

Spamhaus Botnet Threat Update



Q4 2022

Botnet C&C operators gathered momentum in Q4. Spamhaus researchers saw a 56% increase in newly observed botnet C&C servers, the largest increase since Q3 2021. Malware families such as Qakbot grew significantly in popularity, and botnet C&C threats associated with the misuse of the penetration testing framework Cobalt Strike, continued to increase. But it wasn't all bad news - almost all of the listed network operators have taken action to tackle active botnet C&Cs, with numbers reducing almost across the board.

Welcome to the Spamhaus Botnet Threat Update Q4 2022.

About this report

Spamhaus tracks both Internet Protocol (IP) addresses and domain names used by threat actors for hosting botnet command & control (C&C) servers. This data enables us to identify associated elements, including the geolocation of the botnet C&Cs, the malware associated with them, the top-level domains used when registering a domain for a botnet C&C, the sponsoring registrars and the network hosting the botnet C&C infrastructure.

This report provides an overview of the number of botnet C&Cs associated with these elements, along with a quarterly comparison. We discuss the trends we are observing and highlight service providers struggling to control the number of botnet operators abusing their services.



Spotlight

Protecting against threats like Emotet and Qakbot

How prevalent are these threats?

It's no secret that Emotet and Qakbot are two of the biggest malware threats for corporate networks. In Q4, botnet C&Cs associated with Qakbot increased by 379%. Meanwhile, [abuse.ch reported](#) that "QakBot beat Emotet in number of malware sites by over 10 times" in 2022. In fact, every fourth malware site shared by security researchers on abuse.ch's [URLHaus](#) was related to Qakbot. This is not a threat to ignore.

How do these threats operate?

Both Qakbot and Emotet operate as [Initial Access Brokers](#), (IABs). These are threat actors that operate in groups to breach corporate networks, and will often subsequently infect them with ransomware. But they have another thing in common – operators of both malware threats choose to host their botnet C&C infrastructure on compromised devices.



What is Border Gate-way Protocol (BGP) Firewall?

You can apply threat intelligence to any router or modern-day firewall. This threat intelligence consists of lists (communities) of IP addresses that effectively drop malicious traffic from compromised devices within your network perimeter that are communicating with external botnet C&C servers.

Blocking this traffic at the network level prevents spam campaigns, loss of data, and encryption.

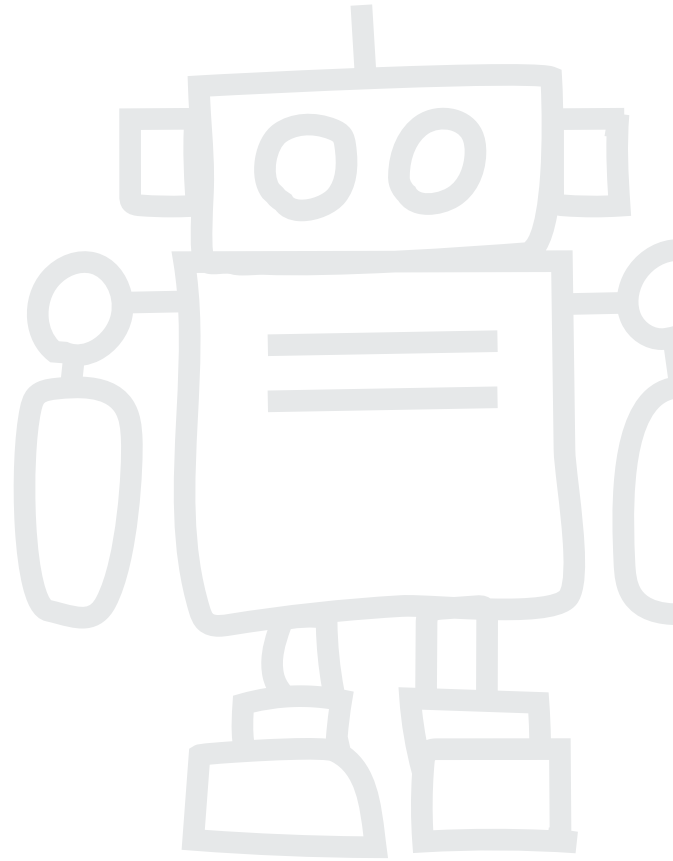
Users can peer with BGP feeds, using existing equipment. If you don't own an ASN, Spamhaus supports the use of private ASNs to establish sessions with the BGP feeds.

Protecting against these threats

To provide better defense against the likes of Qakbot and Emotet, we have enhanced our Border Gateway Protocol (BGP) Firewall offering. At the end of 2022, our team introduced a [BGP community](#) focused on the major malware threats utilizing compromised devices for hosting botnet C&Cs, such as Qakbot and Emotet.

This 'Botnet Controller List (BCL) - Compromised' community is the fourth Spamhaus has provided to BGP subscribers to use with firewalls or routing equipment to block malicious traffic. This includes the worst of the worst; networks entirely controlled by criminal organizations, which send zero legitimate traffic.

To understand how BGP Firewall works, read this [Beginner's Guide](#). It's easy to configure and very cost effective.



Number of botnet C&Cs observed, Q4 2022

In Q4 2022, Spamhaus identified 6,775 botnet C&Cs compared to 4,331 in Q3 2022. This was a +56% increase quarter on quarter. The monthly average increased from 1,444 in Q3 to 2,258 botnet C&Cs per month in Q4.

| Quarter | No. of Botnets | Quarterly Average | % Change |
|---------|----------------|-------------------|----------|
| Q1 2022 | 3,538 | 1,179 | +8% |
| Q2 2022 | 3,141 | 1,047 | -11% |
| Q3 2022 | 4,331 | 1,444 | +38% |
| Q4-2022 | 6,775 | 2,258 | +56% |



What are botnet command & controllers?

A 'botnet controller,' 'botnet C2' or 'botnet command & control' server is commonly abbreviated to 'botnet C&C.' Fraudsters use these to both control malware-infected machines and extract personal and valuable data from malware-infected victims.

Botnet C&Cs play a vital role in operations conducted by cybercriminals who are using infected machines to send out spam or ransomware, launch DDoS attacks, commit e-banking fraud or click-fraud, or mine cryptocurrencies such as Bitcoin.

Desktop computers and mobile devices, like smartphones, aren't the only machines that can become infected. There is an increasing number of devices connected to the internet, for example, the Internet of Things (IoT), devices like webcams, network attached storage (NAS), and many more items. These are also at risk of becoming infected.

Geolocation of botnet C&Cs, Q4 2022

Botnet C&C boom in the West

Last quarter, we observed a significant uptick in botnet C&C activity across central Europe and North America. This didn't abate in Q4, with substantial increases in Canada (+185%), the United Kingdom (+146%), France (+89%), and the United States (+86%). Additionally, all of the Top 20 newcomers were in Europe, including Bulgaria (#12), Poland (#15) and Spain (#19). Venezuela (#19) was the only exception.

China's botnet C&C woes continue

While China only experienced a +4% increase in botnet C&C activity in Q4, it was still hosting more botnet C&C servers than any other country except for the United States.

Further improvements across the LatAm region

We are pleased to report that Brazil and the Dominican Republic have dropped off the Top 20. This is great progress for the region, given that four LatAm countries were in the Top 10 a year ago.

In Q4 2022, only Mexico remains. Hopefully Venezuela, which has recently entered the Top 20, will depart as swiftly as it has appeared.



New entries

Bulgaria (#12), Poland (#15), Spain (#19), Venezuela (#19).



Departures











Brazil, Czechia, Dominican Republic, Lithuania.

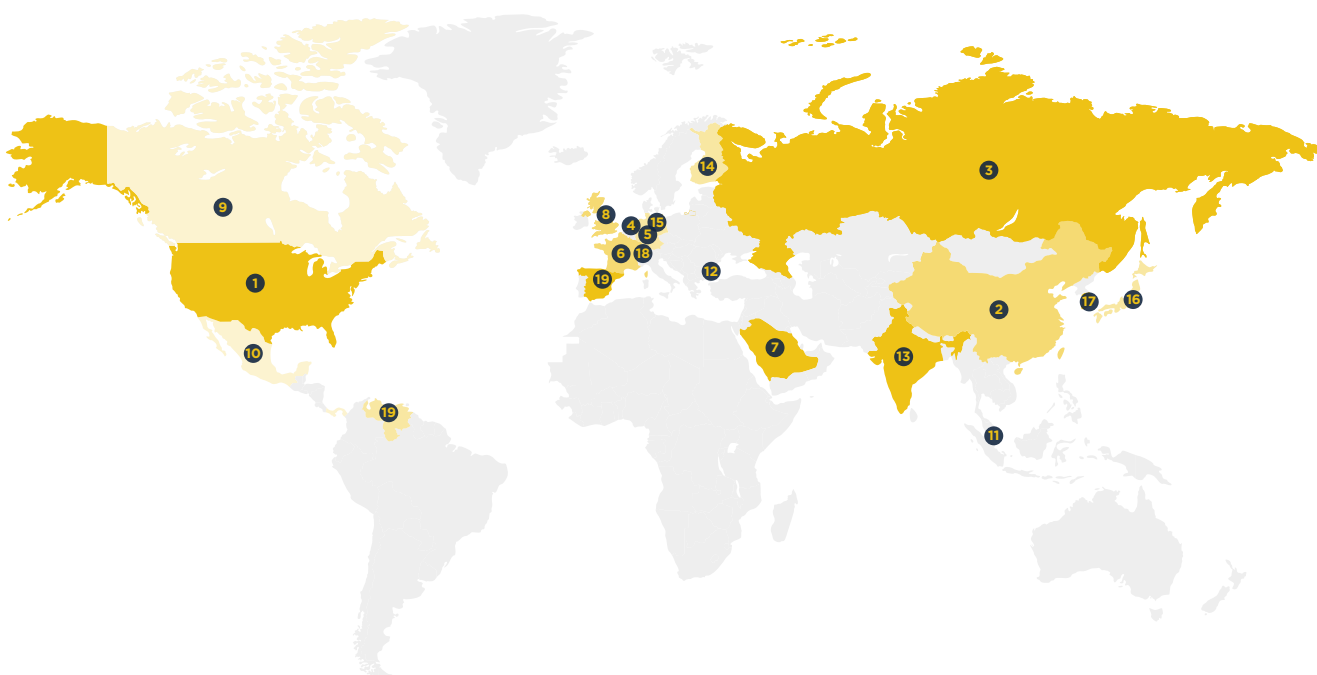
Geolocation of botnet C&Cs, Q4 2022

(continued)

Top 20 locations of botnet C&Cs

| Rank | Country | Q3 2022 | Q4 2022 | % Change Q on Q |
|------|--|---------|---------|-----------------|
| #1 | United States  | 922 | 1713 | 86% |
| #2 | China  | 996 | 1033 | 4% |
| #3 | Russia  | 363 | 500 | 38% |
| #4 | Netherlands  | 293 | 467 | 59% |
| #5 | Germany  | 249 | 391 | 57% |
| #6 | France  | 120 | 227 | 89% |
| #7 | Saudi Arabia  | 110 | 182 | 65% |
| #8 | United Kingdom  | 67 | 165 | 146% |
| #9 | Canada  | 52 | 148 | 185% |
| #10 | Mexico  | 104 | 140 | 35% |

| Rank | Country | Q3 2022 | Q4 2022 | % Change Q on Q |
|------|---|---------|---------|-----------------|
| #11 | Singapore  | 96 | 125 | 30% |
| #12 | Bulgaria  | - | 77 | New entry |
| #13 | India  | 42 | 75 | 79% |
| #14 | Finland  | 47 | 72 | 53% |
| #15 | Poland  | - | 71 | New entry |
| #16 | Japan  | 50 | 67 | 34% |
| #17 | South Korea  | 48 | 65 | 35% |
| #18 | Switzerland  | 43 | 61 | 42% |
| #19 | Venezuela  | - | 60 | New entry |
| #19 | Spain  | - | 60 | New entry |



Malware associated with botnet C&Cs, Q4 2022

Qakbot is gathering momentum

We have seen an increase of +379% in botnet C&Cs associated with Qakbot in the last quarter.

Less RecordBreaker activity

In Q4, we observed far fewer botnet C&C servers associated with RecordBreaker, a malware toolkit sold on the dark web as Malware-as-a-Service (MaaS). RecordBreaker is the successor of RaccoonStealer, which received a major code boost in 2022.

Backdoors increasing in popularity

The most noteworthy commentary when evaluating the types of malware associated with botnet C&Cs this quarter has to be the growing preference for bad actors to use backdoor programs. In Q3, these only accounted for 13% of malware family types; in Q4, this rose to 23%. Backdoors allow cybercriminals to access computers remotely, bypassing authentication and encryption measures.

FluBot labeling

Our researchers continued to associate a high number of newly observed botnet C&Cs with FluBot in Q4. As mentioned in previous updates, FluBot is using a “FastFlux” technique to host its botnet C&Cs, which is also used by other malware families, such as TeamBot. To make our internal tracking of this threat easier, we continue to label the associated infrastructure as “FluBot.”



What is Qakbot?

Qakbot is an [Initial Access Broker \(IAB\)](#) that operates in groups to compromise large corporate networks, often leading to ransomware attacks.



New entries

RedcordStealer (#7), Amadey (#18).

Departures

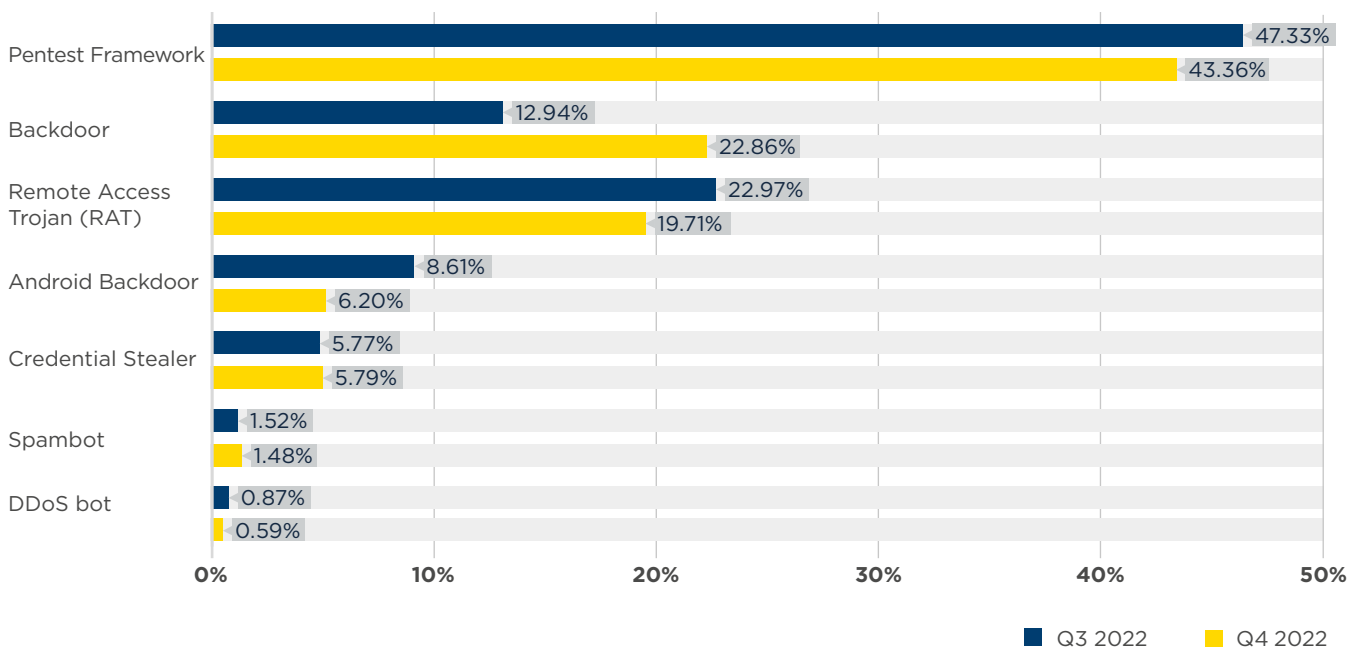
Netwire, Socelars

Malware associated with botnet C&Cs, Q4 2022 (continued)

Malware families associated with botnet C&Cs

| Rank | Q3 2022 | Q4 2022 | % Change | Malware Family | Description |
|------|---------|---------|-----------|----------------|----------------------------|
| #1 | 1902 | 2657 | 40% | Cobalt Strike | Pentest Framework |
| #2 | 213 | 1020 | 379% | Qakbot | Backdoor |
| #3 | 392 | 497 | 27% | RedLineStealer | Remote Access Trojan (RAT) |
| #4 | 346 | 380 | 10% | Flubot | Android Backdoor |
| #5 | 152 | 245 | 61% | Bumblebee | Backdoor |
| #6 | 97 | 177 | 82% | NjRAT | Remote Access Trojan (RAT) |
| #7 | - | 123 | New entry | RecordStealer | Credential Stealer |
| #8 | 87 | 121 | 39% | DCRat | Remote Access Trojan (RAT) |
| #9 | 67 | 120 | 79% | AveMaria | Remote Access Trojan (RAT) |
| #10 | 112 | 100 | -11% | Emotet | Backdoor |
| #11 | 58 | 96 | 66% | Arkei | Credential Stealer |
| #12 | 61 | 91 | 49% | Tofsee | Spambot |
| #13 | 89 | 90 | 1% | AsyncRAT | Remote Access Trojan (RAT) |
| #14 | 87 | 89 | 2% | Remcos | Remote Access Trojan (RAT) |
| #14 | 154 | 89 | -42% | RecordBreaker | Credential Stealer |
| #16 | 51 | 66 | 29% | NanoCore | Remote Access Trojan (RAT) |
| #17 | 25 | 48 | 92% | VjwOrm | Remote Access Trojan (RAT) |
| #18 | - | 47 | New entry | Amadey | Credential Stealer |
| #19 | 35 | 36 | 3% | Loki | DDoS bot |
| #19 | 43 | 36 | -16% | Dridex | Backdoor |

Malware type comparisons between Q3 2022 and Q4 2022



Most abused top-level domains, Q4 2022

Russia's ccTLD returns to the limelight

The country code top-level domain (ccTLD) of Russia (.ru) has been performing reasonably well over the past year in terms of fewer fraudulent domain registrations. Sadly, we have seen a substantial increase of +158% in Q4.

An improving picture for Freenom's TLDs

Having reported on the dominance of Freenom's TLDs in our Q3 Top 20, it's good to see that both .ga & .ml have experienced significant reductions in botnet C&C associations. Let's hope this trend continues into 2023.

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q4 2022, .org had more than 10.6 million domains, of which 0.001% were associated with botnet C&Cs. Meanwhile .tk had approximately 94,000 domains, of which 0.1772% were associated with botnet C&Cs. Both are in the Top 10 of our listings but one had a much higher percentage of domains related to botnet C&Cs than the other.



Top-level domains (TLDs) a brief overview

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

Generic TLDs (gTLDs) - these are under ICANN jurisdiction. Some TLDs 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.

Most abused top-level domains, Q4 2022 (continued)

Working together for a safer internet

Naturally, our preference is for no TLDs to have botnet C&Cs linked with them. But we live in the real world and understand there will always be abuse.

What is crucial is that abuse is dealt with quickly. If domain names are registered solely for distributing malware or hosting botnet C&Cs, we would like registries to suspend these domain names. We greatly appreciate the efforts of many registries who already work with us to ensure action is taken swiftly.



New entries

de (#18), me (#19), cfd (#20)

Departures

co, cyou, fun

Top abused TLDs - number of domains

| Rank | Q3 2022 | Q4 2022 | % Change | TLD | Note |
|------|---------|---------|-----------|--------|--|
| #1 | 1674 | 2184 | 30% | com | gTLD |
| #2 | 134 | 220 | 64% | xyz | gTLD |
| #3 | 244 | 190 | -22% | top | gTLD |
| #4 | 139 | 167 | 20% | tk | Originally ccTLD, now effectively gTLD |
| #5 | 181 | 160 | -12% | cloud | gTLD |
| #6 | 59 | 152 | 158% | ru | ccTLD |
| #7 | 442 | 134 | -70% | ml | Originally ccTLD, now effectively gTLD |
| #8 | 117 | 114 | -3% | org | gTLD |
| #9 | 52 | 84 | 62% | shop | gTLD |
| #10 | 71 | 68 | -4% | net | gTLD |
| #11 | 213 | 64 | -70% | ga | Originally ccTLD, now effectively gTLD |
| #11 | 47 | 63 | 34% | br | ccTLD |
| #13 | 85 | 56 | -34% | cf | Originally ccTLD, now effectively gTLD |
| #14 | 84 | 52 | -38% | us | ccTLD |
| #15 | 56 | 50 | -11% | gq | Originally ccTLD, now effectively gTLD |
| #16 | 73 | 46 | -37% | online | gTLD |
| #17 | 101 | 37 | -63% | info | gTLD |
| #18 | - | 35 | New Entry | de | ccTLD |
| #19 | - | 29 | New Entry | me | ccTLD |
| #20 | - | 23 | New Entry | cfd | gTLD |

Most abused domain registrars, Q4 2022

Tucows takes top spot

NameSilo, the Canadian-based domain registrar, and Namecheap, the US-based domain registrar, have topped this chart for several years. Nevertheless, in Q4, both experienced reductions in fraudulent domain registrations: -56% and -14%, respectively.

Conversely, we saw a massive +260% increase in botnet C&C domain registrations at the Canadian-based Tucows. We hope this domain registrar can improve its ability to prevent fraudulent domain registrations quickly.



New entries





















InterNetworX (#8), west263.com (#16), Gransy (#17).

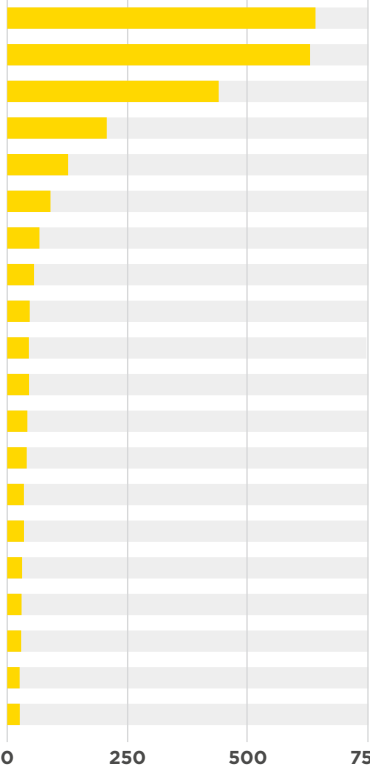
Departures

EuroDNS, NameBright, OwnRegistrar.

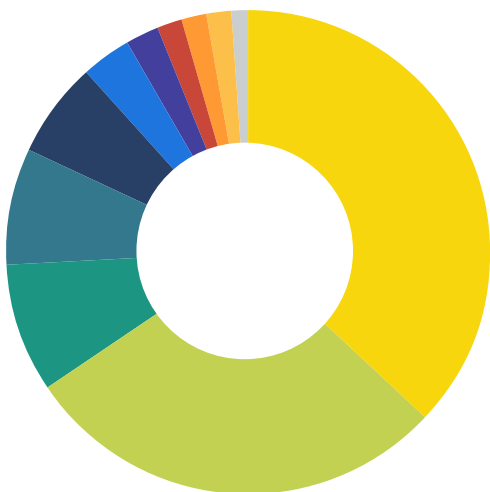
Most abused domain registrars, Q4 2022 (continued)












Most abused domain registrars - number of domains

| Rank | Q3 2022 | Q4 2022 | % Change | Registrar | Country | |
|------|---------|---------|-----------|--------------|----------------|---|
| #1 | 166 | 597 | 260% | Tucows | Canada |  |
| #2 | 644 | 554 | -14% | Namecheap | United States |  |
| #3 | 937 | 414 | -56% | NameSilo | Canada |  |
| #4 | 90 | 190 | 111% | RegRU | Russia |  |
| #5 | 173 | 168 | -3% | PDR | India |  |
| #6 | 105 | 103 | -2% | Sav | United States |  |
| #7 | 62 | 100 | 61% | Alibaba | China |  |
| #8 | - | 95 | New entry | InterNetworX | Germany |  |
| #8 | 103 | 75 | -27% | Nicenic | China |  |
| #10 | 62 | 57 | -8% | GMO | Japan |  |
| #11 | 61 | 56 | -8% | Porkbun | United States |  |
| #12 | 47 | 49 | 4% | Openprovider | Netherlands |  |
| #13 | 51 | 48 | -6% | Google | United States |  |
| #14 | 58 | 46 | -21% | Hostinger | Lithuania |  |
| #15 | 55 | 42 | -24% | Gandi | France |  |
| #16 | - | 31 | New entry | west263.com | China |  |
| #17 | - | 28 | New entry | Gransy | Czech Republic |  |
| #17 | 30 | 28 | -7% | Todaynic | China |  |
| #19 | 25 | 23 | -8% | RU-Center | Russia |  |
| #19 | 33 | 23 | -30% | Name.com | United States |  |



LOCATION OF MOST ABUSED DOMAIN REGISTRARS



| Country | Q3 2022 | Q4 2022 |
|--|---------|---------|
|  Canada | 39.46% | 37.07% |
|  United States | 34.17% | 28.75% |
|  China | 6.98% | 8.58% |
|  Russia | 4.11% | 7.81% |
|  India | 6.19% | 6.16% |
|  Germany | n/a | 3.48% |
|  Japan | 2.22% | 2.09% |
|  Netherlands | 1.68% | 1.80% |
|  Lithuania | 2.08% | 1.69% |
|  France | 1.97% | 1.54% |
|  Czech Republic | n/a | 1.03% |

Networks hosting the most newly observed botnet C&Cs, Q4 2022

More new botnet C&Cs in the West

In the past quarter, we saw an upswing in the number of new botnet C&Cs being set up at cloud providers and those hosted in the West. This quarter, Microsoft experienced the biggest rise in new botnet C&Cs with an increase of +91%, followed by Digitalocean (+66%) and the German hosting company Hetzner (+52%).

Does this list reflect how quickly networks deal with abuse?

While this Top 20 illustrates that there may be an issue with customer vetting processes at some networks, it doesn't reflect the speed at which abuse desks deal with reported problems.

In the next section of this report, we drill further into the networks where abuse isn't dealt with promptly.



Networks and botnet C&C operators

Networks have a reasonable amount of control over operators who fraudulently sign-up for a new service.

A robust customer verification/vetting process should occur before commissioning a service.

Where networks have a high number of listings, it highlights one of the following issues:

1. Networks are not following best practices for customer verification processes.
2. Networks are not ensuring that ALL their resellers follow sound customer verification practices.

In some of the worst-case scenarios, employees or owners of networks are directly benefiting from fraudulent sign-ups, i.e., knowingly taking money from miscreants in return for hosting their botnet C&Cs; however, thankfully, this doesn't often happen.



New entries

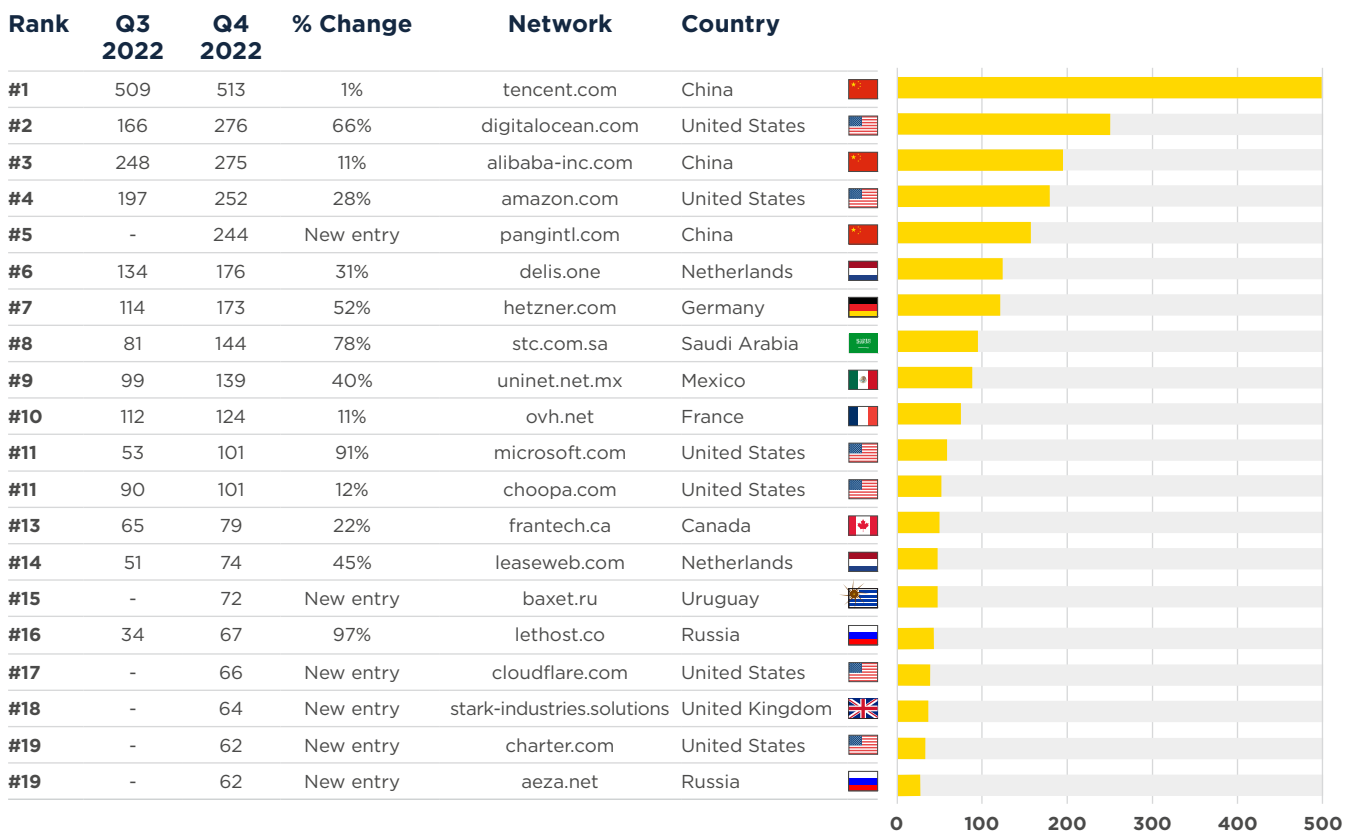
pangintl.com (#5), baxet.ru (#15), cloudflare.com (#17), stark-industries.solutions (#18), aeza.net (#19), charter.com (#19)

Departures

baidu.com, claro.com.do, colocrossing.com, huawei.com, m247.ro, vdsina.ru.

Networks hosting the most newly observed botnet C&Cs, Q4 2022

(continued)



Networks hosting the most active botnet C&Cs, Q4 2022

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs at the end of Q4 2022. Hosting providers included here either have an abuse problem, do not take the appropriate action when receiving abuse reports, or fail to notify us when they have dealt with an issue.

Hosting providers cleaning up

The end of 2022 brought some good news. We saw the majority of hosting and cloud providers taking ownership of persistent abuse problems across their networks and carrying out positive actions to address these issues.

Almost all of the listed networks that appeared to be struggling with botnet C&C abuse problems experienced a decrease in the number of active botnet C&C servers in Q4. We're delighted to report that this occurred across all regions, from China (Tencent, Alibaba) to the US (Amazon, DigitalOcean). Thank you!

What's the story, DigitalOcean?

The keen-eyed among you will have noticed that in Q4, the US-based cloud provider DigitalOcean had one of the largest increases (+66%) in newly observed botnet C&C servers on its network.

Meanwhile, for the same quarter, the number of active botnet C&C servers hosted at DigitalOcean dropped by 61%. You may ask yourself "Why the big differences?" We certainly did. Our analysis suggests that while DigitalOcean's abuse team is addressing abuse issues quickly once they arise, new customer vetting may be lacking. This would allow bad actors to initially register and host botnet C&Cs on their infrastructure before they can be shut down.



New entries

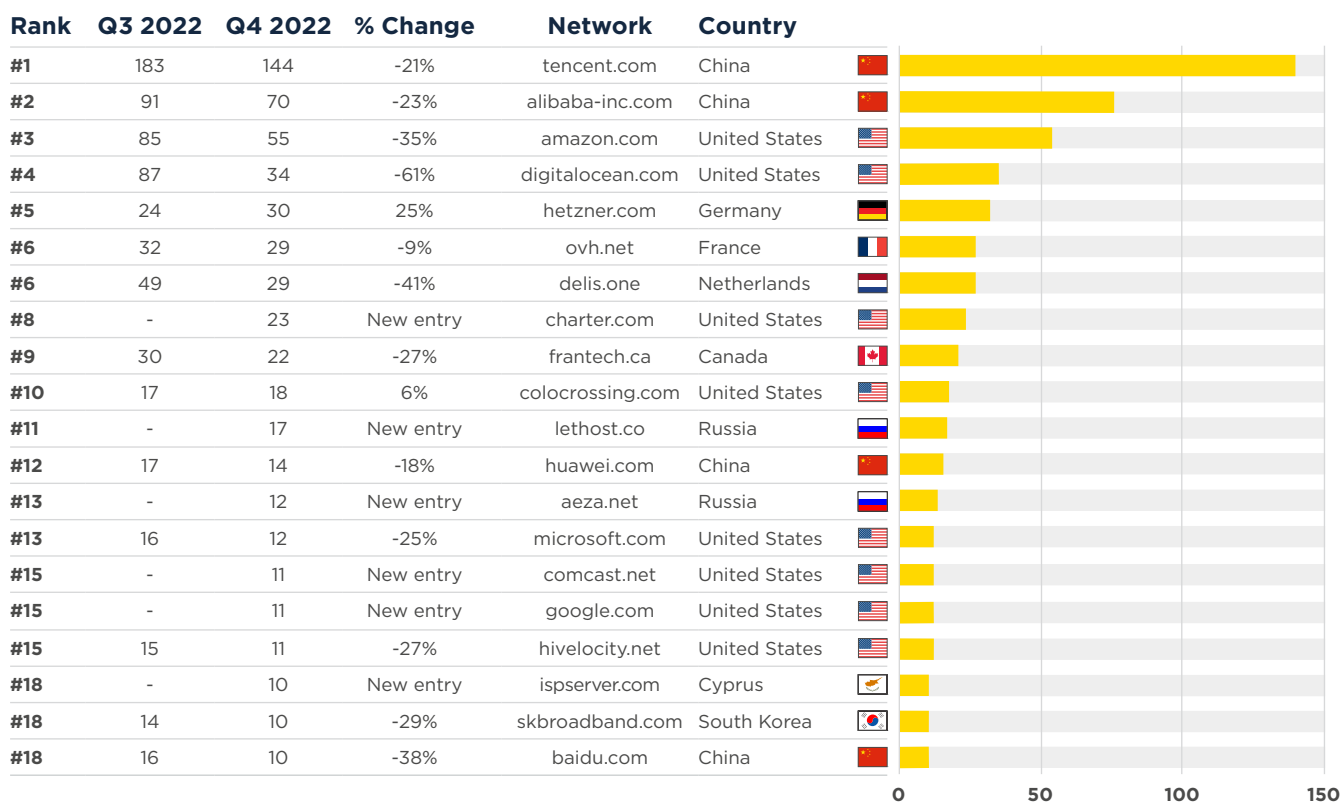
charter.com (#8), lethost.co (#11), aeza.net (#13), google.com (#15), comcast.net (#15), ispserver.com (#18).

Departures

1ue.com, choopa.com, cloudflare.com, combahton.net, contabo.de, leaseweb.com

Networks hosting the most active botnet C&Cs, Q4 2022 (continued)

Total number of active botnet C&Cs per network



That's all for now. Stay safe, and see you in April 2023!