SPAMHAUS

Spamhaus Quarterly Domain Reputation Update

Q2 2022

Spamhaus, the independent leader in IP and domain reputation, reviews the domain name ecosphere. From the number of newly registered domains, to the domain abuse our researchers are observing, this update highlights trends, provides insights into the poor reputation of domains, and champions providers where positive improvements are seen.

Welcome to the Spamhaus Quarterly Domain Reputation Update Q2 2022.

Enter

Contents ×

Contents

01

02

03

04

05

The Overview

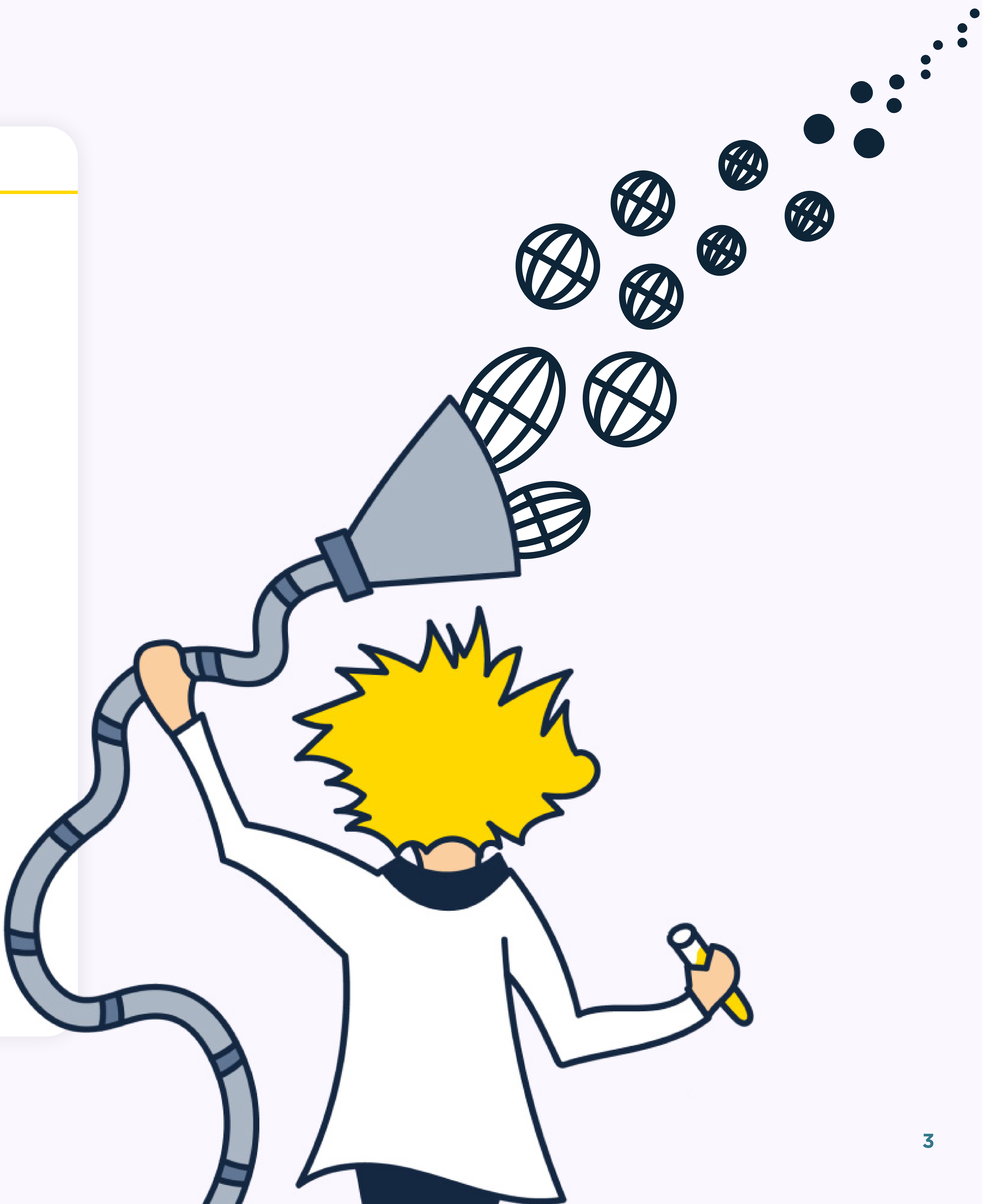
The Overview

So why do we look at domains and their associated reputation? Why does it make sense to use a domain name as a reputation marker in filtering decisions, whether these decisions relate to email, malware, or generic internet traffic?

Domains have a predictable “shape and form”, making them easy to extract and act upon. Multiple types of security software support the use of domains (or hostnames) to highlight issues and influence decisions. This doesn’t come as any great surprise, given that the Domain Name System (DNS) is fundamental to almost everything that happens on the internet, and at its core, “the resource records contained in the DNS associate domain names with other forms of information”.

No matter what you’re doing on the internet, legitimate or otherwise, you must (almost always) use a domain name. Without a domain name, most malicious activity wouldn’t get started, let alone be successful.

Overview continued



Overview cont.

Consider these scenarios:

- A SMS phishing campaign uses a purpose-bought (aka a malicious registration), short domain name to direct recipients to a fake payment portal. Remove or filter the domain, and the fraud cannot happen.
- Malware tries to create a command-and-control channel by using a malicious domain name to contact a server that a bad actor operates. Take out the domain, and communication cannot be established.
- A counterfeit drug-related spam email gets sent with all the authentication protocols correctly set up in the message (SPF, DKIM, DMARC). Even if these all pass, knowing that the domain is malicious will raise a big red flag, and the email will be seen differently.

Seasoned bad actors require domain names to commit abuse – it's as simple as that. Some require hundreds of domains to circumvent bad reputation and blocklisting; meanwhile, some require only a few and carefully select service providers that aren't in the habit of quick takedowns.

We want to shine a light on this kind of nefarious activity and highlight service providers who are going above and beyond to ensure they don't give safe refuge to bad actors. As we publish more reports, we hope to continue adding content to provide additional context and increased insight into the world of domain reputation.

01
02
03
04
05

New domains × Number of new... ×

New domains

New domains overview

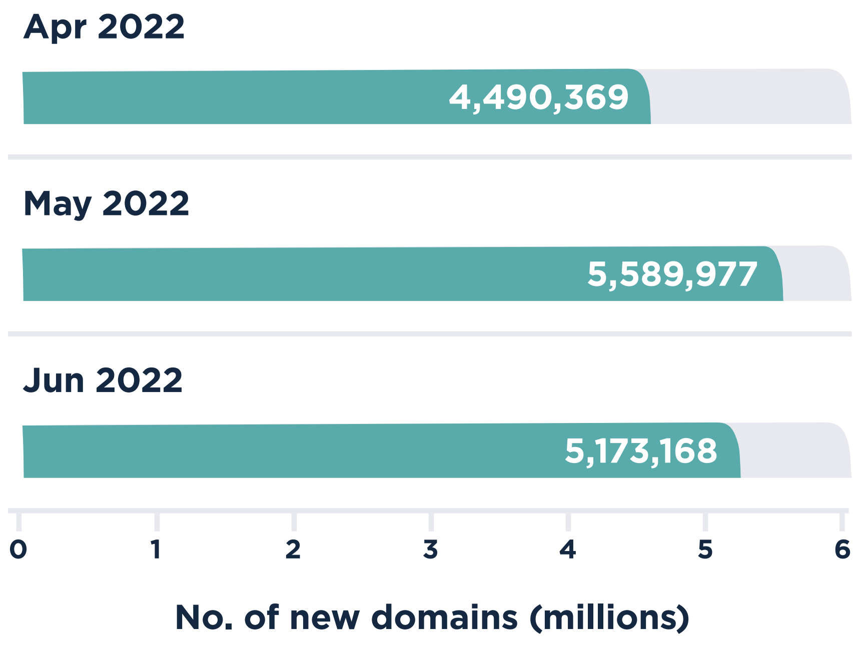
A total of 15.3 million new domains were registered last quarter, with a monthly average of 5.1 million. This was a significant 43% reduction against Q1 of this year when 25.6 million new domains were observed.

May was the busiest month with 5.6 million domains; however, all three months were close to the quarterly monthly average, with minimum variation.

It is important to note that a new domain is not a bad domain per se. However, a considerable amount of abuse is associated with new domain names. One reason is that if a bad actor buys a new domain and uses it immediately, there is minimal chance of security systems and professionals having prior knowledge of this domain's existence. Unfortunately, its existence is only discovered once the malicious campaign starts. Furthermore, by using new domains, bad actors prevent registries and registrars from doing pre-emptive takedowns.

New domains × Number of new... ×

Number of new domains per month



Quarterly Total

15,253,514

▼-43%▼

Monthly Average

5,084,505

▼-3,764,414▼

What is a new domain?

Spamhaus classes a "new domain" as one that has been newly registered or newly observed and is listed by Spamhaus for a 24-hour period in its Zero Reputation Domain (ZRD) dataset. Newly created domains are rarely used for legitimate purposes within 24 hours of registration, meanwhile cybercriminals register and burn hundreds of domains daily. When these new domains are seen in the wild it is a strong indicator of potential malicious behavior.

The research team compiles this list from various data sources including Passive DNS, SMTP data and zone files shared by registries. The new domain data, therefore, is not the exact number of new domains, but the number of new domains Spamhaus has visibility of.

01
02
03
04
05

New domains... TLD types...

New domains by top-level domain (TLD)

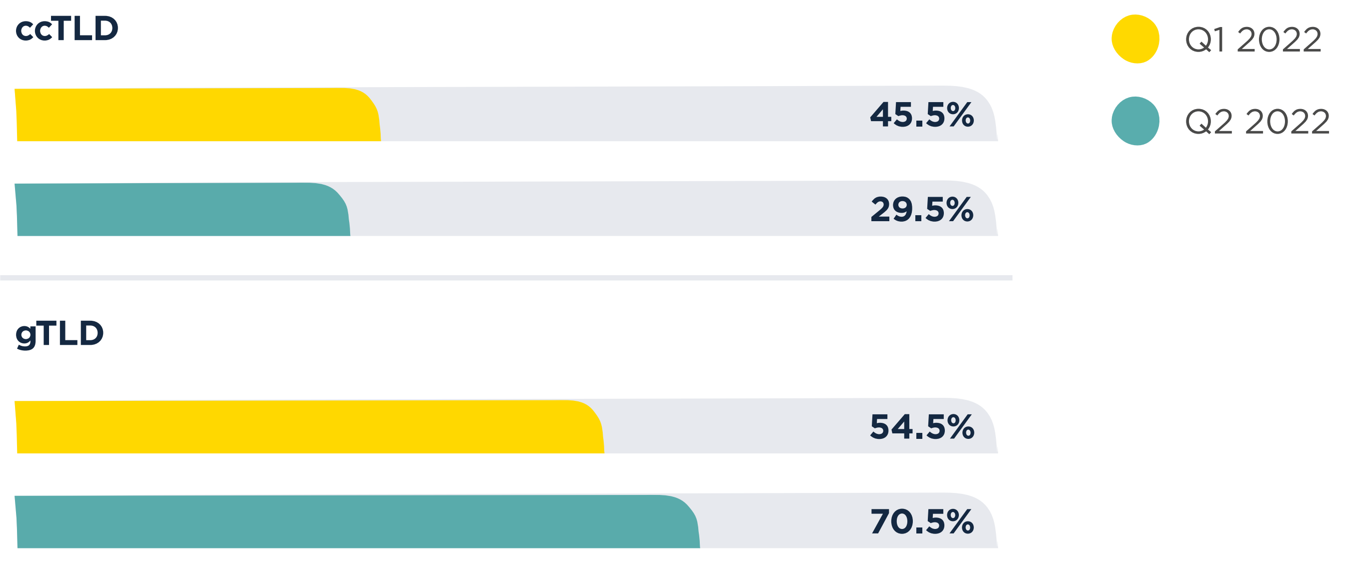
All of the TLDs that dropped off the Top 20 chart in Q2 were ccTLDs. Bearing this in mind, it won't come as a surprise when you review the TLD types' share that the ccTLDs' dropped by over 15% in Q2.

You will note that some gTLDs saw a huge increase in the number of new domains in their zones compared to the previous quarter. For example, .xyz had a massive 4301% increase. In some cases, you can trace the rise in popularity of some gTLD's domains back to promotions run by the TLD. Registries can run these promotions across all their registrars or only at selected ones.

As most of these promotions dramatically reduce the price (a 90% reduction is not uncommon!), it allows a registrant to buy many more domain names for the same amount of money. This is extremely attractive not only to domain name speculators but also to bad actors who burn through domains as part of their "business model."

New domains... TLD types...

New domain TLD types comparison, quarter on quarter



Top-level domains – a quick explanation

There are a couple of different top-level domains (TLDs) including:

- **Generic TLDs (gTLDs)** - these are under ICANN jurisdiction. Some gTLDs are open i.e. can be used by anyone e.g., .com, some have strict policies regulating who and how they can be used e.g., .bank, and some are closed e.g., .honda.
- **Country code TLDs (ccTLDs)** - typically these relate to a country or region. Registries define the policies relating to these TLDs; some allow registrations from anywhere, some require local presence, and some license their namespace wholesale to others.

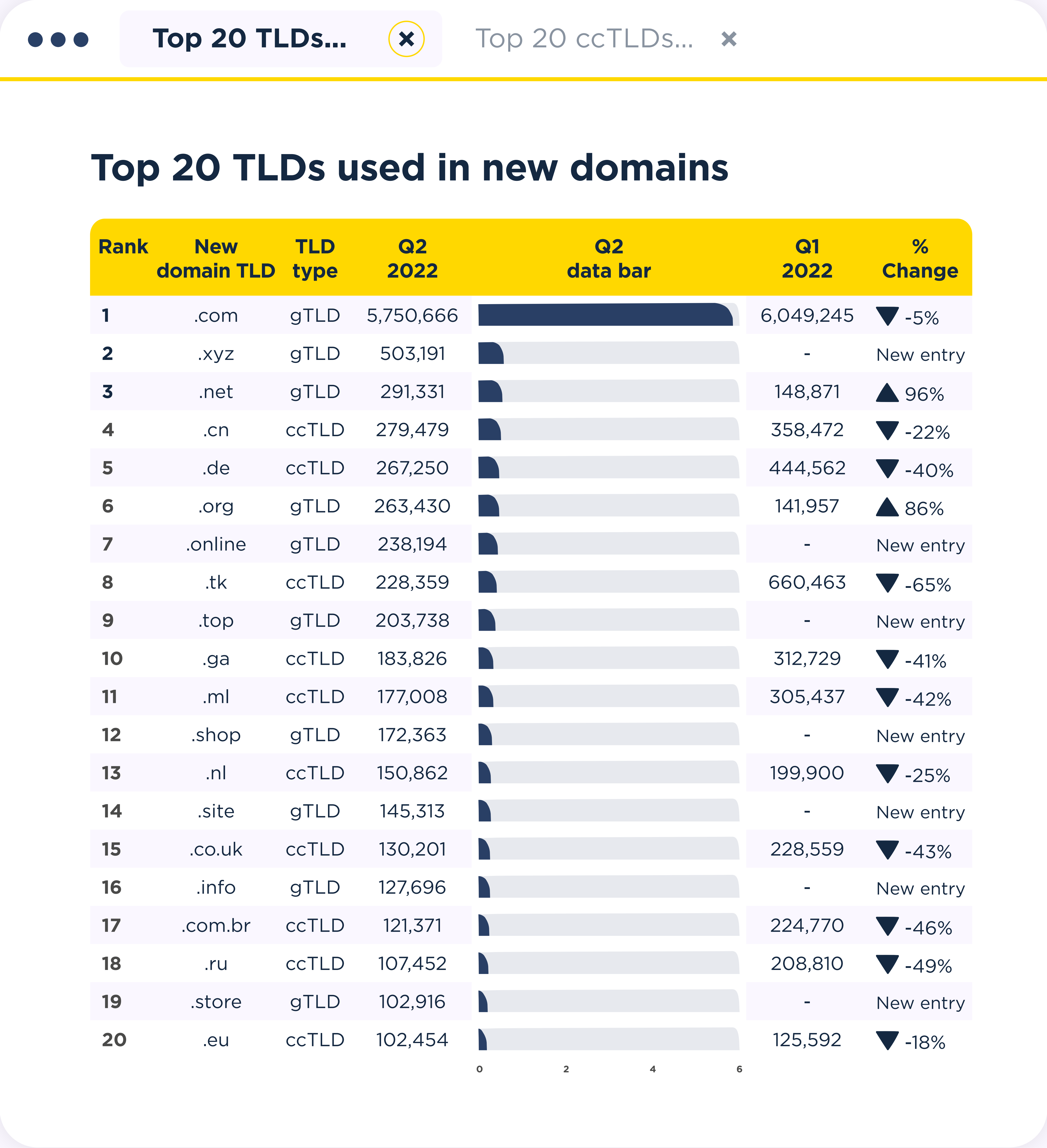
01

02

03

04

05

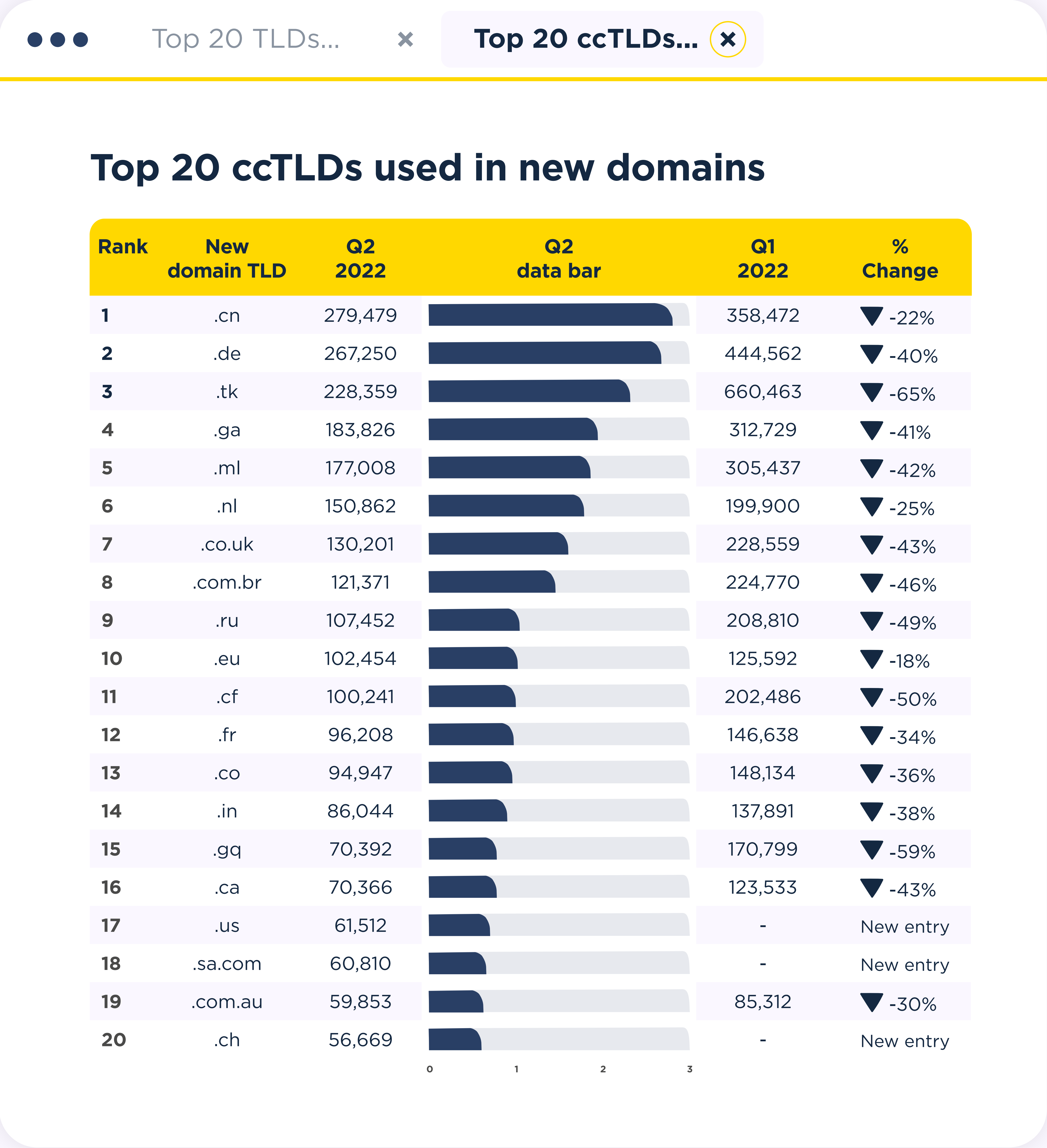


Top 20 TLDs...
Top 20 ccTLDs...

Top 20 TLDs used in new domains

Rank	New domain TLD	TLD type	Q2 2022	Q2 data bar	Q1 2022	% Change
1	.com	gTLD	5,750,666		6,049,245	▼ -5%
2	.xyz	gTLD	503,191		-	New entry
3	.net	gTLD	291,331		148,871	▲ 96%
4	.cn	ccTLD	279,479		358,472	▼ -22%
5	.de	ccTLD	267,250		444,562	▼ -40%
6	.org	gTLD	263,430		141,957	▲ 86%
7	.online	gTLD	238,194		-	New entry
8	.tk	ccTLD	228,359		660,463	▼ -65%
9	.top	gTLD	203,738		-	New entry
10	.ga	ccTLD	183,826		312,729	▼ -41%
11	.ml	ccTLD	177,008		305,437	▼ -42%
12	.shop	gTLD	172,363		-	New entry
13	.nl	ccTLD	150,862		199,900	▼ -25%
14	.site	gTLD	145,313		-	New entry
15	.co.uk	ccTLD	130,201		228,559	▼ -43%
16	.info	gTLD	127,696		-	New entry
17	.com.br	ccTLD	121,371		224,770	▼ -46%
18	.ru	ccTLD	107,452		208,810	▼ -49%
19	.store	gTLD	102,916		-	New entry
20	.eu	ccTLD	102,454		125,592	▼ -18%

0
2
4
6



Top 20 TLDs...
Top 20 ccTLDs...

Top 20 ccTLDs used in new domains

Rank	New domain TLD	Q2 2022	Q2 data bar	Q1 2022	% Change
1	.cn	279,479		358,472	▼ -22%
2	.de	267,250		444,562	▼ -40%
3	.tk	228,359		660,463	▼ -65%
4	.ga	183,826		312,729	▼ -41%
5	.ml	177,008		305,437	▼ -42%
6	.nl	150,862		199,900	▼ -25%
7	.co.uk	130,201		228,559	▼ -43%
8	.com.br	121,371		224,770	▼ -46%
9	.ru	107,452		208,810	▼ -49%
10	.eu	102,454		125,592	▼ -18%
11	.cf	100,241		202,486	▼ -50%
12	.fr	96,208		146,638	▼ -34%
13	.co	94,947		148,134	▼ -36%
14	.in	86,044		137,891	▼ -38%
15	.gq	70,392		170,799	▼ -59%
16	.ca	70,366		123,533	▼ -43%
17	.us	61,512		-	New entry
18	.sa.com	60,810		-	New entry
19	.com.au	59,853		85,312	▼ -30%
20	.ch	56,669		-	New entry

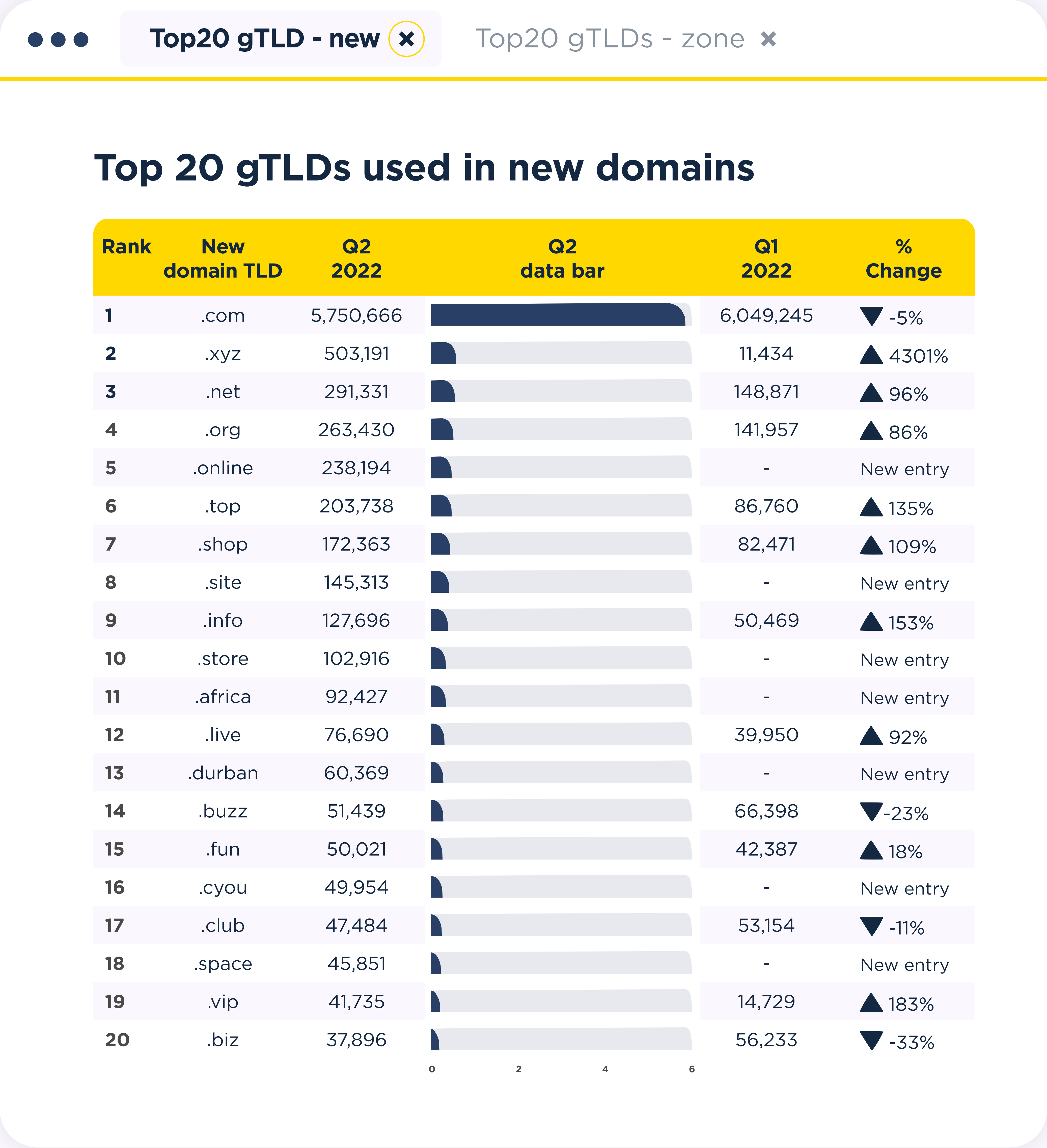
01

02

03

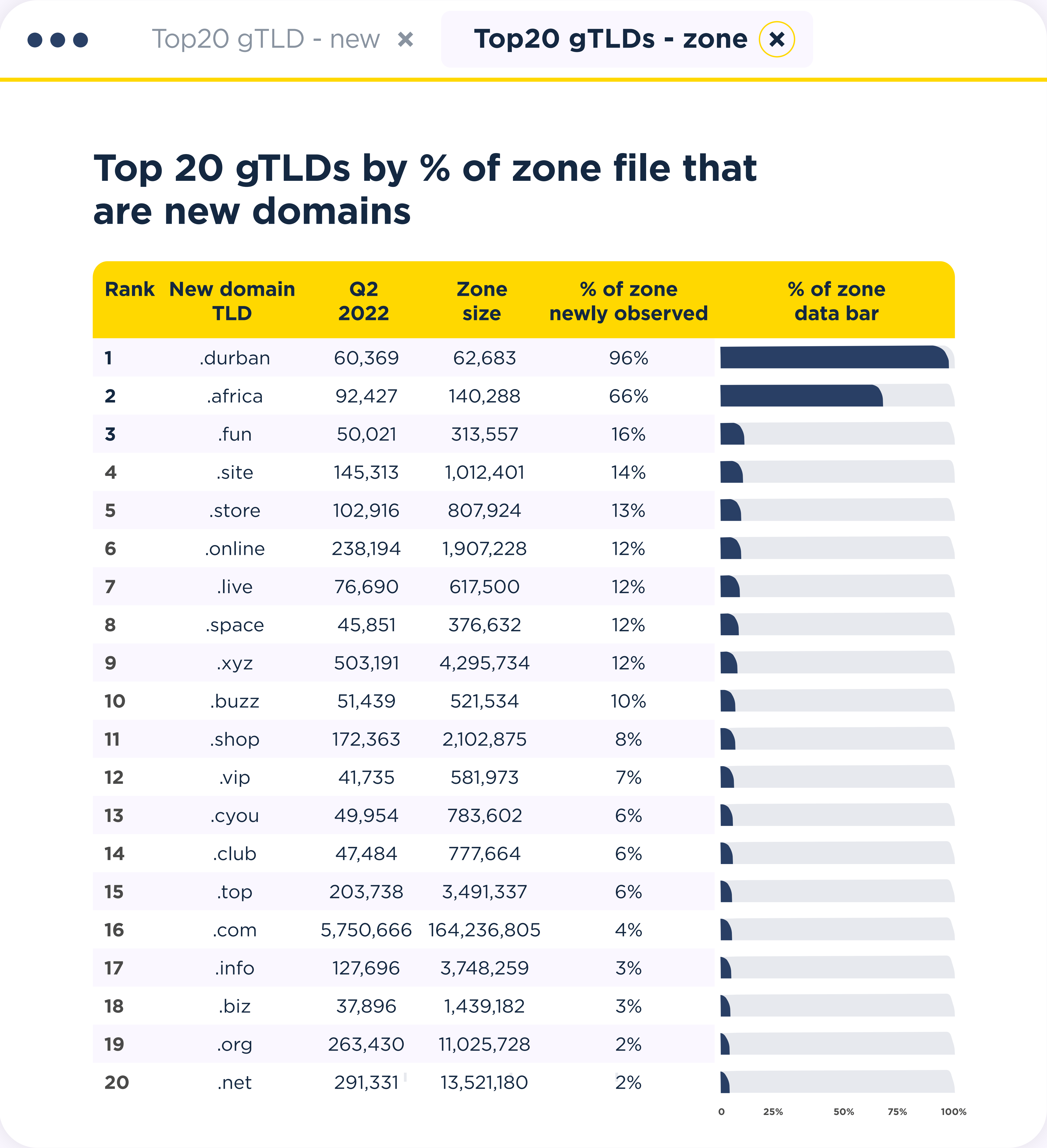
04

05


Top20 gTLD - new ×
Top20 gTLDs - zone ×
0
2
4
6

Top 20 gTLDs used in new domains

Rank	New domain TLD	Q2 2022	Q2 data bar	Q1 2022	% Change
1	.com	5,750,666		6,049,245	▼ -5%
2	.xyz	503,191		11,434	▲ 4301%
3	.net	291,331		148,871	▲ 96%
4	.org	263,430		141,957	▲ 86%
5	.online	238,194		-	New entry
6	.top	203,738		86,760	▲ 135%
7	.shop	172,363		82,471	▲ 109%
8	.site	145,313		-	New entry
9	.info	127,696		50,469	▲ 153%
10	.store	102,916		-	New entry
11	.africa	92,427		-	New entry
12	.live	76,690		39,950	▲ 92%
13	.durban	60,369		-	New entry
14	.buzz	51,439		66,398	▼-23%
15	.fun	50,021		42,387	▲ 18%
16	.cyou	49,954		-	New entry
17	.club	47,484		53,154	▼ -11%
18	.space	45,851		-	New entry
19	.vip	41,735		14,729	▲ 183%
20	.biz	37,896		56,233	▼ -33%


Top20 gTLD - new ×
Top20 gTLDs - zone ×
0
25%
50%
75%
100%

Top 20 gTLDs by % of zone file that are new domains

Rank	New domain TLD	Q2 2022	Zone size	% of zone newly observed	% of zone data bar
1	.durban	60,369	62,683	96%	
2	.africa	92,427	140,288	66%	
3	.fun	50,021	313,557	16%	
4	.site	145,313	1,012,401	14%	
5	.store	102,916	807,924	13%	
6	.online	238,194	1,907,228	12%	
7	.live	76,690	617,500	12%	
8	.space	45,851	376,632	12%	
9	.xyz	503,191	4,295,734	12%	
10	.buzz	51,439	521,534	10%	
11	.shop	172,363	2,102,875	8%	
12	.vip	41,735	581,973	7%	
13	.cyou	49,954	783,602	6%	
14	.club	47,484	777,664	6%	
15	.top	203,738	3,491,337	6%	
16	.com	5,750,666	164,236,805	4%	
17	.info	127,696	3,748,259	3%	
18	.biz	37,896	1,439,182	3%	
19	.org	263,430	11,025,728	2%	
20	.net	291,331	13,521,180	2%	

01

02

03

04

05

Trending terms...

Trending terms in new domains

It is interesting to see how many real-world developments drive new domain registrations. The major declines in cryptocurrency values have clearly affected crypto-related domain registrations, with “crypto” dropping off the Top 20 list in Q2.

In April, “ketous” continued its popularity from Q1 but dropped off the Top 20. We suspect this term is linked to the popularity of the Keto diet.

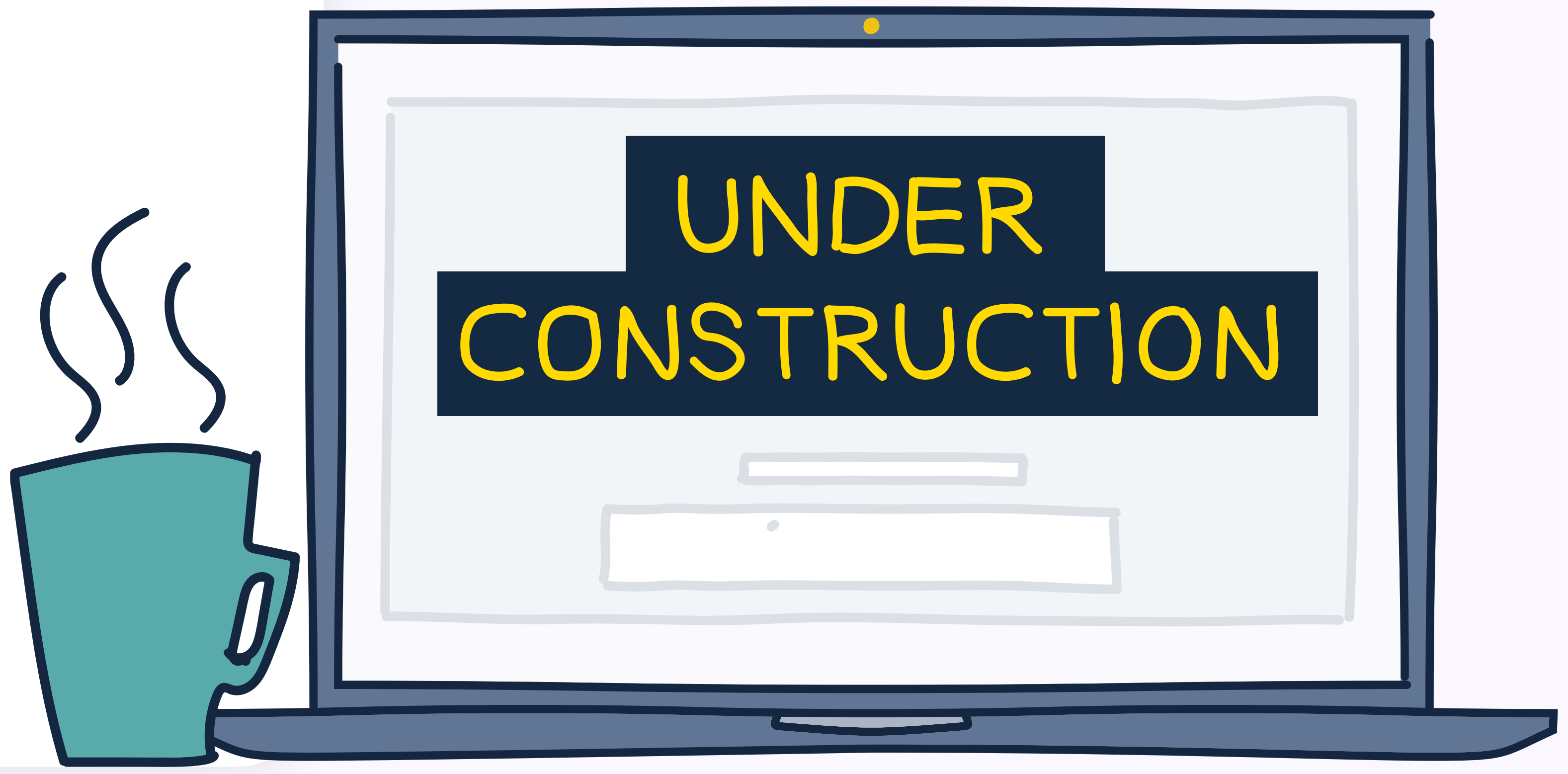
Meanwhile, you may be asking what “yulecheng” is? It’s Chinese for “casino.” While mainland China strictly forbids gambling, it is much harder to regulate this online. Also, historically, the casino industry worldwide has always had high numbers of domains associated with them - casino operators spread their businesses over many brand names and thus, domain names.

When it comes to “ation” here’s a break down of all the words in Q2 containing the term “ation”:

- location **1850**
- ration **1925**
- formation **1974**
- automation **2015**
- restoration **2104**
- corporation **2122**
- transportation **2274**
- renovation **2401**
- association **2824**
- communication **2928**
- vacation **3351**
- innovation **4082**
- station **4955**
- education **6211**
- creation **9680**
- foundation **11715**
- nation **18622**

Methodology for trending terms

We use a text vectorizer to find the most common strings in new domain names and break the counts down by date, which highlights trends in domain name themes. For example, we saw a spike in domain names containing “ukraine” following the Russian invasion.



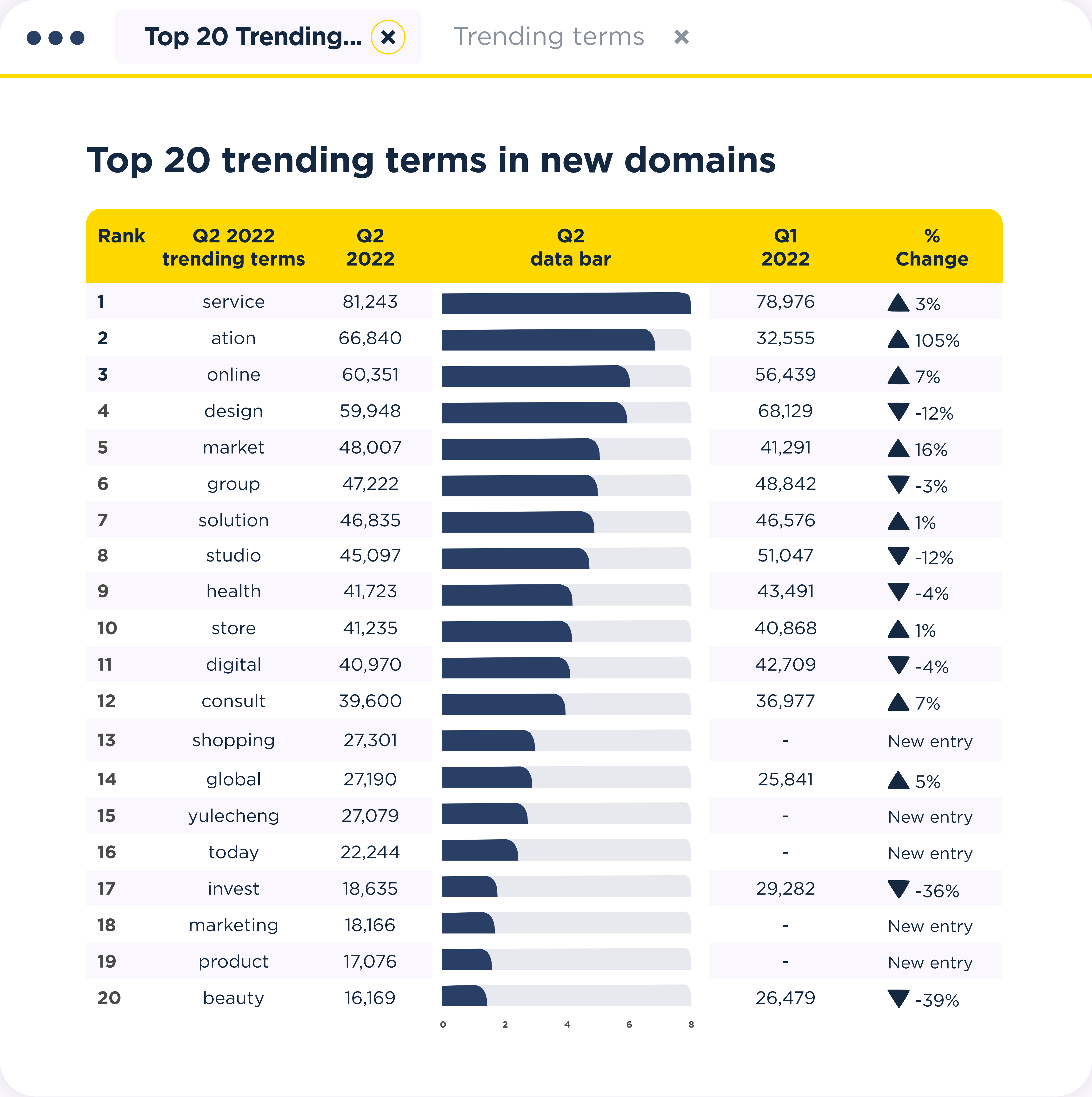
01

02

03

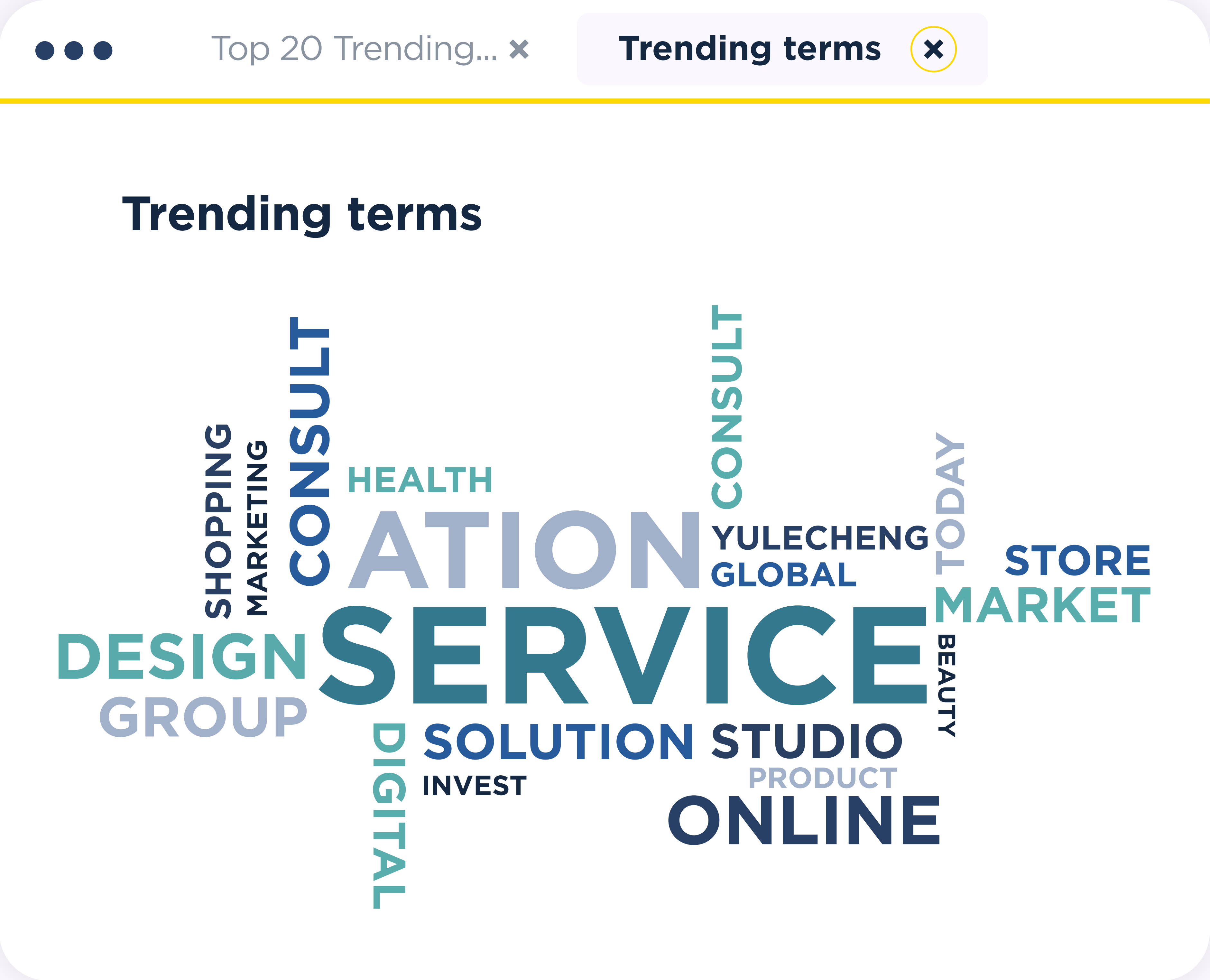
04

05


Top 20 Trending... ×
Trending terms ×
0
2
4
6
8

Top 20 trending terms in new domains

Rank	Q2 2022 trending terms	Q2 2022	Q2 data bar	Q1 2022	% Change
1	service	81,243		78,976	▲ 3%
2	ation	66,840		32,555	▲ 105%
3	online	60,351		56,439	▲ 7%
4	design	59,948		68,129	▼ -12%
5	market	48,007		41,291	▲ 16%
6	group	47,222		48,842	▼ -3%
7	solution	46,835		46,576	▲ 1%
8	studio	45,097		51,047	▼ -12%
9	health	41,723		43,491	▼ -4%
10	store	41,235		40,868	▲ 1%
11	digital	40,970		42,709	▼ -4%
12	consult	39,600		36,977	▲ 7%
13	shopping	27,301		-	New entry
14	global	27,190		25,841	▲ 5%
15	yulecheng	27,079		-	New entry
16	today	22,244		-	New entry
17	invest	18,635		29,282	▼ -36%
18	marketing	18,166		-	New entry
19	product	17,076		-	New entry
20	beauty	16,169		26,479	▼ -39%



Trending terms

Domains listed × Listings per month ×

Domains listed

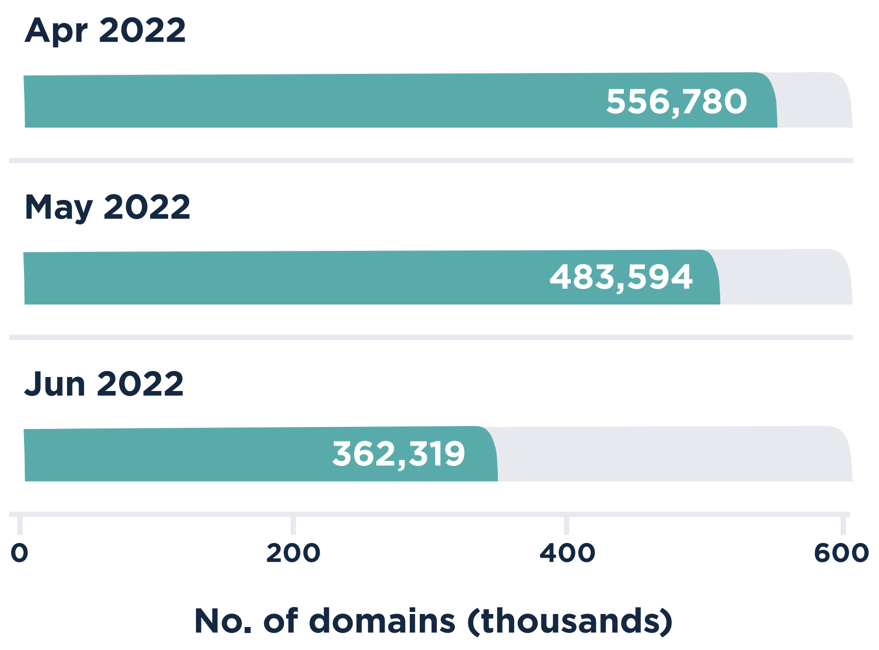
Domain Overview

Just over 1.4 million domains were listed last quarter, with an average of 468K per month. This was a reduction of 11% against the first quarter of 2022. It is too early to tell if this trend will continue. However, we doubt it will - traditionally, the largest number of domains with poor reputation are seen in the second half of the year, peaking towards US holidays like Thanksgiving and Christmas.

- We continue to see a relatively small number of bad operators using a significant number of domains.
- There is a clear divide between bad operators who use new domains as quickly as possible and those who age domains to evade the negative reputational impact of a new domain. Aging times vary from a few weeks to over a year.
- Some bad operators prefer to buy existing domains second-hand to exploit the domains' existing good reputation. The ability to purchase these old and aged domains is becoming easier and easier.

Domains listed × Listings per month ×

Number of Domain listings per month



Quarterly Total

1,402,693

▼ -11% ▼

Monthly Average

467,564

▼ -57,303 ▼

What triggers a domain to be listed by Spamhaus?

Our systems evaluate hundreds of signals relating to a domain and its associated behaviors. Domains get evaluated on the areas listed below, using various automated techniques augmented with human research:

- Authentication and encryption
- Domain ownership
- Signals from large-scale internet traffic
- A domain's hosting environment
- Associations with spam, phishing, malware, ransomware, and other fraudulent activities.

The reputation engine scores a domain; if it meets predefined thresholds and conditions, it is listed in the relevant datasets. This is a continuous process: domains are evaluated and re-evaluated as relevant traffic is observed.

01
02
03
04
05

TLDs listed... × Domain listing... ×

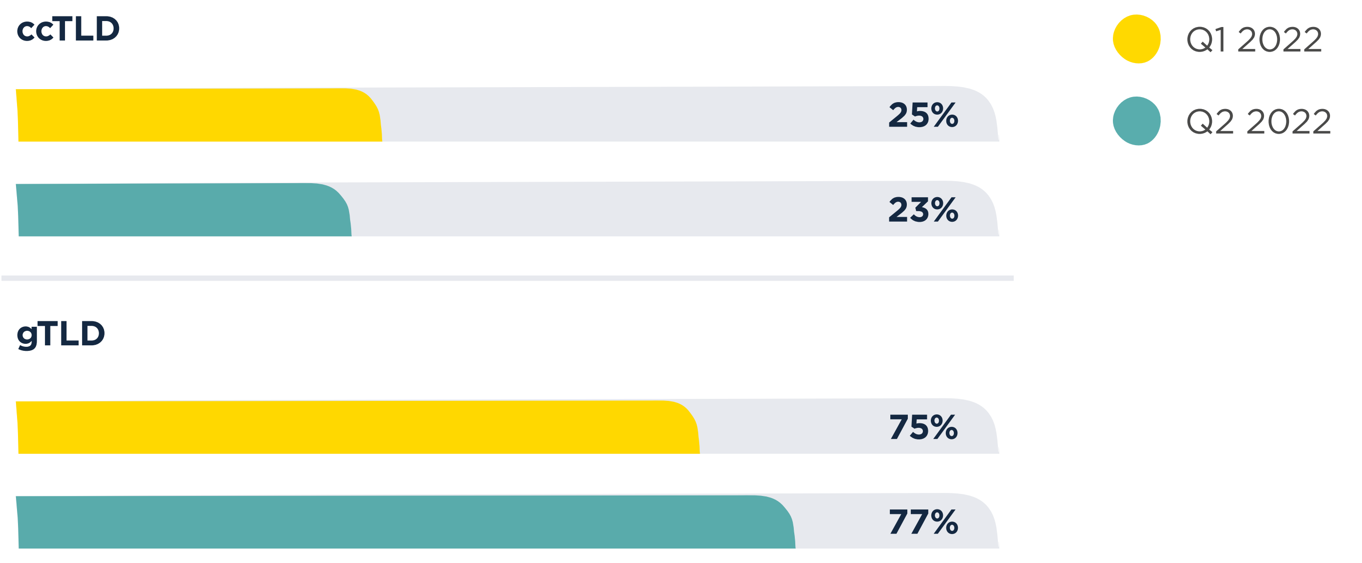
TLDs listed in our domain data

The percentage split between ccTLD and gTLD barely changed between quarters, with ccTLDs accounting for approximately one quarter of listings and gTLD three quarters.

- **.com** remains king. Many bad actors know that there are plenty of scenarios where using cheaper, new gTLD names has more of an adverse impact on their activities. After all, .com is where the internet happens - far fewer people (and automated systems) find it as suspicious if a .com domain is used. Combine this with the open nature of this TLD (anyone from anywhere can buy a .com), and it's not unexpected to see it at number one on the list.
- **.cn** is the highest-ranking ccTLD. We keep seeing large volumes of phishing domains in .cn, where some stay active for a long time. Undoubtedly, the language barrier contributes to the issue; it's hard for entities outside of China to report the problems to Chinese entities. Conversely, it's hard for them to understand the reports and evaluate the cases.
- **The Freenom TLDs** keep experiencing high volumes of abusive and throw-away registrations. Even with anti-abuse APIs, the low price (namely, free) and ease of registration keep these TLDs firmly in the Top 20.

TLDs listed... × Domain listing... ×

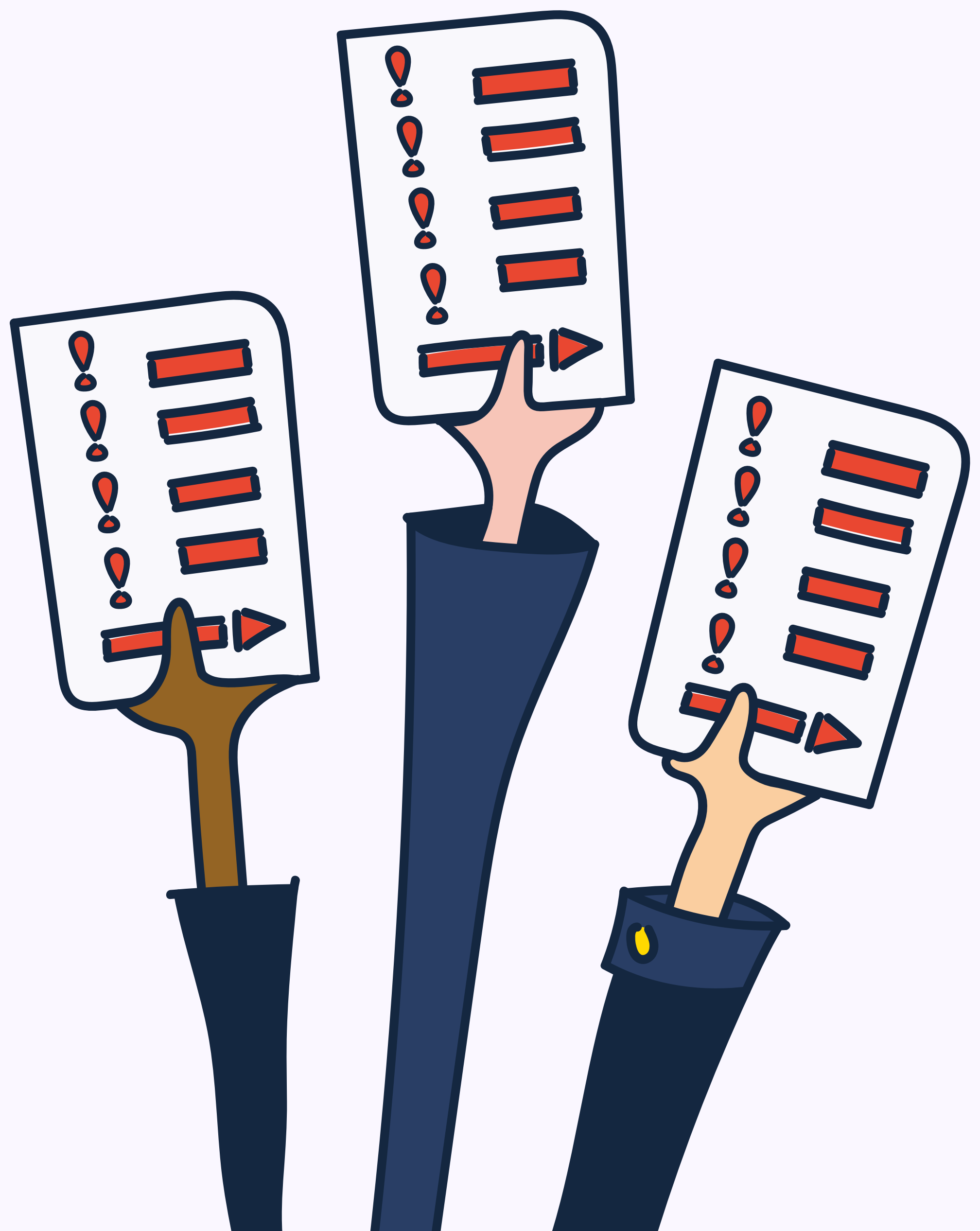
Domain listing TLD type comparison, quarter on quarter



Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q2 2022 .net had more than 13.5 million domains in its zone, of which 0.39% were listed.

Meanwhile, .cam had just over 36,000 domains in its zone, with 17.03% listed in our domain dataset. Both are in the Top 20 of our listings. Still, one had a much higher percentage of active domains listed than the other.



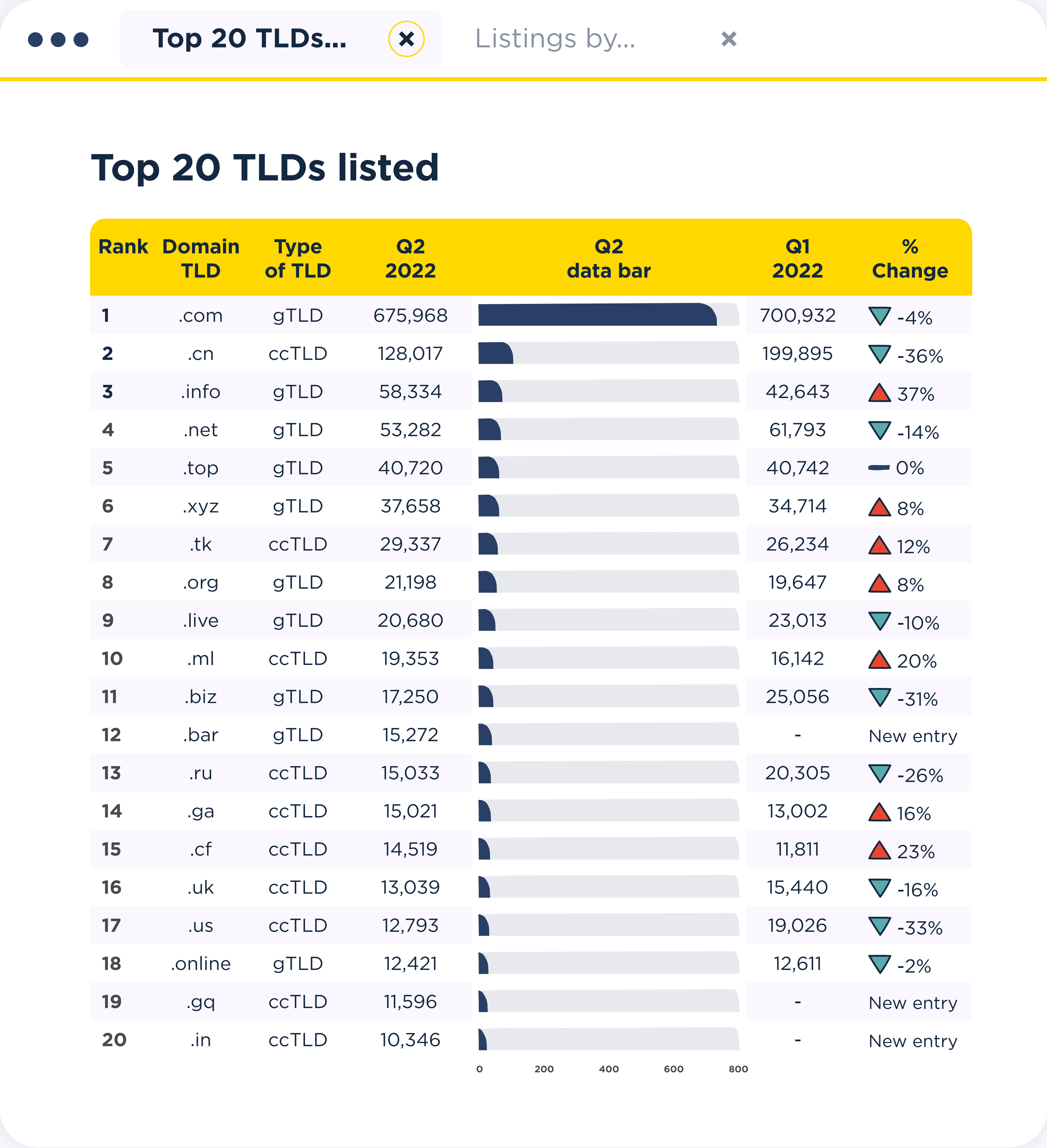
01

02

03

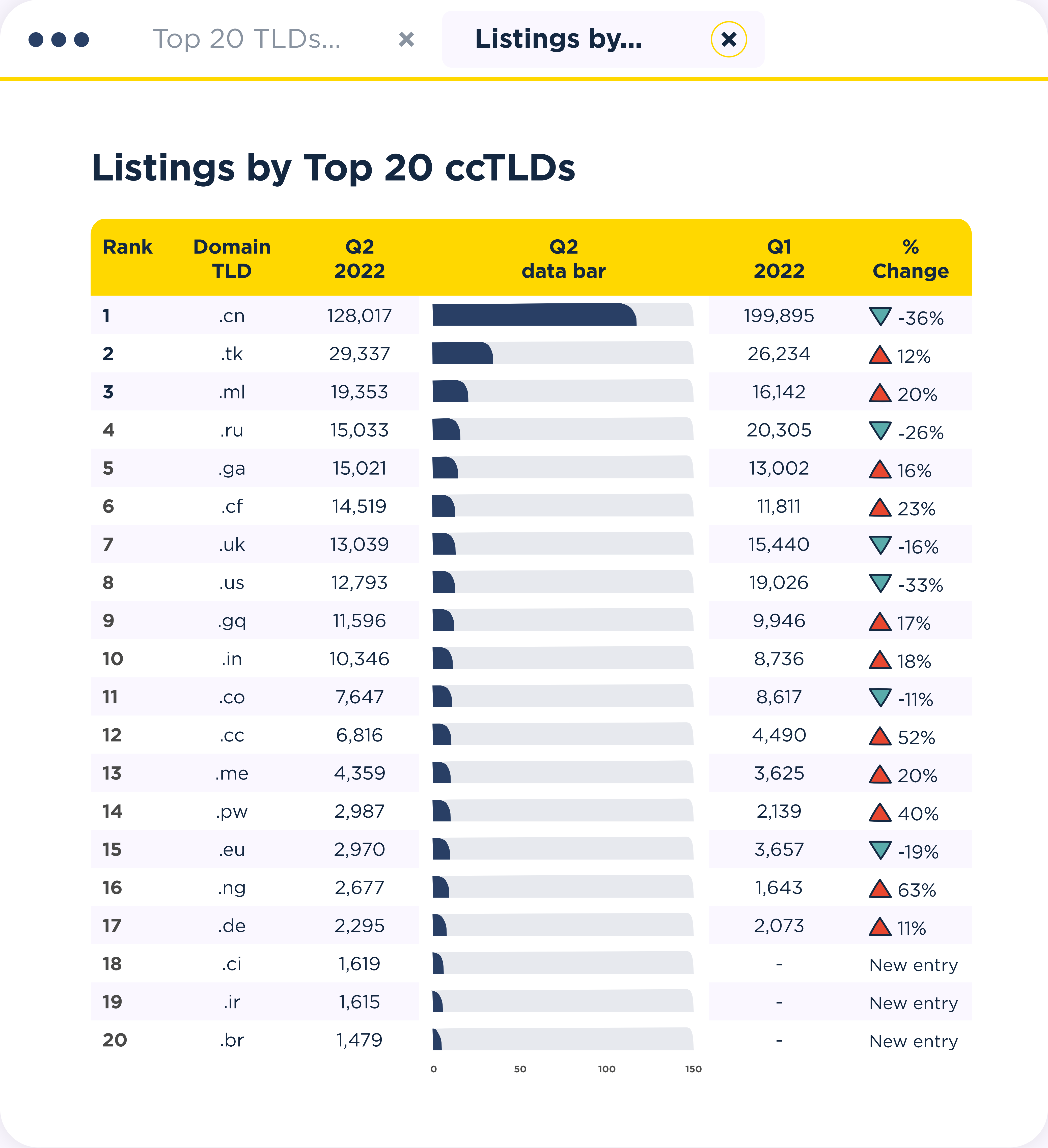
04

05


Top 20 TLDs...
Listings by...
0
200
400
600
800

Top 20 TLDs listed

Rank	Domain TLD	Type of TLD	Q2 2022	Q2 data bar	Q1 2022	% Change
1	.com	gTLD	675,968		700,932	▼ -4%
2	.cn	ccTLD	128,017		199,895	▼ -36%
3	.info	gTLD	58,334		42,643	▲ 37%
4	.net	gTLD	53,282		61,793	▼ -14%
5	.top	gTLD	40,720		40,742	— 0%
6	.xyz	gTLD	37,658		34,714	▲ 8%
7	.tk	ccTLD	29,337		26,234	▲ 12%
8	.org	gTLD	21,198		19,647	▲ 8%
9	.live	gTLD	20,680		23,013	▼ -10%
10	.ml	ccTLD	19,353		16,142	▲ 20%
11	.biz	gTLD	17,250		25,056	▼ -31%
12	.bar	gTLD	15,272		-	New entry
13	.ru	ccTLD	15,033		20,305	▼ -26%
14	.ga	ccTLD	15,021		13,002	▲ 16%
15	.cf	ccTLD	14,519		11,811	▲ 23%
16	.uk	ccTLD	13,039		15,440	▼ -16%
17	.us	ccTLD	12,793		19,026	▼ -33%
18	.online	gTLD	12,421		12,611	▼ -2%
19	.gq	ccTLD	11,596		-	New entry
20	.in	ccTLD	10,346		-	New entry


Top 20 TLDs...
Listings by...
0
50
100
150

Listings by Top 20 ccTLDs

Rank	Domain TLD	Q2 2022	Q2 data bar	Q1 2022	% Change
1	.cn	128,017		199,895	▼ -36%
2	.tk	29,337		26,234	▲ 12%
3	.ml	19,353		16,142	▲ 20%
4	.ru	15,033		20,305	▼ -26%
5	.ga	15,021		13,002	▲ 16%
6	.cf	14,519		11,811	▲ 23%
7	.uk	13,039		15,440	▼ -16%
8	.us	12,793		19,026	▼ -33%
9	.gq	11,596		9,946	▲ 17%
10	.in	10,346		8,736	▲ 18%
11	.co	7,647		8,617	▼ -11%
12	.cc	6,816		4,490	▲ 52%
13	.me	4,359		3,625	▲ 20%
14	.pw	2,987		2,139	▲ 40%
15	.eu	2,970		3,657	▼ -19%
16	.ng	2,677		1,643	▲ 63%
17	.de	2,295		2,073	▲ 11%
18	.ci	1,619		-	New entry
19	.ir	1,615		-	New entry
20	.br	1,479		-	New entry

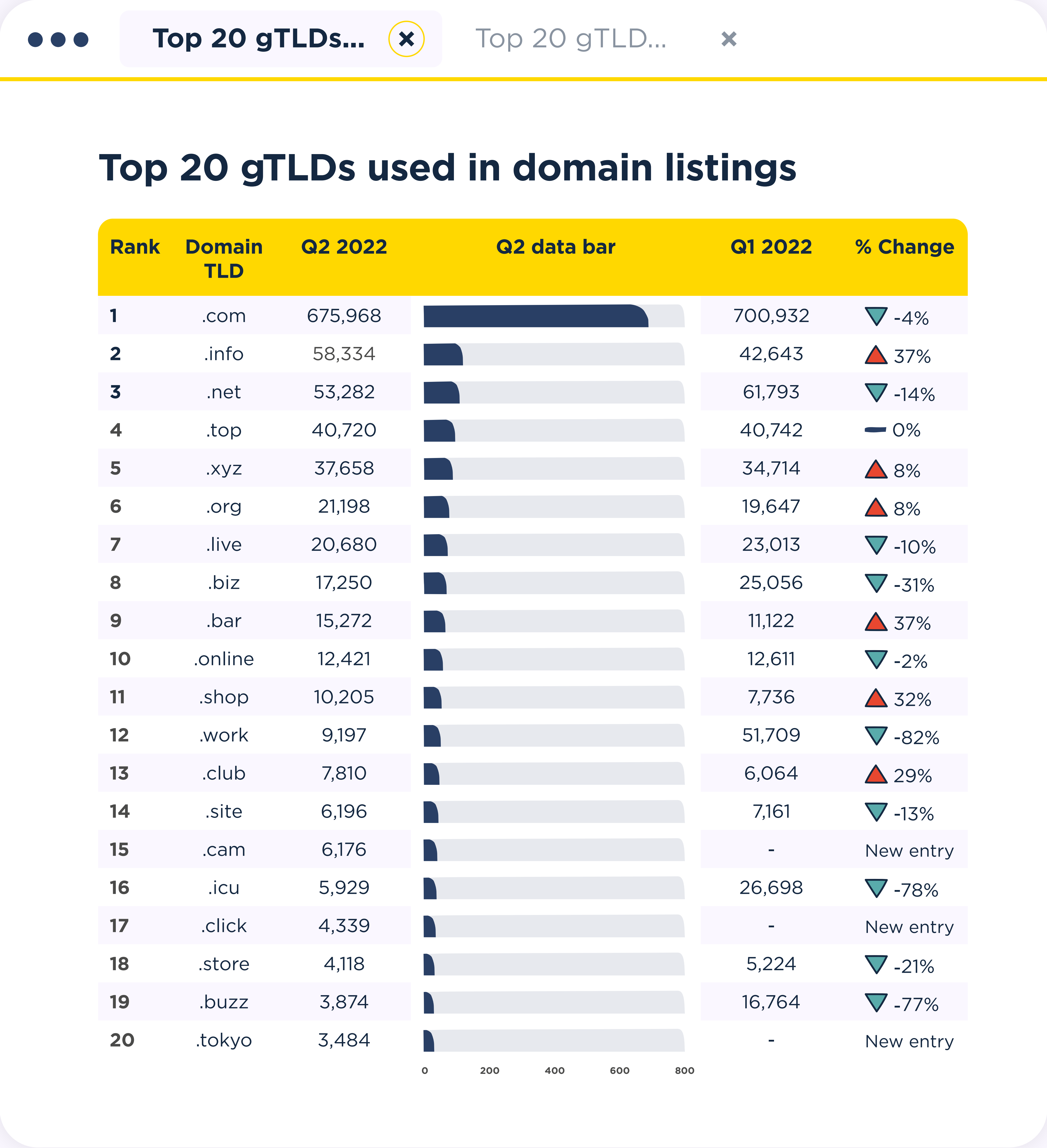
01

02

03

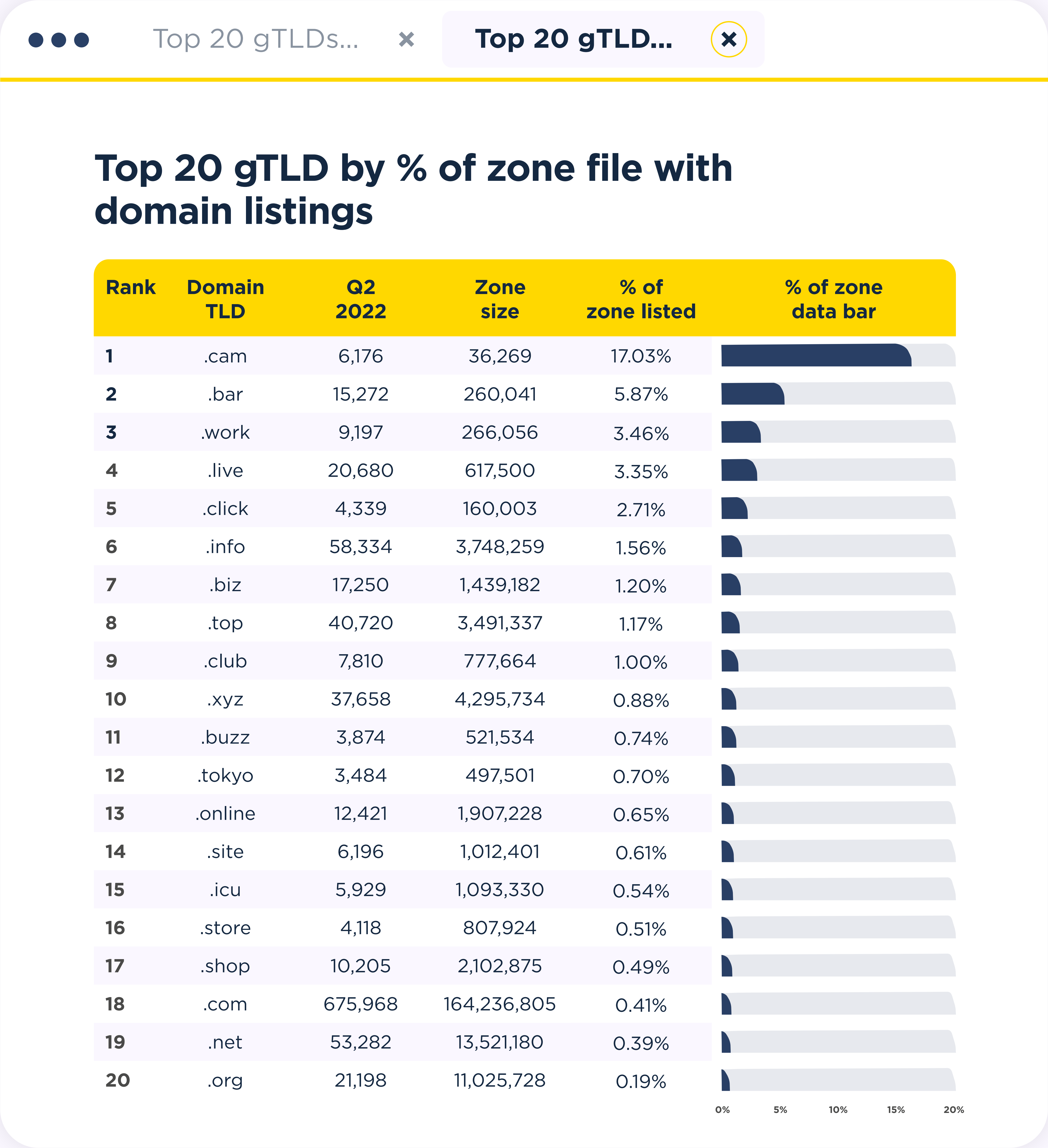
04

05


Top 20 gTLDs...
×
Top 20 gTLD...
×
0
200
400
600
800

Top 20 gTLDs used in domain listings

Rank	Domain TLD	Q2 2022	Q2 data bar	Q1 2022	% Change
1	.com	675,968		700,932	▼ -4%
2	.info	58,334		42,643	▲ 37%
3	.net	53,282		61,793	▼ -14%
4	.top	40,720		40,742	— 0%
5	.xyz	37,658		34,714	▲ 8%
6	.org	21,198		19,647	▲ 8%
7	.live	20,680		23,013	▼ -10%
8	.biz	17,250		25,056	▼ -31%
9	.bar	15,272		11,122	▲ 37%
10	.online	12,421		12,611	▼ -2%
11	.shop	10,205		7,736	▲ 32%
12	.work	9,197		51,709	▼ -82%
13	.club	7,810		6,064	▲ 29%
14	.site	6,196		7,161	▼ -13%
15	.cam	6,176		-	New entry
16	.icu	5,929		26,698	▼ -78%
17	.click	4,339		-	New entry
18	.store	4,118		5,224	▼ -21%
19	.buzz	3,874		16,764	▼ -77%
20	.tokyo	3,484		-	New entry


Top 20 gTLDs...
×
Top 20 gTLD...
×
0%
5%
10%
15%
20%

Top 20 gTLD by % of zone file with domain listings

Rank	Domain TLD	Q2 2022	Zone size	% of zone listed	% of zone data bar
1	.cam	6,176	36,269	17.03%	
2	.bar	15,272	260,041	5.87%	
3	.work	9,197	266,056	3.46%	
4	.live	20,680	617,500	3.35%	
5	.click	4,339	160,003	2.71%	
6	.info	58,334	3,748,259	1.56%	
7	.biz	17,250	1,439,182	1.20%	
8	.top	40,720	3,491,337	1.17%	
9	.club	7,810	777,664	1.00%	
10	.xyz	37,658	4,295,734	0.88%	
11	.buzz	3,874	521,534	0.74%	
12	.tokyo	3,484	497,501	0.70%	
13	.online	12,421	1,907,228	0.65%	
14	.site	6,196	1,012,401	0.61%	
15	.icu	5,929	1,093,330	0.54%	
16	.store	4,118	807,924	0.51%	
17	.shop	10,205	2,102,875	0.49%	
18	.com	675,968	164,236,805	0.41%	
19	.net	53,282	13,521,180	0.39%	
20	.org	21,198	11,025,728	0.19%	

01

02

03

04

05

Trending terms...

Trending phishing terms in domain listings

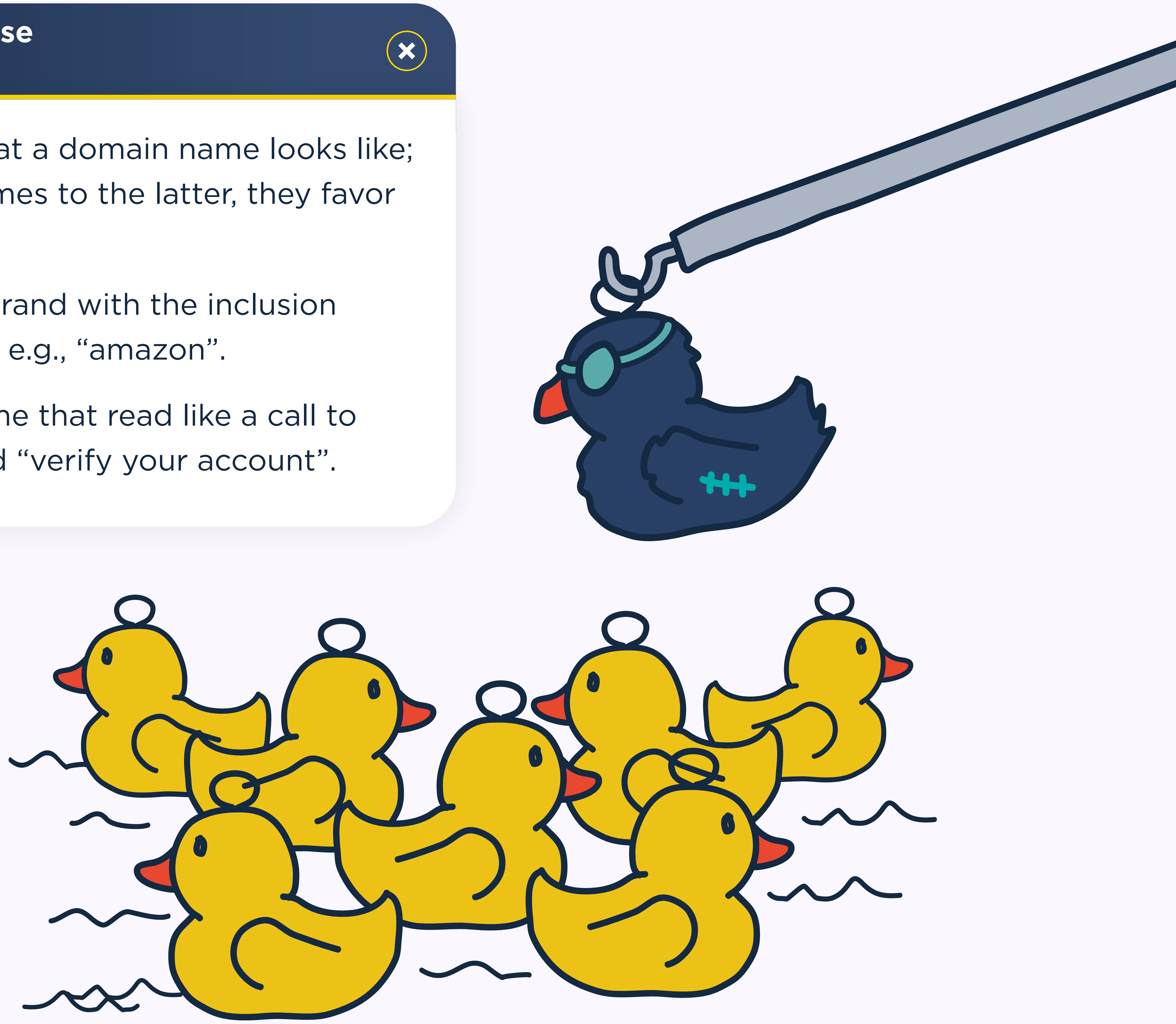
At the top of the table (again) is “amazon” as the number one term and brand name used in phishing domains. Meanwhile, “apple” increased by 104% in popularity for phishing campaigns, only to be outdone by “icloud” with a 133% rise. However, one brand term did drop off the Top 20 list in Q2; “fedex”.

When it comes to phishing domains, Spamhaus researchers regularly see bad actors using a “call to action” in the domain name. The Top 20 reflects this with words like “verify”, “review” and “update” appearing. This quarter we saw “bank” enter straight in at #4, with “info” not far behind at #7.

What terms do bad actors use for domain names?

Some miscreants don’t care what a domain name looks like; however, others do. When it comes to the latter, they favor one of two options:

1. Try to look like a legitimate brand with the inclusion of a well-known brand name, e.g., “amazon”.
2. Use words in the domain name that read like a call to action, e.g. “update now” and “verify your account”.



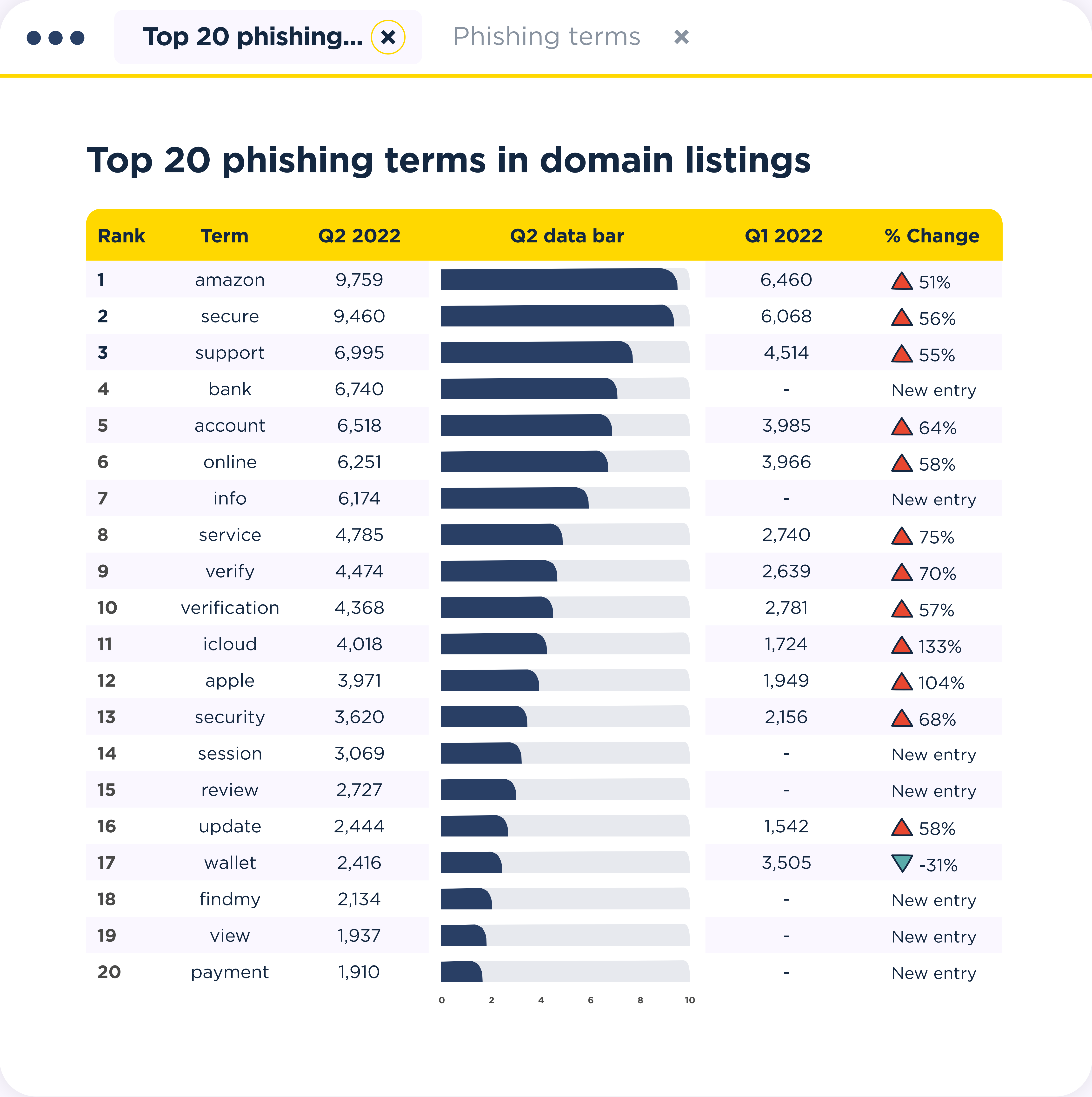
01

02

03

04

05



Top 20 phishing terms in domain listings

Rank	Term	Q2 2022	Q1 2022	% Change
1	amazon	9,759	6,460	▲ 51%
2	secure	9,460	6,068	▲ 56%
3	support	6,995	4,514	▲ 55%
4	bank	6,740	-	New entry
5	account	6,518	3,985	▲ 64%
6	online	6,251	3,966	▲ 58%
7	info	6,174	-	New entry
8	service	4,785	2,740	▲ 75%
9	verify	4,474	2,639	▲ 70%
10	verification	4,368	2,781	▲ 57%
11	icloud	4,018	1,724	▲ 133%
12	apple	3,971	1,949	▲ 104%
13	security	3,620	2,156	▲ 68%
14	session	3,069	-	New entry
15	review	2,727	-	New entry
16	update	2,444	1,542	▲ 58%
17	wallet	2,416	3,505	▼ -31%
18	findmy	2,134	-	New entry
19	view	1,937	-	New entry
20	payment	1,910	-	New entry

Top 20 phishing...
Phishing terms
VERIFICATION
BANK
SECURITY
SERVICE
PAYMENT
VIEW
SUPPORT
UPDATE
REVIEW
ONLINE
AMAZON
INFO
SESSION
VERIFY
ACCOUNT
ICLOUD
APPLE
FINDMY
WALLET
SECURE

Phishing terms

01

02

03

04

05

Types of listings

In Q2, it appears that when it comes to the type of abuse for compromised domains, phishing was the choice of the quarter with an 81% increase, while botnet C&C abuse reduced by 60%.

For compromised domains that are exhibiting malicious behavior, please keep a few things in mind:

- The vast majority of these compromises are done via automated means, and machines do not care about the associated TLD.
- Many compromised websites are given the "gift" of a Traffic Distribution System (TDS). These allow the bad actors to rotate content, URLs, and geoblockling. Our researchers see hundreds of unique URLs for some sites, some of which have been active for months.
- Currently, the majority of compromises we observe are at the website level. In these cases, a content management system (CMS) like WordPress or Drupal usually contains an exploitable flaw that gets used to insert malicious files or code into the website. Bad actors use these to get "free" domains with (almost always) an existing, good reputation - the opposite of buying a brand-new domain with no reputation. The added bonus is that these domains will not be taken down, as the owners are legitimate.
- In a few cases, we see compromises at the DNS level. These usually occur through stolen registrar credentials or sometimes through stolen or hacked administration panels like cPanel or Plesk. Once control over the authoritative DNS is in the hands of bad actors, it's easy for them to add hostnames that can point to their own infrastructure. Again, the benefit here is that existing domains with a good reputation are being used for bad purposes.

Differences between compromised and malicious domains

A **compromised domain** is where it is evident to our research team that the domain has a legitimate owner; however, a bad actor has compromised it. One example is where a content management system (CMS) is hacked, and the domain is being used to send spam resulting in the listing of the domain. Within Spamhaus these types of listings are referred to as "abused-legit".

A **malicious domain** is where a domain is registered by the person committing the internet abuse.

01

02

03

04

05

Types of listings

Bad reputation

	Malicious	Compromised
Count	969,475	12,715
Change	▼ -16% ▼	▼ -22% ▼

A domain's reputation score has exceeded policy limits.

Botnet C&C

	Malicious	Compromised
Count	4,773	57
Change	▼ -25% ▼	▼ -60% ▼

A domain is registered for use for a botnet command and controller (C&C). (A subset of bad reputation.)

Malware

	Malicious	Compromised
Count	6,278	4,400
Change	▲ 55% ▲	▼ -6% ▼

A domain observed to be used in the distribution of malware. (A subset of bad reputation.)

Phishing

	Malicious	Compromised
Count	278,341	14,630
Change	▲ 6% ▲	▲ 81% ▲

A domain is associated with phishing activities. (A subset of bad reputation.)

01

02

03

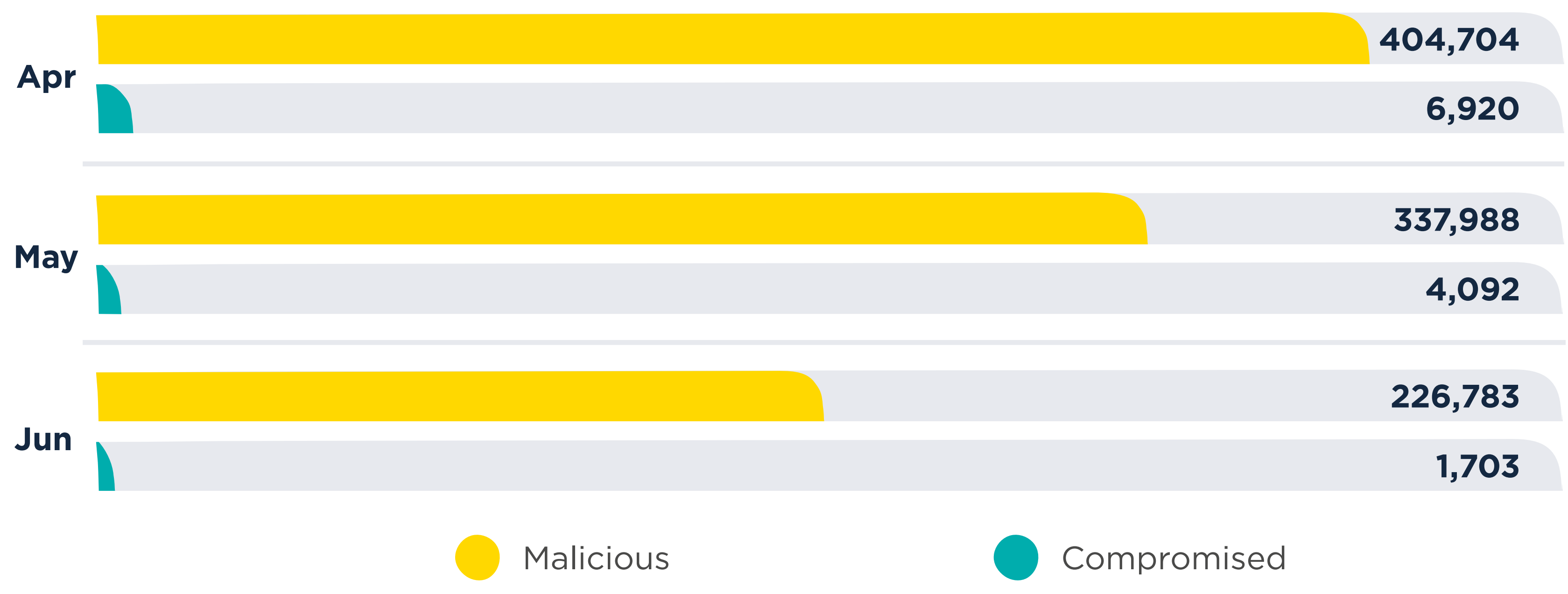
04

05

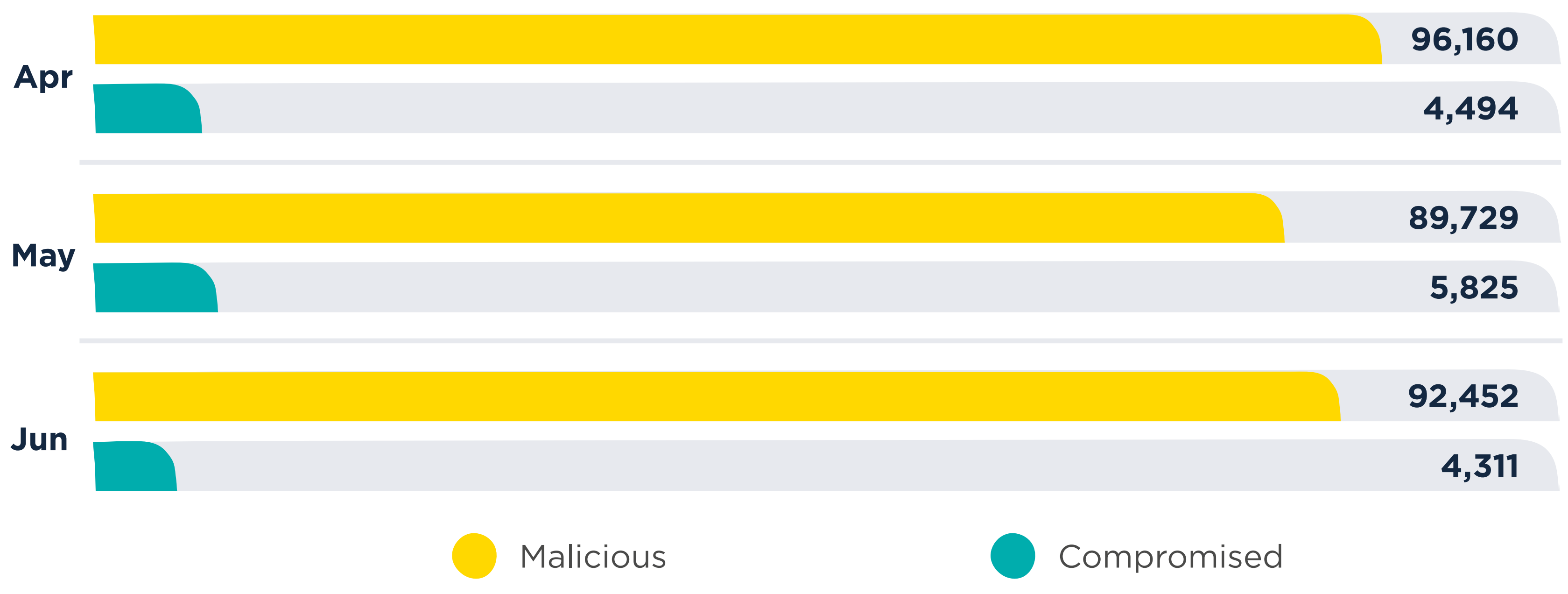
Types of abuse ×

Types of abuse

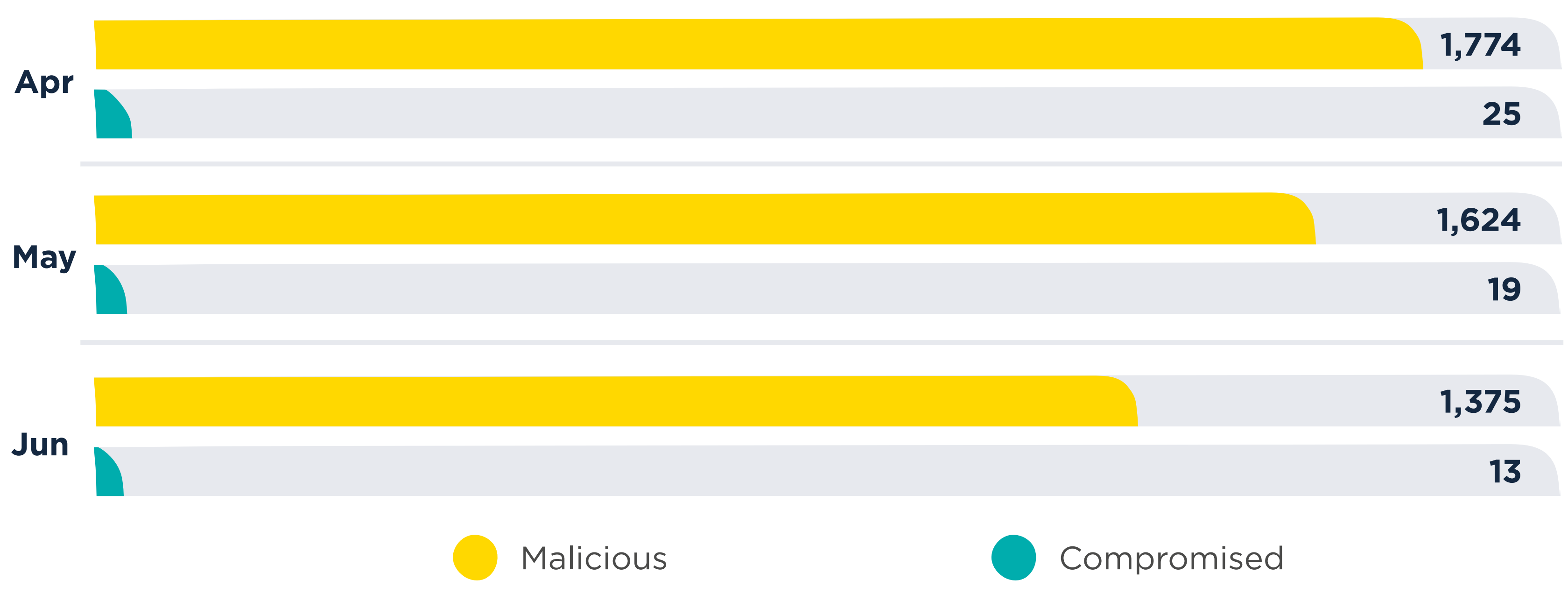
Bad reputation per month



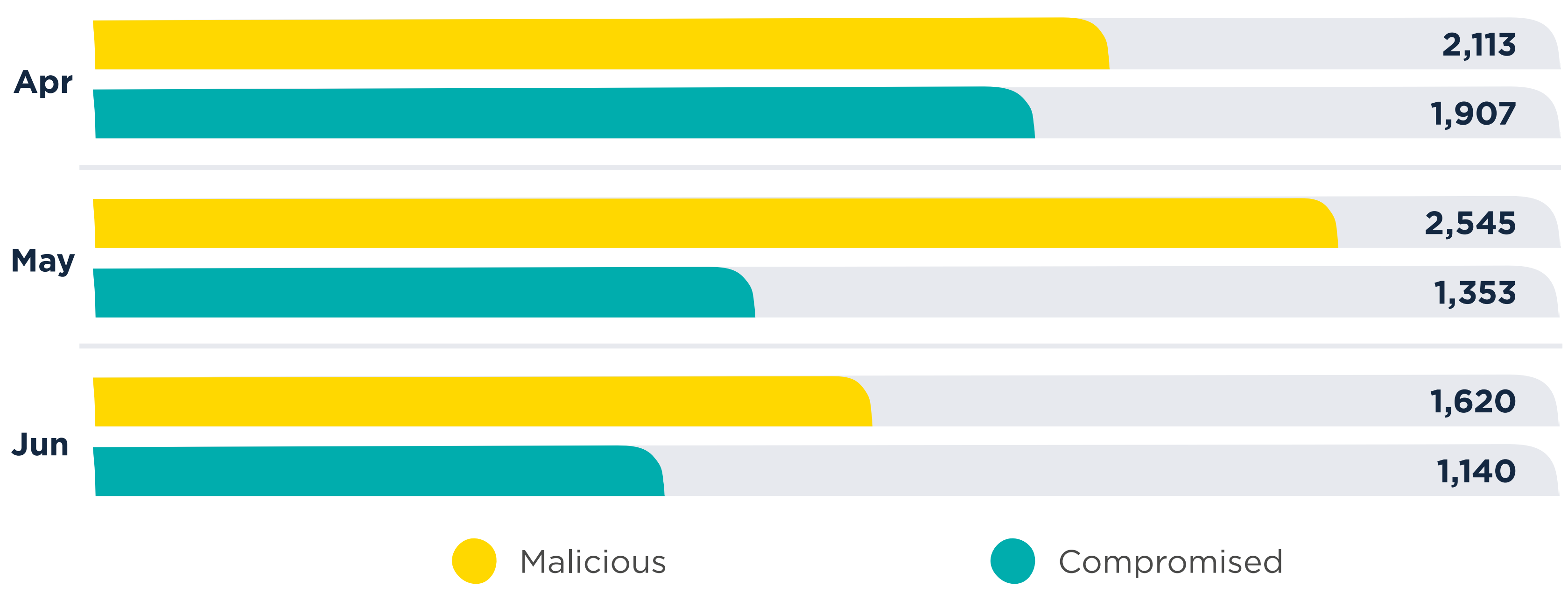
Phishing per month



Botnet C&C per month



Malware per month



Recommendations of the quarter

As this is the first published report, we'll begin with some generic recommendations around domain name reputation for domain owners. Not all of these will apply to everyone, and some may appear on the generic side, but it's good to keep these things in mind when making decisions involving your domain names.

- **If you control your domain name, ensure it stays that way.** Have a strong and unique login/password combination for domain name management and add 2FA onto that.
- **Hosting your domain name on a questionable network may reflect poorly on its reputation.** Just as a business contributes to the character of the neighborhood, so the neighborhood's character reflects on the business. Remember that domains work in the same way!
- **Anonymity does not contribute to good reputation.** If a company/business owns a domain name, make sure it is visible in WHOIS/RDAP. Even though a business name is not PII, many registrars will still filter it.
- **Less is more when it comes to the number of domain names you use.** When buying additional domain names, always ask yourself if using a subdomain of your primary domain name is better. Often it is. If you really need different domain names, ensure they can be easily tied to the primary domain name, and always consider the reputational impact of a new domain name on email, SEO, and customer/audience expectations. A new domain that looks too much like your existing domain may be reported as phishing!

01
02
03
04
05

Additional info

About Spamhaus

Spamhaus is the trusted authority on IP and domain reputation, uniquely placed in the industry because of its strong ethics, impartiality, and quality of actionable data. This data not only protects but also provides insight across networks and email worldwide.

With over two decades of experience, its researchers and threat hunters focus on exposing malicious activity to make the internet a better place for everyone. A wide range of industries, including leading global technology companies, use Spamhaus' data. Currently, it protects over three billion mailboxes worldwide.

Report Methodology

- Various sources, including ISPs, ESPs, Enterprise business and research specialists share data with Spamhaus. This data is analyzed by our researchers via machine learning, heuristics, and manual investigations to identify malicious behavior and poor reputation. The data in this report reflects the malicious domains that Spamhaus has observed identified and listed, it does not reflect the entirety of malicious and bad reputation domains on the internet.
- Malicious campaigns are regularly targeted to specific geographies, ISPs or organizations. This in turn can skew figures.
- Due to ongoing issues outside of our control to do with WHOIS and RDAP data, some of our data is incomplete. This is a direct result of GDPR.
- Where we are missing zone file data we welcome registries to contact us and share this data.