SPAMHAUS

Spamhaus Quarterly Domain Reputation Update

Q2 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 Q2 2023.

Enter

Contents

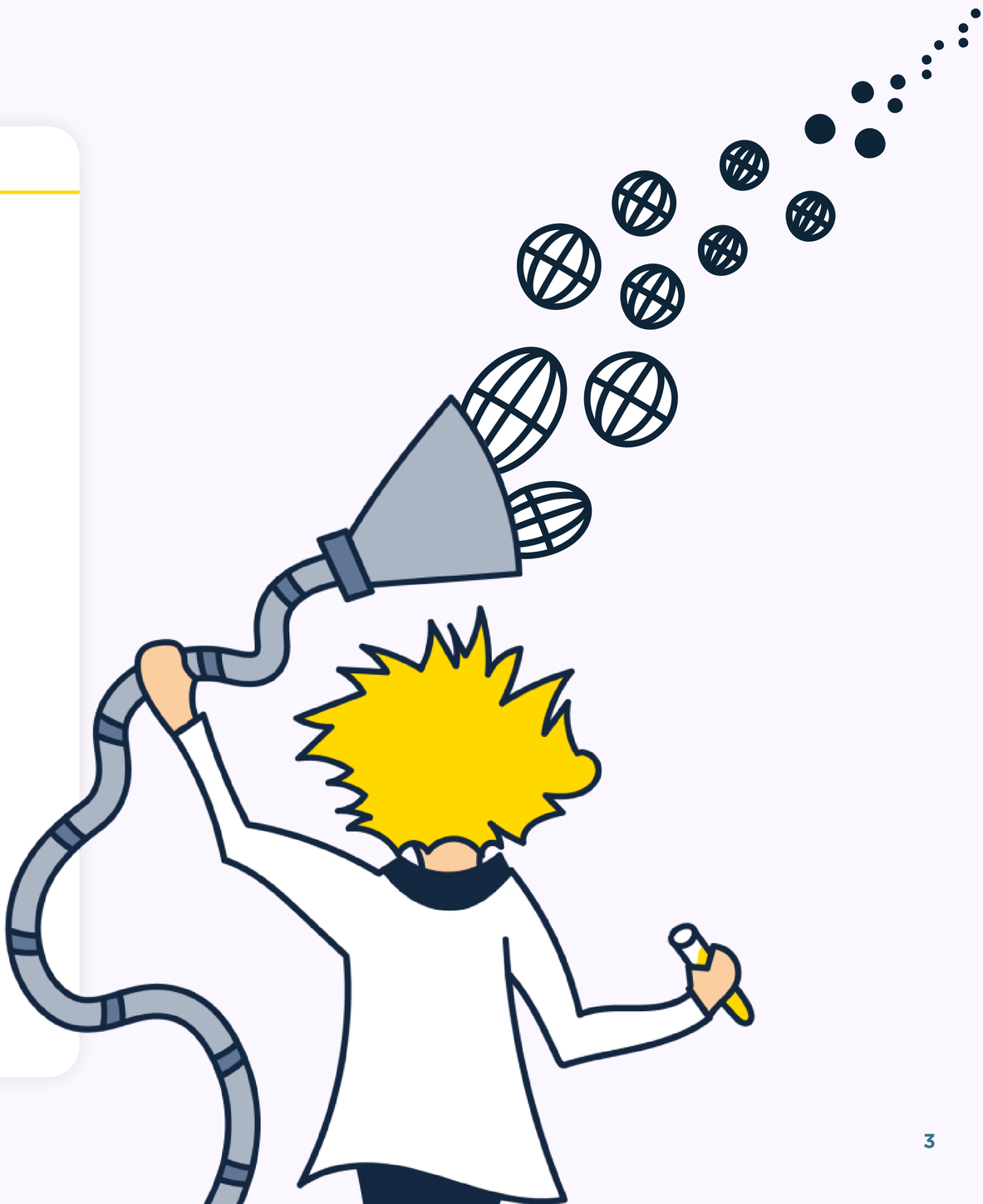
The Overview

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

Having been the main provider of free domains for many years, this cannot be underestimated. And while we've seen the biggest decrease in listed domains since Q3 2022, the abuse, of course, does not stop. Threat actors are migrating to the next best thing - cheap TLDs to replace the endless supply of free domains.

Without cheap domains, many cybercrime and fraud business models would break. Large volumes of suspicious registrations simply do not happen in the more expensive TLDs. To keep beating the drum: cheap domains facilitate cybercrime at scale. Obviously, not every cheap domain name is purchased or sold solely with the intention of enabling cybercrime or fraud. However, the fact remains that aggressive pricing certainly facilitates threat actors' activities.

Overview continued



Overview cont.

From a reputational standpoint, there is another key point to consider: promotions. What does it say about a TLD that uses flash promotions to boost sales, enabling hundreds, even thousands of machine-generated names? Names like ‘29upe0weuu.sbs’, ‘nesgl7qitd.cfd’ or ‘xsh60v8222sg.top’. Names that almost certainly will never be renewed or typed into a browser by a human. These TLDs are clearly ripe for abuse. Our researchers have also observed more subtle patterns of machine-generated TLDs. The existence of abuse is not always evident, but we fail to see the legitimate use case for these domains.

Finally, with Freenom’s departure, TLDs that previously sat outside the Top 20 lists are now in the spotlight. We hope this will encourage those highlighted in this report to investigate and tighten up.

New domains | Number of new...

New domains

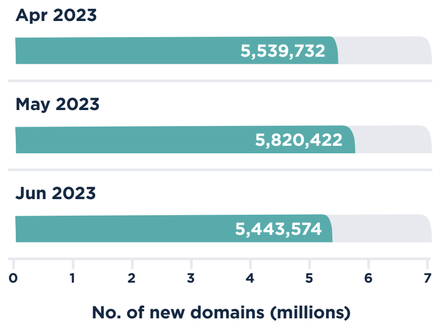
New domains overview

In Q2, we observed almost 17 million new domains across all gTLDs and ccTLDs, down 6% from Q1. The lowest month was June, likely due to the approaching summer season across the northern hemisphere. Overall, the month-to-month figures were similar to previous months, slightly higher than Q2 2022.

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



Quarterly Total
16,803,728
▼ -6% ▼

Monthly Average
5,601,243
▼ -341,684 ▼

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)

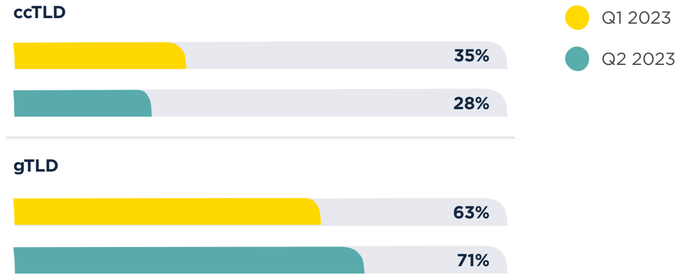
In Q2, almost all newly registered TLDs in the Top 20 declined compared to Q1. However, differences between the TLDs were quite significant - .com decreased slightly by-3% and .org -2%, while .co.uk and .cn experienced more significant decreases of -34% and -26%, respectively.

Well-established TLDs .xyz (+23%) and .top (+48%) were among the top 20 TLDs that increased, as were lesser known .online (+9%) and .store (+9%), plus the relatively obscure new entry .cfd reaching #9. Increases appear to be linked to aggressive promotions at various registrars. While measuring pricing across so many TLDs and registrars is difficult, cheap domains can generally be categorized as those sold for $5 (USD) or less. It's no surprise that the Top 20 TLDs that increased in Q2 can all fall into this category.

Looking at ccTLDs, all Freenom TLDs have now exited the Top 20 due to the registrar still not accepting new registrations. So Q2 saw new entries from .me (#18) and .pw (#19), both technically ccTLDs but operate like gTLDs with open registration policies and a very loose connection to the originating countries. Is this a case of history repeating itself?

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	Q2 2023	Q2 data bar	Q1 2023	% Change
1	.com	gTLD	6,200,946		6,419,862	▼ -3%
2	.xyz	gTLD	546,683		445,801	▲ 23%
3	.online	gTLD	476,268		435,358	▲ 9%
4	.top	gTLD	473,333		319,418	▲ 48%
5	.de	ccTLD	365,417		431,942	▼ -15%
6	.net	gTLD	363,344		398,400	▲ 9%
7	.org	gTLD	347,912		355,681	▼ -2%
8	.shop	gTLD	344,624		320,034	▲ 8%
9	.cfd	gTLD	333,226		-	New entry
10	.site	gTLD	297,222		214,025	▲ 39%
11	.co.uk	ccTLD	274,420		416,655	▼ -34%
12	.store	gTLD	261,710		240,908	▲ 9%
13	.ru	ccTLD	234,458		308,432	▼ -24%
14	.com.br	ccTLD	215,607		239,574	▼ -10%
15	.cn	ccTLD	214,026		287,686	▼ -26%
16	.nl	ccTLD	202,605		236,022	▼ -14%
17	.co	ccTLD	197,432		239,659	▼ -18%
18	.info	gTLD	187,752		195,392	▼ -4%
19	.in	ccTLD	180,128		217,009	▼ -17%
20	.fr	ccTLD	166,363		206,342	▼ -19%

0 2 4 6 8

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

Top 20 ccTLDs used in new domains

Rank	New domain TLD	Q2 2023	Q2 data bar	Q1 2023	% Change
1	.de	365,417		431,942	▼ -15%
2	.co.uk	274,420		416,655	▼ -34%
3	.ru	234,458		308,432	▼ -24%
4	.com.br	215,607		239,574	▼ -10%
5	.cn	214,026		287,686	▼ -26%
6	.nl	202,605		236,022	▼ -14%
7	.co	197,432		239,659	▼ -18%
8	.in	180,128		217,009	▼ -17%
9	.fr	166,363		206,342	▼ -19%
10	.ca	137,857		176,888	▼ -22%
11	.pl	129,308		-	New entry
12	.cc	126,963		118,639	▲ 7%
13	.com.au	111,490		131,826	▼ -15%
14	.us	108,134		114,931	▼ -6%
15	.eu	102,572		117,932	▼ -13%
16	.it	84,234		107,224	▼ -21%
17	.uk	79,029		-	New entry
18	.me	73,691		-	New entry
19	.pw	69,337		-	New entry
20	.ir	65,909		-	New entry

0 100 200 300 400

Top20 gTLD - new | Top20 gTLDs - zone

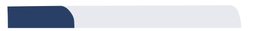
Top 20 gTLDs used in new domains

Rank	New domain TLD	Q2 2023	Q2 data bar	Q1 2023	% Change
1	.com	6,200,946		6,419,862	▼ -3%
2	.xyz	546,683		445,801	▲ 23%
3	.online	476,268		435,358	▲ 9%
4	.top	473,333		319,418	▲ 48%
5	.net	363,344		398,400	▼ -9%
6	.org	347,912		355,681	▼ -2%
7	.shop	344,624		320,034	▲ 8%
8	.cfd	333,226		87,235	▲ 282%
9	.site	297,222		214,025	▲ 39%
10	.store	261,710		240,908	▲ 9%
11	.info	187,752		195,392	▼ -4%
12	.click	127,430		118,338	▲ 8%
13	.vip	93,259		72,115	▲ 29%
14	.fun	79,352		72,504	▲ 9%
15	.buzz	75,888		125,045	▼ -39%
16	.live	75,317		72,768	▲ 4%
17	.sbs	69,350		-	New entry
18	.space	66,558		64,116	▲ 4%
19	.life	61,608		-	New entry
20	.bond	59,587		-	New entry

Top20 gTLD - new | Top20 gTLDs - zone

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

Rank	New domain TLD	Q2 2023	Zone size	% of zone newly observed	% of zone data bar
1	.cfd	333,226	448,471	74.30%	
2	.bond	59,587	86,541	68.85%	
3	.lat	10,683	20,195	52.90%	
4	.zip	14,406	28,600	50.37%	
5	.sbs	69,350	147,103	47.14%	
6	.med	32,560	69,734	46.69%	
7	.bio	22,715	56,683	40.07%	
8	.mom	15,656	41,281	37.93%	
9	.skin	10,687	28,282	37.79%	
10	.boats	3,864	12,226	31.60%	
11	.pics	14,966	50,016	29.92%	
12	.review	3,739	12,518	29.87%	
13	.autos	9,744	32,627	29.86%	
14	.monster	21,471	74,112	28.97%	
15	.click	127,430	458,845	27.77%	
16	.hair	5,061	19,218	26.33%	
17	.makeup	3,616	14,154	25.55%	
18	.icu	43,926	181,465	24.21%	
19	.homes	14,063	60,085	23.41%	
20	.store	261,710	1,142,378	22.91%	



Trending terms...

Trending terms in new domains

In Q2, trending terms in new domains were all relatively generic, with no observable connection to events (wars, elections, etc) or big trends (for example, generative AI). The rise of ‘vacation’ was somewhat predictable though, with summer coming up for many parts of the world.

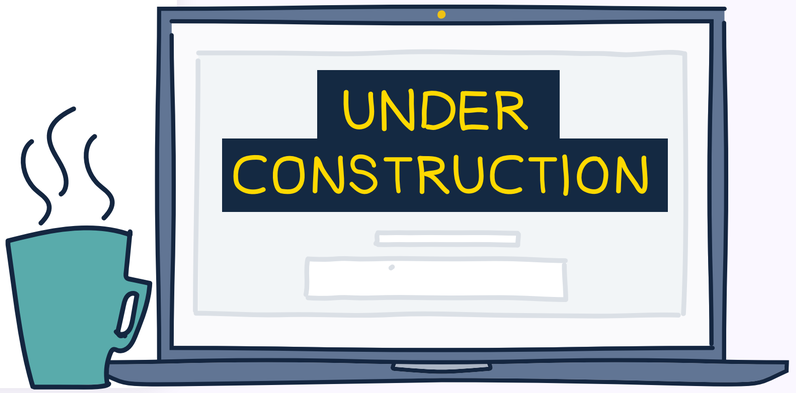
Equally, it is interesting how many domains get registered with a term descriptive of the business that owns the domain. This suggests that even with the thousands of TLDs available, people still prefer to be with more well-known TLDs. This results in longer domain names, such as example-designs.tld versus example.tld – where the latter is shorter, and more memorable, but with a less familiar TLD.

When it comes to “ation”, ranked #2 in trending terms, here’s a breakdown of the top words containing this term in Q2:

- foundation **12,728**
- international **9,875**
- creations **7,933**
- education **6,875**
- nation **4,893**
- national **4,103**
- station **3,902**
- innovation **3,287**
- association **3,239**
- creation **3,107**
- automation **2,961**
- vacation **2,815**
- installation **2,802**
- innovations **2,548**
- corporation **2,356**

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	Q2 2023 trending terms	Q2 2023	Q2 data bar	Q1 2023	% Change
1	service	99,797		114,008	▼ -12%
2	ation	73,239		188,645	▼ -61%
3	online	69,608		73,447	▼ -5%
4	solution	66,423		69,634	▼ -5%
5	design	65,608		75,984	▼ -14%
6	market	64,560		75,225	▼ -14%
7	studio	58,770		66,189	▼ -11%
8	store	56,363		60,237	▼ -6%
9	group	56,117		65,589	▼ -14%
10	digital	54,265		41,151	▲ 32%
11	health	53,646		61,128	▼ -12%
12	consult	51,953		58,694	▼ -11%
13	global	33,263		34,448	▼ -3%
14	travel	32,727		35,633	▼ -8%
15	product	31,887		-	New entry
16	invest	31,142		34,150	▼ -9%
17	official	28,976		-	New entry
18	beauty	28,848		33,628	▼ -14%
19	business	28,373		-	New entry
20	academy	27,665		31,249	▼ -11%

0 50 100 150

Top 20 Trending... | Trending terms

Trending terms

Domains listed | Listings per month

Domains listed

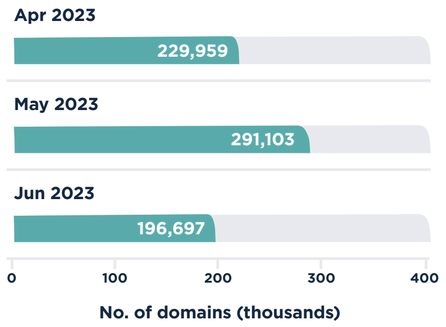
Domain Overview

In Q2, just over 717K domains were listed, with an average of 239K per month – a decrease of -19% - the biggest decrease since Q3 2022. This is almost entirely due to cyber threat actors no longer accessing new Freenom TLDs. That said, some have migrated to other 'cheap' (but still not free!) TLDs. Consequently, threat actors are only able to buy a certain number of these domains for abusive purposes.

In addition to Freenom TLDs, ccTLD .us decreased by -47%. Historically, this TLD has experienced fluctuations, so it comes as no real surprise. Significant increases from TLDs .cfd (+31%) and .site (+19%) reinforce cheap domains often enable abuse. Since both TLDs are sold for very low prices, they are attractive targets for anyone seeking 'domains to burn'.

Domains listed | Listings per month

Number of Domain listings per month



Quarterly Total
717,759
▼ -19% ▼

Monthly Average
239,253
▼ -55,722 ▼

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

Now that Freenom TLDs are no longer dominating the Top 20, it is interesting to see what is replacing them. In the gTLD Top 20, every increase or new entry is considered a cheap TLD (domains sell for less than $5 USD). This further confirms that low pricing not only attracts abuse - but enables it. In certain cybercrime business models, large numbers of domains are necessary to succeed: while filters continue to adapt, more domains are needed to avoid detection. Because in many scenarios (email spam, phishing, malware but also SEO or advertising fraud) domains are an easy hook for filtering.

In Q2, there were two notable entries: .ws, and .biz. The ccTLD .ws ranked #16 in the Top 20 ccTLDs, with a +64% increase - the second largest increase in domains listed. The associated listings can almost entirely be attributed to one operator - a very large, and well-run, spam operation. It is frightening that one actor can move the needle so significantly.

Comparatively, the gTLD .biz ranked #12 in the Top 20 gTLDs, with a -65% decrease in domains listed. For .biz, this is quite an accomplishment, especially considering that in the early days of new gTLDs, .biz was one of the very few domains with targeted rules in spam filters. Well done .biz!

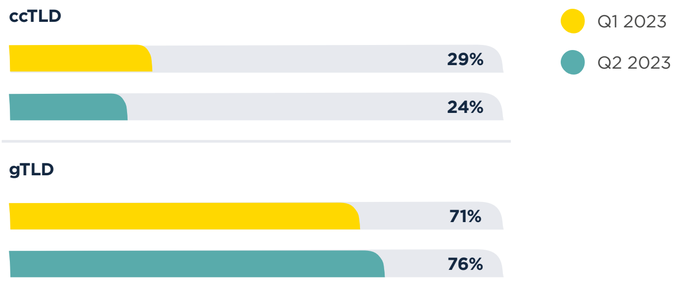
Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q2 2023 .bio had more than 56,000 domains in its zone, of which 2.01% were listed.

Meanwhile, .boats had just over 12,000 domains in its zone, with 4.47% 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	Q2 2023	Q2 data bar	Q1 2023	% Change
1	.com	gTLD	268,562		311,947	-14%
2	.cn	ccTLD	48,913		85,505	-43%
3	.top	gTLD	39,167		39,335	0%
4	.live	gTLD	28,293		27,981	1%
5	.info	gTLD	25,588		31,866	-20%
6	.net	gTLD	17,688		24,533	-28%
7	.xyz	gTLD	16,421		17,443	-6%
8	.tk	ccTLD	11,872		16,866	-30%
9	.cfd	gTLD	11,108		-	New entry
10	.online	gTLD	10,922		13,078	-16%
11	.us	ccTLD	10,317		19,362	-47%
12	.site	gTLD	9,238		-	New entry
13	.me	ccTLD	8,935		11,336	-21%
14	.ru	ccTLD	8,039		10,390	-23%
15	.org	ccTLD	7,960		10,916	-27%
16	.ml	ccTLD	7,801		17,444	-55%
17	.in	ccTLD	7,273		-	New entry
18	.uk	ccTLD	6,774		-	New entry
19	.gq	ccTLD	6,770		10,275	-34%
20	.pw	ccTLD	6,370		-	New entry

0 150 300

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

Listings by Top 20 ccTLDs

Rank	Domain TLD	Q2 2023	Q2 data bar	Q1 2023	% Change
1	.cn	48,913		85,505	-43%
2	.tk	11,872		16,866	-30%
3	.us	10,317		19,362	-47%
4	.me	8,935		11,336	-21%
5	.ru	8,039		10,390	-23%
6	.ml	7,801		17,444	-55%
7	.in	7,273		7,767	-6%
8	.uk	6,774		7,449	-9%
9	.gq	6,770		10,275	-34%
10	.pw	6,370		1,675	280%
11	.cf	5,957		9,977	-40%
12	.co	5,954		7,597	-22%
13	.cc	5,379		4,882	10%
14	.ga	4,906		10,994	-55%
15	.de	4,390		4,600	-5%
16	.ws	2,311		1,412	64%
17	.fr	2,072		2,537	-18%
18	.eu	1,869		2,710	-31%
19	.pl	1,615		3,343	-52%
20	.br	1,418		-	New entry

0 25 50

Top 20 gTLDs...

Top 20 gTLD...

Top 20 gTLDs used in domain listings

Rank	Domain TLD	Q2 2023	Q2 data bar	Q1 2023	% Change
1	.com	268,562		311,947	-14%
2	.top	39,167		39,335	0%
3	.live	28,293		27,981	1%
4	.info	25,588		31,866	-20%
5	.net	17,688		24,533	-28%
6	.xyz	16,421		17,443	-6%
7	.cfd	11,108		8,478	31%
8	.online	10,922		13,078	-16%
9	.site	9,238		7,739	19%
10	.org	7,960		10,916	-27%
11	.vip	6,184		-	New entry
12	.biz	5,575		16,154	-65%
13	.click	5,429		7,518	-28%
14	.shop	5,296		11,743	-55%
15	.sbs	4,435		-	New entry
16	.buzz	4,078		8,680	-53%
17	.cyou	3,945		6,260	-37%
18	.life	3,651		6,689	-45%
19	.club	3,413		4,777	-29%
20	.space	2,992		-	New entry

0 150 300

Top 20 gTLDs...

Top 20 gTLD...

Top 20 gTLD by % of zone file with domain listings

Rank	Domain TLD	Q2 2023	Zone size	% of zone listed	% of zone data bar
1	.wiki	2,484	53,935	4.61%	
2	.boats	546	12,226	4.47%	
3	.live	28,293	647,070	4.37%	
4	.beauty	1,744	40,913	4.26%	
5	.mom	1,659	41,281	4.02%	
6	.wtf	1,689	42,635	3.96%	
7	.autos	1,066	32,627	3.27%	
8	.quest	1,275	39,058	3.26%	
9	.monster	2,287	74,112	3.09%	
10	.sbs	4,435	147,103	3.01%	
11	.rest	1,121	38,368	2.92%	
12	.fyi	1,679	62,211	2.70%	
13	.pics	1,261	50,016	2.52%	
14	.cfd	11,108	448,471	2.48%	
15	.review	299	12,518	2.39%	
16	.hair	448	19,218	2.33%	
17	.bike	493	21,285	2.32%	
18	.support	818	35,763	2.29%	
19	.uno	396	18,671	2.12%	
20	.bio	1,138	56,683	2.01%	

0% 5% 10% 15% 20%

Trending terms...

Trending phishing terms in domain listings

In Q1 2023 Netflix was a target, possibly due to their clampdown on account sharing. This quarter, another tech giant emerged to be popular: Apple. Although not a newcomer, at least a quarter of the trending terms in Q2 were connected to Apple. High-value products seem to make for high-value targets.

Many trending phishing terms are often seen in fraudulent domain registrations: ‘payment’, ‘account’, ‘security’. It’s difficult to comprehend why so many domains pass the due diligence and ‘Know-Your-Customer’ processes of the associated registry and registrar. There is a lot of harm that can be prevented before domains enter the DNS. Having poor customer vetting can be very costly - see the recent Meta vs Freenom case.

Context-related terms such as account (#1) or service (#5), and action-related terms like verification (#13) or payment (#12) are still prevalent among many phishing-related domains. While they are present in other languages, English terms dominate in volume.

Furthermore, as students seek higher educational levels, newcomer ‘degree’, ranked #20, likely connected to the fake and forged degree market.

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	Q2 2023	Q2 data bar	Q1 2023	% Change
1	account	5,499		7,001	▽ -21%
2	online	4,623		5,190	▽ -11%
3	support	4,393		6,200	▽ -29%
4	today	3,923		-	New entry
5	service	3,879		4,634	▽ -16%
6	intl	3,630		2,764	△ 31%
7	apple	3,527		4,288	▽ -18%
8	security	3,209		3,954	▽ -19%
9	icloud	3,077		3,876	▽ -21%
10	cloud	2,641		1,952	△ 35%
11	secure	2,175		3,675	▽ -41%
12	payment	1,999		2,198	▽ -9%
13	verification	1,761		4,031	▽ -56%
14	jobs	1,723		1,527	△ 13%
15	update	1,389		2,101	▽ -34%
16	findmy	1,171		1,734	▽ -32%
17	market	1,150		1,483	▽ -22%
18	saving	1,117		-	New entry
19	cyber	1,075		1,420	▽ -24%
20	degree	1,072		-	New entry

Top 20 phishing... | Phishing terms

Phishing terms

Types of listings

Numbers decreased across all types of abuse in Q2, other than malicious botnet C&C (+9%) and malware (+25%). Increases for these categories were predominantly due to one specific domain generated algorithm (DGA) - which is rare these days.
DGAs used to be a big deal, but due to industry cooperation on reversing algorithms and sharing, preregistering, or blocking-for-registration of the computed names, their use has declined.

Researchers are still observing large batches (1000+) of very short domain names registered for SMS spam/phishing purposes. These often happen in newer, shorter gTLDs, due to the SMS 160-character limit. Since most established TLDs do not have many 4-letter strings available, phishers move to the less popular TLDs where they are available.

Coincidentally, some of these TLDs - such as .sbs which featured in Q2 - are sold cheaply per domain. Once again, aggressive pricing enables cybercrime at scale.

A more worrying trend is an increase in the use of very old domain names for malspam campaigns. These domains are acquired through various marketplaces and sold at a premium price due to their age. Why? Domain age is a key factor in many reputation systems. By combining old domains with reasonably targeted emails that meet all standard authentication checks (SPF, DKIM, DMARC), cyber threat actors appear to be following the best practices. In light of this trend, legitimate senders should be wary of what they are up against.

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
400,628	5,798
▼ -8% ▼	▼ -3% ▼

A domain's reputation score has exceeded policy limits.

Botnet C&C

Malicious	Compromised
4,062	175
▲ 9% ▲	▼ -35% ▼

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

Malware

Malicious	Compromised
9,025	11,003
▲ 25% ▲	▼ -56% ▼

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

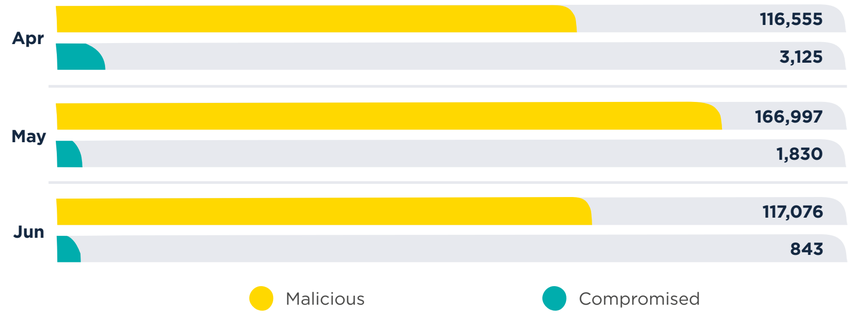
Phishing

Malicious	Compromised
185,508	4,012
▼ -48% ▼	▼ -46% ▼

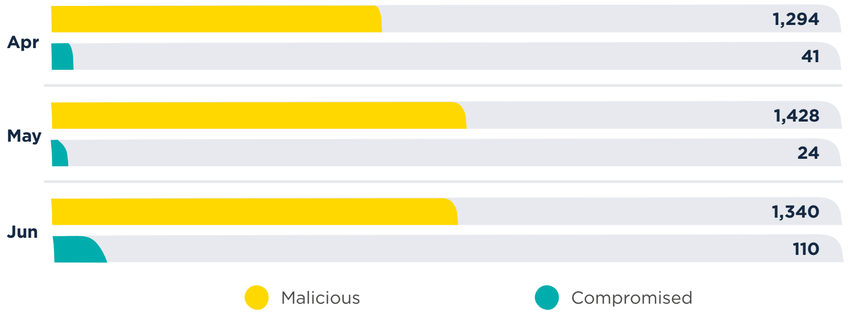
A domain is associated with phishing activities. (A subset of bad reputation.)

Types of abuse

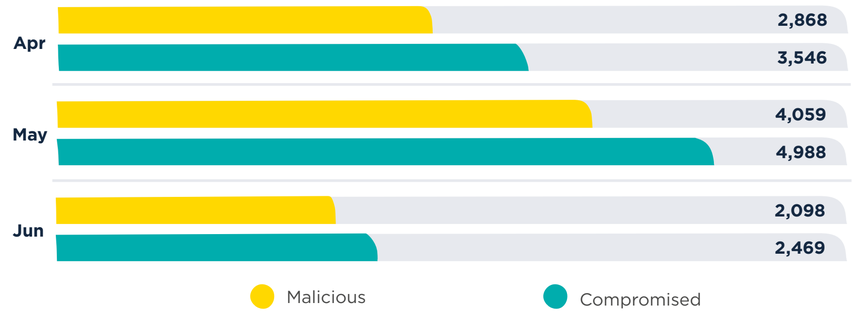
Bad reputation per month



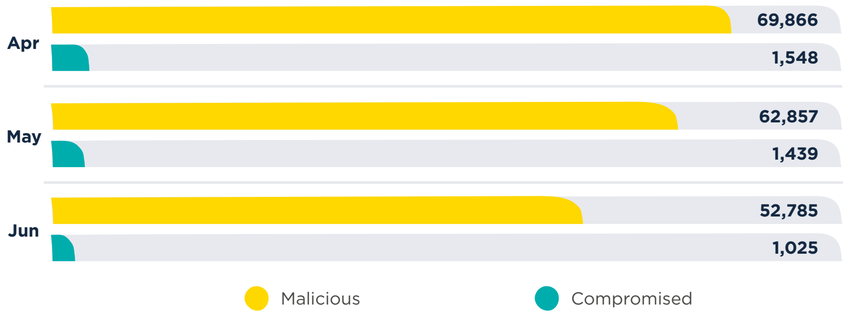
Botnet C&C per month



Malware per month



Phishing per month



Recommend...

Recommendations of the quarter

This quarter, the data has shown a very clear correlation between free/cheap domains and abuse. This is not always the case and furthermore, can be significantly reduced. Registries and registrars – it's time to tighten up your policies and processes to prevent this abuse.

Implement Know-Your-Customer procedures:
To avoid a TLD with many problematic domains like Freenom experienced, registrars need to improve customer vetting at the point of registration and be strict when dealing with malicious domains once registered. Take inspiration from the financial sector regarding Know-Your-Customer procedures. Aggressive pricing is a business model choice, which tends to mean limited resources for strong Know-Your-Customer and after-sale anti-abuse policies. This should be better considered in business planning.

Domain owners, consider the impact of your chosen TLD:
At Spamhaus we don't reveal the inner workings of the reputation engine. Adjustments are frequently made to punish bad behaviour and reward good. Following recent changes, we now consider TLD reputation in various scenarios. Domains that exist under TLDs with many other poor domains will move faster towards a bad reputation. We recommend domain owners think carefully about where they want their domains to live. In addition, TLD owners should consider the domains they sell and who they sell them to.

Refer to the FIRST DNS Abuse Matrix:
Another recommendation for anyone working near the intersection of DNS, abuse, fraud and cybercrime, is to refer to the FIRST DNS Abuse Matrix. It is an excellent document that identifies stakeholder responsibilities for detecting, mitigating, and preventing DNS abuse. If you haven't read this document yet, we strongly suggest you do.

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

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.