



# Spamhaus Quarterly Domain Reputation Update

## Q3 2023

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 Quarterly Domain Reputation Update Q3 2023.**

[Enter](#)



# Contents

## The Overview

01 The Overview

02 Big news! This quarter saw the end of many abusive practices enabled by Freenom domains.

03 Having been the main provider of free domains since Q3 2022, Freenom is migrating to the next business model of free domains.

04 Without cheap domains, the threat actors' activities are broken. Large volumes of new domains are sold solely with the intention of enabling cybercrime or fraud. However, the fact remains that aggressive pricing certainly facilitates threat actors' activities.

05 Overview continued



Spamhaus Quarterly Domain Reputation Update Q2-2023

Go to page 3

## New domains

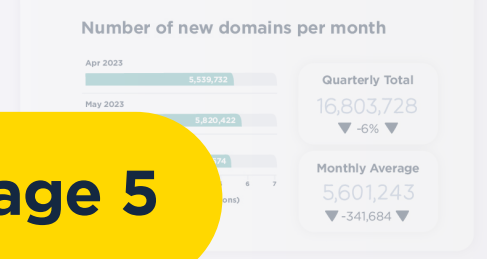
01 New domains

02 New domains overview

03 In Q2, we observed almost 17 million new domains across all gTLDs and ccTLDs, down 6% from 17,440,000 in Q1 2023. However, the number of new domains in the northern hemisphere, October through December, were similar to previous quarters.

04 It is important to note that the number of bad domains, per se, however, is not a strong indicator of abuse associated with new domains. One reason is that if a bad actor registers a 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.

05



Spamhaus Quarterly Domain Reputation Update Q2-2023

Go to page 5

## Domains listed

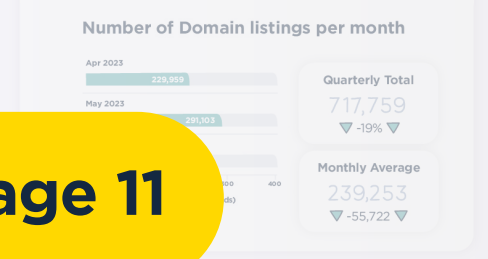
01 Domains listed

02 Domain Overview

03 In Q2, just over 319k domains were listed, with an increase of 239k per month - a decrease of 10% since Q3 2022. This is almost double the number of domains no longer accessing new Freenom domains, which migrated to other 'cheap' providers. Consequently, threat actors are able to access a larger number of these domains.

04

05



Spamhaus Quarterly Domain Reputation Update Q2-2023

Go to page 11

## Recommendations of the quarter

01 Recommendations of the quarter

02 Domain owners, consider the impact of your chosen TLD: At Spamhaus we don't reveal the inner workings of the reputation engine. Adjustments are frequently made to punish bad behaviour and reward good. Following recent changes, we now consider TLD reputation in various scenarios. Domains that exist under TLDs with a bad reputation will move faster towards a bad reputation. Domain owners should consider the impact of their TLD choice carefully about where they register their domains.

03 Implement Know-Your-Customer (KYC) procedures: Working near the intersection of domain registration and KYC is to refer to the FIRST DNS project. To avoid a TLD with many abusive domains once registered, take inspiration from the financial sector regarding Know-Your-Customer procedures. Aggressive pricing is a business model choice, which tends to mean limited resources for strong Know-Your-Customer and after-sale anti-abuse policies. This should be better considered in business planning.

04

05

Spamhaus Quarterly Domain Reputation Update Q2-2023

Go to page 20

## Additional info

01 Additional info

02 About Spamhaus

03 Spamhaus is the trusted authority for domain reputation, unique IP reputation, and quality of actionable intelligence. The data in this report is derived from our threat intelligence networks and email workbooks. With over two decades of experience, our researchers and threat hunters are 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.

04 Report Methodology

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

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

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

Spamhaus Quarterly Domain Reputation Update Q2-2023

Go to page 21

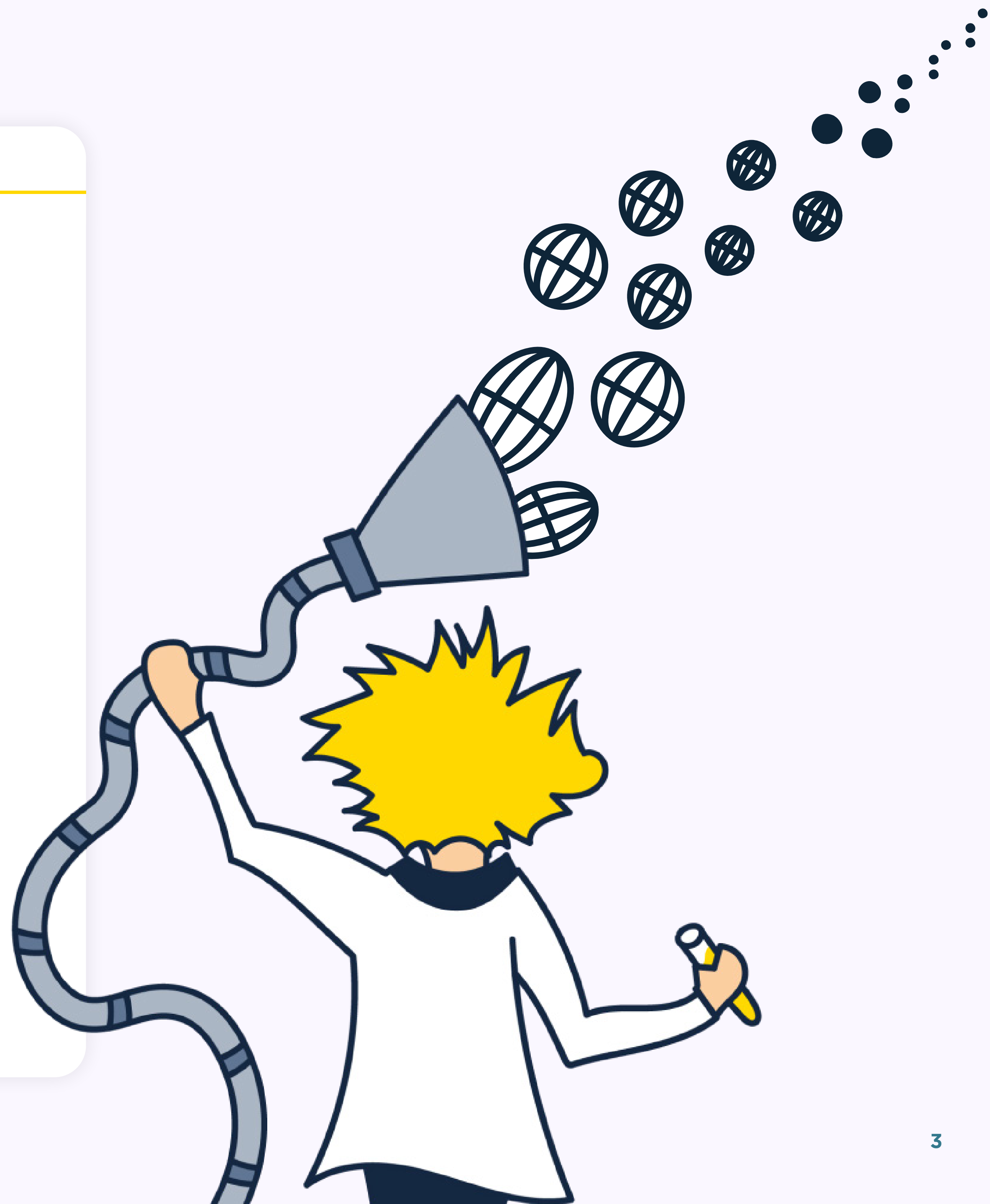
01

## The Overview

With the (almost) demise of Freenom operated TLDs, we predicted that some of the low-reputation registrations that occur would move to different TLDs. While that has definitely happened, it hasn't happened at the scale we anticipated. We can't be 100% sure of the reasoning behind this until various actors tell us. Nevertheless, we have a strong suspicion that price may play a part here. Think of it; while getting a domain name for only US \$2 seems very cheap (and it is!), it is still US \$2 more than free, the price point at which Freenom operated. It certainly looks like some cybercrime business models can be broken after all.

This impacts the tactics and procedures of malicious operators; to continue they must innovate. That means moving away from free bulk registrations that can be quickly burnt through towards domains that can be used for the longer term. We have already observed this with some of the more sophisticated malspam operations, where they prefer second-hand domains provisioned and authenticated according to best current practices over multiple new domains without any reputation associated with them. This change in modus operandi will require a shift from the defensive side as well.

[Overview continued](#)





In the phishing landscape the rising use of short domain names for SMS-based spam (also known as 'smishing') continues to be prevalent. As the SMS medium has very little filtering applied at most telco's, senders of these messages have mostly free reign. This in turn drives large batches of short domains being registered solely for phishing/smishing, with registrations happening in any short TLD that has short names available.

01

02

03

04

05



01

# New domains

## New domains overview

In Q3, we observed just over 16.85 million new domains in the wild, almost the same as in Q2. The busiest month was August, with just under 5.7 million new domains being observed, however, the difference between the months was minimal.

This constant in monthly averages doesn't surprise us – the summer months are usually steady. Naturally, there's the general ebb and flow, with some TLDs having higher-than-average registration numbers, primarily driven by marketing campaigns and cheap prices.

Next quarter, we predict an increase in new domain registrations, as the last quarter of the year generally has more commercial activity and public holidays in many regions throughout the world.

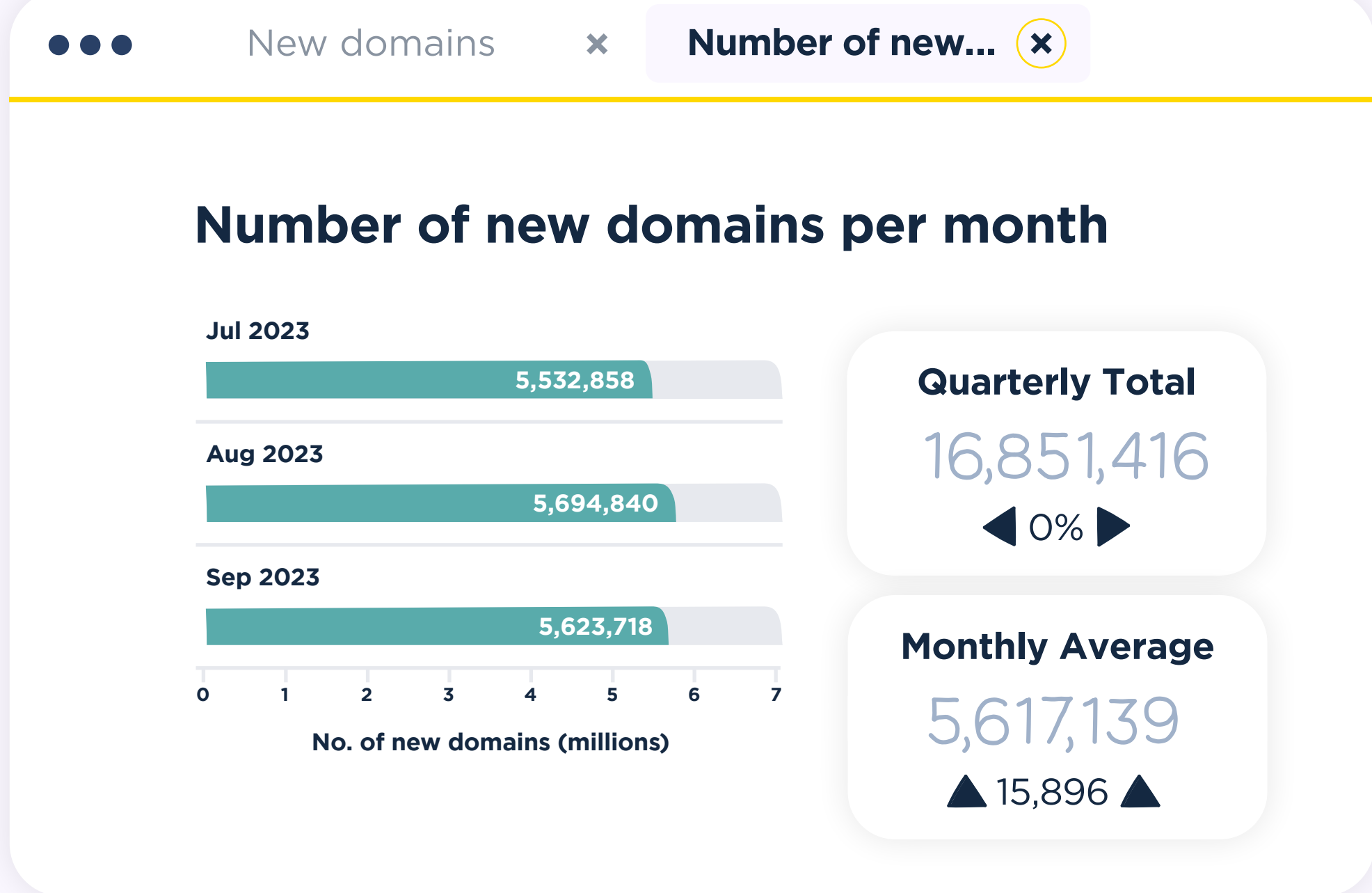
It is important to note that a new domain is not a bad domain, per se. However, a considerable amount of abuse is associated with new domain names. One reason is that if a bad actor buys a new domain and uses it immediately, there is minimal chance of security systems and professionals having prior knowledge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

02

03

04

05

●●● New domains... x TLD types... x

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

Looking at the data, there is clearly an increase in volume across the more “price conscious”, i.e. cheap TLDs. This is hardly surprising, given that the low price point per registered domain allows for more domains to be bought for the same amount of money. Unfortunately, this is taken advantage of by actors making bulk registrations through domain generated algorithms (DGAs). In our opinion, these add very little, if any, value.

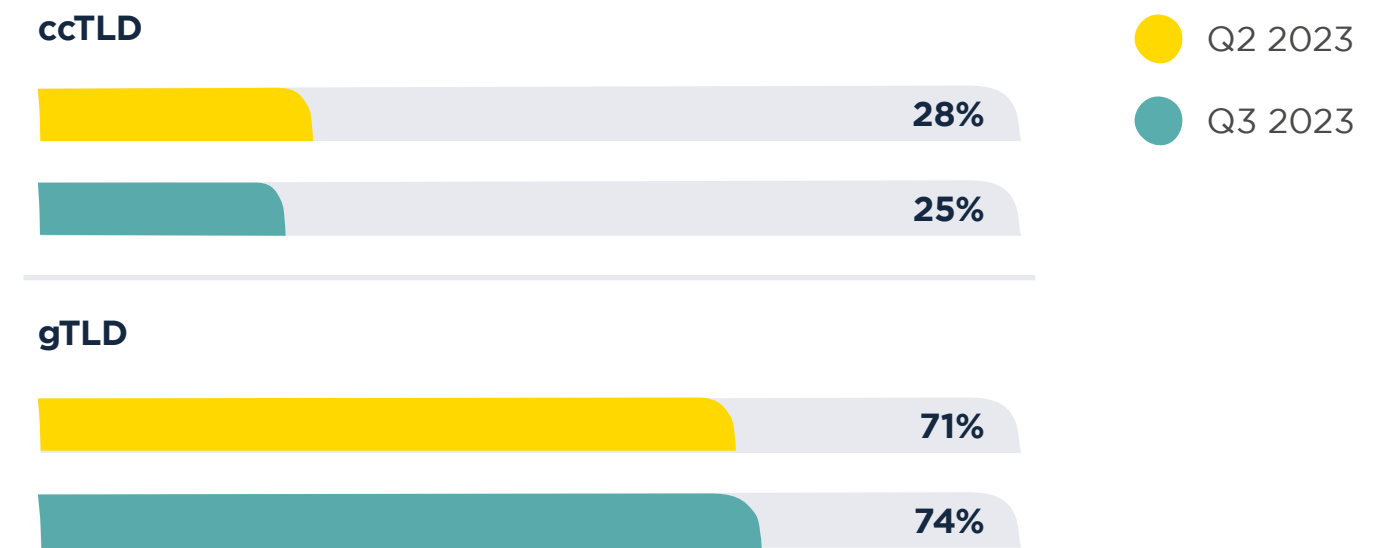
Speaking of generated domains, based on the zone file data, we saw the largest increase in new gTLD domains registered with .bond (178%). That impressive growth of over 97% (165K new domains of a 170K in the total zone file), appears to be largely driven by one entity - creating automatically generated domain names. Experience tells us that very little good is done with these types of domains.

Our experts predict that the vast majority of these domain names will never be renewed, as the renewal price is often four to five times higher than the initial registration price. If you own 10,000s of “word-word-number.tld” domains, renewal costs add up fast!

The .lat TLD also saw some explosive growth (68%). Focused on a Latin American audience, it is peculiar to observe that almost half of these registrations use Chinese nameservers. We again wonder how many of these registrations will survive the first year and for what purpose these domains are being used!

●●● New domains... x TLD types... x

### New domain TLD types comparison, quarter on quarter



#### **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... x Top 20 ccTLDs... x

## Top 20 TLDs used in new domains

Rank	New domain TLD	TLD type	Q3 2023	Q3 data bar	Q2 2023	% Change
1	.com	gTLD	6,086,487		6,200,946	▼ -2%
2	.top	gTLD	704,799		473,333	▲ 49%
3	.online	gTLD	675,305		476,268	▲ 42%
4	.cfid	gTLD	511,191		333,226	▲ 53%
5	.xyz	gTLD	456,072		546,683	▼ -17%
6	.shop	gTLD	375,146		344,624	▲ 9%
7	.net	gTLD	372,563		363,344	▲ 3%
8	.org	gTLD	335,045		347,912	▼ -4%
9	.site	gTLD	300,768		297,222	▲ 1%
10	.de	ccTLD	298,994		365,417	▼ -18%
11	.store	gTLD	266,969		261,710	▲ 2%
12	.ru	ccTLD	254,569		234,458	▲ 9%
13	.co	ccTLD	245,100		197,432	▲ 24%
14	.com.br	ccTLD	221,302		215,607	▲ 3%
15	.cn	ccTLD	213,681		214,026	▶ 0%
16	.co.uk	ccTLD	182,146		274,420	▼ -34%
17	.nl	ccTLD	179,446		202,605	▼ -11%
18	.in	ccTLD	174,811		180,128	▼ -3%
19	.click	gTLD	168,206		-	New entry
20	.bond	gTLD	165,640		-	New entry

02

03

04

05

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

## Top 20 ccTLDs used in new domains

Rank	New domain TLD	Q3 2023	Q3 data bar	Q2 2023	% Change
1	.de	298,994		365,417	▼ -18%
2	.ru	254,569		234,458	▲ 9%
3	.co	245,100		197,432	▲ 24%
4	.com.br	221,302		215,607	▲ 3%
5	.cn	213,681		214,026	▶ 0%
6	.co.uk	182,146		274,420	▼ -34%
7	.nl	179,446		202,605	▼ -11%
8	.in	174,811		180,128	▼ -3%
9	.fr	154,786		166,363	▼ -7%
10	.ca	125,563		137,857	▼ -9%
11	.cc	125,353		126,963	▼ -1%
12	.us	109,012		108,134	▲ 1%
13	.com.au	106,788		111,490	▼ -4%
14	.pl	89,054		129,308	▼ -31%
15	.eu	77,503		102,572	▼ -24%
16	.es	74,656		-	New entry
17	.it	70,439		84,234	▼ -16%
18	.com.tr	64,721		-	New entry
19	.me	58,745		73,691	▼ -20%
20	.ch	58,577		-	New entry

01

●●● Top20 gTLD - new ✕ Top20 gTLDs - zone ✕

## Top 20 gTLDs used in new domains

Rank	New domain TLD	Q3 2023	Q3 data bar	Q2 2023	% Change
1	.com	6,086,487		6,200,946	▼ -2%
2	.top	704,799		473,333	▲ 49%
3	.online	675,305		476,268	▲ 42%
4	.cfd	511,191		333,226	▲ 53%
5	.xyz	456,072		546,683	▼ -17%
6	.shop	375,146		344,624	▲ 9%
7	.net	372,563		363,344	▲ 3%
8	.org	335,045		347,912	▼ -4%
9	.site	300,768		297,222	▲ 1%
10	.store	266,969		261,710	▲ 2%
11	.click	168,206		127,430	▲ 32%
12	.bond	165,640		59,587	▲ 178%
13	.info	161,596		187,752	▼ -14%
14	.icu	157,596		-	▼ -9%
15	.vip	105,388		93,259	▲ 13%
16	.sbs	86,668		69,350	▲ 25%
17	.live	70,952		75,317	▼ -6%
18	.fun	68,246		79,352	▼ -14%
19	.pro	64,030		-	New entry
20	.space	58,743		66,558	▼ -12%

02

03

04

05

●●● Top20 gTLD - new ✕ Top20 gTLDs - zone ✕

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

Rank	New domain TLD	Q3 2023	Zone size	% of zone newly observed	% of zone data bar
1	.bond	165,640	170,457	97.17%	
2	.lat	49,848	73,045	68.24%	
3	.cfd	511,191	922,226	55.43%	
4	.icu	157,596	308,412	51.10%	
5	.sbs	86,668	213,523	40.59%	
6	.baby	5,798	14,882	38.96%	
7	.today	47,541	156,489	30.38%	
8	.skin	9,979	32,904	30.33%	
9	.click	168,206	557,237	30.19%	
10	.yachts	2,718	10,036	27.08%	
11	.mom	11,579	43,018	26.92%	
12	.autos	10,068	37,920	26.55%	
13	.online	675,305	2,813,910	24.00%	
14	.gay	7,431	30,980	23.99%	
15	.lol	24,538	106,173	23.11%	
16	.bio	15,123	69,325	21.81%	
17	.link	50,291	233,626	21.53%	
18	.site	300,768	1,399,733	21.49%	
19	.store	266,969	1,259,345	21.20%	
20	.best	12,777	62,650	20.39%	



01

●●● Trending terms... ✕

### Trending terms in new domains

Domain registrations mirror the 'offline world'. Given the changing way much of the world views energy consumption and fossil fuel usage, it is not surprising to see domains referring to electric cars gained popularity in Q3, hence the entry of "electric" at #20.

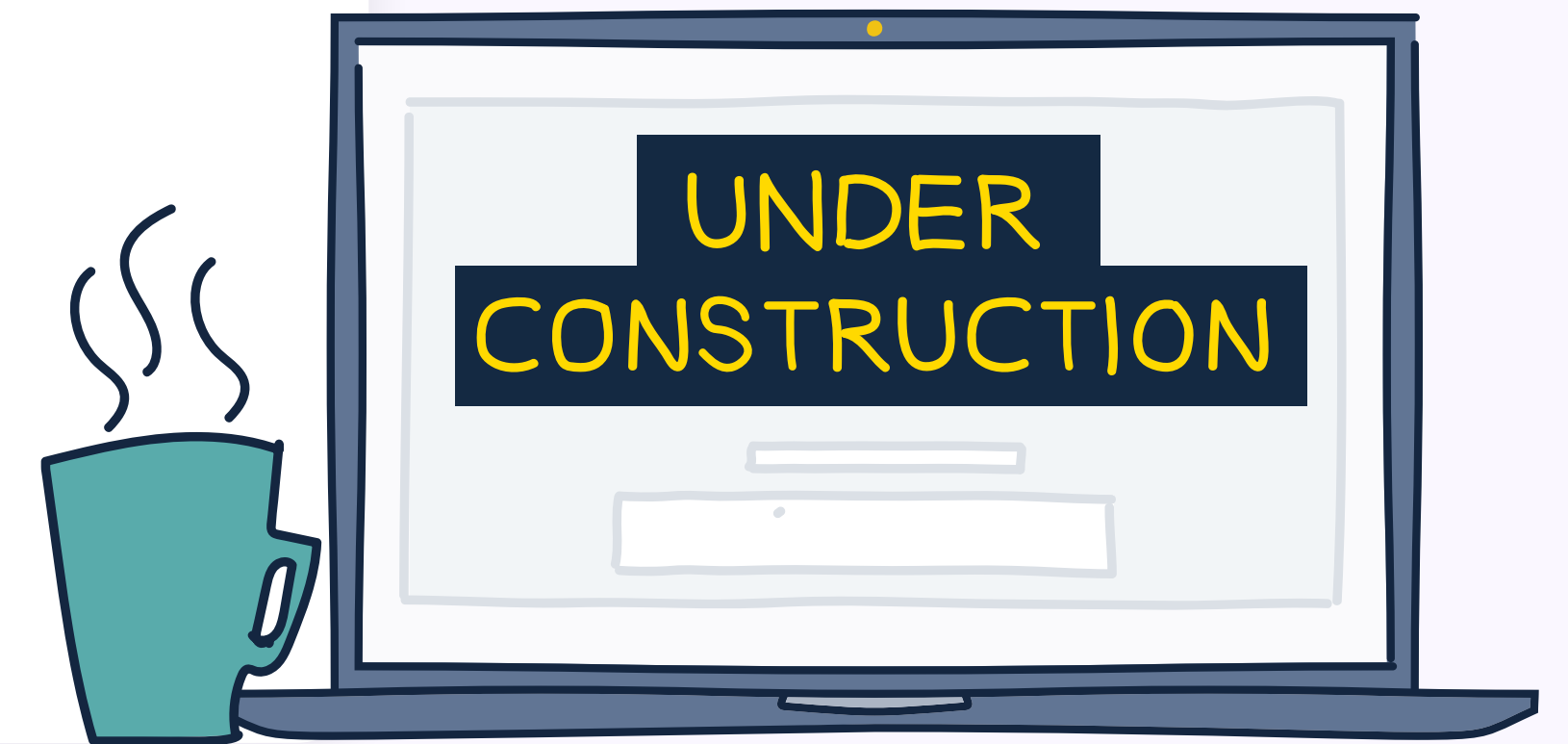
Sometimes the link is a little more opaque, but nevertheless interesting. As interest rates continue to rise in many countries, it gets more and more expensive (and challenging) to close a new mortgage. The effect being that less people can afford new homes, and as such opt to improve or restore their current homes. No doubt also with an eye on energy usage. This is reflected in the trending terms in new domains, such as the rise of "insulation (4,711), "restoration" (3,119), "renovation" (1,983).

When it comes to "ation", ranked #2 in trending terms, here's a breakdown of the top words containing this term in Q3:

- foundation **13,248**
- international **9,811**
- creations **8,549**
- education **6,360**
- installation **4,711**
- nation **4,368**
- national **3,779**
- automation **3,767**
- station **3,701**
- innovation **3,282**
- association **3,246**
- creation **3,185**
- restoration **3,119**
- innovations **2,955**
- vacation **2,670**

#### **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.



05

01

### Top 20 trending terms in new domains

Rank	Q3 2023 trending terms	Q3 2023	Q3 data bar	Q2 2023	% Change
1	service	103,005	<div style="width: 100%;"></div>	99,797	▲ 3%
2	online	82,614	<div style="width: 90%;"></div>	69,608	▲ 19%
3	ation	75,010	<div style="width: 85%;"></div>	73,239	▲ 2%
4	market	71,516	<div style="width: 80%;"></div>	64,560	▲ 11%
5	solution	69,100	<div style="width: 75%;"></div>	66,423	▲ 4%
6	design	65,702	<div style="width: 70%;"></div>	65,608	▶ 0%
7	digital	64,600	<div style="width: 65%;"></div>	54,265	▲ 19%
8	store	58,158	<div style="width: 60%;"></div>	56,363	▲ 3%
9	studio	58,077	<div style="width: 55%;"></div>	58,770	▼ -1%
10	group	55,274	<div style="width: 50%;"></div>	56,117	▼ -2%
11	consult	53,151	<div style="width: 45%;"></div>	51,953	▲ 2%
12	health	51,394	<div style="width: 40%;"></div>	53,646	▼ -4%
13	product	46,166	<div style="width: 35%;"></div>	31,887	▲ 45%
14	marketing	42,011	<div style="width: 30%;"></div>	-	New entry
15	global	34,528	<div style="width: 25%;"></div>	33,263	▲ 4%
16	travel	34,268	<div style="width: 20%;"></div>	32,727	▲ 5%
17	creative	32,177	<div style="width: 15%;"></div>	-	New entry
18	invest	19,082	<div style="width: 10%;"></div>	31,142	▼ -39%
19	cleaning	17,408	<div style="width: 5%;"></div>	-	New entry
20	electric	11,864	<div style="width: 2%;"></div>	-	New entry

02

03

04

05

### Trending terms



01

● ● ● Domains detected ✕ Detections per m... ✕

# Domains detected

## Domain Overview

In Q3, just under 555K domains were detected, with an average of 185K per month – a decrease of -23%. As we have mentioned in past reports – even bad actors take holidays.

Despite .cn experiencing a -10% reduction in Q3, in the number of domains associated with detections, there is still an astonishing number of bad .cn domains in use. A large portion of these are connected to phishing campaigns aimed at the Japanese market, targeting well-known Japanese brands. As the main operator responsible for these campaigns has been able to operate unhindered for years, our threat hunters don't expect to see change any time soon.

Another TLD of note - technically a ccTLD but in practice operated like a gTLD - is .me (+21% quarter on quarter). The key driver in abuse of this TLD is that many 4-letter .me domains are operated as though they are legitimate URL shorteners. In reality, these domains are fully controlled by cybercriminals using them for nothing but SMS-based phishing campaigns - mostly aimed at various European mobile operators. See the [phishing section](#) for more information.

Most of the other TLDs strongly associated with abusive registrations are in the lower price tiers, which we consider to be anything under US \$5 per domain. We beat this drum with great regularity, but the message still holds true: **low pricing attracts abusive and fraudulent registrations.**

02

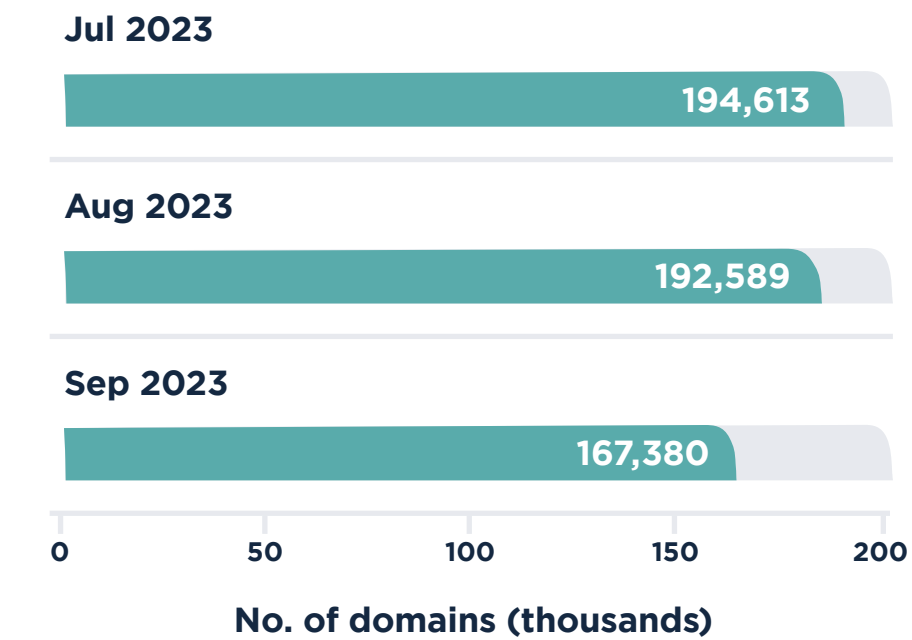
03

04

05

● ● ● Domain detected ✕ Detections per m... ✕

## Number of Domain detections per month



Quarterly Total

554,582

▼ -23% ▼

Monthly Average

184,861

▼ -54,392 ▼

### **i** What triggers a domain to be detected 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

Trending terms... x

### TLDs detected in our domain data

Dealing with abuse on the internet is sometimes akin to watching a zombie movie: the abuse never seems to die! Similarly, and disappointingly, we have four of the five Freenom TLDs back in the ccTLD Top 15 (.tk, .gq, .cf and .ml). Freenom isn't accepting new registrations for these TLDs, but they still manage previously registered domains.

One tier above free is cheap. Cheap gTLDs continue to enable various forms of abuse. The actual number of abuse-enabling and fraudulent domains is greater than our stats depict, which are based around strict criteria for measuring reputation. For example, we don't include the likes of black-hat SEO spam, which is prevalent, but outside our detection policies.

Abused domain names are not isolated to gTLDs, some ccTLDs also have their fair share of fraudulent registrations too, just look at Freenom!

Where registrars operate outside the region that owns the ccTLD, the trend appears to be that while relaxing registration rules may grow the number of domains in the zone; it also attracts bad registrations from outside the region and continent. The greater the distance between owner and operator, the greater the abuse.

### i Interpreting the data x

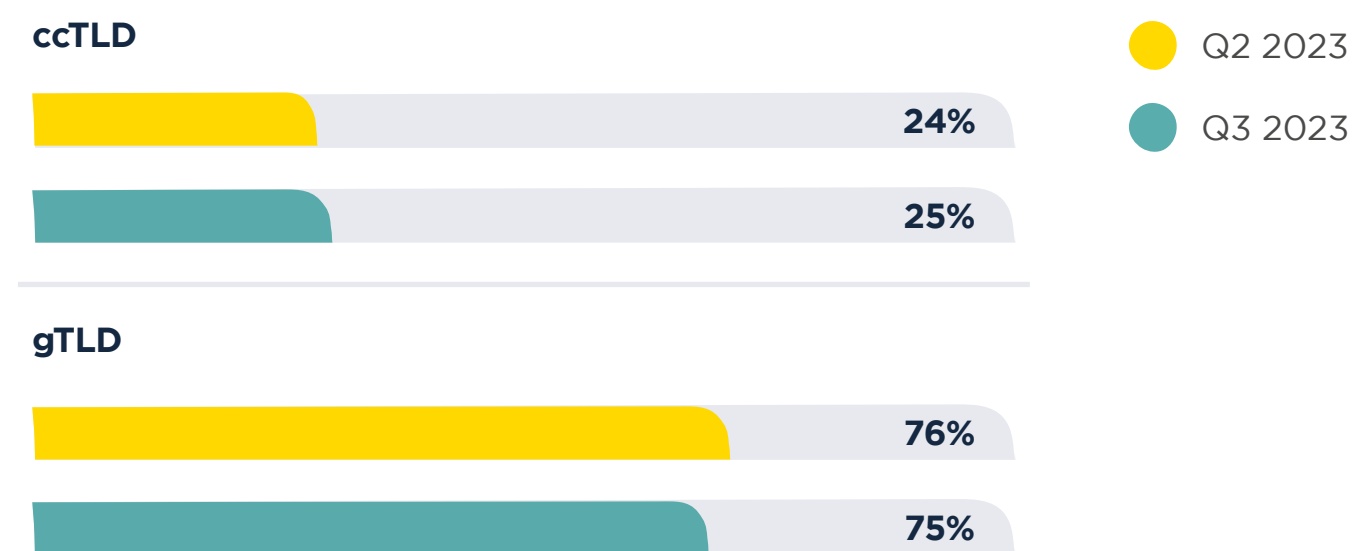
Registries with a greater number of active domains have greater exposure to abuse. For example, in Q3 2023 .cfd had more than 922,000 domains in its zone, of which 1.06% were detected.

Meanwhile, .support had just over 36,000 domains in its zone, with 3.58% listed in our domain dataset. Both are in the Top 20 of our detections. Still, one had a much higher percentage of active domains detected than the other.

03

Domain detecti... x

### Domain detection TLD type comparison



05

01

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

### Top 20 TLDs detected

Rank	Domain TLD	Type of TLD	Q3 2023	Q2 data bar	Q2 2023	% Change
1	.com	gTLD	200,336		268,562	▼ -25%
2	.cn	ccTLD	43,972		48,913	▼ -10%
3	.live	gTLD	30,493		28,293	▲ 8%
4	.top	gTLD	26,748		39,167	▼ -32%
5	.info	gTLD	18,535		25,588	▼ -28%
6	.net	gTLD	16,077		17,688	▼ -9%
7	.tk	ccTLD	15,035		11,872	▲ 27%
8	.xyz	gTLD	12,341		16,421	▼ -25%
9	.site	gTLD	11,888		9,238	▲ 29%
10	.me	ccTLD	10,778		8,935	▲ 21%
11	.online	gTLD	10,353		10,922	▼ -5%
12	.cfd	gTLD	9,816		11,108	▼ -12%
13	.us	ccTLD	8,432		10,317	▼ -18%
14	.gq	ccTLD	8,019		6,770	▲ 18%
15	.co	ccTLD	7,519		-	New entry
16	.ru	ccTLD	6,487		8,039	▼ -19%
17	.cf	ccTLD	6,067		-	New entry
18	.in	ccTLD	5,792		7,273	▼ -20%
19	.uk	ccTLD	5,122		6,774	▼ -24%
20	.org	gTLD	4,877		7,960	▼ -39%

02

03

04

05

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

### Top 20 ccTLDs in domain detections

Rank	Domain TLD	Q3 2023	Q3 data bar	Q2 2023	% Change
1	.cn	43,972		48,913	▼ -10%
2	.tk	15,035		11,872	▲ 27%
3	.me	10,778		8,935	▲ 21%
4	.us	8,432		10,317	▼ -18%
5	.gq	8,019		6,770	▲ 18%
6	.co	7,519		5,954	▲ 26%
7	.ru	6,487		8,039	▼ -19%
8	.cf	6,067		5,957	▲ 2%
9	.in	5,792		7,273	▼ -20%
10	.uk	5,122		6,774	▼ -24%
11	.cc	4,095		5,379	▼ -24%
12	.ml	1,789		7,801	▼ -77%
13	.de	1,468		4,390	▼ -67%
14	.eu	1,308		1,869	▼ -30%
15	.jp	1,246		-	New entry
16	.fr	1,193		2,072	▼ -42%
17	.ng	989		-	New entry
18	.br	971		1,418	▼ -32%
19	.pw	928		6,370	▼ -85%
20	.pl	857		1,615	▼ -47%

01

### Top 20 gTLD in domain detections

Rank	Domain TLD	Q3 2023	Q3 data bar	Q2 2023	% Change
1	.com	200,336		268,562	▼ -25%
2	.live	30,493		28,293	▲ 8%
3	.top	26,748		39,167	▼ -32%
4	.info	18,535		25,588	▼ -28%
5	.net	16,077		17,688	▼ -9%
6	.xyz	12,341		16,421	▼ -25%
7	.site	11,888		9,238	▲ 29%
8	.online	10,353		10,922	▼ -5%
9	.cf	9,816		11,108	▼ -12%
10	.org	4,877		7,960	▼ -39%
11	.fun	4,610		-	New entry
12	.life	3,252		3,651	▼ -11%
13	.shop	3,235		5,296	▼ -39%
14	.fyi	3,035		-	New entry
15	.sbs	2,994		4,435	▼ -32%
16	.icu	2,948		-	New entry
17	.vip	2,600		6,184	▼ -58%
18	.click	2,587		5,429	▼ -52%
19	.lat	2,580		-	New entry
20	.space	2,465		2,992	▼ -18%

02

03

04

05

### Top 20 gTLDs by % of zone file with domain detections

Rank	Domain TLD	Q3 2023	Zone size	% of zone listed	% of zone data bar
1	.live	30,493	629,487	4.84%	
2	.fyi	3,035	62,847	4.83%	
3	.support	1,302	36,411	3.58%	
4	.lat	2,580	73,045	3.53%	
5	.zone	1,497	44,671	3.35%	
6	.beauty	989	36,768	2.69%	
7	.bio	1,774	69,325	2.56%	
8	.quest	798	39,403	2.03%	
9	.makeup	253	13,110	1.93%	
10	.sbs	2,994	213,523	1.40%	
11	.fun	4,610	361,117	1.28%	
12	.market	300	23,711	1.27%	
13	.cam	396	33,790	1.17%	
14	.cf	9,816	922,226	1.06%	
15	.uno	202	19,206	1.05%	
16	.today	1,594	156,489	1.02%	
17	.ink	786	81,019	0.97%	
18	.rest	302	31,236	0.97%	
19	.icu	2,948	308,412	0.96%	
20	.best	567	62,650	0.91%	

01

02

03

04

05

### Trending phishing terms in domain detections

Domains specifically registered for conducting phishing attacks can roughly be divided into two groups.

**Group 1:** These contain predominantly short domains that are often just four or five randomly selected characters.

**Group 2:** These contain some context (security, account, device), a brand or product name (apple, netflix, paypal) and a call to action (manage, update, verify), as the Top 20 phishing terms clearly illustrates.

One of the use cases for Group 1's domain formatting style, is in text/SMS messaging, where the limit of 160 characters favors shorter domain names. This is where established redirectors are utilized, and since even many legitimate brands and their messages use these, receivers are well-conditioned to find short, semi-cryptic URLs in their texts.

The use of lookalike domains as outlined in "Group 2", has been around forever. Therefore, we continue to be puzzled by the fact that many of these blatantly malicious domains pass the registration process without any form of scrutiny. Surely, parsing the requested domain and running it through a list of trending phishing terms (similar to the ones in our chart), could immediately highlight potentially fraudulent registrations? In turn these highlighted registrations could move on to another level of assessment.

We understand this would incur additional cost, which is probably not warranted by the low-margin business model of many registrars. BUT, in our opinion, this additional cost isn't one that the rest of the internet should bear because of bad actors being able to operate.

#### What terms do bad actors use for domain names? x

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

### Top 20 phishing terms in domain listings

Rank	Term	Q3 2023	Q3 data bar	Q2 2023	% Change
1	account	6,036		5,499	▲ 10%
2	apple	4,683		3,527	▲ 33%
3	support	4,462		4,393	▲ 2%
4	online	4,382		4,623	▼ -5%
5	service	4,351		3,879	▲ 12%
6	security	3,854		3,209	▲ 20%
7	icloud	3,511		3,077	▲ 14%
8	verification	3,425		1,761	▲ 94%
9	intl	3,326		3,630	▼ -8%
10	cloud	3,089		2,641	▲ 17%
11	secure	2,596		2,175	▲ 19%
12	jobs	2,343		1,723	▲ 36%
13	payment	2,229		1,999	▲ 12%
14	findmy	1,282		1,171	▲ 9%
15	manage	1,279		-	New entry
16	lcloud	1,274		-	New entry
17	verify	1,268		-	New entry
18	saving	1,255		1,117	▲ 12%
19	login	1,245		-	New entry
20	device	1,214		-	New entry

02

03

04

05

### Phishing terms





01

02

03

04

05

●●● Types of detections ✕

## Types of detections

In Q2's report we discussed the use of old, aged domain names with residual reputation being used for malspam campaigns. There are two ways of acquiring these kinds of domains:

1. Getting access to compromised websites running on these domains (we label these "compromised").
2. Purchasing existing old domains through the 'aftermarket' (we label these "malicious").

The former was utilized by Qakbot. As a result of this malware's takedown, the numbers of compromised legitimate websites observed by our threat hunting team, reduced a huge -89% from 11,003 in Q2, to 1,220 in Q3. However, as always, bad actors are trying to fill the gap left by Qakbot's take down.

The latter way of getting hold of domains with existing reputation, is one of the greatest threats commonly seen in the domain space. These aged domains provide an exceptionally easy way of actors presenting a fully "authentic" identity (including established web presence). The miscreants using them behave the polar opposite to bulk spammers, that acquire large batches of cheap domains. This makes detection on the defense and registrar side much harder. Our threat hunters are keeping a close eye on this.

### 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 detection of the domain. Within Spamhaus these types of detections are referred to as "abused-legit".

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

### Types of detections

#### Bad reputation



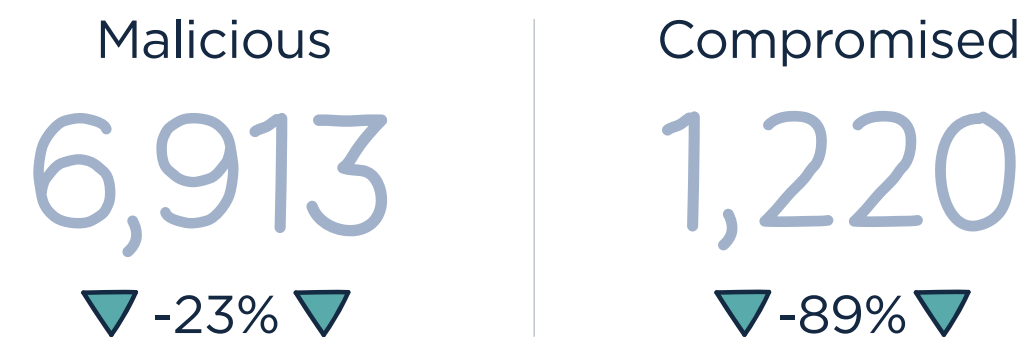
A domain's reputation score has exceeded policy limits.

#### Botnet C&C



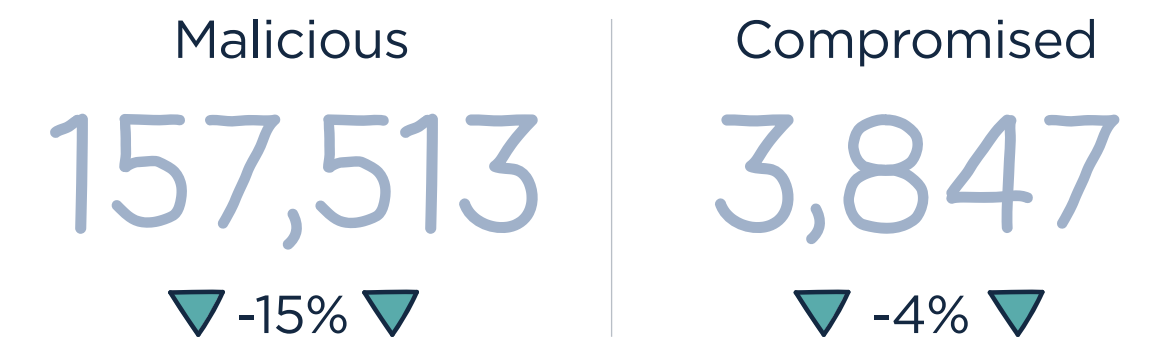
A domain is registered for use for a botnet command and controller (C&C).  
(A subset of bad reputation.)

#### Malware



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

#### Phishing



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

01

02

03

04

05

01

02

03

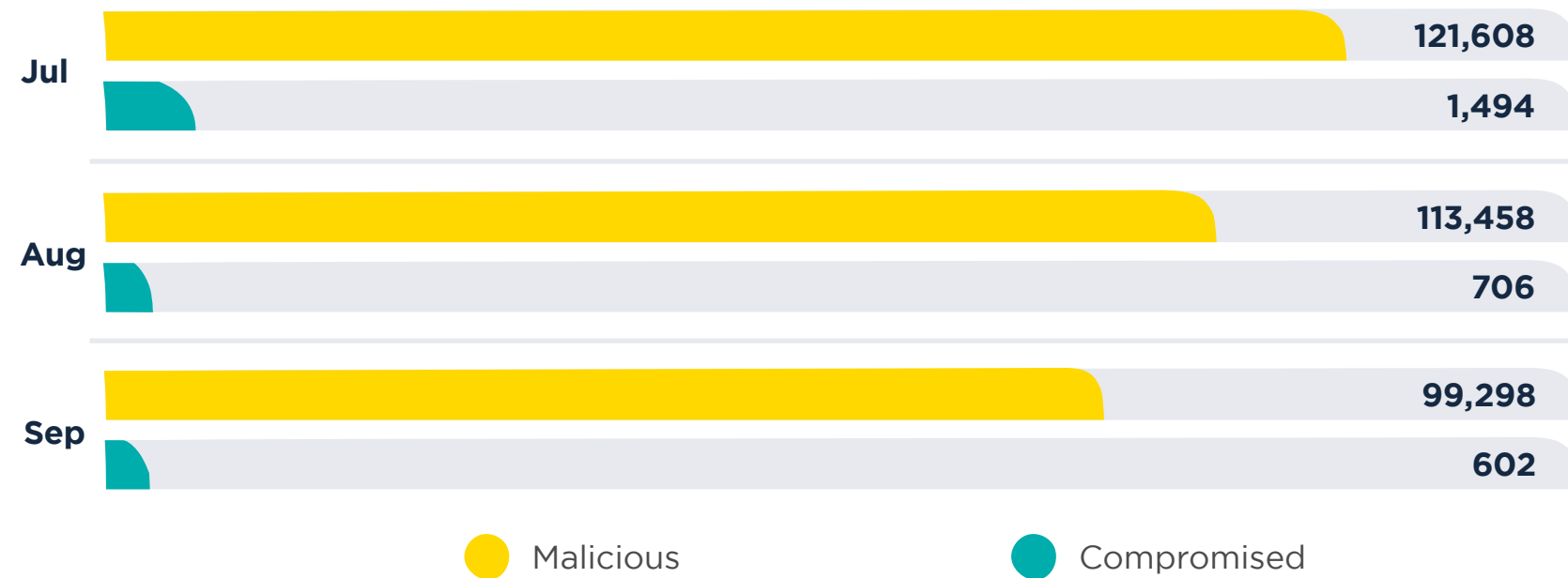
04

05

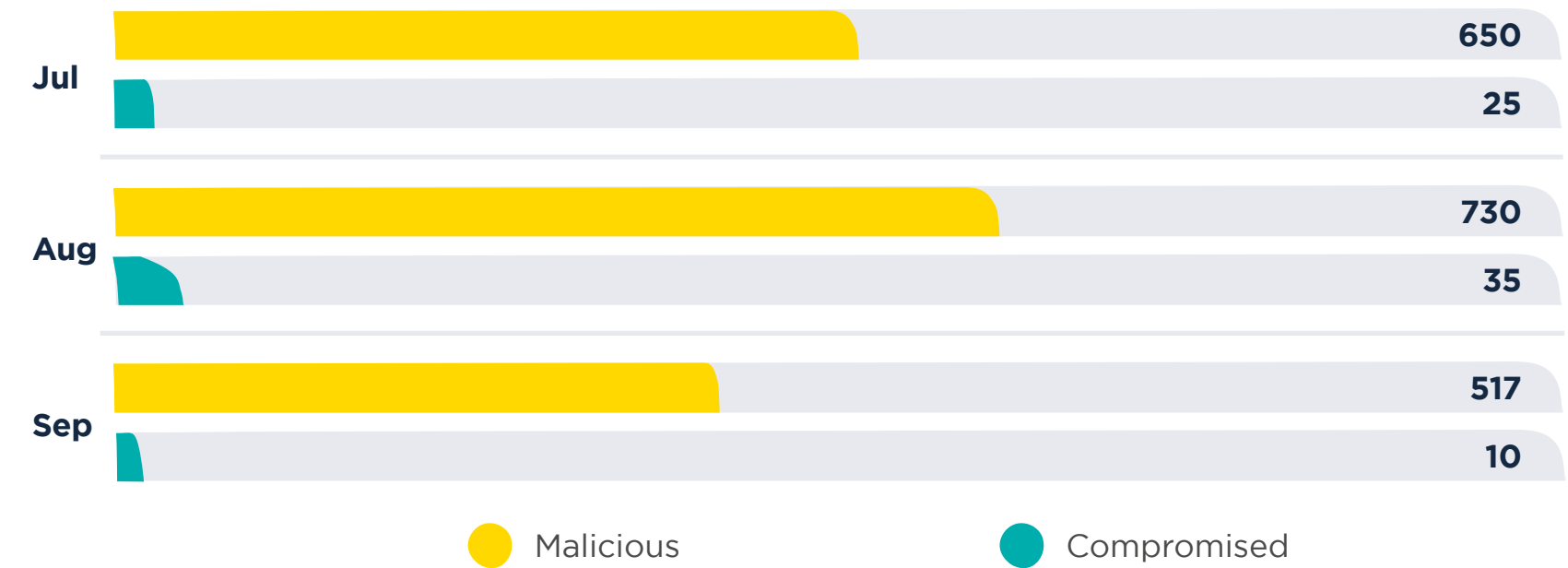
Types of abuse ✕

### Types of abuse

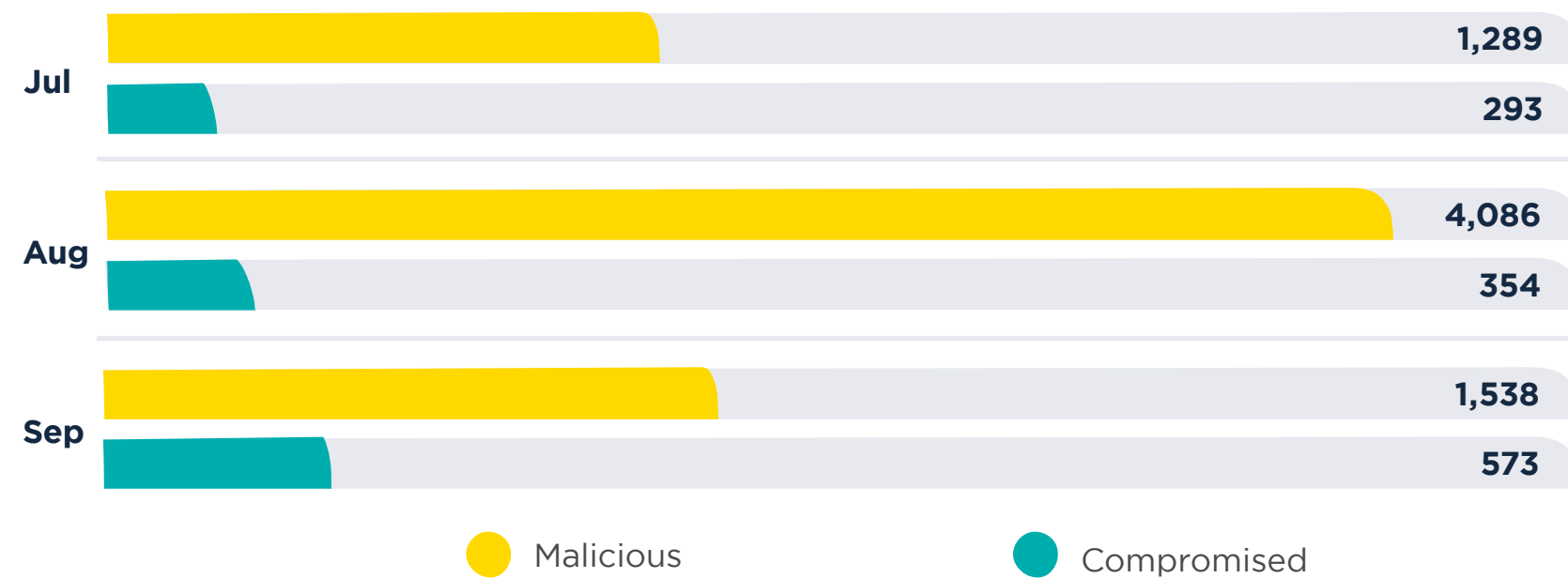
#### Bad reputation per month



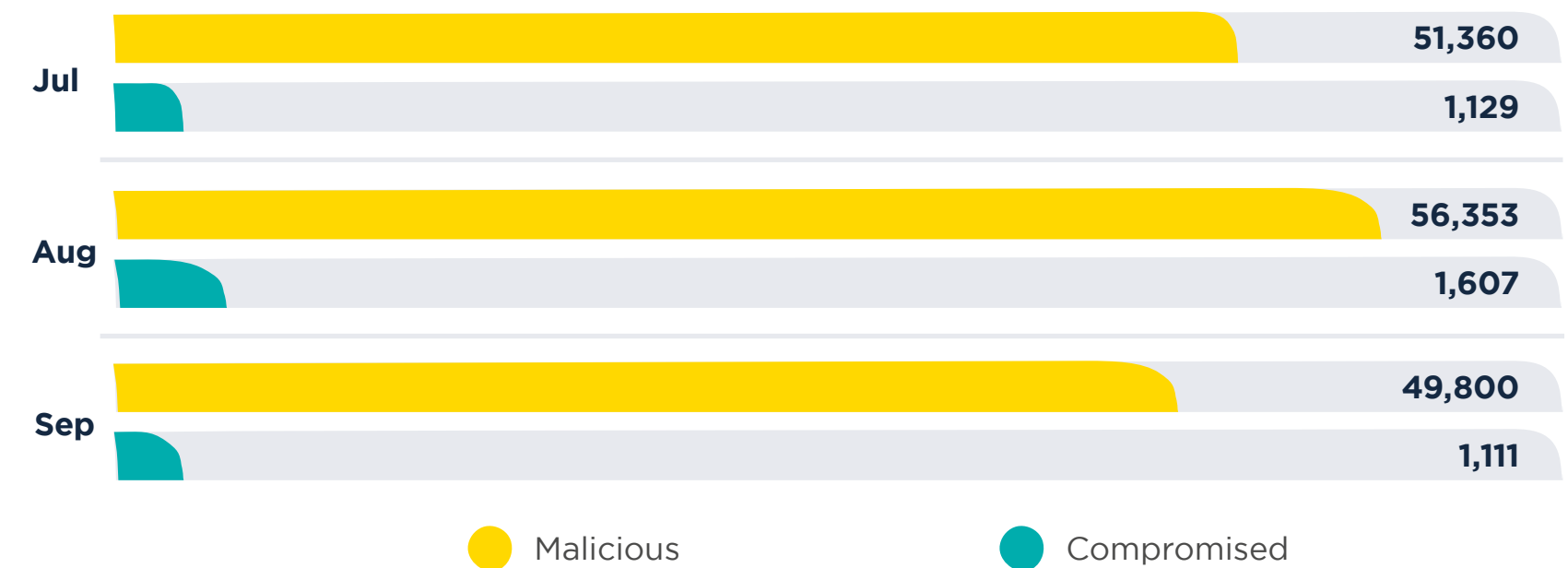
#### Botnet C&C per month



#### Malware per month



#### Phishing per month



# Recommendations of the quarter

## Low priced domains attract bad actors

It will come as no surprise to regular readers of this report, that the vast majority of newly registered bad domains exist among the lower priced tiers. While the effective application of domain reputation, on the defensive side, renders these domains useless and forces miscreants to deploy new ones, low domain price points further enable this business model.

## Check your domain authentication

[With the recently announced requirement of sending authenticated mail by the largest email platform in the world](#), the need for appropriately managing domain names by miscreants is also increasing. This is a positive thing – anything that makes additional work for bad actors has to be applauded. BUT, to make sure that you, as a legitimate mailer, are not put on the same pile as the non-legitimate ones, you must ensure your domain authentication is setup correctly. Our support team sees misconfigured setups on a daily basis, often from organizations that could and should know better.

## Remember that domain reputation is not black and white

In days of old, Spamhaus datasets were only used to make decisions on how to interact with emails. These DNS Blocklists (DNSBLs) provided a user with a very clear “yes the domain’s good” or “no it’s bad”. Nowadays, the data stretches way beyond this, and nuanced reputation is applied to every domain our researchers observe. This means that while a domain may not be listed on a DNSBL, if its reputation is a shade of grey, this data is available to users. This can influence registrar and hosting reputation.

## Get social

As a final recommendation for this quarter, keep an eye on our blog and social media to stay in touch with everything we observe. See you next quarter!

01

02

03

04

05

## Additional info

### About Spamhaus ✕

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

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

### Report Methodology ✕

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

01

02

03

04

05