WhoisXMLAPI

Global Domain Activity Report

Q3 2023

Dear reader,

I am pleased to present the Q3 2023 Global Domain Activity Report, which sheds light on the recent behaviors of domain registrants around the world.

In today's increasingly interconnected world, it is more important than ever to gain and maintain visibility into the domain landscape.

I encourage you to review this report and share the findings relevant to you and your team.

Together, we can create a safer and more secure digital world.

Jonathan Zhang

CEO of WHOIS API Inc.,
doing business as WhoisXML API

Find me on LinkedIn

Table of contents

Executive Summary

Hundreds of thousands of domain names are registered every day, a reflection of the growing global digital economy and massive ongoing digital transformation.

In this quarterly report, we aim to give you a snapshot of the recent prevalent trends in domain registration, both legitimate and suspicious, for popular generic top-level domains (gTLDs) and country code top-level domains (ccTLDs).

1. Newly Registered and Expired Domains by TLD Type

- This section offers a detailed breakdown of domains registered and expired, broken down by top top-level domain (TLD) type.

2. New Domain Activity: gTLD Trends

- Uncover the most sought-after gTLDs in Q3 2023.

3. New Domain Activity: ccTLD Trends

- Explore the ccTLDs that generated significant domain activity in the third quarter.

4. Looking at Inconsistencies between Selected ccTLDs and Registrant Countries

- An analysis of the ccTLDs and their registrant countries.

5. Decoding the TLDs of Potential Phishing Threats

- Anticipate and mitigate phishing with a detailed analysis of TLDs associated with potential malicious activity.

6. Potential Phishing Trends: Which Industries Are Targeted?

- Gain insights into industry-related phishing risks.

7. Analyzing Malicious gTLD Domains

- Leverage Threat Intelligence Data Feeds to identify known malicious activities by gTLD.

8. Analyzing Malicious ccTLD Domains

- Leverage Threat Intelligence Data Feeds to identify known malicious activities by ccTLD.

Methodology Overview

To compile this report, we leveraged advanced WhoisXML API datasets relevant to each facet of the analysis.

Specifically, our trusted Newly Registered Domains solution gave us an overview of new global domain activities.

We tracked the pulse of newly registered domains in Q3 2023 to gain insights into the current domain landscape and identify trends and patterns in domain ownership, administration, and location.

In the field of predictive threat intelligence, our Early Warning Phishing Feed took center stage. The feed delivered up-to-date intelligence on possible upcoming phishing campaigns, enabling timely and predictive threat analysis.

For insights into malicious activities, our comprehensive Threat Intelligence Data Feeds was employed, providing a wealth of data about known malicious indicators. That allowed us to perform a detailed examination of the threat landscape spanning July 1–September 30.

Q3 2023 Findings

Your access to exclusive domain data begins now

Newly Registered and Expired Domains by TLD Type

Every day, thousands of new domains are registered while others expire. It is the natural ebb and flow in a landscape where new businesses emerge daily.

In Q3, about 305,000 domains were registered daily, while a little more than that (around 330,000 daily) were left to expire.

Specifically, we found 14% more domains under gTLDs that expired than there were added.

But this was reversed for domains under ccTLDs, as we found 7% more newly registered than expired domains.

Added/Registered

	July	August	September	**Total**
gTLD	**5,442,407**	**5,445,978**	**7,527,483**	**18,415,868**
ccTLD	**2,357,334**	**2,331,963**	**5,038,082**	**9,727,379**

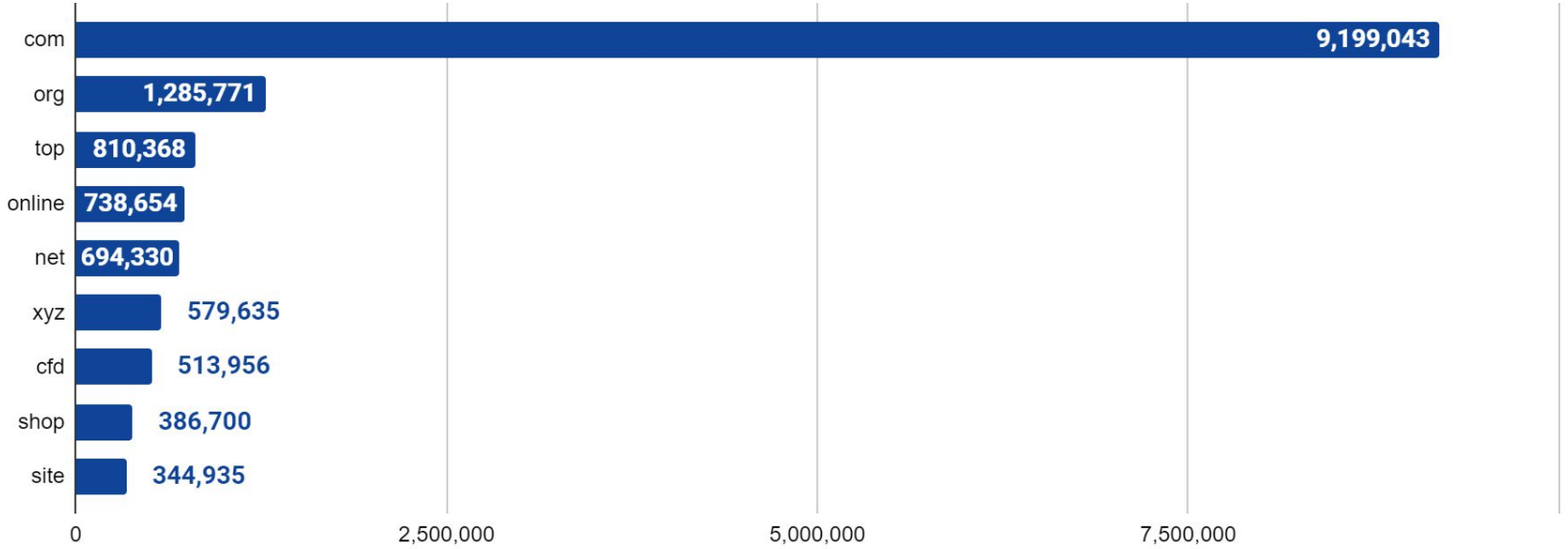
Expired/Dropped

	July	August	September	**Total**
gTLD	**7,009,789**	**7,150,738**	**7,109,170**	**21,269,697**
ccTLD	**3,003,074**	**3,599,483**	**2,482,434**	**9,084,991**

Intelligence source: Newly Registered Domains

New Domain Activity: gTLD Trends

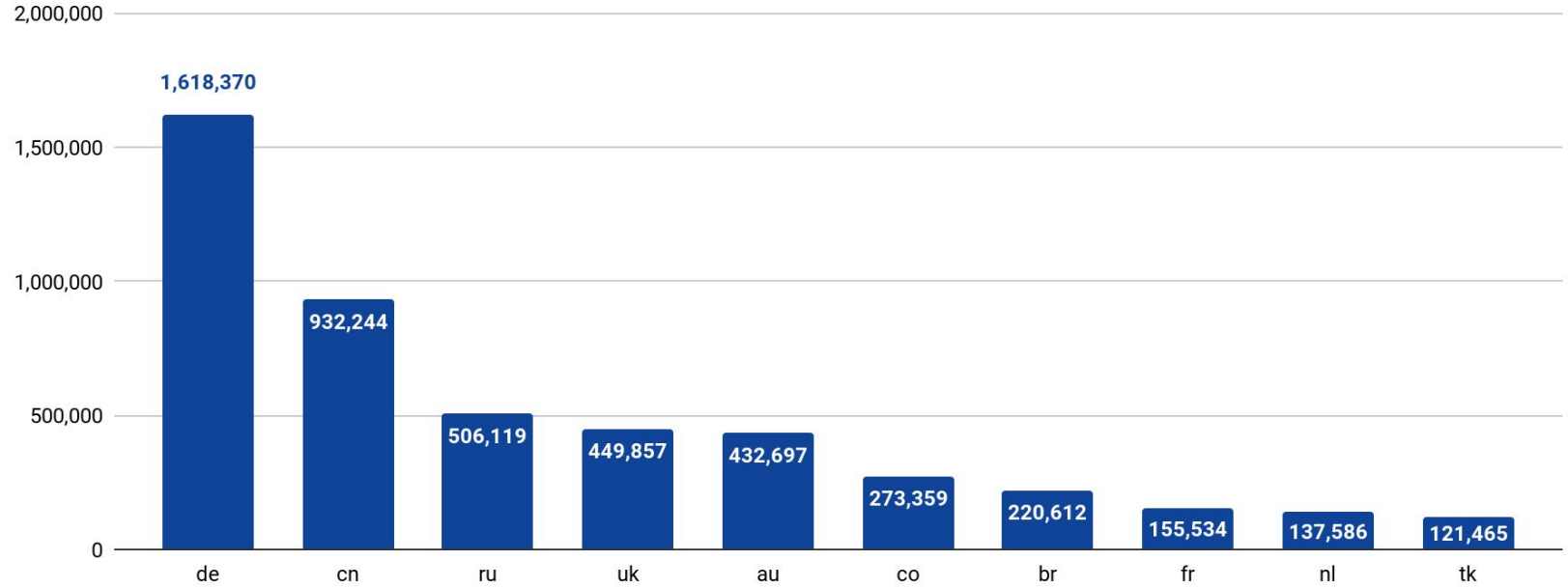
In the daily surge of domain registrations, certain gTLDs are more popular than others. For instance, the frequency of new domain registrations that sported the .com extension in Q3 2023 was significantly higher than that for the other gTLDs on the list. That is not exactly surprising, as .com domains are sought after by individuals and businesses around the world.



Intelligence source: Newly Registered Domains

New Domain Activity: ccTLD Trends

When it came to ccTLDs, Germany (.de), China (.cn), Russia (.ru), the U.K. (.uk), Australia (.au), Colombia (.co), Brazil (.br), France (.fr), the Netherlands (.nl), and Tokelau (.tk) secured the top 10 spots. Are businesses and entrepreneurs in these countries localizing their online presence? Or are there other forces at play?



Intelligence source: Newly Registered Domains

Looking at Inconsistencies between Selected ccTLDs and Registrant Countries

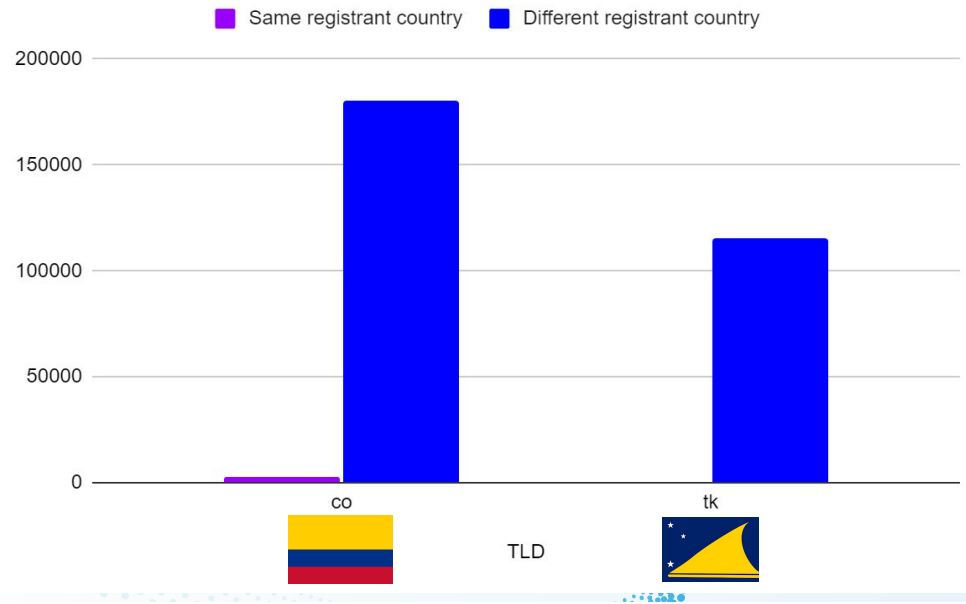
In connection to the previous question, we looked at the registrant countries of the domains sporting two of the most popular ccTLDs—.co and .tk.

If a legitimate entity or individual registers a domain using a given ccTLD, we might expect the registrant to be located in the corresponding country. Of course, some exceptions, such as when the registrant employs a foreign domain privacy service, will occur.

However, the results of our analysis for .co and .tk showed that very few registrants were seemingly from the countries.

In fact, only 1% of the .co registrants mentioned Colombia as their registrant country, indicating that the ccTLD may be used for other purposes. After all, .co resembles .com and it also hints at terms like “company” or “corporation.”

Therefore, .co could have been used by registrants willing to demonstrate their presence as an established company or simply as an alternative should the extension .com already be in use for a domain string of interest.



Meanwhile, Tokelau’s ccTLD domain activity seemed enormous, as 121,000 domains were added in Q3 alone, while the territory’s entire population is estimated to only be 1,900 as of this writing.

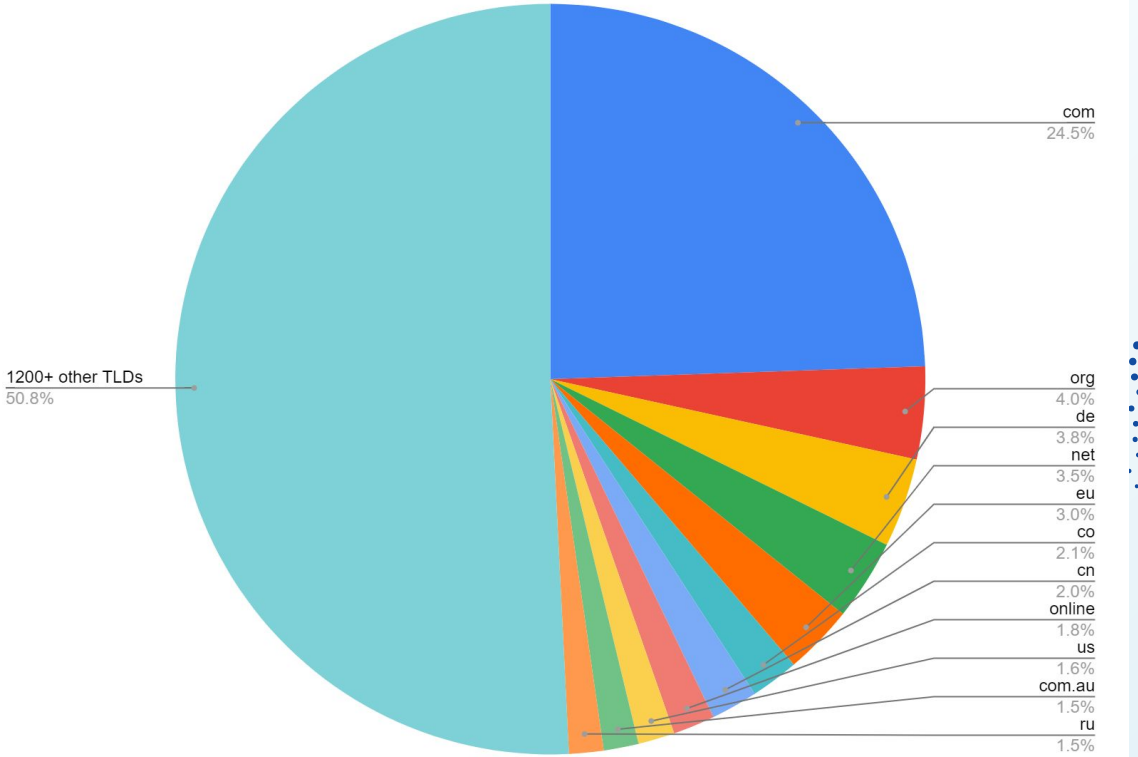
Intelligence source: Newly Registered Domains

Decoding the TLDs of Potential Phishing Threats

Next, we zoomed in on the domains bearing a close resemblance to those belonging to popular companies, brands, and strings by downloading the Early Warning Phishing Feed files for Q3 2023.

These domains can be used in phishing campaigns where threat actors imitate famous entities. Coupled with widely used TLDs, these domains could be powerful threat vectors.

While no TLD is immune to phishing, our analysis shows that nearly half of the potential phishing domains found for Q3 2023 used popular TLDs, including gTLDs like .com and .org and ccTLDs like .de and .eu.

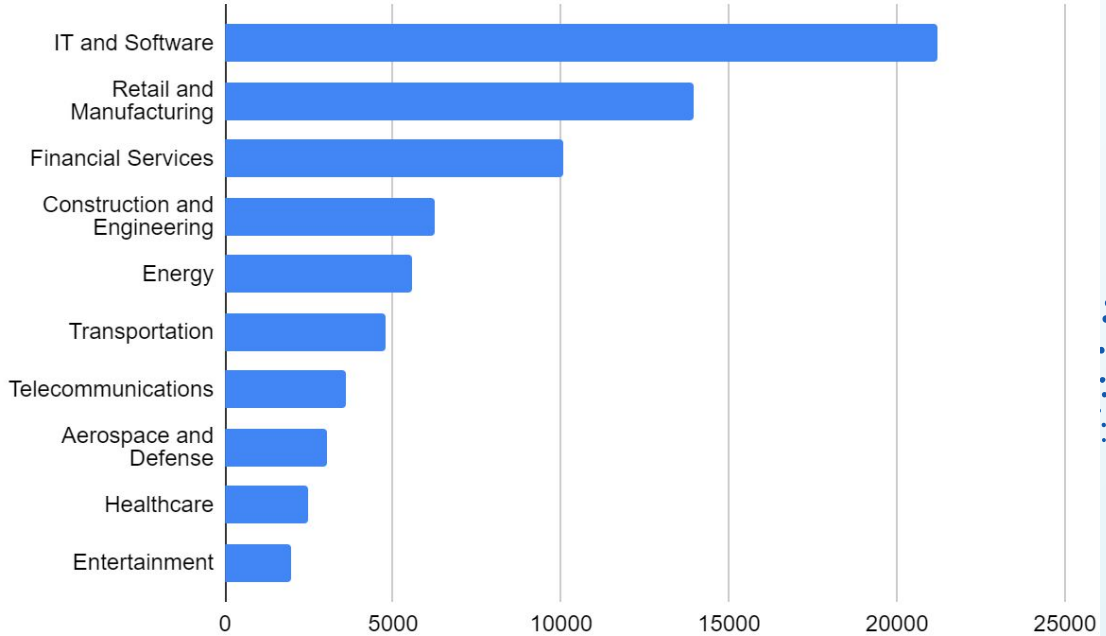


Intelligence source: Early Warning Phishing Feed

Potential Phishing Trends: Which Industries Are Targeted?

For this part of the analysis, we extracted the company-branded domains from the Q3 2023 Early Warning Phishing Feed files. We then assigned an industry to each domain using the imitated companies' business LinkedIn profiles as sources.

In terms of domain volume, the top 10 most targeted industries were IT and Software, Retail and Manufacturing, Financial Services, Construction and Engineering, Energy, Transportation, Telecommunications, Aerospace and Defense, Healthcare, and Entertainment.



Intelligence source: Early Warning Phishing Feed

Analyzing Malicious gTLD Domains

We then moved to actual indicators of compromise (IoCs), specifically domain names listed on the Q3 2023 files of our Threat Intelligence Data Feeds for being linked to phishing, malware, botnet, or spam, among other malicious or suspicious activities.

In terms of absolute number of hits generated, .com, .net, and .xyz were the most common gTLDs present in the Q3 2023 files. However, positions could be driven by the general popularity of certain gTLDs.

To account for this factor, we divided the number of malicious domains listed by the number of domains added per gTLD for Q3 2023. That gave us specific proportions, the highest of which was .xyz (0.205), closely followed by .net (0.197) and .info (0.195).

Top gTLDs

	xyz	net	info	org	com	site	top	shop	online	cfd
[a] = # of malicious domains listed in Q3	118,692	136,803	42,862	113,691	720,462	23,088	31,059	8,513	11,045	2,192
[b] = # of new domains added in Q3	579,635	694,330	219,736	1,285,771	9,199,043	344,935	810,368	386,700	738,654	513,956
N = a/b	0.205	0.197	0.195	0.088	0.078	0.067	0.038	0.022	0.015	0.004

Intelligence source: Threat Intelligence Data Feeds

Analyzing Malicious ccTLD Domains

Now, looking at the domain IoCs sporting ccTLDs, we found that .ru, .cn, and .co were the most common extensions for the domains found in the Q3 2023 files of the Threat Intelligence Data Feeds.

After dividing the number of malicious domains listed by the number of new domains added per ccTLD in Q3 2023, .ru remained proportionally at the top of the list (0.171), this time followed by .tk (0.131) and .co (0.070).

.cn and .co meanwhile had a smaller proportion (0.029 and 0.070 respectively).

Top ccTLDs	ru	tk	co	br	cn	fr	uk	nl	au	de
[a] = # of malicious domains listed in Q3	86,436	15,904	19,055	8,338	27,294	3,974	7,629	1,817	4,178	7,511
[b] = # of new domains added in Q3	506,119	121,465	273,359	220,612	932,244	155,534	449,857	137,586	432,697	1,618,370
N = a/b	0.171	0.131	0.070	0.038	0.029	0.026	0.017	0.013	0.010	0.005

Intelligence source: Threat Intelligence Data Feeds

Q3 2023 - Wrap Up

Thwarting DNS Threats

New domain activity can have significant implications for cybersecurity, as domain names often serve as vehicles for emerging threats. While there is no universal strategy to tackle DNS threats, cybersecurity specialists often recommend to:

- Issue security warnings against or even block newly registered domains unless otherwise sanctioned by organizational controls.
- Be suspicious of new domain names that contain brand names or popular strings. Established and reputable brands typically invest considerable resources in building a strong online presence around a consistent set of domain names, making it improbable for them to frequently register new, almost identical domains for official use.
- Block less common gTLDs and known malicious ccTLDs, especially if they figure on most-abused TLD lists or hint at locations not served by the organization or restricted for compliance reasons.
- Watch out for organizations who pretend to be well-established, unlike suggested by their domains' recent creation date or privacy-shielded WHOIS records.
- Watch out for organizations who pretend to be well-established yet seem to operate using recent or shared DNS infrastructure (e.g., IP addresses, mail servers, nameservers, SSL certificates, etc.).

Conclusion

Knowledge is power, especially in the dynamic digital realm. The Q3 2023 Global Domain Activity Report provides valuable insights into domain registrations, expirations, emerging trends, and malicious indicators.

From the prevalence of TLDs to the nuances of predictive phishing threats, we dissected global domain registrations and examined potential and known malicious properties while shedding light on specific TLDs.

As we continue to deliver the most comprehensive domain, IP, DNS, and cyber threat intelligence data, we invite you to be a part of the collective security effort.

Starting next quarter, we're opening our doors to cybersecurity content contributors who share our vision of making the Internet safer and more transparent.

Get in touch with us to access the data behind this report and discuss collaboration opportunities.

About WhoisXML API

WhoisXML API empowers all types of cyber security enterprises, including MSSP, SOC, Fortune 1000 organizations, government agencies, and SMBs with digital footprints. We relentlessly collect, process, and deliver the most comprehensive and readily available domain, IP, and DNS intelligence there is on the market.

To explore how our data can fortify your digital presence, visit our website or contact our sales team.

4.2 billion+
domains and subdomains

16.7 billion+
historical WHOIS records

Billions
DNS records

12+
years of data crawling


WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence