SPAMHAUS

Spamhaus Quarterly Domain Reputation Update

Q3 2022

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, provides insights into the poor reputation of domains, and champions providers where positive improvements are seen.

Welcome to the Spamhaus Quarterly Domain Reputation Update Q3 2022.

Enter

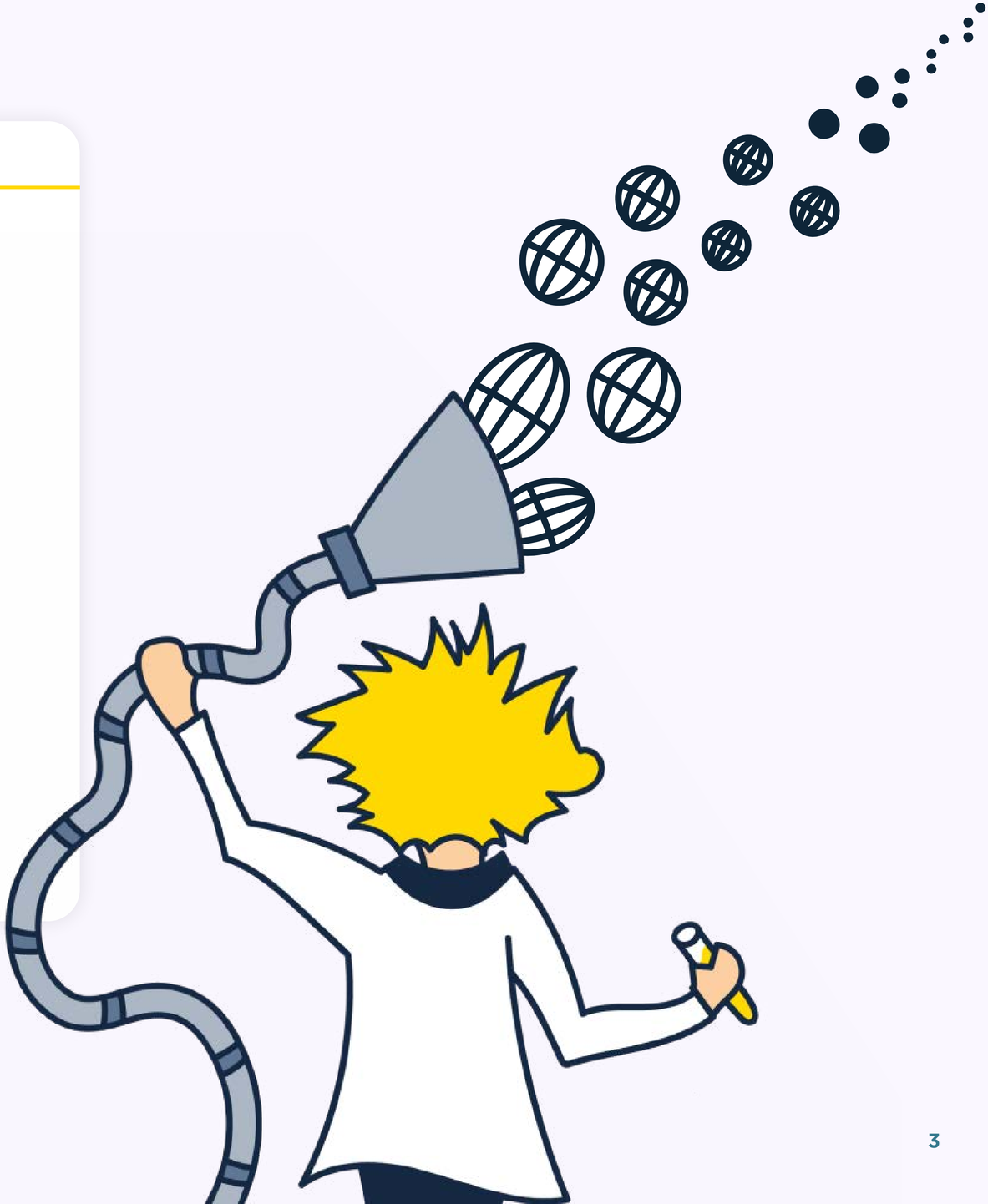
Contents

The Overview

We bear good news regarding domain name abuse: almost all numbers are down compared to last quarter. While it is hard to pinpoint a specific cause for this, we do believe the following three points can partially explain what is happening in the world of domains:

1. **Spotlight on DNS abuse -** There is much talk around the concept of ‘DNS abuse’. Different groups are still debating the definition, including what is and is not considered DNS abuse. Still, it is without a doubt that the abuse of domain names and DNS infrastructure for malicious purposes is in the spotlight. While this attention to the problem will not solve everything, it certainly can’t hurt.

Overview continued



Overview cont.

2. **Too big to block** - As domain reputation-based filtering is widespread these days (and has been for some time), getting away with a wholly bad portfolio of domain names has become increasingly difficult. The blacker side of the malicious operator greyscale often uses free DNS services, abused redirectors, compromised websites, or cloud content hosting URLs as the initial carriers, redirecting to operator-owned domains. Often, the legitimate domains that have been abused are too big to block.
3. **That time of year** - A more short-term effect is that this quarter covers the Northern Hemisphere's summer months, which are historically slower.

It will be interesting to see what the next quarter brings as the Western world enters a time of year filled with numerous events, usually exploited by cybercriminals, including Black Friday and the holiday season.

New domains | Number of new...

New domains

New domains overview

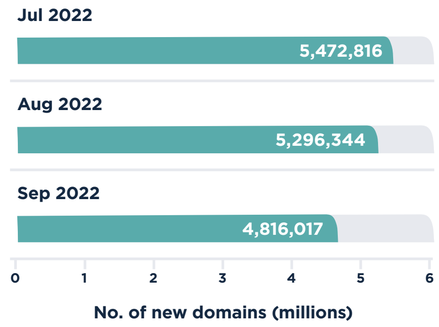
A total of 15.6 million new domains were registered last quarter, with a monthly average of 5.2 million. This was a marginal increase of 2% against Q2 of this year when researchers observed 15.3 million new domains.

July was the busiest month, with 5.5 million new domains; however, all three months were close to the quarterly monthly average, with minimum variation.

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.

New domains | Number of new...

Number of new domains per month



Quarterly Total
15,585,177
▲ 2% ▲

Monthly Average
5,195,059
▲ 110,554 ▲

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)

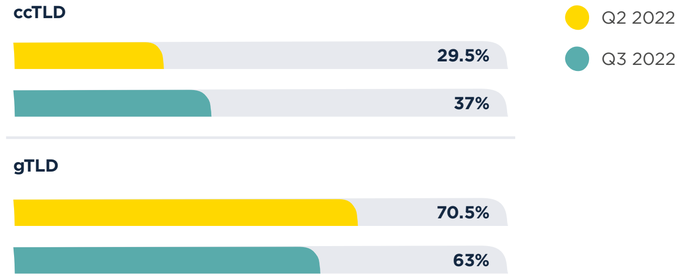
As previously mentioned, Q3 was a “slow” quarter in terms of newly observed domains. There was a slight shift towards more ccTLDs being used for new domains, increasing from 29.5% in Q2 to 37% in Q3. However, new domain owners continued to favor gTLDs at 63%.

Looking at the specific ccTLD Top 20, .gq (121%), .tk (115%), and .cf (103%) all had the highest number of new domains observed. However, it is worth noting that all three TLDs operate like a gTLD under Freenom who give away domains – increasing market share is accomplished by low prices!

When analyzing the Top 20 gTLDs by percentage of zone file that are new domains it’s evident that the registry XYZ is trying to increase its market share across their lesser used TLDs; .skin (50%), .beauty (41%), .autos (39%), .mom (35%), .lol (34%), .pics (32%), .hair (26%) and .homes (21%) all had high percentages of new domains compared to zone files.

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	Q3 2022	Q3 data bar	Q2 2022	% Change
1	.com	gTLD	5,808,863		5,750,666	▲ 1%
2	.tk	ccTLD	491,807		228,359	▲ 115%
3	.xyz	gTLD	447,214		503,191	▼ -11%
4	.net	gTLD	382,156		291,331	▲ 31%
5	.de	ccTLD	352,811		267,250	▲ 32%
6	.org	gTLD	315,205		263,430	▲ 20%
7	.online	gTLD	306,458		238,194	▲ 29%
8	.cn	ccTLD	291,411		279,479	▲ 4%
9	.ga	ccTLD	290,995		183,826	▲ 58%
10	.top	gTLD	257,526		203,738	▲ 26%
11	.ml	ccTLD	252,551		177,008	▲ 43%
12	.nl	ccTLD	240,556		150,862	▲ 59%
13	.shop	gTLD	237,288		172,363	▲ 38%
14	.cf	ccTLD	203,546		-	New entry
15	.site	gTLD	197,213		145,313	▲ 36%
16	.co.uk	ccTLD	189,694		130,201	▲ 46%
17	.ru	ccTLD	189,140		107,452	▲ 76%
18	.com.br	ccTLD	177,186		121,371	▲ 46%
19	.info	gTLD	174,525		127,696	▲ 37%
20	.co	ccTLD	160,411		-	New entry

0 2 4 6

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

Top 20 ccTLDs used in new domains

Rank	New domain TLD	Q3 2022	Q3 data bar	Q2 2022	% Change
1	.tk	491,807		228,359	▲ 115%
2	.de	352,811		267,250	▲ 32%
3	.cn	291,411		279,479	▲ 4%
4	.ga	290,995		183,826	▲ 58%
5	.ml	252,551		177,008	▲ 43%
6	.nl	240,556		150,862	▲ 59%
7	.cf	203,546		100,241	▲ 103%
8	.co.uk	189,694		130,201	▲ 46%
9	.ru	189,140		107,452	▲ 76%
10	.com.br	177,186		121,371	▲ 46%
11	.co	160,411		94,947	▲ 69%
12	.gq	155,426		70,392	▲ 121%
13	.in	139,536		86,044	▲ 62%
14	.fr	131,042		96,208	▲ 36%
15	.ca	108,670		70,366	▲ 54%
16	.me	108,104		-	New entry
17	.us	107,482		61,512	▲ 75%
18	.com.au	98,809		59,853	▲ 65%
19	.eu	96,261		102,454	▼ -6%
20	.au	89,693		-	New entry

0 1 2 3 4 5

Top20 gTLD - new | Top20 gTLDs - zone

Top 20 gTLDs used in new domains

Rank	New domain TLD	Q3 2022	Q3 data bar	Q2 2022	% Change
1	.com	5,808,863		5,750,666	▲ 1%
2	.xyz	447,214		503,191	▼ -11%
3	.net	382,156		291,331	▲ 31%
4	.org	315,205		263,430	▲ 20%
5	.online	306,458		238,194	▲ 29%
6	.top	257,526		203,738	▲ 26%
7	.shop	237,288		172,363	▲ 38%
8	.site	197,213		145,313	▲ 36%
9	.info	174,525		127,696	▲ 37%
10	.store	146,189		102,916	▲ 42%
11	.live	106,475		76,690	▲ 39%
12	.buzz	87,554		51,439	▲ 70%
13	.vip	86,703		41,735	▲ 108%
14	.click	78,824		-	New entry
15	.space	56,370		45,851	▲ 23%
16	.fun	56,202		50,021	▲ 12%
17	.tech	45,326		-	New entry
18	.app	42,247		-	New entry
19	.club	41,286		47,484	▼ -13%
20	.biz	39,764		37,896	▲ 5%

0 2 4 6

Top20 gTLD - new | Top20 gTLDs - zone

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

Rank	New domain TLD	Q3 2022	Zone size	% of zone newly observed	% of zone data bar
1	.skin	5,409	10,744	50.34%	
2	.beauty	9,922	24,121	41.13%	
3	.autos	5,241	13,400	39.11%	
4	.sbs	20,079	54,115	37.10%	
5	.click	78,824	214,774	36.70%	
6	.mom	4,095	11,608	35.28%	
7	.lol	14,197	41,634	34.10%	
8	.pics	6,861	21,218	32.34%	
9	.hair	3,042	11,860	25.65%	
10	.homes	6,973	33,765	20.65%	
11	.rest	10,567	53,260	19.84%	
12	.cam	5,083	26,925	18.88%	
13	.site	197,213	1,060,170	18.60%	
14	.gay	3,165	18,370	17.23%	
15	.store	146,189	862,305	16.95%	
16	.fun	56,202	334,481	16.80%	
17	.cfd	19,176	115,120	16.66%	
18	.live	106,475	641,652	16.59%	
19	.buzz	87,554	555,728	15.75%	
20	.online	306,458	1,981,087	15.47%	

0 20% 40% 60%

Trending terms...

Trending terms in new domains

There is little change in this list, with the first eight terms listed in this quarter's Top 20 identical to last quarter's. As many of the best names are gone, new domain owners are forced to add extra words to their names or business names if they want their domain to be in one of the more popular TLDs. This explains the large number of domains containing generic words associated with business, like "service", "online" or "store".

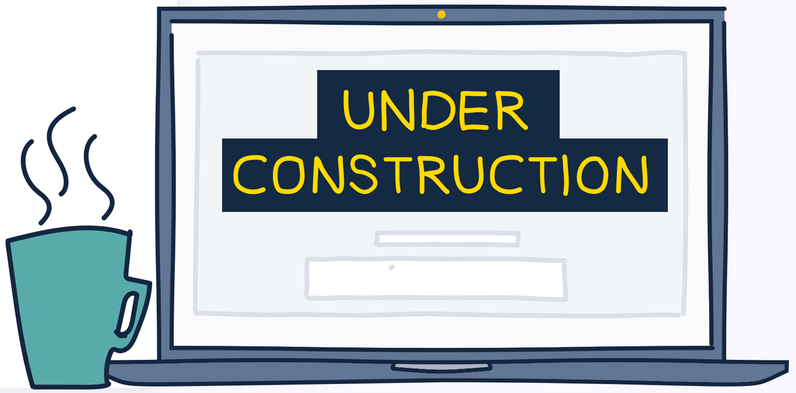
The most interesting change to note is the entry of "travel" in the Top 20. The world has almost entirely opened again after more than two years of Covid-related travel limitations, so domain buyers are clearly seeing opportunities.

When it comes to "ation," here's a breakdown of all the words in Q3 containing the term "ation":

- vacations **1073**
- transformation **1077**
- mediation **1165**
- renovations **1236**
- cation **1263**
- ovation **1388**
- installation **1402**
- communications **1429**
- ration **1430**
- immigration **1435**
- verification **1535**
- location **1581**
- innovations **1587**
- formation **1637**
- renovation **1674**

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	Q3 2022 trending terms	Q3 2022	Q3 data bar	Q2 2022	% Change
1	service	92,635		81,243	▲ 14%
2	ation	68,835		66,840	▲ 3%
3	online	67,872		60,351	▲ 12%
4	design	59,668		59,948	— 0%
5	market	56,031		48,007	▲ 17%
6	group	53,550		47,222	▲ 13%
7	solution	52,802		46,835	▲ 13%
8	studio	51,952		45,097	▲ 15%
9	store	49,365		41,235	▲ 20%
10	digital	48,777		40,970	▲ 19%
11	health	48,617		41,723	▲ 17%
12	consult	43,556		39,600	▲ 10%
13	product	37,263		17,076	▲ 118%
14	global	31,432		27,190	▲ 16%
15	invest	30,343		18,635	▲ 63%
16	today	28,990		22,244	▲ 30%
17	beauty	28,899		16,169	▲ 79%
18	travel	27,916		-	New entry
19	business	25,143		-	New entry
20	finance	25,046		-	New entry

Top 20 Trending... | Trending terms

Trending terms

Domains listed

Domain Overview

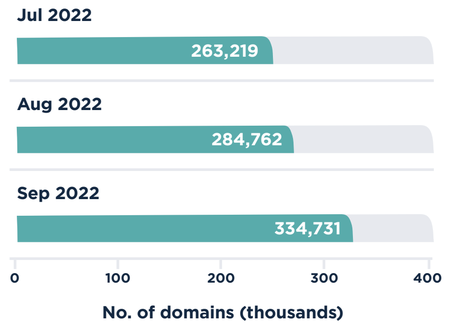
Over 880K domains were listed last quarter, with an average of 294K per month. This significantly reduced by 37% against the second quarter of 2022.

While most domain-related abuse still happens using very new domains, there is a slow but steady shift occurring where certain actors only use older domains. Some buy domains and let them age, regularly for a period of more than a year before usage.

Meanwhile, others use domain aftermarket operators where older domains can be acquired from sellers while retaining the original registration date. These domains come with an existing good reputation out of the box, which is, without doubt, the big driver for this “business” model.

Most concerning is that at least two malware operators now purchase old domains like these and repurpose them to send out their first-stage malware campaign emails. Using old and correctly set up domains increases their inbox reach and makes these malicious mails harder to detect.

Number of Domain listings per month



Quarterly Total
882,712
▼ -37% ▼

Monthly Average
294,237
▼ -173,327 ▼

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

There are two key issues this quarter's data highlights:

1. **.live –** We regularly see a connection between when registries run promotions and increased abusive/ fraudulent registrations. An excellent example of this was .live, which saw an 89% increase in the number of bad reputation domains listed in Q3. Over the same period, certain registrars offered this TLD with up to 90% off. Bad actors requiring multiple domains to try to avoid various filtering mechanisms will often use these promotions to get as many domains as possible for minimum cost. To these malicious operators, there is little care about what TLD they use.
2. **.live (#5) and .me (#10) –** These TLDs were associated with numerous bad reputation domains linked to SMS spam or phishing. As text messages offer only 160 characters, there is an inherent need for short domain names. At the same time, short domains are also more valuable, meaning that most TLDs will have had all the short names registered a long time ago.

Here, the less popular TLDs have a role to play, where plenty of four, five, or six-letter names are available and often for a bargain price compared to more established TLDs. We find large clusters connected to the increase in bad reputation domains.

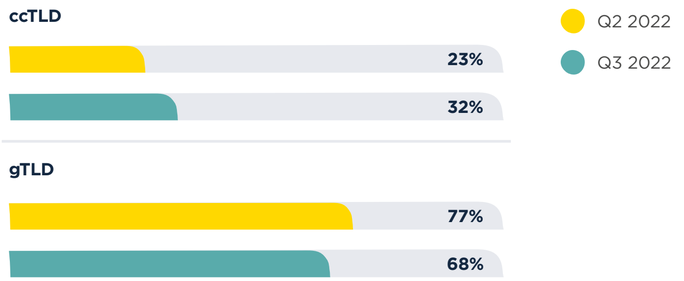
Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q3 2022 .info had more than 3.7 million domains in its zone, of which 1.23% were listed.

Meanwhile, .sbs had just over 54,000 domains in its zone, with 7.18% 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	Q3 2022	Q3 data bar	Q2 2022	% Change
1	.com	gTLD	278,077		675,968	-59%
2	.cn	ccTLD	93,086		128,017	-27%
3	.info	gTLD	46,245		58,334	-21%
4	.net	gTLD	44,474		53,282	-17%
5	.live	gTLD	38,987		20,680	89%
6	.top	gTLD	33,655		40,720	-17%
7	.tk	ccTLD	29,596		29,337	1%
8	.ml	ccTLD	24,222		19,353	25%
9	.xyz	gTLD	19,887		37,658	-47%
10	.me	ccTLD	15,147		-	New entry
11	.ga	ccTLD	14,694		15,021	-2%
12	.org	gTLD	14,670		21,198	-31%
13	.us	ccTLD	14,435		12,793	13%
14	.cf	ccTLD	12,458		14,519	-14%
15	.gq	ccTLD	11,966		11,596	3%
16	.online	gTLD	11,005		12,421	-11%
17	.uk	ccTLD	10,573		13,039	-19%
18	.shop	gTLD	9,070		-	New entry
19	.biz	gTLD	8,609		17,250	-50%
20	.icu	gTLD	8,422		-	New entry

0 150 300

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

Listings by Top 20 ccTLDs

Rank	Domain TLD	Q3 2022	Q3 data bar	Q2 2022	% Change
1	.cn	93,086		128,017	-27%
2	.tk	29,596		29,337	1%
3	.ml	24,222		19,353	25%
4	.me	15,147		4,359	247%
5	.ga	14,694		15,021	-2%
6	.us	14,435		12,793	13%
7	.cf	12,458		14,519	-14%
8	.gq	11,966		11,596	3%
9	.uk	10,573		13,039	-19%
10	.co	7,871		7,647	3%
11	.ru	6,492		15,033	-57%
12	.cc	6,187		6,816	-9%
13	.in	5,484		10,346	-47%
14	.de	4,091		2,295	78%
15	.fr	3,679		-	New entry
16	.pw	2,852		2,987	-5%
17	.pl	2,833		-	New entry
18	.eu	2,389		2,970	-20%
19	.id	1,858		-	New entry
20	.nl	1,469		-	New entry

0 50 100

Top 20 gTLDs...

Top 20 gTLDs used in domain listings

Rank	Domain TLD	Q3 2022	Q3 data bar	Q2 2022	% Change
1	.com	278,077		675,968	▽ -59%
2	.info	46,245		58,334	▽ -21%
3	.net	44,474		53,282	▽ -17%
4	.live	38,987		20,680	△ 89%
5	.top	33,655		40,720	▽ -17%
6	.xyz	19,887		37,658	▽ -47%
7	.org	14,670		21,198	▽ -31%
8	.online	11,005		12,421	▽ -11%
9	.shop	9,070		10,205	▽ -11%
10	.biz	8,609		17,250	▽ -50%
11	.icu	8,422		5,929	△ 42%
12	.site	6,571		6,196	△ 6%
13	.click	5,609		4,339	△ 29%
14	.buzz	4,960		3,874	△ 28%
15	.club	3,913		7,810	▽ -50%
16	.sbs	3,886		-	New entry
17	.rest	3,709		-	New entry
18	.link	2,738		-	New entry
19	.fun	2,544		-	New entry
20	.cfd	2,416		-	New entry

0 150 300

Top 20 gTLD...

Top 20 gTLD by % of zone file with domain listings

Rank	Domain TLD	Q3 2022	Zone size	% of zone listed	% of zone data bar
1	.cam	2,230	26,925	8.28%	
2	.sbs	3,886	54,115	7.18%	
3	.rest	3,709	53,260	6.96%	
4	.live	38,987	641,652	6.08%	
5	.beauty	928	24,121	3.85%	
6	.casa	659	18,666	3.53%	
7	.support	969	34,176	2.84%	
8	.click	5,609	214,774	2.61%	
9	.fyi	1,295	51,003	2.54%	
10	.autos	306	13,400	2.28%	
11	.fit	1,041	47,275	2.20%	
12	.cfd	2,416	115,120	2.10%	
13	.best	517	31,271	1.65%	
14	.bid	290	18,038	1.61%	
15	.bond	374	23,543	1.59%	
16	.haus	160	10,242	1.56%	
17	.link	2,738	191,792	1.43%	
18	.zone	614	44,034	1.39%	
19	.pics	272	21,218	1.28%	
20	.info	46,245	3,761,411	1.23%	

0% 2% 4% 6% 8% 10%

Trending phishing terms in domain listings

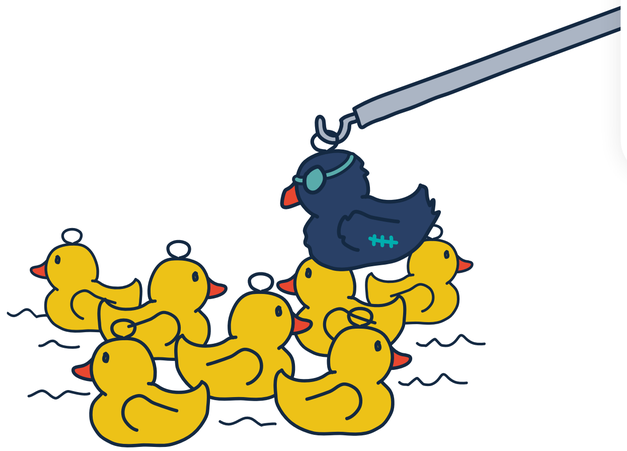
With fraudulent phishing domains (as opposed to legitimate ones that get abused due to website compromises), most bad actors try to create something that looks somewhat legitimate. As the actual target brand names, e.g., amazon, are obviously unavailable, many resort to creating URLs with domains that convey a sense of urgency. Many of these names can be split into sections, each with a role to play in luring the victim in:

- **The brand name -** (icloud, amazon, paypal, etc.) attracts the eye and conveys legitimacy.
- **The context -** (id, account, service, etc.) provides the user with the subject matter.
- **The action -** (update, verify, check, resolve, payment) is the call to action to make the victim click.

In addition to using the full domain name, the above can also be employed to the hostnames. Despite this being a well-known method, we still see plenty of domains that start with ".com", often followed by some other technical-looking term we classify as 'infrastructure words'.

Examples include strings like "ssl", "config", "app", or technical-looking strings with numbers. The target part of the phishing URL is then placed in the hostname, e.g. www.apple.com-en.us, to create a familiar-looking URL for the victim.

The Top 20 terms in phishing domains change position, but in general, we see the same terms repeatedly. Consequently, it should be possible for registrars and registries to be more proactive in finding these domains and applying extra verification in case of possibly malicious names.



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	Q3 2022	Q3 data bar	Q2 2022	% Change
1	secure	6,802		9,460	▼ -28%
2	online	6,614		6,251	▲ 6%
3	support	6,370		6,995	▼ -9%
4	account	6,183		6,518	▼ -5%
5	service	5,488		4,785	▲ 15%
6	security	3,956		3,620	▲ 9%
7	verification	3,950		4,368	▼ -10%
8	verify	3,275		4,474	▼ -27%
9	amazon	3,240		9,759	▼ -67%
10	check	3,210		-	New entry
11	icloud	3,184		4,018	▼ -21%
12	session	3,134		3,069	▲ 2%
13	apple	3,131		3,971	▼ -21%
14	intl	2,824		-	New entry
15	cloud	2,493		-	New entry
16	info	2,397		6,174	▼ -61%
17	update	2,369		2,444	▼ -3%
18	payment	2,024		1,910	▲ 6%
19	connect	2,010		-	New entry
20	jobs	1,883		-	New entry

Top 20 phishing... | Phishing terms

Phishing terms

Types of listings

The enormous increase in compromised URLs in the malware category in September stands out immediately. This becomes even more interesting once you know that the increase only happened in the last two weeks of the month, when researchers started to see a large influx of similar-looking URLs that have been traced back to being part of Quakbot infrastructure.

These are all website compromises, often due to outdated, insecure, or backdoored content management systems (CMS), mostly WordPress. The problem here is not very different from why a home or office device gets compromised; website owners or maintainers often do not apply long-available patches and updates. Miscreants scan for these versions automatically, and it is not uncommon to see one scanner try hundreds of different URLs for various plugins and versions.

For compromised domains that are exhibiting malicious behavior, please keep a few things in mind:

- The vast majority of these compromises are done via automated means, and machines do not care about the associated TLD.
- Many compromised websites are given the "gift" of a Traffic Distribution System (TDS). These allow the bad actors to rotate content, URLs, and geoblockling. Our researchers see hundreds of unique URLs for some sites, some of which have been active for months.
- Currently, the majority of compromises we observe are at the website level, as described above. Bad actors use these to get "free" domains with an existing, good reputation. The added bonus is that these domains will not be taken down, as the owners are legitimate.
- In a few cases, we see compromises at the DNS level. These usually occur through stolen registrar credentials or sometimes through stolen or hacked administration panels like cPanel or Plesk. Once control over the authoritative DNS is in the hands of bad actors, it's easy for them to add hostnames that can point to their own infrastructure. Again, the benefit here is that existing domains with a good reputation are being used for bad purposes.

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
438,101	10,410
▼ -55% ▼	▼ -18% ▼

A domain's reputation score has exceeded policy limits.

Botnet C&C

Malicious	Compromised
3,608	29
▼ -24% ▼	▼ -49% ▼

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

Malware

Malicious	Compromised
5,181	3,514
▼ -17% ▼	▼ -20% ▼

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

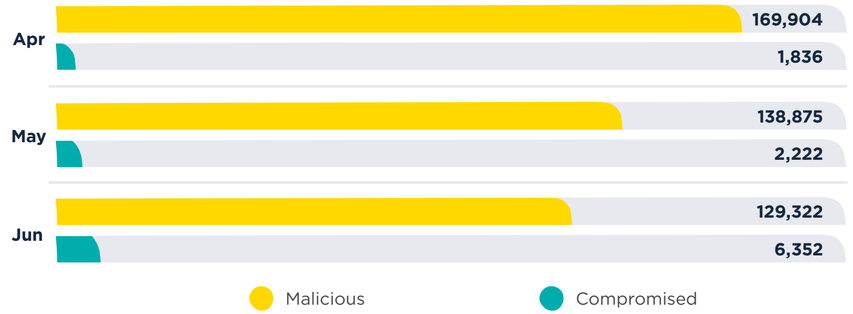
Phishing

Malicious	Compromised
316,215	10,459
▲ 14% ▲	▲ 67% ▲

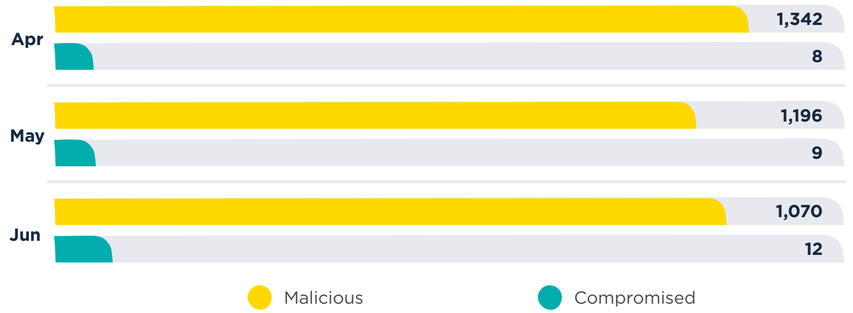
A domain is associated with phishing activities. (A subset of bad reputation.)

Types of abuse

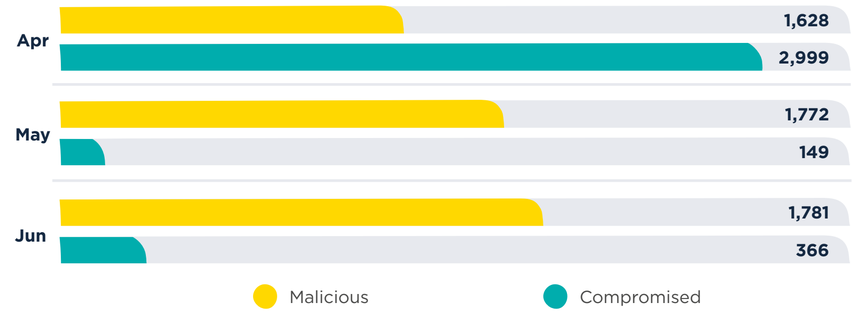
Bad reputation per month



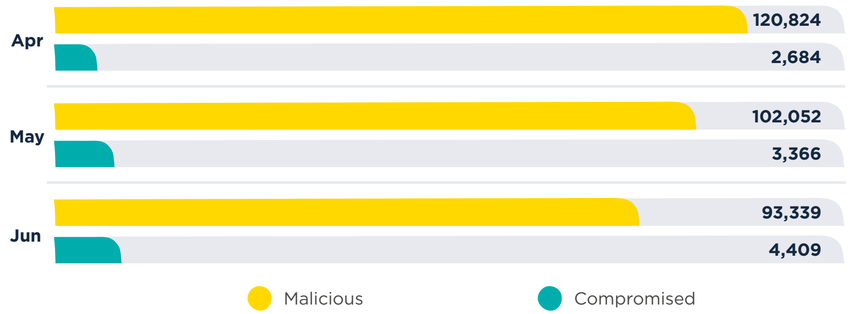
Botnet C&C per month



Malware per month



Phishing per month



Recommend...

Recommendations of the quarter

As seen in the previous section, malware operators can quickly gain control of many unique domains and URLs. Part of this is enabled by an ecosystem of actors specializing in uncovering and compromising these sites and supplying them to others for use in malware or phishing campaigns. Demand is high, and with so many websites vulnerable, many are ripe for the picking. This is what this quarter's recommendations focus on. Some of these apply to website owners, some to developers, and some to hosting companies:

1. **Keep your CMS updated** - Website owners that run popular third-party software such as WordPress or Drupal need to ensure these packages are updated. Both offer notifications in case problems are found and are very quick in pushing out updates.
2. **Plugins should also be updated** - More often than not, it isn't the core software but a plugin that is vulnerable. The same advice applies here: keep your additional applications up to date.
3. **Website owners know your skill limitations –** If you are not comfortable running website infrastructures, ensure you find someone who can help. Managed hosting providers usually can assist, but please remember to you do your homework. After all, you don't want your website hosted in a bad neighborhood, which could negatively affect your domain's reputation.
4. **Don't wait for an issue to be raised** - Hosting companies with multiple websites should proactively scan their environments, monitor complaints, and, where possible, monitor feeds of compromised URLs.
5. **Thoroughly remediate when problems occur** - Compromises happen, and luckily so do cleanups. However, just deleting the malicious files is not enough, as the problem that caused the malicious content to appear will still be there – ensure you get to the root cause of the problem.

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.