SPAMHAUS

Spamhaus Domain Reputation Update

April – September 2025

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.

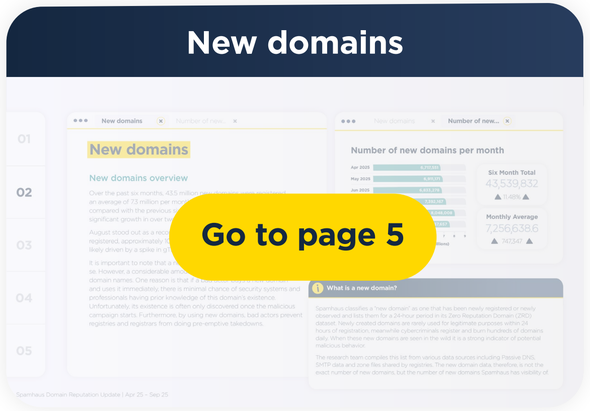
Welcome to the Spamhaus Domain Reputation Update April - September 2025.

Enter

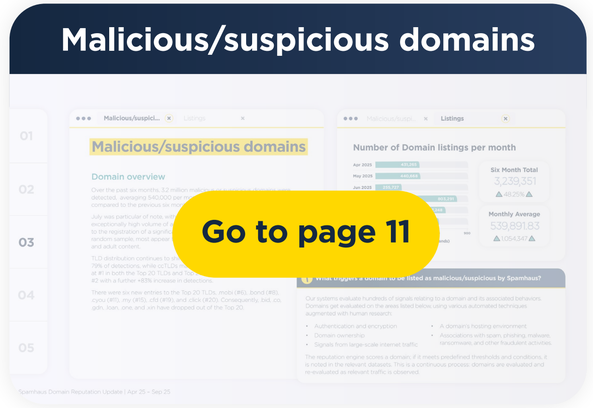
Contents

The Spotlight

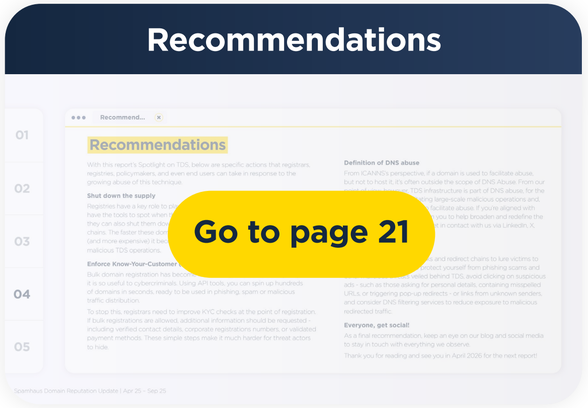
New domains



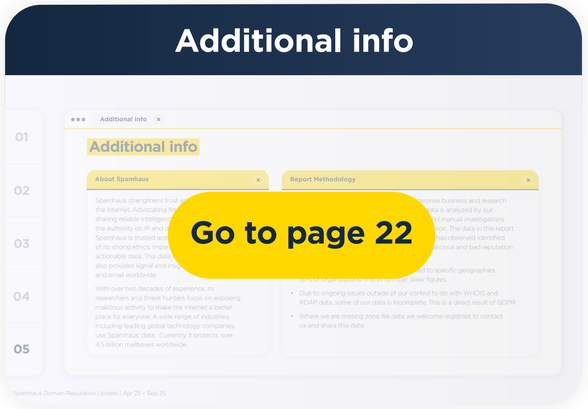
Malicious/suspicious domains



Recommendations



Additional info



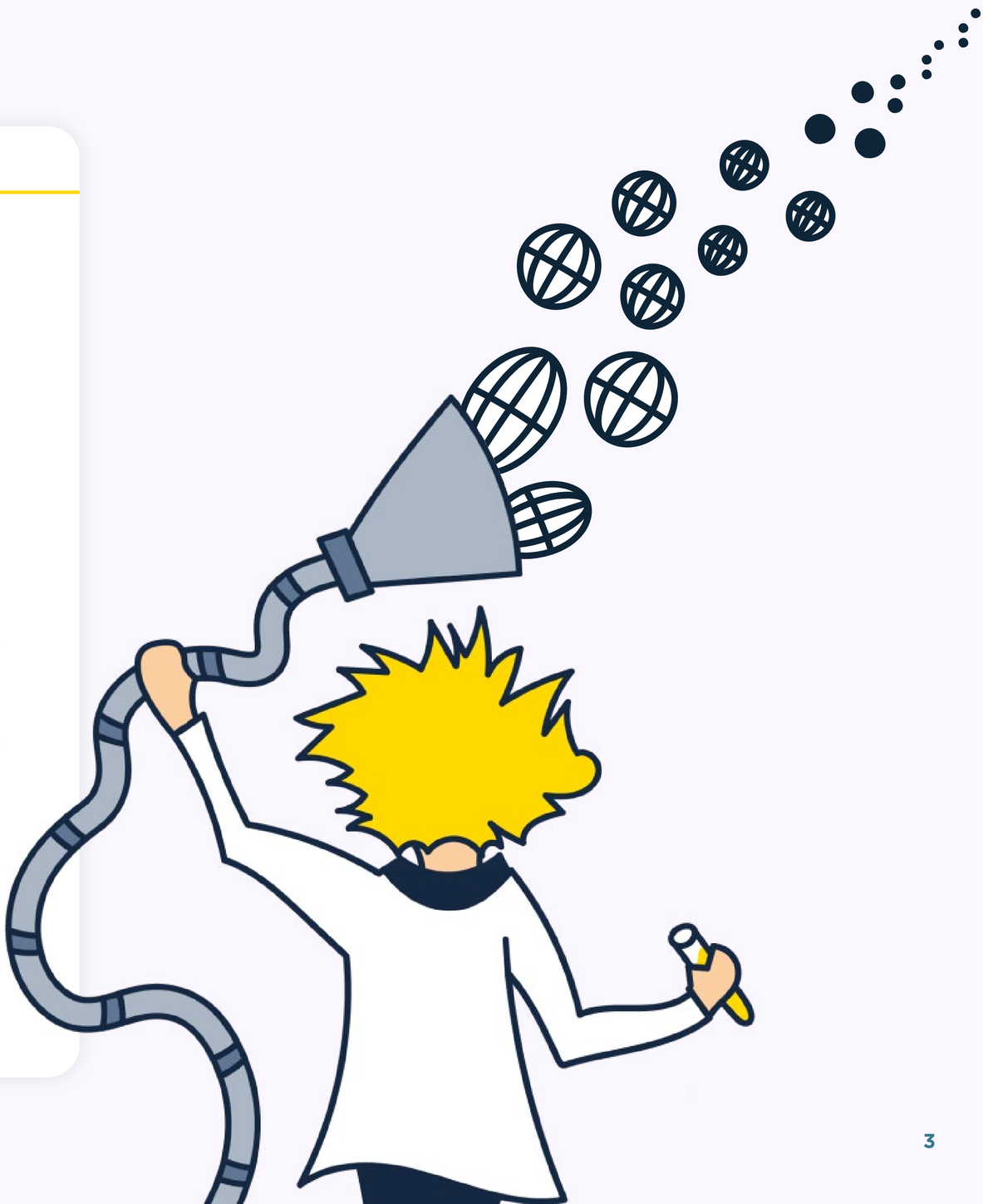
The Spotlight

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 infrastructure for malicious purposes - particularly in phishing campaigns - is becoming increasingly common. But what exactly are TDS?

A TDS is a network that **redirects** or **filters web traffic**; typical use includes advertising and affiliate tracking or geolocation targeting. TDS essentially act as intermediaries, often sitting between the link you click—say, in an email—and the page or service you ultimately reach. There *are* legitimate use cases for a TDS, but the advantages they offer are useful for cybercriminals too. Spamhaus has observed an increase in their use, enabling large-scale phishing, 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 are met.

Spotlight continued



Spotlight cont.

It's also important to note that, as the technology itself has legitimate applications, they aren't *technically* abuse, even when exploited for malicious purposes. This makes TDS abuse a bit of a grey area. When it comes to takedowns, it poses a unique challenge because registrars may not necessarily view them as abuse. They might contact the domain owner to remove the malicious link, but they wouldn't necessarily consider the entire domain as malicious. Unfortunately, this would be compliant with ICANN's definition of abuse.

In June 2025, core network services provider, Infoblox, shared 100,000 domain names with Spamhaus, identified as belonging to the notorious Vextrio. Researchers have found these domains to be spread across the globe, with many using top-level domains (TLDs) .life, .com, .club, and .top - many of which you will see in this report. The good news? To provide user protection, we've added these domains to the Spamhaus Domain Blocklist and are now actively tracking TDS activity!

As a community, we need to raise awareness among registrars and the wider industry that: this is a growing problem that is actively enabling malicious behaviour. You can help by sharing suspicious or malicious domains and urls with us via the Spamhaus Threat Intel Community Portal.

New domains | Number of new...

New domains

New domains overview

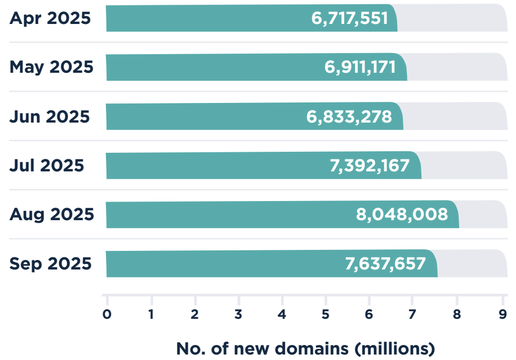
Over the past six months, 43.5 million new domains were registered, an average of 7.3 million per month. This marks an +11.48% increase compared with the previous six months, representing the most significant growth in over two years.

August stood out as a record month, with over 8 million new domains registered, approximately 10% greater than the monthly average, and likely driven by a spike in gTLD activity.

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

New domains | Number of new...

Number of new domains per month



Six Month Total
43,539,832
▲ 11.48% ▲

Monthly Average
7,256,639
▲ 747,347 ▲

What is a new domain?

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

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

New domains... TLD types...

New domains by top-level domain (TLD)

Over the last six months, the distribution of new TLD registrations shifted towards gTLDs, which now account for 75% and ccTLDs for 25%. Overall, among the Top 20 TLDs, only .de recorded a decrease (-34%) in new domains, dropping down to #2 for ccTLDs.

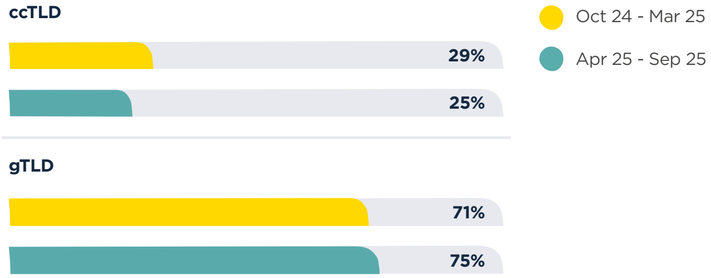
There were two new entries in the Top 20 ccTLDs this period, .my (Malaysia), and .es (Spain). After a brief appearance, .my.id (Indonesia) dropped out of the Top 20 ccTLDs used in new domains. Meanwhile, .ai (Anguilla) continues an upward trend with a +39% increase, climbing four positions to #12.

Among gTLDs used in new domain registrations, .top (#2) and .xyz (#3) maintain momentum, ranking in the top three with +94% and +103% increases, respectively. Shortdot SA registered, .sbs, re-entered the Top 20 TLDs with a +95% increase, also securing its position at #11 in the Top 20 gTLDs. In contrast another Shortdot SA gTLD, .bond saw new registrations drop by -78%.

Nevertheless, .bond remains the #1 gTLD for percentage of newly observed zones against total zone size; new domain registrations exceed its total zone count by 187%, a highly abnormal pattern. Over the past 6 months, 238,000 new domains were registered, yet only 127,000 remain active in the zone file. This indicates that the unusual trend of large-scale suspensions is continuing.

New domains... TLD types...

New domain TLD types - six month comparison



Top-level domains – a quick explanation

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

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

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

Top 20 TLDs used in new domains

Rank	New domain TLD	TLD type	Apr 25 - Sep 25	Apr 25 - Sep 25 data bar	Oct 24 - Mar 25	% Change
1	.com	gTLD	13,317,985		12,010,547	▲ 11%
2	.top	gTLD	2,793,617		1,443,265	▲ 94%
3	.xyz	gTLD	2,568,825		1,267,627	▲ 103%
4	.shop	gTLD	1,479,708		1,264,489	▲ 17%
5	.online	gTLD	1,044,785		953,490	▲ 10%
6	.cn	ccTLD	1,042,402		1,033,556	▲ 1%
7	.org	gTLD	958,255		845,989	▲ 13%
8	.info	gTLD	906,640		674,892	▲ 34%
9	.de	ccTLD	861,901		1,303,249	▼ -34%
10	.store	gTLD	761,187		713,080	▲ 7%
11	.net	gTLD	720,128		699,451	▲ 3%
12	.cc	ccTLD	678,006		564,865	▲ 20%
13	.site	gTLD	631,962		618,246	▲ 2%
14	.sbs	gTLD	600,420		-	New entry
15	.ru	ccTLD	590,687		565,741	▲ 4%
16	.com.br	ccTLD	580,617		563,556	▲ 3%
17	.vip	gTLD	467,086		394,526	▲ 18%
18	.co.uk	ccTLD	462,636		425,014	▲ 9%
19	.co	ccTLD	419,534		-	New entry
20	.pro	gTLD	336,561		-	New entry

0 2 4 6 8 10 12 14

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

Top 20 ccTLDs used in new domains

Rank	New domain TLD	Apr 25 - Sep 25	Apr 25 - Sep 25 data bar	Oct 24 - Mar 25	% Change
1	.cn	1,042,402		1,033,556	▲ 1%
2	.de	861,901		1,303,249	▼ -34%
3	.cc	678,006		564,865	▲ 20%
4	.ru	590,687		565,741	▲ 4%
5	.com.br	580,617		563,556	▲ 3%
6	.co.uk	462,636		425,014	▲ 9%
7	.co	419,534		387,260	▲ 8%
8	.in	320,552		336,862	▼ -5%
9	.nl	317,392		393,961	▼ -19%
10	.my	304,812		-	New entry
11	.fr	304,669		333,700	▼ -9%
12	.ai	249,217		179,369	▲ 39%
13	.ca	235,901		225,562	▲ 5%
14	.eu	231,682		206,872	▲ 12%
15	.com.au	207,923		199,254	▲ 4%
16	.it	188,980		193,481	▼ -2%
17	.us	170,593		457,503	▼ -63%
18	.pl	161,109		175,096	▼ -8%
19	.me	160,983		171,129	▼ -6%
20	.es	152,523		-	New entry

0 0.5 1 1.5

Top20 gTLD - new | Top20 gTLDs - zone

Top 20 gTLDs used in new domains

Rank	New domain TLD	Apr 25 - Sep 25	Apr 25 - Sep 25 data bar	Oct 24 - Mar 25	% Change
1	.com	13,317,985		12,010,547	▲ 11%
2	.top	2,793,617		1,443,265	▲ 94%
3	.xyz	2,568,825		1,267,627	▲ 103%
4	.shop	1,479,708		1,264,489	▲ 17%
5	.online	1,044,785		953,490	▲ 10%
6	.org	958,255		845,989	▲ 13%
7	.info	906,640		674,892	▲ 34%
8	.store	761,187		713,080	▲ 7%
9	.net	720,128		699,451	▲ 3%
10	.site	631,962		618,246	▲ 2%
11	.sbs	600,420		308,638	▲ 95%
12	.vip	467,086		394,526	▲ 18%
13	.pro	336,561		281,162	▲ 20%
14	.click	279,080		314,134	▼ -11%
15	.cfd	269,177		193,824	▲ 39%
16	.icu	245,402		203,831	▲ 20%
17	.bond	237,903		1,104,249	▼ -78%
18	.app	215,081		-	New entry
19	.autos	214,799		-	New entry
20	.cyou	189,933		-	New entry

0 2 4 6 8 10 12 14

Top20 gTLD - new | Top20 gTLDs - zone

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

Rank	New domain TLD	Apr 25 - Sep 25	Zone size	% of zone newly observed	% of zone data bar
1	.bond	237,903	126,951	187.40%	
2	.autos	214,799	262,427	81.85%	
3	.sbs	600,420	893,649	67.19%	
4	.cfd	269,177	441,655	60.95%	
5	.cyou	189,933	311,885	60.90%	
6	.icu	245,402	476,064	51.55%	
7	.xyz	2,568,825	6,036,585	42.55%	
8	.click	279,080	661,640	42.18%	
9	.shop	1,479,708	3,653,372	40.50%	
10	.site	631,962	1,681,370	37.59%	
11	.store	761,187	2,029,731	37.50%	
12	.vip	467,086	1,413,805	33.04%	
13	.pro	336,561	1,021,264	32.96%	
14	.online	1,044,785	3,179,223	32.86%	
15	.top	2,793,617	10,288,743	27.15%	
16	.info	906,640	4,505,315	20.12%	
17	.app	215,081	1,800,228	11.95%	
18	.com	13,317,985	163,456,232	8.15%	
19	.org	958,255	11,921,687	8.04%	
20	.net	720,128	12,890,943	5.59%	

0 50% 100% 150% 200%

Trending terms...

Trending terms in new domains

This reporting period saw 10 new entries among trending terms in new domain registrations, with six appearing in the top ten: system (#2), engine (#4), search (#6), intern (#8), internet (#9), information (#10).

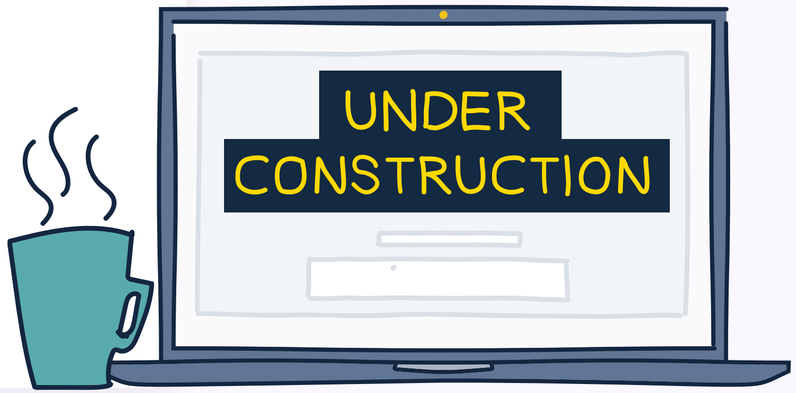
Many of these terms link to user internet behaviour and search activity, a trend likely influenced by the growth of Large Language Models (LLMs). For example, the new domain registration data shows many .xyz domains like “aio-engine-search-llmo-aeo.xyz” combining multiple terms from AI to SEO to LLM. This may reflect increased activity associated with black hat SEO, the practice of manipulating search rankings using unethical techniques, and therefore indicating adversarial activity on these new domains.

Meanwhile, business-related terms decreased in popularity with “global”, “invest” and “training” dropping out of the Top 20. Even “service”, normally the #1 term, fell two places to #3, with an -18% decrease.

Finally, there was an increase in regional activity involving the terms japan (#18) and fukuoka (#20). While the reasons for these Japan-related terms are not clear to us, we’ll be monitoring whether these domains begin to appear among compromised or malicious detections in future reports.

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.



Top 20 Trending... | Trending terms

Top 20 trending terms in new domains

Rank	Apr 25 - Sep 25 trending terms	Apr 25 - Sep 25	Apr 25 - Sep 25 data bar	Oct 24 - Mar 25	% Change
1	market	282,827		190,582	▲ 48%
2	system	247,038		-	New entry
3	service	242,579		295,934	▼ -18%
4	engine	232,584		-	New entry
5	solution	186,579		179,518	▲ 4%
6	search	179,080		-	New entry
7	studio	171,933		142,592	▲ 21%
8	intern	167,699		-	New entry
9	internet	154,784		-	New entry
10	information	149,622		-	New entry
11	keyword	149,569		-	New entry
12	group	148,320		128,211	▲ 16%
13	casino	146,952		127,523	▲ 15%
14	program	140,503		-	New entry
15	digital	132,304		129,824	▲ 2%
16	online	124,168		236,629	▼ -48%
17	consult	112,657		130,227	▼ -13%
18	japan	106,306		-	New entry
19	health	106,109		134,866	▼ -21%
20	fukuoka	82,835		-	New entry

Top 20 Trending... | Trending terms

Trending terms

Malicious/suspici... | Listings

Malicious/suspicious domains

Domain overview

Over the past six months, 3.2 million malicious or suspicious domains were detected, averaging 540,000 per month. This represents a 48.3% increase compared to the previous six month period (October 2024 to March 2025).

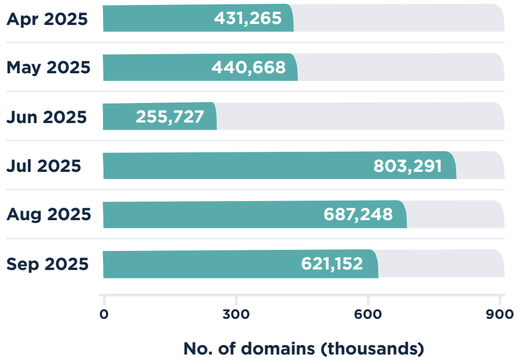
July was of particular note, with 803,291 domains detected, highlighting an exceptionally high volume of activity during this period. This was largely due to the registration of a significant number of abusive domains; based on a random sample, most appear to be targeting China, with a focus on casinos and adult content.

TLD distribution continues to shift towards gTLDs, which accounted for 79% of detections, while ccTLDs made up 21%. .com maintains its position at #1 in both the Top 20 TLDs and Top 20 gTLDs, while .top remains at #2 with a further +83% increase in detections.

There were six new entries to the Top 20 TLDs, .mobi (#6), .bond (#8), .cyou (#11), .my (#15), .cfd (#19), and .click (#20). Consequently, .bid, .co, .gdn, .loan, .one, and .xin have dropped out of the Top 20.

Malicious/suspi... | Listings

Number of Domain listings per month



Six Month Total
3,239,351
▲48.25%▲

Monthly Average
539,892
▲1,054,347▲

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.

Trending terms...

TLDs listed in our domain data

Four new countries entered the ccTLD Top 20 this reporting period: .ee (Estonia, #10), .ro (Romania, #18), .pw (Republic of Palau, #19), and .id (Indonesia, #20). The ccTLD for Malaysia, .my (#3), saw a staggering +543% increase in detections.

This surge in detections is most likely due to a change in policy. In 2024, MYNIC removed its restriction limiting registrations to Malaysian residents and local legal entities, opening up second-level domains like “com.my” to registrants worldwide.

The .my domains are mostly 5-letters followed by digits, with content largely associated with Chinese casinos; similar to .cn domains (which also saw a significant +292% increase).

Meanwhile, this period saw eight new entries in gTLDs listed in our domain data: .mobi (#4), .cyou (#9), .cfd (#15), .click (#16), .live (#17), .life (#18), .blog (#19), .app (#20).

.mobi, a new entry at #4 and .pro at #5 (+294%) are both operated by Afilias, one of the largest internet domain name registries.

Other gTLDs showing the most significant increases include .bond (+316%), .icu (+265%), and .sbs (+131%) which are all managed by Shortdot SA.

As highlighted earlier in this report, Shortdot SA continues to register high volumes of new domains, a pattern often associated with malicious activity. Although still in the very early stages, NetBeacon Institute has issued a proposal for ICANN policy development on DNS abuse that would introduce additional friction for bulk registrations by new customers.

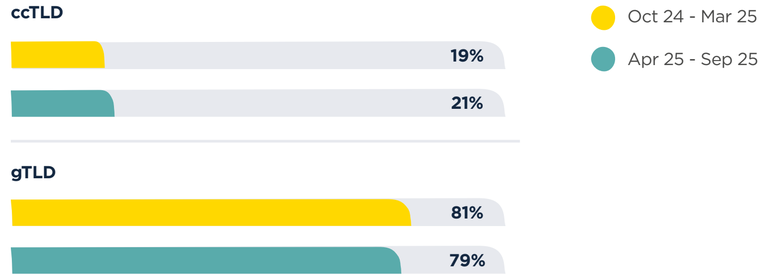
Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, between April and September 2025, .vip had more than 1.4 million domains in its zone, of which 9% were listed.

Meanwhile, .bond had 127,000 domains in its zone, with 54% listed in our domain dataset. Both are in the Top 20 of our listings. Still, one had a much higher percentage of active domains listed than the other.

TLD type - six...

TLD type - six month comparison



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

Top 20 TLDs

Rank	Domain TLD	Type of TLD	Apr 25 - Sep 25	Apr 25 - Sep 25 data bar	Oct 24 - Mar 25	% Change
1	.com	gTLD	813,514		513,292	▲ 58%
2	.top	gTLD	577,797		316,433	▲ 83%
3	.cn	ccTLD	317,707		81,146	▲ 292%
4	.cc	ccTLD	216,942		148,868	▲ 46%
5	.vip	gTLD	126,458		115,032	▲ 10%
6	.mobi	gTLD	120,197		-	New entry
7	.pro	gTLD	79,617		20,190	▲ 294%
8	.bond	gTLD	68,171		-	New entry
9	.icu	gTLD	60,407		16,566	▲ 265%
10	.shop	gTLD	54,565		59,830	▼ -9%
11	.cyou	gTLD	52,009		-	New entry
12	.net	gTLD	47,754		57,410	▼ -17%
13	.sbs	gTLD	41,029		17,744	▲ 131%
14	.xyz	gTLD	39,660		85,176	▼ -53%
15	.my	ccTLD	36,443		-	New entry
16	.ru	ccTLD	32,492		39,984	▼ -19%
17	.org	gTLD	29,166		22,240	▲ 31%
18	.info	gTLD	28,353		22,116	▲ 28%
19	.cfd	gTLD	24,760		-	New entry
20	.click	gTLD	21,687		-	New entry

0 300 600 900

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

Top 20 ccTLDs

Rank	Domain TLD	Apr 25 - Sep 25	Apr 25 - Sep 25 data bar	Oct 24 - Mar 25	% Change
1	.cn	317,707		81,146	▲ 292%
2	.cc	216,942		148,868	▲ 46%
3	.my	36,443		5,666	▲ 543%
4	.ru	32,492		39,984	▼ -19%
5	.co	15,247		42,087	▼ -64%
6	.me	7,862		13,353	▼ -41%
7	.tv	4,804		6,007	▼ -20%
8	.de	4,459		8,327	▼ -46%
9	.us	4,009		7,454	▼ -46%
10	.ee	3,168		-	New entry
11	.pl	2,961		1,565	▲ 89%
12	.tw	2,926		5,310	▼ -45%
13	.eu	2,619		2,478	▲ 6%
14	.uk	2,334		4,569	▼ -49%
15	.fr	1,802		1,998	▼ -10%
16	.jp	1,745		1,839	▼ -5%
17	.in	1,676		2,418	▼ -31%
18	.ro	1,661		-	New entry
19	.pw	1,657		-	New entry
20	.id	1,602		-	New entry

0 100 200 300 400

Top 20 gTLDs... | Top 20 gTLD...

Top 20 gTLD

Rank	Domain TLD	Apr 25 - Sep 25	Apr 25 - Sep 25 data bar	Oct 24 - Mar 24	% Change
1	.com	813,514		513,292	▲ 58%
2	.top	577,797		316,433	▲ 83%
3	.vip	126,458		115,032	▲ 10%
4	.mobi	120,197		-	New entry
5	.pro	79,617		20,190	▲ 294%
6	.bond	68,171		16,391	▲ 316%
7	.icu	60,407		16,566	▲ 265%
8	.shop	54,565		59,830	▼ -9%
9	.cyou	52,009		-	New entry
10	.net	47,754		57,410	▼ -17%
11	.sbs	41,029		17,744	▲ 131%
12	.xyz	39,660		85,176	▼ -53%
13	.org	29,166		22,240	▲ 31%
14	.info	28,353		22,116	▲ 28%
15	.cfd	24,760		-	New entry
16	.click	21,687		-	New entry
17	.live	21,251		-	New entry
18	.life	20,485		-	New entry
19	.blog	20,358		-	New entry
20	.app	18,632		-	New entry

0 300 600 900

Top 20 gTLDs... | Top 20 gTLD...

Top 20 gTLDs by % of zone file

Rank	Domain TLD	Apr 25 - Sep 25	Zone size	% of zone listed	% of zone data bar
1	.bond	68,171	126,951	53.70%	
2	.town	10,553	35,872	29.42%	
3	.qpon	10,832	38,019	28.49%	
4	.mobi	120,197	440,654	27.28%	
5	.auction	2,812	15,927	17.66%	
6	.cyou	52,009	311,885	16.68%	
7	.lgbt	2,885	18,371	15.70%	
8	.xin	8,088	52,101	15.52%	
9	.locker	3,346	21,649	15.46%	
10	.icu	60,407	476,064	12.69%	
11	.loan	15,888	127,671	12.44%	
12	.reviews	1,611	13,398	12.02%	
13	.win	9,086	92,821	9.79%	
14	.wiki	7,026	75,561	9.30%	
15	.vip	126,458	1,413,805	8.94%	
16	.pro	79,617	1,021,264	7.80%	
17	.bid	4,923	66,722	7.38%	
18	.rip	885	12,173	7.27%	
19	.tube	796	11,372	7.00%	
20	.pet	1,905	27,471	6.93%	

0% 50% 100%

Trending phishing terms for malicious or suspicious domains

It's all changed in the Top 20 phishing terms. Over the past 6 months, ten new terms have entered the rankings, following a mass exodus of delivery and tracking related keywords such as "deliver", "correo", "tracking", and "com-track".

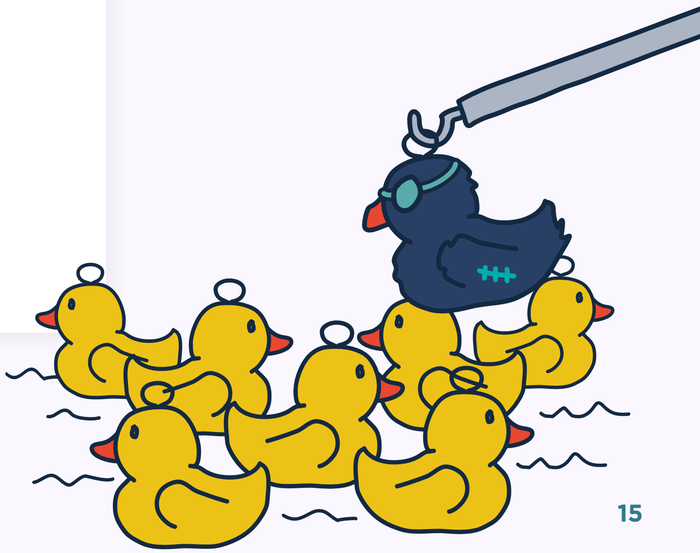
In our previous Spotlight, we highlighted the rise of toll road scams, and the trend continues. Over the last six months, "tollbill" saw the most significant increase at +66% (#11). Similarly, a new entry "ov-pay" at #19, representative of the Dutch public transport system, is seemingly caught up in the same style of phishing activity.

We also have a new entry "casino" (#15), linking back to the continuing growth of Chinese gambling sites noted earlier in this report.

What terms do bad actors use for domain names?

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

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



01

02

03

04

05

Top 20 phishing... | Phishing terms

Top 20 phishing terms

Rank	Term	Apr 25 - Sep 25	Apr 25 - Sep 25 data bar	Oct 24 - Mar 25	% Change
1	com-	5,506		-	New entry
2	service	5,490		12,835	-57%
3	login	5,113		4,803	6%
4	account	4,723		6,372	-26%
5	security	3,948		3,697	7%
6	verification	3,726		2,322	60%
7	track	3,714		-	New entry
8	secure	3,619		2,889	25%
9	support	3,470		3,679	-6%
10	online	3,221		2,807	15%
11	tollbill	3,117		1,875	66%
12	oferta	3,009		-	New entry
13	gov-	2,950		-	New entry
14	comsit	2,931		-	New entry
15	casino	2,913		-	New entry
16	teleg	2,648		-	New entry
17	wallet	2,517		3,923	New entry
18	verify	2,419		3,115	-22%
19	ov-pay	2,413		-	New entry
20	park-	2,253		-	New entry

Top 20 phishing... | Phishing terms

Phishing terms

Types of abuse

Over the last six months, detections relating to **compromised domains** associated with:

- **botnet C&Cs** increased by **+100%**
- **malware**-related abuse increased by **+118%**

While these percentage increases are high, this is largely due to detection improvements, not more abuse.

In September, our engineers developed a tighter integration, specifically with ThreatFox, a platform from abuse.ch and Spamhaus dedicated to sharing indicators of compromise (IOCs) associated with malware. More visibility means more detections, and more detections mean more impact from the data shared.

In terms of malicious domains, percentage increases for all types are significant, ranging between 46-77%. While this may indicate a genuine rise in abuse activity, it also reflects proactive improvements in our detection capabilities and new industry partnerships.

Included in 'Bad reputation' malicious domains are Traffic Distribution Systems (TDS), which we are actively researching and tracking. We will continue monitoring this activity and our findings will be reported in the next update.

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

Types of abuse

Bad reputation

Malicious	Compromised
2,645,792	15,446
▲ 46% ▲	▲ 6% ▲

A domain's reputation score has exceeded policy limits.

Botnet C&C

Malicious	Compromised
2,962	104
▲ 77% ▲	▲ 100% ▲

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

Malware

Malicious	Compromised
3,355	45,787
▲ 53% ▲	▲ 118% ▲

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

Phishing

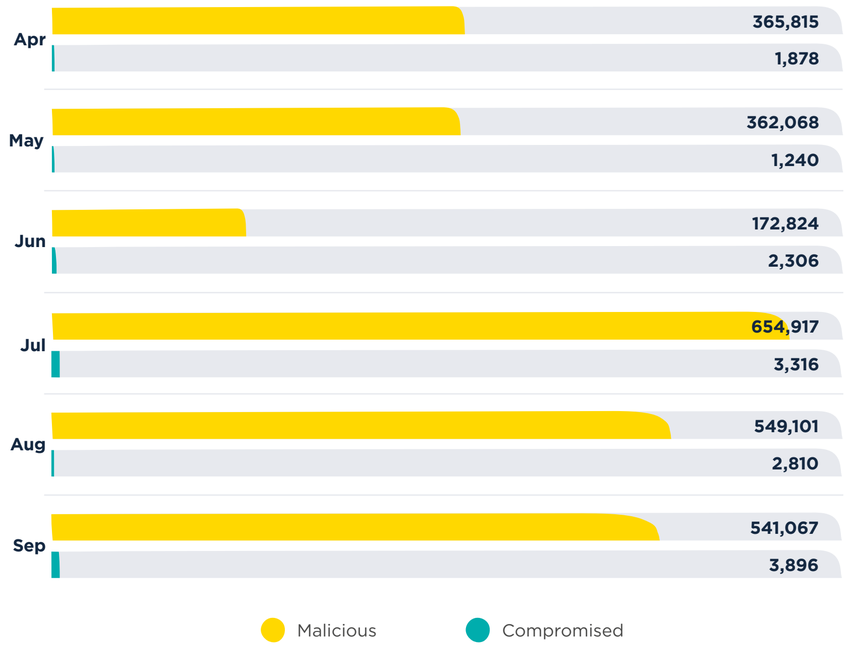
Malicious	Compromised
581,108	97,704
▲ 58% ▲	▼ -2% ▼

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

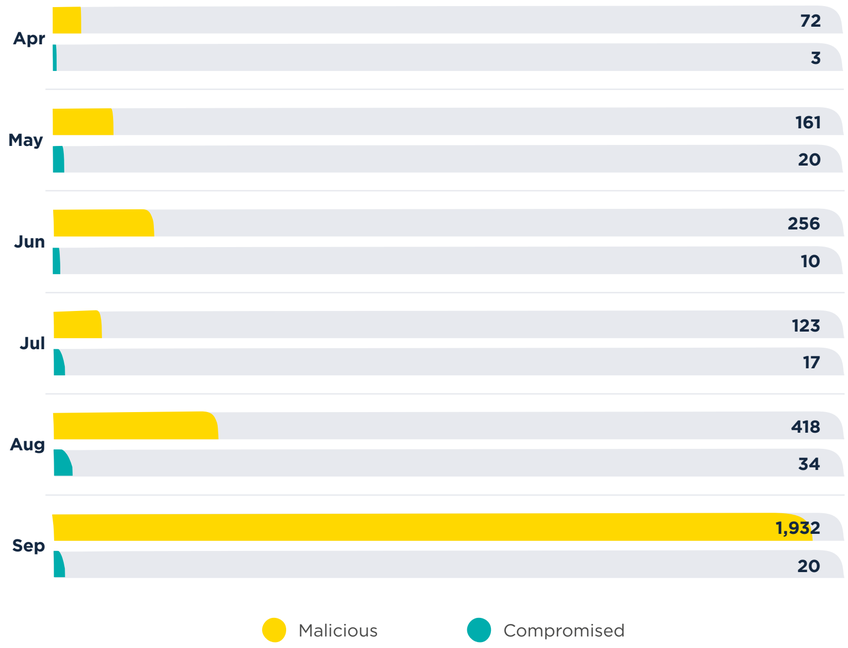
Types of abuse

Types of abuse per month

Bad reputation per month



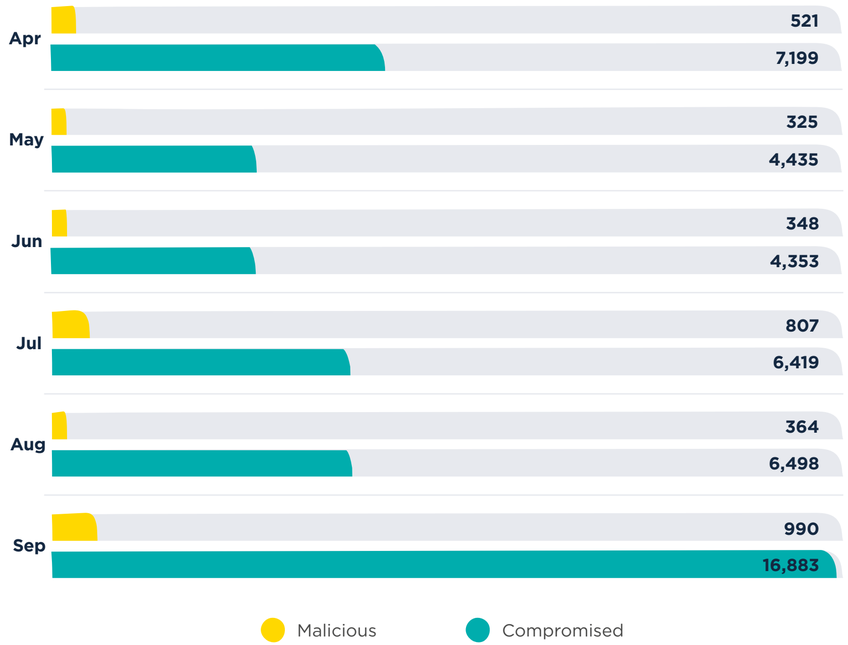
Botnet C&C per month



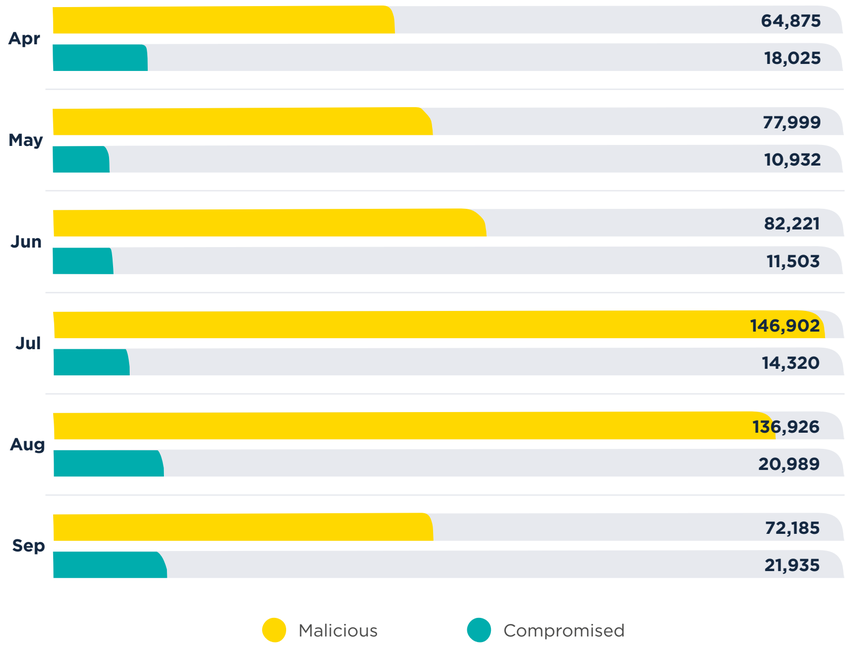
Types of abuse

Types of abuse per month

Malware per month



Phishing per month



Recommendations

With this report's Spotlight on TDS, below are specific actions that registrars, registries, 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 stopping TDS abuse. Not only do they have the tools to spot when threat actors set up hundreds of lookalike domains, they can also shut them down before they can be used in malicious redirect chains. The faster these domains are identified and taken down, the harder (and more expensive) it becomes for threat actors to keep running their malicious TDS operations.

Enforce Know-Your-Customer (KYC)

Bulk domain registration has become far too easy, and that's exactly why 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, registrars 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 point of view, however, TDS infrastructure **is** part of DNS abuse, for the very reason that it is facilitating large-scale malicious operations, and in these cases, exists solely to facilitate abuse. If you're aligned with our view, we'd love to hear from you to help broaden and redefine the scope of DNS abuse - please get in contact with us via LinkedIn, X, or Mastodon.

Advice to end-users

TDS operators rely on ad clicks and redirect chains to lure victims to their malicious content. To protect yourself from phishing scams and other malicious threats veiled behind TDS, avoid clicking on suspicious ads - such as those asking for personal details, containing misspelled URLs, or triggering pop-up redirects - or links from unknown senders, and consider DNS filtering services to reduce exposure to malicious redirected traffic.

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!

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.