



Spamhaus Domain Reputation Update

April 2026 – September 2026

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 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

01

02

03

04

05

The Spotlight

Those who follow the DNS abuse landscape closely may have noticed an increase in activity and abuse reports related to Traffic Distribution Systems (TDS). The use of this technology is particularly in phishing campaigns. But what exactly are TDS?

A TDS is a network that advertises and affiliates with legitimate domains as intermediaries, often used to host malicious content and the page or service for a TDS, but the advantage is that the traffic is distributed across many domains. Spamhaus has observed an increase in TDS usage for malware distribution, malvertising, and other harmful activities that rely on domains to distribute, conceal, and accurately target victims.

Adversarial use of TDS also makes life much harder for researchers and successful takedowns because they don't deliver malicious content consistently. Instead, content is only served if a specific set of parameters is met.

Spotlight continued

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 3

01

02

03

04

05

New domains

New domains overview

Over the past six months, 455 million new domains were registered, an average of 75 million per month, compared with the previous six months. Significant growth in over 100,000 new domains was observed in August, standing out as a registered domain, approximately 10% of the total, likely driven by a spike in registrations.

It is important to note that a significant portion of these new domains are used for malicious purposes. However, a considerable amount of new domains are legitimate. Unfortunately, its evidence 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.

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.

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 5

01

02

03

04

05

Malicious/suspicious domains

Malicious/suspicious domains

Domain overview

Over the past six months, 12 million domains were listed as malicious or suspicious, an average of 2 million per month, compared to the previous six months. Significant growth in over 100,000 new domains was observed in August, standing out as a registered domain, approximately 10% of the total, likely driven by a spike in registrations.

It is important to note that a significant portion of these new domains are used for malicious purposes. However, a considerable amount of new domains are legitimate. Unfortunately, its evidence 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.

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 behavior. Domains are 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.

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 12

01

02

03

04

05

Recommendations

With this report's Spotlight on TDS, below are specific actions that registries, registrars, policymakers, and even end users can take in response to the growing abuse of this technique.

Shut down the supply

Registries have a key role to play in the DNS ecosystem. They have the tools to spot when a domain is being used for malicious operations and they can also shut them down. The faster these domains are removed, the less damage they can do. Spamhaus has observed an increase in TDS usage for malware distribution, malvertising, and other harmful activities that rely on domains to distribute, conceal, and accurately target victims.

Enforce Know-Your-Customer

Bulk domain registration has become a popular tool for bad actors. It is so useful to cybercriminals. Using API tools, you can spin up hundreds of domains in seconds, ready to be used in phishing, spam or malicious traffic distribution.

To stop this, registries need to improve KYC checks at the point of registration. If bulk registrations are allowed, additional information should be requested - including verified contact details, corporate registrations numbers, or validated payment methods. These simple steps make it much harder for threat actors to hide.

Definition of DNS abuse

From ICANN's perspective, if a domain is used to facilitate abuse, but not to host it, it's often outside the scope of DNS Abuse. From our perspective, if a domain is used to facilitate large-scale malicious operations and facilitate abuse, if you're aligned with the community, you should help broaden and redefine the scope of DNS Abuse. Get in contact with us via LinkedIn, X, or email.

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 April 2026 for the next report!

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 22

01

02

03

04

05

Additional info

Additional info

About Spamhaus

Spamhaus strengthens trust in the internet. Advocating for the authority on IP and domain reputation. Spamhaus is trusted across the globe for its strong ethics, independent, actionable data. This data is also provided signal and intelligence to specific geographies, governments, and law enforcement. This is not a list of IP addresses or domain names. This is a list of IP addresses and domain names that are used for malicious purposes. This is a list of IP addresses and domain names that are used for malicious purposes. This is a list of IP addresses and domain names that are used for malicious purposes.

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

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.

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 23

01

02

03

04

05



The Spotlight



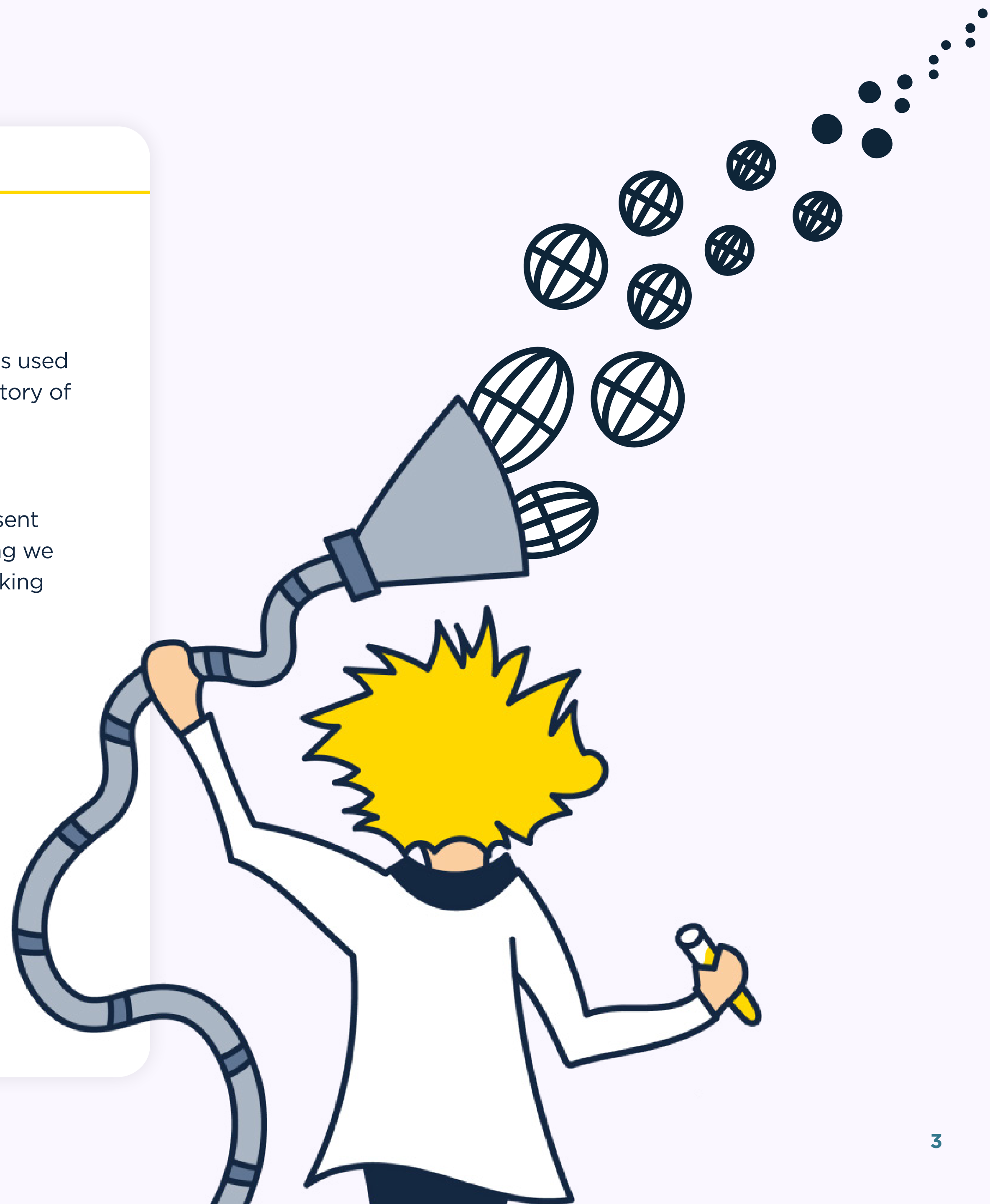
The Spotlight

Since late August 2026, Spamhaus has listed approximately one million domains used for cold email. This is one of the most significant increases we've seen in the history of this report, but [what exactly is cold email](#) and why the sudden surge in listings?

Where did the spike come from?

As part of a data-sharing collaboration, email deliverability specialists, Validity, sent us a set of known cold email domains. When compared against our own tracking we found a strong correlation among the top contributors, confirming we were looking at the same underlying activity... and so the domains were listed.

As a result, in this reporting period, bad reputation listings (the category that includes spam... AKA cold email) more than doubled in a month, from 468K in August to 987K in September.

[Spotlight continued](#)

01

02

03

04

05



Spotlight cont.

**But what exactly is cold email?**

Simply put, it's spam. It's unsolicited bulk email sent to people who have not given verifiable permission for the message to be sent. No consent. No commercial relationship (despite often being personalized) and often some form of bulk, automated distribution. The emails typically include offers, sales leads or financial opportunities, and are sent at volume from domains registered only for that purpose.

To be clear it's not the same as [phishing](#). The emails aren't trying to steal your credentials and our data shows that the domain names used for cold email don't overlap with those used for phishing.

Nevertheless, it's still unwanted email that is flooding inboxes, destroying trust, and using the same disposable domain model we see across so much abuse.

Cheap domains, the same story repeated

This is yet another example of a problem we've raised many times over the years: cheap domains enable abuse at scale. We said in our [Q2 2023 update](#), "without cheap domains, many cybercrime and fraud business models would break."

Cold email operators use this same model: register domains in bulk, burn through them and register more. Registries and registrars should be savvy at spotting these patterns early, but to help we've set out recommendations at the end of this report.

Welcome to the latest Spamhaus Domain Reputation Update.



01

02

03

04

05

New domains

New domains overview

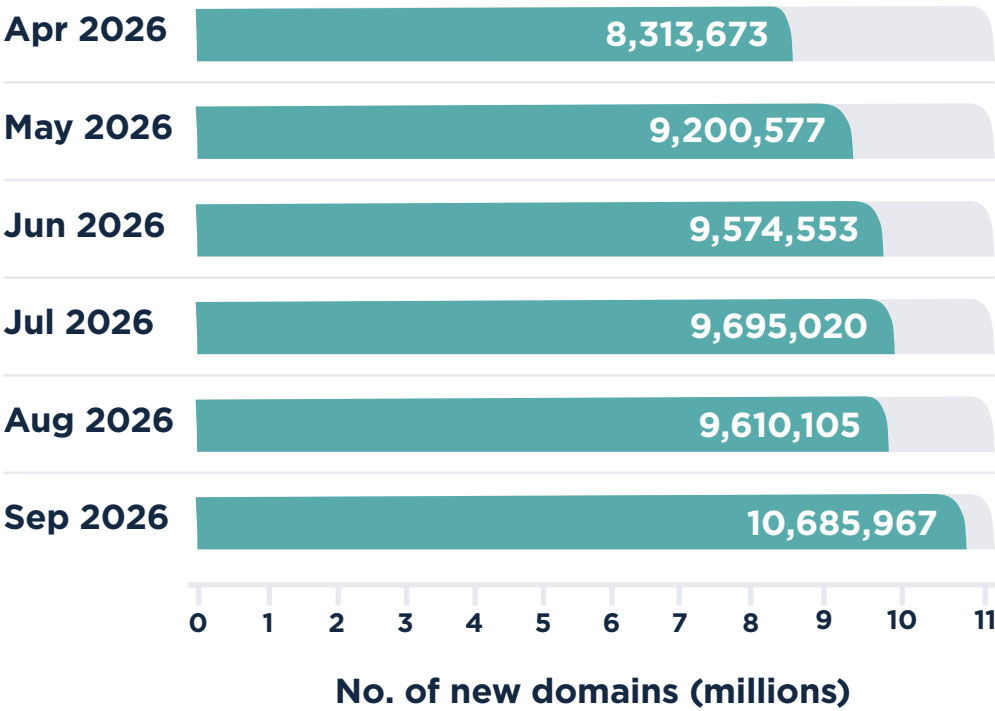
Over the past six months, approximately 57.1 million new domains were registered, a +21.8% increase compared with the previous six months, and the biggest growth in over two years. The monthly average rose to 9.5 million new domains.

Registrations climbed steadily from April, peaking in September with a record 10.7 million new domains. Higher volumes in this period are consistent with seasonal patterns, but the scale of growth particularly stands out.

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 & 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.

Number of new domains per month



Six Month Total
57,079,895
▲ 21.81% ▲

Monthly Average
9,513,316
▲ 1,703,349 ▲

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.

01

02

03

04

05

New domains by top-level domain (TLD)

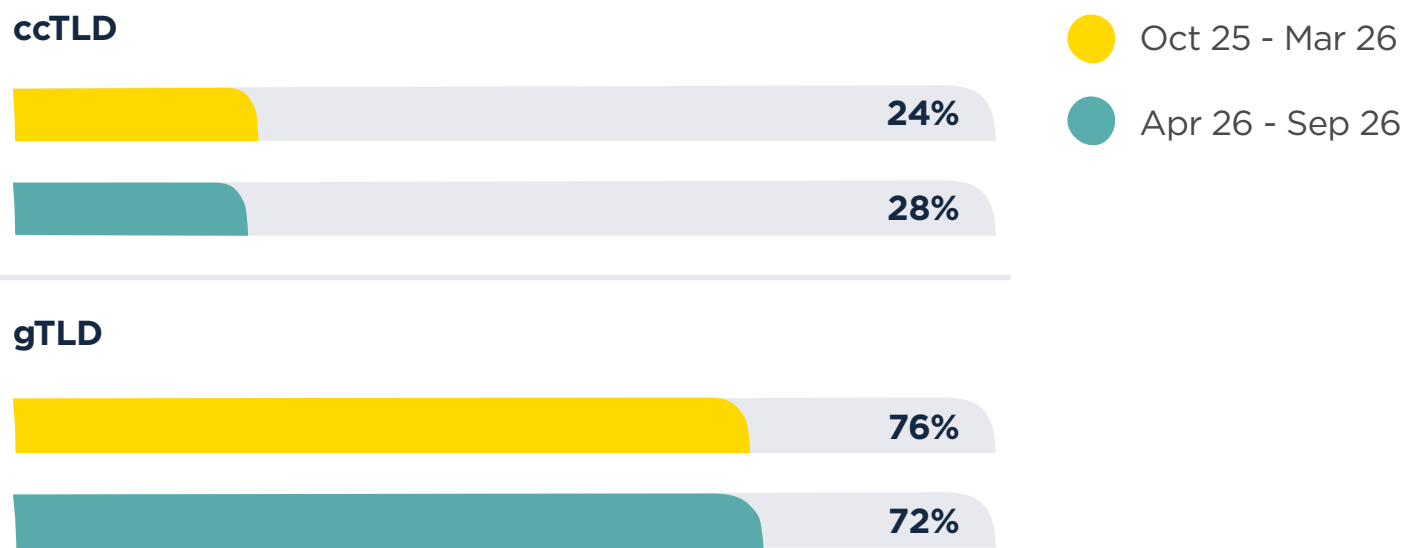
gTLDs remain dominant this reporting period (72%), but there has been a slight shift towards ccTLDs, which now account for 28% of new domain registrations (up from 24%). Growth is spread across many gTLDs and ccTLDs, with very few decreases.

A China story

Between April and September 2026, Chinese domains accounted for much of the ccTLD growth. .cn (#1) increased +77% to 1.96 million new domains, while .com.cn climbed the Top 20 ccTLDs to #2, up +515% to 1.37 million. Many of these new domains can be attributed to Chinese gambling activity that appears to have moved across from the gTLD .bond.

Elsewhere, .co (#8), the ccTLD for Colombia increased +113%, after a -31% decrease in the previous reporting period ([October 2025 - March 2026](#)). Meanwhile, Iran’s ccTLD, .ir (#17), was the only new entry in the Top 20 ccTLDs.

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



New domains...



gTLDs

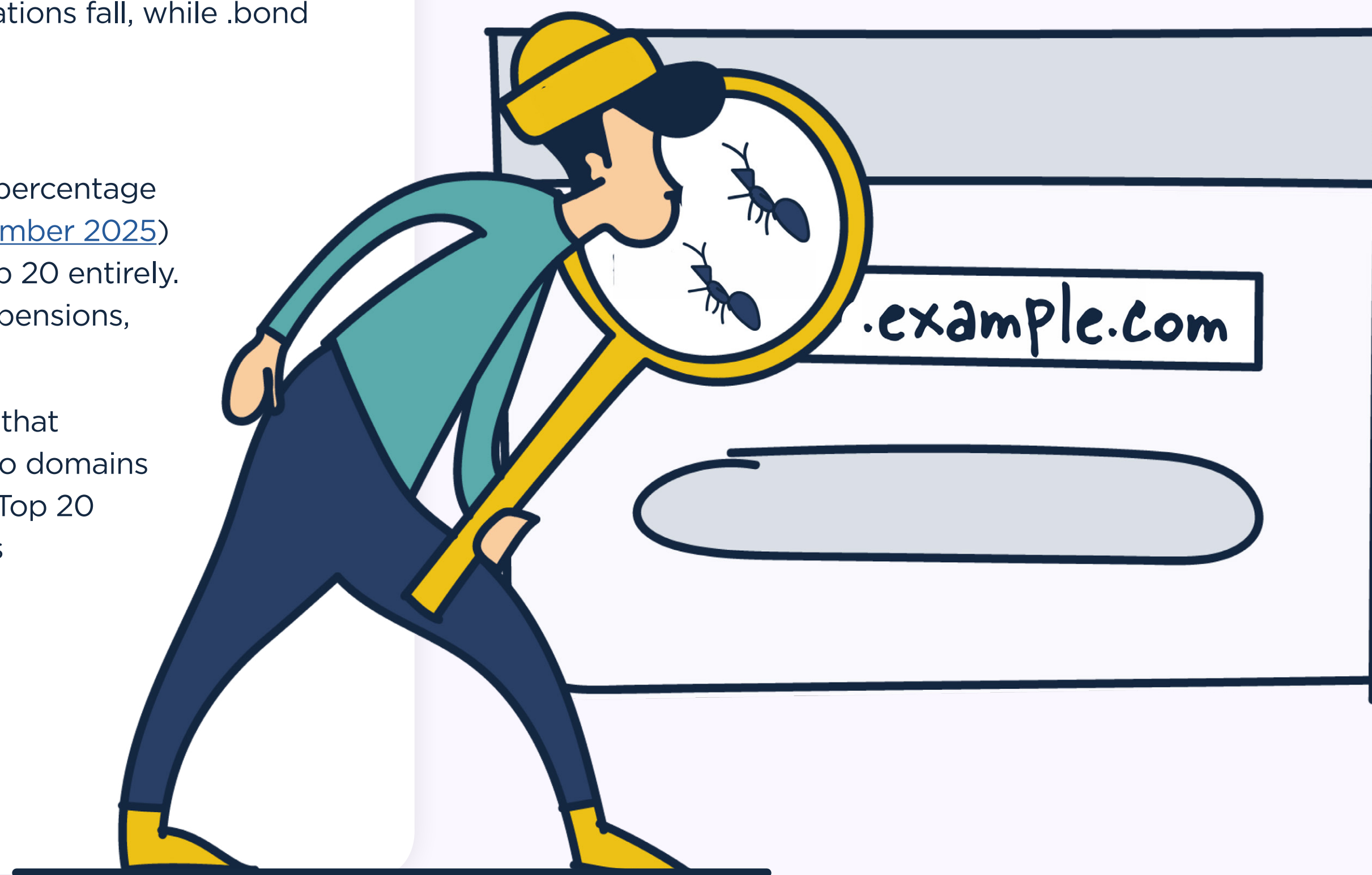
.lol (+138%, #10) and .app (+97%, #13) saw the biggest increases among gTLDs. .app is operated by Charleston Road Registry, which is owned by Google. It's a higher-priced TLD, costing between [\\$4.98](#) and [\\$15.99](#), and typically sees less abuse, although some abuse is still present, including random five-digit .app domains.

In contrast, .sbs (-59%, #17) and .info (-52%, #9) saw new registrations fall, while .bond and .space dropped out of the Top 20.

A turnaround for .bond

In the previous two reports, .bond topped the Top 20 gTLDs by percentage of zone file that are new domains. It fell from 187% ([April - September 2025](#)) to 99% ([October 2025 - March 2026](#)), and it's now exited the Top 20 entirely. Figures above 100% point to unusually high levels of domain suspensions, so this is a big improvement, and one we welcome.

.cam (76%) and .lol (70%) now lead this table, and it's low prices that play a role here - .cam registrations start at [\\$1.69](#), and .lol [\\$1.99](#), so domains are registered cheaply and rarely renewed. As for the remaining Top 20 gTLDs, the percentage of newly observed domains in the zone is at least 50%, indicating a high rate of new registration activity.



01

02

03

04

05



Top 20 TLDs...



Top 20 ccTLDs...



Top 20 TLDs used in new domains

Rank	New domain TLD	TLD type	Apr 26 - Sep 26	Apr 26 - Sep 26 data bar	Oct 25 - Mar 26	% Change
1	.com	gTLD	16,889,452		14,306,314	▲ 18%
2	.xyz	gTLD	3,618,900		2,669,919	▲ 36%
3	.top	gTLD	2,690,126		2,038,137	▲ 32%
4	.cn	ccTLD	1,959,931		1,109,303	▲ 77%
5	.shop	gTLD	1,749,862		1,650,665	▲ 6%
6	.com.cn	ccTLD	1,373,302		-	New entry
7	.online	gTLD	1,231,982		1,116,916	▲ 10%
8	.org	gTLD	1,182,361		1,069,625	▲ 11%
9	.de	ccTLD	965,785		801,018	▲ 21%
10	.net	gTLD	956,513		782,812	▲ 22%
11	.cc	ccTLD	952,709		658,778	▲ 45%
12	.site	gTLD	809,479		639,273	▲ 27%
13	.info	gTLD	778,330		1,624,577	▼ -52%
14	.lol	gTLD	775,787		-	New entry
15	.com.br	ccTLD	766,774		591,556	▲ 30%
16	.store	gTLD	669,696		732,635	▼ -9%
17	.vip	gTLD	667,698		545,417	▲ 22%
18	.ru	ccTLD	637,601		639,722	► 0%
19	.app	gTLD	617,959		-	New entry
20	.co.uk	ccTLD	615,794		535,646	▲ 15%

0 3 6 9 12 15 18



Top 20 TLDs...



Top 20 ccTLDs...



Top 20 ccTLDs used in new domains

Rank	New domain TLD	Apr 26 - Sep 26	Apr 26 - Sep 26 data bar	Oct 25 - Mar 26	% Change
1	.cn	1,959,931		1,109,303	▲ 77%
2	.com.cn	1,373,302		223,187	▲ 515%
3	.de	965,785		801,018	▲ 21%
4	.cc	952,709		658,778	▲ 45%
5	.com.br	766,774		591,556	▲ 30%
6	.ru	637,601		639,722	► 0%
7	.co.uk	615,794		535,646	▲ 15%
8	.co	614,512		288,868	▲ 113%
9	.fr	432,576		386,242	▲ 12%
10	.nl	410,978		300,745	▲ 37%
11	.in	387,906		380,747	▲ 2%
12	.ai	347,402		290,901	▲ 19%
13	.ca	299,939		252,201	▲ 19%
14	.com.au	258,921		204,664	▲ 27%
15	.eu	247,467		254,624	▼ -3%
16	.pl	232,152		192,863	▲ 20%
17	.ir	219,468		-	New entry
18	.io	217,533		164,062	▲ 33%
19	.it	213,638		174,205	▲ 23%
20	.my	198,147		157,551	▲ 26%

0 1 2

01

02

03

04

05

Top 20 gTLDs used in new domains

Rank	New domain TLD	Apr 26 - Sep 26	Apr 26 - Sep 26 data bar	Oct 25 - Mar 26	% Change
1	.com	16,889,452		14,306,314	▲ 18%
2	.xyz	3,618,900		2,669,919	▲ 36%
3	.top	2,690,126		2,038,137	▲ 32%
4	.shop	1,749,862		1,650,665	▲ 6%
5	.online	1,231,982		1,116,916	▲ 10%
6	.org	1,182,361		1,069,625	▲ 11%
7	.net	956,513		782,812	▲ 22%
8	.site	809,479		639,273	▲ 27%
9	.info	778,330		1,624,577	▼ -52%
10	.lol	775,787		326,607	▲ 138%
11	.store	669,696		732,635	▼ -9%
12	.vip	667,698		545,417	▲ 22%
13	.app	617,959		313,290	▲ 97%
14	.click	454,916		332,132	▲ 37%
15	.cfd	410,963		229,379	▲ 79%
16	.pro	387,533		349,498	▲ 11%
17	.sbs	306,767		744,244	▼ -59%
18	.icu	304,770		-	New entry
19	.asia	296,786		-	New entry
20	.cyou	257,763		256,455	▲ 1%

0369121518

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

Rank	New domain TLD	Apr 26 - Sep 26	Zone size	% of zone newly observed	% of zone data bar
1	.cam	101,438	133,811	75.81%	
2	.lol	775,787	1,107,385	70.06%	
3	.lifestyle	10,834	15,486	69.96%	
4	.onl	45,082	65,992	68.31%	
5	.study	21,563	31,932	67.53%	
6	.surf	76,974	115,439	66.68%	
7	.garden	177,893	267,821	66.42%	
8	.cfd	410,963	634,726	64.75%	
9	.christmas	11,740	18,262	64.29%	
10	.motorcycles	8,704	13,588	64.06%	
11	.living	21,333	34,072	62.61%	
12	.mom	51,125	82,562	61.92%	
13	.help	109,191	184,662	59.13%	
14	.wiki	91,035	157,569	57.77%	
15	.lat	131,040	228,335	57.39%	
16	.casa	61,551	109,360	56.28%	
17	.best	45,802	83,751	54.69%	
18	.homes	69,295	126,842	54.63%	
19	.icu	304,770	564,061	54.03%	
20	.courses	16,257	30,206	53.82%	

050%100%

01

02

03

04

05

● ● ● Trending terms... ✕

Trending terms in new domains

Gambling continues to dominate, as “casino” (+71%) remains the #1 trending term with 448,100 new domains.

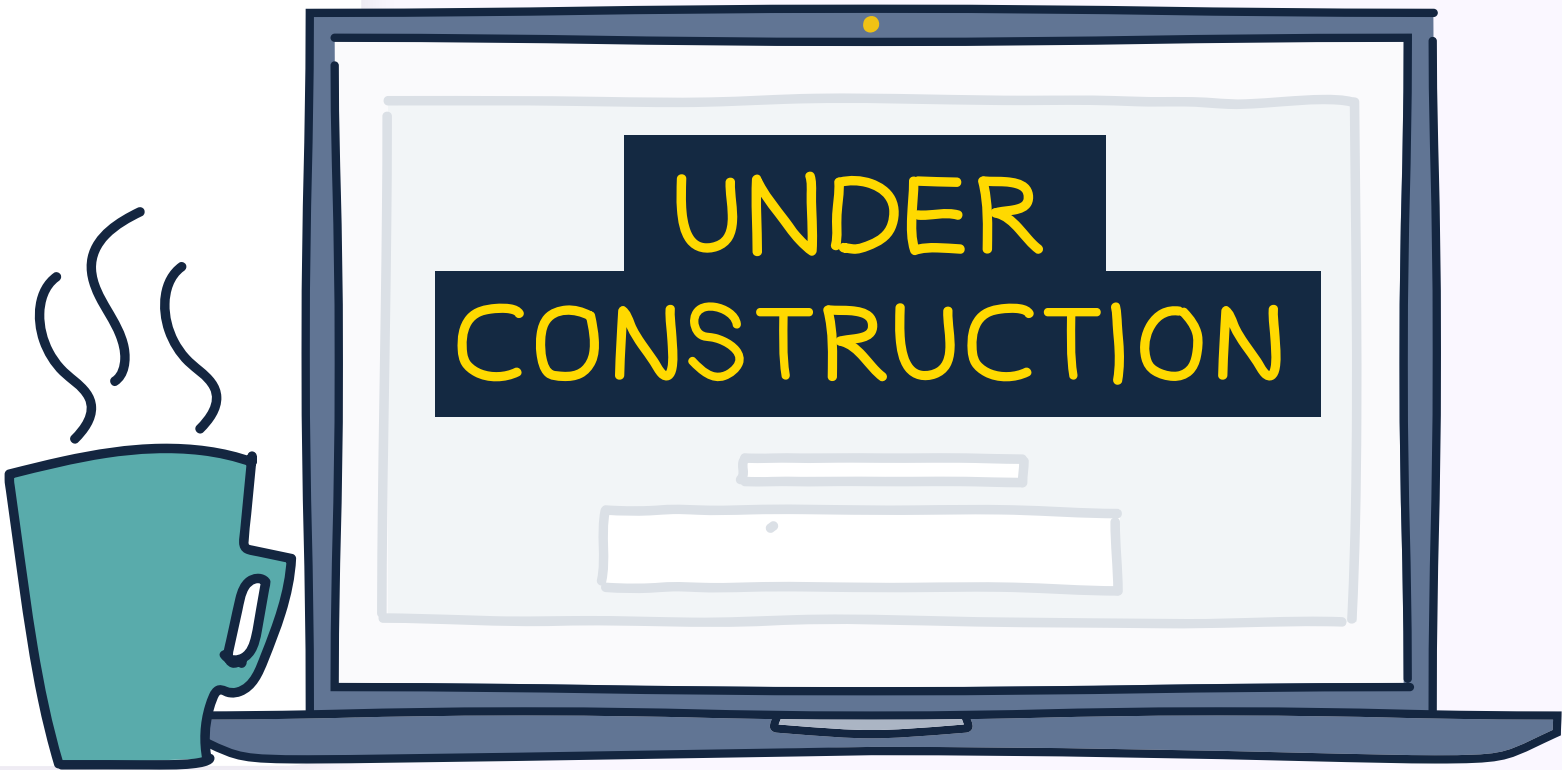
The 2026 FIFA World Cup took place within this reporting period, along with a rise in betting-themed domain registrations: “sports” (+190%) had the biggest increase, climbing to #4. Registrations peaked in June, during the tournament’s opening month, with approximately 67,500 new sports domains.

Chinese gambling terms also surfaced around the World Cup. New entry “kaiyun” - a Chinese gambling brand - joined the Top 20 at #20 (74,897 domains), with most registrations in June. “shijiebei” (“World Cup” in Chinese) also appeared in June, with around 35,100 new domains, although it sits outside the Top 20 trending terms.

“official” (#16) was the only other new entry, while “finance” and “travel” exited the Top 20.

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

Top 20 trending terms in new domains

Rank	Apr 26 - Sep 26 trending terms	Apr 26 - Sep 26	Apr 26 - Sep 26 data bar	Oct 25 - Mar 26	% Change
1	casino	448,100		261,665	▲ 71%
2	studio	292,651		220,257	▲ 33%
3	service	266,220		247,767	▲ 7%
4	sports	248,243		85,463	▲ 190%
5	group	216,328		179,656	▲ 20%
6	solution	201,343		225,337	▼ -11%
7	market	172,442		166,909	▲ 3%
8	online	160,461		146,844	▲ 9%
9	digital	151,588		212,375	▼ -29%
10	consult	147,337		146,838	► 0%
11	global	140,290		125,599	▲ 12%
12	capital	136,142		102,306	▲ 33%
13	health	132,566		122,082	▲ 9%
14	design	117,879		127,629	▼ -8%
15	store	114,391		93,969	▲ 22%
16	official	106,984		-	New entry
17	system	104,660		82,188	▲ 27%
18	partner	99,129		81,341	▲ 22%
19	collect	77,721		54,585	▲ 42%
20	kaiyun	74,897		-	New entry



Top 20 Trending...

Trending terms

Trending terms



01

02

03

04

05

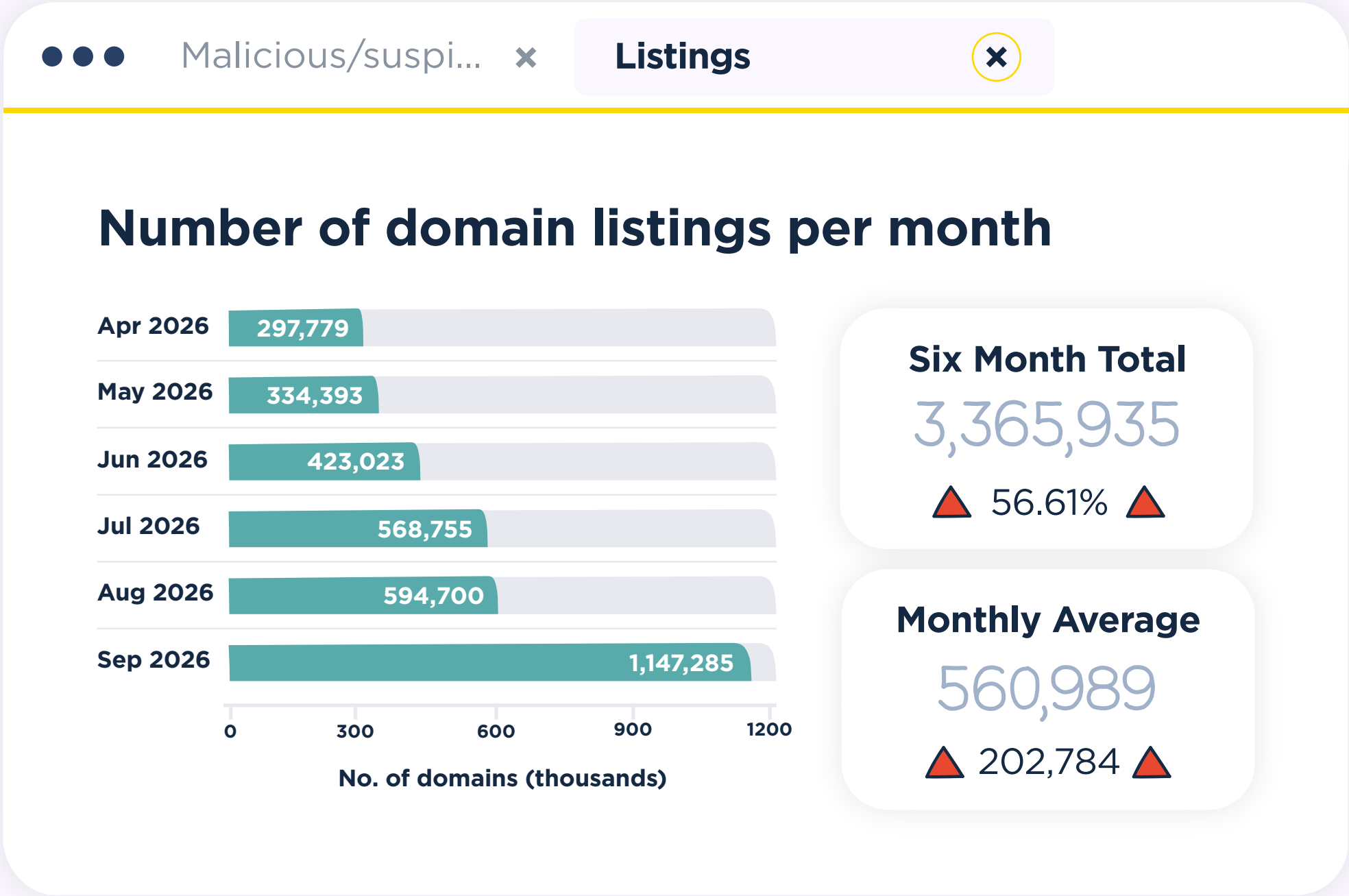
●●● Malicious/suspici... x Listings x

Malicious/suspicious domains

Domain overview

Over the past six months (April – September 2026), 3.37 million malicious or suspicious domains were detected, averaging approximately 561K per month. This is a +56.6% increase on the previous six months. After a significant decrease in the last report (-33.7%), levels have returned to where they were this time last year: 3.24 million between April – September 2025.

Listings rose steadily from 298K in April to 595K in August, before jumping to 1.15 million in September. This is the highest monthly figure in our data to date. Two core factors led to this surge: the growth in new domains registered and cold email listings made in September (see the Spotlight).



i 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

TLDs listed in our domain data

.com (+43%) and .top (+132%) retain the #1 and #2 positions, respectively (in both rankings), while .vip (+186%) and .info (+248%) climb to #4 and #5 in the Top 20 TLDs.

There are three new entries: .help (#11), .biz (#12) and .my (Malaysia, #20). On a positive note, .cfd (#14) listings fell -53%, and the share of its zone file listed dropped from 17.5% to 7%; .bond (#16) listings also decreased, by -31%.

.info: fewer new domains, far more abuse

.info listings increased +248% to 131,578, ranking #5 in the Top 20 TLDs and #4 in the Top 20 gTLDs. This is despite new .info registrations falling -52% over the same period.

The main driver is spam, specifically cold email, followed by phishing and Chinese gambling. Cold email activity was identified through in-house research, industry collaboration, and data sharing (see The Spotlight).

China dominates the ccTLDs

.cn (China, #1) has 465,270 listings, more than four times #2, .cc (Cocos Islands). Roughly 40% of these are .com.cn (second level ccTLD for China) domains, and around 12%

of .com.cn listings contain “whatsapp”, pointing to WhatsApp-themed phishing.

There were also increases for .me (Montenegro, +382%), .id (Indonesia, +233%) and .co (Colombia, +221%), and five new entries: .tw (Taiwan, #7), .ee (Estonia, #11), .at (Austria, #15), .st (São Tomé and Príncipe, #16) and .cm (Cameroon, #20).

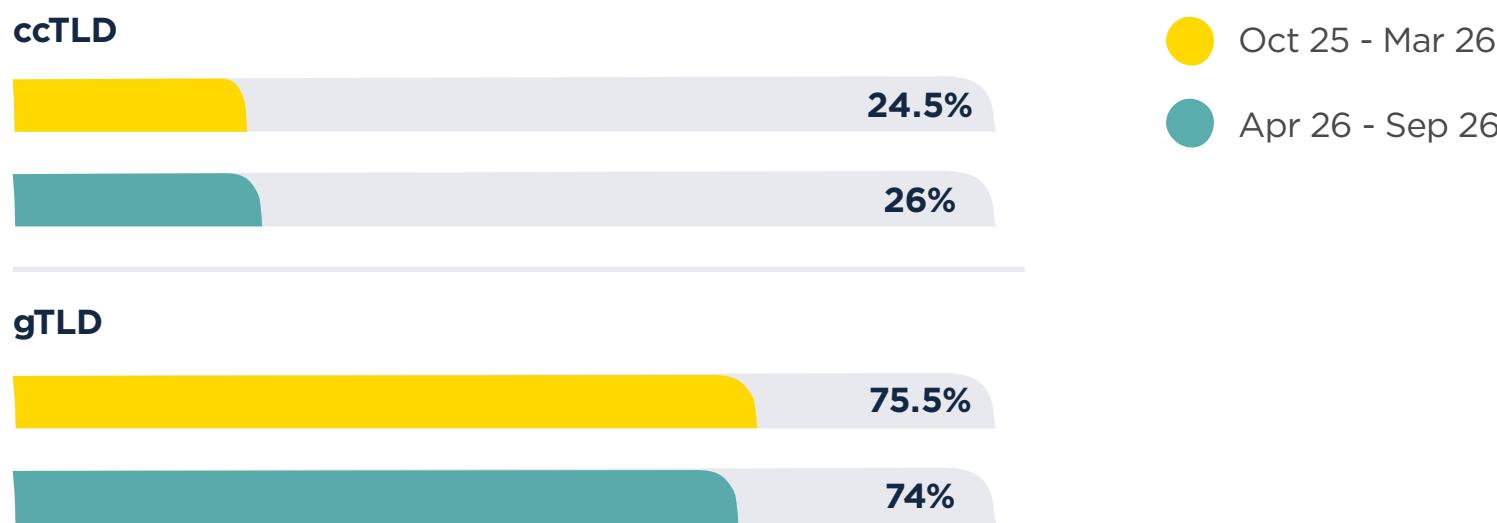
Percentage of zone file listed

As highlighted previously, a threshold of 5% of the zone file listed is a red flag; anything above 10% is indicative of a problematic TLD. Between April and September 2026, three gTLDs exceed this threshold: .help (#1) with 26.5% of its zone file listed, largely due to cold email, .qpon (#2) at 15.1%, and .study (#3) at 12.4%.

Registries with a greater number of active domains have greater exposure to abuse. For example, between April 2026 and September 2026, .vip had almost 2 million domains in its zone, of which 7% were listed.

Meanwhile, .help had just under 185K domains in its zone, with 27% 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 month comparison



01

02

03

04

05



Top 20 TLDs...



Top 20 ccTLDs...



Top 20 TLDs

Rank	Domain TLD	Type of TLD	Apr 26 - Sep 26	Apr 26 - Sep 26 data bar	Oct 25 - Mar 26	% Change
1	.com	gTLD	724,149		506,482	▲ 43%
2	.top	gTLD	627,907		270,121	▲ 132%
3	.cn	ccTLD	465,270		252,852	▲ 84%
4	.vip	gTLD	146,856		51,280	▲ 186%
5	.info	gTLD	131,578		37,786	▲ 248%
6	.cc	ccTLD	113,432		94,415	▲ 20%
7	.shop	gTLD	81,476		52,350	▲ 56%
8	.xyz	gTLD	65,463		47,547	▲ 38%
9	.icu	gTLD	50,942		46,350	▲ 10%
10	.net	gTLD	49,439		43,593	▲ 13%
11	.help	gTLD	48,897		-	New entry
12	.biz	gTLD	47,522		-	New entry
13	.ru	ccTLD	45,472		54,612	▼ -17%
14	.cfd	gTLD	44,502		93,940	▼ -53%
15	.org	gTLD	42,534		31,057	▲ 37%
16	.bond	gTLD	41,186		59,271	▼ -31%
17	.sbs	gTLD	38,626		42,115	▼ -8%
18	.cyou	gTLD	30,486		18,291	▲ 67%
19	.click	gTLD	29,668		24,004	▲ 24%
20	.my	ccTLD	26,949		-	New entry



Top 20 TLDs...



Top 20 ccTLDs...



Top 20 ccTLDs

Rank	Domain TLD	Apr 26 - Sep 26	Apr 26 - Sep 26 data bar	Oct 25 - Mar 26	% Change
1	.cn	465,270		252,852	▲ 84%
2	.cc	113,432		94,415	▲ 20%
3	.ru	45,472		54,612	▼ -17%
4	.my	26,949		14,669	▲ 84%
5	.me	20,630		4,278	▲ 382%
6	.co	18,179		5,662	▲ 221%
7	.tw	15,324		-	New entry
8	.uk	13,298		6,687	▲ 99%
9	.id	12,176		3,652	▲ 233%
10	.de	11,044		9,678	▲ 14%
11	.ee	10,582		-	New entry
12	.us	7,891		2,981	▲ 165%
13	.io	5,908		2,194	▲ 169%
14	.cz	5,593		6,394	▼ -13%
15	.at	5,153		-	New entry
16	.st	4,514		-	New entry
17	.eu	3,740		6,080	▼ -38%
18	.ng	3,720		3,159	▲ 18%
19	.tr	3,699		2,157	▲ 71%
20	.cm	3,100		-	New entry

01

02

03

04

05



Top 20 gTLDs...



Top 20 gTLD...



Top 20 gTLD

Rank	Domain TLD	Apr 26 - Sep 26	Apr 26 - Sep 26 data bar	Oct 25 - Mar 26	% Change
1	.com	724,149		506,482	▲ 43%
2	.top	627,907		270,121	▲ 132%
3	.vip	146,856		51,280	▲ 186%
4	.info	131,578		37,786	▲ 248%
5	.shop	81,476		52,350	▲ 56%
6	.xyz	65,463		47,547	▲ 38%
7	.icu	50,942		46,350	▲ 10%
8	.net	49,439		43,593	▲ 13%
9	.help	48,897		-	New entry
10	.biz	47,522		15,078	▲ 215%
11	.cfd	44,502		93,940	▼ -53%
12	.org	42,534		31,057	▲ 37%
13	.bond	41,186		59,271	▼ -31%
14	.sbs	38,626		42,115	▼ -8%
15	.cyou	30,486		18,291	▲ 67%
16	.click	29,668		24,004	▲ 24%
17	.online	22,659		23,528	▼ -4%
18	.live	18,988		13,245	▲ 43%
19	.app	17,850		-	New entry
20	.site	17,073		12,530	▲ 36%

0

500,000

1,000,000



Top 20 gTLDs...



Top 20 gTLD...



Top 20 gTLDs by % of zone file

Rank	Domain TLD	Apr 26 - Sep 26	Zone size	% of zone listed	% of zone data bar
1	.help	48,897	184,662	26.48%	
2	.qpon	10,185	67,418	15.11%	
3	.study	3,949	31,932	12.37%	
4	.icu	50,942	564,061	9.03%	
5	.bid	4,452	53,877	8.26%	
6	.vip	146,856	1,995,083	7.36%	
7	.cfd	44,502	634,726	7.01%	
8	.you	747	11,218	6.66%	
9	.loan	1,353	21,574	6.27%	
10	.xin	3,636	61,170	5.94%	
11	.cyou	30,486	556,097	5.48%	
12	.top	627,907	12,587,990	4.99%	
13	.cam	5,421	133,811	4.05%	
14	.ink	6,013	151,367	3.97%	
15	.mom	3,270	82,562	3.96%	
16	.biz	47,522	1,350,895	3.52%	
17	.bond	41,186	1,182,419	3.48%	
18	.sbs	38,626	1,127,997	3.42%	
19	.click	29,668	909,284	3.26%	
20	.casa	3,551	109,360	3.25%	

0%

50%

100%

01

02

03

04

05



Trending terms...

Trending phishing terms for malicious or suspicious domains

“whatsapp” remains the #1 phishing term, with 16,723 domains, despite a -32% decrease on the last reporting period. A misspelled variant, “whatapp”, is a new entry at #12, suggesting threat actors are leveraging typo domains. Much of this WhatsApp-themed phishing is linked to the .cn and .com.cn ccTLD activity highlighted earlier in the report.

The Turkish-language theme from the last report continues to grow, with “guncel” (current, +102%), “giris” (entrance/login, +106%) and “adresi” (address, +119%) all rising. Turkish casino “jojobet” (+62%) also climbed to #14, while “casibom” and “holiganbet” dropped out of the Top 20.

The World Cup left its mark here too, with “sports” entering at #8, “kaiyun” - the aforementioned Chinese gambling site - entered at #16, and “casino” rose +73% to #3.

Meanwhile, call-to-action terms surged: “online” (+238%, #2), “portal” (+145%, #4) and “login” (+135%, #5) recorded the biggest increases. Six new terms entered the Top 20, while “signin”, “tracking” and “reward” were among those that dropped out.

**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

Rank	Term	Apr 26 - Sep 26	Apr 26 - Sep 26 data bar	Oct 25 - Mar 26	% Change
1	whatsapp	16,723		24,640	▼ -32%
2	online	13,446		3,977	▲ 238%
3	casino	11,179		6,473	▲ 73%
4	portal	9,780		3,985	▲ 145%
5	login	9,444		4,024	▲ 135%
6	guncel	7,699		3,807	▲ 102%
7	giris	7,460		3,620	▲ 106%
8	sports	7,092		-	New entry
9	verify	5,681		2,832	▲ 101%
10	adresi	5,572		2,545	▲ 119%
11	wallet	5,059		3,023	▲ 67%
12	whatapp	4,838		-	New entry
13	service	4,585		3,286	▲ 40%
14	jojobet	4,503		2,787	▲ 62%
15	support	3,882		3,049	▲ 27%
16	kaiyun	3,854		-	New entry
17	secure	3,730		4,130	▼ -10%
18	adress	3,677		-	New entry
19	finance	3,508		-	New entry
20	merit	3,315		-	New entry

Phishing terms



01

02

03

04

05

● ● ● Types of abuse x

Types of abuse

Malicious bad reputation domains increased +62% to 2.61 million over the last six months, more than three times the number of malicious phishing domains (728,660, +42%). Bad reputation is a broad category that covers spam, including cold email, domains linked by association to known bad infrastructure, and domains where abuse is strongly suspected but not yet confirmed.

Among compromised domains, botnet C&Cs (+145%) and bad reputation (+113%) saw the largest increases, while phishing increased +16%. Compromised malware domains fell by -51%. For malicious domains, botnet C&Cs increased +50% and malware +23%.

The overall increase in listings across almost all abuse types can, in part, be attributed to the preventative listing of large domain portfolios, where only a subset of the domains had already been used. Taking this action decreases the value of investment and raises the cost for bad actors.

i Differences between compromised and malicious domains x

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.

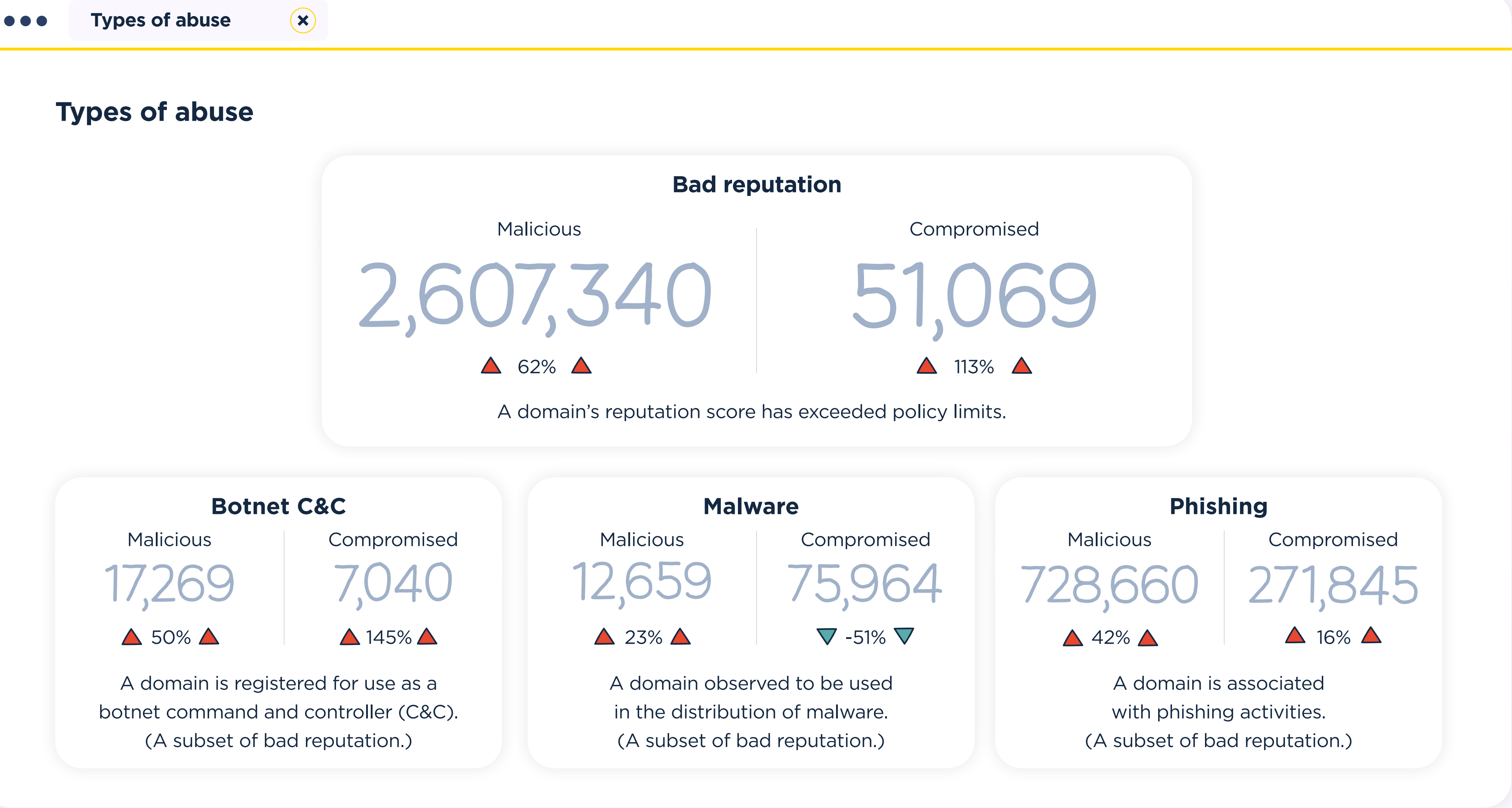
01

02

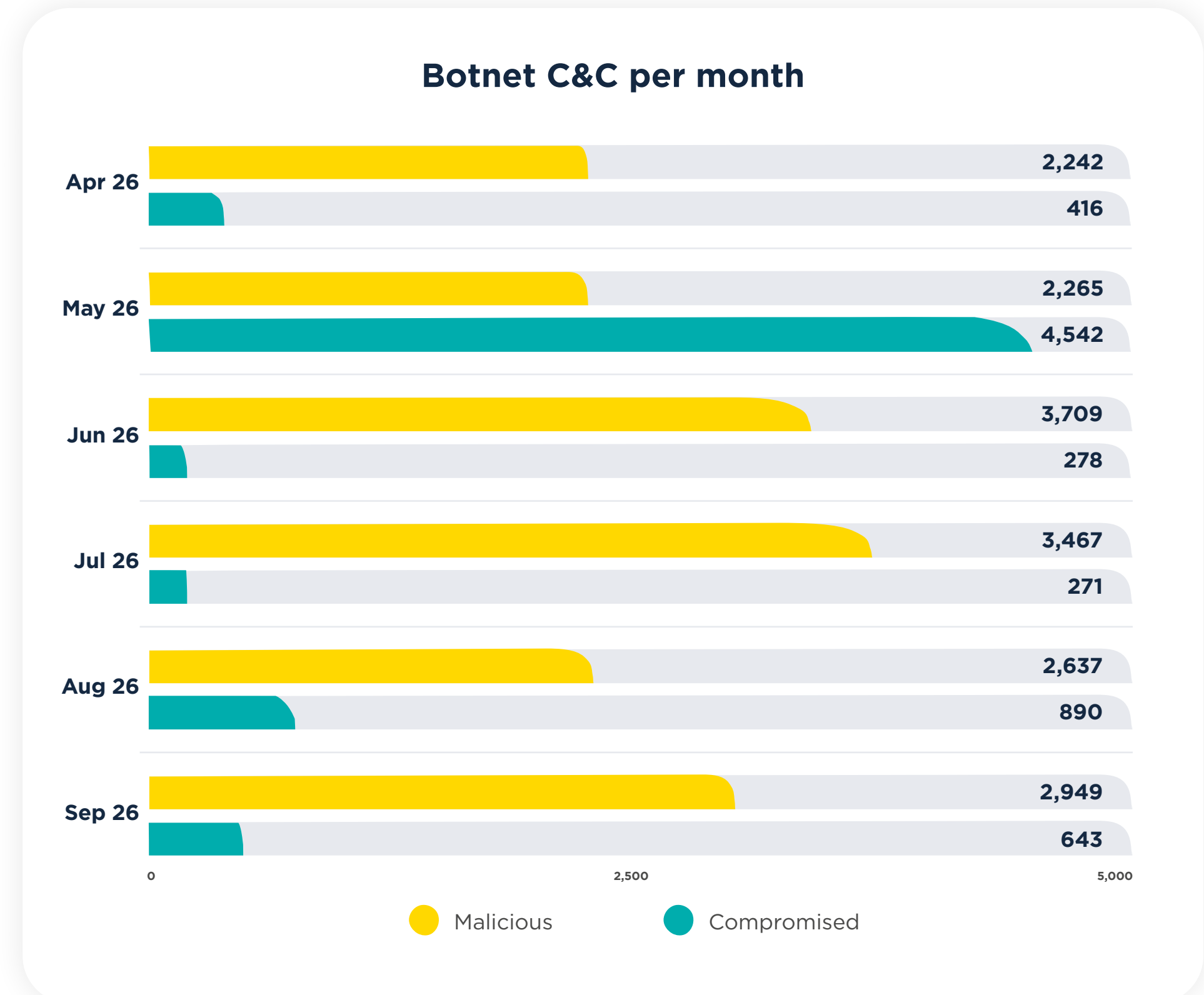
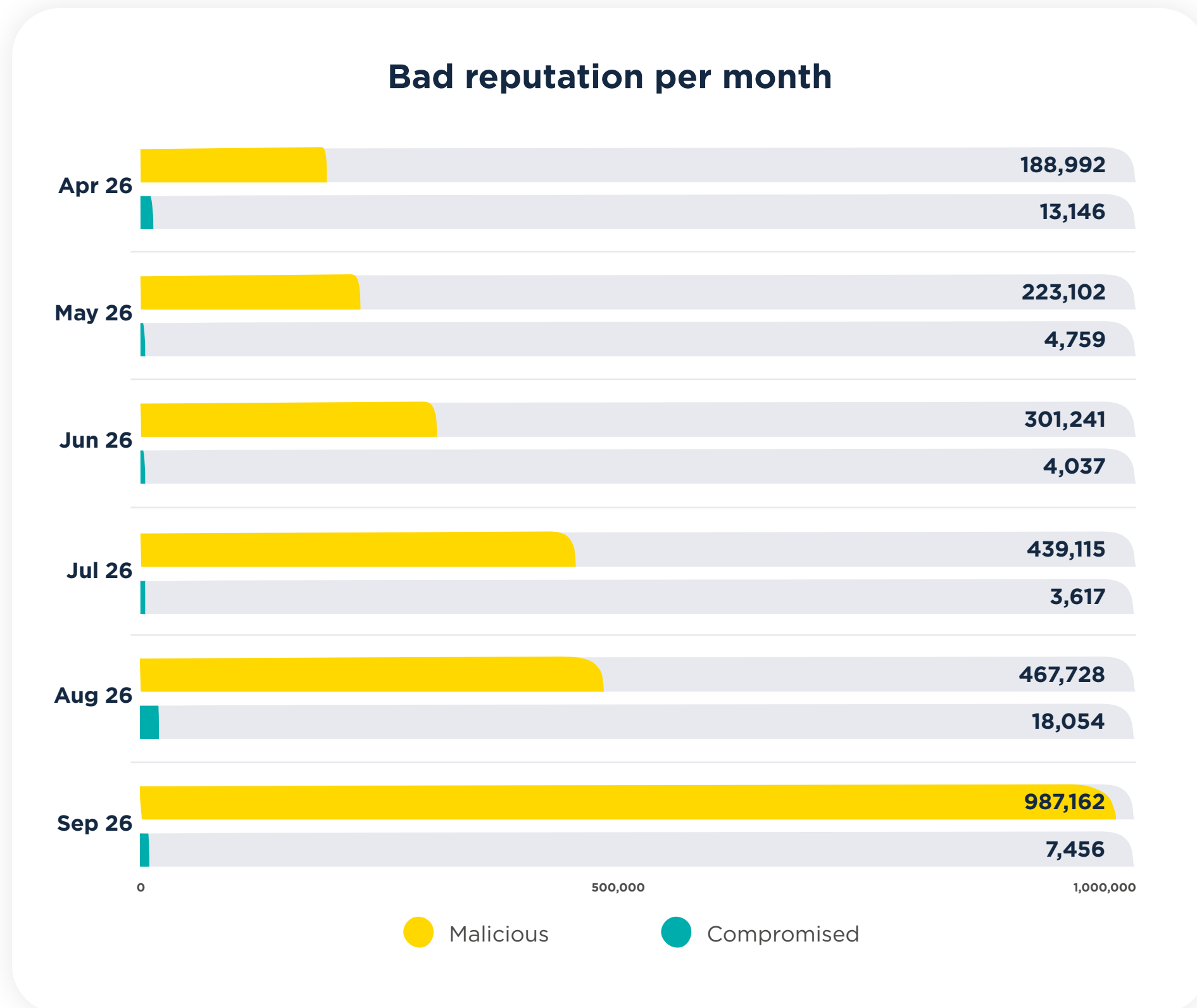
03

04

05



Types of abuse per month



01

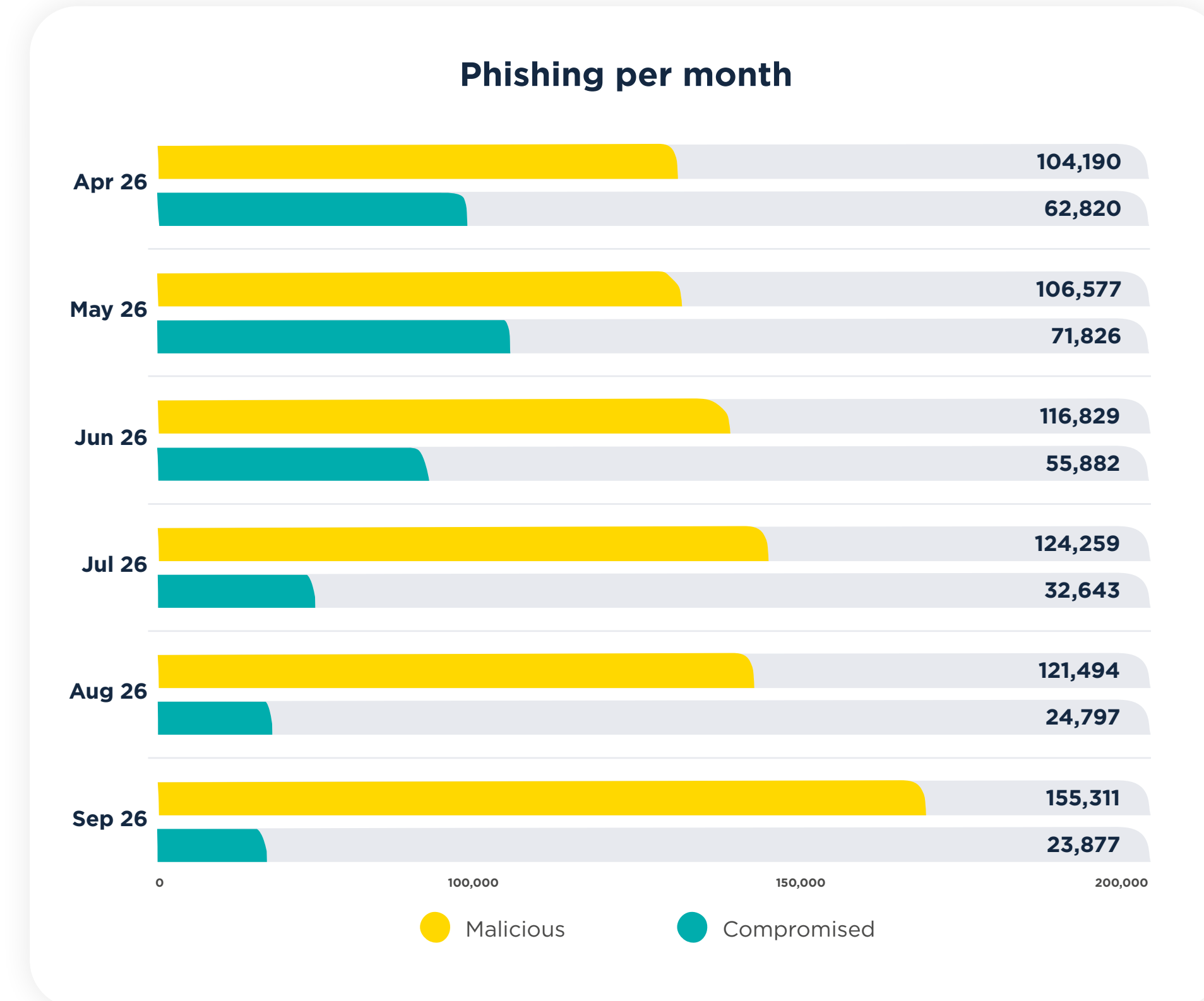
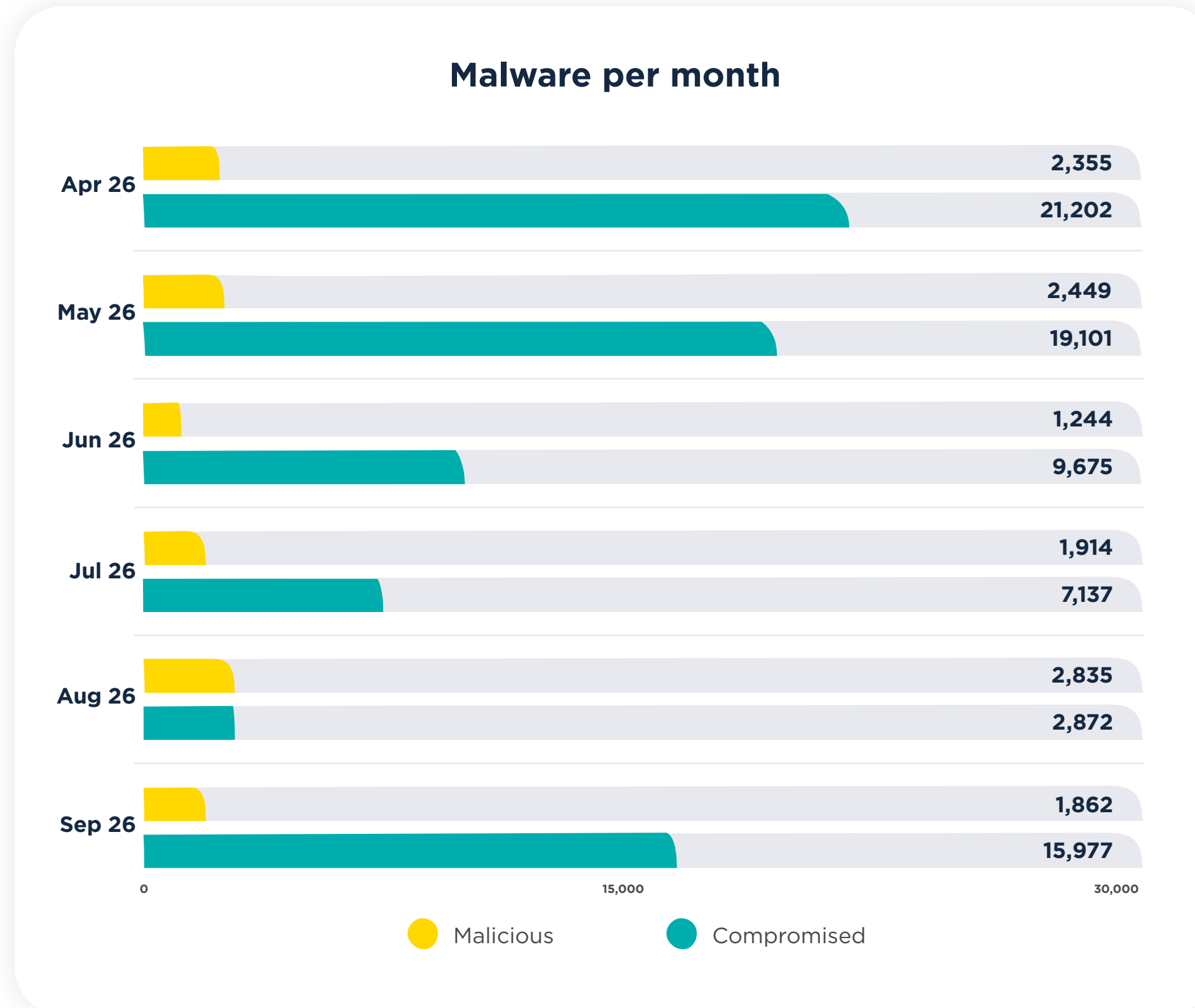
02

03

04

05

Types of abuse per month



01

02

03

04

05

01

02

03

04

05



Recommend...



Recommendations

The rapid growth of cold email shows how quickly spammers can register cheap domains in bulk to send unwanted email (see the Spotlight). But it's one of a number of themes in this report, from brand impersonation to abuse concentrated in specific TLDs.

Here are a few recommendations for registrars and registries to spot this activity early and stop abuse.

Look for patterns, not single domains

Monitor for suspicious naming patterns at the point of domain registration, such as random combinations of words or digits registered in bulk. When you action one domain, check for associated domains registered by the same customer or in the same way.

Price and policy shape abuse

Low cost domains that are registered and never renewed carry a higher risk, as demonstrated by the high churn of almost all TLDs in the Top 20 gTLDs by zone file for new domains. If you run pricing promotions, monitor them closely, and be mindful of betting and scam domains around major events like the FIFA World Cup showed.

Track the share of your zone that's listed

Some TLDs have a disproportionate share of their zone listed with Spamhaus. This reporting period, .help increased from 4.1% to 26.5%, well above the 10% threshold indicating a problematic TLD. Check your own zone against that threshold rather than wait for a report like this to point it out. Registries can also share zone files with Spamhaus to help improve visibility of abuse.

Look for brand names at registration

Flagging well-known brand names and common misspellings when someone registers a domain is an easy way to filter out abusive registrations, for example "whatsapp", the #1 phishing term in this report, and the misspelling "whatapp" a new entry at #12.

Follow us on socials!

As a final recommendation, keep an eye on our blog and social media ([LinkedIn](#), [Mastodon](#), [X](#)) to stay in touch with everything we observe.

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.