SPAMHAUS

Spamhaus Domain Reputation Update

Oct 24 – Mar 25

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 threat hunters are observing, this update highlights trends and provides insights into the poor reputation of domains, and champions providers where positive improvements are seen.

Welcome to the Spamhaus Domain Reputation Update.

Enter

Contents

Contents

01
02
03
04
05

●●● The Spotlight ×

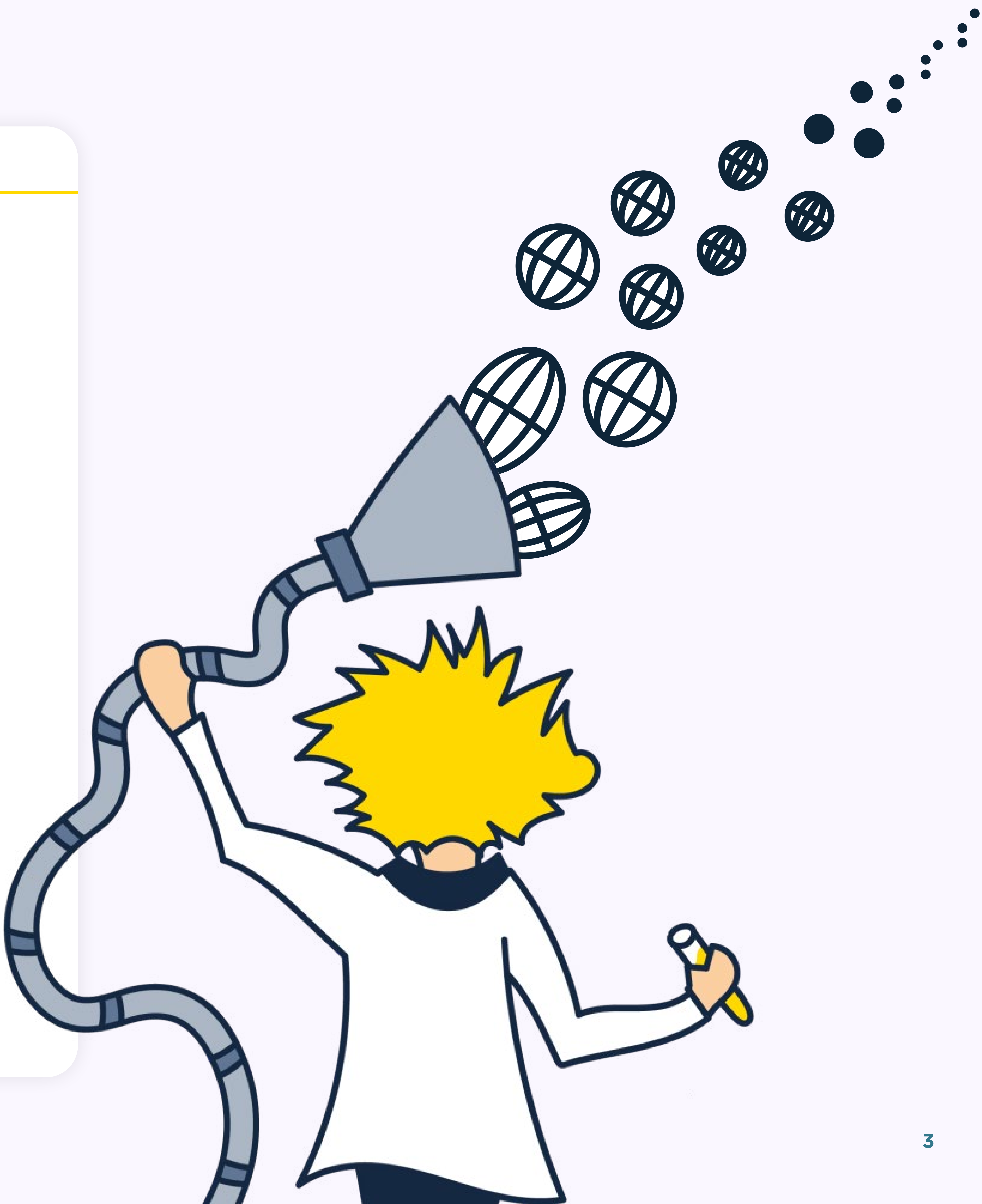
The Spotlight

Despite ICANN's formal notice citing a breach of contract and failures in handling DNS abuse, .top's abuse levels haven't improved over the last six months - in fact, they've actually gotten worse!

Having highlighted the issue in the Domain Reputation Update Oct 23 - Mar 24, .top continues to be plagued by abuse, with Spamhaus researchers observing a 50% increase and 316,433 detections over the last six months. Furthermore, APWG's Q4 2024 Phishing Activity Trends Report links .top to a growing trend of toll road scams.

These scams, often delivered via "smishing" (SMS phishing), trick recipients into believing that they owe unpaid toll fees. The messages warn of fines or even the loss of their driving license if they don't pay immediately via a provided link.

Spotlight continued



01

02

03

04

05

Spotlight cont.

Another player in this scheme is the TLD .xin. Note, this TLD also appears later in the report in relation to abuse where cybercriminals are using hyphenated domains, for example, “com-tollbillx.xin” to exploit the credibility of TLDs like .com.

Most interestingly, both .top and .xin domains are primarily registered through Dominet (HK) Limited, a registrar that until recently operated under the name Alibaba.com Singapore E-Commerce Private Limited. Why the sudden name change? It comes after ICANN issued them with a compliance notice last year.

Is this all a wild coincidence? Given .top’s history, it seems unlikely. With .top once again in the spotlight, we hope ICANN takes a closer look and intensifies its efforts to tackle this escalating abuse.

01

02

03

04

05

New domains × Number of new... ×

New domains

New domains overview

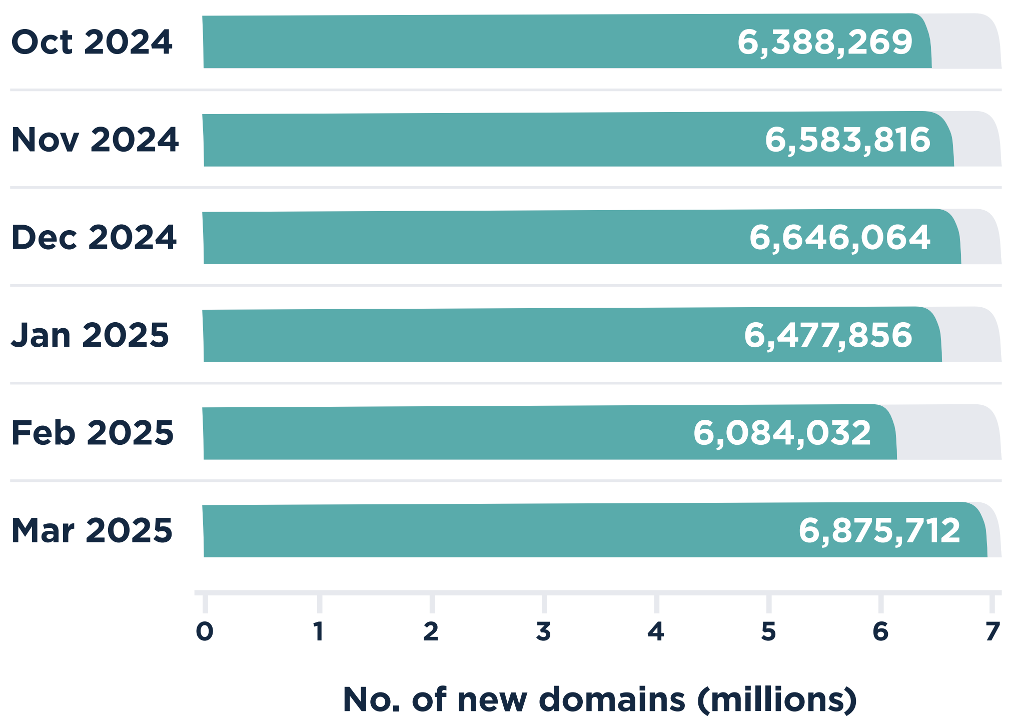
Over 39 million new domains were registered over the last six months, averaging 6.5 million new registrations per month. Compared with the previous six months, registrations have increased by 7.39%.

The busiest month was March with almost 6.9 million new domains, however all six months were close to the monthly average with minimal difference.

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 often 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



Six Month Total

39,055,749

▲ 7.39% ▲

Monthly Average

6,509,291.5

▲ 447,934 ▲

What is a new domain?

Spamhaus classifies a "new domain" as one that has been newly registered or newly observed and lists them 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.

New domains... × TLD types... ×

New domains by top-level domain (TLD)

Over the last six months, the distribution of new TLD registrations remains unchanged, with ccTLDs accounting for 29% and gTLDs for 71%.

After almost six years, .my.id, the ccTLD for Indonesia, entered the Top 20 at #18 for the first time. Although intended for personal domain names, most new registrations are due to phishing activity with domains like “signin.my.id and iosweb.my.id.”

The ccTLD for Anguilla in the Caribbean, .ai, continues its rise in popularity, climbing three places to #16, with a 23% increase. Meanwhile, new domain registrations were unusually high for .de, Germany’s ccTLD.

Radix-linked gTLDs continue to hold strong, with four entries in the Top 20 gTLDs: .online (#6), .store (#8), .site (#11), and .fun (#17). These TLDs are typically known for being low cost, with some promotions offering domains for as little as $1.

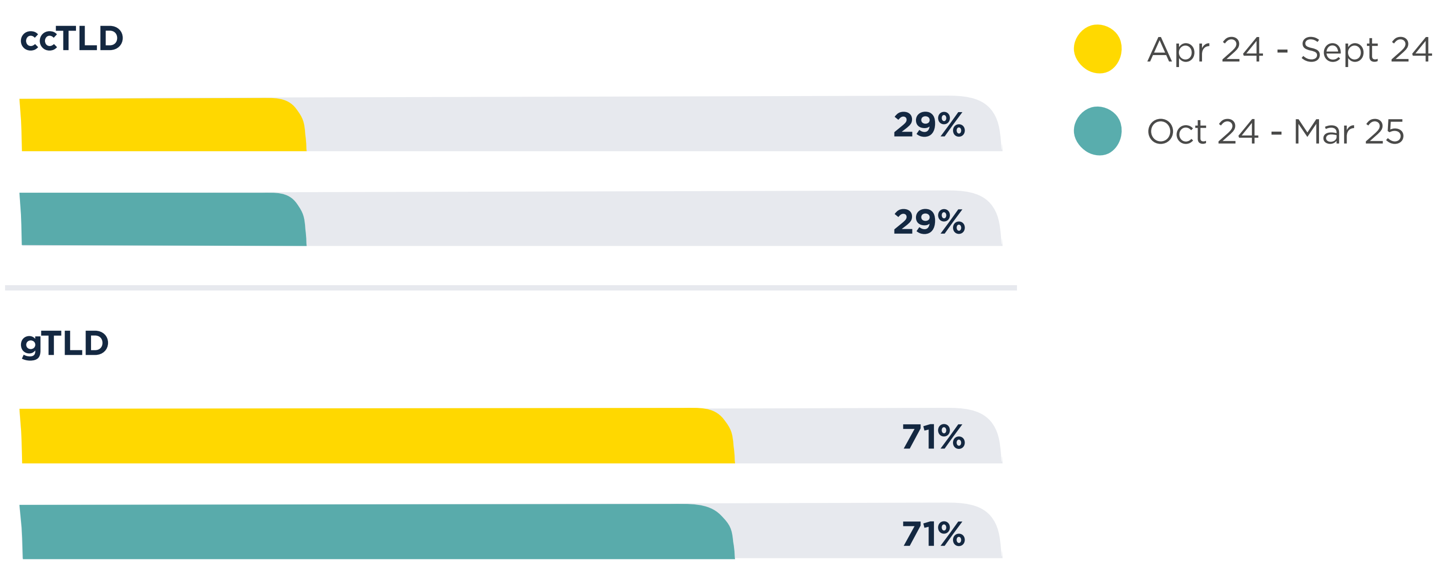
.info has also seen a surge in new domains, increasing by 75% due to a pricing drop to less than $3. If you lower prices, predictably, you’ll get more registrations - and often more abuse!

Finally, .bond remains #1 for gTLDs by zone size. In the last report, new domain registrations exceeded the zone size, a pattern we continue to observe. Over the last 6 months, despite 1.1 million new registrations, only 560,000 remain in the zone file - this suggests approximately 1 million suspensions!

Perhaps unsurprisingly, .bond continues to feature in our poor reputation TLD statistics, as detailed later in this report.

New domains... × TLD types... ×

New domain TLD types - six month comparison



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.

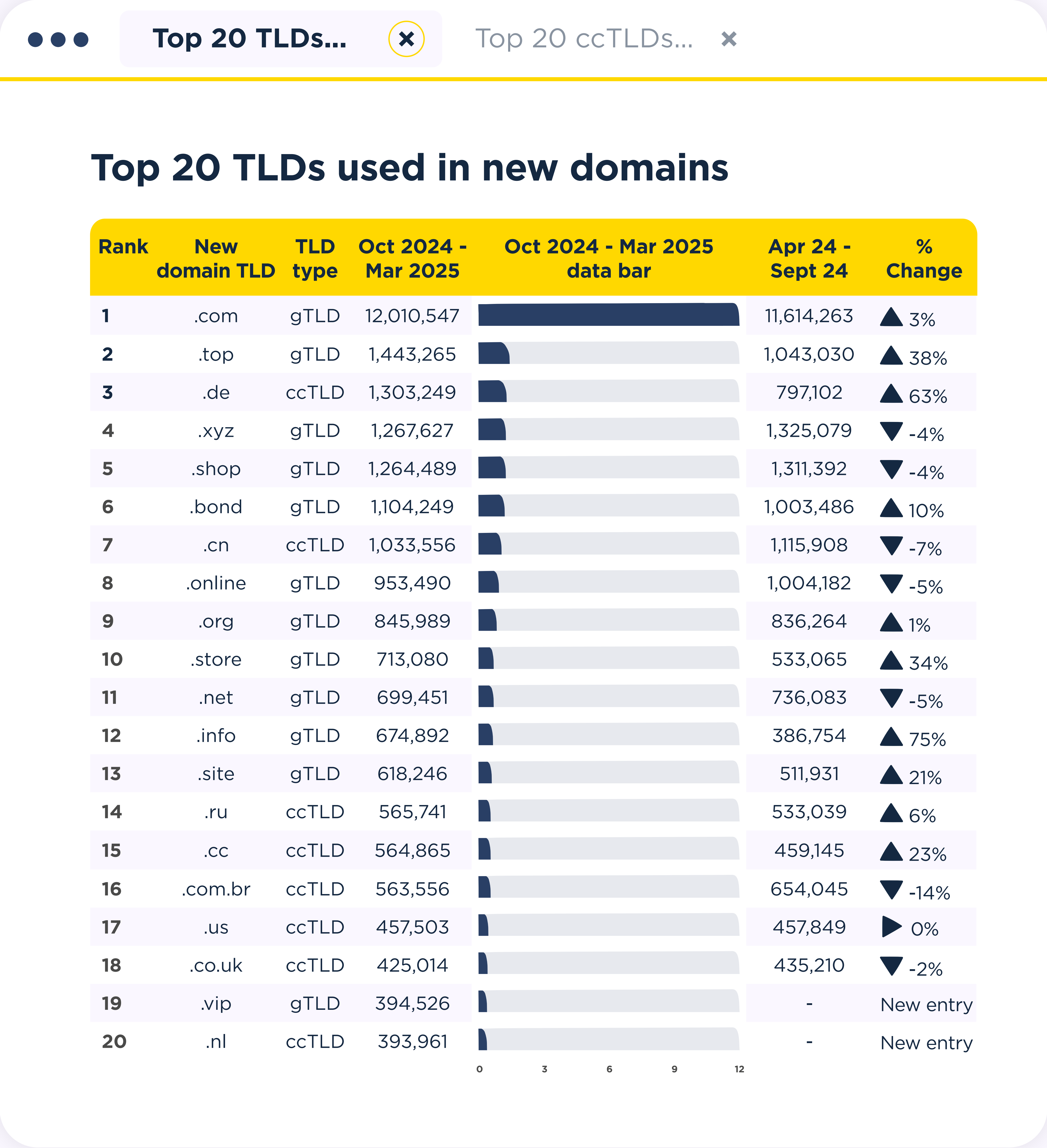
01

02

03

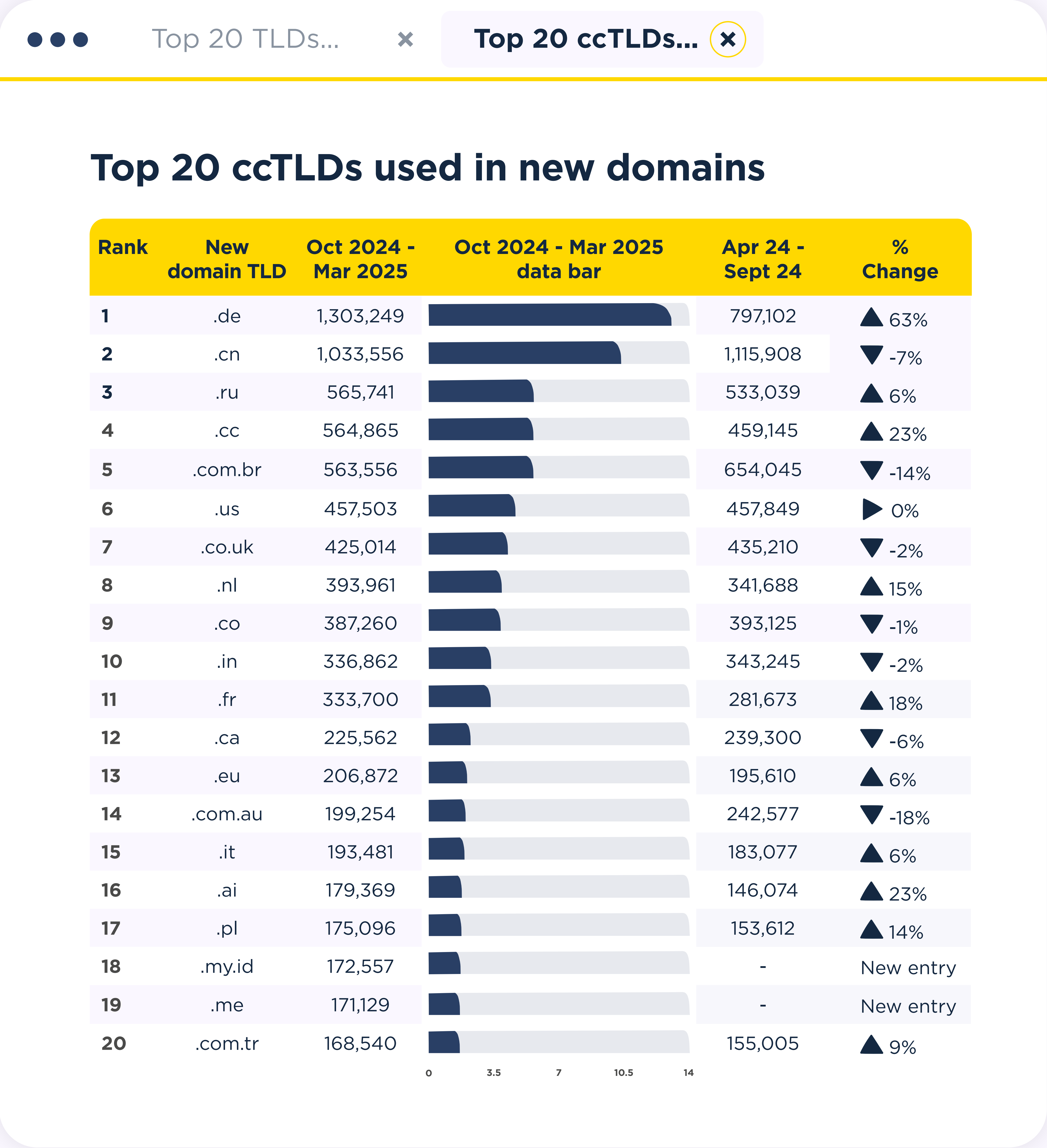
04

05


Top 20 TLDs...
Top 20 ccTLDs...
0
3
6
9
12

Top 20 TLDs used in new domains

Rank	New domain TLD	TLD type	Oct 2024 - Mar 2025	Oct 2024 - Mar 2025 data bar	Apr 24 - Sept 24	% Change
1	.com	gTLD	12,010,547		11,614,263	▲ 3%
2	.top	gTLD	1,443,265		1,043,030	▲ 38%
3	.de	ccTLD	1,303,249		797,102	▲ 63%
4	.xyz	gTLD	1,267,627		1,325,079	▼ -4%
5	.shop	gTLD	1,264,489		1,311,392	▼ -4%
6	.bond	gTLD	1,104,249		1,003,486	▲ 10%
7	.cn	ccTLD	1,033,556		1,115,908	▼ -7%
8	.online	gTLD	953,490		1,004,182	▼ -5%
9	.org	gTLD	845,989		836,264	▲ 1%
10	.store	gTLD	713,080		533,065	▲ 34%
11	.net	gTLD	699,451		736,083	▼ -5%
12	.info	gTLD	674,892		386,754	▲ 75%
13	.site	gTLD	618,246		511,931	▲ 21%
14	.ru	ccTLD	565,741		533,039	▲ 6%
15	.cc	ccTLD	564,865		459,145	▲ 23%
16	.com.br	ccTLD	563,556		654,045	▼ -14%
17	.us	ccTLD	457,503		457,849	▶ 0%
18	.co.uk	ccTLD	425,014		435,210	▼ -2%
19	.vip	gTLD	394,526		-	New entry
20	.nl	ccTLD	393,961		-	New entry


Top 20 TLDs...
Top 20 ccTLDs...
0
3.5
7
10.5
14

Top 20 ccTLDs used in new domains

Rank	New domain TLD	Oct 2024 - Mar 2025	Oct 2024 - Mar 2025 data bar	Apr 24 - Sept 24	% Change
1	.de	1,303,249		797,102	▲ 63%
2	.cn	1,033,556		1,115,908	▼ -7%
3	.ru	565,741		533,039	▲ 6%
4	.cc	564,865		459,145	▲ 23%
5	.com.br	563,556		654,045	▼ -14%
6	.us	457,503		457,849	▶ 0%
7	.co.uk	425,014		435,210	▼ -2%
8	.nl	393,961		341,688	▲ 15%
9	.co	387,260		393,125	▼ -1%
10	.in	336,862		343,245	▼ -2%
11	.fr	333,700		281,673	▲ 18%
12	.ca	225,562		239,300	▼ -6%
13	.eu	206,872		195,610	▲ 6%
14	.com.au	199,254		242,577	▼ -18%
15	.it	193,481		183,077	▲ 6%
16	.ai	179,369		146,074	▲ 23%
17	.pl	175,096		153,612	▲ 14%
18	.my.id	172,557		-	New entry
19	.me	171,129		-	New entry
20	.com.tr	168,540		155,005	▲ 9%

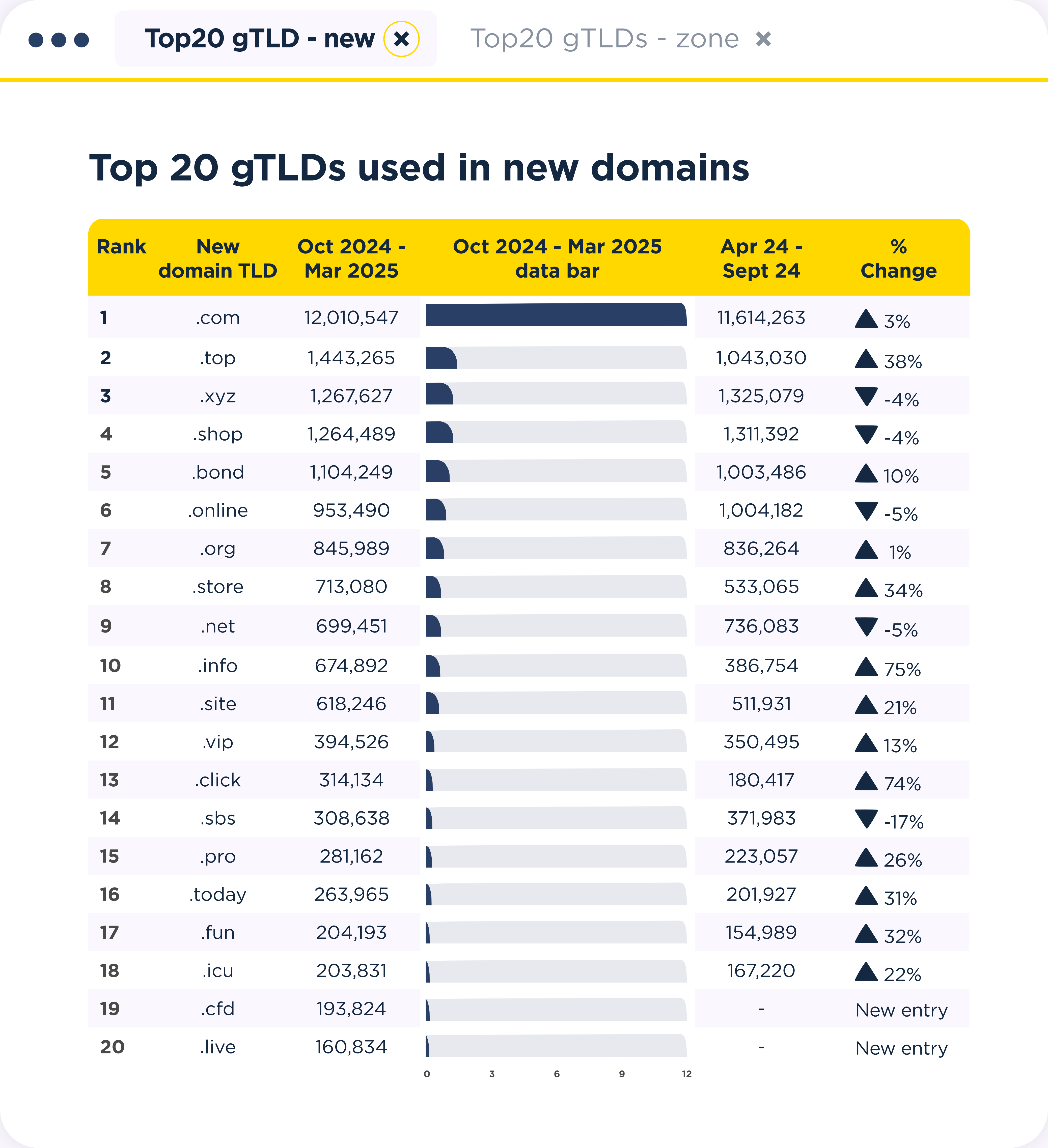
01

02

03

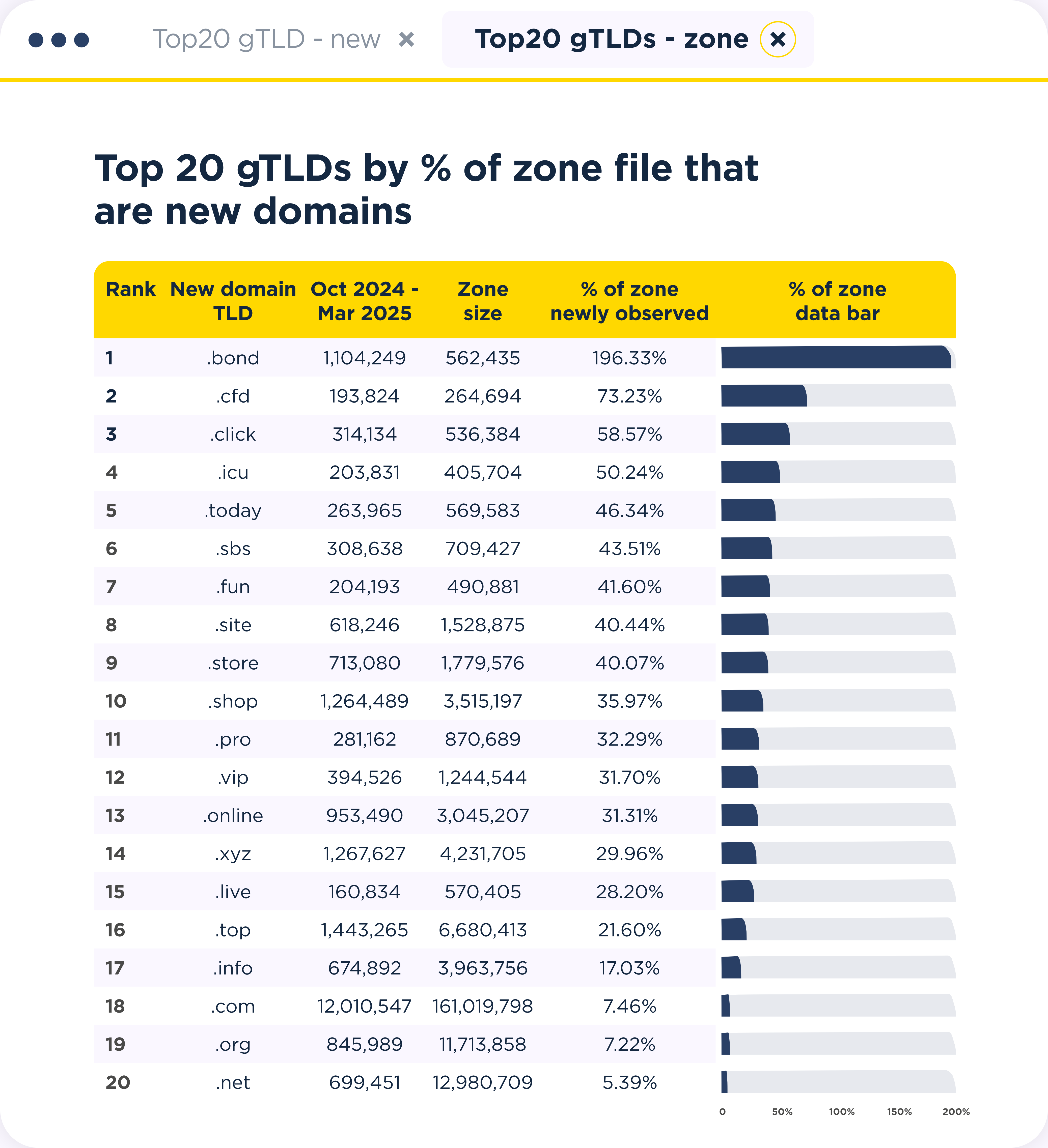
04

05


Top20 gTLD - new
Top20 gTLDs - zone
0
3
6
9
12

Top 20 gTLDs used in new domains

Rank	New domain TLD	Oct 2024 - Mar 2025	Oct 2024 - Mar 2025 data bar	Apr 24 - Sept 24	% Change
1	.com	12,010,547		11,614,263	▲ 3%
2	.top	1,443,265		1,043,030	▲ 38%
3	.xyz	1,267,627		1,325,079	▼ -4%
4	.shop	1,264,489		1,311,392	▼ -4%
5	.bond	1,104,249		1,003,486	▲ 10%
6	.online	953,490		1,004,182	▼ -5%
7	.org	845,989		836,264	▲ 1%
8	.store	713,080		533,065	▲ 34%
9	.net	699,451		736,083	▼ -5%
10	.info	674,892		386,754	▲ 75%
11	.site	618,246		511,931	▲ 21%
12	.vip	394,526		350,495	▲ 13%
13	.click	314,134		180,417	▲ 74%
14	.sbs	308,638		371,983	▼ -17%
15	.pro	281,162		223,057	▲ 26%
16	.today	263,965		201,927	▲ 31%
17	.fun	204,193		154,989	▲ 32%
18	.icu	203,831		167,220	▲ 22%
19	.cfd	193,824		-	New entry
20	.live	160,834		-	New entry


Top20 gTLD - new
Top20 gTLDs - zone
0
50%
100%
150%
200%

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

Rank	New domain TLD	Oct 2024 - Mar 2025	Zone size	% of zone newly observed	% of zone data bar
1	.bond	1,104,249	562,435	196.33%	
2	.cfd	193,824	264,694	73.23%	
3	.click	314,134	536,384	58.57%	
4	.icu	203,831	405,704	50.24%	
5	.today	263,965	569,583	46.34%	
6	.sbs	308,638	709,427	43.51%	
7	.fun	204,193	490,881	41.60%	
8	.site	618,246	1,528,875	40.44%	
9	.store	713,080	1,779,576	40.07%	
10	.shop	1,264,489	3,515,197	35.97%	
11	.pro	281,162	870,689	32.29%	
12	.vip	394,526	1,244,544	31.70%	
13	.online	953,490	3,045,207	31.31%	
14	.xyz	1,267,627	4,231,705	29.96%	
15	.live	160,834	570,405	28.20%	
16	.top	1,443,265	6,680,413	21.60%	
17	.info	674,892	3,963,756	17.03%	
18	.com	12,010,547	161,019,798	7.46%	
19	.org	845,989	11,713,858	7.22%	
20	.net	699,451	12,980,709	5.39%	

01
02
03
04
05

Trending terms...

Trending terms in new domains

As the new year begins, many people start thinking about self-improvement. This is reflected in the latest Top 20 trending terms, with new entries like training (#17), train (#18), and develop (#19).

The most interesting change to note is the 87% increase in “jobs”, which has climbed nine places to rank #5. Less than two years ago, “jobs” didn’t even feature as a trending term!

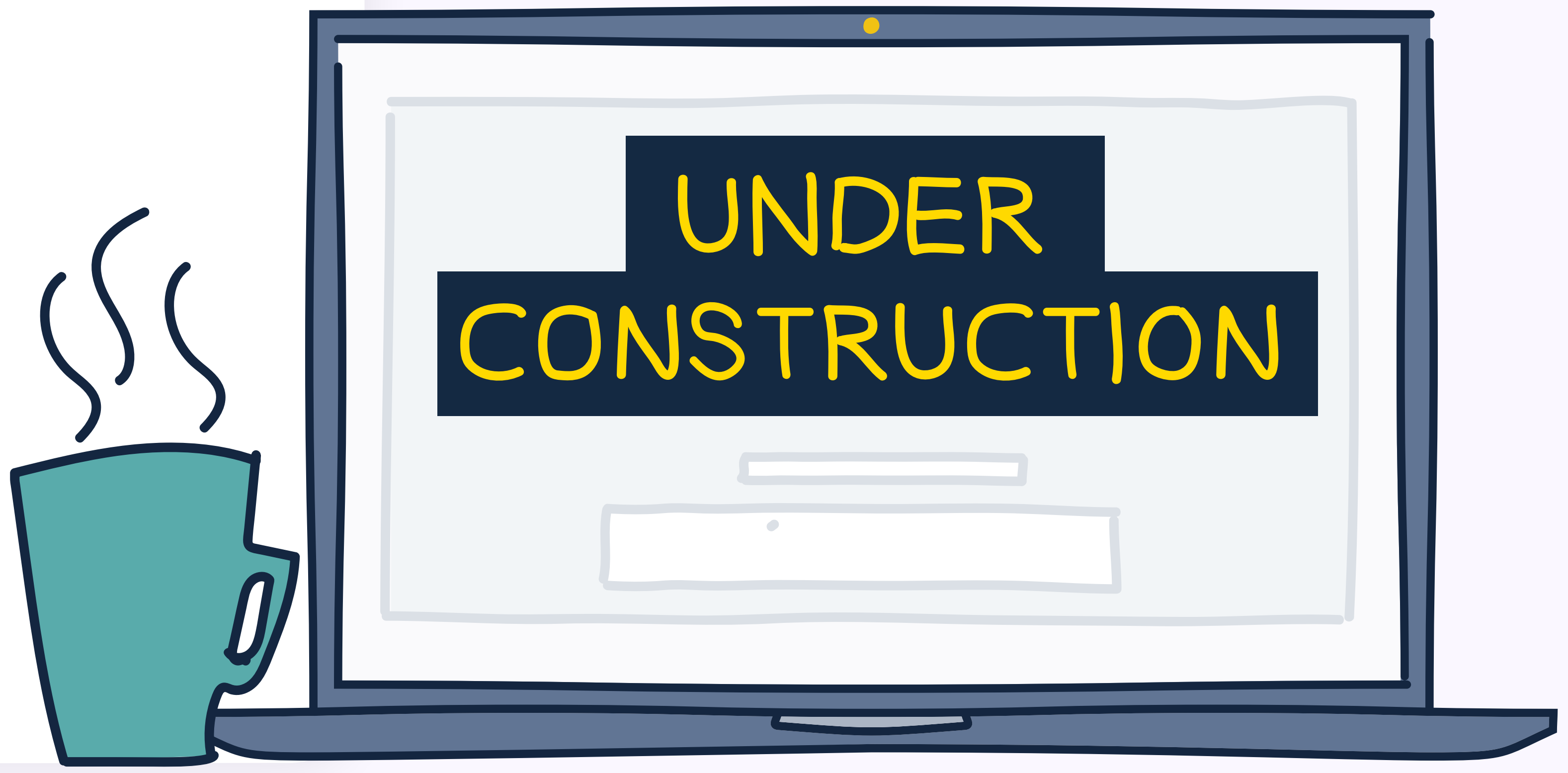
Many of these domains are registered under the gTLD , .bond, featuring the term “jobs” followed by a five-digit number, for example, “accountant-jobs-87665.bond”. As a result of these kinds of domains, we are seeing more new .bond domains being registered than currently existing in the zone file!

While the exact purpose of these domains remains unclear, many appear to be parked domains. Recently, we’ve observed an increase in parked domains being abused - a trend we’ll be monitoring.

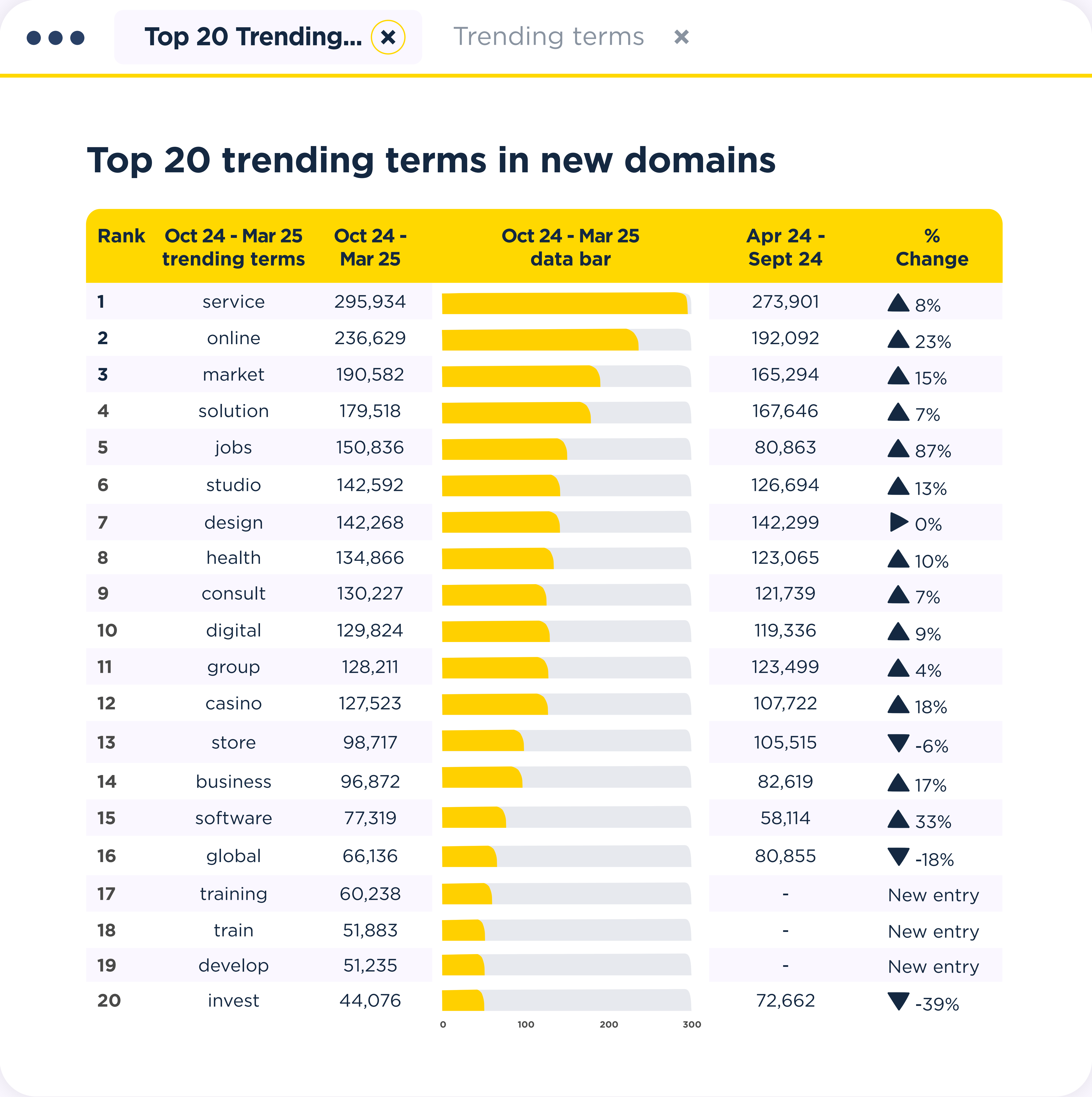
Finally, no surprises, trending terms “service” and “online” continue to hold the #1 and #2 spots.

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.

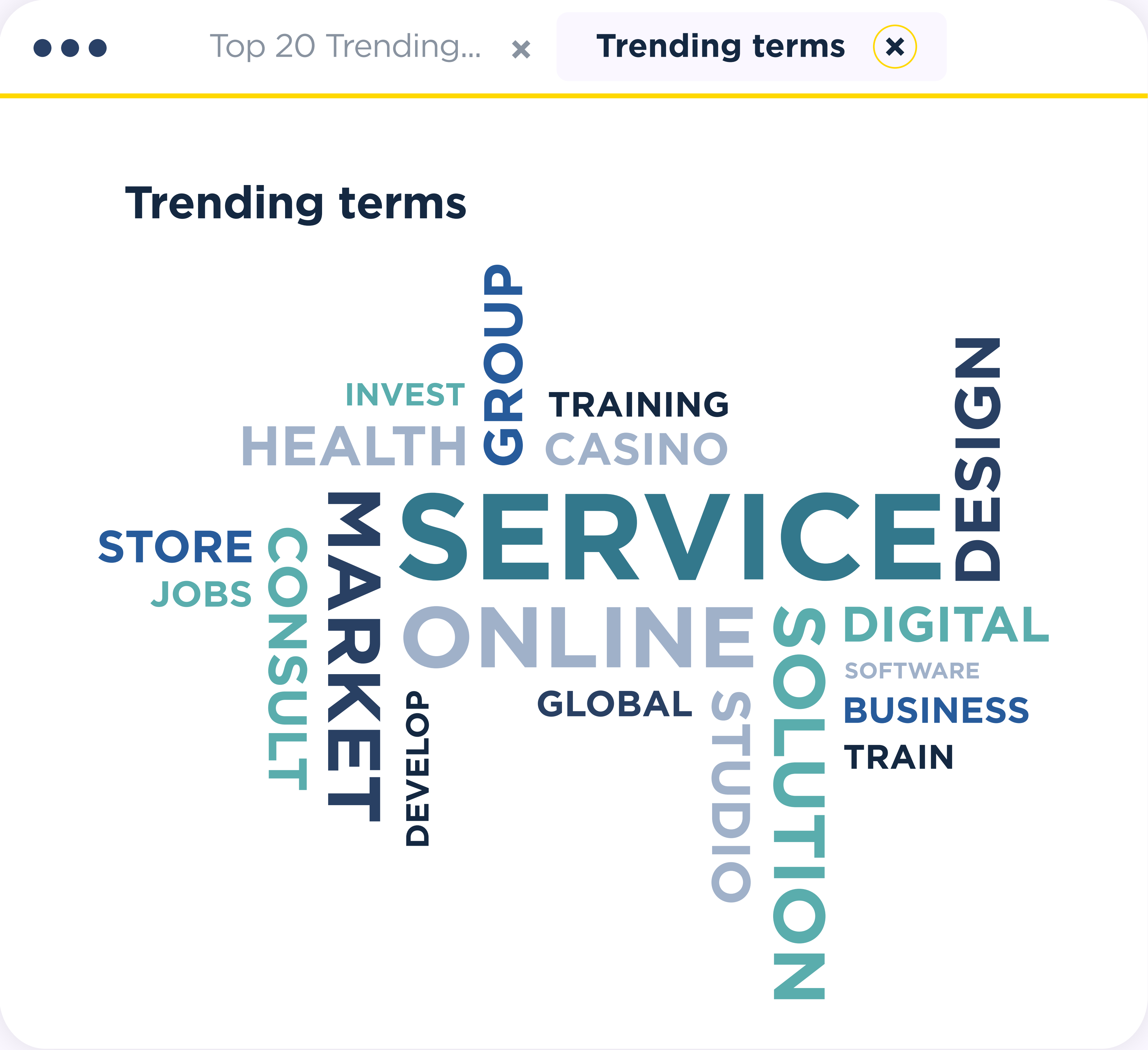


01
02
03
04
05


Top 20 Trending...
Trending terms
0
100
200
300

Top 20 trending terms in new domains

Rank	Oct 24 - Mar 25 trending terms	Oct 24 - Mar 25	Oct 24 - Mar 25 data bar	Apr 24 - Sept 24	% Change
1	service	295,934		273,901	▲ 8%
2	online	236,629		192,092	▲ 23%
3	market	190,582		165,294	▲ 15%
4	solution	179,518		167,646	▲ 7%
5	jobs	150,836		80,863	▲ 87%
6	studio	142,592		126,694	▲ 13%
7	design	142,268		142,299	▶ 0%
8	health	134,866		123,065	▲ 10%
9	consult	130,227		121,739	▲ 7%
10	digital	129,824		119,336	▲ 9%
11	group	128,211		123,499	▲ 4%
12	casino	127,523		107,722	▲ 18%
13	store	98,717		105,515	▼ -6%
14	business	96,872		82,619	▲ 17%
15	software	77,319		58,114	▲ 33%
16	global	66,136		80,855	▼ -18%
17	training	60,238		-	New entry
18	train	51,883		-	New entry
19	develop	51,235		-	New entry
20	invest	44,076		72,662	▼ -39%



Trending terms

01

02

03

04

05

Malicious/suspici... ⊗ Listings ×

Malicious/suspicious domains

Domain overview

Over the past six months, 2.19 million malicious or suspicious domains were detected, averaging 364K per month. This represents a 19.3% increase compared to the previous six months (April 2024 to September 2024).

In this reporting period, there is a significant overlap between the Top 20 TLDs for new domain registrations and those with the most malicious or suspicious activity, with 11 TLDs featuring in both Top 20 charts. As new domain registrations increase, so does abuse! Notably, .com and .top hold the #1 and #2 positions in both Top 20s.

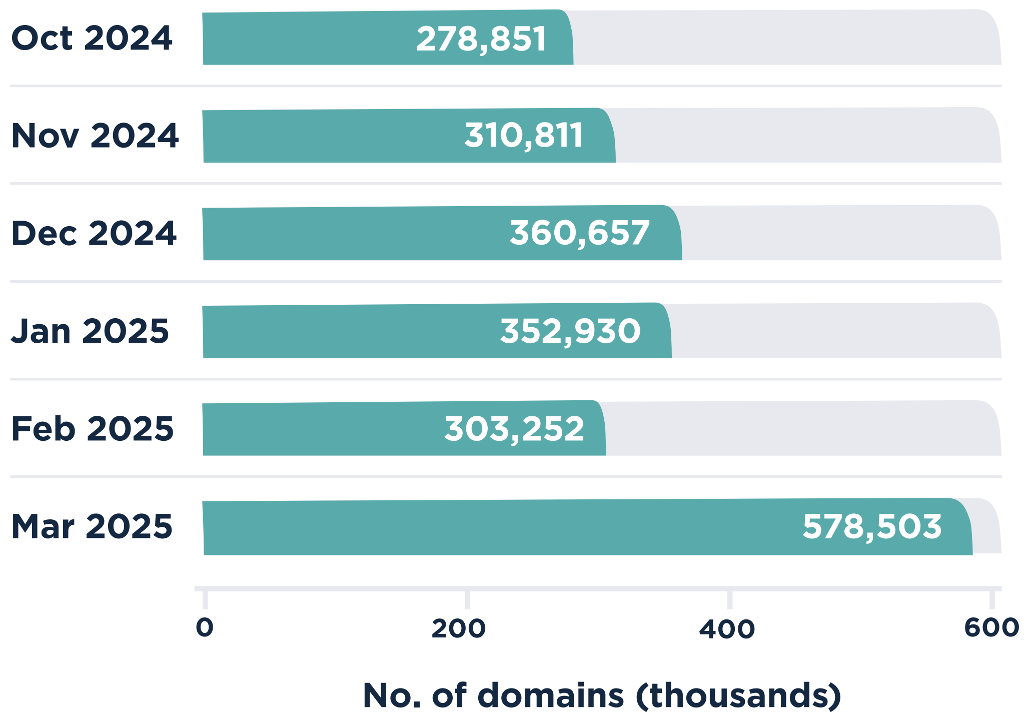
The distribution between ccTLD and gTLD has shifted marginally, with ccTLDs accounting for 19% of detections and gTLDs 81%.

.top remains at #2, with a 50% increase. As discussed earlier, despite ICANN's formal notice citing a breach of contract and failures in handling DNS abuse, there has been no positive impact on its abuse levels.

.cc (#3) and .co (#9) continue to see a rise in detections, with .cc up 66% and .co up 59%. Both remain attractive for abuse, with new domains available for less than $3.

Malicious/suspi... × Listings ⊗

Number of Domain listings per month



Six Month Total
2,185,004
△ 19.30% △

Monthly Average
364,167
△ 353,477 △

What triggers a domain to be listed as malicious/suspicious 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 noted 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

Trending terms...

TLDs listed in our domain data

Five new ccTLDs entered the Top 20 this reporting period: .my (#10), .ac (#16), .fr (#17), .jp (#18), and .ge (#19). However, .cz (#9) experienced the most significant increase of 215%. Despite this, .cc, is the most detected ccTLD, taking the top spot with 148,868 detections, over 83% more than .cn at #2.

A closer look reveals that most domains are linked to Chinese gambling sites. As gambling is illegal in mainland China, this comes as no surprise. Whilst demand exists, miscreants continue to burn through hundreds of thousands of domains to try and avoid detection.

This trend also extends to other TLDs, including .tw (#11 for ccTLDs) which saw a 109% increase, and .vip (#3 for gTLDs), which increased by 66% - both are heavily associated with Chinese gambling sites.

Eight out of the top 20 gTLDs by percentage of zone file belong to the registry BinkyMoon LLC: .town (#5), .pizza (#6), .pictures (#7), .loans (#12), .academy (#16), .plus (#17), .gold (#19), and .legal (#20). It appears they're attempting to drive new domain registrations through aggressive pricing, which as our regular readers will know, attracts abuse.

Meanwhile, new entry .xin raises concerns. More than three-quarters (82.16%) of all .xin domains in the zone file are flagged as malicious or suspicious. 75% of these domains begin with “com-”, using deceptive domains like “com-tollbillx.xin” or “com-tracking-helpbtre.xin”. To the untrained eye, these domains can be easily mistaken for legitimate sites. Interestingly, at least 90% of these .xin domains are registered through the earlier mentioned, Dominet (HK) Limited.

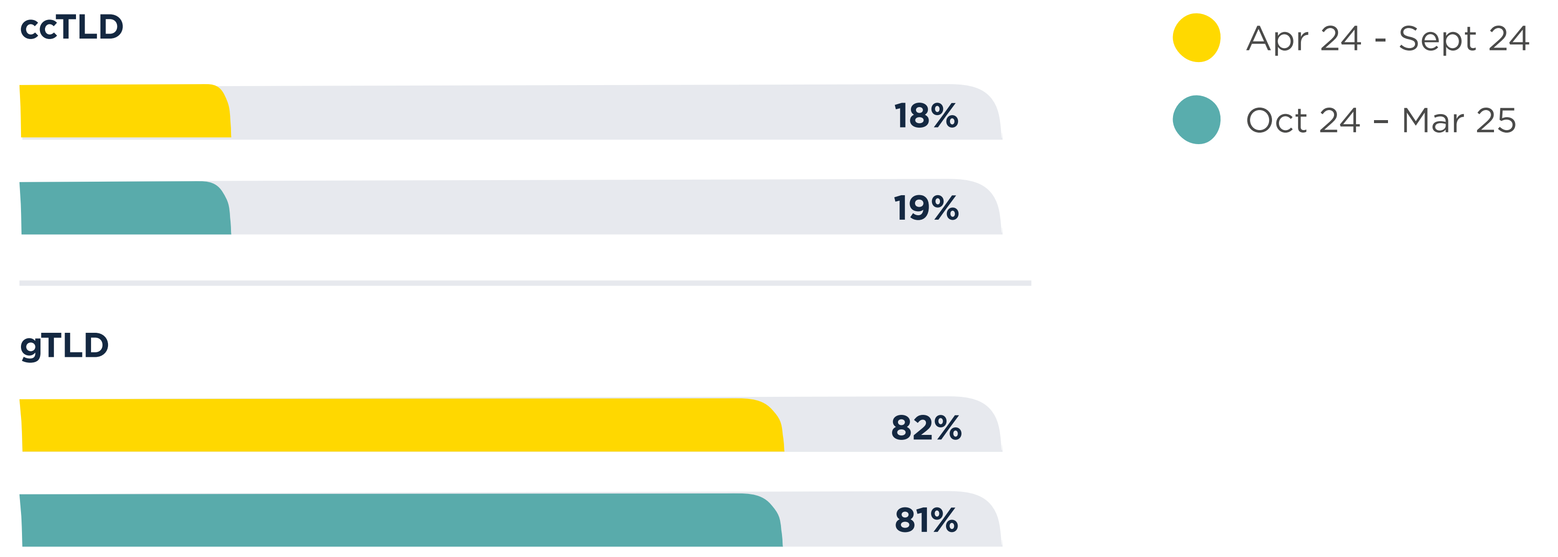
Interpreting the data

Interpreting the data - Registries with a greater number of active domains have greater exposure to abuse. For example, between Oct 2024 and Mar 2025, .gdn had more than 181,000 domains in its zone, of which 18.11% were listed.

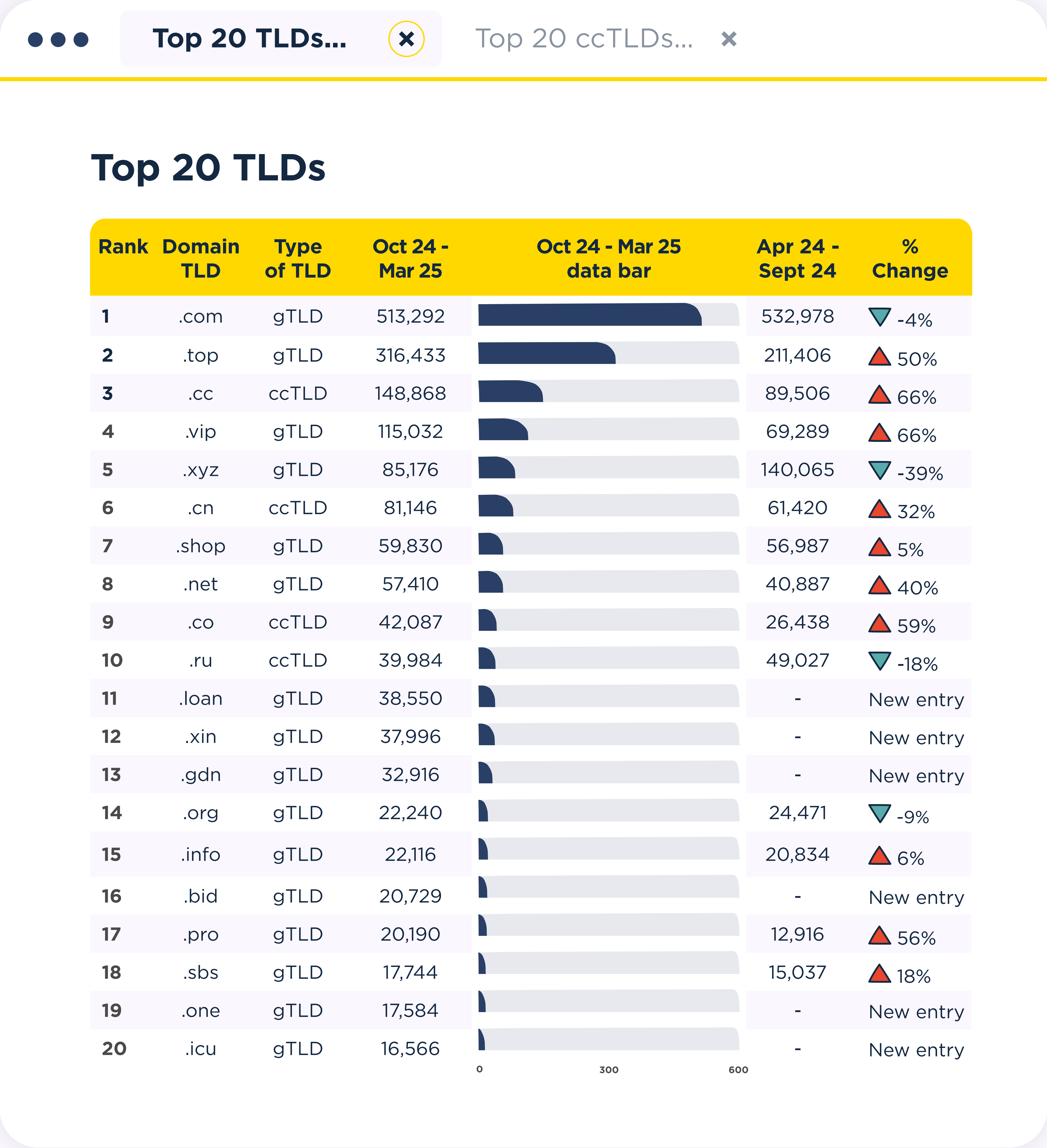
Meanwhile, .qpon had 11,655 domains in its zone, with 71.12% listed in our domain dataset. Both are in the Top 20 of our listings. Still, one had a much higher percentage of active domains listed than the other.

TLD type - six...

TLD type - six month comparison

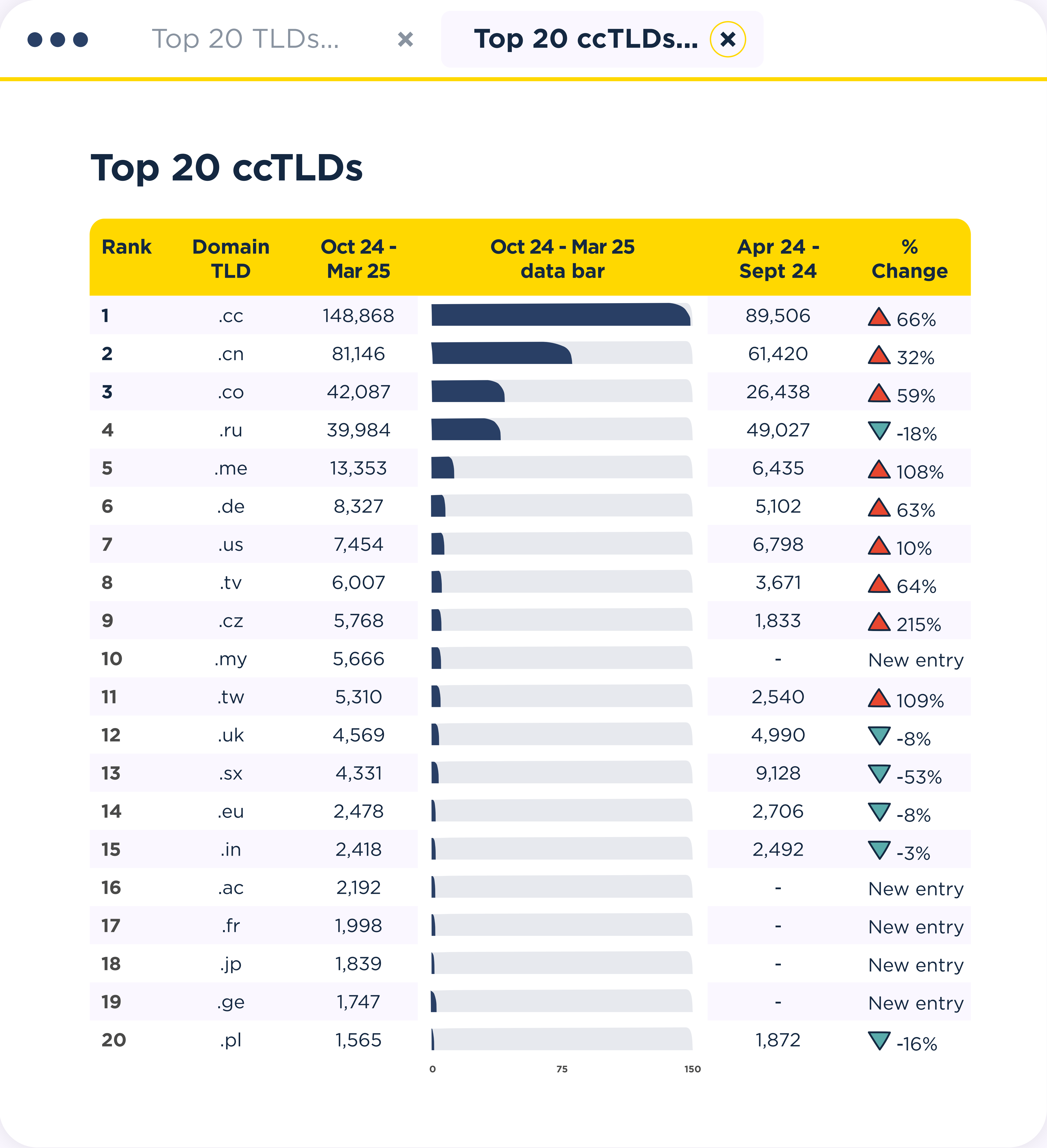


01
02
03
04
05


Top 20 TLDs...
Top 20 ccTLDs...
0
300
600

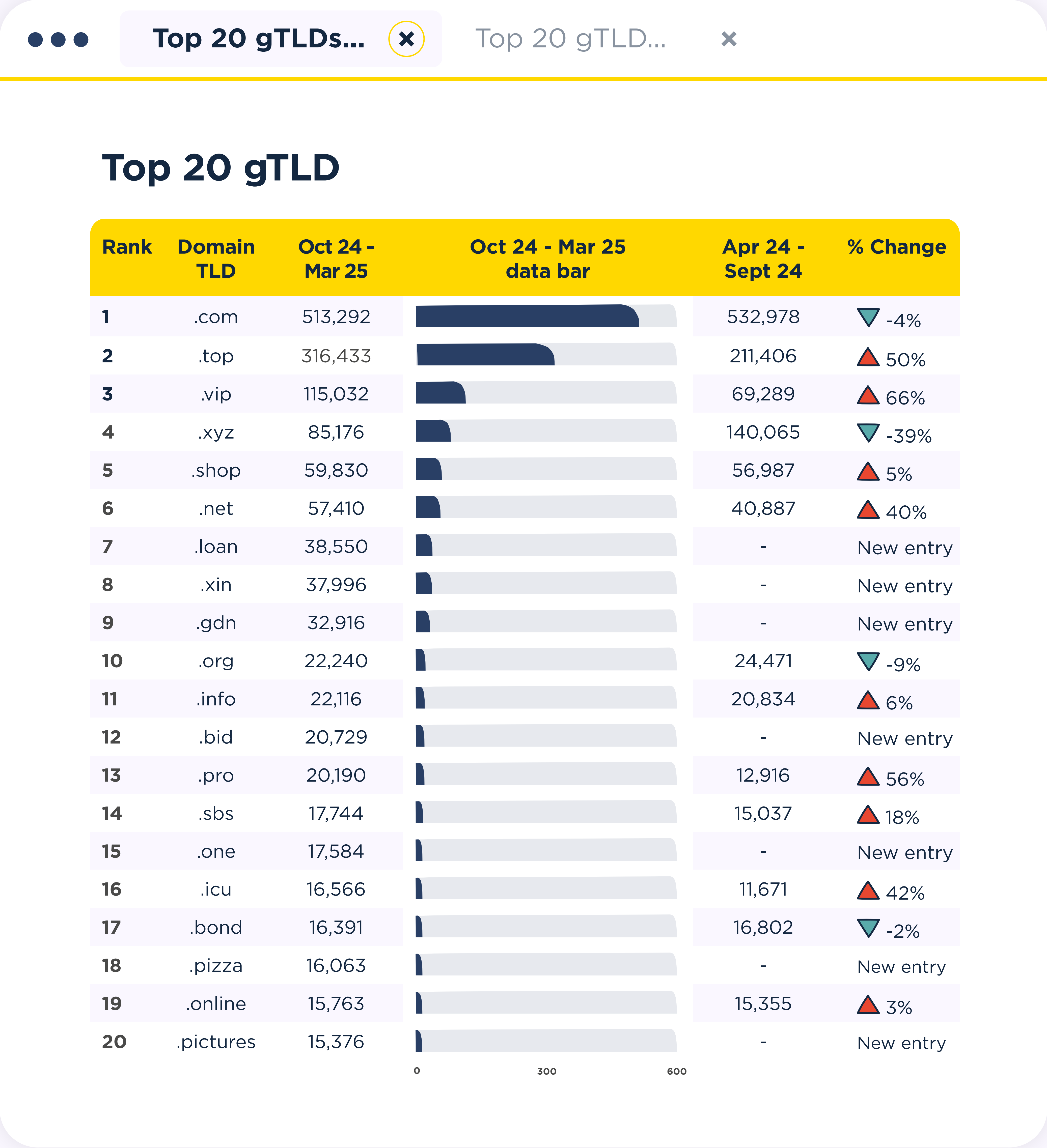
Top 20 TLDs

Rank	Domain TLD	Type of TLD	Oct 24 - Mar 25	Oct 24 - Mar 25 data bar	Apr 24 - Sept 24	% Change
1	.com	gTLD	513,292		532,978	▼ -4%
2	.top	gTLD	316,433		211,406	▲ 50%
3	.cc	ccTLD	148,868		89,506	▲ 66%
4	.vip	gTLD	115,032		69,289	▲ 66%
5	.xyz	gTLD	85,176		140,065	▼ -39%
6	.cn	ccTLD	81,146		61,420	▲ 32%
7	.shop	gTLD	59,830		56,987	▲ 5%
8	.net	gTLD	57,410		40,887	▲ 40%
9	.co	ccTLD	42,087		26,438	▲ 59%
10	.ru	ccTLD	39,984		49,027	▼ -18%
11	.loan	gTLD	38,550		-	New entry
12	.xin	gTLD	37,996		-	New entry
13	.gdn	gTLD	32,916		-	New entry
14	.org	gTLD	22,240		24,471	▼ -9%
15	.info	gTLD	22,116		20,834	▲ 6%
16	.bid	gTLD	20,729		-	New entry
17	.pro	gTLD	20,190		12,916	▲ 56%
18	.sbs	gTLD	17,744		15,037	▲ 18%
19	.one	gTLD	17,584		-	New entry
20	.icu	gTLD	16,566		-	New entry


Top 20 TLDs...
Top 20 ccTLDs...
0
75
150

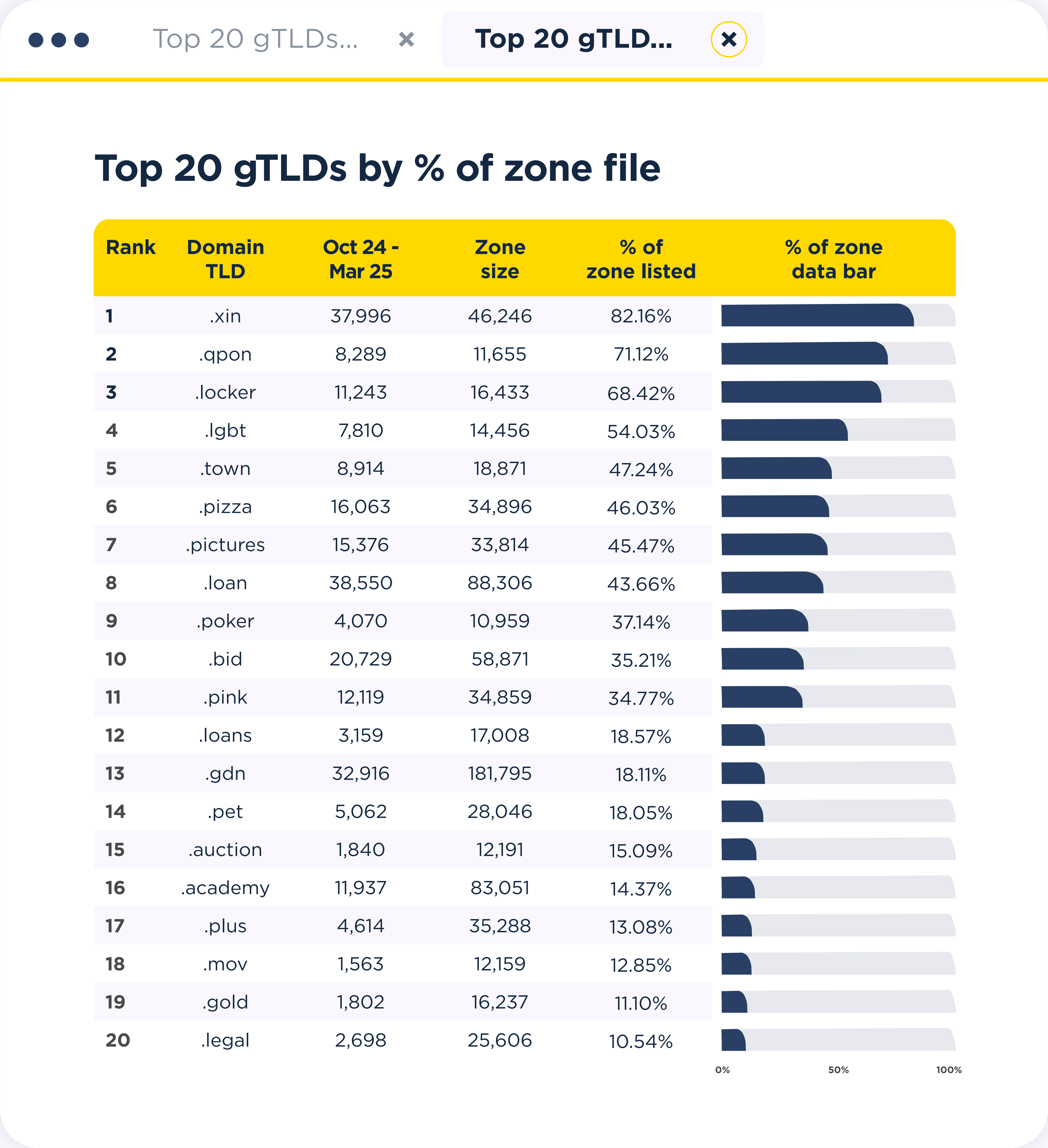
Top 20 ccTLDs

Rank	Domain TLD	Oct 24 - Mar 25	Oct 24 - Mar 25 data bar	Apr 24 - Sept 24	% Change
1	.cc	148,868		89,506	▲ 66%
2	.cn	81,146		61,420	▲ 32%
3	.co	42,087		26,438	▲ 59%
4	.ru	39,984		49,027	▼ -18%
5	.me	13,353		6,435	▲ 108%
6	.de	8,327		5,102	▲ 63%
7	.us	7,454		6,798	▲ 10%
8	.tv	6,007		3,671	▲ 64%
9	.cz	5,768		1,833	▲ 215%
10	.my	5,666		-	New entry
11	.tw	5,310		2,540	▲ 109%
12	.uk	4,569		4,990	▼ -8%
13	.sx	4,331		9,128	▼ -53%
14	.eu	2,478		2,706	▼ -8%
15	.in	2,418		2,492	▼ -3%
16	.ac	2,192		-	New entry
17	.fr	1,998		-	New entry
18	.jp	1,839		-	New entry
19	.ge	1,747		-	New entry
20	.pl	1,565		1,872	▼ -16%


●●● Top 20 gTLDs... ✕ Top 20 gTLD... ✕
0
300
600

Top 20 gTLD

Rank	Domain TLD	Oct 24 - Mar 25	Oct 24 - Mar 25 data bar	Apr 24 - Sept 24	% Change
1	.com	513,292		532,978	▼ -4%
2	.top	316,433		211,406	▲ 50%
3	.vip	115,032		69,289	▲ 66%
4	.xyz	85,176		140,065	▼ -39%
5	.shop	59,830		56,987	▲ 5%
6	.net	57,410		40,887	▲ 40%
7	.loan	38,550		-	New entry
8	.xin	37,996		-	New entry
9	.gdn	32,916		-	New entry
10	.org	22,240		24,471	▼ -9%
11	.info	22,116		20,834	▲ 6%
12	.bid	20,729		-	New entry
13	.pro	20,190		12,916	▲ 56%
14	.sbs	17,744		15,037	▲ 18%
15	.one	17,584		-	New entry
16	.icu	16,566		11,671	▲ 42%
17	.bond	16,391		16,802	▼ -2%
18	.pizza	16,063		-	New entry
19	.online	15,763		15,355	▲ 3%
20	.pictures	15,376		-	New entry


●●● Top 20 gTLDs... ✕ Top 20 gTLD... ✕
0%
50%
100%

Top 20 gTLDs by % of zone file

Rank	Domain TLD	Oct 24 - Mar 25	Zone size	% of zone listed	% of zone data bar
1	.xin	37,996	46,246	82.16%	
2	.qpon	8,289	11,655	71.12%	
3	.locker	11,243	16,433	68.42%	
4	.lgbt	7,810	14,456	54.03%	
5	.town	8,914	18,871	47.24%	
6	.pizza	16,063	34,896	46.03%	
7	.pictures	15,376	33,814	45.47%	
8	.loan	38,550	88,306	43.66%	
9	.poker	4,070	10,959	37.14%	
10	.bid	20,729	58,871	35.21%	
11	.pink	12,119	34,859	34.77%	
12	.loans	3,159	17,008	18.57%	
13	.gdn	32,916	181,795	18.11%	
14	.pet	5,062	28,046	18.05%	
15	.auction	1,840	12,191	15.09%	
16	.academy	11,937	83,051	14.37%	
17	.plus	4,614	35,288	13.08%	
18	.mov	1,563	12,159	12.85%	
19	.gold	1,802	16,237	11.10%	
20	.legal	2,698	25,606	10.54%	

01

02

03

04

05

Trending terms...

Trending phishing terms for malicious or suspicious domains

In this reporting period, the trend of brand-related terms exiting the Top 20 continues. First, “apple” dropped out, and now “amazon” has followed. This is likely due to trademark enforcement leading to domain takedowns. Meanwhile, postage-related phishing terms remain a dominant theme, with terms like: canada (#4), deliver (#5), tracking (#10), usps (#13), and correo (#15).

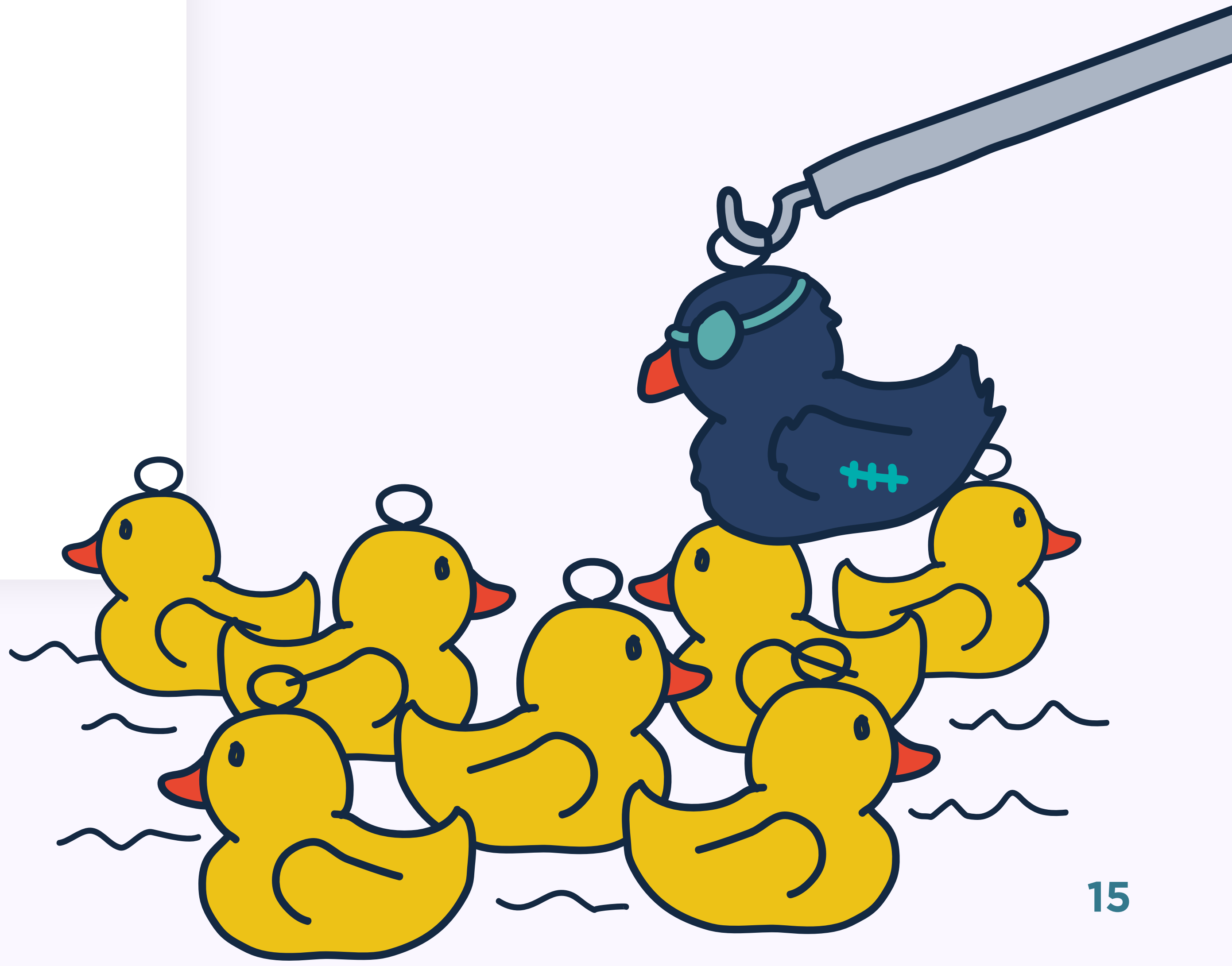
Over the past six months, seven new phishing terms have entered the Top 20, led by “com-track” taking the #1 spot with 17,061 detections. Similar to the abuse with .xin domains, cybercriminals are using hyphenated domains to exploit the credibility of TLDs like “.com”, deceiving users into mistaking the domains for legitimate sites.

Another example is “com-toll” (#18), no doubt linked to the growth in toll road scams, along with “tollbill” (#20).

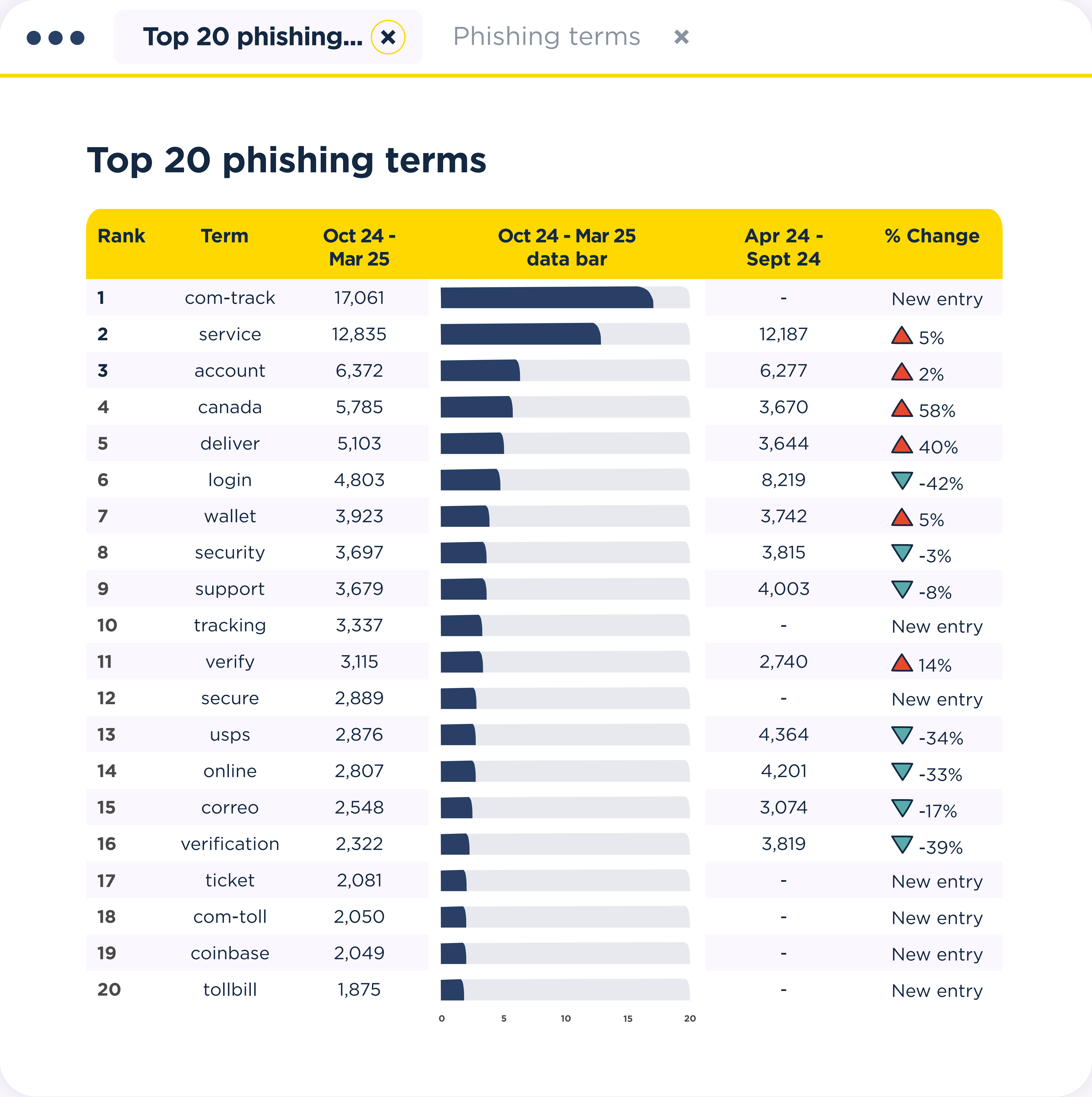
What terms do bad actors use for domain names?

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...
Phishing terms
0
5
10
15
20

Top 20 phishing terms

Rank	Term	Oct 24 - Mar 25	Oct 24 - Mar 25 data bar	Apr 24 - Sept 24	% Change
1	com-track	17,061		-	New entry
2	service	12,835		12,187	▲ 5%
3	account	6,372		6,277	▲ 2%
4	canada	5,785		3,670	▲ 58%
5	deliver	5,103		3,644	▲ 40%
6	login	4,803		8,219	▼ -42%
7	wallet	3,923		3,742	▲ 5%
8	security	3,697		3,815	▼ -3%
9	support	3,679		4,003	▼ -8%
10	tracking	3,337		-	New entry
11	verify	3,115		2,740	▲ 14%
12	secure	2,889		-	New entry
13	usps	2,876		4,364	▼ -34%
14	online	2,807		4,201	▼ -33%
15	correo	2,548		3,074	▼ -17%
16	verification	2,322		3,819	▼ -39%
17	ticket	2,081		-	New entry
18	com-toll	2,050		-	New entry
19	coinbase	2,049		-	New entry
20	tollbill	1,875		-	New entry

Phishing terms

01

02

03

04

05

Types of abuse

Types of abuse

Over the past six months, it appears that when it comes to the type of abuse for compromised domains, botnet command and controllers (C&Cs) were the first choice with a 767% increase, while phishing abuse reduced by 29%. However, these statistics may be somewhat skewed due to Spamhaus' improved Botnet C&C detection techniques.

Additionally, there was a -42% decrease in malicious malware domains while a 16% increase in compromised malware domains. This shift suggests that miscreants are opting to host their malware on compromised websites and file hosting sites like Google Drive and GitHub rather than malicious registrations.

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 abuse ⊗

Types of abuse

Bad reputation

Malicious	Compromised
1,813,805	14,594
▲ 21% ▲	▲ 156% ▲

A domain's reputation score has exceeded policy limits.

Botnet C&C

Malicious	Compromised
1,671	52
▲ 62% ▲	▲ 767% ▲

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

Malware

Malicious	Compromised
2,190	21,001
▼ -42% ▼	▲ 16% ▲

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

Phishing

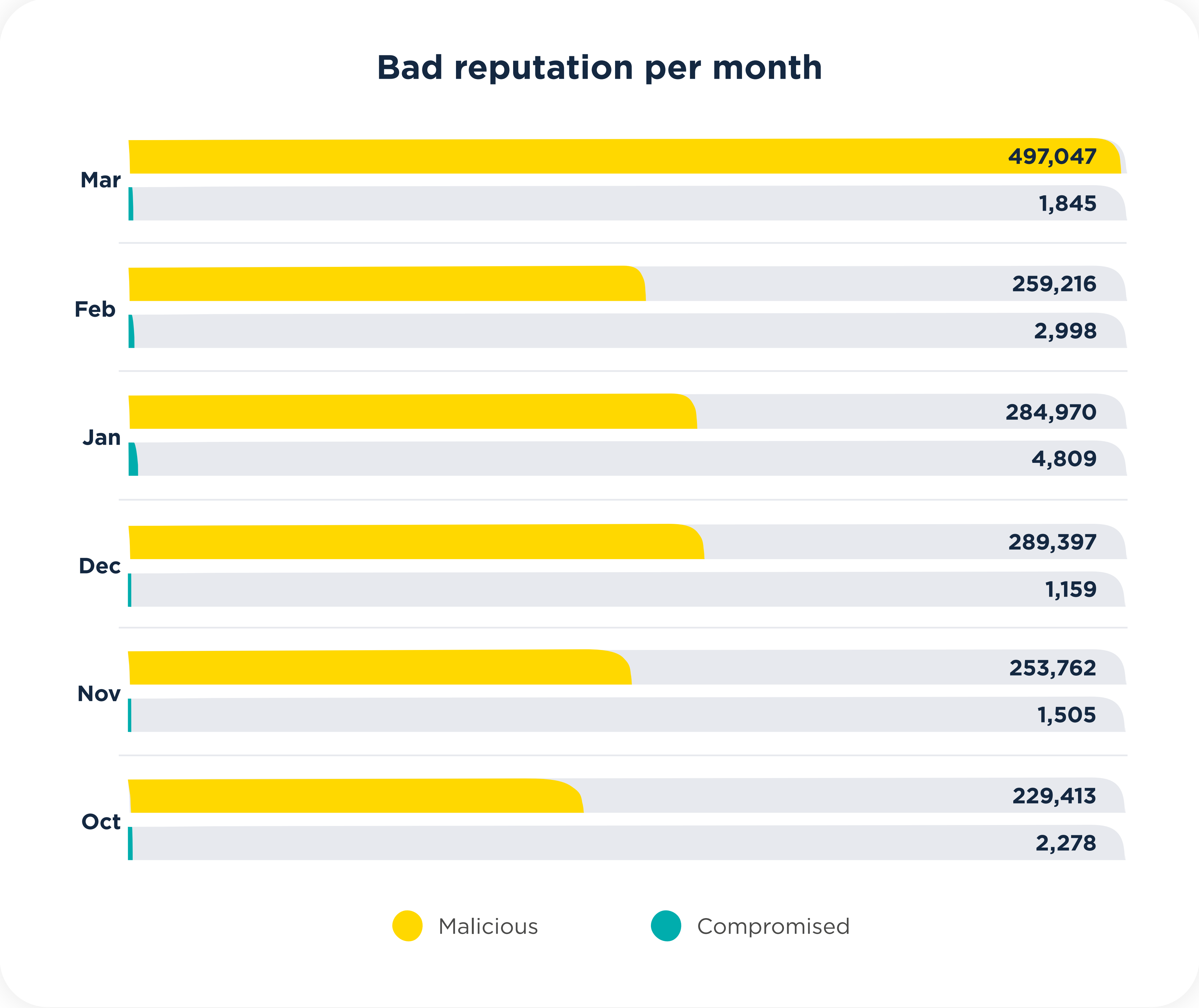
Malicious	Compromised
367,329	99,240
▲ 11% ▲	▼ -29% ▼

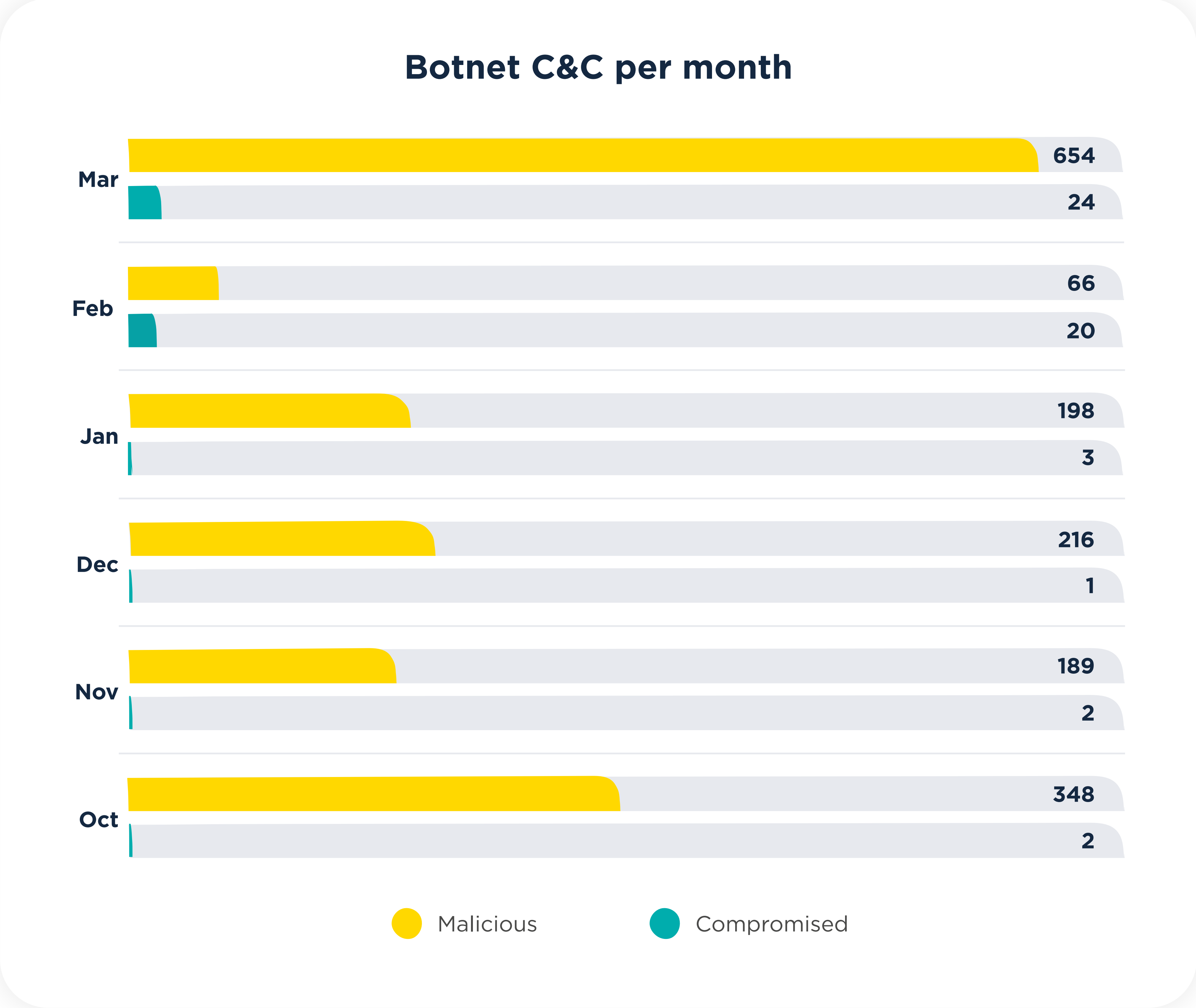
A domain is associated with phishing activities. (A subset of bad reputation.)

01
02
03
04
05

Types of abuse

Types of abuse per month





01

02

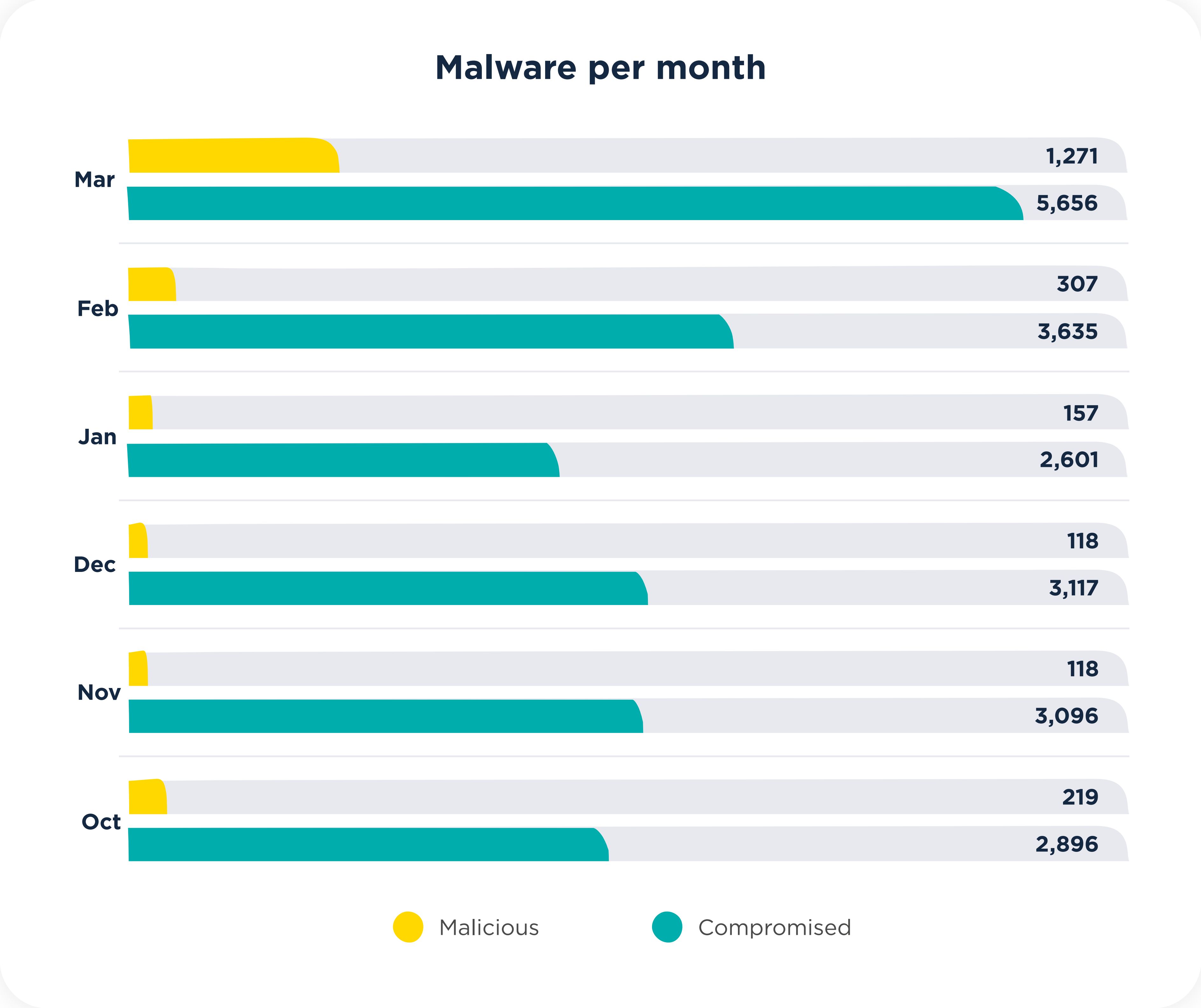
03

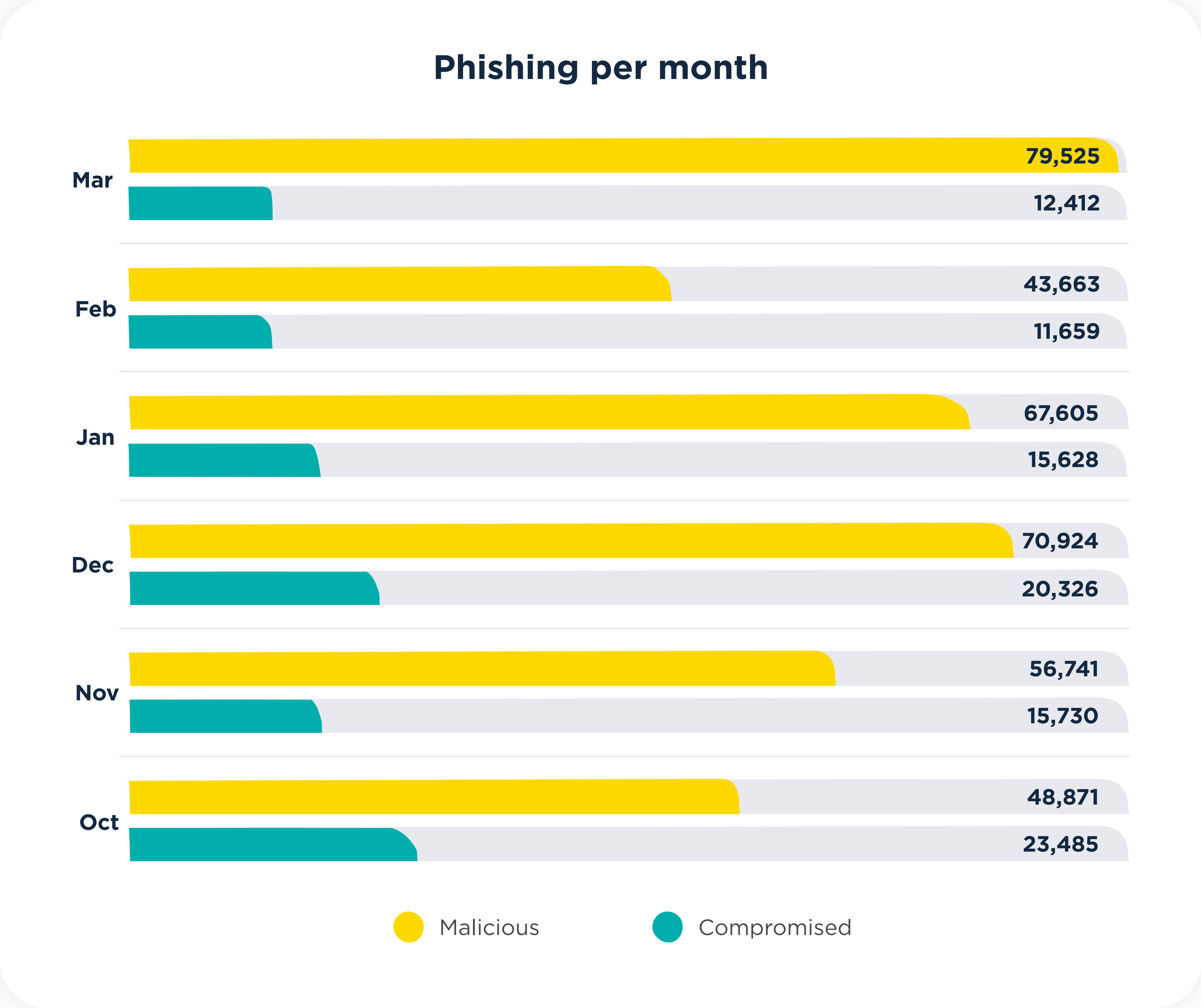
04

05

Types of abuse ✕

Types of abuse per month


Malware per month


Phishing per month

Recommendations

As this report is read by different people in many different roles, providing recommendations that will benefit everyone is challenging. So in this report, we've highlighted specific actions that registrars, registries, policymakers, and even end users can take in response to the growing abuse at .top.

Enforce Know-Your-Customer procedures

To avoid a TLD with hundreds of thousands of problematic domains like .top, registrars need to improve customer vetting at the point of registration. For example, not allowing thousands of registrations with names such as "com-tollbillalu.xin" and registration information like "Registrant Organization: asdad" and "Registrant State/Province: asdasd". Where processing bulk domain registrations happens, always request additional identity checks to prevent fraudulent registrations.

Low-priced domains attract abuse

There's no escaping, the vast majority of newly registered malicious domains exist at the lower-priced tiers. While defensive measures like domain reputation scoring limit their impact, cheap domains further enable this business model by allowing cybercriminals to quickly replace suspended domains. Increase the financial barrier to abuse by considering tiered pricing models where high-risk domains or frequently abused patterns cost more to register.

Hold those responsible accountable

Yes, policy makers, we're talking to you. ICANN needs to prioritize stronger compliance measures for registries with persistently high abuse rates and review the effectiveness of actions taken. Where .top is concerned, what are the next steps for repeat violations? Financial penalties? Contract termination?

Advice to the end-user

To protect yourself from devious scams like the "Toll road scam" don't click on any links in unsolicited texts, or reply to unknown messages. Do verify legitimacy by contacting the company directly using a trusted telephone number or official website. Scammers always emphasize urgency as they want you to act quickly. Take your time and do your research.

Everyone, get social!

As a final recommendation, keep an eye on our blog and social media to stay in touch with everything we observe.

Thank you for reading and see you in October 2025 for the next report!

01

02

03

04

05

Additional info

About Spamhaus

Spamhaus strengthens trust and safety for the Internet. Advocating for change through sharing reliable intelligence and expertise. As the authority on IP and domain reputation data, Spamhaus is trusted across the industry because of its strong ethics, impartiality, and quality of actionable data. This data not only protects but also provides signal and 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 4.5 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.