SPAMHAUS

Spamhaus Domain Reputation Update

Oct 2023 - Mar 2024

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

Welcome to the Spamhaus Domain Reputation Update Oct 23 - Mar 24.

Enter

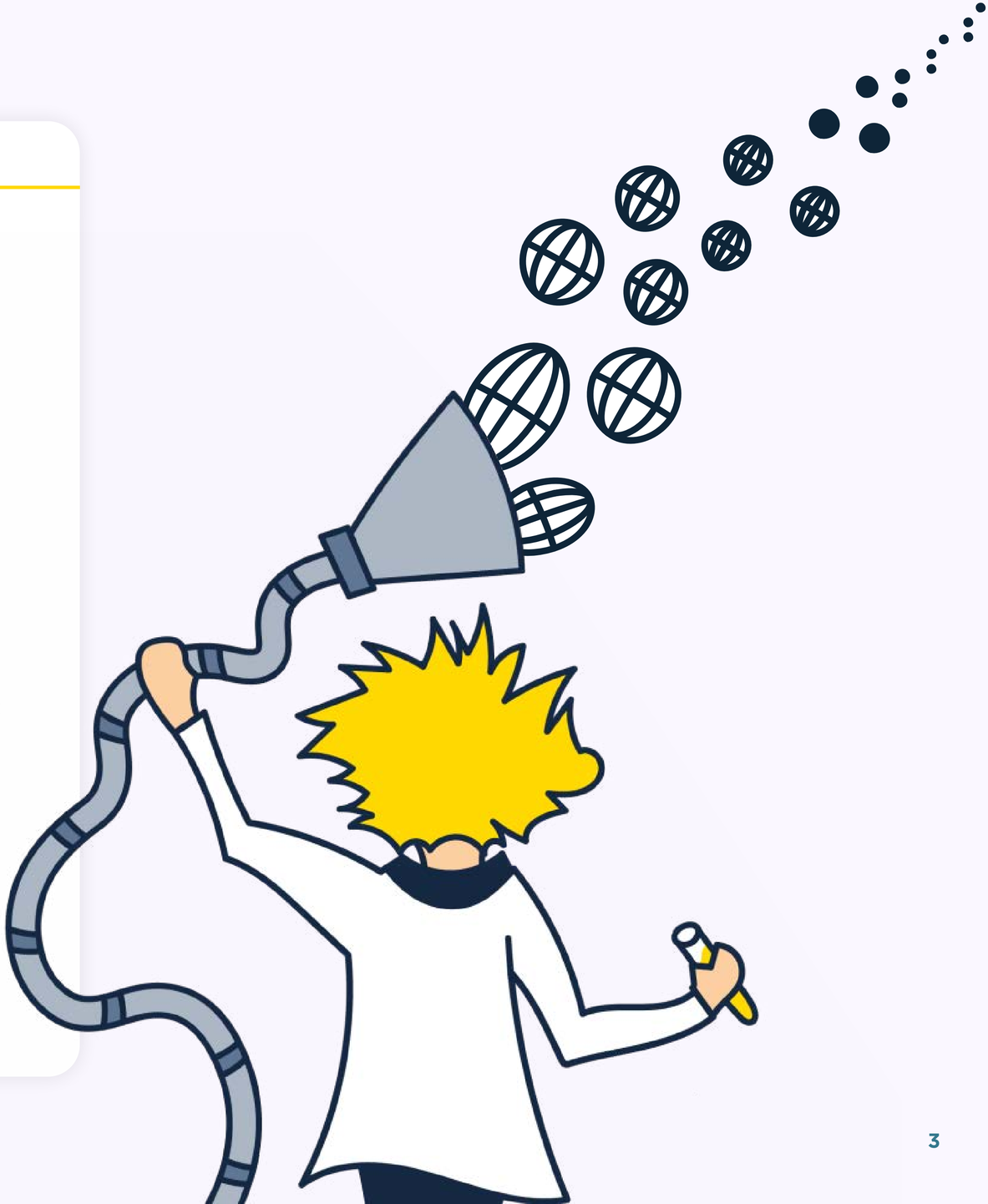
Contents

The Overview

This is a report of two tales – changes observed with individual TLDs, and updates across the broader TLD ecosystem. On the former, this period saw .io becoming increasingly popular among tech (and, nowadays, generative AI) startups. Could this be due to the recent rise of AI? Possibly. However, as the price per domain has dropped considerably, we also detect more .io domains being used for nefarious purposes – a pattern we're quite familiar with.

Other 'new' TLDs observed as associated with malicious domains follow a similar pattern: almost all, without fail, are cheap. This affordability enables bulk buying, shielding domain owners from the risk of their domains being flagged, blocked, or taken down. Consequently, this paves the way for various forms of abuse that would otherwise not be scalable. We will continue to emphasize that this systemic issue is a breeding ground for large-scale (DNS) abuse.

Overview continued



Overview cont.

The other story focuses on the TLD ecosystem. We often observe the same behavior happening across multiple TLDs. Most threat actors don't care which TLD their domains reside in; they're willing to buy anything that will keep their operations live while not having to disclose their true identities. Bonus points if these domains are cheap or can be purchased 'offshore.'

However, for this reporting period, after over a decade of serial abuse of free domains, Freenom's exit was a real high point. Sadly, this was not the result of responsible action taken by registries and registrars, or increased regulation. 'All' it took was a lawsuit from a powerful social media company, which made it more expensive (than free!) to enable domain name-based abuse. As a result – goodbye to Freenom TLDs in this report. If we can continue the trend of making abuse more expensive, there may be hope yet!

New domains | Number of new...

New domains

New domains overview

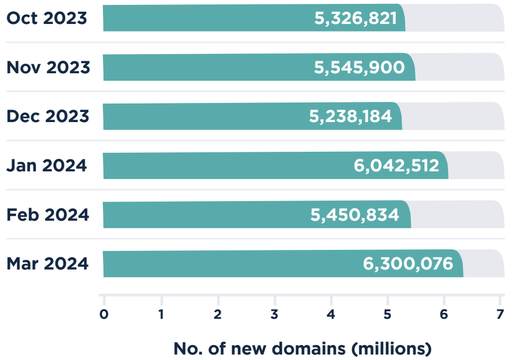
Almost 34 million new domains were registered over the last six months, averaging 5.6 million new registrations per month. Compared with the previous year, the numbers are slightly lower due to Freenom's endless stream of free domains finally coming to a stop. Whether used for good or bad, any price other than zero seems to act as a deterrent for registering nefarious domains.

When looking at domain registrations over the holiday season, the usual peak was less visible this year. One possible explanation for this shift is that smaller, lifestyle-oriented businesses are now opting to set up shops on platforms like Instagram, rather than investing in an e-commerce website. It will be interesting to see if this trend continues into the coming holiday season.

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

33,904,327

◀ 0% ▶

Monthly Average

5,650,721

▲ 41,531 ▲

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.

New domains... TLD types...

New domains by top-level domain (TLD)

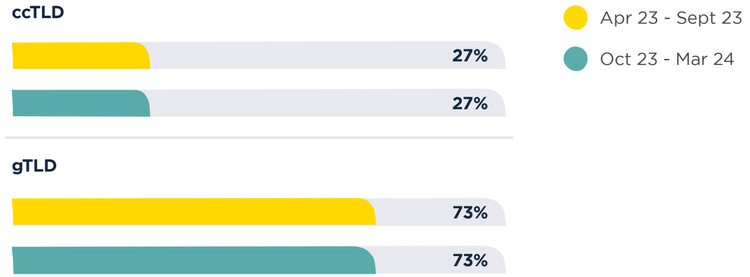
Over the last six months, the percentage of ccTLDs has remained at 27%. Although the disappearance of free domains from a particular provider will undoubtedly impact registrations, there is evidence of gTLD-like ccTLDs, such as .io (the TLD for the British Indian Ocean Territory), becoming increasingly popular.

As with ccTLDs, the percentage of new gTLD registrations also remained unchanged at 73%. This high figure could be attributed to the global appeal of certain gTLD domain names, despite their focus on the English language. However, we believe that ease of registration and price per domain are the key factors driving the popularity of gTLDs.

One interesting entry is .ru (#3). It is quite remarkable how this ccTLD has increased by 26% despite the ever-increasing regulation of everything internet-related within Russia. The current geopolitical situation can explain this, however: While sanctions make it more difficult for outsiders to conduct business with Russia, it's also more difficult for Russians to conduct business with the rest of the world. As a result, Russians who need domains are more likely to purchase .ru domains, regardless of whether they like it or not.

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	Oct 23 - Mar 24	Oct 23 - Mar 24 data bar	Apr 23 - Sept 23	% Change
1	.com	gTLD	11,639,454		12,287,433	▼ -5%
2	.shop	gTLD	1,377,092		719,770	▲ 91%
3	.online	gTLD	1,067,222		1,151,573	▼ -7%
4	.xyz	gTLD	987,598		1,002,755	▼ -2%
5	.net	gTLD	830,805		735,907	▲ 13%
6	.top	gTLD	823,320		1,178,132	▼ -30%
7	.org	gTLD	729,065		682,957	▲ 7%
8	.site	gTLD	680,511		597,990	▲ 14%
9	.cn	ccTLD	646,482		427,707	▲ 51%
10	.de	ccTLD	621,992		664,411	▼ -6%
11	.ru	ccTLD	615,020		489,027	▲ 26%
12	.store	gTLD	595,228		528,679	▲ 13%
13	.bond	gTLD	557,932		-	New entry
14	.co.uk	ccTLD	502,739		456,566	▲ 10%
15	.com.br	ccTLD	480,118		436,909	▲ 10%
16	.sbs	gTLD	424,338		-	New entry
17	.co	ccTLD	396,904		442,532	▼ -10%
18	.fr	ccTLD	351,893		321,149	▲ 10%
19	.info	gTLD	351,338		349,348	▲ 1%
20	.in	ccTLD	333,679		354,939	▼ -6%

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

Top 20 ccTLDs used in new domains

Rank	New domain TLD	Oct 23 - Mar 24	Oct 23 - Mar 24 data bar	Apr 23 - Sept 23	% Change
1	.cn	646,482		427,707	▲ 51%
2	.de	621,992		664,411	▼ -6%
3	.ru	615,020		489,027	▲ 26%
4	.co.uk	502,739		456,566	▲ 10%
5	.com.br	480,118		436,909	▲ 10%
6	.co	396,904		442,532	▼ -10%
7	.fr	351,893		321,149	▲ 10%
8	.in	333,679		354,939	▼ -6%
9	.nl	321,826		382,051	▼ -16%
10	.ca	275,314		263,420	▲ 5%
11	.cc	258,567		252,316	▲ 2%
12	.us	210,435		217,146	▼ -3%
13	.com.au	208,724		218,278	▼ -4%
14	.eu	200,988		180,075	▲ 12%
15	.it	189,547		154,673	▲ 23%
16	.pl	175,597		218,362	▼ -20%
17	.io	149,745		-	New entry
18	.com.tr	146,900		-	New entry
19	.es	140,831		140,548	▶ 0%
20	.ir	139,670		122,990	▲ 14%

Top20 gTLD - new | Top20 gTLDs - zone

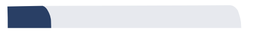
Top 20 gTLDs used in new domains

Rank	New domain TLD	Oct 23 - Mar 24	Oct 23 - Mar 24 data bar	Apr 23 - Sept 23	% Change
1	.com	11,639,454		12,287,433	▼ -5%
2	.shop	1,377,092		719,770	▲ 91%
3	.online	1,067,222		1,151,573	▼ -7%
4	.xyz	987,598		1,002,755	▼ -2%
5	.net	830,805		735,907	▲ 13%
6	.top	823,320		1,178,132	▼ -30%
7	.org	729,065		682,957	▲ 7%
8	.site	680,511		597,990	▲ 14%
9	.store	595,228		528,679	▲ 13%
10	.bond	557,932		225,227	▲ 148%
11	.sbs	424,338		156,018	▲ 172%
12	.info	351,338		349,348	▲ 1%
13	.lol	260,161		-	New entry
14	.vip	258,415		198,647	▲ 30%
15	.cfd	216,974		844,417	▼ -74%
16	.click	177,547		295,636	▼ -40%
17	.icu	171,208		201,522	▼ -15%
18	.cyou	164,704		-	New entry
19	.pro	161,626		-	New entry
20	.fun	160,391		147,598	▲ 9%

Top20 gTLD - new | Top20 gTLDs - zone

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

Rank	New domain TLD	Oct 23 - Mar 24	Zone size	% of zone newly observed	% of zone data bar
1	.bond	557,932	265,018	210.53%	
2	.lol	260,161	238,928	108.89%	
3	.bot	9,224	11,385	81.02%	
4	.sbs	424,338	573,687	73.97%	
5	.rip	13,999	19,033	73.55%	
6	.cyou	164,704	227,098	72.53%	
7	.tokyo	100,360	187,737	53.46%	
8	.skin	26,614	51,232	51.95%	
9	.shop	1,377,092	2,693,833	51.12%	
10	.pics	31,994	62,644	51.07%	
11	.lat	71,267	140,905	50.58%	
12	.ing	19,107	38,052	50.21%	
13	.today	139,255	281,175	49.53%	
14	.quest	20,705	44,437	46.59%	
15	.rest	8,118	17,523	46.33%	
16	.autos	19,366	44,052	43.96%	
17	.site	680,511	1,576,781	43.16%	
18	.yachts	4,876	11,340	43.00%	
19	.boats	6,319	15,000	42.13%	
20	.mom	18,646	45,006	41.43%	



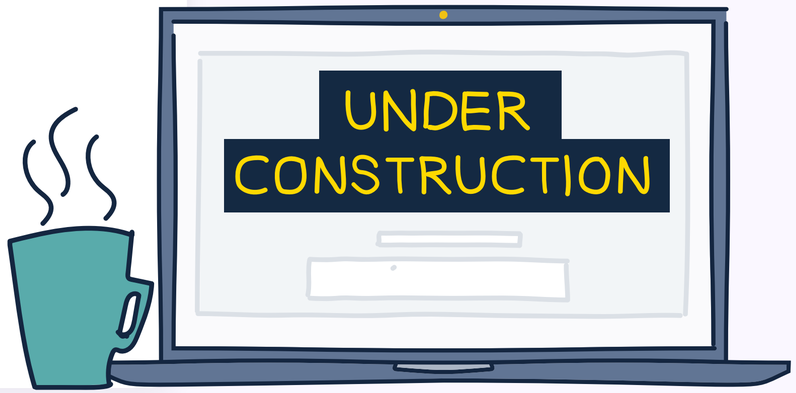
Trending terms in new domains

One of the most surprising changes in trending terms this period is in domains containing the word ‘casino’ – a new entry at #12, as shown on page 10. The increasingly open market for online gambling across parts of Europe could be one explanation. Although, 70,000 new domains containing the word ‘casino’ is puzzling since it seems unlikely that so many casinos opened in the last six months!

As the job market in many countries remains constrained, it is unsurprising to see new entry ‘jobs’. However, like casinos, there are unlikely to be 70,000 new job platforms... Instead, it is entirely plausible that many of these domains are used for SEO purposes, therefore adding little to the overall ecosystem.

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	Oct 23 - Mar 24 trending terms	Oct 23 - Mar 24	Oct 23 - Mar 24 data bar	Apr 23 - Sept 23	% Change
1	service	231,943		202,802	▲ 14%
2	online	174,054		152,222	▲ 14%
3	solution	149,273		135,523	▲ 10%
4	design	138,133		131,310	▲ 5%
5	digital	136,266		118,865	▲ 15%
6	market	129,044		136,076	▼ -5%
7	studio	126,593		116,847	▲ 8%
8	group	124,565		111,391	▲ 12%
9	consult	119,380		105,104	▲ 14%
10	store	111,476		114,521	▼ -3%
11	health	106,871		105,040	▲ 2%
12	casino	73,812		-	New entry
13	global	73,498		67,791	▲ 8%
14	jobs	72,853		-	New entry
15	marketing	69,718		42,011	▲ 66%
16	travel	67,314		66,995	▶ 0%
17	creation	66,312		-	New entry
18	cleaning	64,017		-	New entry
19	invest	61,427		50,224	▲ 22%
20	company	59,304		-	New entry

Top 20 Trending... | Trending terms

Trending terms

Malicious/suspici... | Listings

Malicious/suspicious domains

Domain Overview

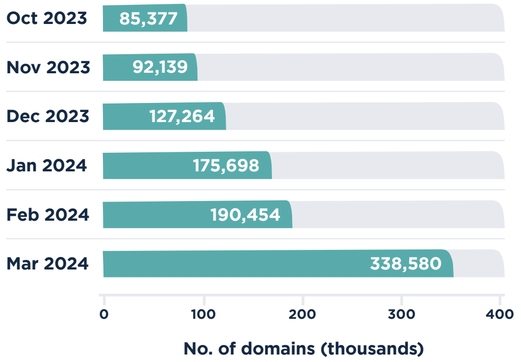
Over the past six months, we've detected over 1 million malicious or suspicious domains, averaging approximately 168K per month. This represents a welcomed 21% decrease compared to the previous six months (April 2023 to September 2023).

Before we dive into the details, it is important to note that these numbers include a period of technical transition to an upgraded platform. Due to the migration, the figures reported in the first three months may appear lower than expected. This is due to underreporting to ensure the upgraded platform correctly classified "bad" domains.

This was a one-time event that will only affect this report.

Malicious/suspi... | Listings

Number of Domain listings per month



Six Month Total

1,009,512

▼ -21% ▼

Monthly Average

168,252

▼ -43,805 ▼

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

Two TLDs stood out in this report: .cn (#3) and .lol (#11). The number of listings for both TLDs were heavily influenced by a single Chinese threat actor targeting Japanese brands and payment platforms like Suica and Pasmo. However, thanks to the swift action of the .xyz registry, the threat actor has been successfully disabled and has now relocated to .asia. It remains to be seen how this move will impact .asia.

This will likely be the last time Freenom and their controversial free TLDs are mentioned in the domain report. With Freenom's departure from the domain registration business (taking 20 million domain names with them!), a significant number of domains with bad reputation have disappeared for good.

And due to the increased cost of any alternatives, the actual number of malicious or fraudulent domain registrations will be lower. However, that does not mean the amount of internet abuse will also decrease.

With that, please take note of the following:

- Most malware relies on relatively new domains. Even though the risk of new domain names is well understood, these domains often only appear in DNS traffic, where domain-based reputation is less common than, for example, in the email ecosystem.
- SMS-based phishing and scams are increasingly buying large batches of short domain names. While the domains used are often borderline gibberish, most recipients skip searching for meaningful names within texts due to the limited characters allowed.

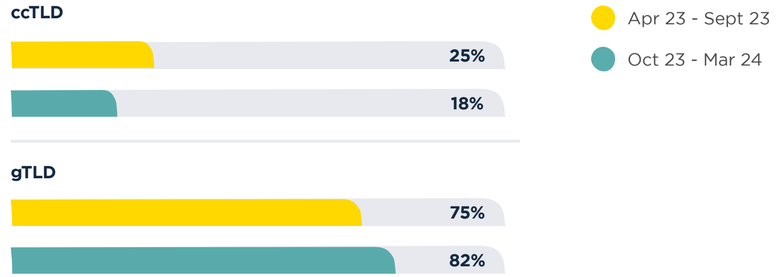
Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, between October 2023 and March 2024 .vip had more than 887,000 domains in its zone, of which 1.92% were detected to be malicious or suspicious.

Meanwhile, .rip had just over 19,000 domains in its zone, with 5.17% 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	Oct 23 - Mar 24	Oct 23 - Mar 24 data bar	Apr 23 - Sept 23	% Change
1	.com	gTLD	343,299		468,898	▽ -27%
2	.top	gTLD	86,718		65,915	△ 32%
3	.cn	ccTLD	70,279		92,885	▽ -24%
4	.xyz	gTLD	64,650		28,762	△ 125%
5	.net	gTLD	34,093		33,765	△ 1%
6	.ru	ccTLD	26,856		14,526	△ 85%
7	.sbs	gTLD	26,564		-	New entry
8	.shop	gTLD	22,542		-	New entry
9	.online	gTLD	22,285		21,275	△ 5%
10	.info	gTLD	21,079		44,123	▽ -52%
11	.lol	gTLD	20,119		-	New entry
12	.org	gTLD	19,614		12,837	△ 53%
13	.cc	ccTLD	19,228		-	New entry
14	.vip	gTLD	17,080		-	New entry
15	.cfd	gTLD	14,967		20,924	▽ -28%
16	.site	gTLD	12,859		21,126	▽ -39%
17	.club	gTLD	12,791		-	New entry
18	.tk	ccTLD	9,064		26,907	▽ -66%
19	.life	gTLD	8,290		-	New entry
20	.bond	gTLD	8,054		-	New entry

0 200 400

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

Top 20 ccTLDs

Rank	Domain TLD	Oct 23 - Mar 24	Oct 23 - Mar 24 data bar	Apr 23 - Sept 23	% Change
1	.cn	70,279		92,885	▽ -24%
2	.ru	26,856		14,526	△ 85%
3	.cc	19,228		9,474	△ 103%
4	.tk	9,064		26,907	▽ -66%
5	.co	5,771		13,473	▽ -57%
6	.us	4,807		18,749	▽ -74%
7	.me	4,308		19,713	▽ -78%
8	.uk	3,866		11,896	▽ -68%
9	.in	3,387		13,065	▽ -74%
10	.de	2,850		5,858	▽ -51%
11	.pw	2,532		7,298	▽ -65%
12	.ng	2,469		-	New entry
13	.tv	1,612		-	New entry
14	.eu	1,597		3,177	▽ -50%
15	.cf	1,402		12,024	▽ -88%
16	.gq	1,391		14,789	▽ -91%
17	.br	1,287		2,389	▽ -46%
18	.fr	1,064		3,265	▽ -67%
19	.jp	964		-	New entry
20	.io	931		-	New entry

0 25 50

01

02

03

04

05

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

Top 20 gTLD

Rank	Domain TLD	Oct 23 - Mar 24	Oct 23 - Mar 24 data bar	Apr 23 - Sept 23	% Change
1	.com	343,299		468,898	▽ -27%
2	.top	86,718		65,915	△ 32%
3	.xyz	64,650		28,762	△ 125%
4	.net	34,093		33,765	△ 1%
5	.sbs	26,564		7,429	△ 258%
6	.shop	22,542		8,531	△ 164%
7	.online	22,285		21,275	△ 5%
8	.info	21,079		44,123	▽ -52%
9	.lol	20,119		-	New entry
10	.org	19,614		12,837	△ 53%
11	.vip	17,080		8,784	△ 94%
12	.cfd	14,967		20,924	▽ -28%
13	.site	12,859		21,126	▽ -39%
14	.club	12,791		-	New entry
15	.life	8,290		6,903	△ 20%
16	.bond	8,054		-	New entry
17	.live	6,220		58,786	▽ -89%
18	.buzz	5,386		5,094	△ 6%
19	.icu	5,371		-	New entry
20	.click	4,173		8,016	▽ -48%

0 200 400

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

Top 20 gTLDs by % of zone file

Rank	Domain TLD	Oct 23 - Mar 24	Zone size	% of zone listed	% of zone data bar
1	.lol	20,119	238,928	8.42%	
2	.rip	984	19,033	5.17%	
3	.sbs	26,564	573,687	4.63%	
4	.quest	1,881	44,437	4.23%	
5	.pics	2,474	62,644	3.95%	
6	.boats	574	15,000	3.83%	
7	.yachts	414	11,340	3.65%	
8	.uno	703	19,943	3.53%	
9	.bond	8,054	265,018	3.04%	
10	.media	2,549	90,426	2.82%	
11	.baby	585	22,232	2.63%	
12	.hair	494	18,885	2.62%	
13	.support	980	38,850	2.52%	
14	.mom	1,123	45,006	2.50%	
15	.club	12,791	603,262	2.12%	
16	.beauty	688	32,987	2.09%	
17	.makeup	220	10,613	2.07%	
18	.life	8,290	405,574	2.04%	
19	.win	1,897	95,364	1.99%	
20	.vip	17,080	887,549	1.92%	

0% 2.5% 5% 7.5% 10%

Trending terms...

Trending phishing terms for malicious or suspicious domains

Eight out of twelve new entries in the Phishing Terms Top 20 relate to package delivery: login, correo, order, deliver, post, tracking, package, and amazon. This is not entirely surprising given that for most of the world, the holiday season falls within this reporting period. Even so, it is interesting to see the terms wallet (#16), apple (#16), and finance (#18) ranking lower on the list.

As more people order online (and often overseas), receiving an email about a shipping delay, additional delivery, or import costs is expected. These factors present the perfect opportunity for cybercriminals. As long as they use a well-known delivery brand name (e.g., the local postal service or any commercial shipping companies that operate in the targeted demographic), a sentence like 'the package you have been expecting' is almost guaranteed to have a much higher success rate.

People don't like waiting for deliveries, and it is this sense of urgency that cybercriminals exploit. Furthermore, it's often unclear which shipping company will deliver. If an email (and that includes the domain name) looks like it could be from a legitimate shipper, the chances of people clicking are high.

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".

Top 20 phishing... | Phishing terms

Top 20 phishing terms

Rank	Term	Oct 23 - Mar 24	Oct 23 - Mar 24 data bar	Apr 23 - Sept 23	% Change
1	service	6,582		8,230	▽ -20%
2	login	4,028		-	New entry
3	correo	3,993		-	New entry
4	online	3,692		9,005	▽ -59%
5	support	3,324		8,855	▽ -62%
6	order	3074		-	New entry
7	deliver	3,033		-	New entry
8	secure	2,942		4,771	▽ -38%
9	verify	2,458		1,268	△ 94%
10	account	2,211		11,535	▽ -81%
11	post	1,986		-	New entry
12	tracking	1,794		-	New entry
13	usps	1,543		-	New entry
14	canada	1532		-	New entry
15	cloud	1,386		5,730	▽ -76%
16	wallet	1,134		-	New entry
16	apple	1,134		8,210	▽ -86%
18	finance	1,074		-	New entry
19	package	1,011		-	New entry
20	amazon	1,009		-	New entry

0 2 4 6

Top 20 phishing... | Phishing terms

Phishing terms

Types of abuse

Without the notorious Qakbot and Emotet malware families, the practice of using compromised, legitimate domains for malware is not as prevalent as it once was before. However, other malware families have slowly emerged to fill the gap created by the absence of these giants. Currently, two campaigns stand out: Wikiloader and Latrodectus. Wikiloader relies heavily on compromised websites, whereas Latrodectus has its own dedicated domains. The methods used by these threat actors are both viable, each with unique advantages and disadvantages, from the attacker and the defensive side.

We often find that TLDs with a significant increase in detections of malicious domains run aggressive promotions during the reporting period.

Unfortunately, this pumping of zones is still common. And despite the short-term benefit, most of these domains will not be renewed at the – much higher – regular pricing. Furthermore, it opens the door to the slash-and-burn tactics of cybercriminals, who simply need a number of records in the DNS. Only a few registries have control over these registrations, promptly cancelling bad ones as soon as they are created. A strong 'Know Your Customer (KYC)' can deter malicious registrations, but unless such measures are made mandatory by registries or ICANN, we see no change in the near future.

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
702,235	439,517
▼ -4% ▼	▲ 5011% ▲

A domain's reputation score has exceeded policy limits.

Botnet C&C

Malicious	Compromised
786	11
▼ -87% ▼	▼ -96% ▼

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

Malware

Malicious	Compromised
4,264	61,932
▼ -73% ▼	▲ 407% ▲

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

Phishing

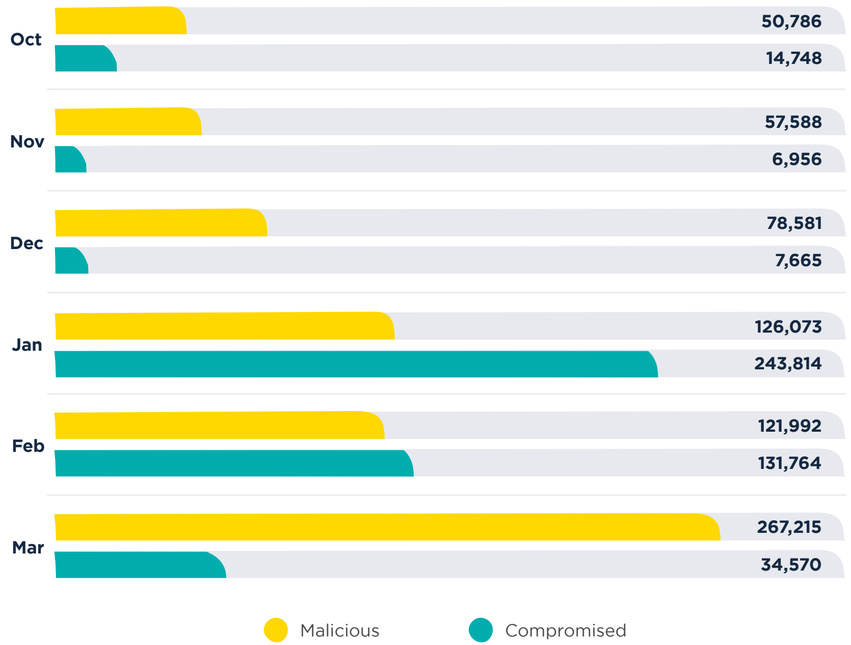
Malicious	Compromised
302,227	54,880
▼ -12% ▼	▲ 598% ▲

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

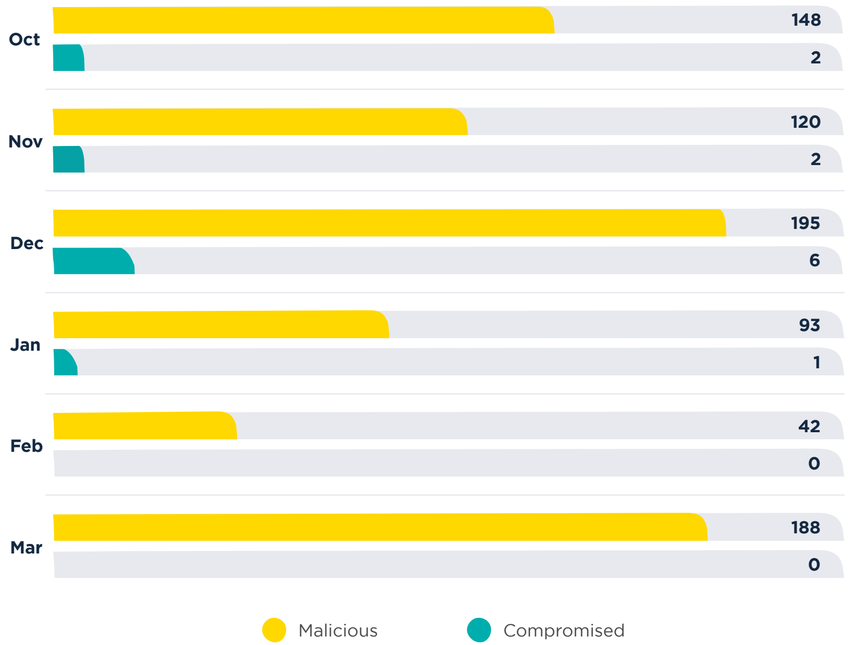
Types of abuse

Types of abuse per month

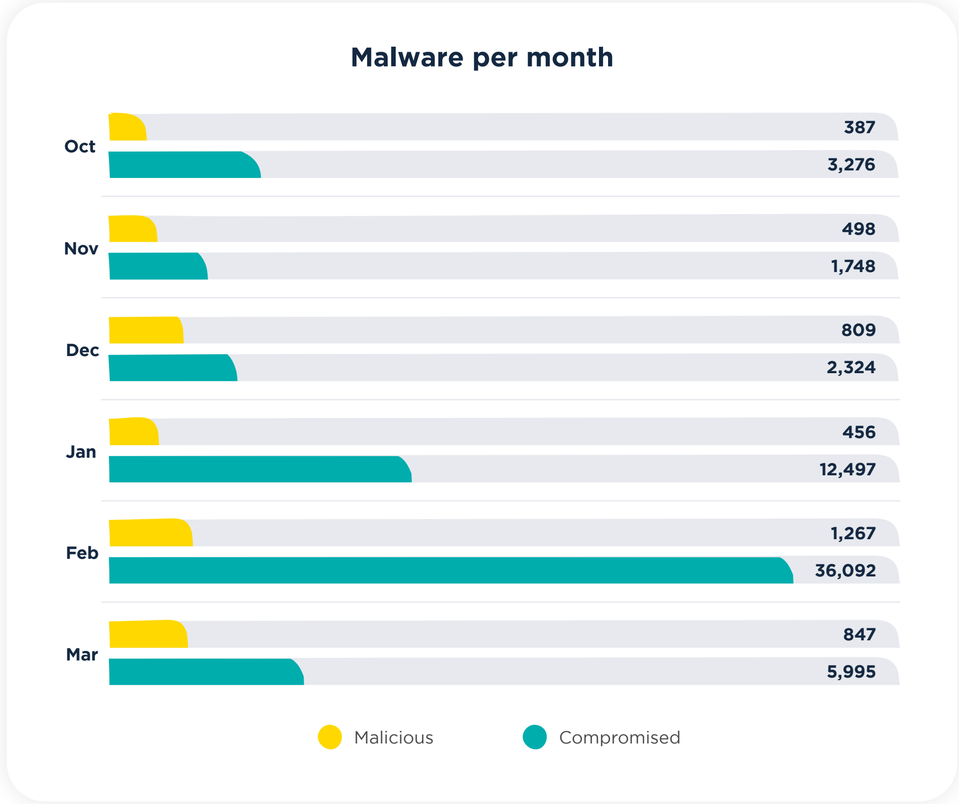
Bad reputation per month

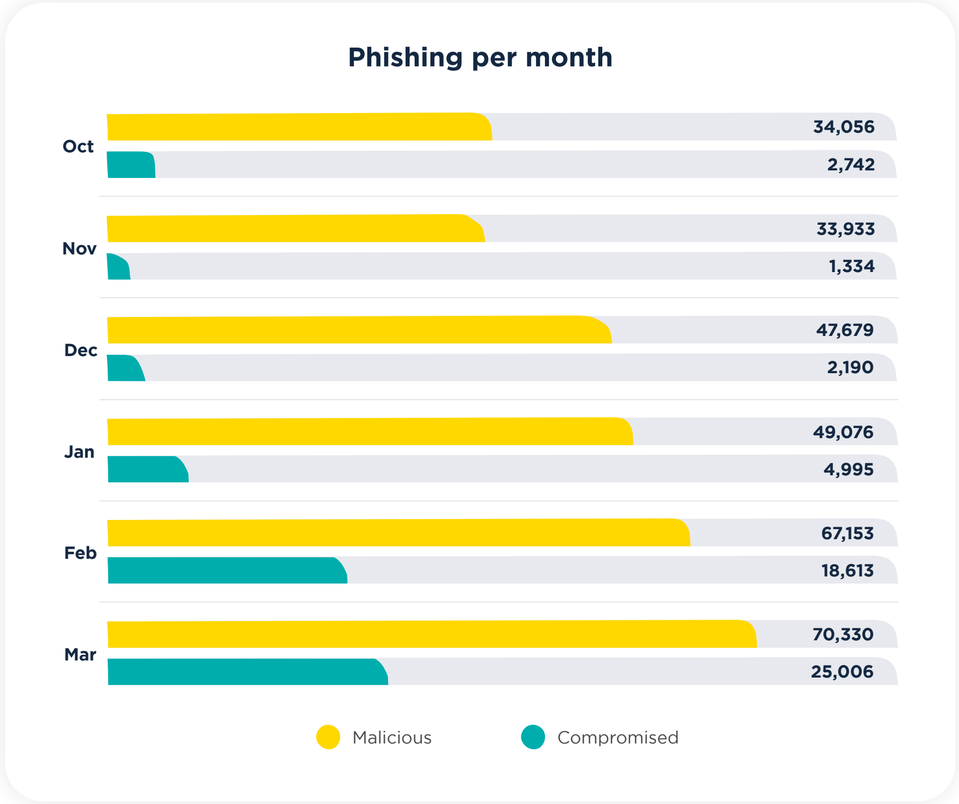


Botnet C&C per month



Types of abuse per month





Recommendations

Taking into consideration the aforementioned technical changes and their influence on this report, the underlying issue remains the same: for such a vital piece of internet infrastructure, it is extremely easy and inexpensive to abuse the DNS system through domain name registrations. Still, we recognize that this is a highly complex problem, involving many operational and regulatory challenges. These are:

- Compared to other industries, KYC is very limited in the domain space. Most sites that sell domains make it very easy for you to become a customer and buy 100s (even 1000s) of domains, or buy domains that impersonate well-known brands. Both these behaviors should immediately raise flags.
- Regulation has made it harder, not easier, to verify the true owner of a domain name. ICANN is still deliberating on how to handle the disclosure of ownership information, and even with the introduction of NIS2 in Europe, operational changes are yet to be seen.
- As the Internet becomes more centralized, only a few entities are responsible for providing extensive parts of the Internet infrastructure. As a result, their role in dealing with abuse, and more importantly, preventing it, becomes ever more important. Again, changes in this area are slow to happen.
- The various types of abuse we monitor tend to be concentrated in TLDs with less regulation and lower pricing. Due to the market's competitive nature, pricing is low, which makes for shallow profit margins in what is largely an automated business. Lack of funding to proactively fight abuse also contributes to the problem. Since many of the simpler cases aren't dealt with, the more complex cases need not worry.

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

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

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.