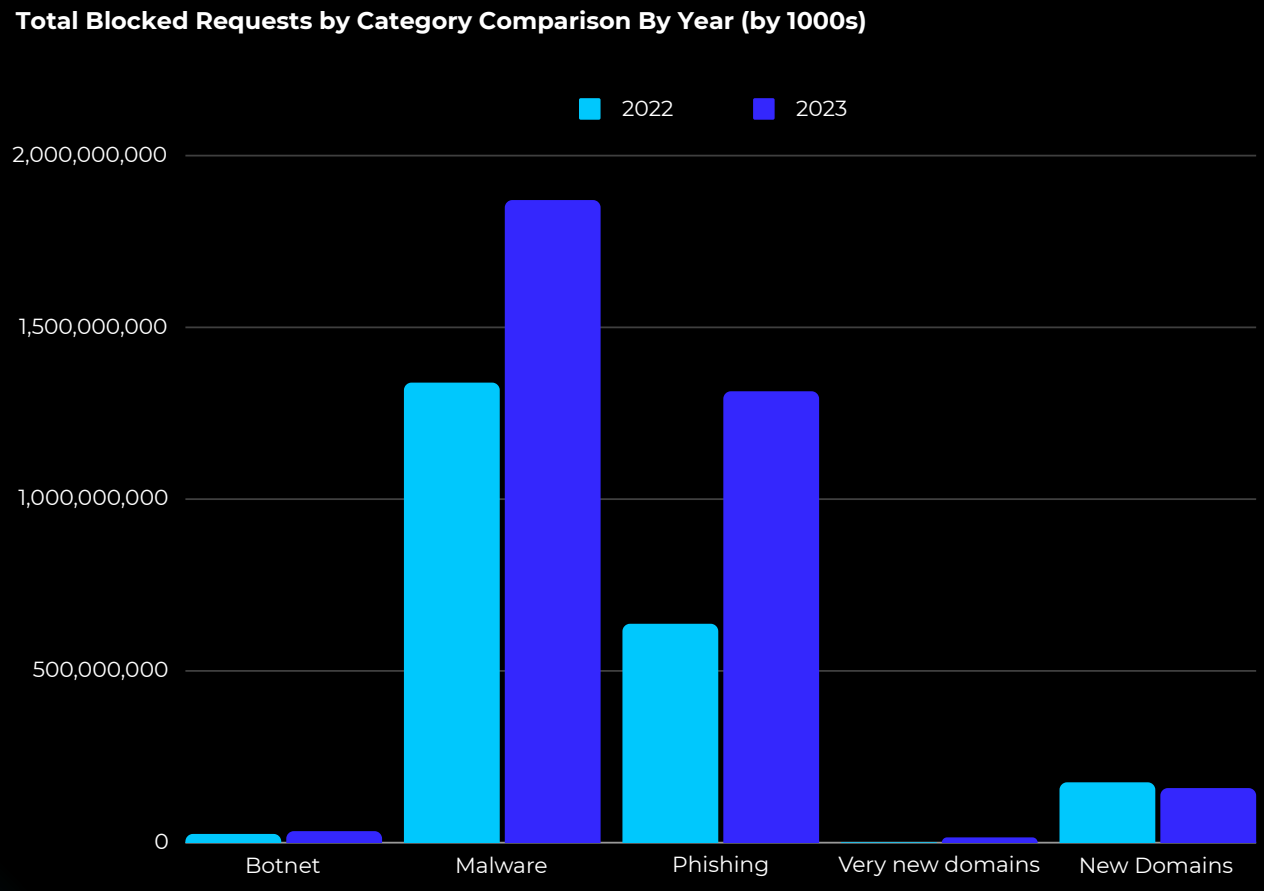


Figure 7. Side-by-Side Comparison of Total Blocks in 2023 Per Security Category Versus the Same Categories in 2022. Vertical Scale Is Divided by 1000 For Readability.

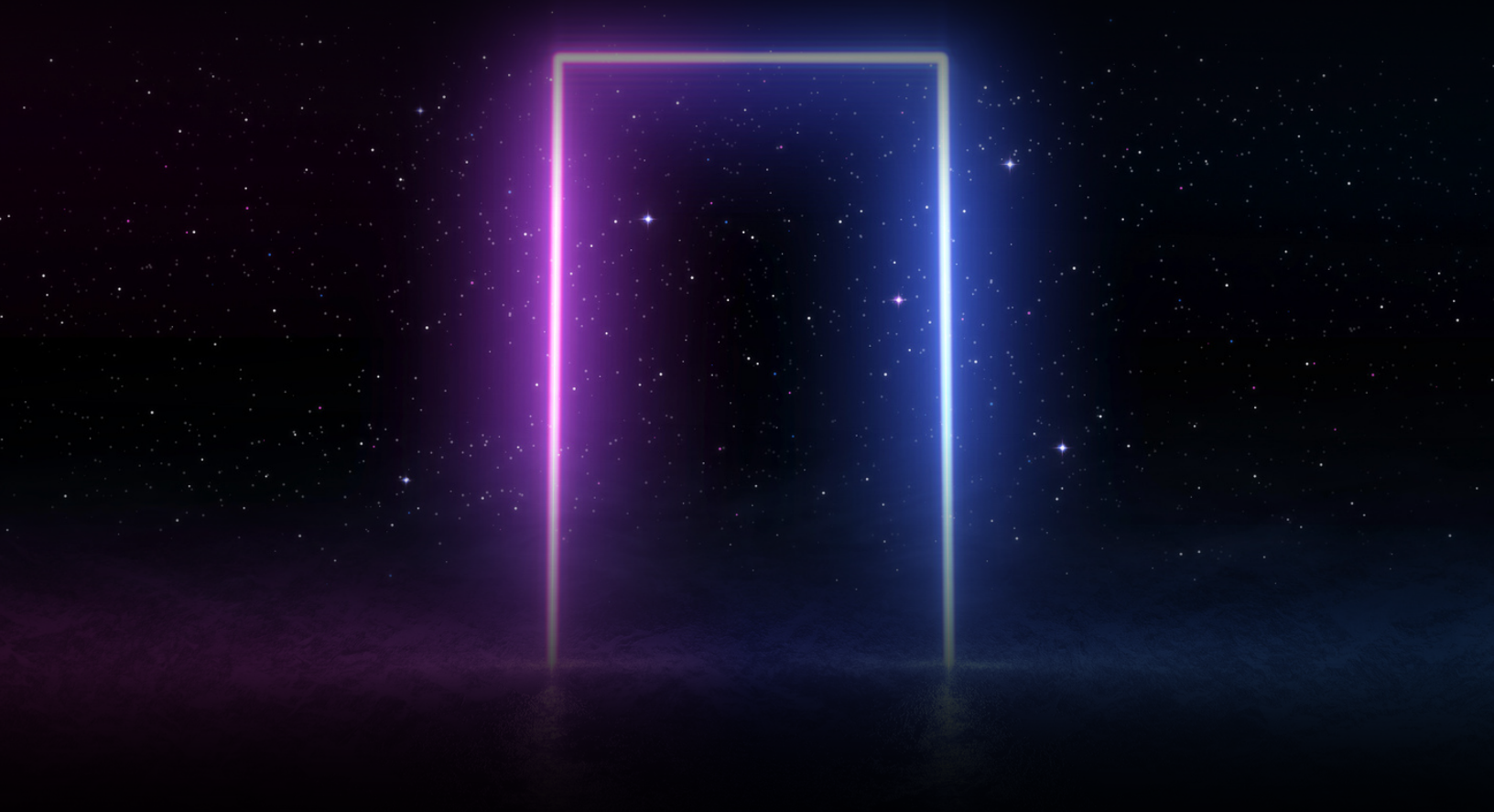
HOW OFTEN IS THE AVERAGE PERSON ENCOUNTERING A THREAT?

Some people exhibit riskier behaviors than others, putting them at a higher threat risk. While others might be power users and encounter far more threats than the average person simply because they're engaging with more of the Internet—a larger variety of domains means a larger likelihood of encountering threats.

On average, many of our users access roughly 5,000 queries per day. In our research, we've found that for every ~1,000 queries more than one of them is likely to be malicious.

The average user is likely to encounter 5 malicious queries per day—or 1,825 every year.

Meanwhile, 2 out of every 100 domains on our network are found to be malicious in some way, proving that there are a large amount of malicious domains doing a small fraction of the work for threat actors.



LLMS, AI, AND THE RISE OF CHATGPT

It's undeniable that 2023 was the year that AI caught its stride. Though the trend, largely centered around Large Language Models and Generative Artificial Intelligence, really began when the release of DALL-E 2 was opened to everyone and the waitlist requirement was removed in September 2022, the explosive growth of the industry, including widespread adoption and the evolution of a competitive environment, continued throughout 2023.

The chart below shows the explosive growth we have seen at DNSFilter in terms of requests to the common GenAI domains on our architecture for the year between September 2022 and September 2023. In the first chart, the singular growth of OpenAI's ChatGPT platform and its related domains renders a distorted flattening of representation of its competitors, demonstrating its popularity and market dominance.

That being the case, another representation is made in the next figure demonstrating the number of DNS queries observed for each of the other popular GenAI domains with the results for OpenAI removed. This results in a more representative display of the activity of the industry. There are clearly delineated surges that indicate the public launch of Google's Bard.ai and Anthropic's Claude.ai, as well as a significant spike in the number of requests for Midjourney that corresponds with its launch of the alpha release of Version 5 in March 2023.

Figure 8. The Breakdown of Total DNS Requests for GenAI Domains for One Year

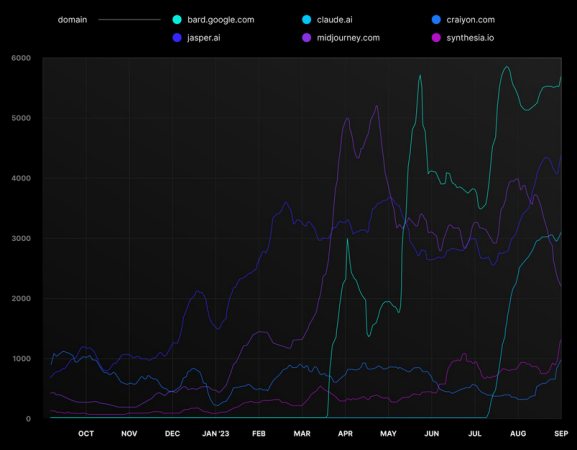


Figure 9. Total DNS Requests for GenAI Domains Excluding OpenAI

There was a 279% increase in GenAI sites accessed on the DNSFilter network between January 2023 and August 2023 when including ChatGPT. When excluding ChatGPT from that list of the top seven AI sites, the delta is more staggering with a 326% increase in traffic to those sites. While ChatGPT gained early popularity, these other sites truly took off deeper into 2023.

The popularity and versatility of these easy-to-use tools quickly evolved beyond toys and found their way into everyday life in unexpected ways. Probably the most expected first step was that students used them to write their homework, which led to an arms race for teachers to be able to detect such activities. But then authors started using them to flood the entire market with AI-generated works and articles, writers and actors went on months-long strikes to protect their scripts and their likenesses from studios working to find more cost-effective approaches. Music was being generated, even in ways that were difficult to discern from original copyrighted works. And lawyers even tried to use them to draft legal briefs. Somewhere along the way with each innovative use, the world began to learn about another potential problem: When the AI returns unexpected and inaccurate results. The term “AI Hallucination" began to enter the common vernacular.

Despite the obstacles, the continuous expansion of AI into every aspect of the tech industry marched on unabated as companies sought to introduce an AI aspect to their products, or release an AI product of their own. Meta was in the latter group, announcing the release of a suite of AI tools, but withholding their voice-synthesis product because it made it too easy to create realistic voice-impressions that could be used in deepfakes and other malicious ways, according to their own reports. It would be impossible to list all of the companies who incorporated AI, but SalesForce, NVidia, Microsoft, Slack, Samsung and Accenture are all examples of companies who launched entire campaigns to advertise their inclusion of AI in their platforms.

Not to be left out, cyber threat actors took advantage of the opportunity as well. WormGPT, FraudGPT, and DarkBERT malicious AI tool sets were all publicly announced. Attacking vulnerabilities in AI, and even using AI to attack other AI, became a common topic. Phishing actors have leveraged GenAI heavily to improve the accuracy of their attacks, hoping that the improvements in quality result in an increase in success. And deepfakes as a source of dis- and misinformation have already seen real-world usage in what is sure to be an increasingly problematic trend.

CRYPTOCURRENCY

TThe news around cryptocurrencies in 2023 has been anything but comforting. By January, the flagship token, Bitcoin, had lost almost three quarters of its high-water-mark value in a matter of months, tumbling from $67,617.02 per coin on November 16th to $16,540.69 on January 1st[1]. While some of that value has been recovered over the span of the year ($27,967.51/BTC as of this writing), it's still a bitter position, and the year has been fraught with setbacks and challenges along the way.

Even professional investors had difficulty with the volatility of the market with approximately 13% of crypto-based hedge funds permanently closing their doors[2]. The FBI executed a series of cryptocurrency seizures throughout the year: $112M in April[3], they shutdown nine entire exchanges in May[4], grabbed almost another $2M over the span of June, July, and August[5], and had totalled 39 various seizures over the course of the year (through the end of September)[6].

Reverberations are still being felt throughout the cryptocurrency world after the collapse of FTX cryptocurrency exchange in late 2022, as well as the sanctions against Suex, Tornado Cash, HydraMarket, Garantex, BitRiver, and Blender.io by the US Treasury Department, but there are still strong interests in cryptocurrency, and there are no signals that a permanent ban against using them is anywhere on the horizon. Still, there is cause for a healthy concern while dealing with cryptocurrency. If the issues we've mentioned already aren't enough to warrant careful consideration, there are still major ties to malicious threat actors in the industry, with between 0.12% and 1.90% of transactions being tied to criminal activity[7]. That may not seem like much, but the 0.24% that was reported for 2022 translated to $20.1B[8].

An interesting question presents itself when one considers where the threats are found. Obviously, different organizations use different criteria for attribution of malice to crypto-related activity. What we've found when we look at our own internal data is that a very high volume of the traffic we see with cryptocurrency domain requests is for domains associated with malware and botnets.

[1] https://ycharts.com/indicators/bitcoin_price
[2] https://news.bloomberglaw.com/crypto/crypto-hedge-funds-hit-by-shutdowns-lagging-returns-in-2023
[3] https://www.justice.gov/opa/pr/justice-department-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes
[4] https://www.bleepingcomputer.com/news/security/fbi-seizes-9-crypto-exchanges-used-to-launder-ransomware-payments/
[5] https://cointelegraph.com/news/crypto-fbi-seizes-almost-2-m-in-crypto-assets-in-three-months
[6] https://www.cutoday.info/Fresh-Today/FBI-Increasingly-Seizing-Cryptocurrency-From-Criminal-Enterprises
[7] https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/
[8] ibid.

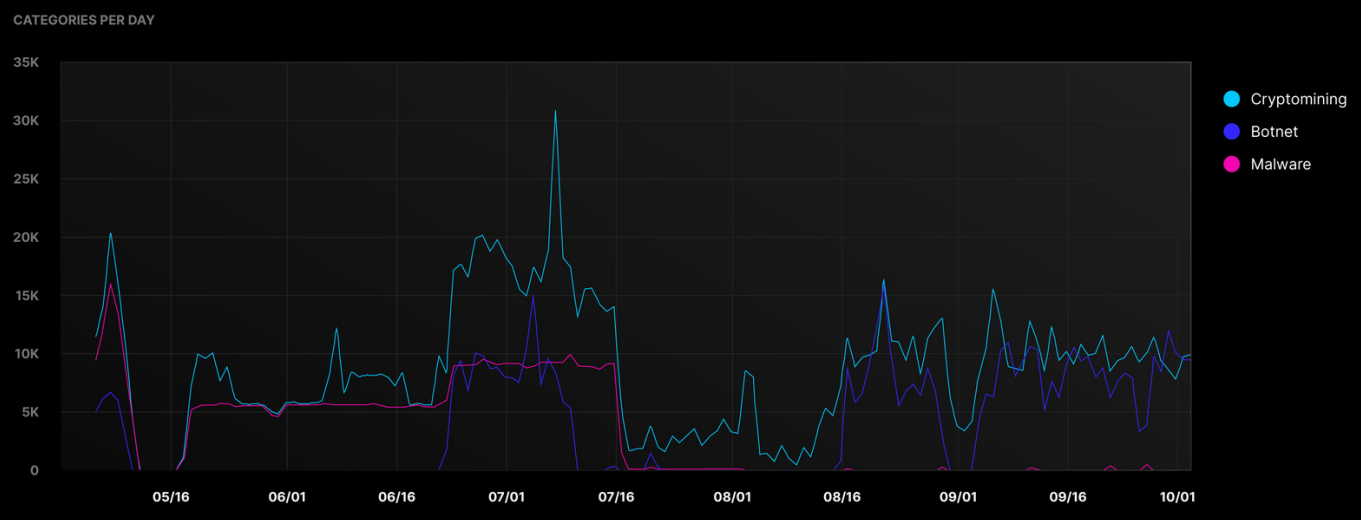


Figure 10. Total Cryptocurrency Domain Requests v. Cryptocurrency Domain Requests with Malware and Botnet Classifications (May - Sept 2023, Source: DNSFilter Labs Research)

As can be seen in the diagram above, there is a very close similarity between the trends for all cryptocurrency domains and malicious cryptocurrency domains. Spikes in activity occur with a very high correlation between both Malware classifications and Botnet classifications. It is important to note that a domain can carry more than one of these classifications simultaneously, so it is possible, and even likely, that there is some overlap between the lists. However, the chart shapes between Malware classifications and Botnet classifications are not often similar in shape or period, which would suggest that the effects are largely independent, and thus also likely cumulative. Even considered separately, however, when there is a high level of requests for cryptocurrency domains on our servers, there are also correlated spikes in activity to cryptocurrency domains associated with bad actors. This is highly suggestive that the majority, and maybe even the vast majority, of the domain requests we get with cryptocurrency are related to dangerous activity, and that a large increase at any given time holds a strong likelihood of being part of a potential scam or campaign by a bad actor.

Dealing in cryptocurrencies is not inherently bad, however, in looking at these issues, risks, and analyses, it does carry a high degree of risk. If you choose to participate in that sector, it should be approached with a great deal of caution and significant due diligence. From a position of corporate network security, it would be an unnecessary risk, and we would highly advise blocking cryptocurrency categorized domains on your devices unless you have a clear justification to do otherwise.

THREATS BY REGION

DNSFilter hosts a robust, worldwide anycast network which gives us unique insight into which areas have the most active threat activity. Here, we examine just our botnet, cryptomining, malware, and phishing & deception categories and which of our servers receive which type of traffic. The following data shows where the query was resolved, which may indicate close proximity to the initial origin of the threat. However, it is possible that threats originating on one side of the globe are resolved in a completely different hemisphere.

Looking at the raw query data, Chicago and Dallas were in the top three malicious regions on our network. 53% of the malicious queries in Chicago were categorized as malware between Q4 2022 - Q3 2023. Frankfurt, Germany had the highest raw count of malicious queries, with the region being responsible for over 44% of all malicious queries on our network. Chicago was responsible for close to 10% while Dallas was responsible for roughly 9% of malicious queries.

However when we look at the number of malicious queries on each regional network as a whole, these are the servers on our network that encounter the most threat domains:

	Total Malicious Queries	Top Threat Category
Santiago, Chile	4.23%	**Phishing & Deception** 99.24% of all threats within this region
Singapore	.51%	**Malware** 74% of all threats within this region
Frankfurt, Germany	.25%	**Malware** 85% of all threats within this region
Vienna, Austria	.17%	**Phishing & Deception** 72% of all threats within this region

Top region for each threat category:

Botnet	**Copenhagen, Denmark*** 8% of all threats within this region
Cryptomining	**Milan, Italy*** 5% of all threats within this region
Malware	**Frankfurt, Germany** 85% of all threats within this region
Phishing & Deception	**Santiago, Chile** 99% of all threats within this region

**Note: Fortaleza, Brazil had the highest distribution of botnet and cryptomining threats within its region but the numbers were significantly lower than the other regions and removed for statistical significance.*

Phishing continues to be the most popular threat on our network, with the majority of regions seeing a high volume of phishing queries compared to other threats with malware a close second.

TLD ANALYSIS

We observed a number of very interesting trends in the focus of Top Level Domain (TLD) blocks this year. Across the board, our number of total DNS requests increased, but the raw number of blocked domains in many of them stayed near constant or even went down. Some of that can be attributed to the increases that we did see in other TLDs, but there is also a significant shift toward custom TLDs – a trend that we observed in some capacity last year.

This year, in an effort to better refine the analysis of the threat landscape, we also examined the percentage of blocked requests with respect to the total number of requests for that TLD. For the purposes of this report, we are combining the blocks that are a result of a reported security threat with the blocks that are part of the local policy. For our internal analysis, we did review the types of block separately, but we don't have room to print them all here. If you would like to review that data as well, please submit your request to **help@dnsfilter.com**.

AVERAGE TOTAL BLOCKED REQUESTS PER DAY BY CCTLD

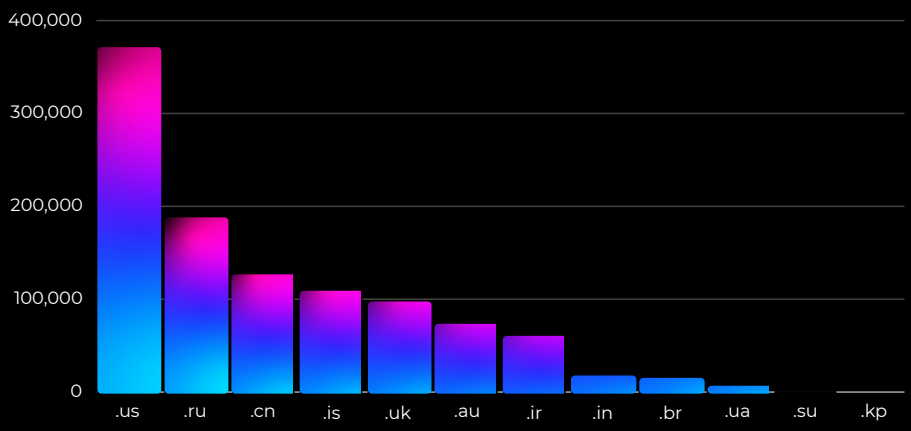


Figure 11. Histogram of the Average Number of DNS Requests Blocked by Major Country Code Top-Level Domains Per Day

AVERAGE DAILY PERCENTAGE OF BLOCKED REQUESTS BY CCTLD

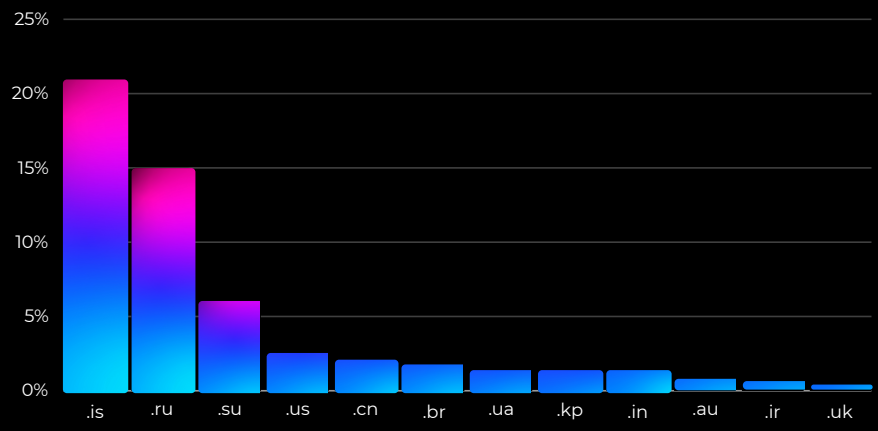


Figure 12. Histogram of the Average Percentage of DNS Requests Blocked by Major Country Code Top-Level Domains Per Day

AVERAGE TOTAL BLOCKED REQUESTS PER DAY BY GTLD

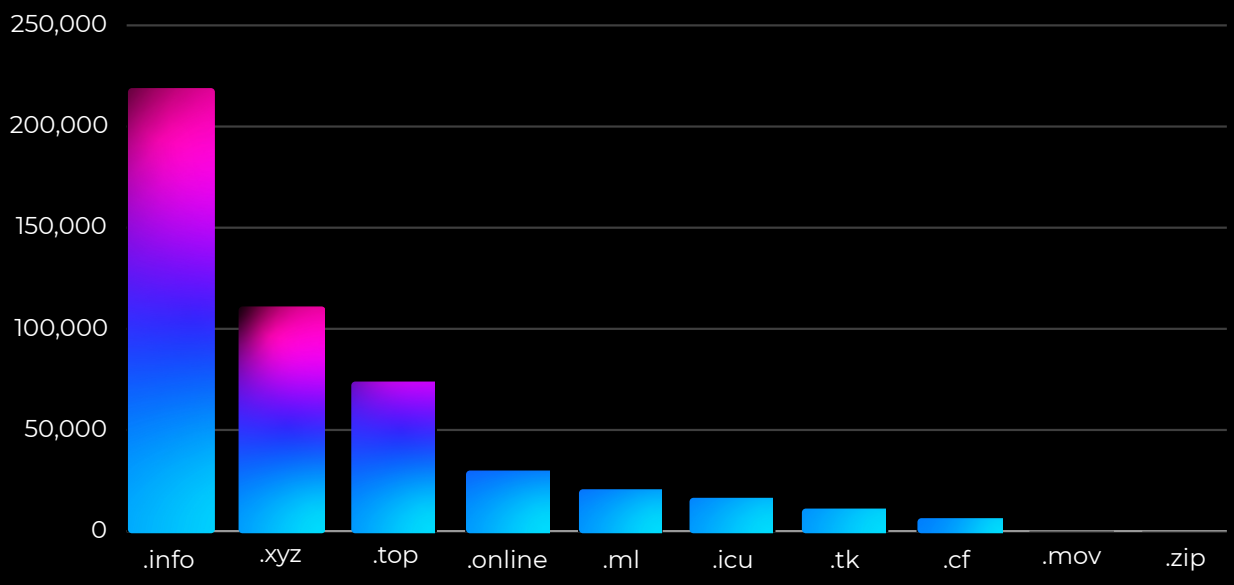


Figure 13. Histogram of the Average Number of DNS Requests Blocked by Major Generic Top-Level Domains Per Day (Excluding .com, .org, .net, and .gov)

AVERAGE DAILY PERCENTAGE OF BLOCKED REQUESTS BY GTLD

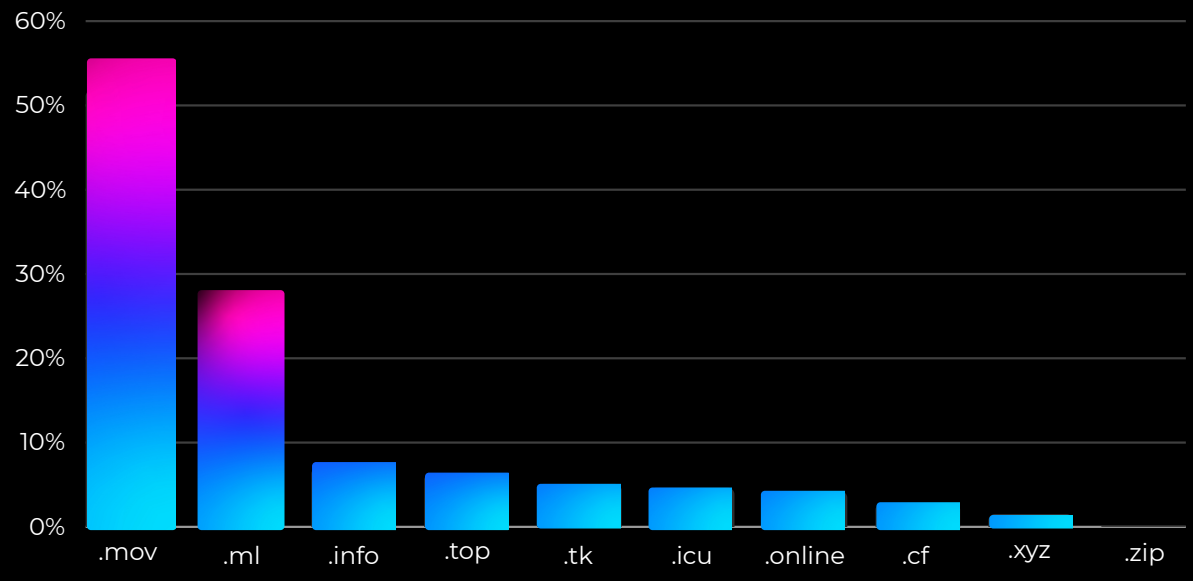


Figure 14. Histogram of the Average Percentage of DNS Requests Blocked by Major Generic Top-Level Domains Per Day (Excluding .com, .org, .net, and .gov)

THE FUTURESCAPE IN CYBERSECURITY: PROJECTIONS FOR THE COMING YEAR

Generative AI became a household term this year. Ask anyone on the street and they'll be able to tell you what ChatGPT is. We recognize that saying artificial intelligence is going to be a major topic this year seems a bit lazy. It's kind of like saying that threat actors are going to write more malware or there are going to be more ransomware attacks this year. But the potential uses (or misuses) of AI will continue to grow exponentially in new ways throughout 2024—which is precisely why our predictions are all AI-themed.

GENERATIVE AI IS GOING TO MAKE A MALWARE MESS

The AI craze doesn't show any signs of slowing down, and malware groups tend to stay on the forefront of major events—but they tend to do so without a lot of guardrails. This lack of attention to detail is going to lead to a situation where attacker AI will perform unexpectedly, and will break containment in ways that were not originally intended.

DEEPFAKES WILL BE LEVERAGED DURING ELECTION SEASON

Deepfakes and artificially generated computer content is already reaching a level where it is difficult to detect without a fair amount of scrutiny. In one report, the use of deepfakes grew in North America a staggering 1740%. Deepfakes will act as a force multiplier for adversarial governments with the intent to sow chaos in the current political climate in the United States. With some resources already diverted to other international operations, it will be irresistible to capitalize on such tools to crank out effective campaigns that require very few personnel. While not the first to signal the possibility of the use of deepfakes during election season, we do think the 2024 cycle will be unlike anything we've seen before.

RUSHED GENAI IMPLEMENTATION AS A THREAT VECTOR

There is an inherent flaw in artificial intelligence as a business tool in that it almost certainly requires allowances for imprecise behaviors. In other words, there are parts of the model that are working in ways that are not known at any specific point in time. The business world, including the cybersecurity industry, is in a rush to leverage the popularity of generative AI and many companies are going to implement AI in ways that they don't have fine control over, and threat actors are going to take advantage of that ripe attack surface in every way they can find.

AI REGULATION WILL COME TOO LATE

It's commendable that governments around the world have realized the potential danger that unregulated artificial intelligence could pose in every industry given its meteoric rise in popularity and endless flexibility. Unfortunately, legislation and regulation tends to move very slowly, while technology tends to evolve at an ever-accelerating pace. Further compounding the issues, slow-moving governments are trying to catch up to an emergent technology that already has a great deal of inertia. Governments are going to aim their regulations at a target that has already moved, and will be unprepared to adapt to the genie that is already out of its lamp

CONCLUSIONS

In the spirit of 2024's predictions, the following conclusion was written with the help of ChatGPT:

In conclusion, this year's annual security report underscores the critical significance of understanding domain-based threats and the pivotal role of DNS queries in safeguarding digital infrastructure. The escalating sophistication of cyber threats has reiterated the need for robust defense mechanisms to counteract malicious activities targeting domains and exploiting vulnerabilities within DNS systems.

The comprehensive analysis presented in this report has highlighted the evolving landscape of domain-based threats, emphasizing the importance of proactive measures and continual vigilance. From phishing attacks and malware propagation to DNS tunneling and domain hijacking, the spectrum of threats remains diverse and adaptable, posing persistent challenges to organizational security.

Moreover, the correlation between increased DNS queries and potential risks demands a multifaceted approach, encompassing advanced monitoring, threat intelligence integration, DNS security enhancements, and robust incident response strategies. It's crucial for organizations to prioritize investment in cutting-edge technologies, regular audits, and employee training to fortify defenses against emerging threats.

As the digital ecosystem evolves, collaboration and information sharing among industry peers, cybersecurity experts, and regulatory bodies will be pivotal in fortifying global cybersecurity posture against domain-based threats. By fostering a culture of awareness, resilience, and swift response, organizations can effectively mitigate risks and secure their domains, ensuring the integrity and confidentiality of critical data and systems.

Moving forward, a proactive and adaptive stance will be indispensable in countering the ever-evolving domain-based threatscape. By leveraging insights gleaned from this report and embracing a comprehensive security approach, organizations can navigate the intricacies of DNS-related vulnerabilities, fortify their defenses, and proactively mitigate risks in an increasingly complex digital environment.

...We couldn't agree more, ChatGPT.

GLOSSARY

+AI - Artificial Intelligence

+BERT - Bidirectional Encoder Representations from Transformers

+BTC - Bitcoin

+ccTLD - Country Code Top-Level Domain

+CISA - Cybersecurity and Infrastructure Security Agency

CSAM - Child Sexual Abuse Material

+DDoS - Distributed Denial of Service

+Deepfake - A computer-generated or computer-altered image, video, or audio file designed to falsely impersonate a real person or scene, typically for the purpose of mis- or disinformation

+DGA - Domain Generation Algorithm

+DNS - Domain Name Service

+DoH - DNS Over HTTP/S

+DoQ - DNS Over QUIC

+DoT - DNS Over TLS

+GenAI - Generative Artificial Intelligence

+GPT - Generative Pre-Trained Transformers

+gTLD - Generic TLD, an umbrella for a spectrum of topics. Includes .com, .net, .org, etc.

+HTTP/S - HTTP stands for HyperText Transfer Protocol. HTTPS is HTTP Secure

ICANN - The Internet Corporation for Assigned Names and Numbers

+LLM - Large Language Model

+MSP - Managed Service Provider

+QUIC - Quick UDP Internet Connections protocol

+RMM - Remote Monitoring and Management

+TLD - Top Level Domain

+TLS - Transport Layer Security

CITATIONS/ SOURCES

https://www.dnsfilter.com/blog/malicious-domain-protection

https://www.jdsupra.com/legalnews/cybersecurity-incident-at-fidelity-9850811/

https://www.darkreading.com/application-security/t-mobile-third-consumer-data-exposure-2023

https://blog.23andme.com/articles/addressing-data-security-concerns

https://www.cnn.com/2023/10/05/business/mgm-100-million-hit-data-breach/index.html

https://www.egress.com/blog/phishing/phishing-statistics-round-up

https://www.cisa.gov/stopransomware/general-information

https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown

https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot

https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/

https://www.huntress.com/hubfs/SMB-Threat-Report-Huntress.pdf

https://www.npr.org/2023/02/24/1159286436/ai-chatbot-chatgpt-magazine-clarkesworld-artificial-intelligence

https://www.dnsfilter.com/blog/unreliable-narrators-hallucinations-may-be-causing-your-generative-ai-tools-to-lie-to-you

https://ycharts.com/indicators/bitcoin_price

https://news.bloomberglaw.com/crypto/crypto-hedge-funds-hit-by-shutdowns-lagging-returns-in-2023

https://www.justice.gov/opa/pr/justice-department-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes

https://www.bleepingcomputer.com/news/security/fbi-seizes-9-crypto-exchanges-used-to-launder-ransomware-payments/

https://cointelegraph.com/news/crypto-fbi-seizes-almost-2-m-in-crypto-assets-in-three-months

https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/

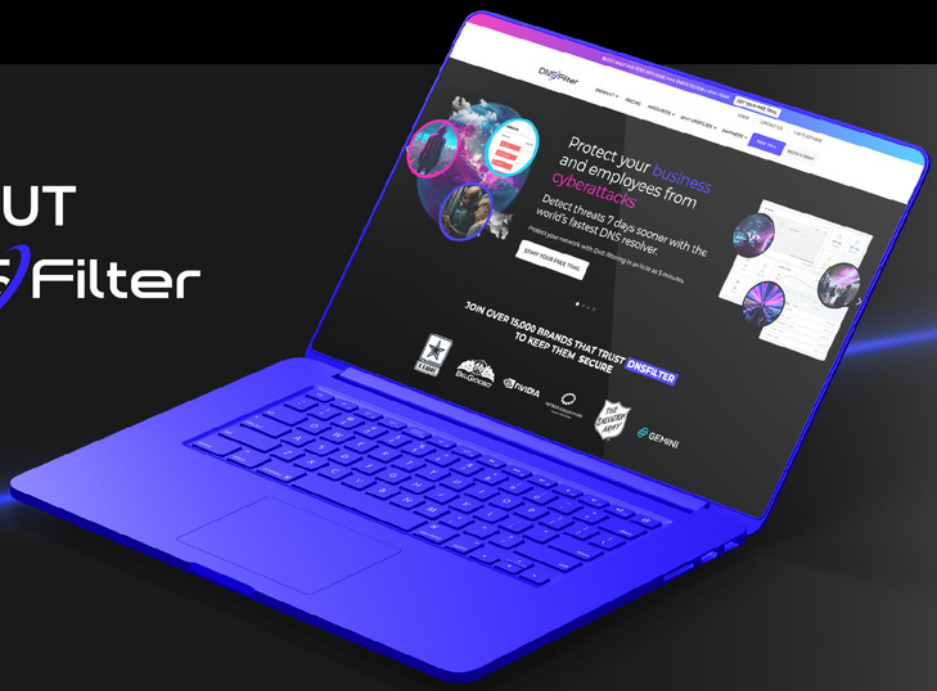
https://www.cutoday.info/Fresh-Today/FBI-Increasingly-Seizing-Cryptocurrency-From-Criminal-Enterprises

https://www.infosecurity-magazine.com/news/deepfake-identity-fraud-surges/

https://www.wired.com/story/chatgpt-generative-ai-deepfake-2024-us-presidential-election/

SUMMARY

ABOUT DNSFilter



DNSFilter is redefining how organizations secure their largest threat vector: the Internet itself. DNSFilter is making the internet safer and workplaces more secure. Through Q3 of 2023 alone, DNSFilter blocked over 24 billion attempts to access threats. With 70% of attacks involving the Domain Name System (DNS) layer, DNSFilter provides Protective DNS powered by machine learning that uniquely identifies 61% more threats than competitors on an average of seven days earlier, including zero-day attacks.

Over 26 million monthly users trust DNSFilter to protect them from phishing, malware, and advanced cyber threats.

DNSFilter's brands include Webshrinker, its next generation web categorization software and Guardian, a consumer app focused on privacy protection.

GET A FREE TRIAL TODAY