WhoisXMLAPI

Global Domain Activity Report

Q4 2023

Dear Reader,

I proudly present another edition of the Global Domain Activity Report, this time scrutinizing newly registered domains and confirmed malicious indicators of compromise in Q4 2023.

As the domain landscape continues to rapidly evolve, gaining visibility into global domain registrant activities and emerging DNS trends is more important than ever.

Feel free to review this report carefully and share the insights with your team.

Let us make the Internet a safer place.

Jonathan Zhang

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

Find me on LinkedIn

Executive Summary

In Q4 2023, we saw more than 31 million NRDs, indicating a 10.24% increase from Q3, a testament to the growing global digital economy and threat landscape.

We analyzed the NRDs in this report to provide an overview of the most notable domain registration trends, such as the use of popular gTLDs and ccTLDs among both legitimate and malicious domains.

1. **Newly Registered Domains by TLD Type**

   Check the breakdown of domains registered by top TLD type.

2. **New Domain Activity: gTLD Trends**

   Uncover the most widely used gTLDs during the quarter.

3. **New Domain Activity: ccTLD Trends**

   Discover the most widely used ccTLDs during the quarter.

4. **New Domain Activity: Most Popular Registrars**

   Identify the most popular registrars during the quarter.

5. **Decoding the TLDs of Malicious Domains**

   Analyze the TLD usage of newly found IoCs during the quarter.

6. **Analyzing Malicious gTLD Domains**

   Check the prevalence of malicious gTLD domains.

7. **Analyzing Malicious ccTLD Domains**

   Check the prevalence of malicious ccTLD domains

Methodology

WhoisXML API researchers tapped into the company's extensive domain and cyber threat intelligence sources to create this report.

Our first step was to leverage our Newly Registered Domains solution to obtain a snapshot of new domain activities worldwide.

Specifically, we looked for patterns and trends in new domain registrations in Q4 2023, including TLD usage, registrar breakdown, and WHOIS data redaction.

Our second step was to collect data from our Threat Intelligence Data Feeds to look into confirmed malicious IoCs first seen between 1 November and 31 December 2023.

Q4 2023 Findings

Newly Registered Domains by TLD Type

Domain registrations continued to soar as their total volume was 10.24% higher in Q4 compared to Q3. Note, however, that while the gTLD usage increased by 25.8%, the ccTLD domain registrations declined by 19.2%.

In Q4, about 337, 000 domains were registered daily on average across all TLDs. Altogether, 2.95 times more domains with gTLD extensions were registered than ccTLD domains.

	October	November	December	**Total (Q4)**	**Total (Q3)**
gTLD	**8,128,859**	**7,222,370**	**7,818,462**	**23,169,691**	**18,415,868**
ccTLD	**4,558,378**	**1,503,973**	**1,792,532**	**7,854,883**	**9,727,379**
Total	**12,687,237**	**8,726,343**	**9,610,994**	**31,024,574**	**28,143,247**

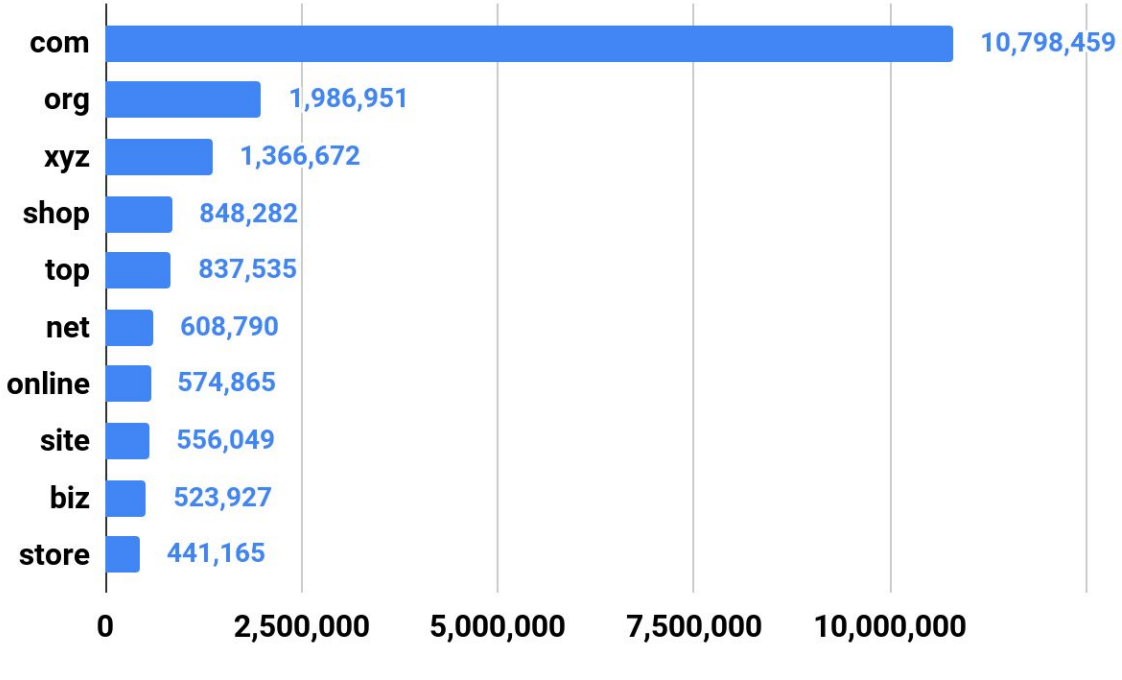
Intelligence source: Newly Registered Domains

New Domain Activity: gTLD Trends

The number of new domain registrations sporting the .com extension in Q4 2023 was significantly higher compared with other gTLDs.

The same was true in Q3, which is understandable since individuals and organizations alike often prefer to register .com domains when available.

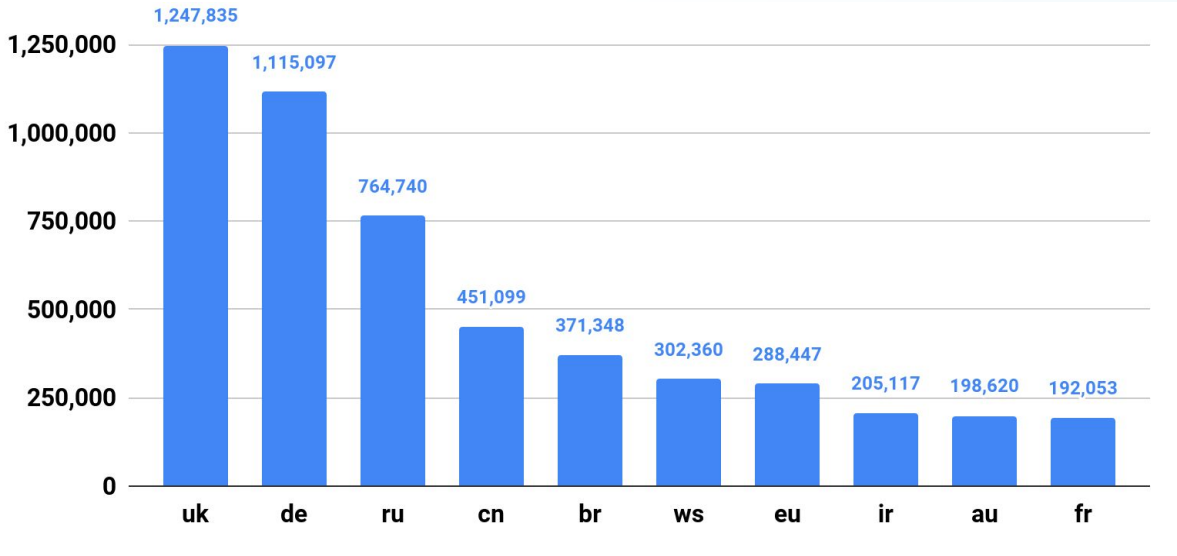
The other popular gTLDs included .org, .xyz, .shop, .top, .net, .online, .site, .biz, and .store.



Intelligence source: Newly Registered Domains

New Domain Activity: ccTLD Trends

The ccTLD extension with the highest number of new domain registrations in Q4 was .uk (U.K.), followed by .de (Germany), .ru (Russia), .cn (China), .br (Brazil), .ws (Samoa), .eu (European Union), .ir (Iran), .au (Australia), and .fr (France).



Intelligence source: Newly Registered Domains

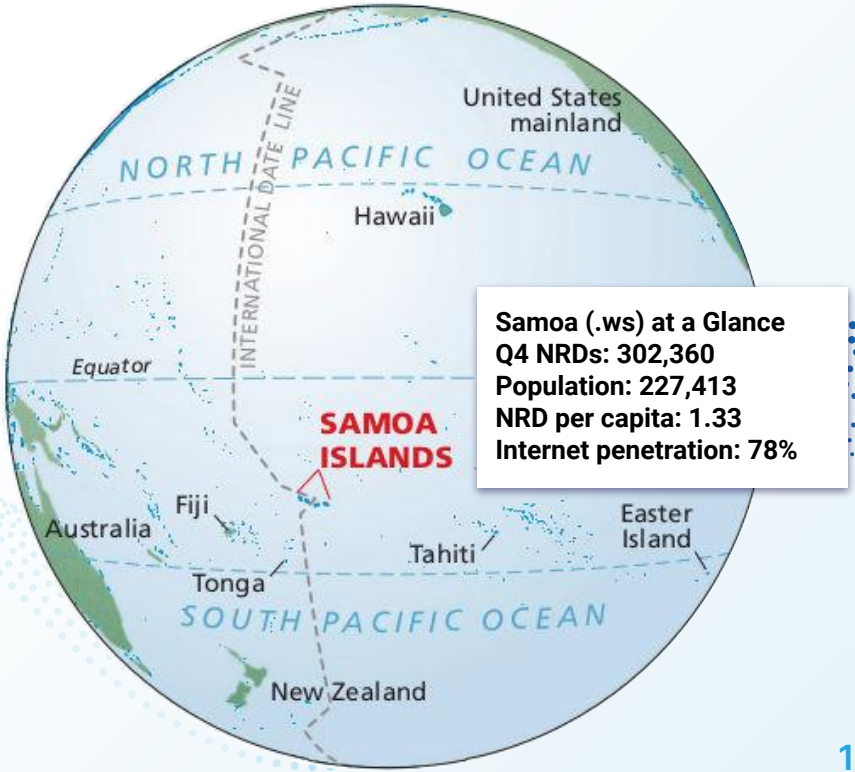
Is ccTLD Registration Congruent with Population Size?

A primary reason for registering a ccTLD domain is to start a new venture or business operations locally. Are there, however, ccTLDs whose use appeared abnormal when considering country populations?

Take Samoa's ccTLD domain activity. The ccTLD .ws ranked sixth among 250+ ccTLDs in terms of domain registration volume in Q4, accounting for 302,360 NRDs. The country's entire population, however, is only estimated at 227,413. If only residents registered .ws domains during the quarter, the NRD per capita would be 1.33 despite the nation having only a 78% Internet penetration rate.

A similar finding was described for Tokelau (.tk) in our Q3 2023 report. For instance, a total of 121,000 domains were added in Q3 alone while the territory's entire population was only estimated at 1,900. In Q4 2023, .tk only ranked 52nd in terms of registration volume, highlighting the dynamic nature of domain activity.

Intelligence source: Newly Registered Domains

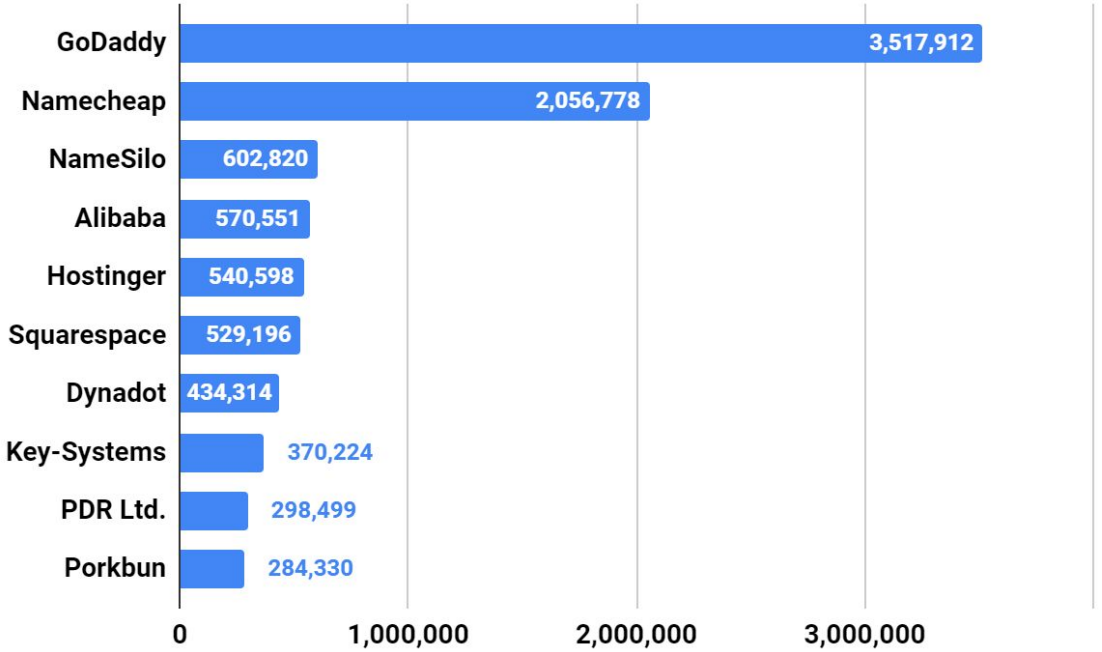


New Domain Activity: Most Popular Registrars

While registrants have thousands of registrars to choose from, our research found that most chose GoDaddy during the quarter.

Namecheap, NameSilo, Alibaba Cloud Computing, Hostinger, Squarespace, Dynadot, Key-Systems LLC, PDR Ltd., and Porkbun completed the top 10 registrars.

The presence of Squarespace and Hostinger on our list is consistent with the popularity of e-commerce gTLDs like .store or .site.



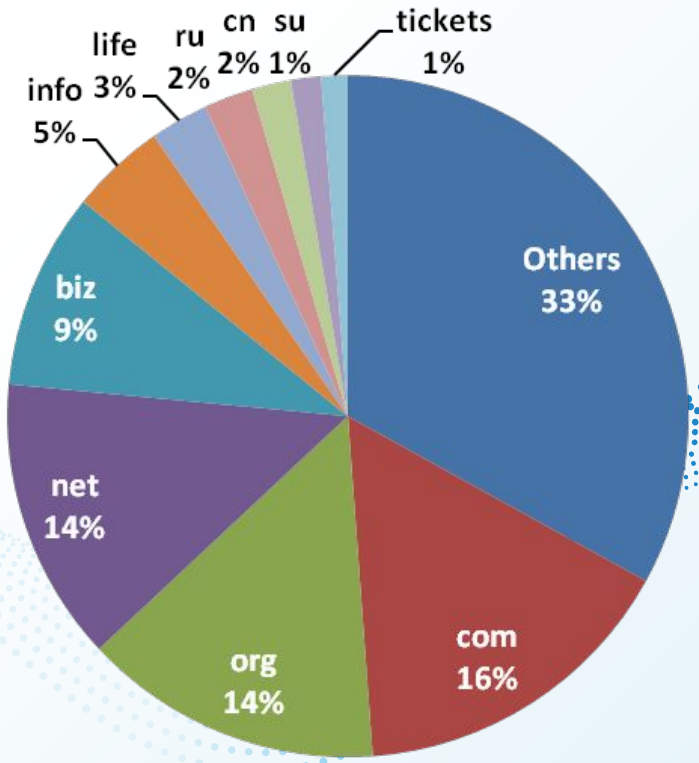
Intelligence source: Newly Registered Domains

Decoding the TLDs of Malicious Domains

Next, we zoomed in on 2.6+ million domains that were first seen as IoCs across threat types—phishing, malware, C&C, and other suspicious and malicious activities—in our Threat Intelligence Data Feed (TIDF) files in November and December 2023.

The malicious domains sported a combination of popular gTLDs like .com and less common ones like .life.

The same was true for ccTLDs. The malicious domains used a combination of popular (e.g., .cn and .ru) and less popular (e.g., .so and .to) ccTLD extensions.



Intelligence source: Newly Registered Domains

Analyzing Malicious gTLD Domains

No TLD is immune to malicious usage or abuse.

In Q4, .com, .org, .net, .biz, .info, and .life were most frequently first seen among domain IoCs. Their usage could be correlated to their popularity, notably since various extensions, except for .info and .life, were among the top 10 gTLDs used in new domains registered during the quarter.

For instance, more than 400,000 malicious domains sported the .com extension while the gTLD accounted for more than 10.7 million domain registrations during the quarter.

Interestingly, the volumes of new domains registered sporting .org and .net were significantly lower while the number of new malicious domains was comparable to .com's.

	com	org	net	biz	info	life
New malicious domains listed in Q4	**418,956**	**376,572**	**356,589**	**247,751**	**119,896**	**72,805**
New domains added in Q4	**10,798,459**	**1,986,951**	**608,790**	**523,927**	**234,726**	**93,707**

Intelligence source: Threat Intelligence Data Feeds

Analyzing Malicious ccTLD Domains

When it came to new domain IoCs sporting ccTLDs, .ru, .cn, .su, .cc, and five other extensions were most frequently first seen in November and December 2023.

Also, three of the nine top ccTLDs used for Q4 malicious domains were among the most popular among the NRDs. These were .ru, .cn, and .eu.

	ru	cn	su	cc	in	to	so	eu	pw
New malicious domains listed in Q4	62,171	49,087	37,839	24,795	22,715	18,114	17,962	15,314	14,580
New domains added in Q4	1,247,835	451,099	10,138	119,543	156,713	8,560	480	288,447	27,695

Intelligence source: Threat Intelligence Data Feeds

Q4 2023 Wrap-Up

Conclusion

Knowledge is power, especially in the dynamic DNS landscape. The Q4 2023 Global Domain Activity Report provides valuable insights into domain registrations, expirations, emerging trends, and IoCs.

The report looked into the TLD usage of legitimate and malicious domains, along with other emerging trends that can help shed light on domain activities, preferences, and usage.

You can be part of our collective security effort, too. As we continue to deliver the most comprehensive domain, IP, DNS, and cyber threat intelligence, our doors are open to cybersecurity partnerships.

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 cybersecurity enterprises, including MSSPs, SOCs, 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 on the market.

To explore how our data can support your cybersecurity and business use cases, 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