



# Spamhaus Domain Reputation Update

**Apr 2024 - Sept 2024**

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  
Apr 2024 - Sept 2024.**

**Enter**





# Contents

## The Overview


01 The Overview

02 This is a report of two tales – changes observed with individual TLDs, and updates across the broader TLD ecosystem. On the former, this period saw us become increasingly popular as a startup. Could this be the sign that we detect more so domains for price per domain has dropped with.

03 Other 'new' TLDs observe similar patterns almost all buying, switching domain blocked, or taken down. Consider abuse that would otherwise not be scalable. We will continue to emphasize that this systemic issue is a breeding ground for large-scale (DNS) abuse.

04 Overview continued

05



Go to page 3

## New domains

01 New domains

02 New domains overview

03 Number of new domains per month

04 6 month Total: 33,904,327

05 Monthly Average: 5,650,721

What is a new domain?

Go to page 5

## Malicious/suspicious domains

01 Domains detected

02 Domain Overview

03 Number of Domain detections per month

04 6 month total: 1,009,512

05 Monthly Average: 168,252

What triggers a domain to be detected by Spamhaus?

Go to page 11

## Recommendations

01 Recommendations

02 Taking into consideration the aforementioned technical changes and their influence on this report, the extensive parts of the Internet are in dealing with abuse, and more and more important. Again, registrations, still, we more involving many operational.

03 Compared to other industries, which makes for shallow profit become a customer and business. Lack of funding to that operates well-known because of the simpler cases aren't dealt with, the more complex cases need not worry.

04 So, is there light at the end of the tunnel? We believe so. There has never been as much industry interest in topics involving malicious domain names. As long as every stakeholder keeps pushing, the critical mass for change seems almost within reach. We'll certainly continue to do our part in strengthening trust and safety on the Internet.

05 Thank you for reading and see you for the next report in October 2024.

Go to page 21

## Additional info

01 Additional info

02 About Spamhaus

03 Report Methodology

04 Spamhaus is the trusted authority in domain reputation, unique in its industry because of its quality and quality of actionable intelligence. The data in this report only protects but also provides malicious and bad reputation.

05 With over two decades of its researchers and threat intelligence 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.

Go to page 22

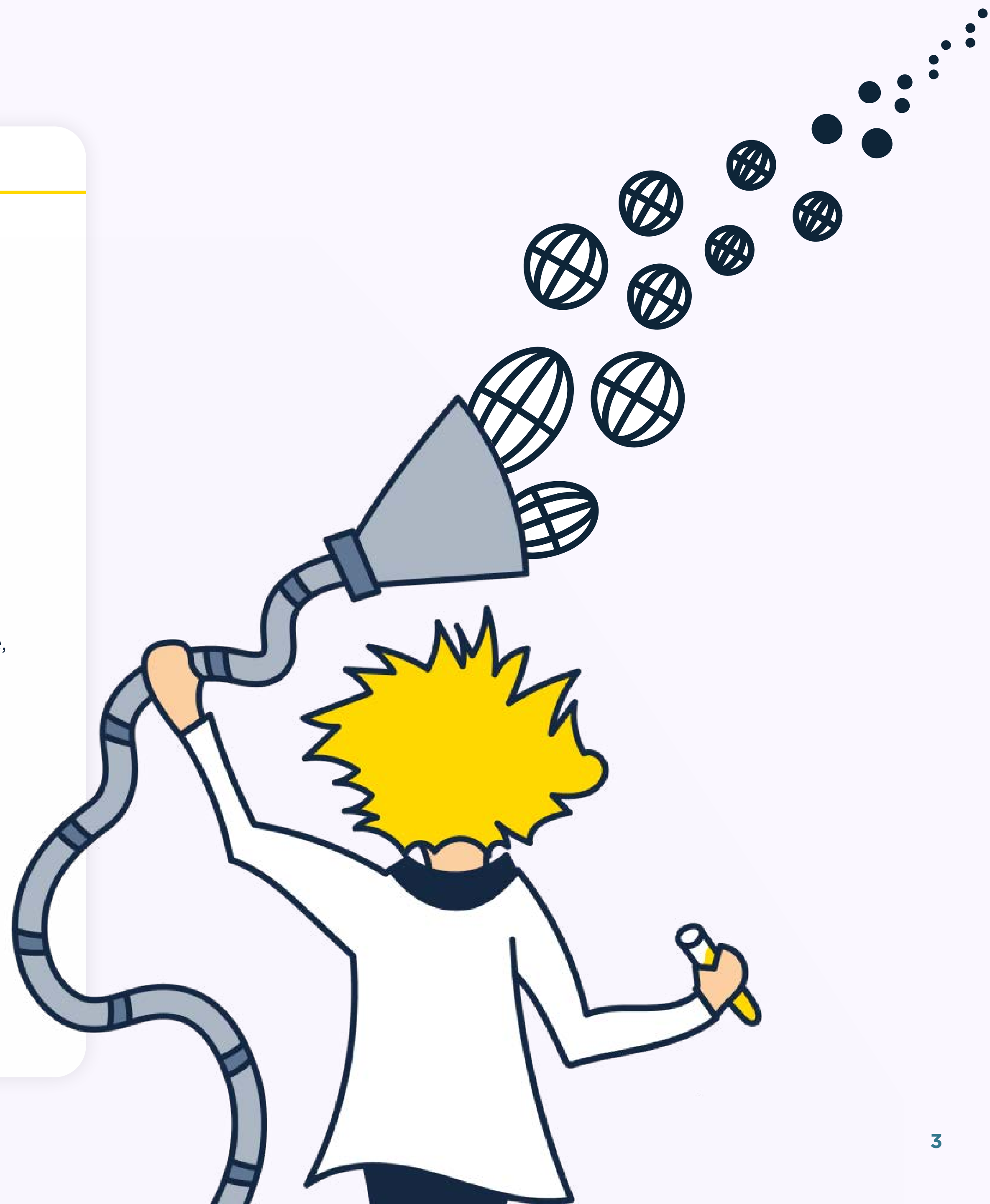
01

## The Overview

Readers of this report who follow ICANN proceedings may have noticed that, in mid July, [ICANN sent out a letter to the .TOP registry](#), notifying them of a breach of contract. This notification highlights their shortcomings in handling (DNS) abuse in various forms. Some pessimistic observers might also point out that one of the issues raised was about late payment to ICANN - but let's focus on the positives!

ICANN is using the recently updated Registry Agreement (RA), which now includes language about dealing with abuse, to enforce better anti-abuse practices amongst gTLD registry operators. Given .top TLD's poor performance, when it comes to (DNS) abuse, we applaud this action.

Overview continued



01

Overview cont. ✕

While some of the reported contractual breaches are straightforward (like not having a published abuse contact) it should serve as a warning to other TLDs that frequently appear in our statistics. In this report, we give context to TLD activity by providing the percentage of bad reputation domains relative to their total zone file size. This edition features six gTLDs whose zone files have over 25% of domain names in one of our bad reputation datasets.

This makes them outliers - even compared to .top - that require special attention. We hope the newly added provisions around dealing with abuse will empower ICANN to investigate these cases as well.

02

03

04

05



01

# New domains

## New domains overview

Over 36 million new domains were registered over the last six months, averaging 6 million new registrations per month. Compared with the previous six months, registrations have increased by 7%.

The busiest month was May with just over 6.3 million new domains, however all six months were close to the monthly average with minimal difference.

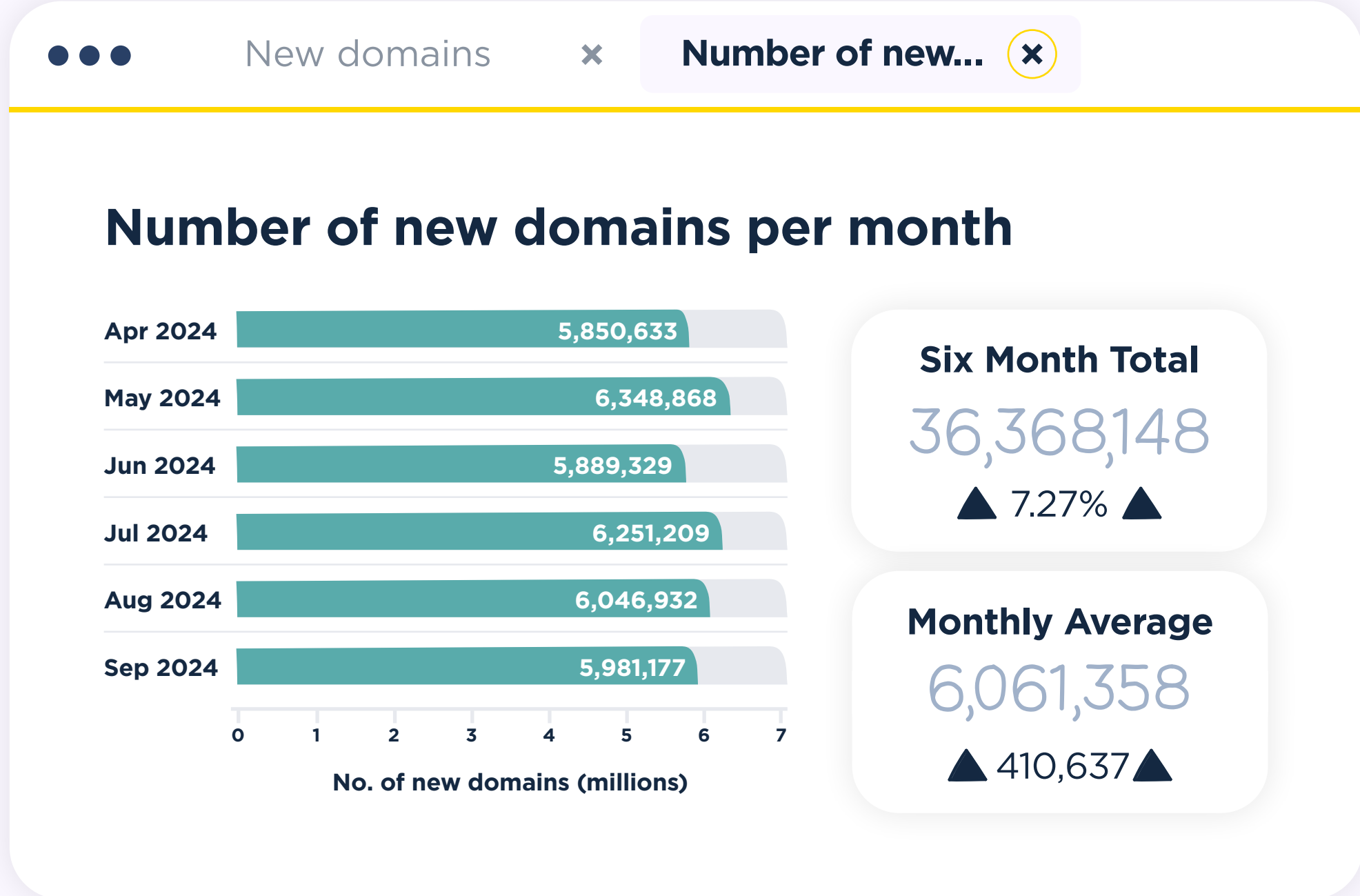
It is important to note that a new domain is not a bad domain, per se. However, a considerable amount of abuse is associated with new domain names. One reason is that if a bad actor buys a new domain and uses it immediately, there is minimal chance of security systems and professionals having prior knowledge 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.

02

03

04

05



**i 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

## New domains by top-level domain (TLD)

Over the last six months, the percentage of ccTLDs increased marginally to 29%, with a corresponding decrease in gTLD registrations to 71%.

Looking at ccTLDs, .cn (#1), .cc (#5) and .us (#6), all had significant increases in new domain registrations, which appear to be linked to promotions at various registrars. Customers can purchase .cc for \$2.40 at Porkbun with promo code 'awesomeness' - not so awesome - enabling abuse with such low price points.

With the continued growth in tech and start-ups, ccTLD .ai entered the Top 20 at rank #19 for the first time. Primarily the ccTLD for Anguilla in the Caribbean, this TLD operates as a gTLD with open registration policies. Available for anywhere between \$33 - \$99 it's unlikely this TLD is being used for abuse.

The gTLD .bond saw an 80% rise in new domain registrations over the past six months, climbing six spots to rank #6 with over 1 million domains, which is more than its current zone file size. This shows how many domains are canceled in relation to abuse issues. Unsurprisingly, readers will see .bond make an appearance in our poor reputation TLD statistics, as when new registrations occur, the number of malicious domains is often relative.

This reporting period also includes new entries from gTLDs .buzz (#16) and .today (#17). Unfortunately, a considerable number of entries are domains that either use domain generated algorithms (DGAs), or otherwise appear unsuitable for human consumption - often consisting of 12 random alphanumeric characters followed by the TLD. We question the value of these registrations and would be surprised to see a legitimate use case for them.

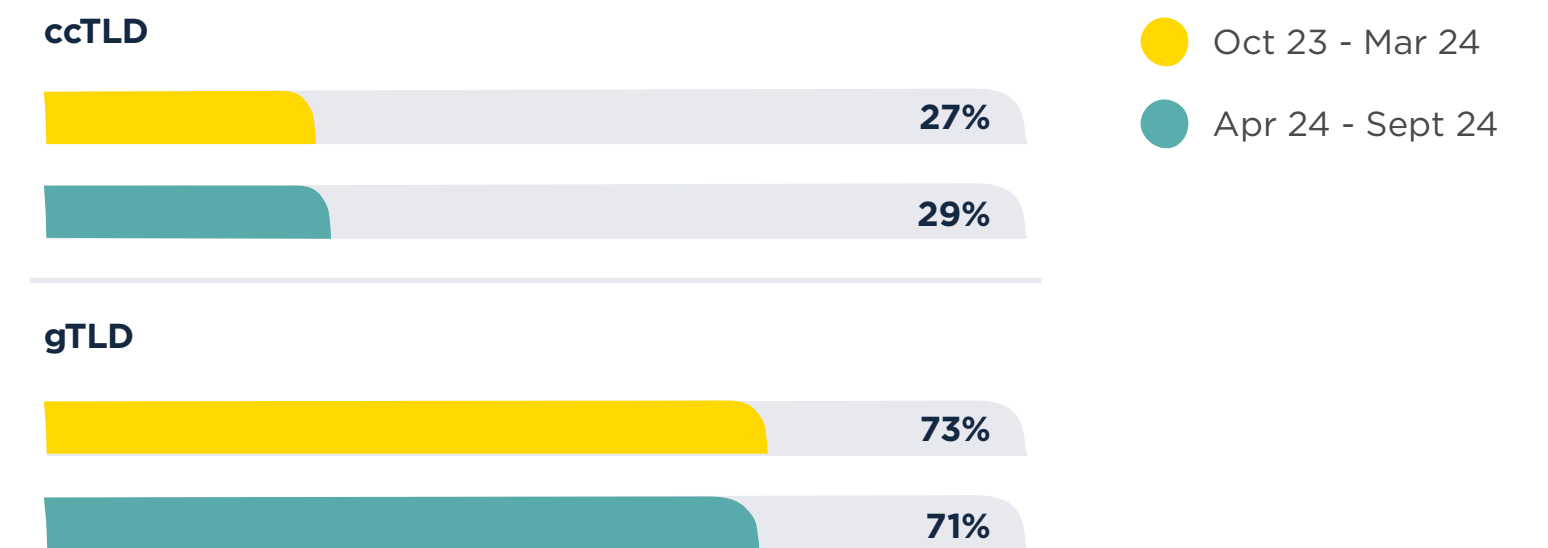
02

03

04

05

## New domain TLD types - six month comparison



### **i** 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

### Top 20 TLDs used in new domains

Rank	New domain TLD	TLD type	Apr 24 - Sept 24	Apr 24 - Sept 24 data bar	Oct 23 - Mar 24	% Change
1	.com	gTLD	11,614,263		11,639,454	▶ 0%
2	.xyz	gTLD	1,325,079		987,598	▲ 34%
3	.shop	gTLD	1,311,392		1,377,092	▼ -5%
4	.cn	ccTLD	1,115,908		646,482	▲ 73%
5	.top	gTLD	1,043,030		823,320	▲ 27%
6	.online	gTLD	1,004,182		1,067,222	▼ -6%
7	.bond	gTLD	1,003,486		557,932	▲ 80%
8	.org	gTLD	836,264		729,065	▲ 15%
9	.de	ccTLD	797,102		621,992	▲ 28%
10	.net	gTLD	736,083		830,805	▼ -11%
11	.com.br	ccTLD	654,045		480,118	▲ 36%
12	.store	gTLD	533,065		595,228	▼ -10%
13	.ru	ccTLD	533,039		615,020	▼ -13%
14	.site	gTLD	511,931		680,511	▼ -25%
15	.cc	ccTLD	459,145		-	New entry
16	.us	ccTLD	457,849		-	New entry
17	.co.uk	ccTLD	435,210		502,739	▼ -13%
18	.co	ccTLD	393,125		396,904	▼ -1%
19	.info	gTLD	386,754		351,338	▲ 10%
20	.lol	gTLD	383,141		-	New entry

02

03

04

05

### Top 20 ccTLDs used in new domains

Rank	New domain TLD	Apr 24 - Sept 24	Apr 24 - Sept 24 data bar	Oct 23 - Mar 24	% Change
1	.cn	1,115,908		646,482	▲ 73%
2	.de	797,102		621,992	▲ 28%
3	.com.br	654,045		480,118	▲ 36%
4	.ru	533,039		615,020	▼ -13%
5	.cc	459,145		258,567	▲ 78%
6	.us	457,849		210,435	▲ 118%
7	.co.uk	435,210		502,739	▼ -13%
8	.co	393,125		396,904	▼ -1%
9	.in	343,245		333,679	▲ 3%
10	.nl	341,688		321,826	▲ 6%
11	.fr	281,673		351,893	▼ -20%
12	.com.au	242,577		208,724	▲ 16%
13	.ca	239,300		275,314	▼ -13%
14	.eu	195,610		200,988	▼ -3%
15	.au	191,874		-	New entry
16	.it	183,077		189,547	▼ -3%
17	.com.tr	155,005		146,900	▲ 6%
18	.pl	153,612		175,597	▼ -13%
19	.ai	146,074		-	New entry
20	.ir	144,614		139,670	▲ 4%

01

### Top 20 gTLDs used in new domains

Rank	New domain TLD	Apr 24 - Sept 24	Apr 24 - Sept 24 data bar	Oct 23 - Mar 24	% Change
1	.com	11,614,263		11,639,454	▶ 0%
2	.xyz	1,325,079		987,598	▲ 34%
3	.shop	1,311,392		1,377,092	▼ -5%
4	.top	1,043,030		823,320	▲ 27%
5	.online	1,004,182		1,067,222	▼ -6%
6	.bond	1,003,486		557,932	▲ 80%
7	.org	836,264		729,065	▲ 15%
8	.net	736,083		830,805	▼ -11%
9	.store	533,065		595,228	▼ -10%
10	.site	511,931		680,511	▼ -25%
11	.info	386,754		351,338	▲ 10%
12	.lol	383,141		260,161	▲ 47%
13	.sbs	371,983		424,338	▼ -12%
14	.vip	350,495		258,415	▲ 36%
15	.pro	223,057		161,626	▲ 38%
16	.buzz	210,829		-	New entry
17	.today	201,927		-	New entry
18	.click	180,417		177,547	▲ 2%
19	.icu	167,220		171,208	▼ -2%
20	.fun	154,989		160,391	▼ -3%

02

03

04

05

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

Rank	New domain TLD	Apr 24 - Sept 24	Zone size	% of zone newly observed	% of zone data bar
1	.bond	1,003,486	464,385	216.09%	
2	.lol	383,141	573,896	66.76%	
3	.buzz	210,829	336,408	62.67%	
4	.today	201,927	432,436	46.70%	
5	.sbs	371,983	805,396	46.19%	
6	.click	180,417	429,115	42.04%	
7	.shop	1,311,392	3,362,971	39.00%	
8	.xyz	1,325,079	3,688,719	35.92%	
9	.fun	154,989	437,399	35.43%	
10	.icu	167,220	483,318	34.60%	
11	.site	511,931	1,510,354	33.89%	
12	.store	533,065	1,573,843	33.87%	
13	.vip	350,495	1,074,824	32.61%	
14	.online	1,004,182	3,177,266	31.61%	
15	.pro	223,057	708,501	31.48%	
16	.top	1,043,030	5,735,506	18.19%	
17	.info	386,754	3,657,425	10.57%	
18	.org	836,264	11,521,597	7.26%	
19	.com	11,614,263	160,666,523	7.23%	
20	.net	736,083	13,205,699	5.57%	



01

●●● Trending terms... ✕

## Trending terms in new domains

In the last six months, trending terms in new domain registrations have remained fairly generic, with little change to the Top 20 list. Trending terms “service” and “online” continue to hold the #1 and #2, spots. A new entry, “course” likely reflects the end of the holiday season and a return to work or education.

Building on the last report, the term “casino” remains prevalent, with 107,722 new registrations - a 46% increase on the previous six months. Aside from the regulatory changes mentioned in the [previous report](#), another possible factor could be domain squatting or flipping. This is when criminals register domains with trademarks belonging to someone else for profit. Due to the high value of certain keywords, the online gaming sector is especially attractive to miscreants.

02

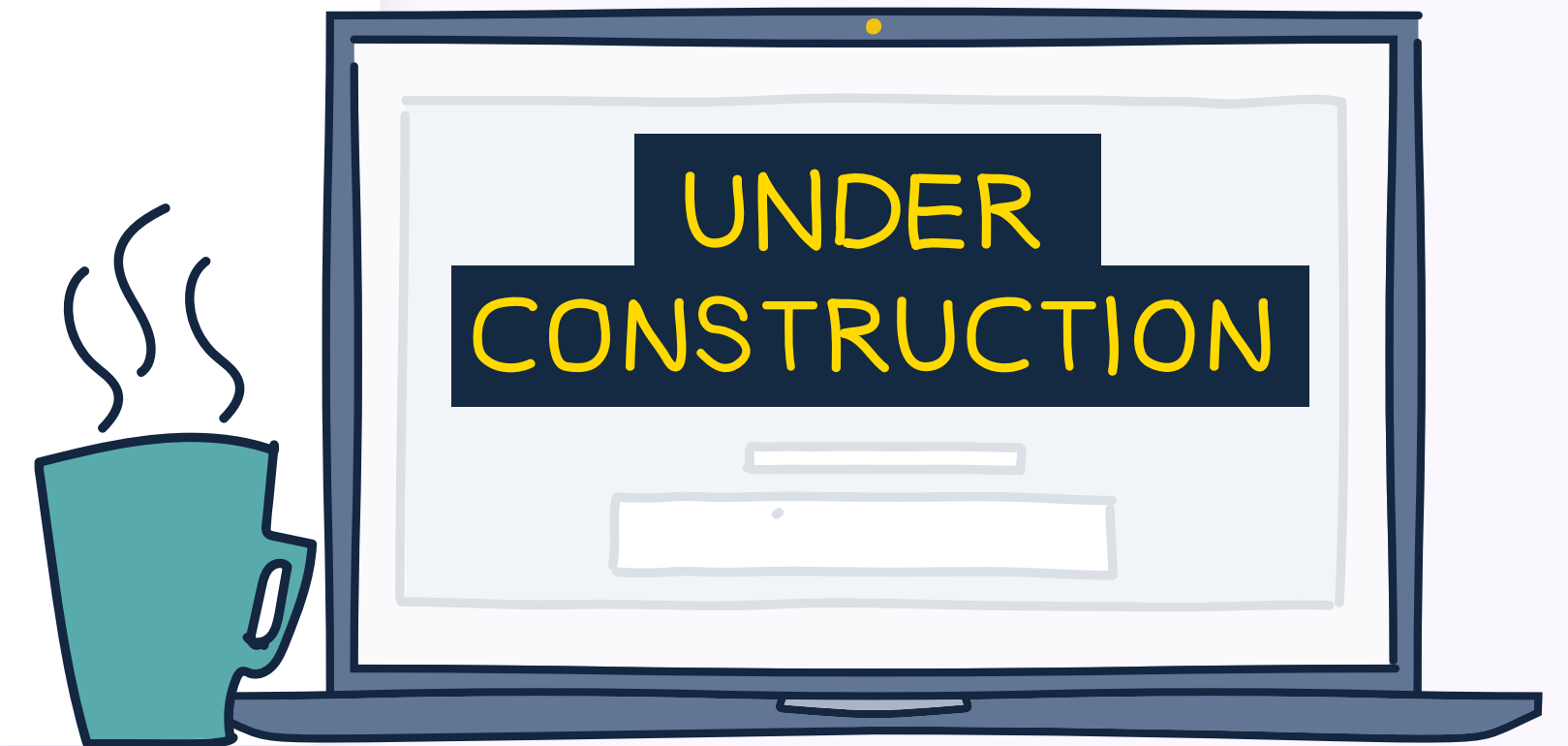
03

04

05

### **i** 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

### Top 20 trending terms in new domains

Rank	Apr 24 - Sept 24 trending terms	Apr 24 - Sept 24	Apr 24 - Sept 24 data bar	Oct 23 - Mar 24	% Change
1	service	273,901		231,943	▲ 18%
2	online	192,092		174,054	▲ 10%
3	solution	167,646		149,273	▲ 12%
4	market	165,294		129,044	▲ 28%
5	design	142,299		138,133	▲ 3%
6	studio	126,694		126,593	▶ 0%
7	group	123,499		124,565	▼ -1%
8	health	123,065		106,871	▲ 15%
9	consult	121,739		119,380	▲ 2%
10	digital	119,336		136,266	▼ -12%
11	casino	107,722		73,812	▲ 46%
12	store	105,515		111,476	▼ -5%
13	business	82,619		-	New entry
14	jobs	80,863		72,853	▲ 11%
15	global	80,855		73,498	▲ 10%
16	invest	72,662		61,427	▲ 18%
17	travel	72,637		67,314	▲ 8%
18	software	58,114		-	New entry
19	course	51,403		-	New entry
20	dental	47,099		-	New entry

02

03

04

05

### Trending terms



01

# Malicious/suspicious domains

## Domain overview

In the past six months, over 1.8 million malicious or suspicious domains were detected, averaging approximately 305K per month. This represents an 81% increase compared to the previous six months (October 2023 to March 2024).

While this increase is significant, it's important to note that the previous report included a period of technical transition to an upgraded platform. This means the figures reported may have been lower than normally expected.

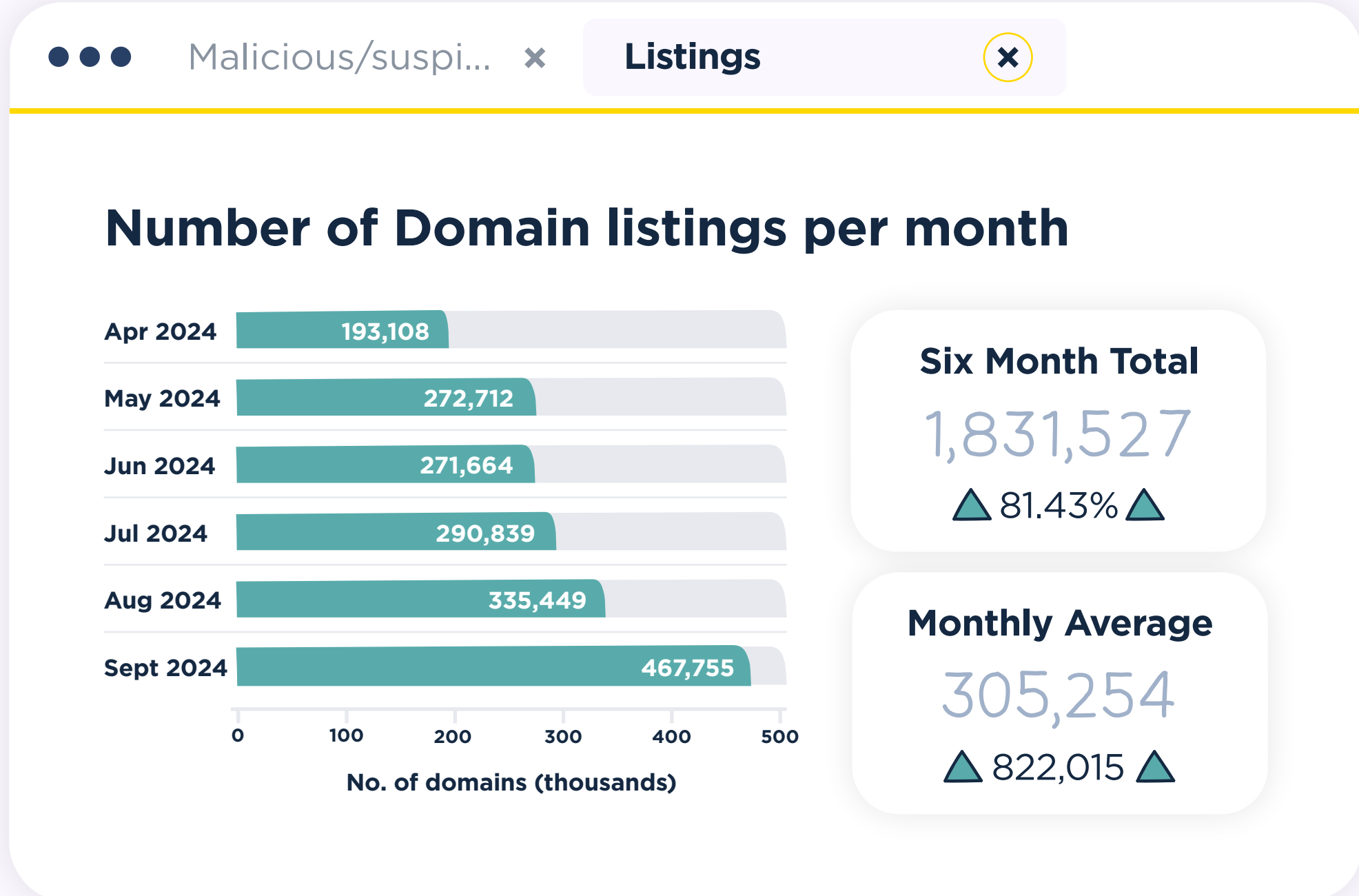
Additionally, changes to our Domain Blocklist expiration policy mean certain domains which are inherently bad, will remain part of various datasets for longer. Normally these listings would be removed after a two week period, and only readded if detected again in the future. However, the opportunity to reuse these domains once they are out of the zone file is no more. As a result, the number of listings is expected to increase.

02

03

04

05



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

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... x

### TLDs listed in our domain data

As expected, Freenom and its controversial free ccTLDs are no more, with .cf, .gq and .tk finally dropping out of the Top 20 TLDs listed in our domain data. Although, the percentage of malicious or suspicious ccTLDs stayed at 18% and gTLDs at 82%, there has been some interesting activity.

This reporting period saw two notable gTLD entries: .vip and .pink. The gTLD .vip ranked #4 in the Top 20 gTLDs, with a 306% increase - the second largest increase with 69,289 domains listed. Meanwhile, nearly half (48.96%) of all .pink domains in the zone file are listed as malicious or suspicious. Both make suitable candidates for ICANN to pursue further!

Seven new ccTLDs entered the Top 20: .sx (#5), .st (#8), .pm (#11), .lc (#14), .tw (#16), .pl (#19), .cz (#20). Many of these listings featured thousands of unpronounceable short length domains, primarily associated with sms-based abuse such as phishing or delivery scams.

There were also significant increases for TLDs .cc (365%), .co (358%), and .tv (128%). Unsurprisingly, these ccTLDs are cheap to register, with minimal restrictions, and available for global use - a hotbed for malicious activity.

The ccTLD, .tv, which belongs to Tuvalu, a small Pacific island, is more commonly used as a gTLD, due to the surge in video content and live streaming platforms. It's an obvious choice for content creators, and equally attractive to cybercriminals!

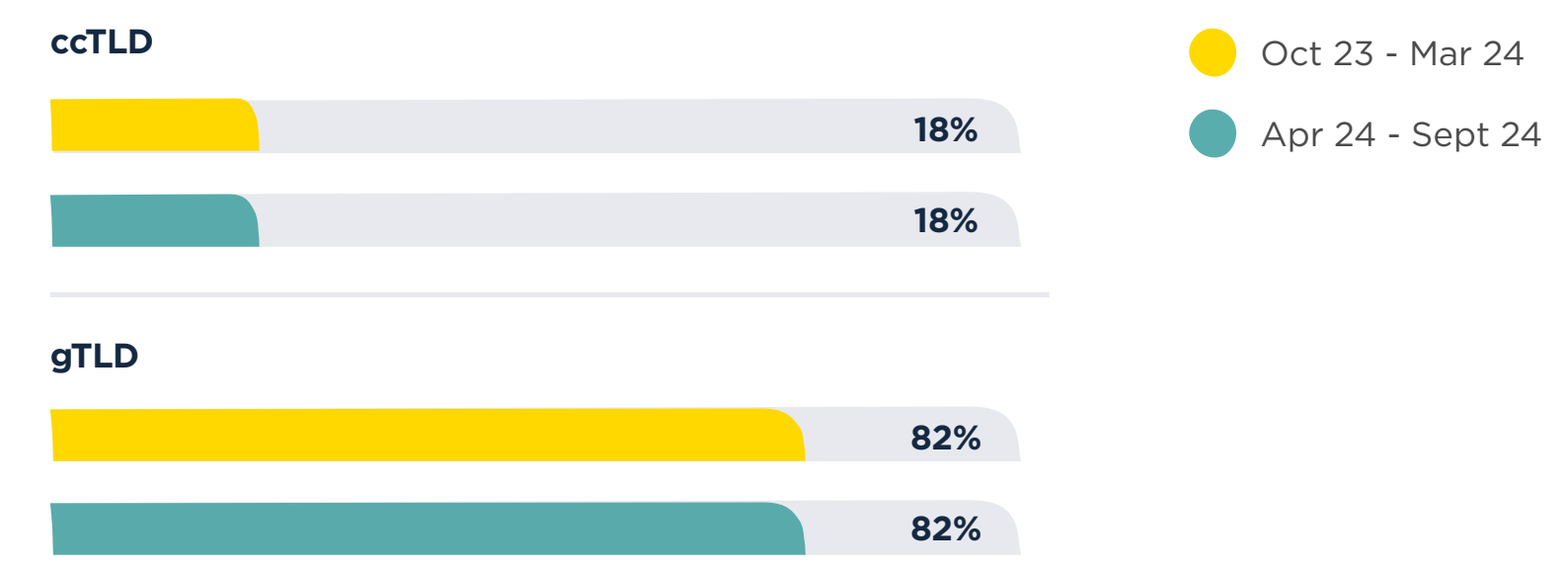
### i Interpreting the data x

Registries with a greater number of active domains have greater exposure to abuse. For example, between April 2024 and Sept 2024 .wang had 109,332 domains in its zone, of which 5.06% were listed.

Meanwhile, .loans had 11,187 domains in its zone, with 41.62% 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... x

### TLD type - six month comparison



01

02

03

04

05

●●● Top 20 TLDs... x Top 20 ccTLDs... x

### Top 20 TLDs

Rank	Domain TLD	Type of TLD	Apr 24 - Sept 24	Apr 24 - Sept 24 data bar	Oct 23 - Mar 24	% Change
1	.com	gTLD	532,978		343,299	▲ 55%
2	.top	gTLD	211,406		86,718	▲ 144%
3	.xyz	gTLD	140,065		64,650	▲ 117%
4	.cc	ccTLD	89,506		19,228	▲ 365%
5	.vip	gTLD	69,289		17,080	▲ 306%
6	.cn	ccTLD	61,420		70,279	▼ -13%
7	.shop	gTLD	56,987		22,542	▲ 153%
8	.ru	ccTLD	49,027		26,856	▲ 83%
9	.club	gTLD	46,239		12,791	▲ 261%
10	.net	gTLD	40,887		34,093	▲ 20%
11	.co	ccTLD	26,438		-	New entry
12	.rest	gTLD	24,641		-	New entry
13	.org	gTLD	24,471		19,614	▲ 25%
14	.app	gTLD	23,223		-	New entry
15	.info	gTLD	20,834		21,079	▼ -1%
16	.bond	gTLD	16,802		8,054	▲ 109%
17	.online	gTLD	15,355		22,285	▼ -31%
18	.sbs	gTLD	15,037		26,564	▼ -43%
19	.buzz	gTLD	14,344		-	New entry
20	.pro	gTLD	12,916		-	New entry

●●● Top 20 TLDs... x Top 20 ccTLDs... x

### Top 20 ccTLDs

Rank	Domain TLD	Apr 24 - Sept 24	Apr 24 - Sept 24 data bar	Oct 23 - Mar 24	% Change
1	.cc	89,506		19,228	▲ 365%
2	.cn	61,420		70,279	▼ -13%
3	.ru	49,027		26,856	▲ 83%
4	.co	26,438		5,771	▲ 385%
5	.sx	9,128		-	New entry
6	.us	6,798		4,807	▲ 41%
7	.me	6,435		4,308	▲ 49%
8	.st	5,256		-	New entry
9	.de	5,102		2,850	▲ 79%
10	.uk	4,990		3,866	▲ 29%
11	.pm	4,139		-	New entry
12	.tv	3,671		1,612	▲ 128%
13	.eu	2,706		1,597	▲ 69%
14	.lc	2,691		-	New entry
15	.ng	2,565		2,469	▲ 4%
16	.tw	2,540		-	New entry
17	.in	2,492		3,387	▼ -26%
18	.pw	2,160		2,532	▼ -15%
19	.pl	1,872		-	New entry
20	.cz	1,833		-	New entry

01

02

03

04

05

### Top 20 gTLD

Rank	Domain TLD	Apr 24 - Sept 24	Apr 24 - Sept 24 data bar	Oct 23 - Mar 24	% Change
1	.com	532,978		343,299	▲ 55%
2	.top	211,406		86,718	▲ 144%
3	.xyz	140,065		64,650	▲ 117%
4	.vip	69,289		17,080	▲ 306%
5	.shop	56,987		22,542	▲ 153%
6	.club	46,239		12,791	▲ 261%
7	.net	40,887		34,093	▲ 20%
8	.rest	24,641		-	New entry
9	.org	24,471		19,614	▲ 25%
10	.app	23,223		-	New entry
11	.info	20,834		21,079	▼ -1%
12	.bond	16,802		8,054	▲ 109%
13	.online	15,355		22,285	▼ -31%
14	.sbs	15,037		26,564	▼ -43%
15	.buzz	14,344		5,386	▲ 166%
16	.pro	12,916		-	New entry
17	.cam	12,127		-	New entry
18	.ooo	11,808		-	New entry
19	.icu	11,671		5,371	▲ 117%
20	.cfd	10,194		14,967	▼ -32%

### Top 20 gTLDs by % of zone file

Rank	Domain TLD	Apr 24 - Sept 24	Zone size	% of zone listed	% of zone data bar
1	.pink	9,020	18,422	48.96%	
2	.loans	4,656	11,187	41.62%	
3	.loan	6,750	17,208	39.23%	
4	.rest	24,641	66,757	36.91%	
5	.ooo	11,808	43,023	27.45%	
6	.photo	7,732	28,217	27.40%	
7	.cam	12,127	51,662	23.47%	
8	.wiki	10,121	74,098	13.66%	
9	.party	3,024	23,602	12.81%	
10	.miami	1,875	15,736	11.92%	
11	.christmas	2,204	21,341	10.33%	
12	.bid	2,107	21,709	9.71%	
13	.pet	1,876	20,360	9.21%	
14	.photos	2,109	26,138	8.07%	
15	.college	1,907	24,472	7.79%	
16	.club	46,239	627,148	7.37%	
17	.vip	69,289	1,074,824	6.45%	
18	.men	799	14,985	5.33%	
19	.wang	5,529	109,332	5.06%	
20	.skin	3,081	61,572	5.00%	

01

●●● Trending terms... ✕

## Trending phishing terms for malicious or suspicious domains

Over the past year, we've continued to see a recurring pattern in the Top 20 Phishing Terms related to package delivery, specifically targeting well-known postal services or known large volume shippers, including: "usps" (#4), "correo" (#13), "laposte" (#19), and "amazon" (#20).

Our researchers are observing a rise in delivery scams, where recipients receive messages, often via SMS, asking them to reschedule a delivery or pay an import tax fee. These scams are becoming increasingly sophisticated, using previously stolen names, email addresses, and phone numbers to deceive victims into transferring money. The scams are so convincing that many fall victim.

In a turn of events, "apple" has finally dropped out of the Top 20, after being a fixture since the very first Domain Report. Meanwhile, context-related terms such as "service" (#1), "account" (#3), or "online" (#5) and action-related terms like login (#2) and verification (#7) continue to remain popular in phishing domains.

### **i** 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".



05

01

### Top 20 phishing terms

Rank	Term	Apr 24 - Sept 24	Apr 24 - Sept 24 data bar	Oct 23 - Mar 24	% Change
1	service	12,187		6,582	▲ 85%
2	login	8,219		4,028	▲ 104%
3	account	6,277		2,211	▲ 184%
4	usps	4,364		1,543	▲ 183%
5	online	4,201		3,692	▲ 14%
6	support	4,003		3,324	▲ 20%
7	verification	3,819		-	New entry
8	security	3,815		-	New entry
9	wallet	3,742		1,134	▲ 230%
10	canada	3,670		1,532	▲ 140%
11	deliver	3,644		3,033	▲ 20%
12	livery	3,489		-	New entry
13	correo	3,074		3,993	▼ -23%
14	verify	2,740		2,458	▲ 11%
15	vices	2,673		-	New entry
16	post	2,502		1,986	▲ 26%
17	counting	2,127		-	New entry
18	finance	1,733		1,074	▲ 61%
19	laposte	1,604		-	New entry
20	amazon	1,567		1,009	▲ 55%

02

03

04

05

### Phishing terms





01

02

03

04

05



## Types of abuse



### Types of abuse

During this reporting period, the number of compromised domains decreased across all types of abuse, except for phishing, which increased by 156%. This is largely due to an increased focus by Spamhaus researchers in this area. Malware distribution took a big hit in May thanks to [Operation Endgame](#) - the largest ever takedown operation targeting botnets involved with ransomware.

As mentioned earlier in the report, in malicious registrations thousands of domains listed during this period consist of four or five random characters. This pattern is typical of sms-based phishing abuse, where the 160 character limit encourages the use of shorter domain names.

As most established TLDs no longer have many 4-letter domains available, phishers are moving to less popular TLDs where these are still unregistered. Unsurprisingly, some of these TLDs, such as .buzz (#15) which featured in the Top 20 gTLDs, cost less than \$1. Unfortunately, this very low pricing makes such domains ripe for abuse.



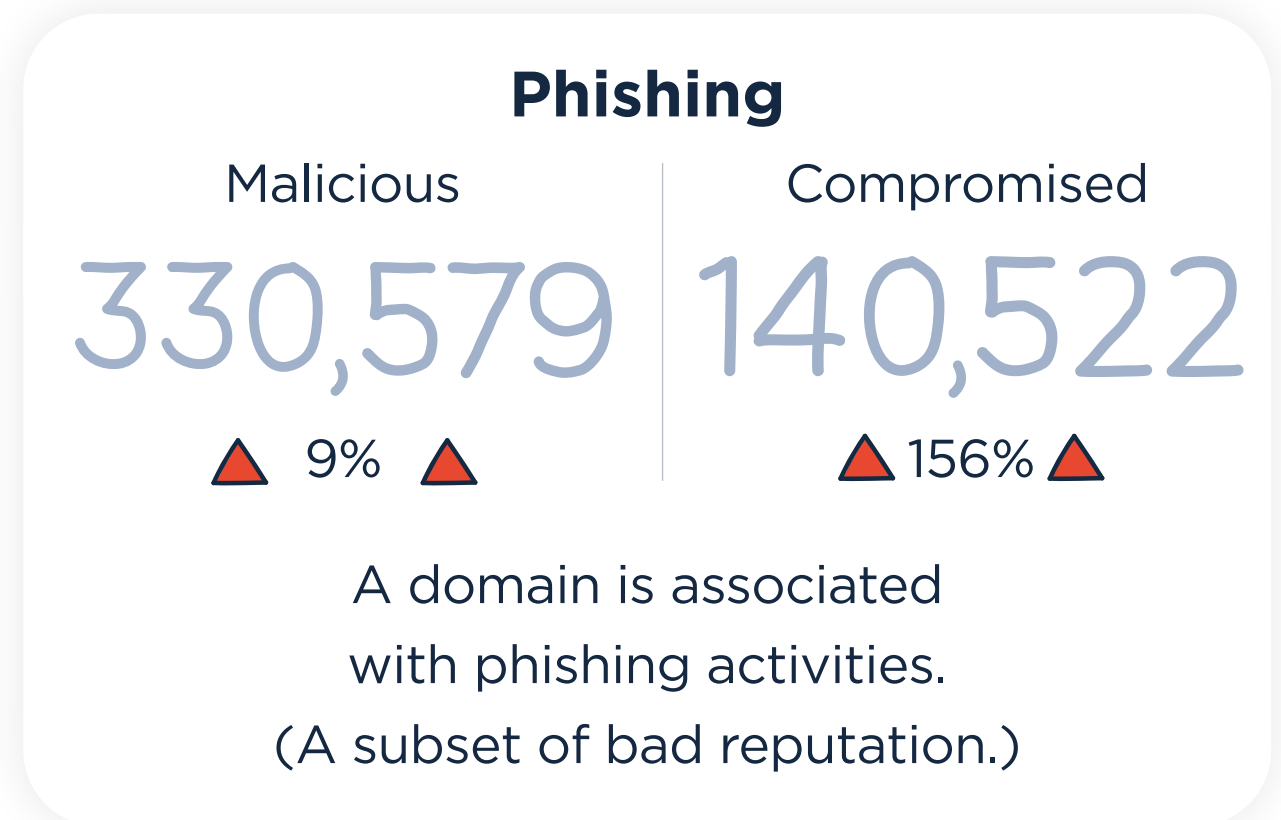
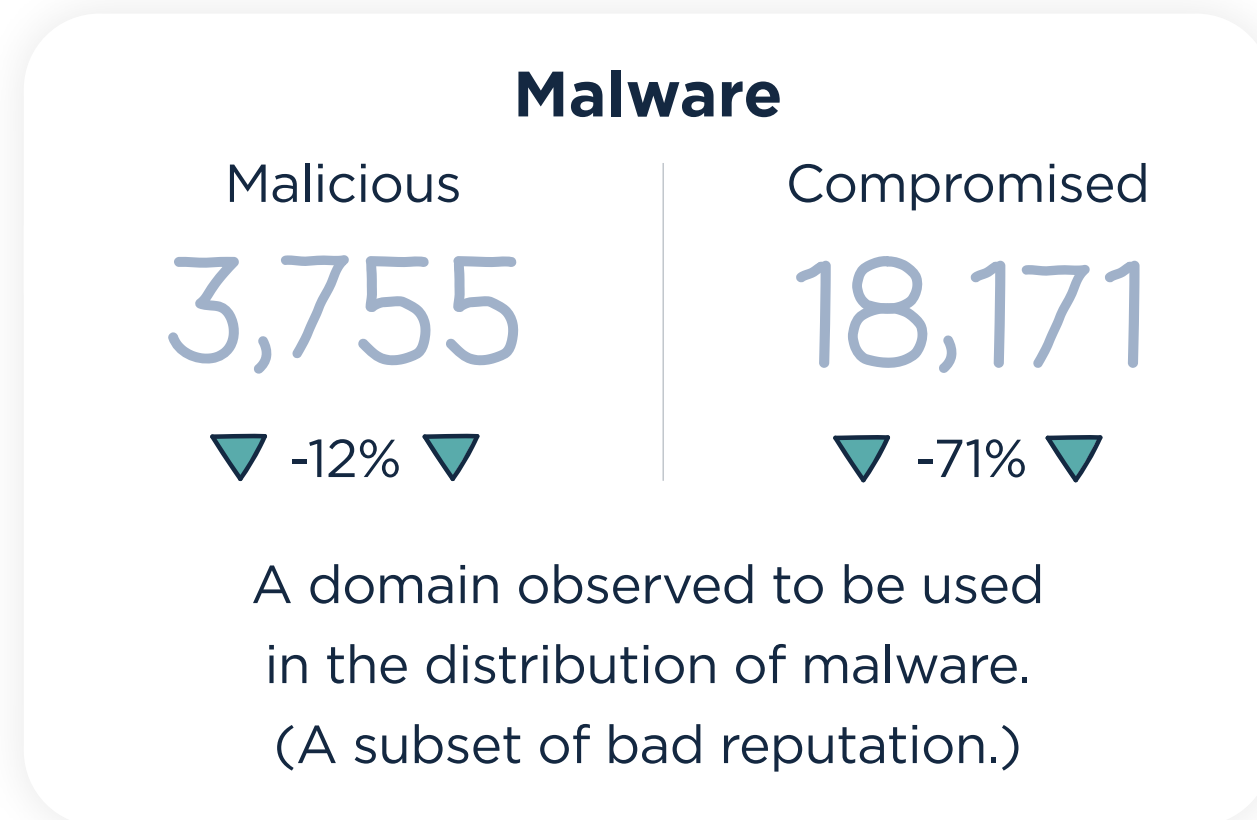
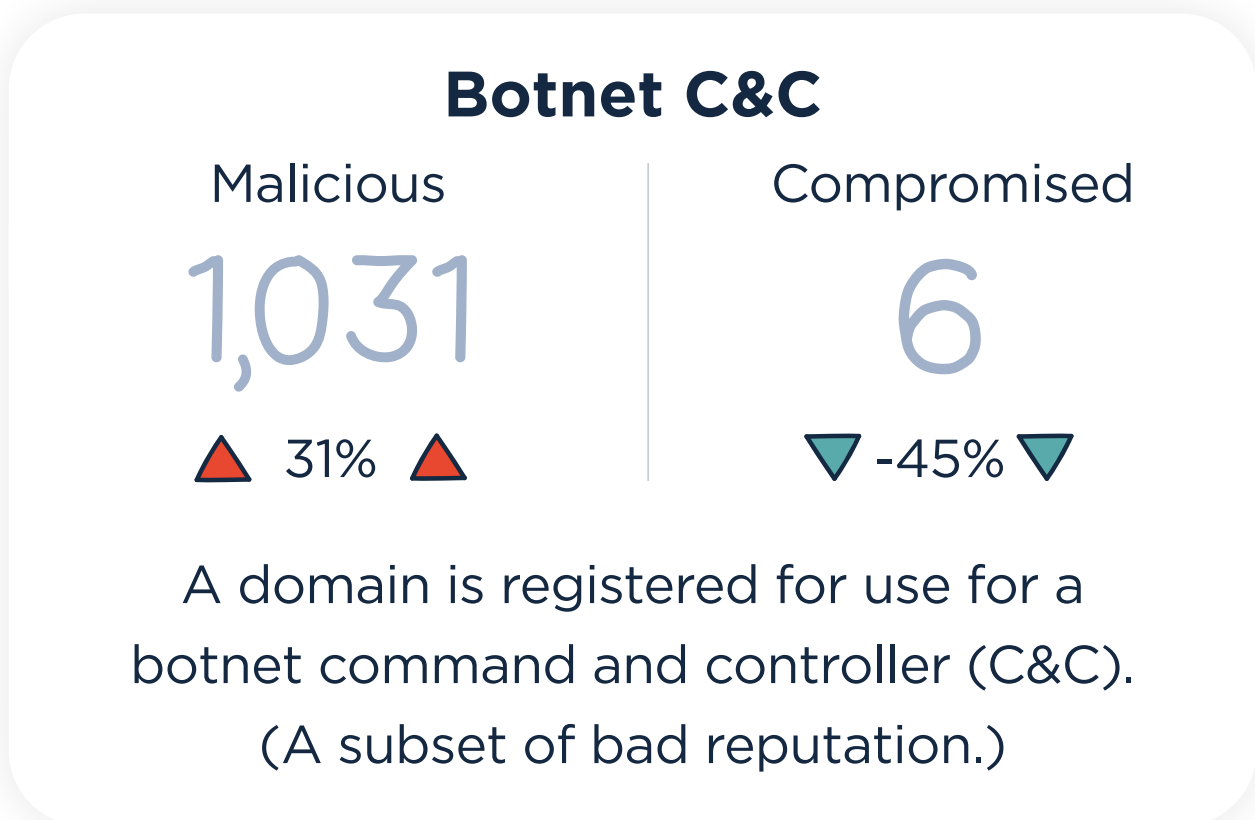
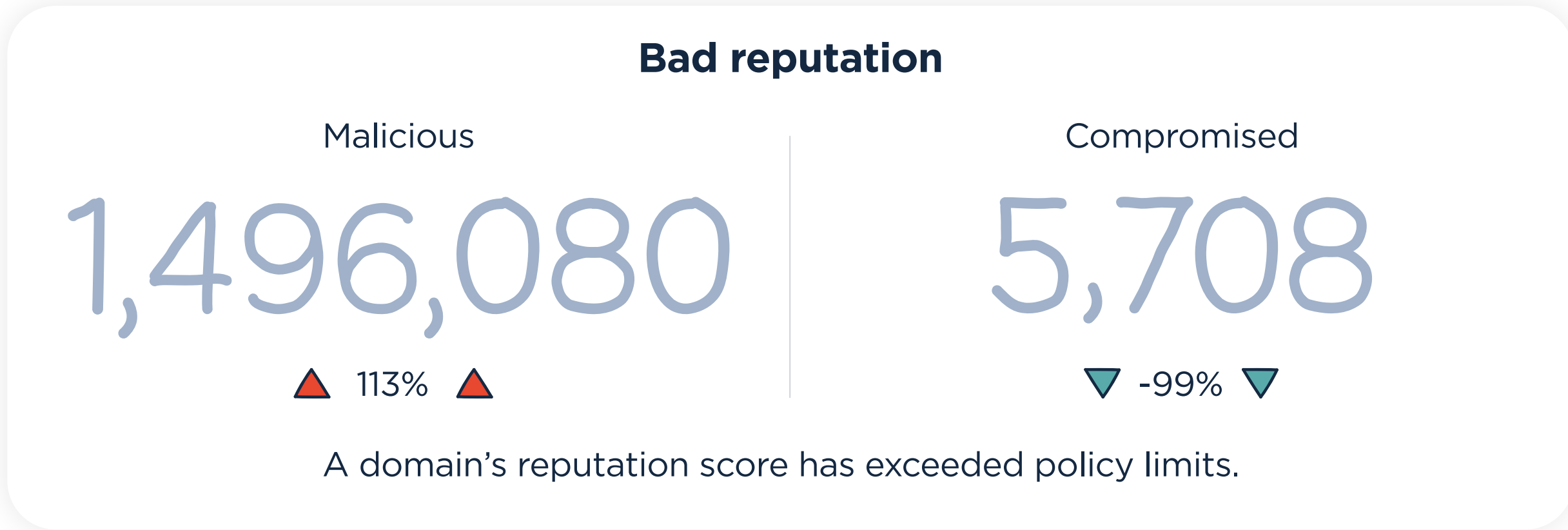
### Differences between compromised and malicious domains



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.

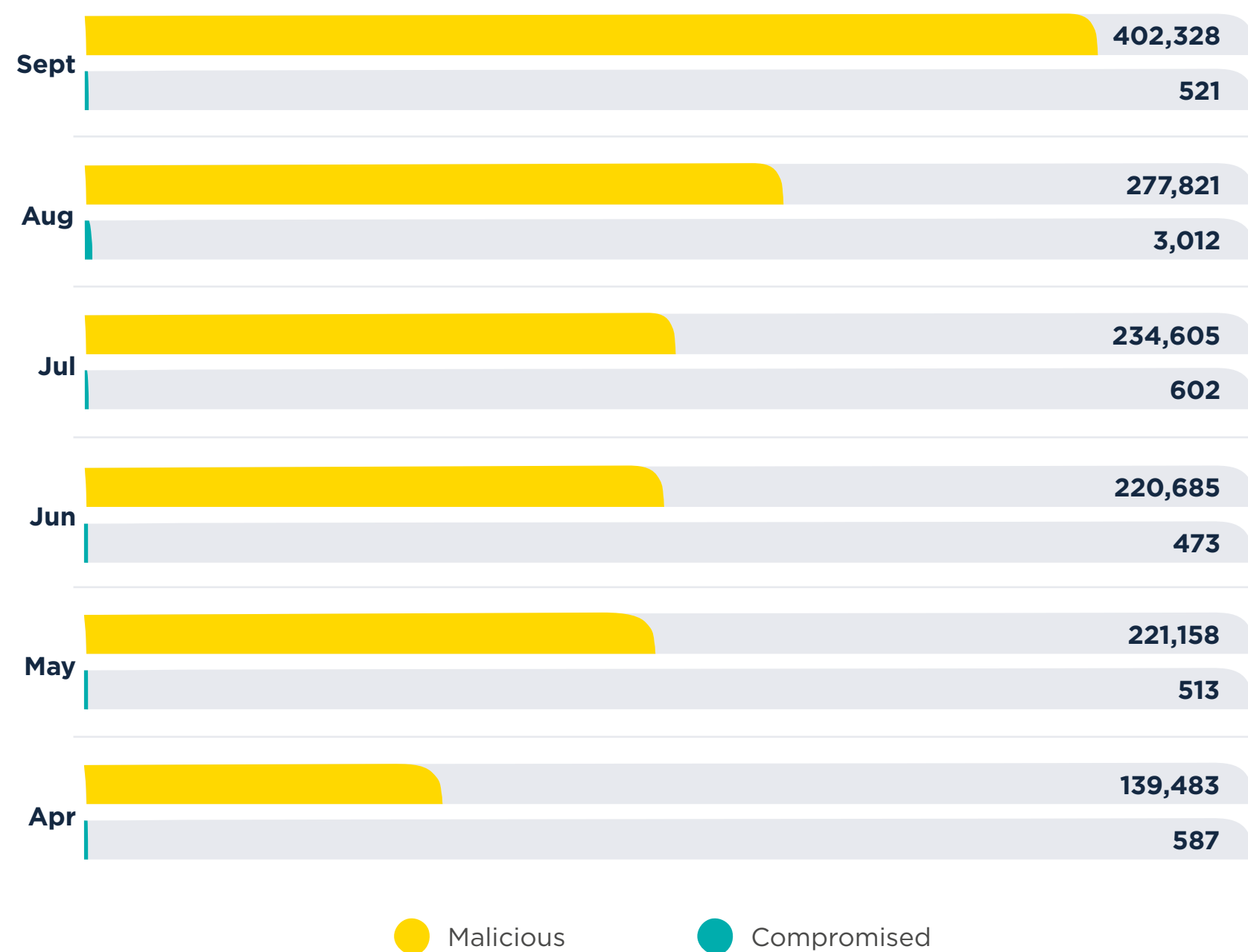
### Types of abuse



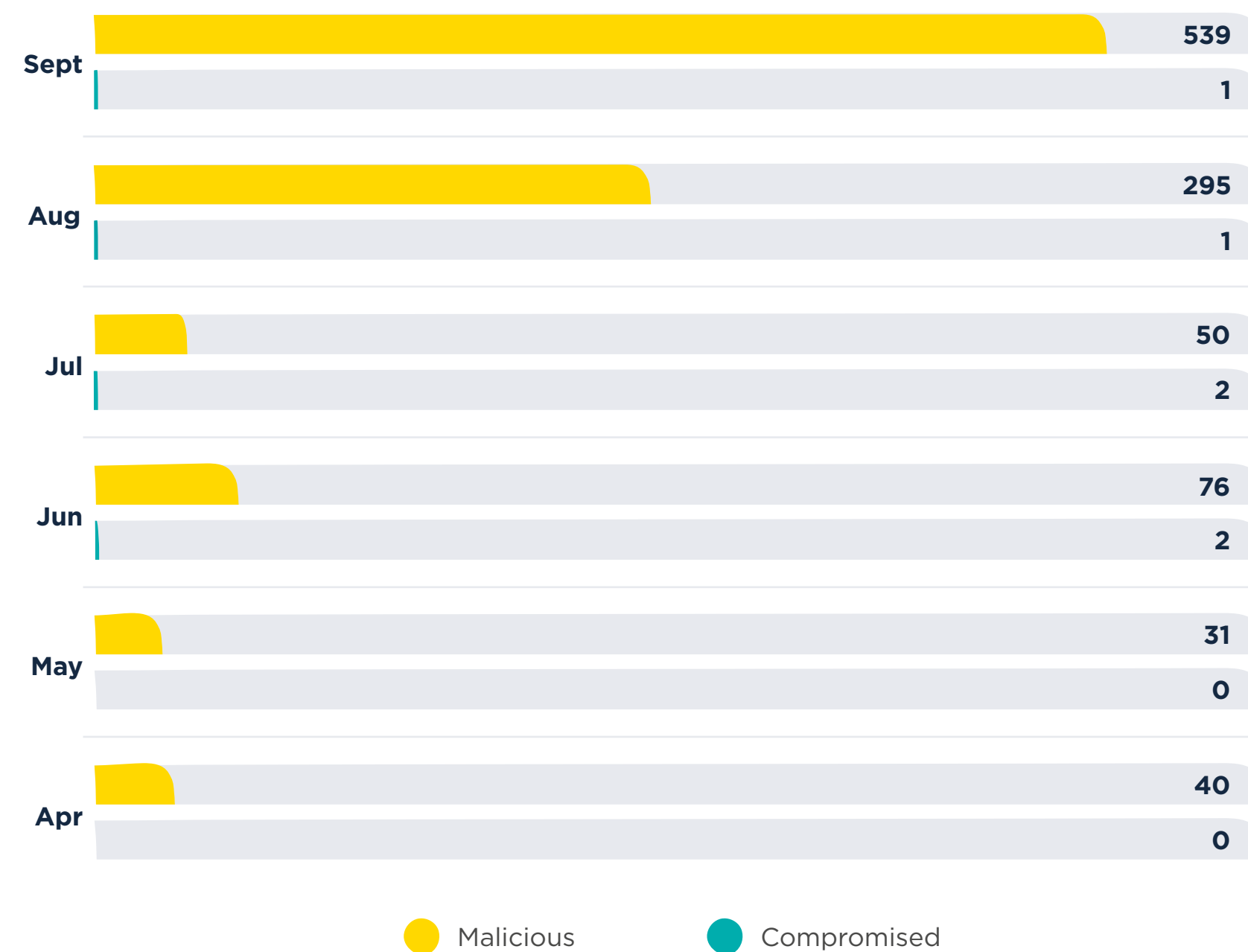
- 01
- 02
- 03
- 04
- 05

### Types of abuse per month

#### Bad reputation per month



#### Botnet C&C per month



01

02

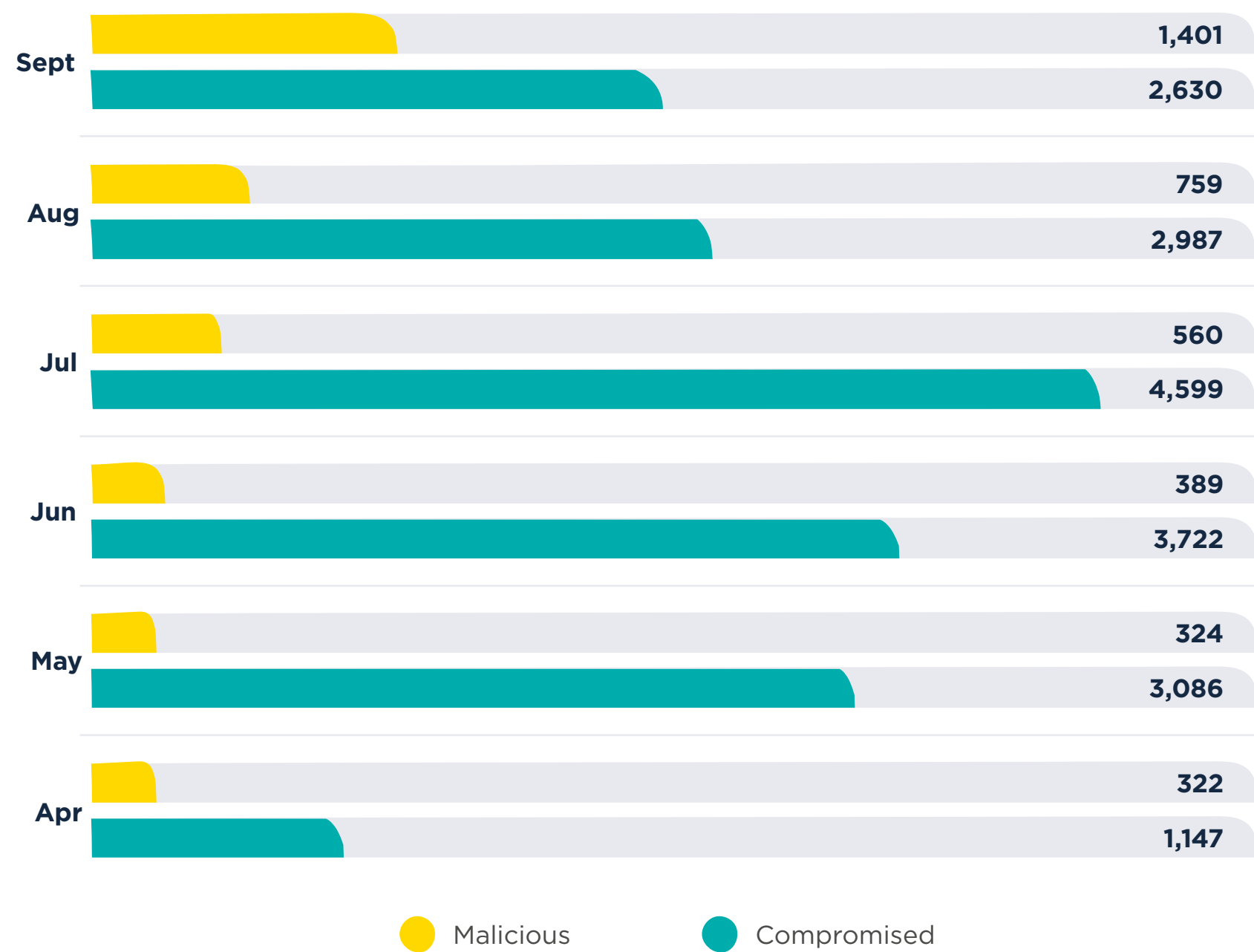
03

04

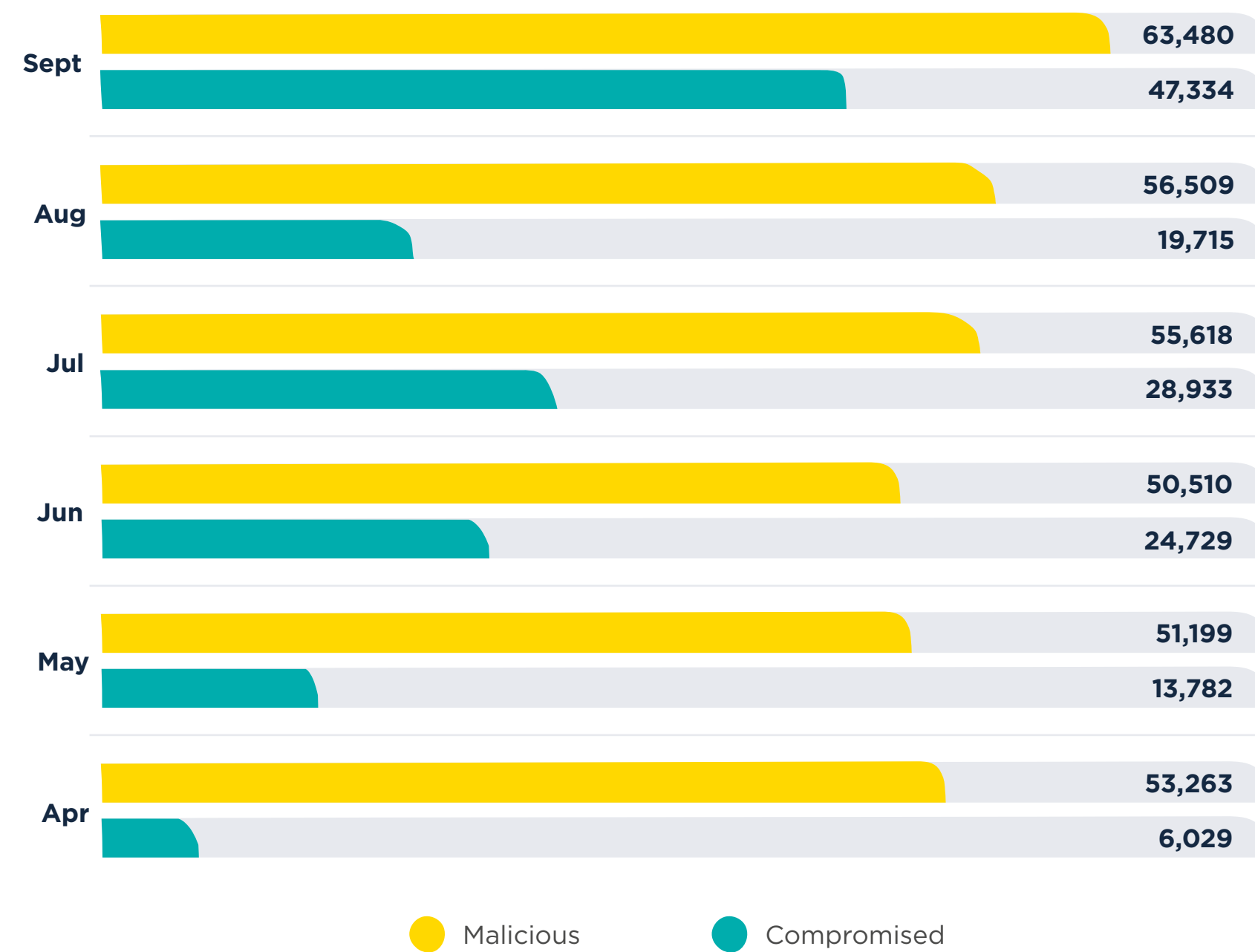
05

### Types of abuse per month

#### Malware per month



#### Phishing per month



01

02

03

04

05

# Recommendations

As these reports are consumed by many registries and registrars, we want to take this opportunity to provide additional background information and recommendations regarding the data we publish. This applies to the data we publish in our blocklists, the website [reputation statistics](#) and the data in these reports.

## Takedown isn't always a requirement

The inclusion of a domain (or cluster of domains) in any blocklist does not mean that we expect the responsible registry or registrar to immediately take down the domain. Our systems are driven by reputation engines. This means good or legitimate domain names may end up in a blocklist due to poor decisions made by their owners. While these decisions may be poor, they don't always warrant immediate action from registrars or registries.

## Expiration dates change

When using this data for statistical purposes, keep in mind that different entries in datasets may have different expiration dates, depending on how the domains are used, whether they are fully malicious registrations or simply compromised domains. These expirations can also change over time.

## Make sure you always fully understand the data

If your use case does not involve blocking or scoring domains with our data, make sure you consider the various policies and details around the listings. If you're ever unsure, don't hesitate to reach out to us - we always welcome working with the community.

## Get social

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

See you in April 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.

01

02

03

04

05