



Spamhaus Domain Reputation Update

October 2025 - March 2026

Spamhaus, the independent leader in IP and domain reputation, reviews the domain name ecosphere. From the number of newly registered domains to the domain abuse our researchers are observing, this update highlights trends and provides insights into the poor reputation of domains, and champions providers where positive improvements are seen.

Welcome to the Spamhaus Domain Reputation Update.

Enter





Contents

The Spotlight

01 The Spotlight

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

03 A TDS is a network that advertises and affiliates with intermediaries, often used to serve content for a TDS, but the advantage is that it can be used to distribute, conceal, and accurately target victims. Spamhaus has observed an increase in TDS activity, malware distribution, monetizing, and other harmful activities that rely on domains to distribute, conceal, and accurately target victims.

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

05 [Spotlight continued](#)

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 3

New domains

01 New domains

02 New domains overview

03 Over the past six months, 455 million new domains were registered, an average of 22 million per month, compared with the previous six months. August stood out as a record month with approximately 40 million registrations, largely driven by a spike in registrations from China.

04 It is important to note that a significant number of these new domains are used for malicious purposes. Unfortunately, its evidence is often only discovered once the malicious campaign starts. Furthermore, by using new domains, bad actors prevent registrars and registrars from stopping preventatives takedowns.

05 **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 compiled this list from various data sources including Passive DNS, SHODAN data and zone files shared by registrars. The new domain data, therefore, is not the most recent number of new domains, but the number of new domains Spamhaus has visibility of.

Month	Number of new domains
Apr 2024	21,072,523
May 2024	22,523,123
Jun 2024	23,123,456
Jul 2024	24,567,890
Aug 2024	40,123,456
Sep 2024	25,678,901
Oct 2024	26,789,012
Nov 2024	27,890,123
Dec 2024	28,901,234
Jan 2025	29,012,345
Feb 2025	30,123,456
Mar 2025	31,234,567
Apr 2025	32,345,678
May 2025	33,456,789
Jun 2025	34,567,890
Jul 2025	35,678,901
Aug 2025	36,789,012
Sep 2025	37,890,123
Oct 2025	38,901,234
Nov 2025	39,012,345
Dec 2025	40,123,456
Jan 2026	41,234,567
Feb 2026	42,345,678
Mar 2026	43,456,789
Apr 2026	44,567,890
May 2026	45,678,901
Jun 2026	46,789,012
Jul 2026	47,890,123
Aug 2026	48,901,234
Sep 2026	49,012,345
Oct 2026	50,123,456
Nov 2026	51,234,567
Dec 2026	52,345,678
Jan 2027	53,456,789
Feb 2027	54,567,890
Mar 2027	55,678,901
Apr 2027	56,789,012
May 2027	57,890,123
Jun 2027	58,901,234
Jul 2027	59,012,345
Aug 2027	60,123,456
Sep 2027	61,234,567
Oct 2027	62,345,678
Nov 2027	63,456,789
Dec 2027	64,567,890
Jan 2028	65,678,901
Feb 2028	66,789,012
Mar 2028	67,890,123
Apr 2028	68,901,234
May 2028	69,012,345
Jun 2028	70,123,456
Jul 2028	71,234,567
Aug 2028	72,345,678
Sep 2028	73,456,789
Oct 2028	74,567,890
Nov 2028	75,678,901
Dec 2028	76,789,012
Jan 2029	77,890,123
Feb 2029	78,901,234
Mar 2029	79,012,345
Apr 2029	80,123,456
May 2029	81,234,567
Jun 2029	82,345,678
Jul 2029	83,456,789
Aug 2029	84,567,890
Sep 2029	85,678,901
Oct 2029	86,789,012
Nov 2029	87,890,123
Dec 2029	88,901,234
Jan 2030	89,012,345
Feb 2030	90,123,456
Mar 2030	91,234,567
Apr 2030	92,345,678
May 2030	93,456,789
Jun 2030	94,567,890
Jul 2030	95,678,901
Aug 2030	96,789,012
Sep 2030	97,890,123
Oct 2030	98,901,234
Nov 2030	99,012,345
Dec 2030	100,123,456

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 6

Malicious/suspicious domains

01 Malicious/suspicious domains

02 Domain overview

03 Over the past six months, 32 million domains were identified as malicious or suspicious, an average of 540,000 per day, compared to the previous six months. July was particularly notable with a record number of 600,000 domains identified. This was due to a significant increase in the registration of a significant number of domains, most of which were used for malicious purposes.

04 TLD distribution continues to be a key factor in identifying malicious domains. 79% of detections, while still dominated by .com, .net, and .org, saw a further +87% increase in detections.

05 **What triggers a domain to be listed as malicious/suspicious by Spamhaus?**
Our systems evaluate hundreds of signals relating to a domain and to associated behavior. 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.

Month	Number of Domain listings
Apr 2024	1,234,567
May 2024	1,345,678
Jun 2024	1,456,789
Jul 2024	600,000
Aug 2024	1,567,890
Sep 2024	1,678,901
Oct 2024	1,789,012
Nov 2024	1,890,123
Dec 2024	1,901,234
Jan 2025	2,012,345
Feb 2025	2,123,456
Mar 2025	2,234,567
Apr 2025	2,345,678
May 2025	2,456,789
Jun 2025	2,567,890
Jul 2025	2,678,901
Aug 2025	2,789,012
Sep 2025	2,890,123
Oct 2025	2,901,234
Nov 2025	3,012,345
Dec 2025	3,123,456
Jan 2026	3,234,567
Feb 2026	3,345,678
Mar 2026	3,456,789
Apr 2026	3,567,890
May 2026	3,678,901
Jun 2026	3,789,012
Jul 2026	3,890,123
Aug 2026	3,901,234
Sep 2026	4,012,345
Oct 2026	4,123,456
Nov 2026	4,234,567
Dec 2026	4,345,678
Jan 2027	4,456,789
Feb 2027	4,567,890
Mar 2027	4,678,901
Apr 2027	4,789,012
May 2027	4,890,123
Jun 2027	4,901,234
Jul 2027	5,012,345
Aug 2027	5,123,456
Sep 2027	5,234,567
Oct 2027	5,345,678
Nov 2027	5,456,789
Dec 2027	5,567,890
Jan 2028	5,678,901
Feb 2028	5,789,012
Mar 2028	5,890,123
Apr 2028	5,901,234
May 2028	6,012,345
Jun 2028	6,123,456
Jul 2028	6,234,567
Aug 2028	6,345,678
Sep 2028	6,456,789
Oct 2028	6,567,890
Nov 2028	6,678,901
Dec 2028	6,789,012
Jan 2029	6,890,123
Feb 2029	6,901,234
Mar 2029	7,012,345
Apr 2029	7,123,456
May 2029	7,234,567
Jun 2029	7,345,678
Jul 2029	7,456,789
Aug 2029	7,567,890
Sep 2029	7,678,901
Oct 2029	7,789,012
Nov 2029	7,890,123
Dec 2029	7,901,234
Jan 2030	8,012,345
Feb 2030	8,123,456
Mar 2030	8,234,567
Apr 2030	8,345,678
May 2030	8,456,789
Jun 2030	8,567,890
Jul 2030	8,678,901
Aug 2030	8,789,012
Sep 2030	8,890,123
Oct 2030	8,901,234
Nov 2030	9,012,345
Dec 2030	9,123,456
Jan 2031	9,234,567
Feb 2031	9,345,678
Mar 2031	9,456,789
Apr 2031	9,567,890
May 2031	9,678,901
Jun 2031	9,789,012
Jul 2031	9,890,123
Aug 2031	9,901,234
Sep 2031	10,012,345
Oct 2031	10,123,456
Nov 2031	10,234,567
Dec 2031	10,345,678

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 13

Recommendations

01 Recommendations

02 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.

03 **Shut down the supply**
Registrars have a key role to play in ensuring that they have the tools to spot when they can also shut them down. The factor these should consider most important is the malicious TDS operations.

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

05 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 perspective, if a domain is used to facilitate abuse, it's often outside the scope of DNS Abuse. For the purposes of this report, we are focusing on large-scale malicious operators and facilitators.

Protect yourself from phishing scams and malware
If you're aligned with the good side of the internet, you should 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!

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 23

Additional info

01 Additional info

02 **About Spamhaus**
Spamhaus strengthens trust in the internet. Advocating for a safer, more secure internet, we share reliable intelligence and insights from our manual investigations and automated systems. Spamhaus is trusted by governments, law enforcement, and industry for its strong ethics, in-depth research, and actionable data. This data is also used to provide signal and intelligence to specific geographies, such as the UK, the EU, and the US.

03 **Report Methodology**
Due to ongoing issues outside of our control to do with WHOIS and IPAP data, some of our data is incomplete. This is a direct result of GDPR. Where we see missing zone file data we welcome registries to contact us and share this data.

04 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.

05

Spamhaus Domain Reputation Update | Apr 25 - Sep 25

Go to page 24

01

The Spotlight

ICANN proposes required checks on “associated domains”

A new policy against DNS abuse

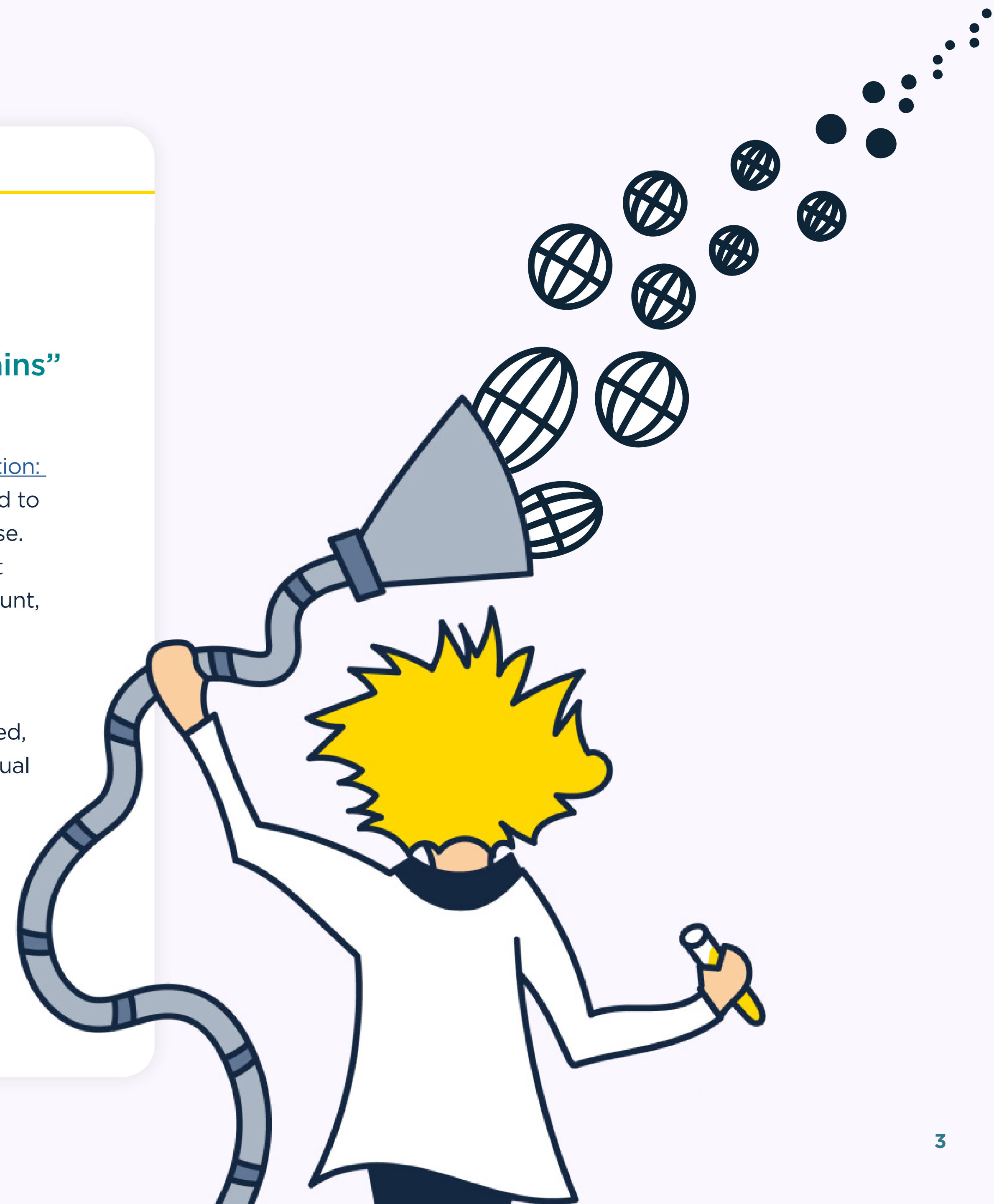
In January 2026, ICANN gNSO announced a new initiative, [“DNS Abuse Mitigation: PDP 1 on Associated Domain Checks”](#), under which registrars would be required to identify and review “associated domains” as part of their response to DNS abuse. This means that when a single domain is identified as malicious, registrars must investigate and check other domains associated with the same registrant, account, infrastructure, or behaviour.

What’s the objective here?

A theme we see in every [Domain Reputation Update](#) is the use of bulk registered, disposable domains, enabling threat actors to burn through domains as individual ones are detected and taken down.

By requiring registrars to check related domains, ICANN’s objective is to disrupt this disposable lifecycle, by limiting the ability to quickly pivot and restore their infrastructure.

Spotlight continued



01

●●● Spotlight cont. ✕

Breaking the chain

This initiative represents another step towards a proactive approach to tackling domain abuse at scale, instead of reacting to single domain takedowns. If implemented effectively, it has the potential to significantly weaken campaigns that rely on large domain portfolios spread across multiple top-level domains (TLDs).

In this report, there is clear evidence of threat actors actively rotating between TLDs, high churn in domains, and abuse concentrated at specific registries. For three consecutive reports, .bond, operated by Shortdot SA, continues to display patterns of high churn, with new domain registrations (1.13 million) almost equal to its total zone count (1.15 million).

By requiring registrars that currently enable this behaviour, to check all associated domains, this policy would help address the following practices by:

- Limiting the ability to move between TLDs and avoid detection
- Disrupting campaigns utilizing a large number of domains
- Making it harder for threat actors to use bulk registrations to deploy abuse

Spotlight continued



01

●●● Spotlight cont. ✕

This is a good thing!

Spamhaus fully supports these policy developments. While most leading registrars already perform checks on associated domains when responding to abuse, introducing these changes will help raise the bar across the industry.

However, this will not be without challenges. Defining what qualifies as an “associated domain” will not be straightforward. An associated domain could be one of many things: it may belong to the same registrant or account, be paid for with the same credit card, or be hosted on the same infrastructure. Some checks will be more difficult to complete than others. For example, a bulk registrar operating under a reseller model. In this scenario, the registrar is responsible but does not have a direct customer relationship meaning it has access to very little information.

Additionally, registrars will need to be able to demonstrate that appropriate checks have been completed in a way that meets ICANN compliance requirements.

Nevertheless, we welcome this policy and its proactive and effective approach to mitigating DNS abuse.

02

03

04

05



01

New domains

New domains overview

Over the past six months, approximately 46.9 million new domains were registered, a +7.6% increase compared with the previous six months. The monthly average increased to 7.8 million domains, but growth was less significant than between April - September 2025 (+11.48%).

There was a seasonal dip between December-February, followed by a strong rebound in March, recording the highest monthly volume of domains, with over 8.4 million new domains registered.

It is important to note that a new domain is not a bad domain per se. However, a considerable amount of abuse is associated with new domain names.

One reason is that if a bad actor buys a new domain and uses it immediately, there is minimal chance of security systems & professionals having prior knowledge of this domain's existence. Unfortunately, its existence is only discovered once the malicious campaign starts. Furthermore, by using new domains, bad actors prevent registries and registrars from doing pre-emptive takedowns.

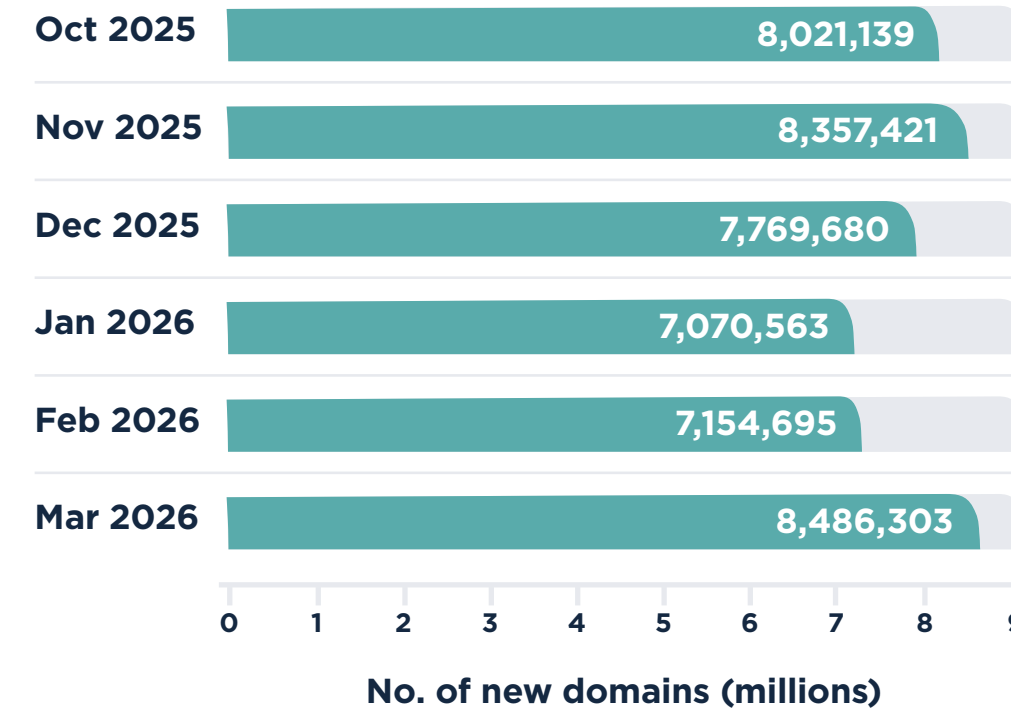
02

03

04

05

Number of new domains per month



Six Month Total
46,859,801
▲ 7.63% ▲

Monthly Average
7,809,967
▲ 533,328 ▲

i What is a new domain?

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

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

01

02

03

04

05

New domains... x TLD types... x

New domains by top-level domain (TLD)

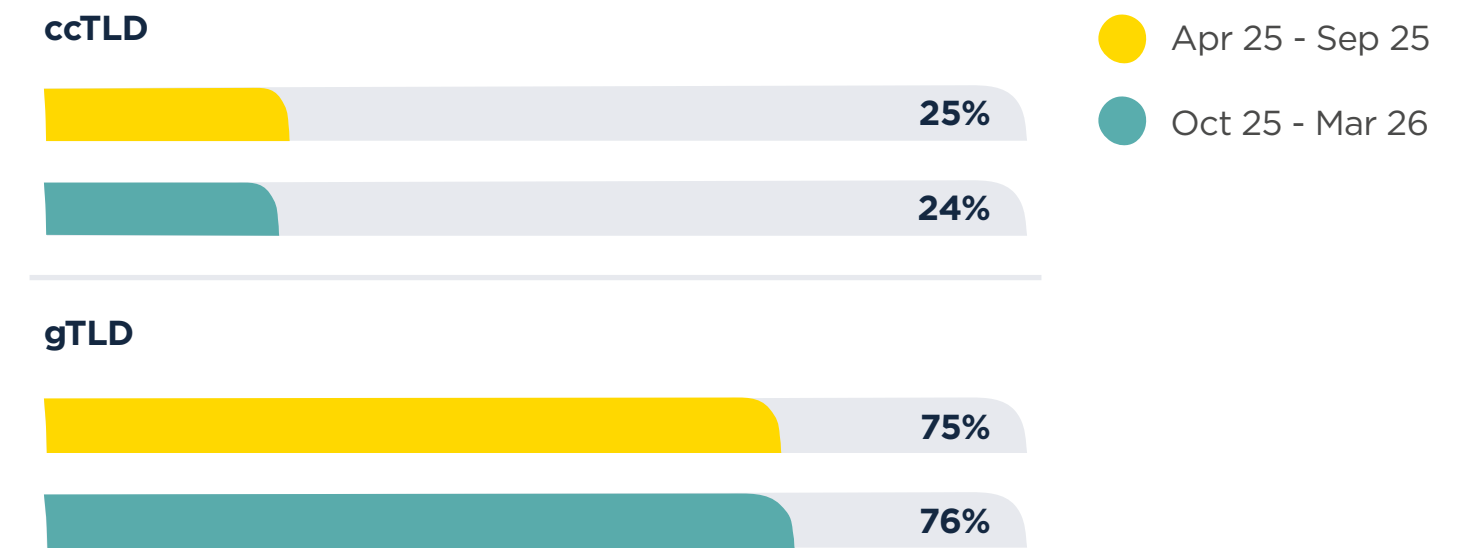
Over the last six months, gTLDs remain dominant (76%), with ccTLDs accounting for 24% of new TLD registrations. However, this reporting period growth appears less concentrated, shifting from a few dominant TLDs to a more fragmented landscape.

Among gTLDs, .bond (#6) increased by +375%. Meanwhile, .info (#5) grew by +79%, likely influenced by a sales promotion, and .app (#17) increased +46%, reflecting continued growth in app-based services. Other significant increases included .cyo (+35%) and .sbs (+24%), both well known as low-cost, high-volume gTLDs. In contrast, .top (#3) and .cfd (#19) saw new registrations drop by -27% and -15%, respectively.

There were two new entries in the Top 20 ccTLDs this period, .com.cn (second-level domain for China, #14), and .io (British Indian Ocean Territory, #18). .io is operated by the Internet Computer Bureau and is widely used as a gTLD in the technology start up sector.

x TLD types... x

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

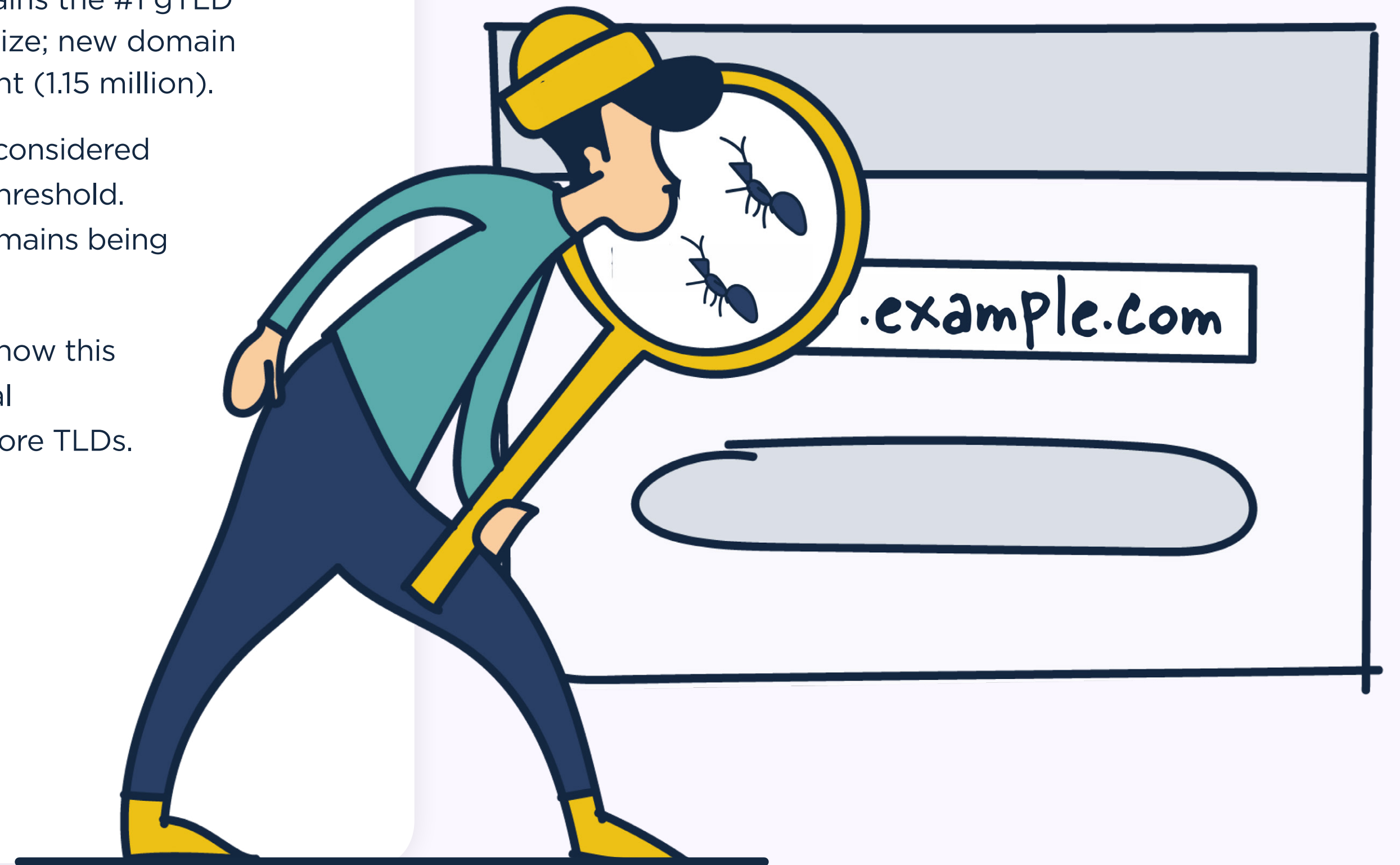
●●● New domains... ✕

After a brief appearance, .es (Spain) dropped out of the Top 20 ccTLDs used in new domain registrations, joined by .us (United States). Meanwhile, .ai (Anguilla) continued its upward trend inline with the explosion of AI, climbing a further two positions to #10, joined by .fr (+27%), .in (+19%), and .pl (+20%).

.bond (#6) continues to display abnormal registration patterns, consistent with the [Domain Reputation Update April - September 2025](#). It remains the #1 gTLD for percentage of newly observed domains against total zone size; new domain registrations (1.13 million) are almost equal to its total zone count (1.15 million).

A threshold of approximately 10-20% new domains is generally considered unusually high. In fact, three quarters of the top 20 exceed this threshold. This behavior suggests a large volume of domain churn, with domains being registered and cancelled quickly.

Registries including Identity Digital, Radix and Shortdot S.A all show this high-churn pattern, while larger operators such as Identity Digital and GoDaddy do not appear in the Top 20, despite managing more TLDs.



01

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

Top 20 TLDs used in new domains

Rank	New domain TLD	TLD type	Oct 25 - Mar 26	Oct 25 - Mar 26 data bar	Apr 25 - Sep 25	% Change
1	.com	gTLD	14,306,314		13,317,985	▲ 7%
2	.xyz	gTLD	2,669,919		2,568,825	▲ 4%
3	.top	gTLD	2,038,137		2,793,617	▼ -27%
4	.shop	gTLD	1,650,665		1,479,708	▲ 12%
5	.info	gTLD	1,624,577		906,640	▲ 79%
6	.bond	gTLD	1,130,779		-	New entry
7	.online	gTLD	1,116,916		1,044,785	▲ 7%
8	.cn	ccTLD	1,109,303		1,042,402	▲ 6%
9	.org	gTLD	1,069,625		958,255	▲ 12%
10	.de	ccTLD	801,018		861,901	▼ -7%
11	.net	gTLD	782,812		720,128	▲ 9%
12	.sbs	gTLD	744,244		600,420	▲ 24%
13	.store	gTLD	732,635		761,187	▼ -4%
14	.cc	ccTLD	658,778		678,006	▼ -3%
15	.ru	ccTLD	639,722		590,687	▲ 8%
16	.site	gTLD	639,273		631,962	▲ 1%
17	.com.br	ccTLD	591,556		580,617	▲ 2%
18	.vip	gTLD	545,417		467,086	▲ 17%
19	.co.uk	ccTLD	535,646		462,636	▲ 16%
20	.fr	ccTLD	386,242		-	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	Oct 25 - Mar 26	Oct 25 - Mar 26 data bar	Apr 25 - Sep 25	% Change
1	.cn	1,109,303		1,042,402	▲ 6%
2	.de	801,018		861,901	▼ -7%
3	.cc	658,778		678,006	▼ -3%
4	.ru	639,722		590,687	▲ 8%
5	.com.br	591,556		580,617	▲ 2%
6	.co.uk	535,646		462,636	▲ 16%
7	.fr	386,242		304,669	▲ 27%
8	.in	380,747		320,552	▲ 19%
9	.nl	300,745		317,392	▼ -5%
10	.ai	290,901		249,217	▲ 17%
11	.co	288,868		419,534	▼ -31%
12	.eu	254,624		231,682	▲ 10%
13	.ca	252,201		235,901	▲ 7%
14	.com.cn	223,187		-	New entry
15	.com.au	204,664		207,923	▼ -2%
16	.pl	192,863		161,109	▲ 20%
17	.it	174,205		188,980	▼ -8%
18	.io	164,062		-	New entry
19	.me	162,677		160,983	▲ 1%
20	.my	157,551		304,812	▼ -48%

01

Top 20 gTLDs used in new domains

Rank	New domain TLD	Oct 25 - Mar 26	Oct 25 - Mar 26 data bar	Apr 25 - Sep 25	% Change
1	.com	14,306,314		13,317,985	▲ 7%
2	.xyz	2,669,919		2,568,825	▲ 4%
3	.top	2,038,137		2,793,617	▼ -27%
4	.shop	1,650,665		1,479,708	▲ 12%
5	.info	1,624,577		906,640	▲ 79%
6	.bond	1,130,779		237,903	▲ 375%
7	.online	1,116,916		1,044,785	▲ 7%
8	.org	1,069,625		958,255	▲ 12%
9	.net	782,812		720,128	▲ 9%
10	.sbs	744,244		600,420	▲ 24%
11	.store	732,635		761,187	▼ -4%
12	.site	639,273		631,962	▲ 1%
13	.vip	545,417		467,086	▲ 17%
14	.pro	349,498		336,561	▲ 4%
15	.click	332,132		279,080	▲ 19%
16	.lol	326,607		-	New entry
17	.app	313,290		215,081	▲ 46%
18	.cyou	256,455		189,933	▲ 35%
19	.cf	229,379		269,177	▼ -15%
20	.space	210,868		-	New entry

02

03

04

05

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

Rank	New domain TLD	Oct 25 - Mar 26	Zone size	% of zone newly observed	% of zone data bar
1	.bond	1,130,779	1,147,185	98.57%	
2	.lol	326,607	455,492	71.70%	
3	.cyou	256,455	455,512	56.30%	
4	.sbs	744,244	1,414,674	52.61%	
5	.click	332,132	732,673	45.33%	
6	.cf	229,379	535,716	42.82%	
7	.shop	1,650,665	4,188,186	39.41%	
8	.space	210,868	537,132	39.26%	
9	.site	639,273	1,760,628	36.31%	
10	.store	732,635	2,121,288	34.54%	
11	.vip	545,417	1,632,292	33.41%	
12	.online	1,116,916	3,399,618	32.85%	
13	.xyz	2,669,919	8,205,754	32.54%	
14	.pro	349,498	1,111,213	31.45%	
15	.info	1,624,577	5,495,829	29.56%	
16	.top	2,038,137	11,398,102	17.88%	
17	.app	313,290	2,329,053	13.45%	
18	.org	1,069,625	12,342,109	8.67%	
19	.com	14,306,314	168,024,226	8.51%	
20	.net	782,812	12,803,743	6.11%	

01

●●● Trending terms... ✕

Trending terms in new domains

casino (+78%) is the #1 trending term for new domain registrations, indicating a strong focus on gambling-related domains, a pattern that reappears later in this report.

There were nine new entries among trending terms used in new domains, reflecting the rapidly changing keyword landscape. This report shows a transition from LLM and search-related terms (engine, search, keyword) to commercial, financial, and transactional terms, with new entries: capital (#13), store (#14), sports (#15), finance (#17), and travel (#20).

More specific business terms also continued to rise, including consult (+30%), digital (+61%), group (+21%), and solution (+21%). In contrast, several business operations terms decreased in popularity: information, keyword and program, all dropped out of the Top 20, while system (#16) dropped 14 places with a -67% decrease.

02

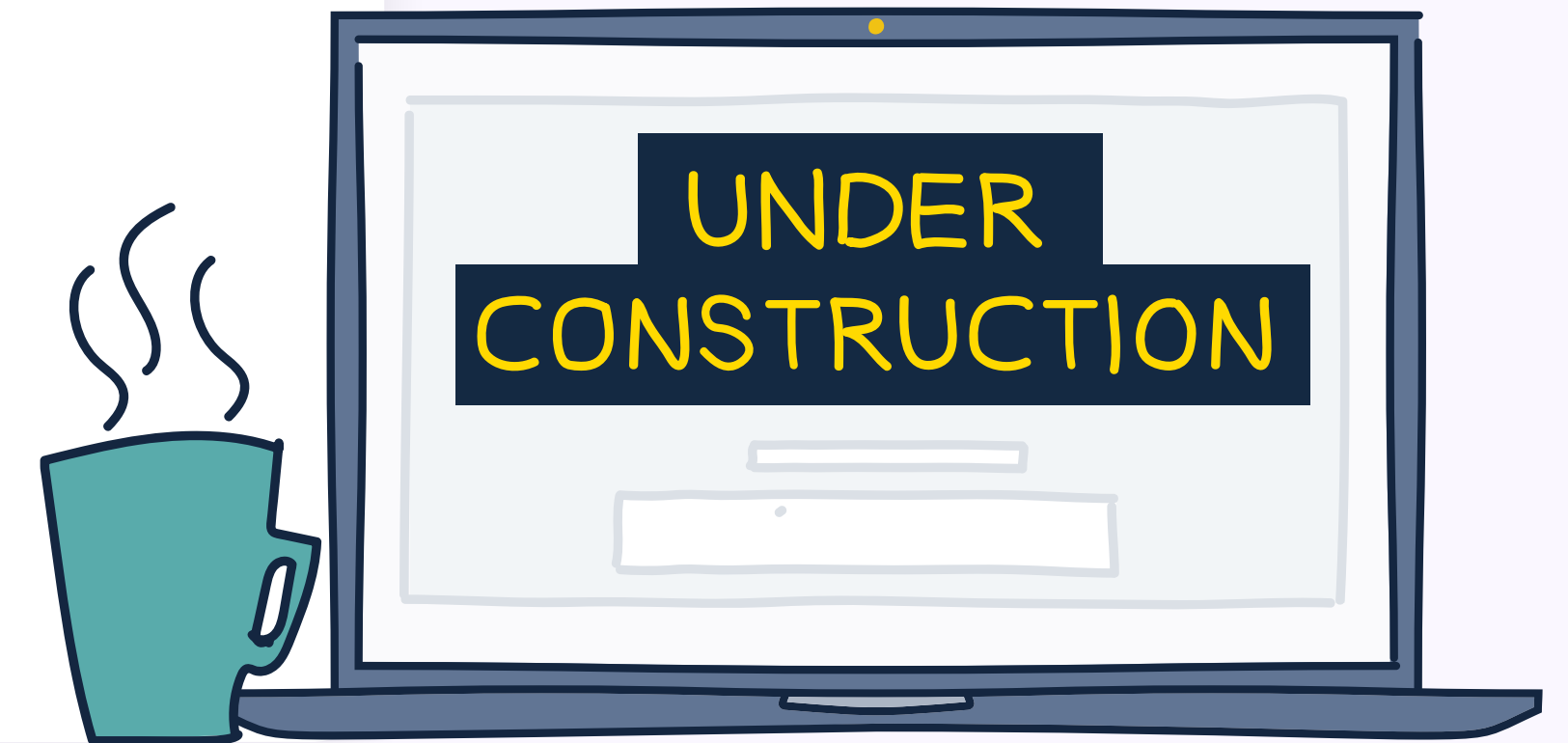
03

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	Oct 25 - Mar 26 trending terms	Oct 25 - Mar 26	Oct 25 - Mar 26 data bar	Apr 25 - Sep 25	% Change
1	casino	261,665		146,952	▲ 78%
2	service	247,767		242,579	▲ 2%
3	solution	225,337		186,579	▲ 21%
4	studio	220,257		171,933	▲ 28%
5	digital	212,375		132,304	▲ 61%
6	group	179,656		148,320	▲ 21%
7	market	166,909		282,827	▼ -41%
8	online	146,844		124,168	▲ 18%
9	consult	146,838		112,657	▲ 30%
10	design	127,629		-	New entry
11	global	125,599		-	New entry
12	health	122,082		106,109	▲ 15%
13	capital	102,306		-	New entry
14	store	93,969		-	New entry
15	sports	85,463		-	New entry
16	system	82,188		247,038	▼ -67%
17	finance	81,556		-	New entry
18	partner	81,341		-	New entry
19	collect	54,585		-	New entry
20	travel	50,719		-	New entry

02

03

04

05

Trending terms



01

02

03

04

05

Malicious/suspicious domains

Domain overview

Over the past six months, 2.15 million malicious or suspicious domains were detected, averaging approximately 358,000 per month. This represents a -33.7% decrease compared to the previous six month period (April - September 2025).

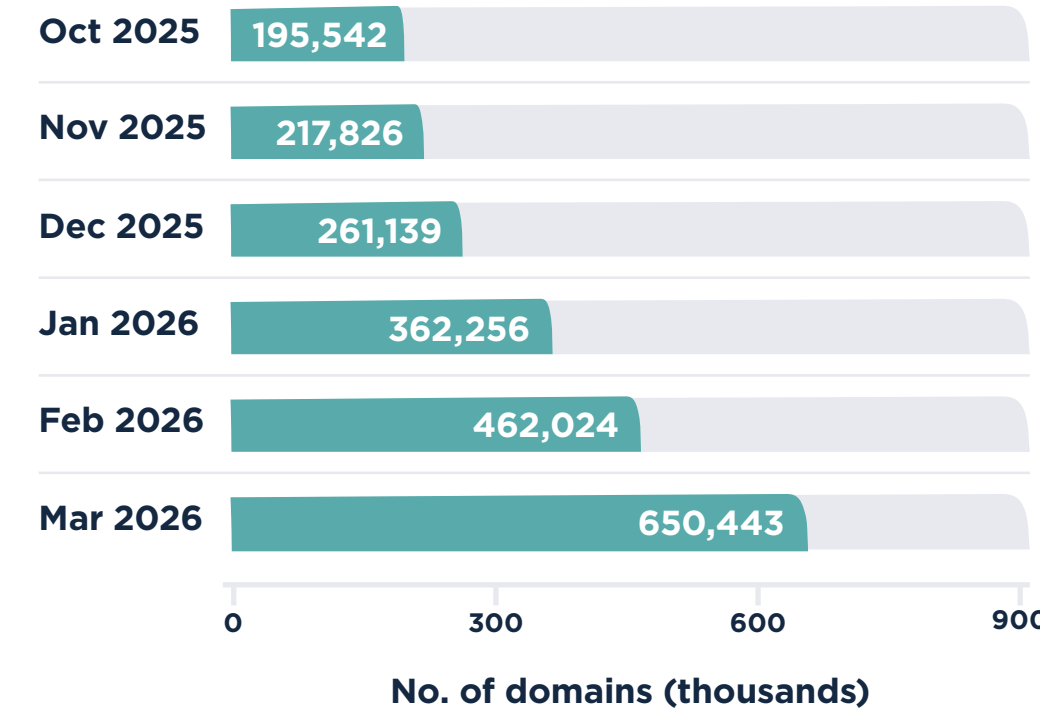
Activity started off low between October and November, with a consistent month-on-month increase, before returning to levels seen in the [April - September 2025 Domain Reputation Update](#), with 650,443 detections in March.

Over this period, the distribution between ccTLD and gTLD domains has shifted marginally, with ccTLDs accounting for 24.5% of detections and gTLDs for 75.5%.

.cfd climbed 14 places to #5 in the Top 20 TLDs and 12 places to #3 in the Top 20 gTLDs, while .com and .top retained their positions at #1 and #2, respectively, in both rankings.

Meanwhile, there were only two new entries in the Top 20 TLDs: .asia (#10) and .online (#18). As a result, .mobi and .my have dropped out of this Top 20.

Number of Domain listings per month



Six Month Total

2,149,230

▼ -33.65% ▼

Monthly Average

358,205

▼ -1,090,121 ▼

What triggers a domain to be listed as malicious/suspicious by Spamhaus?

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

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

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

01

02

03

04

05

Trending terms... ✕

TLDs listed in our domain data

The TLDs typically responsible for the largest number of listings experienced significant decreases between October 2025 - March 2026, including .vip (-59%), .cc (-56%), .top (-53%), and .com (-38%). At the same time, growth of abuse in gTLDs is concentrated in fewer TLDs, notably .cfd (+279%), with more moderate increases for .info (+33%) and .xyz (+20%), alongside new entries .online (#14), .biz (#17), and .site (#19).

A portion of the increase in .cfd domains detected may be linked to Spamhaus' improved ingestion of smishing (SMS phishing) data from large US telcos, with approximately 21,000 domains categorised as phishing. There is also a large volume of Chinese casino and gambling-related domains within this TLD.

.cfd also stands out as a high-risk TLD, with approximately 17.5% of its zone file listed. A threshold of 5% listed is considered a red flag, meaning anything above 10% is clearly indicative of a problematic TLD.

European ccTLDs take the spotlight this reporting period with significant increases for .uk (United Kingdom, +187%), .eu (European Union, +132%), and .de (Germany, +117%). Much of the .eu domain activity appears to be spam-related, while the rise in .de listings

is largely due to phishing campaigns. Meanwhile, .uk domains include a large number of numeric-only domain names, likely linked to Chinese domain squatters, as well as casino-related domains.

Seven new ccTLDs entered the Top 20 this reporting period: .br (Brazil, #5), .ua (Ukraine, #7), .cz (Czech Republic, #9), .ng (Nigeria, #14), .io (British Indian Ocean Territory, #18), .tr (Turkey, #19) and .nl (The Netherlands, #20). The appearance of .io as a new entry is consistent with its growth in new domain registrations.

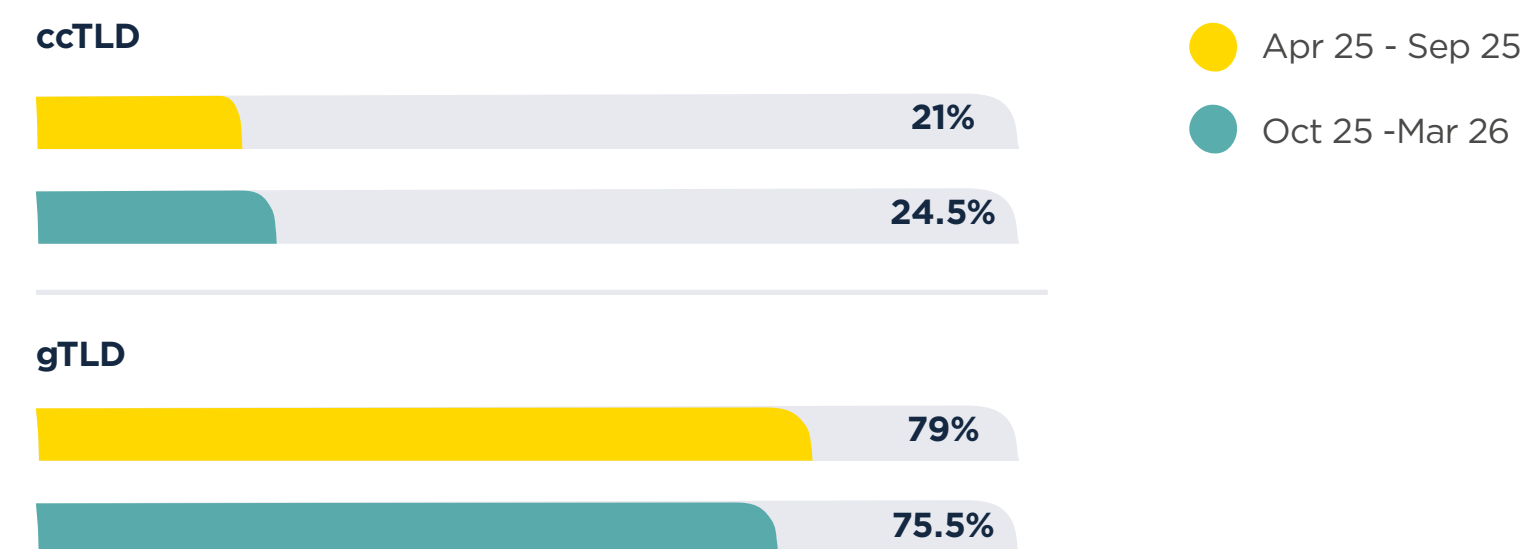
i Interpreting the data ✕

Registries with a greater number of active domains have greater exposure to abuse. For example, between October 2025 and March 2026, .cyou had more than 455,000 domains in its zone, of which 4% were listed.

Meanwhile, .qpon had just over 67,000 domains in its zone, with 12% listed in our domain dataset. Both are in the Top 20 of our listings. Still, one had a much higher percentage of active domains listed than the other.

TLD type - six... ✕

TLD type - six month comparison



01

02

03

04

05

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

Top 20 TLDs

Rank	Domain TLD	Type of TLD	Oct 25 - Mar 26	Oct 25 - Mar 26 data bar	Apr 25 - Sep 25	% Change
1	.com	gTLD	506,482		813,514	▼ -38%
2	.top	gTLD	270,121		577,797	▼ -53%
3	.cn	ccTLD	252,852		317,707	▼ -20%
4	.cc	ccTLD	94,415		216,942	▼ -56%
5	.cfd	gTLD	93,940		24,760	▲ 279%
6	.bond	gTLD	59,271		68,171	▼ -13%
7	.ru	ccTLD	54,612		32,492	▲ 68%
8	.shop	gTLD	52,350		54,565	▼ -4%
9	.vip	gTLD	51,280		126,458	▼ -59%
10	.asia	gTLD	48,766		-	New entry
11	.xyz	gTLD	47,547		39,660	▲ 20%
12	.icu	gTLD	46,350		60,407	▼ -23%
13	.net	gTLD	43,593		47,754	▼ -9%
14	.sbs	gTLD	42,115		41,029	▲ 3%
15	.info	gTLD	37,786		28,353	▲ 33%
16	.org	gTLD	31,057		29,166	▲ 6%
17	.click	gTLD	24,004		21,687	▲ 11%
18	.online	gTLD	23,528		-	New entry
19	.cyou	gTLD	18,291		52,009	▼ -65%
20	.pro	gTLD	17,005		79,617	▼ -79%

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

Top 20 ccTLDs

Rank	Domain TLD	Oct 25 - Mar 26	Oct 25 - Mar 26 data bar	Apr 25 - Sep 25	% Change
1	.cn	252,852		317,707	▼ -20%
2	.cc	94,415		216,942	▼ -56%
3	.ru	54,612		32,492	▲ 68%
4	.my	14,669		36,443	▼ -60%
5	.br	11,599		-	New entry
6	.de	9,678		4,459	▲ 117%
7	.ua	6,803		-	New entry
8	.uk	6,687		2,334	▲ 187%
9	.cz	6,394		-	New entry
10	.eu	6,080		2,619	▲ 132%
11	.co	5,662		15,247	▼ -63%
12	.me	4,278		7,862	▼ -46%
13	.id	3,652		1,602	▲ 128%
14	.ng	3,159		-	New entry
15	.us	2,981		4,009	▼ -26%
16	.pl	2,645		2,961	▼ -11%
17	.in	2,406		1,676	▲ 44%
18	.io	2,194		-	New entry
19	.tr	2,157		-	New entry
20	.nl	1,952		-	New entry

01

Top 20 gTLD

Rank	Domain TLD	Oct 25 - Mar 26	Oct 25 - Mar 26 data bar	Apr 25 - Sep 25	% Change
1	.com	506,482		813,514	▼ -38%
2	.top	270,121		577,797	▼ -53%
3	.cfd	93,940		24,760	▲ 279%
4	.bond	59,271		68,171	▼ -13%
5	.shop	52,350		54,565	▼ -4%
6	.vip	51,280		126,458	▼ -59%
7	.xyz	47,547		39,660	▲ 20%
8	.icu	46,350		60,407	▼ -23%
9	.net	43,593		47,754	▼ -9%
10	.sbs	42,115		41,029	▲ 3%
11	.info	37,786		28,353	▲ 33%
12	.org	31,057		29,166	▲ 6%
13	.click	24,004		21,687	▲ 11%
14	.online	23,528		-	New entry
15	.cyou	18,291		52,009	▼ -65%
16	.pro	17,005		79,617	▼ -79%
17	.biz	15,078		-	New entry
18	.live	13,245		21,251	▼ -38%
19	.site	12,530		-	New entry
20	.life	12,204		20,485	▼ -40%

02

03

04

05

Top 20 gTLDs by % of zone file

Rank	Domain TLD	Oct 25 - Mar 26	Zone size	% of zone listed	% of zone data bar
1	.cfd	93,940	535,716	17.54%	
2	.qpon	8,157	67,024	12.17%	
3	.icu	46,350	476,188	9.73%	
4	.bid	3,278	38,586	8.50%	
5	.xin	4,931	62,251	7.92%	
6	.mom	3,975	52,811	7.53%	
7	.wiki	5,530	80,798	6.84%	
8	.bond	59,271	1,147,185	5.17%	
9	.loan	2,867	65,285	4.39%	
10	.help	6,721	163,001	4.12%	
11	.food	1,080	26,283	4.11%	
12	.cyou	18,291	455,512	4.02%	
13	.pizza	453	11,376	3.98%	
14	.forum	2,549	74,232	3.43%	
15	.rest	2,776	81,230	3.42%	
16	.click	24,004	732,673	3.28%	
17	.ink	3,609	111,597	3.23%	
18	.vip	51,280	1,632,292	3.14%	
19	.life	12,204	407,624	2.99%	
20	.sbs	42,115	1,414,674	2.98%	

01

●●● Trending terms... ✕

Trending phishing terms for malicious or suspicious domains

Trending phishing terms have changed significantly once again, with a high number of new entries in the Top 20. Over the past six months, 11 new terms have entered the rankings, while previously prominent toll scam-related keywords have dropped out completely, including: tollbill, ov-pay and park-.

Whatsapp is the top new entry, debuting at #1 with 24,640 domains, suggesting increased impersonation of this messaging platform.

Although, it's casino (+122%) that shows the strongest growth among existing terms, reinforcing the popularity of gambling-related phishing infrastructure. This is further supported by new entries jojobet (#15), casibom (#17), and holiganbet (#19) — all Turkish casinos.

There is a clear rise in Turkish-language phishing activity, with terms guncel (current), giris (entrance/login) and adresi (address) featuring in the Top 20 between October 2025 - March 2026. Approximately two-thirds of these domains use the .com TLD, with the remaining third using .vip. The consistent TLD distribution across multiple Turkish terms suggests a single threat actor.

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".



01

Top 20 phishing terms

Rank	Term	Oct 25 - Mar 26	Oct 25 - Mar 26 data bar	Apr 25 - Sep 25	% Change
1	whatsapp	24,640		-	New entry
2	casino	6,473		2,913	▲ 122%
3	secure	4,130		3,619	▲ 14%
4	login	4,024		5,113	▼ -21%
5	portal	3,985		-	New entry
6	online	3,977		3,221	▲ 23%
7	guncel	3,807		-	New entry
8	giris	3,620		-	New entry
9	tracking	3,410		-	New entry
10	oferta	3,377		3,009	▲ 12%
11	service	3,286		5,490	▼ -40%
12	support	3,049		3,470	▼ -12%
13	wallet	3,023		2,517	▲ 20%
14	verify	2,832		2,419	▲ 17%
15	jojobet	2,787		-	New entry
16	adresi	2,545		-	New entry
17	casibom	2,519		-	New entry
18	signin	2,106		-	New entry
19	holiganbet	2,027		-	New entry
20	reward	1,995		-	New entry

02

03

04

05

Phishing terms



01

● ● ● Types of abuse



Types of abuse

Over the last six months, compromised domains associated with botnet C&Cs saw a significant +665% increase, while malware and phishing also experienced increases of +238% and +140% respectively. As [highlighted in the April - September 2025 report](#), these increases are largely driven by increased contributions from the [abuse.ch](#) community platforms.

In terms of malicious domains, those associated with botnet C&C's increased by a further +289% and malware by +206%, an ongoing impact of improved detection capabilities and industry partnerships.

02

03

04

05



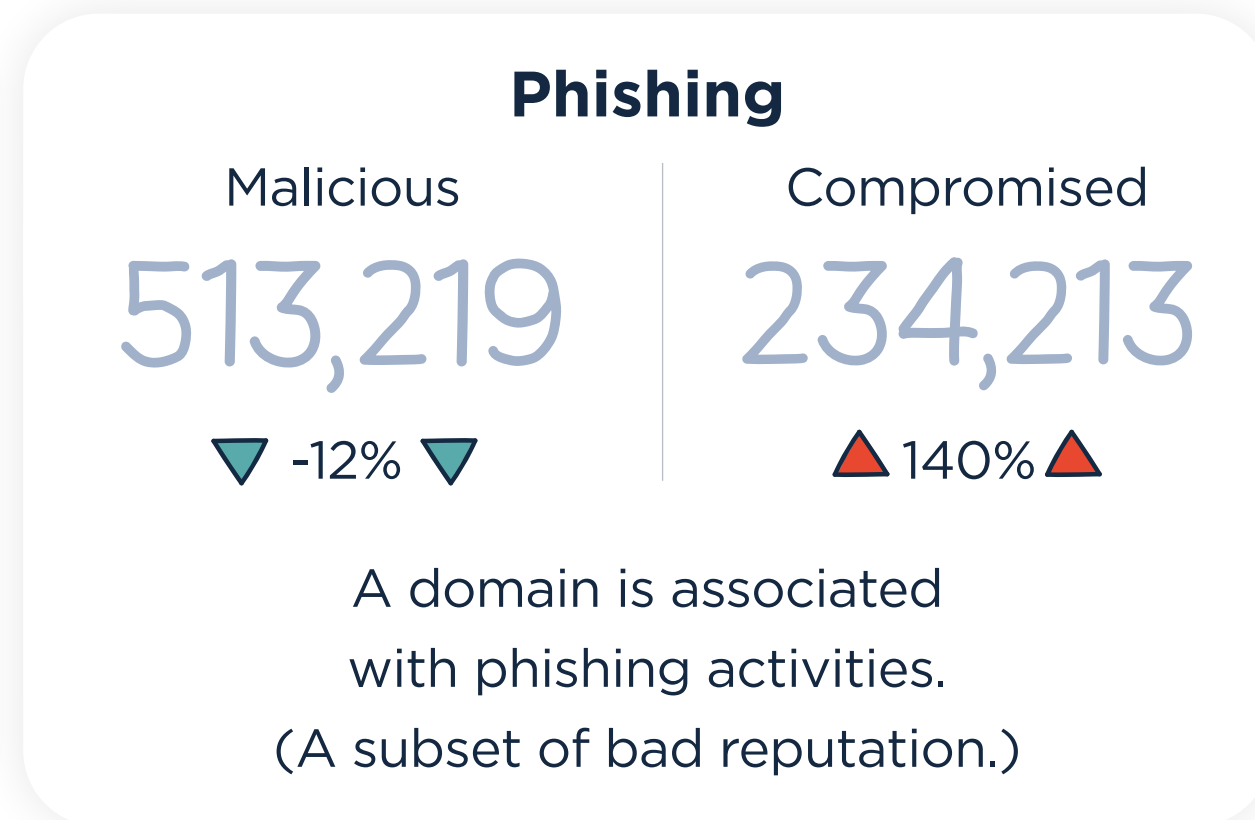
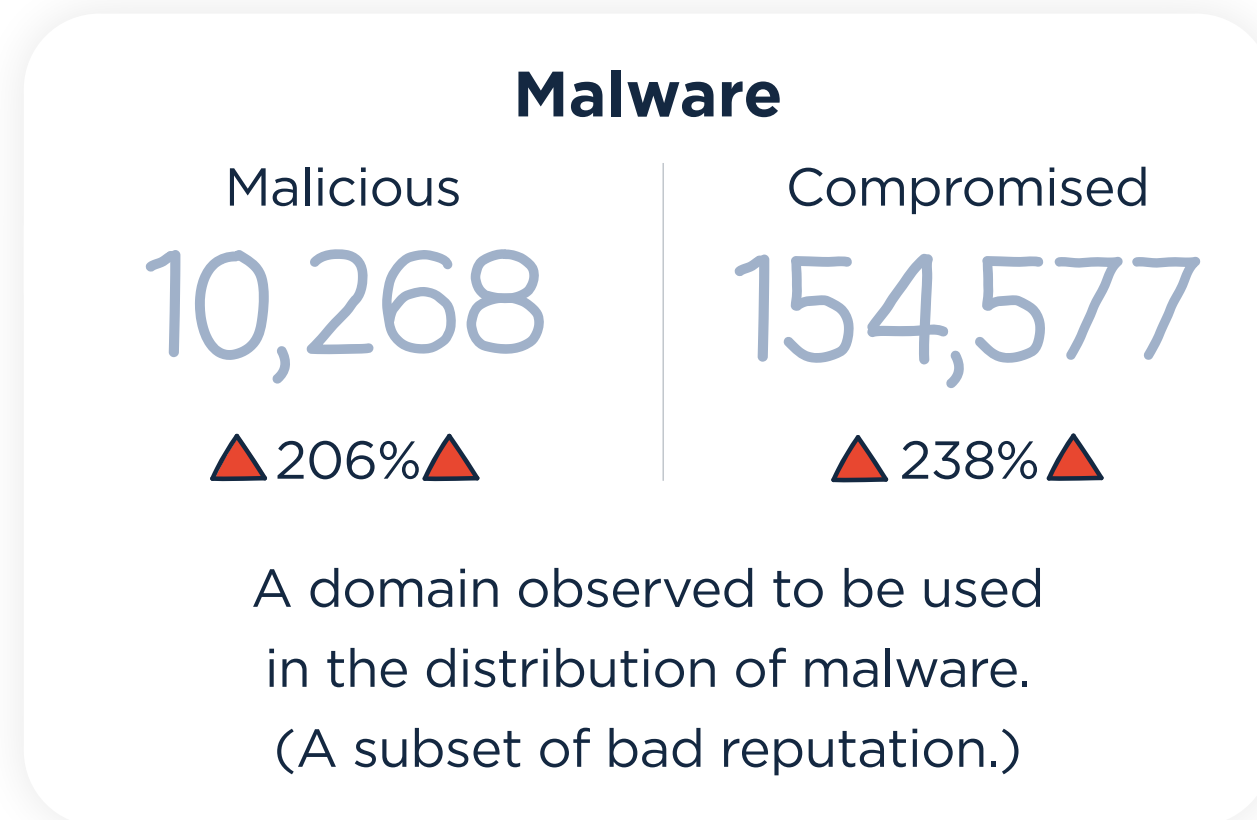
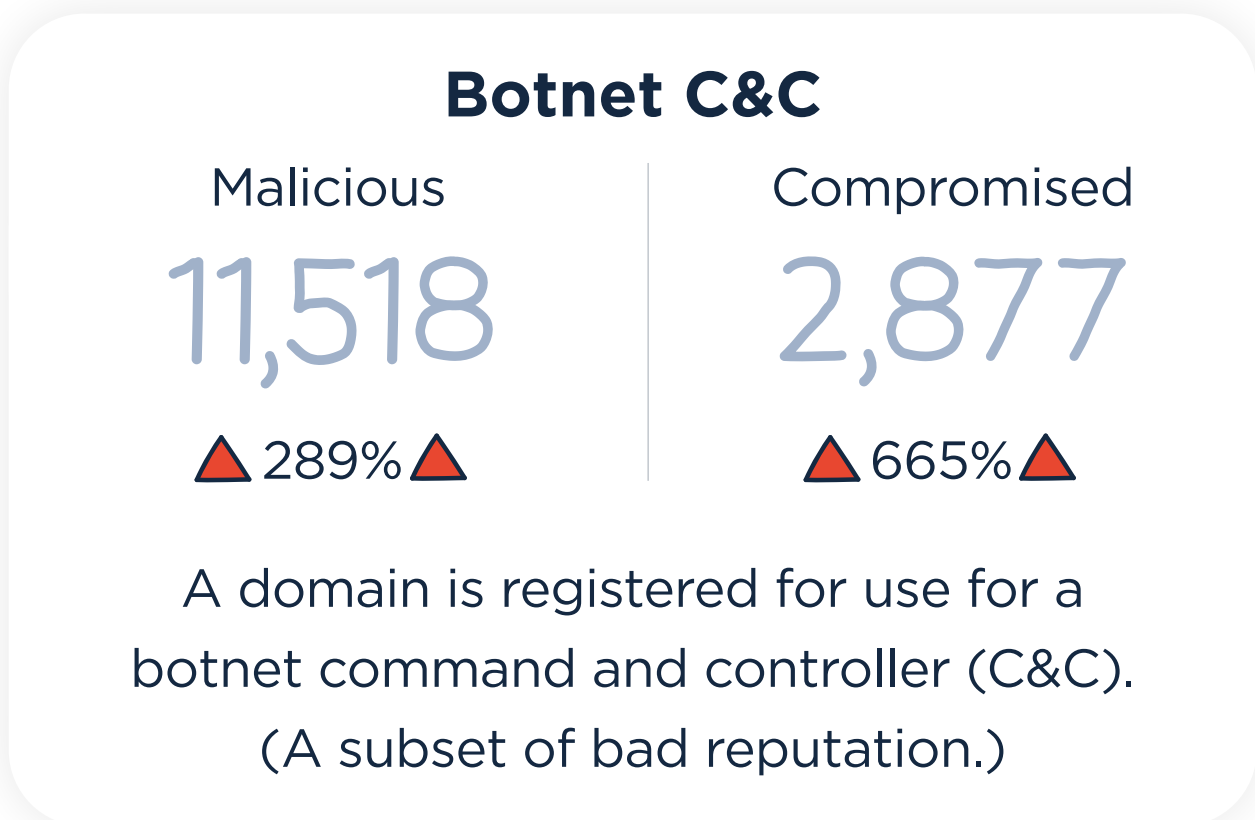
Differences between compromised and malicious domains



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

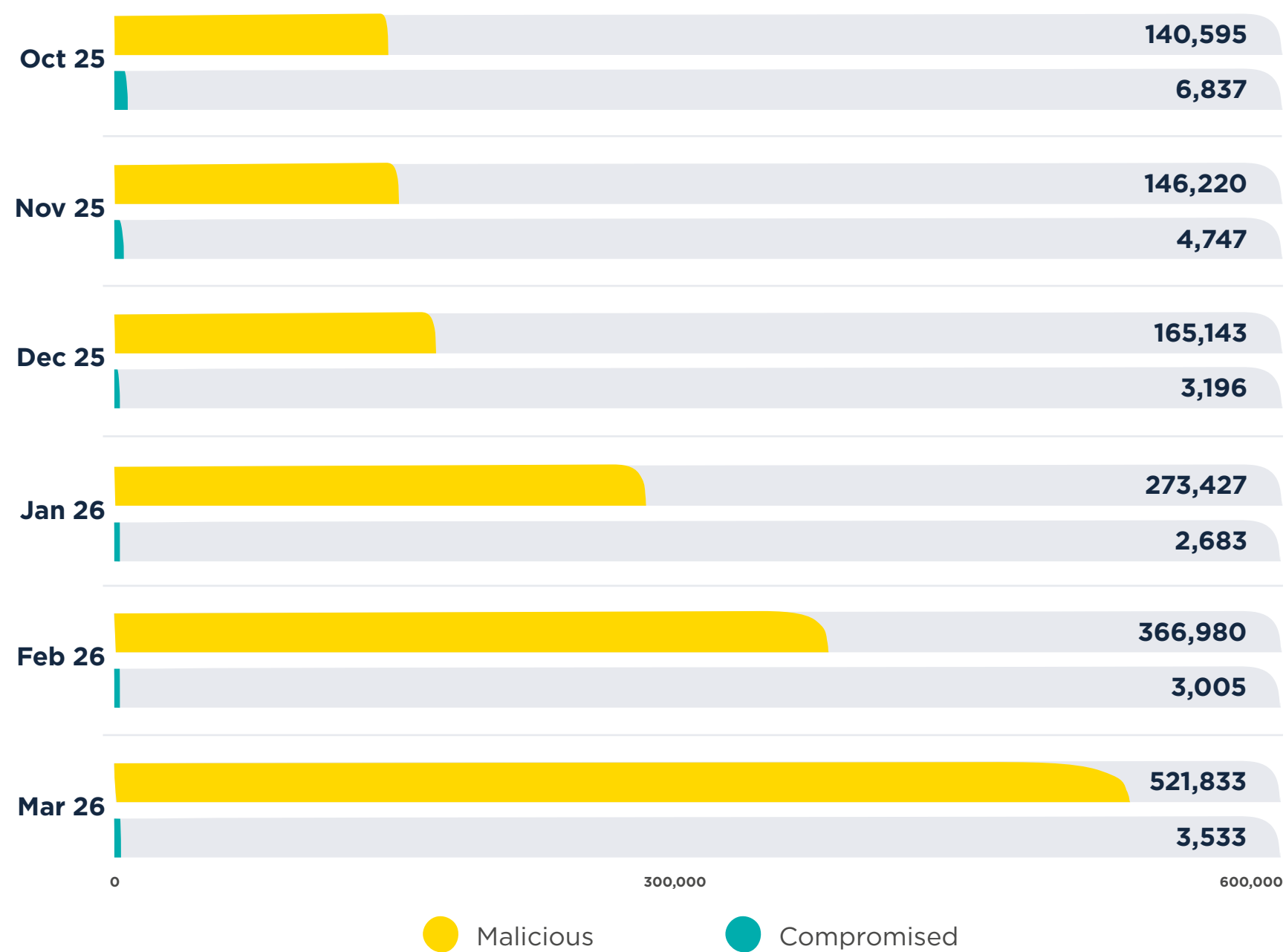
03

04

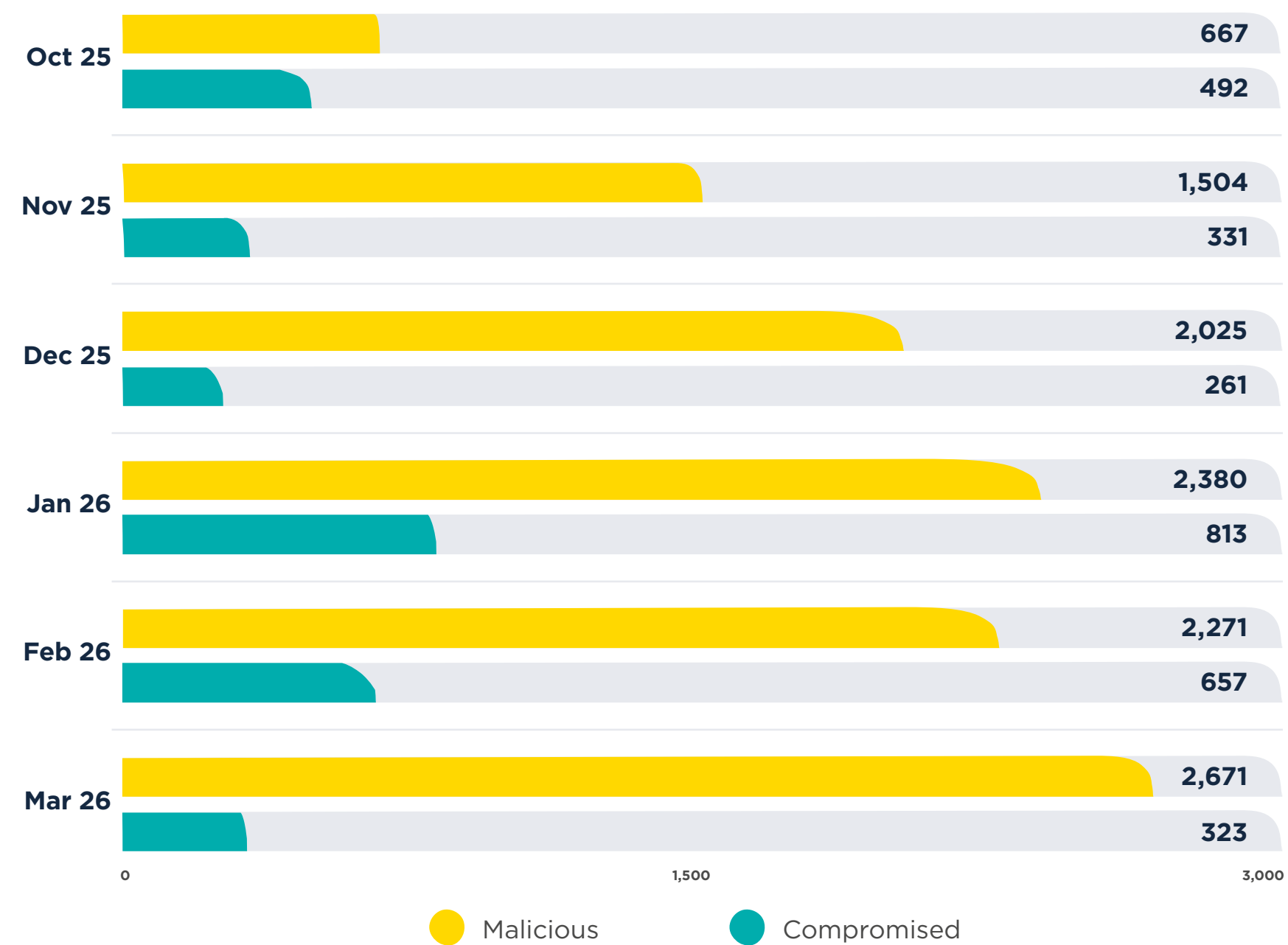
05

Types of abuse per month

Bad reputation per month



Botnet C&C per month



01

02

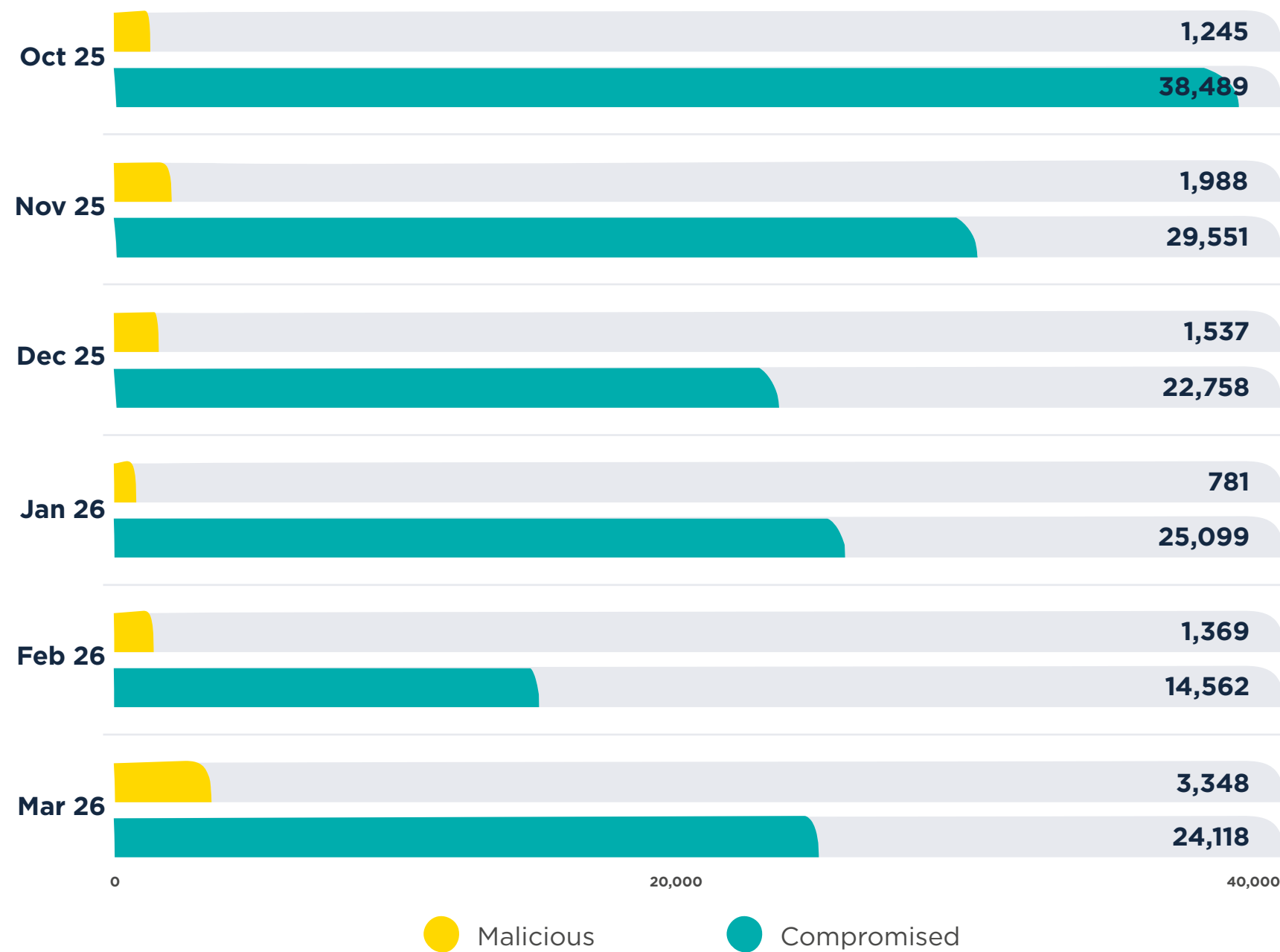
03

04

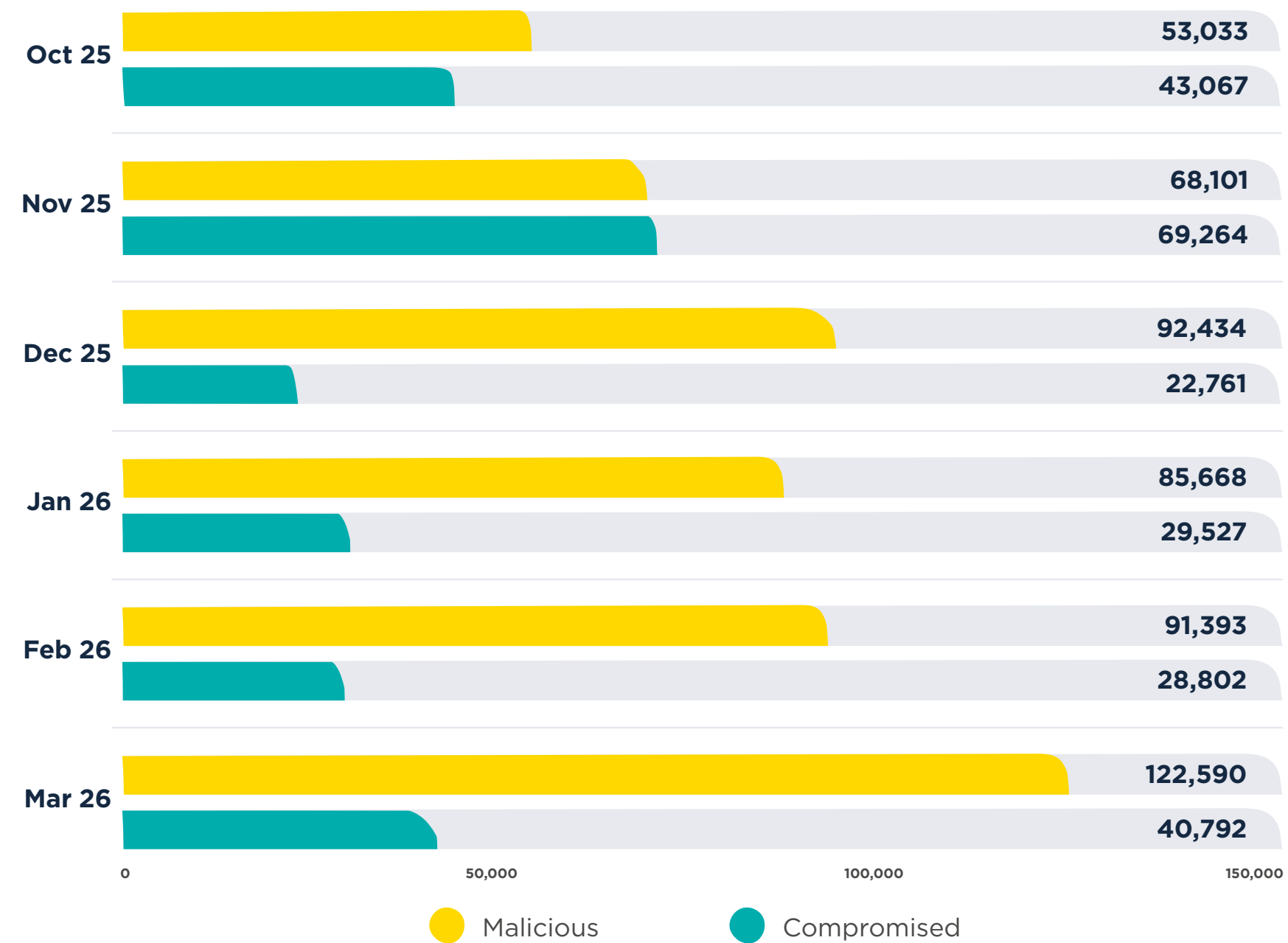
05

Types of abuse per month

Malware per month



Phishing per month



01

02

03

04

05

Recommendations

With new policy on the horizon, and recognising that change takes time, here are specific actions that registrars, registries, and defenders alike can adopt in the meantime.

Trust your gut: look for associated domains

If you've taken action against a malicious domain, and there's reason to believe that associated domains may exist, identify these domains, and determine if they are also malicious. These checks could be based on naming patterns, infrastructure similarities, or hosting the same content. If the associated domains look like they are - or will be - used for abusive activity, then they too should be actioned.

Share data and collaborate

When it comes to reports of abuse, unusual registration patterns, and reuse of infrastructure, registries and registrars need to work together, share data and collaborate - even more so in reseller models. Having a clear process for reporting and escalations can go a long way to help registries overcome the lack of direct customer relationships.

Correlate domains using all available intelligence

Defenders should not rely on single-domain assessments. Enrich assessments with external intelligence to build a more complete picture. Use all available signals to correlate domains and prioritise further investigations based on indicators of abuse, such as domain clustering, or unusual behavioral patterns.

Champion new policy!

Introducing change is never easy and will always be met with resistance and barriers. Requiring registrars to check associated domains will mean new processes, additional resources, and investment. However, measures like this are necessary to improve the visibility of abusive activity. Ultimately, all stakeholders need to prioritise strengthening abuse detection and mitigation.

Follow us on socials!

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

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