



Spamhaus Quarterly Domain Reputation Update

Q4 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 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 Q4 2022.

[Enter](#)





Contents

The Overview

01 The Overview

02 So why do we look at domains and their associated reputation? Why does it make sense to use a domain name as a reputation marker?

03 Decisions relate to...

04 Domains have a predict...

05 extract and act upon...

06 use of domains (or host...

07 This doesn't come as an...

08 System (DNS) is fundame...

09 the internet, and at its core...

10 DNS associate domain names with...

11 (https://en.wikipedia.org/wiki/Domain_name_system)

12 No matter what you're doing on the internet, legitimate or otherwise, you must (almost always) use a domain name. Without a domain name, most malicious activity wouldn't get started, let alone be successful.

Spamhaus Quarterly Domain Name Update Q4-2022

Go to page 3

New domains

01 New domains

02 New domains overview

03 A total of 15.3 million new domains were registered in the first quarter of 2022, with a monthly average of 5.1 million. This is a significant increase from the 12.5 million domains registered in Q4 2021, with a monthly average of 4.2 million domains.

04 May was the busiest month with 6.5 million domains registered, followed by April with 6.2 million and June with 5.8 million. All three months were close to the monthly average.

05 It is important to note that a significant portion of these new domains are used for legitimate purposes. However, a considerable amount of new domain names are used for malicious purposes. 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.

Spamhaus Quarterly Domain Name Update Q4-2022

Go to page 5

Domains listed

01 Domains listed

02 Domain Overview

03 Just over 1.4 million domains were listed in the first quarter of 2022, with an average of 466k per month. This is a significant increase from the 1.1 million domains listed in Q4 2021, with an average of 367k per month.

04 There is a clear divide between bid operators who use new domains as quickly as possible and those who age domains to evade the negative reputational impact of a new domain. Aging times vary from a few weeks to over a year.

05 Some bad operators prefer to buy existing domains second-hand to exploit the domains' existing good reputation. The ability to purchase domains is becoming easier and easier.

Spamhaus Quarterly Domain Reputation Update Q4-2022

Go to page 11

Recommendations of the quarter

01 Recommendations of the quarter

02 Assuming you control your domain name, ensure it stays that way. Have a strong and unique login/pass combination for domain name management and add 2FA onto that.

03 Hosting your domain name on a questionable network may affect your domain's reputation. Just as a business contributes to its neighborhood, so the neighborhood's reputation affects the business. Remember that domains with a good reputation...

04 Domain name, make sure it is easy to remember and filter it.

05 Limit the number of domain names you use. When buying additional domain names, always ask yourself if using a subdomain of your primary domain name is better. Often it is. If you really need different domain names, ensure they can be easily tied to the primary domain name, and always consider the reputational impact of a new domain name on email, SEO, etc.

Spamhaus Quarterly Domain Name Update Q4-2022

Go to page 20

Additional info

01 Additional info

02 About Spamhaus

03 Spamhaus is the trusted authority for domain reputation. We are uniquely placed in the industry to provide this data. Our data is impartial, and quality is maintained through rigorous processes and machine learning, heuristics, and manual review. Our report reflects the malicious activity identified and listed, and is a reflection of the malicious and bad reputation of domains.

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

05 Previous reports: This won't be applicable for the first, but providing a URL to the where all the other reports are kept would be helpful (once we have a resource center that can provide this functionality. In the meantime maybe we send the to a piece of meaningful content.

Spamhaus Quarterly Domain Name Update Q4-2022

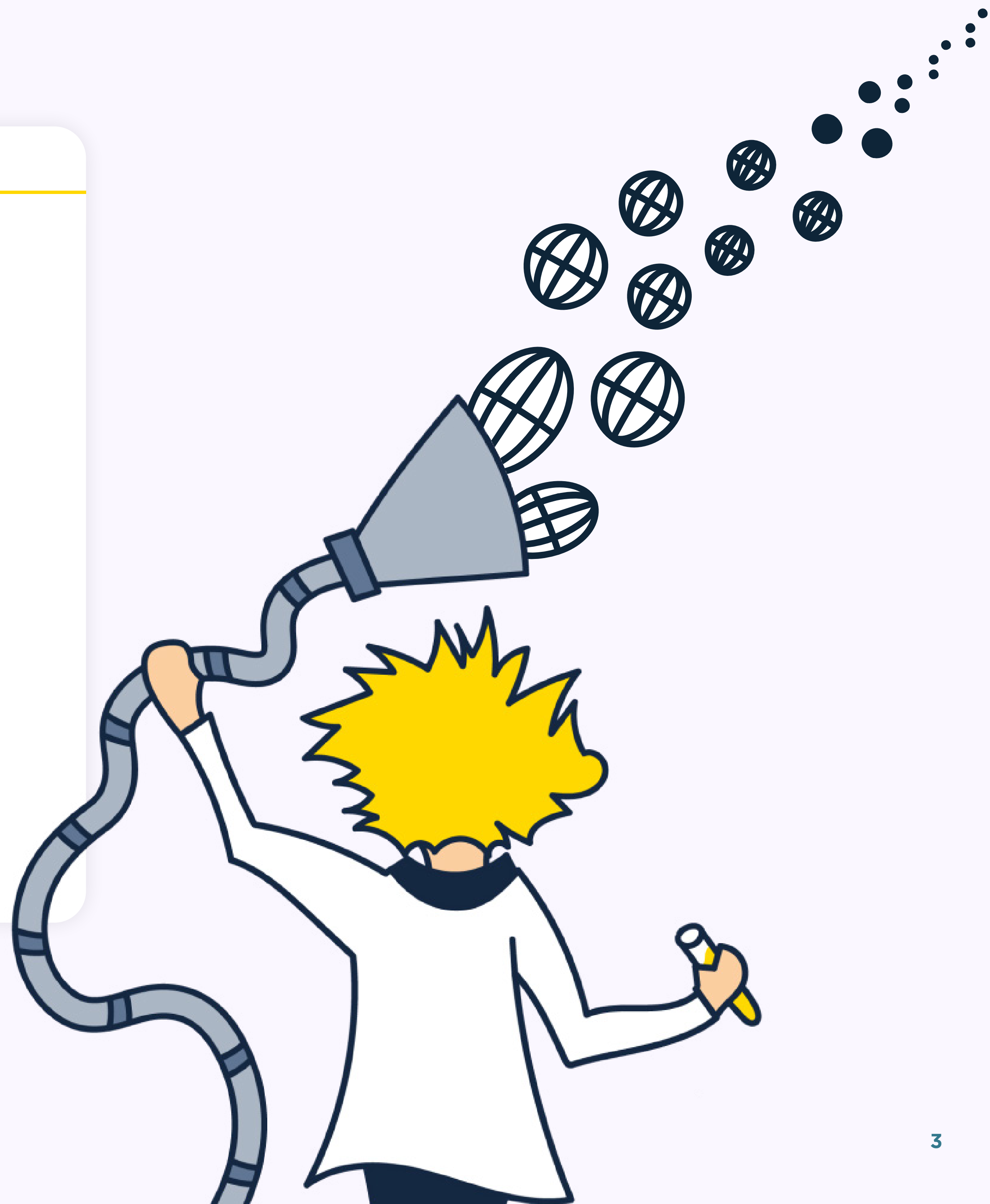
Go to page 21

The Overview

As anticipated, the number of newly observed and listed domains increased in Q4 2022. That's no surprise, given the increase in e-commerce activity which occurred every month during this quarter. This increased activity isn't just down to legitimate traders but also includes spammers, phishers, and other cybercriminals, all trying to capture the same money.

When considering the +7% domain listing increase in Q4, compared to last quarter, there isn't one issue to blame; it's just more of everything. More phishing targeting the same brands. More spam from the same spammers. But the increase was undoubtedly partially driven by some specific top level domains (TLDs) having aggressive sales campaigns that enabled bad actors to abuse a larger volume of domains for the same budget.

[Overview continued](#)



01

02

03

04

05

01

Overview cont. ✕

This isn't anything out of the ordinary, of course. In the search for revenue before the end of the year, it's not unusual for even established bonafide companies to cut corners. They may, for example, send one more email to a segment of non-responsive customers one more time in the hope of making a sale. The bad operators are no different, although they will target more people with more communications overall.

The good news is while the domains listed for Q4 are up, they are still lower than Q4 2021, when Spamhaus had listed over 2.1 million domains. Before readers get too excited, this does not necessarily mean that there is less abuse. We still see a considerable amount of domain re-usage and abuse of free services in places where filtering happens (e.g, the body of an email). But we are hopeful this may quickly turn around again if some of the most commonly exploited free services clamp down on abuse by nefarious players.

02

03

04

05



01

New domains

New domains overview

A total of 18.5 million new domains were registered last quarter, with a monthly average of 6.2 million. This was a reasonable increase of 18% against Q3 2022, when researchers observed 15.6 million new domains.

November was the busiest month of Q4, with close to 7 million new domains. That doesn't come as a big surprise, given that there are notable shopping events in November - Black Friday, Cyber Monday - and the lead up to the festive holiday period begins.

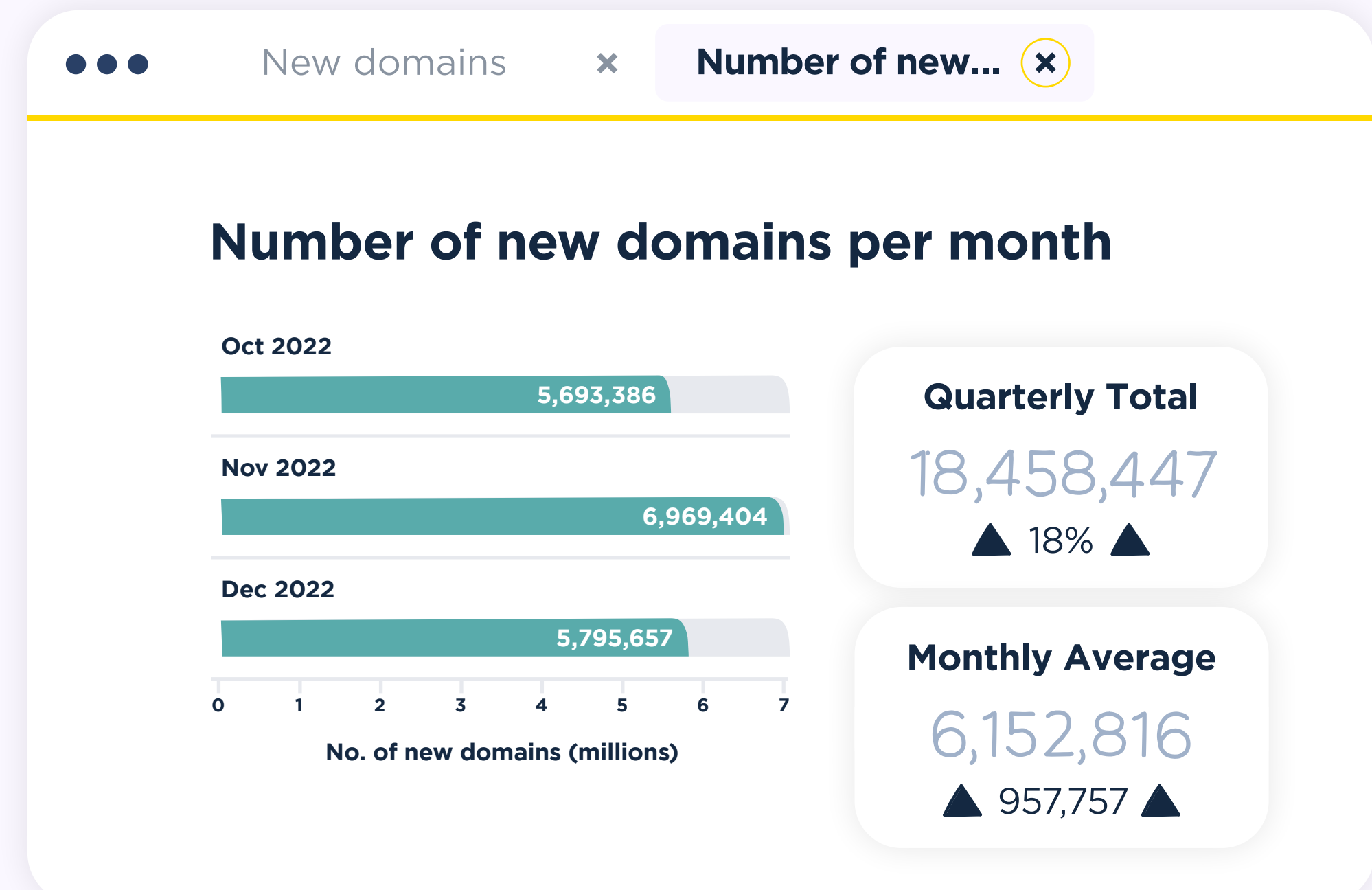
It is important to note that a new domain is not a bad domain per se. However, a considerable amount of abuse is associated with new domain names. One reason is that if a bad actor buys a new domain and uses it immediately, there is minimal chance of security systems & professionals having prior knowledge of this domain's existence. Unfortunately, its existence is only discovered once the malicious campaign starts. Furthermore, by using new domains, bad actors prevent registries and registrars from doing pre-emptive takedowns.

02

03

04

05



i 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.

01

New domains by top-level domain (TLD)

ccTLDs continued in popularity (rising from 37% in Q3 to 43% in Q4). However, it's important to understand the ccTLD landscape. Some of the ccTLDs with the largest number of new domains are not only run as a gTLD (anyone, anywhere, can register a domain in these TLDs), but are given away for free. Unsurprisingly, a large amount of abuse can be connected to these registrations.

As mentioned, Black Friday, Cyber Monday, and Christmas all fall within Q4 and are associated with online shopping. It's no wonder that there was a sharp increase of +47% in .shop domains. Another driver for that growth, along with .click's (+33%), could be that these gTLDs were sold at select registrars for just over US \$2, reducing to US \$1.69 for bulk registrations. Historically TLDs with aggressive pricing have been targeted by operators that require large amounts of domains to enable their abuse.

We expect this to continue.

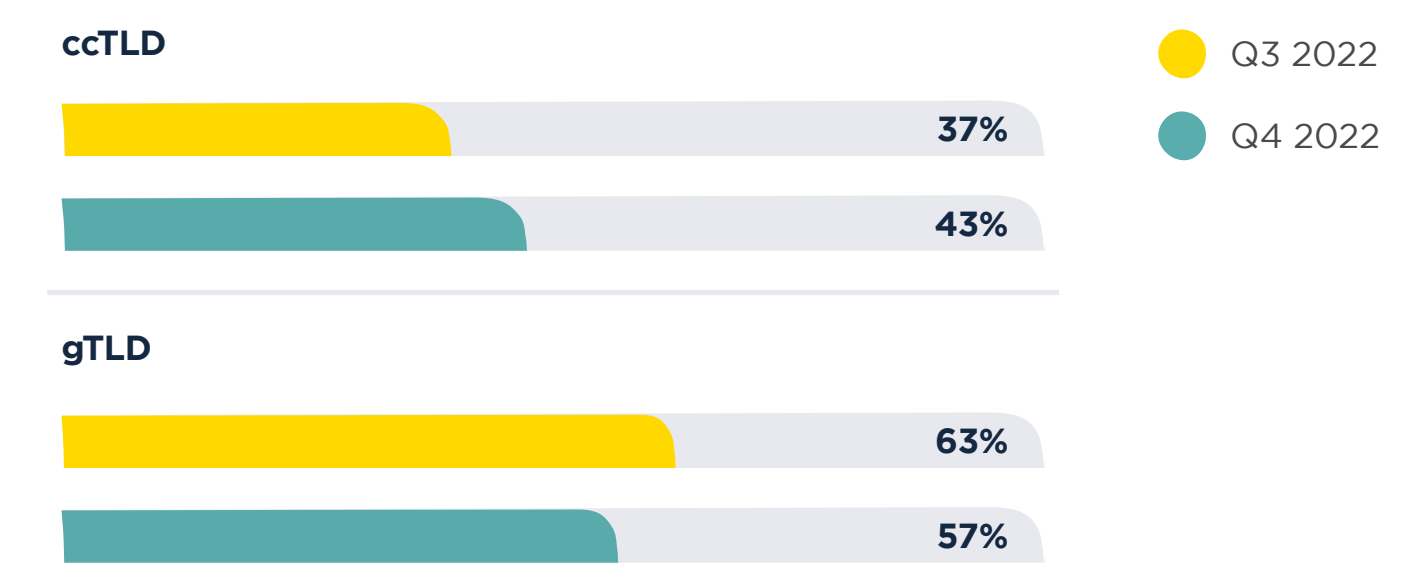
02

03

04

05

New domain TLD types comparison, quarter on quarter



i Top-level domains – a quick explanation

There are a couple of different top-level domains (TLDs) including:

- **Generic TLDs (gTLDs)** - these are under ICANN jurisdiction. Some gTLDs are open i.e. can be used by anyone e.g., .com, some have strict policies regulating who and how they can be used e.g., .bank, and some are closed e.g., .honda.
- **Country code TLDs (ccTLDs)** - typically these relate to a country or region. Registries define the policies relating to these TLDs; some allow registrations from anywhere, some require local presence, and some license their namespace wholesale to others.

01

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

Top 20 TLDs used in new domains

| Rank | New domain TLD | TLD type | Q4 2022 | Q4 data bar | Q3 2022 | % Change |
|------|----------------|----------|-----------|-------------|-----------|-----------|
| 1 | .com | gTLD | 5,823,730 | | 5,808,863 | ▶ 0% |
| 2 | .tk | ccTLD | 868,574 | | 491,807 | ▲ 77% |
| 3 | .ml | ccTLD | 570,075 | | 252,551 | ▲ 126% |
| 4 | .xyz | gTLD | 451,091 | | 447,214 | ▲ 1% |
| 5 | .ga | ccTLD | 444,697 | | 290,995 | ▲ 53% |
| 6 | .de | ccTLD | 398,781 | | 352,811 | ▲ 13% |
| 7 | .online | gTLD | 374,985 | | 306,458 | ▲ 22% |
| 8 | .cf | ccTLD | 368,491 | | 203,546 | ▲ 81% |
| 9 | .net | gTLD | 361,308 | | 382,156 | ▼ -5% |
| 10 | .cn | ccTLD | 350,215 | | 291,411 | ▲ 20% |
| 11 | .shop | gTLD | 348,971 | | 237,288 | ▲ 47% |
| 12 | .org | gTLD | 329,624 | | 315,205 | ▲ 5% |
| 13 | .gq | ccTLD | 327,203 | | - | New entry |
| 14 | .top | gTLD | 291,013 | | 257,526 | ▲ 13% |
| 15 | .ru | ccTLD | 258,471 | | 189,140 | ▲ 37% |
| 16 | .co.uk | ccTLD | 248,291 | | 189,694 | ▲ 31% |
| 17 | .nl | ccTLD | 244,664 | | 240,556 | ▲ 2% |
| 18 | .com.br | ccTLD | 235,377 | | 177,186 | ▲ 33% |
| 19 | .co | ccTLD | 230,478 | | 160,411 | ▲ 44% |
| 20 | .fr | ccTLD | 223,428 | | - | New entry |

02

03

04

05

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

Top 20 ccTLDs used in new domains

| Rank | New domain TLD | Q4 2022 | Q4 data bar | Q3 2022 | % Change |
|------|----------------|---------|-------------|---------|-----------|
| 1 | .tk | 868,574 | | 491,807 | ▲ 77% |
| 2 | .ml | 570,075 | | 252,551 | ▲ 126% |
| 3 | .ga | 444,697 | | 290,995 | ▲ 53% |
| 4 | .de | 398,781 | | 352,811 | ▲ 13% |
| 5 | .cf | 368,491 | | 203,546 | ▲ 81% |
| 6 | .cn | 350,215 | | 291,411 | ▲ 20% |
| 7 | .gq | 327,203 | | 155,426 | ▲ 111% |
| 8 | .ru | 258,471 | | 189,140 | ▲ 37% |
| 9 | .co.uk | 248,291 | | 189,694 | ▲ 31% |
| 10 | .nl | 244,664 | | 240,556 | ▲ 2% |
| 11 | .com.br | 235,377 | | 177,186 | ▲ 33% |
| 12 | .co | 230,478 | | 160,411 | ▲ 44% |
| 13 | .fr | 223,428 | | 131,042 | ▲ 71% |
| 14 | .in | 178,681 | | 139,536 | ▲ 28% |
| 15 | .au | 170,589 | | 89,693 | ▲ 90% |
| 16 | .ca | 143,743 | | 108,670 | ▲ 32% |
| 17 | .eu | 119,524 | | 96,261 | ▲ 24% |
| 18 | .cc | 117,063 | | - | New entry |
| 19 | .ch | 115,865 | | - | New entry |
| 20 | .com.au | 113,880 | | 98,809 | ▲ 15% |

01

●●● Top20 gTLD - new ✕ Top20 gTLDs - zone ✕

Top 20 gTLDs used in new domains

| Rank | New domain TLD | Q4 2022 | Q4 data bar | Q3 2022 | % Change |
|------|----------------|-----------|-------------|-----------|-----------|
| 1 | .com | 5,823,730 | | 5,808,863 | ▶ 0% |
| 2 | .xyz | 451,091 | | 447,214 | ▲ 1% |
| 3 | .online | 374,985 | | 306,458 | ▲ 22% |
| 4 | .net | 361,308 | | 382,156 | ▼ -5% |
| 5 | .shop | 348,971 | | 237,288 | ▲ 47% |
| 6 | .org | 329,624 | | 315,205 | ▲ 5% |
| 7 | .top | 291,013 | | 257,526 | ▲ 13% |
| 8 | .site | 220,922 | | 197,213 | ▲ 12% |
| 9 | .info | 198,675 | | 174,525 | ▲ 14% |
| 10 | .store | 149,160 | | 146,189 | ▲ 2% |
| 11 | .cyou | 134,946 | | - | New entry |
| 12 | .buzz | 116,313 | | 87,554 | ▲ 33% |
| 13 | .click | 104,836 | | 78,824 | ▲ 33% |
| 14 | .live | 71,105 | | 106,475 | ▼ -33% |
| 15 | .work | 64,794 | | - | New entry |
| 16 | .vip | 63,529 | | 86,703 | ▼ -27% |
| 17 | .space | 53,138 | | 56,370 | ▼ -6% |
| 18 | .fun | 48,508 | | 56,202 | ▼ -14% |
| 19 | .tech | 46,609 | | 45,326 | ▲ 3% |
| 20 | .club | 43,627 | | 41,286 | ▲ 6% |

02

03

04

05

●●● Top20 gTLD - new ✕ Top20 gTLDs - zone ✕

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

| Rank | New domain TLD | Q4 2022 | Zone size | % of zone newly observed | % of zone data bar |
|------|----------------|---------|-----------|--------------------------|--------------------|
| 1 | .kred | 26,007 | 53,060 | 49.01% | |
| 2 | .cfd | 34,904 | 77,584 | 44.99% | |
| 3 | .bond | 16,724 | 37,474 | 44.63% | |
| 4 | .football | 4,372 | 10,165 | 43.01% | |
| 5 | .mom | 7,311 | 19,004 | 38.47% | |
| 6 | .click | 104,836 | 292,402 | 35.85% | |
| 7 | .best | 11,044 | 31,271 | 35.32% | |
| 8 | .rest | 16,076 | 46,178 | 34.81% | |
| 9 | .sbs | 25,475 | 75,235 | 33.86% | |
| 10 | .monster | 23,886 | 74,412 | 32.10% | |
| 11 | .autos | 5,741 | 18,850 | 30.46% | |
| 12 | .lol | 17,384 | 59,507 | 29.21% | |
| 13 | .beauty | 9,714 | 33,556 | 28.95% | |
| 14 | .homes | 11,845 | 43,813 | 27.04% | |
| 15 | .pics | 7,096 | 27,905 | 25.43% | |
| 16 | .shop | 348,971 | 1,377,691 | 25.33% | |
| 17 | .skin | 3,430 | 14,005 | 24.49% | |
| 18 | .shopping | 2,995 | 12,436 | 24.08% | |
| 19 | .work | 64,794 | 271,336 | 23.88% | |
| 20 | .bar | 25,078 | 105,781 | 23.71% | |

01

02

03

04

05

●●● Trending terms... ✕

Trending terms in new domains

With the year’s final quarter so heavily focused on shopping, it wasn’t surprising to see the term ‘store’ climbing from #9 in Q3 to #6 in Q4, with a 21% increase. However, there were no vast increases or decreases in other trending terms, compared to Q3. Most of the key words were reasonably generic. This happens when the initial desired term (which is usually in high demand) is no longer available.

The second most popular term was “ation”. Here’s a breakdown of the top 15 words containing “ation” we saw in Q4:

- innovations **1,875**
- aviation **1,984**
- location **2,046**
- formation **2,057**
- renovation **2,127**
- transportation **2,146**
- corporation **2,247**
- information **2,317**
- vacation **2,395**
- automation **2,863**
- creation **3,114**
- innovation **3,273**
- association **3,315**
- station **4,333**
- national **4,476**

i Methodology for trending terms ✕

We use a text vectorizer to find the most common strings in new domain names and break the counts down by date, which highlights trends in domain name themes. For example, we saw a spike in domain names containing “ukraine” following the Russian invasion.



01

02

03

04

05

Top 20 trending terms in new domains

| Rank | Q4 2022 trending terms | Q4 2022 | Q4 data bar | Q3 2022 | % Change |
|------|------------------------|---------|-------------|---------|-----------|
| 1 | service | 100,221 | | 92,635 | ▲ 8% |
| 2 | ation | 76,330 | | 68,835 | ▲ 11% |
| 3 | online | 75,182 | | 67,872 | ▲ 11% |
| 4 | design | 65,343 | | 59,668 | ▲ 10% |
| 5 | market | 61,122 | | 56,031 | ▲ 9% |
| 6 | store | 59,925 | | 49,365 | ▲ 21% |
| 7 | studio | 58,062 | | 51,952 | ▲ 12% |
| 8 | group | 57,699 | | 53,550 | ▲ 8% |
| 9 | solution | 56,807 | | 52,802 | ▲ 8% |
| 10 | digital | 54,303 | | 48,777 | ▲ 11% |
| 11 | health | 53,865 | | 48,617 | ▲ 11% |
| 12 | consult | 47,804 | | 43,556 | ▲ 10% |
| 13 | invest | 32,322 | | 30,343 | ▲ 7% |
| 14 | marketing | 32,051 | | - | New entry |
| 15 | beauty | 30,320 | | 28,899 | ▲ 5% |
| 16 | product | 30,290 | | 37,263 | ▼ -19% |
| 17 | creative | 29,924 | | - | New entry |
| 18 | business | 29,245 | | 25,143 | ▲ 16% |
| 19 | travel | 29,216 | | 27,916 | ▲ 5% |
| 20 | media | 29,045 | | - | New entry |

0 20 40 60 80 100

Trending terms



01

Domains listed

Domain Overview

Over 940K domains were listed in Q4, with an average of 315K per month. This was a marginal increase of 7% against the third quarter of 2022.

Most phishing, business email compromise (BEC) fraud, and related cybercrime still favors new domain names. This, no doubt, is because the domain name involved in this type of abuse must be similar to the company or brand name the bad actor is targeting, so specific new domains need to be purchased. In cases where this is less important, we do see a slow but steady increase in the use of older, more established domain names.

As discussed last quarter, the latter concerns us the most when aged domains are used to facilitate spamming that delivers malware by email. Using established domain names with good reputation makes it harder for these malicious emails to be identified and dealt with.

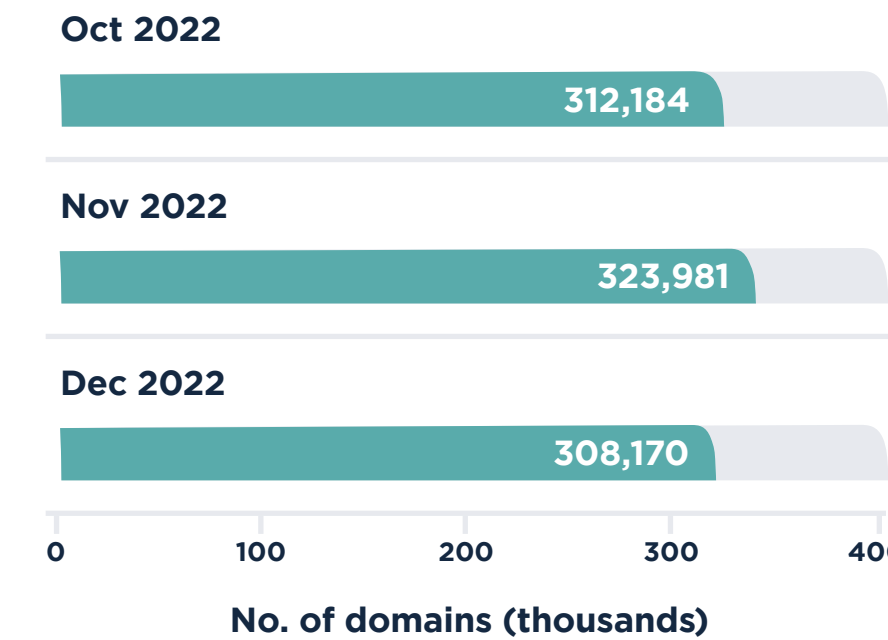
02

03

04

05

Number of Domain listings per month



Quarterly Total

944,335

▲ 7% ▲

Monthly Average

314,778

▲ 20,541 ▲

i 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.

01

Trending terms... x

TLDs listed in our domain data

All Freenom pseudo gTLDs experienced sharp increases in the number of domains listed, but the surge (+172%) in .ml domains stands out. Jump to [Types of Abuse](#) to find out why.

When it comes to nonsense names, these come in various shapes and sizes. Some of them immediately look suspicious. Domain-generated algorithms (DGAs) can easily create random nonsensical names, which ensures that an outsider (such as a threat researcher) can't guess the next domain name in the sequence.

When we can attribute a TLD's growth almost entirely to these nonsense strings, we question the validity of these registrations. Such is the case for .co, which experienced a +112% increase in listings in Q4. While .co is technically the country TLD for Colombia, it has an open registration and is actively promoted as an alternative to .com. We have seen many questionable new registrations inside the .co space, consisting of these random strings. We suspect these are all owned by one or, at most, a handful of owners.

It's worth mentioning that not all malicious bulk registrations are as easy to identify. Some operators go to great lengths to make correlations almost impossible to spot. This allows them to fly below the radar for as long as possible.

Interpreting the data x

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q4 2022, .click had almost 300k domains in its zone, of which 1.7% were listed.

Meanwhile, .beauty had just over 33.5k domains in its zone, with 6.37% 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.

02

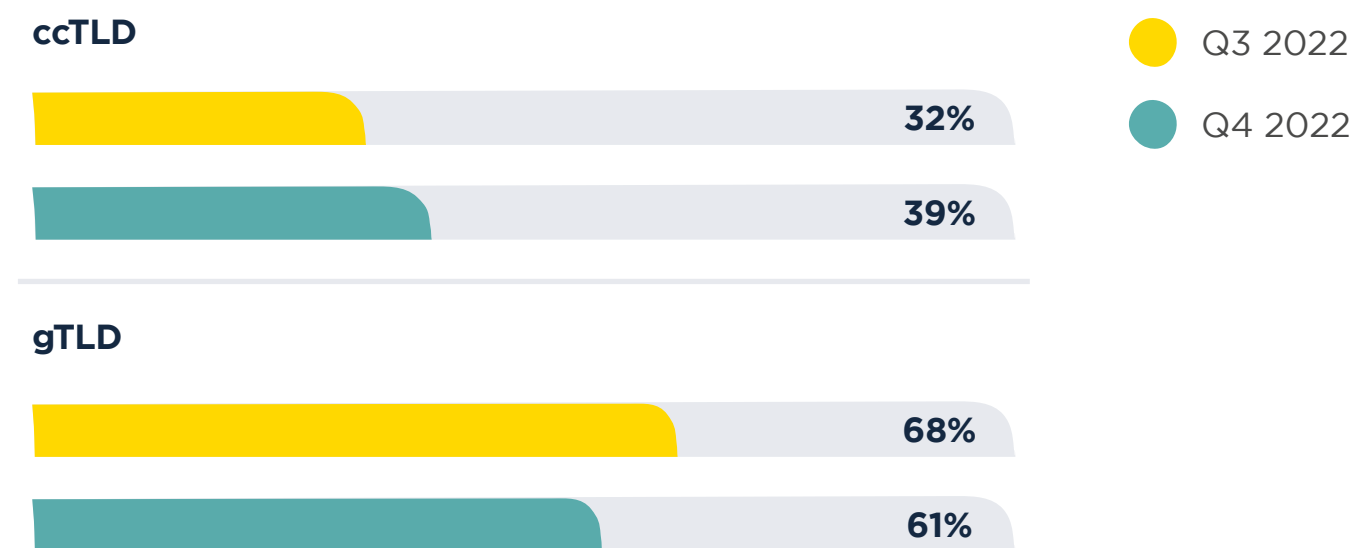
03

04

05

Domain listing... x

Domain listing TLD type comparison, quarter on quarter



01

●●● Top 20 TLDs... x Listings by... x

Top 20 TLDs listed

| Rank | Domain TLD | Type of TLD | Q4 2022 | Q4 data bar | Q3 2022 | % Change |
|------|------------|-------------|---------|-------------|---------|-----------|
| 1 | .com | gTLD | 278,629 | | 278,077 | ▶ 0% |
| 2 | .cn | ccTLD | 87,989 | | 93,086 | ▼ -5% |
| 3 | .ml | ccTLD | 65,866 | | 24,222 | ▲ 172% |
| 4 | .top | gTLD | 46,052 | | 33,655 | ▲ 37% |
| 5 | .tk | ccTLD | 36,662 | | 29,596 | ▲ 24% |
| 6 | .net | gTLD | 35,940 | | 44,474 | ▼ -19% |
| 7 | .info | gTLD | 29,169 | | 46,245 | ▼ -37% |
| 8 | .live | gTLD | 22,198 | | 38,987 | ▼ -43% |
| 9 | .ga | ccTLD | 19,979 | | 14,694 | ▲ 36% |
| 10 | .me | ccTLD | 19,742 | | 15,147 | ▲ 30% |
| 11 | .us | ccTLD | 18,771 | | 14,435 | ▲ 30% |
| 12 | .xyz | gTLD | 18,182 | | 19,887 | ▼ -9% |
| 13 | .cf | ccTLD | 17,646 | | 12,458 | ▲ 42% |
| 14 | .gq | ccTLD | 16,693 | | 11,966 | ▲ 40% |
| 15 | .co | ccTLD | 16,674 | | - | New entry |
| 16 | .ru | ccTLD | 13,817 | | - | New entry |
| 17 | .link | ccTLD | 13,545 | | - | New entry |
| 18 | .org | gTLD | 12,778 | | 14,670 | ▼ -13% |
| 19 | .shop | gTLD | 10,966 | | 9,070 | ▲ 21% |
| 20 | .site | gTLD | 9,603 | | - | New entry |

02

03

04

05

●●● Top 20 TLDs... x Listings by... x

Listings by Top 20 ccTLDs

| Rank | Domain TLD | Q4 2022 | Q4 data bar | Q3 2022 | % Change |
|------|------------|---------|-------------|---------|-----------|
| 1 | .cn | 87,989 | | 93,086 | ▼ -5% |
| 2 | .ml | 65,866 | | 24,222 | ▲ 172% |
| 3 | .tk | 36,662 | | 29,596 | ▲ 24% |
| 4 | .ga | 19,979 | | 14,694 | ▲ 36% |
| 5 | .me | 19,742 | | 15,147 | ▲ 30% |
| 6 | .us | 18,771 | | 14,435 | ▲ 30% |
| 7 | .cf | 17,646 | | 12,458 | ▲ 42% |
| 8 | .gq | 16,693 | | 11,966 | ▲ 40% |
| 9 | .co | 16,674 | | 7,871 | ▲ 112% |
| 10 | .ru | 13,817 | | 6,492 | ▲ 113% |
| 11 | .uk | 9,204 | | 10,573 | ▼ -13% |
| 12 | .in | 6,896 | | 5,484 | ▲ 26% |
| 13 | .pl | 4,094 | | 2,833 | ▲ 45% |
| 14 | .cc | 3,863 | | 6,187 | ▼ -38% |
| 15 | .eu | 3,360 | | 2,389 | ▲ 41% |
| 16 | .de | 3,192 | | 4,091 | ▼ -22% |
| 17 | .fr | 2,896 | | 3,679 | ▼ -21% |
| 18 | .pw | 2,887 | | 2,852 | ▲ 1% |
| 19 | .su | 2,013 | | - | New entry |
| 20 | .br | 1,800 | | - | New entry |

01

●●● Top 20 gTLDs... x Top 20 gTLD... x

Top 20 gTLDs used in domain listings

| Rank | Domain TLD | Q4 2022 | Q4 data bar | Q3 2022 | % Change |
|------|------------|---------|-------------|---------|-----------|
| 1 | .com | 278,629 | | 278,077 | ▶ 0% |
| 2 | .top | 46,052 | | 33,655 | ▲ 37% |
| 3 | .net | 35,940 | | 44,474 | ▼ -19% |
| 4 | .info | 29,169 | | 46,245 | ▼ -37% |
| 5 | .live | 22,198 | | 38,987 | ▼ -43% |
| 6 | .xyz | 18,182 | | 19,887 | ▼ -9% |
| 7 | .link | 13,545 | | 2,738 | ▲ 395% |
| 8 | .org | 12,778 | | 14,670 | ▼ -13% |
| 9 | .shop | 10,966 | | 9,070 | ▲ 21% |
| 10 | .site | 9,603 | | 6,571 | ▲ 46% |
| 11 | .online | 9,142 | | 11,005 | ▼ -17% |
| 12 | .buzz | 6,285 | | 4,960 | ▲ 27% |
| 13 | .biz | 5,759 | | 8,609 | ▼ -33% |
| 14 | .click | 4,985 | | 5,609 | ▼ -11% |
| 15 | .club | 4,577 | | 3,913 | ▲ 17% |
| 16 | .cyou | 4,264 | | - | New entry |
| 17 | .work | 3,111 | | - | New entry |
| 18 | .life | 2,930 | | - | New entry |
| 19 | .store | 2,861 | | - | New entry |
| 20 | .icu | 2,856 | | 8,422 | ▼ -66% |

0 150 300

02

03

04

05

●●● Top 20 gTLDs... x Top 20 gTLD... x

Top 20 gTLD by % of zone file with domain listings

| Rank | Domain TLD | Q4 2022 | Zone size | % of zone listed | % of zone data bar |
|------|------------|---------|-----------|------------------|--------------------|
| 1 | .link | 13,545 | 201,260 | 6.73% | |
| 2 | .beauty | 2,137 | 33,556 | 6.37% | |
| 3 | .fit | 2,388 | 45,271 | 5.27% | |
| 4 | .live | 22,198 | 643,919 | 3.45% | |
| 5 | .rest | 1,413 | 46,178 | 3.06% | |
| 6 | .bid | 551 | 18,829 | 2.93% | |
| 7 | .bond | 1,034 | 37,474 | 2.76% | |
| 8 | .monster | 1,996 | 74,412 | 2.68% | |
| 9 | .support | 912 | 34,757 | 2.62% | |
| 10 | .best | 771 | 31,271 | 2.47% | |
| 11 | .fyi | 1,267 | 53,670 | 2.36% | |
| 12 | .cfd | 1,750 | 77,584 | 2.26% | |
| 13 | .autos | 369 | 18,850 | 1.96% | |
| 14 | .cam | 491 | 27,053 | 1.81% | |
| 15 | .football | 182 | 10,165 | 1.79% | |
| 16 | .click | 4,985 | 292,402 | 1.70% | |
| 17 | .sbs | 1,262 | 75,235 | 1.68% | |
| 18 | .quest | 1,064 | 67,079 | 1.59% | |
| 19 | .haus | 162 | 10,391 | 1.56% | |
| 20 | .pics | 413 | 27,905 | 1.48% | |

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

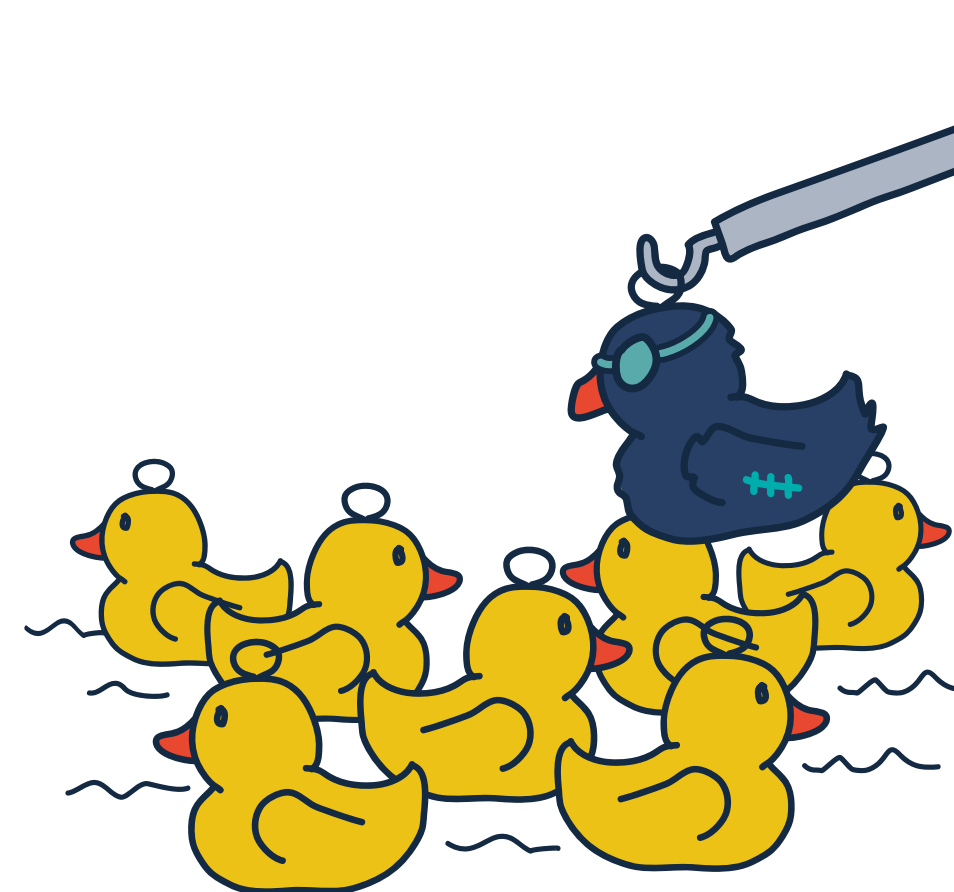
Trending phishing terms in domain listings

With fraudulent phishing domains, 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. These names can usually be split into three types, each of which are aimed at luring the victim in:

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

The Top 20 terms in phishing domains change position constantly, but are usually the same. Despite being as generic as most of the other terms, we attribute the increase in “sign-in” almost entirely to phishing campaigns connected with the .ml TLD, which we discuss in greater detail later in this report.

As the terms detailed in our Top 20 are relatively constant and predictable, it should be possible for registrars and registries to be more proactive in pinpointing these domains and applying extra verification measures. This would significantly limit fraudulent registrations and malicious use.



i What terms do bad actors use for domain names? ✕

Some miscreants don't care what a domain name looks like; however, others do. When it comes to the latter, they favor one of two options:

1. Try to look like a legitimate brand with the inclusion of a well-known brand name, e.g., “amazon”.
2. Use words in the domain name that read like a call to action, e.g. “update now” and “verify your account”.

01

Top 20 phishing terms in domain listings

| Rank | Term | Q4 2022 | Q4 data bar | Q3 2022 | % Change |
|------|--------------|---------|-------------|---------|-----------|
| 1 | account | 11,155 | | 6,183 | ▲ 80% |
| 2 | support | 6,568 | | 6,370 | ▲ 3% |
| 3 | online | 5,565 | | 6,614 | ▼ -16% |
| 4 | secure | 4,975 | | 6,802 | ▼ -27% |
| 5 | verification | 4,951 | | 3,950 | ▲ 25% |
| 6 | service | 4,636 | | 5,488 | ▼ -16% |
| 7 | security | 4,077 | | 3,956 | ▲ 3% |
| 8 | sign-in | 3,478 | | - | New entry |
| 9 | icloud | 3,408 | | 3,184 | ▲ 7% |
| 10 | apple | 3,368 | | 3,131 | ▲ 8% |
| 11 | intl | 3,136 | | 2,824 | ▲ 11% |
| 12 | amazon | 3,062 | | 3,240 | ▼ -5% |
| 13 | update | 2,900 | | 2,369 | ▲ 22% |
| 14 | cloud | 2,816 | | 2,493 | ▲ 13% |
| 15 | verify | 2,533 | | 3,275 | ▼ -23% |
| 16 | login | 2,453 | | - | New entry |
| 17 | client | 2,154 | | - | New entry |
| 18 | center | 2,145 | | - | New entry |
| 19 | payment | 2,036 | | 2,024 | ▲ 1% |
| 20 | jobs | 1,948 | | 1,883 | ▲ 3% |

02

03

04

05

Phishing terms



01

02

03

04

05

Types of listings

In Q4, there was a noticeable increase in the number of domains contained in the URLs hosting QakBot. This, in part, caused the steep increase in both compromised malware (+616%) and botnet command and controller (C&C) (+828%) listings. Anyone who reads our [Malware](#) or [Botnet updates](#) will know of the significant increases in Qakbot activity over the past quarter.

In Q4, we attributed around 36% of all reported compromised malware URLs to Qakbot. This malware is generally used by [Initial Access Brokers \(IABs\)](#), who compromise large corporate networks, and often sell access to cybercriminals who launch ransomware attacks. Operators of Qakbot prefer to host their malware operations on compromised devices, which explains the significant increase in Q4's compromised figures.

There was also a 14% rise in malicious phishing domains. When reduced to its most basic concept, a domain name is like an entry in a global internet phonebook, under which the owner can publish additional names that point to IP addresses (in the case of DNS, A records).

As with the somewhat redundant phone directory, a large part of a domain's functionality ensures that humans can find or utilize services offered on an IP address. With this in mind, the existence of domain names that consist of long strings of numbers, such as "5656320259656314.ml" is somewhat puzzling. After all, what user types in 16 digits into their browser address bar to navigate to a website?

Once we analyzed the host names observed, the picture became clearer – they're all part of phishing campaigns. To the general masses, the difference between a fraudulent and legitimate host name is hard to recognize, particularly when it boils down to the location of a dot and/or a forward slash. We've seen tens of thousands of these kinds of domains listed in Q4 across multiple TLDs. Still, the largest proportion was associated with .ml.

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

Bad reputation

Malicious

436,320

▶ 0% ◀

Compromised

5,949

-43% ▼

A domain's reputation score has exceeded policy limits.

Botnet C&C

Malicious

3,724

▲ 3% ▲

Compromised

269

▲ 828% ▲

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

Malware

Malicious

7,205

▲ 39% ▲

Compromised

25,519

▲ 616% ▲

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

Phishing

Malicious

359,916

▲ 14% ▲

Compromised

5,949

▼ -29% ▼

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

01

02

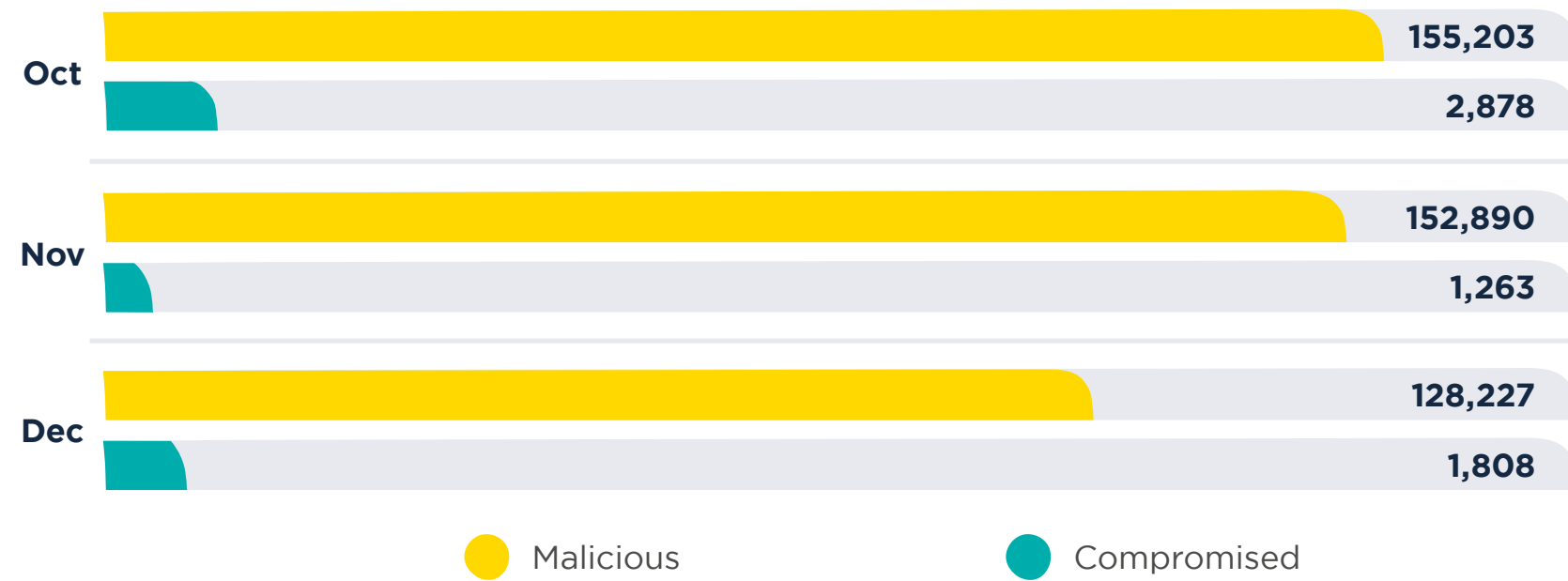
03

04

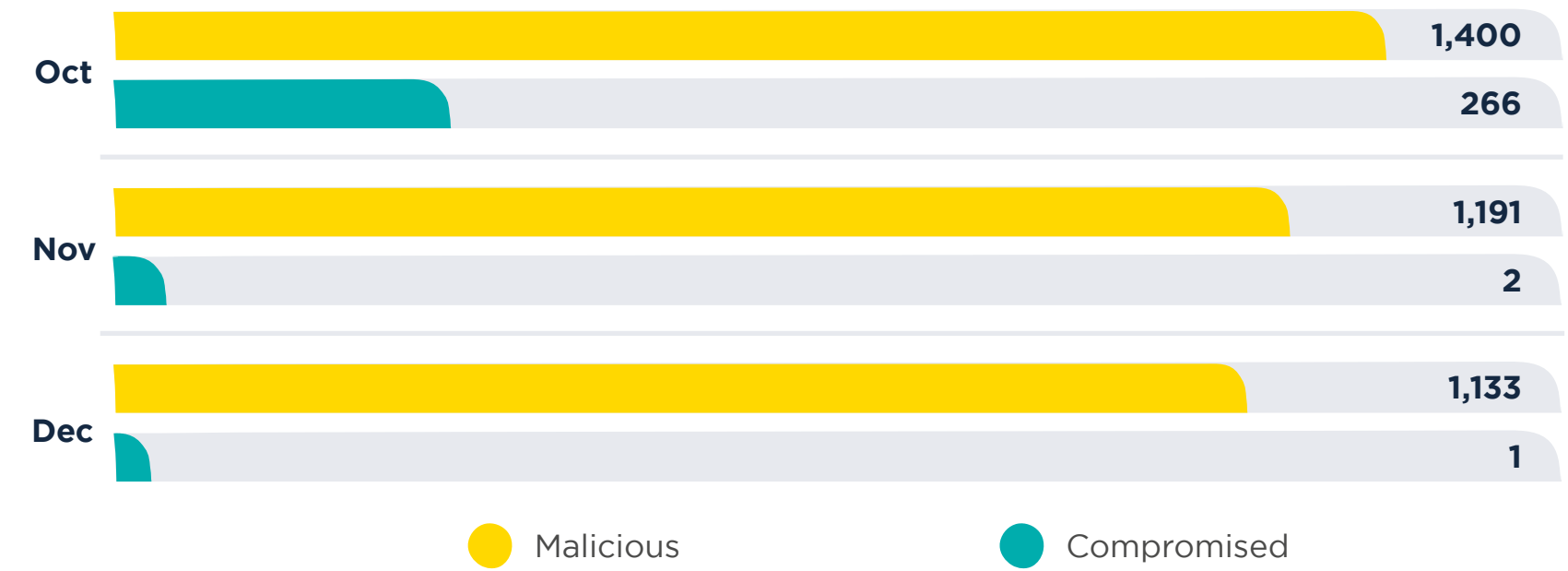
05

Types of abuse

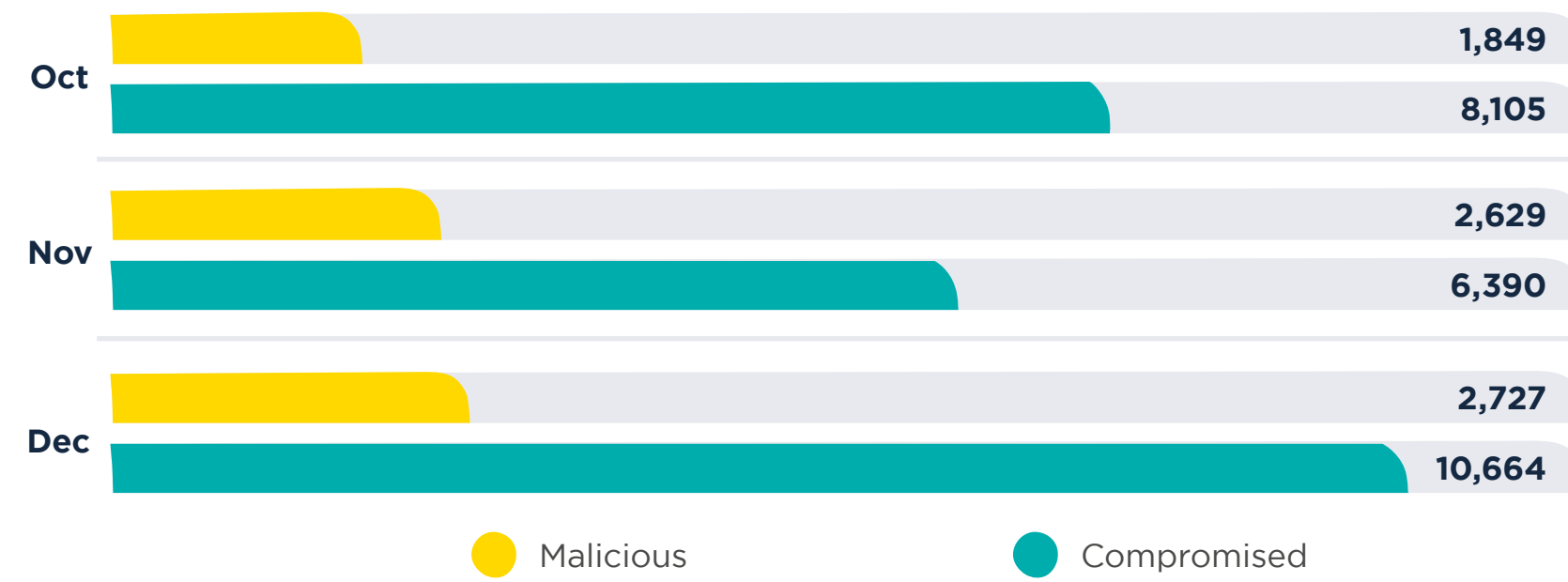
Bad reputation per month



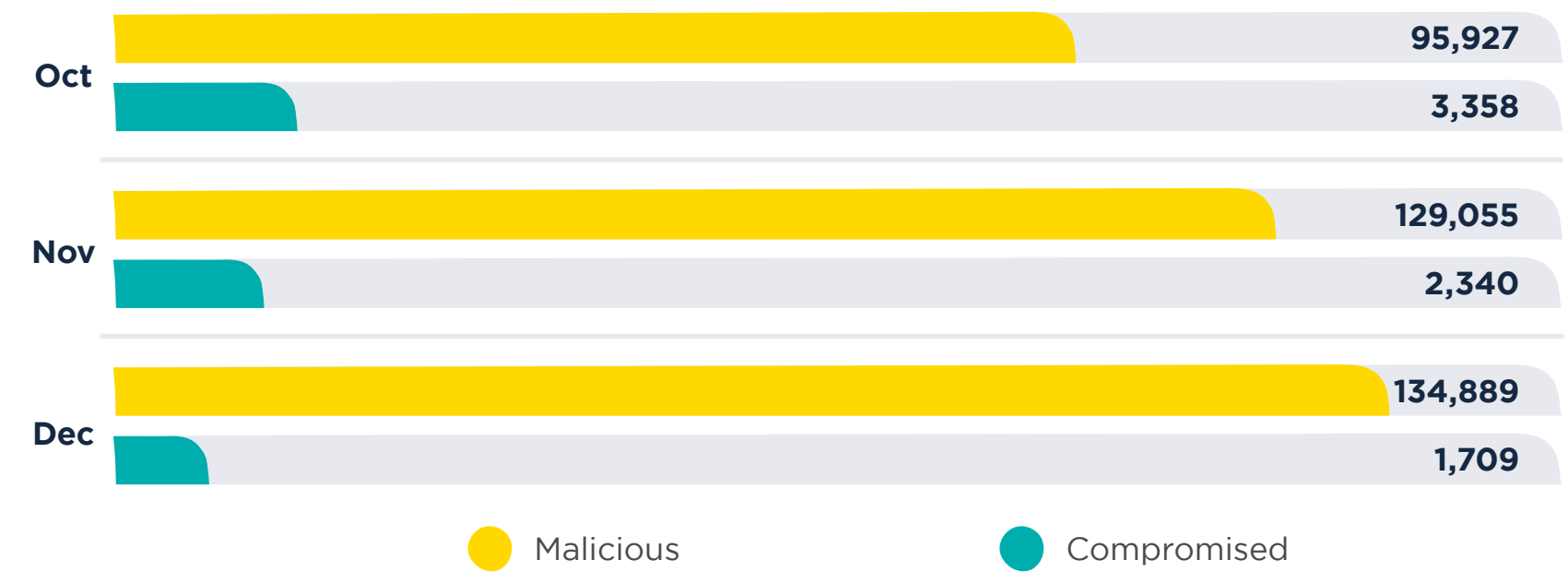
Botnet C&C per month



Malware per month



Phishing per month



01

02

03

04

05

Recommendations of the quarter

As this report is read by many different people in many different roles, providing recommendations that will benefit everyone is almost impossible. So this quarter, we're taking a slightly different approach, and addressing our recommendations to those registering and hosting domain names. We realize this might be considered wishful thinking, but the bar needs to be raised.



If a layman saw what we and others see, they would quite rightly ask why this type of abuse is allowed to continue. How can miscreants create thousands upon thousands of unpronounceable, nonsense names to facilitate serious cybercrime such as phishing? Why do hosting and content delivery network (CDN) providers permit their systems to keep this abuse online?

A big part of the answer to those questions is automation. As you would expect, most new domains or accounts get approved automatically. But we hope that providers can apply this “automation focus” to finding and dealing with the kind of criminal activity detailed above.

Part of the bigger picture is that many companies continue to see abuse as a cost center, where spending less money is the prevailing aim. It will be no surprise that we at Spamhaus vehemently disagree with this. And as much as we think the industry could do a much better job of dealing with abuse without regulation, it is fast becoming clear that the threat of enforcement may be required to move the needle in the right direction.

01

02

03

04

05

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.

01

02

03

04

05