SPAMHAUS

Spamhaus Quarterly Domain Reputation Update

Q1 2023

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

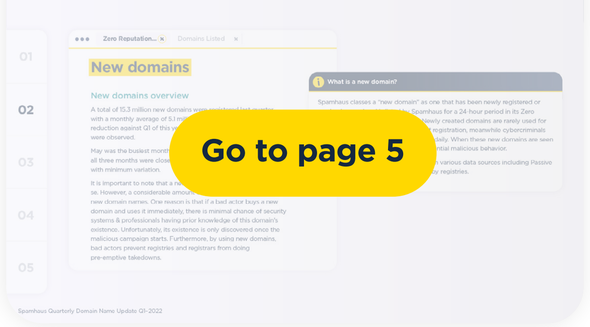
Welcome to the Spamhaus Quarterly Domain Reputation Update Q1 2023.

Enter

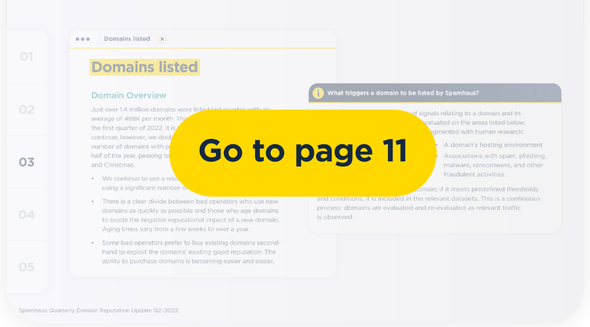
Contents

The Overview

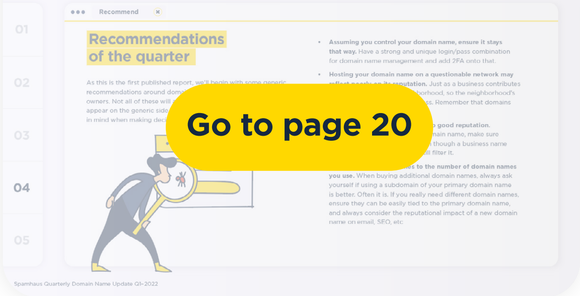
New domains



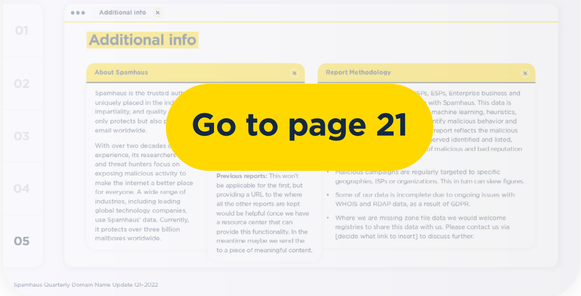
Domains listed



Recommendations of the quarter



Additional info



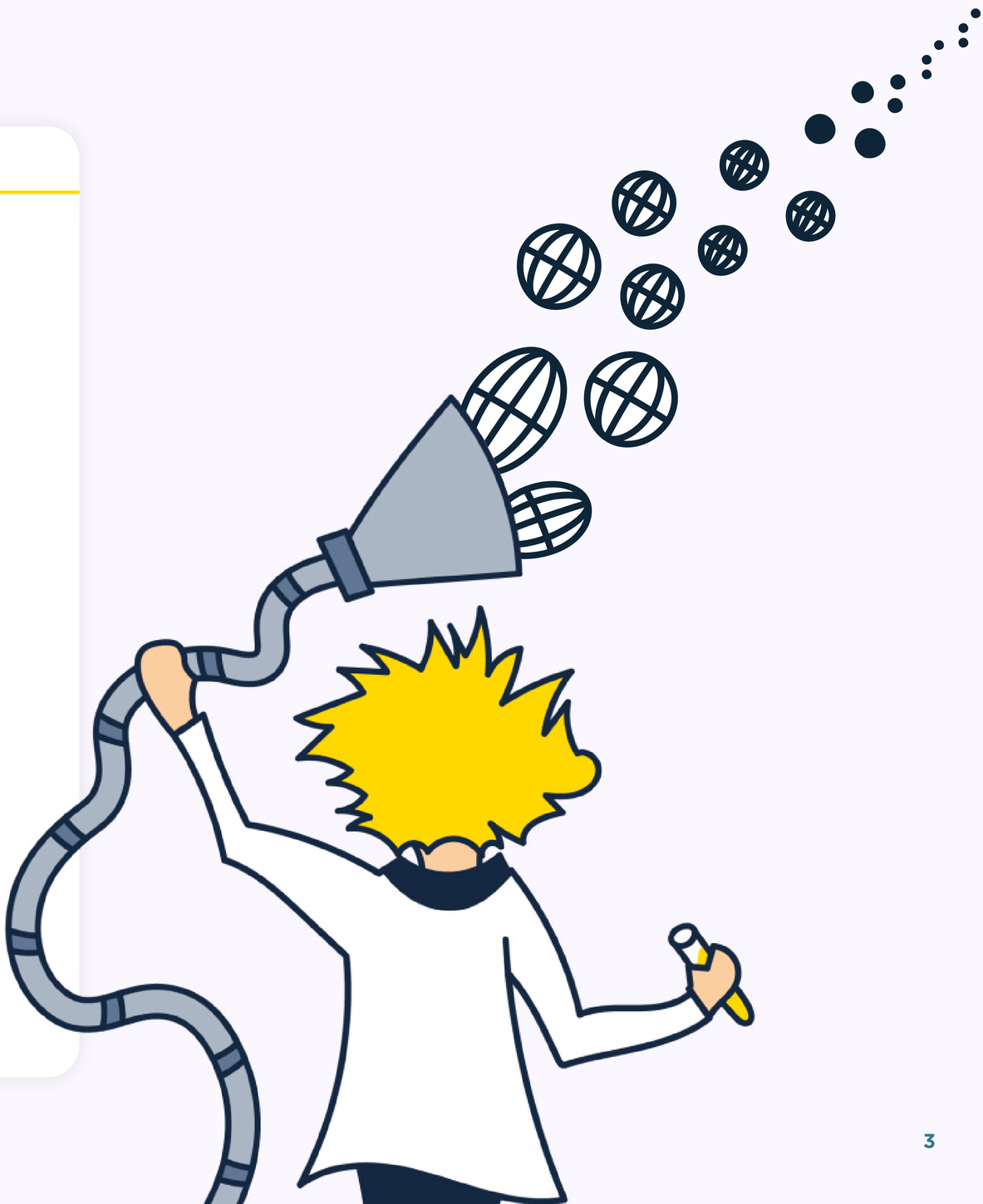
The Overview

There is nothing so constant as change. Well, change has been abundant this quarter, and none more so than that caused by the circumstances surrounding Freenom.

Many factors drive the ever-changing domain landscape, like the usual ebbs and flows of domain registrations tied to current events or seasonal activities. There are aggressive promotions, driving short bursts of sales in various TLDs, usually fuelled by speculators and abusive or highly fraudulent registrations. Then there are longer-term trends, such as the popularity of .xyz in the cryptocurrency world or .io with tech start-up companies.

Last quarter we ended this overview with the sentence, “It will be interesting to see what the next quarter brings.” Considering current affairs, this statement seems prescient because for (almost) as long as our domain experts have been in this industry (and that’s quite some time), they have never seen a change as dramatic as the one we’ll be covering this quarter.

Overview continued



Overview cont.

All five Freenom-operated ccTLDs (.tk, .ml, .gq, .cf, and .ga) have dramatically decreased in registration and abuse numbers. This is an unprecedented change, given these TLDs have been a constant in the statistics Spamhaus reports on, relating specifically to domains associated with spam, phishing, and malware.

The obvious question is, “Why are numbers down?” Well, a quick visit to their site reveals Freenom appear to be experiencing “technical issues”:

“IMPORTANT NOTICE: Because of technical issues the Freenom application for new registrars is temporarily out-of-order. Please accept our apologies for the inconvenience. We are working on a solution and hope to resume operations shortly. Thank you for your understanding.”

Interestingly, these temporary issues have been ongoing since at least January 26th when some forum users reported the problems. One can’t help wondering if this is connected to Meta’s recent court filing in March against Freenom and another (unrelated) legal case against Freenom, based in the Netherlands.

What seems relatively certain is that Freenom won’t be accepting new domain registrations anytime soon, if ever again!

It will be fascinating to see how things pan out in the longer term. Operators who require large numbers of domains because theirs keep getting taken down or blocked had access to what amounted to an infinite supply at Freenom. Now that this never-ending reservoir is gone (or so it seems), the alternatives for actual domains (instead of free hostnames at dynamic DNS providers) are all paid options. Granted, some are available at a pretty low cost, for example, at the time of publication you can purchase .online for USD 0.98 at Namecheap or .top at USD 1.88 at Namesilo. Nevertheless, this may drastically change an operator’s business model and operational costs.

There is so much to discuss around this matter that it doesn’t fit into this report. You can look forward to a blog post focusing on the subject soon! Meanwhile, with an event of this magnitude, you’d almost think there is nothing else to report. That’s certainly not true; there’s plenty to discuss, some of it related, though not all. Keep reading to find out more.

New domains | Number of new...

New domains

New domains overview

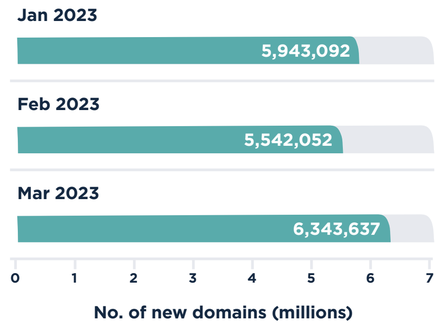
A total of 17.8 million new domains were registered last quarter, with a monthly average of 5.9 million. This was a slight decrease of -3% against Q4 of last year when researchers observed 18.5 million new domains.

March was the busiest month, with 6.3 million new domains, which we would anticipate, as it's normal for January to be relatively quiet after a busy December.

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 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



Quarterly Total
17,828,781
▼ -3% ▼

Monthly Average
5,942,927
▼-209,889▼

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)

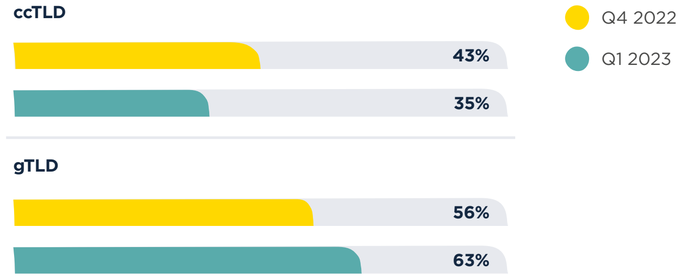
All five Freenom TLDs were in steep decline in Q1 2023 due to new registrations being closed. In the Top 20 TLDs .cf, .ga, .gq, and .ml all dropped off, and .tk saw a -67% drop. However, we observed some new domains in these zones because:

1. We believe registrations stopped at some point during the first quarter.
2. Domains registered in previous quarters but only used for the first time in Q1 will have been recorded as newly observed by our systems.

We think the significant increases experienced by the gTLDs .store (+62%) and .fun (+49%) in Q1 may be related to the Freenom effect. Both TLDs are at the lower end of the pricing scale, and as mentioned in the overview, it is only to be expected for some (most?) Freenom customers to look for the next best thing to free... very cheap!

New domains... TLD types...

New domain TLD types comparison, quarter on quarter



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	Q1 2023	Q1 data bar	Q4 2022	% Change
1	.com	gTLD	6,419,862		5,823,730	▲ 10%
2	.xyz	gTLD	445,801		451,091	▼ -1%
3	.online	gTLD	435,358		374,985	▲ 16%
4	.de	ccTLD	431,942		398,781	▲ 8%
5	.co.uk	ccTLD	416,655		248,291	▲ 68%
6	.net	gTLD	398,400		361,308	▲ 10%
7	.org	gTLD	355,681		329,624	▲ 8%
8	.shop	gTLD	320,034		348,971	▼ -8%
9	.top	gTLD	319,418		291,013	▲ 10%
10	.ru	ccTLD	308,432		258,471	▲ 19%
11	.cn	ccTLD	287,686		350,215	▼ -18%
12	.tk	ccTLD	282,598		868,574	▼ -67%
13	.store	gTLD	240,908		-	New entry
14	.co	ccTLD	239,659		230,478	▲ 4%
15	.com.br	ccTLD	239,574		235,377	▲ 2%
16	.nl	ccTLD	236,022		244,664	▼ -4%
17	.in	ccTLD	217,009		-	New entry
18	.site	gTLD	214,025		-	New entry
19	.fr	ccTLD	206,342		223,428	▼ -8%
20	.info	gTLD	195,392		-	New entry

0 2 4 6 8

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

Top 20 ccTLDs used in new domains

Rank	New domain TLD	Q1 2023	Q1 data bar	Q4 2022	% Change
1	.de	431,942		398,781	▲ 8%
2	.co.uk	416,655		248,291	▲ 68%
3	.ru	308,432		258,471	▲ 19%
4	.cn	287,686		350,215	▼ -18%
5	.tk	282,598		868,574	▼ -67%
6	.co	239,659		230,478	▲ 4%
7	.com.br	239,574		235,377	▲ 2%
8	.nl	236,022		244,664	▼ -4%
9	.in	217,009		178,681	▲ 21%
10	.fr	206,342		223,428	▼ -8%
11	.ga	194,510		444,697	▼ -56%
12	.ca	176,888		143,743	▲ 23%
13	.ml	163,629		570,075	▼ -71%
14	.cf	134,223		368,491	▼ -64%
15	.com.au	131,826		113,880	▲ 16%
16	.gq	125,898		327,203	▼ -62%
17	.cc	118,639		117,063	▲ 1%
18	.eu	117,932		119,524	▼ -1%
19	.us	114,931		-	New entry
20	.it	107,224		-	New entry

0 200 400 500

Top20 gTLD - new | Top20 gTLDs - zone

Top 20 gTLDs used in new domains

Rank	New domain TLD	Q1 2023	Q1 data bar	Q4 2022	% Change
1	.com	6,419,862		5,823,730	▲ 10%
2	.xyz	445,801		451,091	▼ -1%
3	.online	435,358		374,985	▲ 16%
4	.net	398,400		361,308	▲ 10%
5	.org	355,681		329,624	▲ 8%
6	.shop	320,034		348,971	▼ -8%
7	.top	319,418		291,013	▲ 10%
8	.store	240,908		149,160	▲ 62%
9	.site	214,025		220,922	▼ -3%
10	.info	195,392		198,675	▼ -2%
11	.buzz	125,045		116,313	▲ 8%
12	.click	118,338		104,836	▲ 13%
13	.cyou	111,235		134,946	▼ -18%
14	.cfd	87,235		-	New entry
15	.live	72,768		71,105	▲ 2%
16	.fun	72,504		48,508	▲ 49%
17	.vip	72,115		63,529	▲ 14%
18	.space	64,116		53,138	▲ 21%
19	.tech	55,796		46,609	▲ 20%
20	.app	51,638		-	New entry

Top20 gTLD - new | Top20 gTLDs - zone

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

Rank	New domain TLD	Q1 2023	Zone size	% of zone newly observed	% of zone data bar
1	.cfd	87,235	122,641	71.13%	
2	.best	17,111	31,271	54.72%	
3	.mba	5,425	10,759	50.42%	
4	.autos	12,590	27,935	45.07%	
5	.mom	13,406	32,652	41.06%	
6	.productions	7,309	18,878	38.72%	
7	.pics	14,488	41,917	34.56%	
8	.sbs	30,277	87,856	34.46%	
9	.skin	7,140	20,921	34.13%	
10	.click	118,338	363,030	32.60%	
11	.makeup	3,908	12,238	31.93%	
12	.monster	19,403	64,107	30.27%	
13	.lol	24,489	84,600	28.95%	
14	.gay	5,269	18,370	28.68%	
15	.cyou	111,235	390,496	28.49%	
16	.hair	5,592	19,839	28.19%	
17	.beauty	10,852	38,512	28.18%	
18	.store	240,908	998,735	24.12%	
19	.buzz	125,045	555,728	22.50%	
20	.fun	72,504	334,541	21.67%	

Trending terms...

Trending terms in new domains

There is a clear connection between what's trending in new domain terms and real-life events. At this the time of year, many young people are choosing their future schools or universities, which explains "education" in the "ation" list opposite, as well as newcomer "academy" (#17) to the Top 20 list.

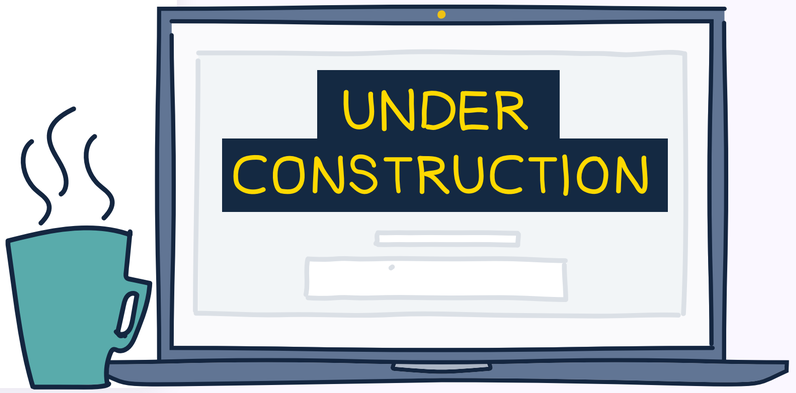
This is also the time of year many people in the Western world start thinking about where to go on their summer vacation. Hence, terms like "vacation" (opposite) and travel (#13), which experienced a +22% increase, are popular in new domain registrations. This may still be an after-effect of the past two years of reduced travel due to the Covid pandemic.

Here is a breakdown of the top words in Q1 containing the term "ation":

- foundation **14,643**
- international **10,940**
- creations **9,286**
- education **7,696**
- nation **5,479**
- national **4,463**
- station **4,263**
- association **3,713**
- innovation **3,640**
- creation **3,540**
- automation **3,108**
- vacation **2,580**
- transportation **2,488**
- installation **2,447**
- corporation **2,422**

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	Q4 2022 trending terms	Q1 2023	Q1 data bar	Q4 2022	% Change
1	ation	188,645		76,330	▲147%
2	service	114,008		100,221	▲14%
3	design	75,984		65,343	▲16%
4	market	75,225		61,122	▲23%
5	online	73,447		75,182	▼-2%
6	solution	69,634		56,807	▲23%
7	studio	66,189		58,062	▲14%
8	group	65,589		57,699	▲14%
9	health	61,128		53,865	▲13%
10	store	60,237		59,925	▲1%
11	consult	58,694		47,804	▲23%
12	digital	41,151		54,303	▼-24%
13	travel	35,633		29,216	▲22%
14	global	34,448		-	New entry
15	invest	34,150		32,322	▲6%
16	beauty	33,628		30,320	▲11%
17	academy	31,249		-	New entry
18	media	31,219		29,045	▲7%
19	company	30,557		-	New entry
20	property	28,599		-	New entry

0 50 100 150 200

Top 20 Trending... | Trending terms

Trending terms

Domains listed | Listings per month

Domains listed

Domain Overview

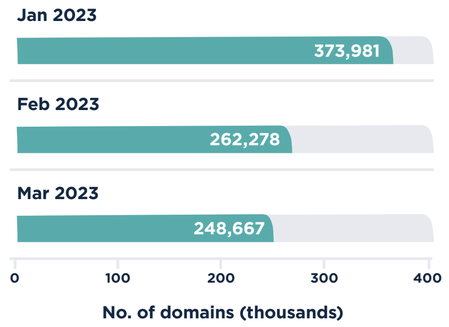
Over 880K domains were listed last quarter, with an average of 295K per month. This marginally decreased by -6% against the final quarter of 2022.

This small decline could be seasonal, nevertheless, we cannot escape the fact of the dramatic decrease in Freenom-operated TLDs. These five TLDs have exceptionally high levels of abuse and since they were free, the volume of bad domains was also high. Freenom's TLDs have had a poor reputation for a long time, across many areas of internet security, but the fact that miscreants could endlessly rotate through new names meant that supplies were endless.

Assuming Freenom continues with its "technical issues" a change will be forced upon the operations of those who rely on free domains to circumvent domain-based blocking. It will be interesting to see where operators who utilized Freenom TLDs will go to, and if they will ever return in the same volume. We predict (and hope) they won't.

Domains listed | Listings per month

Number of Domain listings per month



Quarterly Total

884,926

▼ -6% ▼

Monthly Average

294,975

▼ -19,803 ▼

What triggers a domain to be listed 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 listed 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

It will come as no surprise that all five of Freenom's TLDs experienced significant decreases - .ml (-74%), .tk (-54%), .ga (-45%), .cf (-43%), .gq (-38%).

Additionally, in the ccTLD space, malicious domains with the TLD .cn continue to dominate at #1. Most of this is associated with large-scale phishing campaigns targeting Japanese businesses, and worldwide companies like Amazon, along with local businesses such as Japan Railways. While it may seem strange to an outsider to start phishing against a railway operator, the card used for travel is also a widely accepted payment method outside the railway system. In Q1, bad .cn domains outnumber the combined total number of the five Freenom ccTLDs.

Classification

We classify all Freenom's TLDs as ccTLDs, as they are technically assigned to five countries, even though they operate like gTLDs, accepting registrations from anywhere.

All the new entries in the gTLD list are, or have been, heavily discounted at popular registrars in the first quarter of this year, further strengthening our belief that low pricing inevitably attracts abusive registrations.

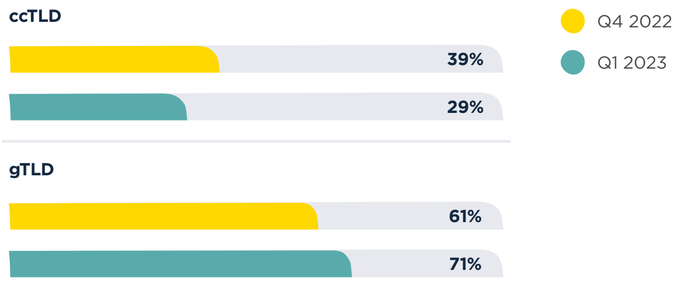
Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q1 2023 .life had over 320k domains in its zone, of which 2.09% were listed.

Meanwhile, .beauty had just over 38.5k domains in its zone, with 7.37% 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.

Domain listing...

Domain listing TLD type comparison, quarter on quarter



Top 20 TLDs... | Listings by...

Top 20 TLDs listed

Rank	Domain TLD	Type of TLD	Q1 2023	Q1 data bar	Q4 2022	% Change
1	.com	gTLD	311,947		278,629	▲ 12%
2	.cn	ccTLD	85,505		87,989	▼ -3%
3	.top	gTLD	39,335		46,052	▼ -15%
4	.info	gTLD	31,866		29,169	▲ 9%
5	.live	gTLD	27,981		22,198	▲ 26%
6	.net	gTLD	24,533		35,940	▼ -32%
7	.us	ccTLD	19,362		18,771	▲ 3%
8	.ml	ccTLD	17,444		65,866	▼ -74%
9	.xyz	gTLD	17,443		18,182	▼ -4%
10	.tk	ccTLD	16,866		36,662	▼ -54%
11	.biz	gTLD	16,154		-	New entry
12	.online	gTLD	13,078		-	New entry
13	.shop	gTLD	11,743		10,966	▲ 7%
14	.me	ccTLD	11,336		19,742	▼ -43%
15	.ga	ccTLD	10,994		19,979	▼ -45%
16	.org	gTLD	10,916		12,778	▼ -15%
17	.ru	ccTLD	10,390		13,817	▼ -25%
18	.gq	ccTLD	10,275		16,693	▼ -38%
19	.cf	ccTLD	9,977		17,646	▼ -43%
20	.buzz	gTLD	8,680		-	New entry

0 175 350

Top 20 TLDs... | Listings by...

Listings by Top 20 ccTLDs

Rank	Domain TLD	Q1 2023	Q1 data bar	Q4 2022	% Change
1	.cn	85,505		87,989	▼ -3%
2	.us	19,362		18,771	▲ 3%
3	.ml	17,444		65,866	▼ -74%
4	.tk	16,866		36,662	▼ -54%
5	.me	11,336		19,742	▼ -43%
6	.ga	10,994		19,979	▼ -45%
7	.ru	10,390		13,817	▼ -25%
8	.gq	10,275		16,693	▼ -38%
9	.cf	9,977		17,646	▼ -43%
10	.in	7,767		6,896	▲ 13%
11	.co	7,597		16,674	▼ -54%
12	.uk	7,449		9,204	▼ -19%
13	.cc	4,882		3,863	▲ 26%
14	.de	4,600		3,192	▲ 44%
15	.pl	3,343		4,094	▼ -18%
16	.eu	2,710		3,360	▼ -19%
17	.fr	2,537		2,896	▼ -12%
18	.nl	1,853		-	New entry
19	.pw	1,675		2,887	▼ -42%
20	.ws	1,412		-	New entry

0 50 100

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

Top 20 gTLDs used in domain listings

Rank	Domain TLD	Q1 2023	Q1 data bar	Q4 2022	% Change
1	.com	311,947		278,629	▲ 12%
2	.top	39,335		46,052	▼ -15%
3	.info	31,866		29,169	▲ 9%
4	.live	27,981		22,198	▲ 26%
5	.net	24,533		35,940	▼ -32%
6	.xyz	17,443		18,182	▼ -4%
7	.biz	16,154		5,759	▲ 181%
8	.online	13,078		9,142	▲ 43%
9	.shop	11,743		10,966	▲ 7%
10	.org	10,916		12,778	▼ -15%
11	.buzz	8,680		6,285	▲ 38%
12	.cfd	8,478		-	New entry
13	.site	7,739		9,603	▼ -19%
14	.click	7,518		4,985	▲ 51%
15	.life	6,689		2,930	▲ 128%
16	.cyou	6,260		4,264	▲ 47%
17	.club	4,777		4,577	▲ 4%
18	.work	4,178		3,111	▲ 34%
19	.monster	4,046		-	New entry
20	.website	3,515		-	New entry

0 175 350

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

Top 20 gTLD by % of zone file with domain listings

Rank	Domain TLD	Q1 2023	Zone size	% of zone listed	% of zone data bar
1	.uno	2,288	19,038	12.02%	
2	.beauty	2,837	38,512	7.37%	
3	.cfd	8,478	122,641	6.91%	
4	.monster	4,046	64,107	6.31%	
5	.autos	1,577	27,935	5.65%	
6	.live	27,981	658,669	4.25%	
7	.rest	1,586	41,400	3.83%	
8	.quest	1,542	45,153	3.42%	
9	.fyi	1,827	60,758	3.01%	
10	.support	1,055	35,220	3.00%	
11	.mom	919	32,652	2.81%	
12	.cam	728	28,642	2.54%	
13	.best	752	31,271	2.40%	
14	.fit	870	40,155	2.17%	
15	.life	6,689	320,290	2.09%	
16	.click	7,518	363,030	2.07%	
17	.sbs	1,737	87,856	1.98%	
18	.zone	865	44,404	1.95%	
19	.productions	339	18,878	1.80%	
20	.makeup	202	12,238	1.65%	

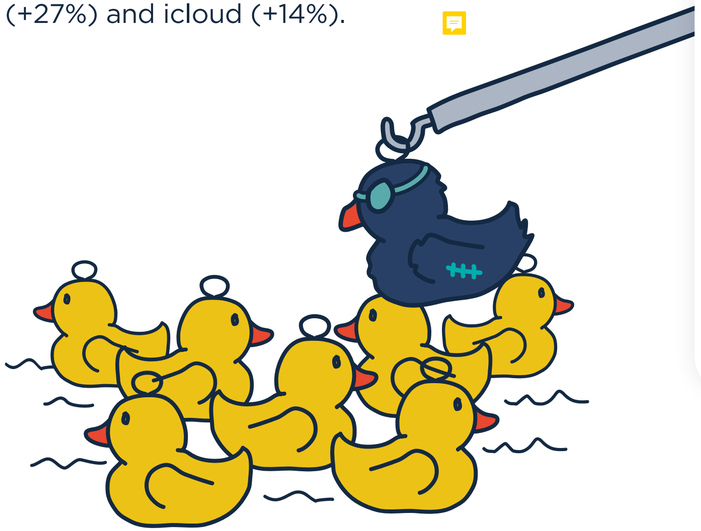
0% 5% 10% 15% 20%

Trending phishing terms in domain listings

One of the most interesting phishing term observations happened just outside of the Top 20: the rise of the term “netflix” (#21) and multiple obfuscated variations of it. Undoubtedly, the increase in Netflix-targeted phishing is due to the much-publicized clampdown by the streaming service on account and password sharing.

Netflix are limiting this abuse of their system, creating a black market for other people’s Netflix log-in credentials. As demand drives supply, one easy way to address this is to launch phishing campaigns, utilizing any readily available online kits (phishing-as-a-service).

Context (id, account, service, etc.) and action (update, verify, check, resolve, payment) related terms are still going strong. Also, the Apple brand and associated applications were heavily targeted in Q1, with a new entry for findmy (#15), along with increases in the following terms; apple (+27%) and icloud (+14%).



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 in domain listings

Rank	Term	Q1 2023	Q4 data bar	Q4 2022	% Change
1	account	7,001		11,155	-37%
2	support	6,200		6,568	-6%
3	online	5,190		5,565	-7%
4	service	4,634		4,636	0%
5	apple	4,288		3,368	27%
6	verification	4,031		4,951	-19%
7	security	3,954		4,077	-3%
8	icloud	3,876		3,408	14%
9	secure	3,675		4,975	-26%
10	intl	2,764		3,136	-12%
11	payment	2,198		2,036	8%
12	amazon	2,118		3,062	-31%
13	update	2,101		2,900	-28%
14	cloud	1,952		2,816	-31%
15	findmy	1,734		-	New entry
16	login	1,585		2,453	-35%
17	wallet	1,547		-	New entry
18	jobs	1,527		1,948	-22%
19	market	1,483		-	New entry
20	cyber	1,420		-	New entry

Top 20 phishing... | Phishing terms

Phishing terms

Types of listings

We attribute most categories that experienced decreases to the reduction in Freenom TLD registrations, except compromised malware. The reason for these decreases is that in Q4 2022, there was a spike caused by the heavy use of compromised websites by Qakbot malware. Qakbot's activity declined in the first quarter of 2023, particularly last month, so the numbers have decreased by a huge -79%.

In comparison, there is a significant rise of +76% in the number of dedicated malware domains: domains solely used to distribute or aid malware. As we reported in a blog, "A surge of malvertising across Google Ads is distributing dangerous malware," we've observed an upswing in the number of malware families, for example, Aurora Stealer and Vidar, that rely on offering updates for popular software packages to spread.

To increase the likeliness of downloading these files, miscreants often present them on reasonably convincing websites with domain names that contain the name of the software product. This strategy is not new per se, but activity noticeably grew in Q1 2023.

These domains are often short-lived, but it is not unusual to see up to 20 being used for one campaign. While this is undoubtedly done to subvert quick takedowns and fly below the radar, we notice that campaigns using larger numbers of domains often run across cheaper TLDs. As such, the pricing enables a rather successful circumvention strategy.

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 listings

Types of listings

Bad reputation

Malicious	Compromised
369,050	5,730
▼ -15% ▼	▼ -4% ▼

A domain's reputation score has exceeded policy limits.

Botnet C&C

Malicious	Compromised
4,581	253
▲ 23% ▲	▼ -6% ▼

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

Malware

Malicious	Compromised
12,704	5,324
▲ 76% ▲	▼ -79% ▼

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

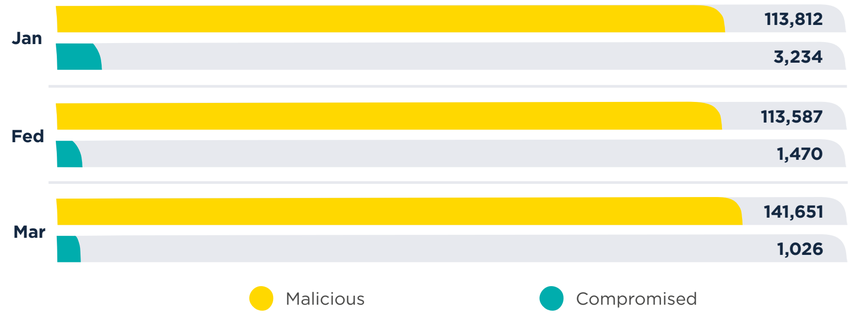
Phishing

Malicious	Compromised
369,206	5,730
▲ 3% ▲	▼ -25% ▼

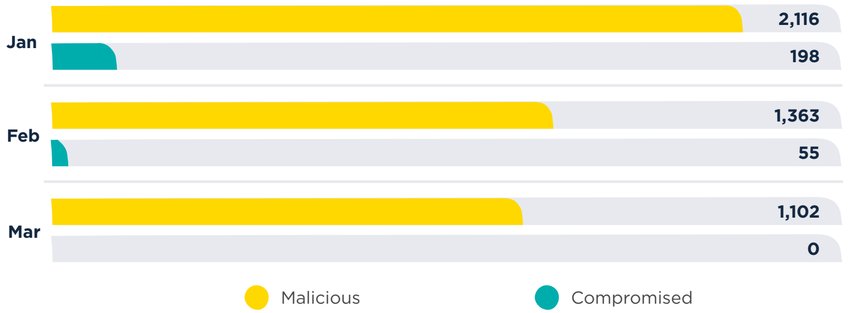
A domain is associated with phishing activities. (A subset of bad reputation.)

Types of abuse

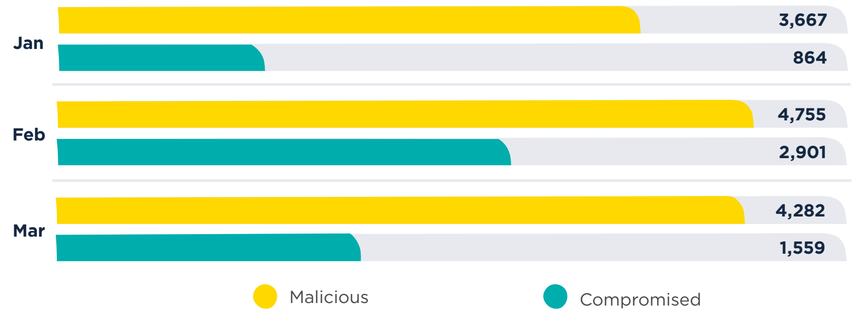
Bad reputation per month



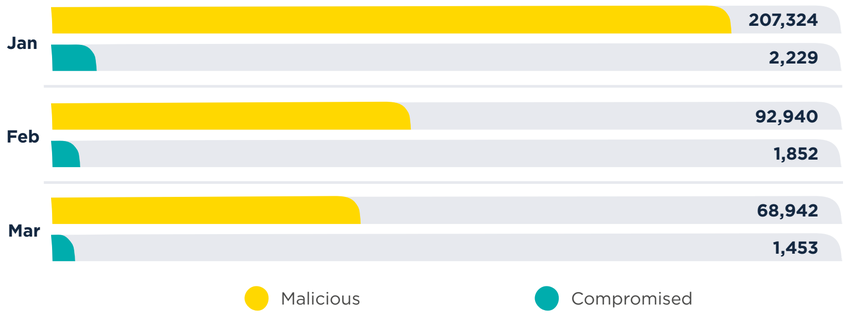
Botnet C&C per month



Malware per month



Phishing per month



Recommend...

Recommendations of the quarter

Q1 2023 has been an unusual quarter. The current reduction in malicious free domains has certainly caught our attention. Looking ahead, we can't imagine that all malicious operators who relied on these domains will evaporate. Cybercrime is often quite profitable, and while free domains may give one the best margins, cheap will also work for many.

Registries - more badness is coming: Those who operate TLDs at the lower end of the pricing spectrum should be vigilant for increased registrations by bad actors for malware, phishing, spam, and other fraudulent activity. Q1's report has evidenced that those zones at the lower end of the scale are susceptible to more significant abuse.

Newly registered domains are a well-known and well-understood risk. While it's hard to say exactly when a domain is not new anymore (as this very much depends on the context it is used in), everyone in the security space agrees that a domain that is not even 24 hours old should be treated with a fair bit of suspicion. After all, this is no different in the real world: new businesses often are required to do a down payment on orders or provide some third-party guarantee that they will live up to financial obligations.

Applying reputation data for increased visibility and protection. Our domain experts were surprised to witness malware campaigns promoted through various advertising platforms, including Google Ads, with these ultra-new domains as the sole point of contact. Almost certainly, the platforms didn't realize this, which means there are opportunities to prevent fraud and compromises by looking at domain reputation data, especially in contexts where it is not yet being used.

Sharing for the good of the internet. At the same time, some TLDs make it exceptionally hard to get data contributing to a domain's reputation. We urge those opaque providers across the industry to be more transparent.

Hopefully, the internet security community can nudge everybody in the right direction by applying domain reputation data across far more areas.

Additional info

About Spamhaus

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

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

Report Methodology

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