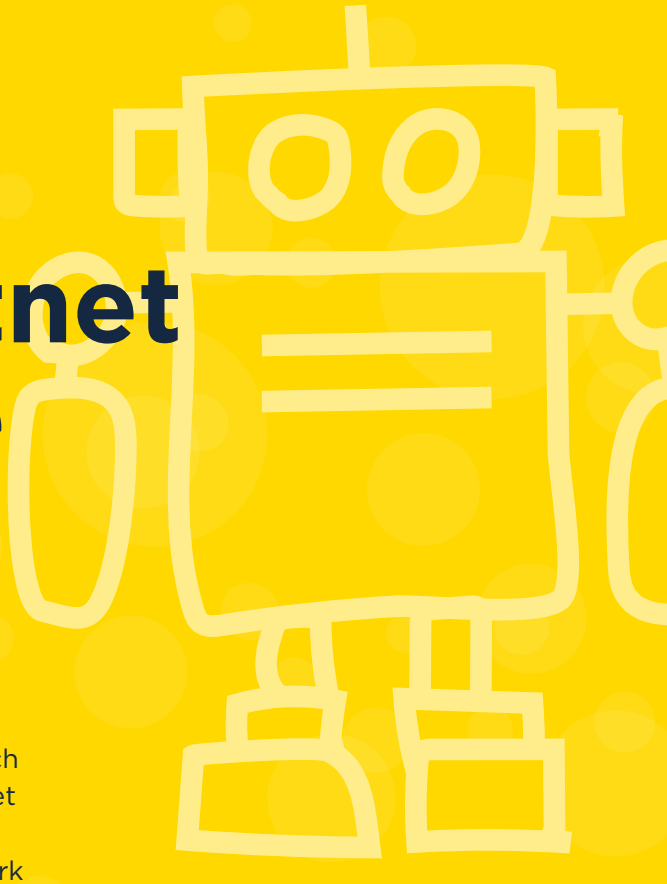
SPAMHAUS



# Spamhaus Botnet Threat Update

## Q2 2022

Botnet command and controller (C&C) activity reduced slightly in Q2 with an 11% decrease, which is always good news. Operators within the LatAm region appeared to be getting control of newly observed botnet C&C abuse, which is reassuring, although the region's number of active botnet C&Cs continued to grow. Perhaps the most concerning development in Q2 was that two well-known global network operators struggled to get to grips with continuing abuse. We urge operators to reach out to our experts for assistance.

**Welcome to the Spamhaus Botnet Threat Update Q2 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, and 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

# The Spamhaus Reputation Portal

## A free tool to help networks proactively manage IP reputation

Spamhaus released a new free tool for network owners this month: The Spamhaus Reputation Portal[1]. This service enables anyone who owns at least one Autonomous System Number (ASN) to quickly assess reputation across their IPs and rapidly resolve listing issues via an easy-to-use Ticket Center.

## What IP reputation data does the portal include?

Once you've successfully registered for an account, you will have complete visibility of any IP that Spamhaus is listing that relate to your network. This includes Botnet C&Cs that we list on the Botnet Controller List (BCL) and eXploits Blocklist (XBL), which also lists IPs showing signs of infections and third-party exploits like proxies. Additionally, listings on the Spamhaus Blocklist (SBL) and CSS Blocklist (CSS) are also highlighted; the only IP blocklist that isn't represented is the Policy Blocklist (PBL).

Users can manage all removal requests from within the Portal. Where the delisting team doesn't permit automatic removals, the Ticket Center makes it easy to track the status of requests and view communication history with the team. The one exception is any listing on the SBL, which continue to be dealt directly with the SBL team via email.

(1) www.spamhaus.com/campaign/reputation-portal/

## Get notified of listings as they occur

To help you proactively manage listings on your network, you can sign up for an email which details new listings and is sent every 24 hours. Alternatively, you can use the API to integrate this data into your existing systems, which is updated hourly.

Watch this video[1] to learn more about the tool, or you can register for an account[2] immediately.



(1) www.youtube.com/watch?v=KUuWP0jDUqs&t=14s
(2) https://manage.spamhaus.com/register/

# Number of botnet C&Cs observed, Q2 2022

In Q2 2022, Spamhaus identified 3,141 botnet C&Cs compared to 3,538 in Q1 2022. This was an 11% decrease quarter on quarter. The monthly average decreased from 1,179 in Q1 to 1,047 botnet C&Cs per month in Q2.

| Quarter | No. of Botnets | Quarterly Average | % Change |
|---|---|---|---|
| Q3, 2021 | 2,656 | 885 | +82% |
| Q4, 2021 | 3,271 | 1,090 | +23% |
| Q1, 2022 | 3,538 | 1,179 | +8% |
| Q2, 2022 | 3,141 | 1,047 | -11% |

### 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, Q2 2022

## Another quarter, another increase for Russia

Once again, for the fifth quarter running, we have seen an increase in new botnet C&Cs hosted in Russia.

- 2021 Q1 to Q2 – 19% increase
- 2021 Q2 to Q3 – 64% increase
- 2021 Q3 to Q4 – 124% increase
- 2021 Q4 to 2022 Q1 – 24% increase
- 2022 Q1 to Q2 – 18% increase

In Q2, over one-third of all botnet C&C servers that our researchers observed were located in Russia.

### New entries

Portugal (#12), Switzerland (#19), Romania (#20).

### Departures

Seychelles, Estonia, Czech Republic.

## Ups and downs across Europe

The numbers of newly observed botnet C&C servers across several European countries increased, including Moldova with a massive 81% surge, the Netherlands experiencing a 13% rise, and France with a 5% increase. Meanwhile, Portugal, Switzerland, and Romania all entered the Top 20 as newcomers.

However, it's not all bad news for European-based countries. The following saw significant reductions; Ukraine (-69%), which is more than likely a result of the ongoing conflict, Bulgaria (-55%), the United Kingdom (-52%), Latvia (-35%), and Germany (-17%).

## Significant improvements in LatAm

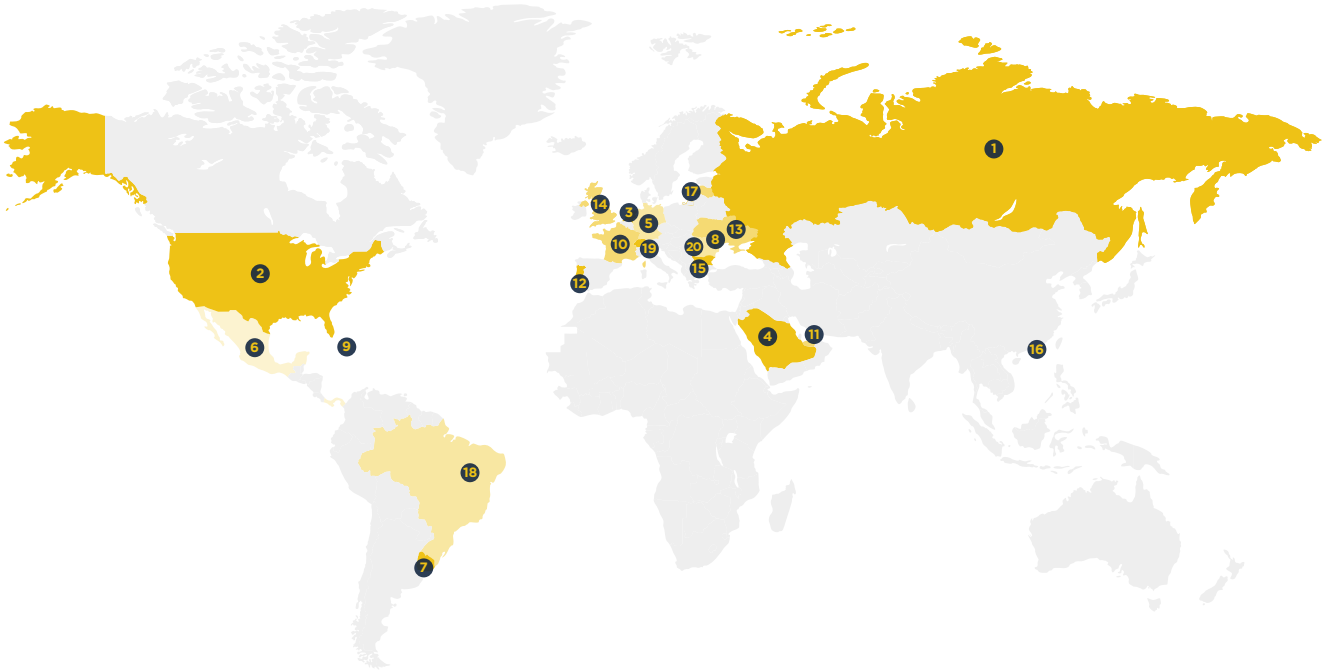
The positive trend we witnessed in Q1 2022 in the LatAm region continued in Q2. Spamhaus researchers observed improvements across Brazil, Dominican Republic, Mexico, and Uruguay. The number of newly observed botnet C&C servers hosted in Uruguay decreased by almost 50%, and the numbers for Brazil look even better with a decrease of 70%!

# Geolocation of botnet C&Cs, Q1 2022 (continued)

## Top 20 locations of botnet C&Cs

| Rank | Country | Q1 2022 | Q2 2022 | % Change Q on Q |
|---|---|---|---|---|
| #1 | Russia | 1059 | 1254 | 18% |
| #2 | United States | 461 | 384 | -17% |
| #3 | Netherlands | 191 | 216 | 13% |
| #4 | Saudi Arabia | 163 | 205 | 26% |
| #5 | Germany | 191 | 159 | -17% |
| #6 | Mexico | 163 | 137 | -16% |
| #7 | Uruguay | 170 | 100 | -41% |
| #8 | Moldova | 54 | 98 | 81% |
| #9 | Dominican Rep | 128 | 85 | -34% |
| #10 | France | 74 | 78 | 5% |

| Rank | Country | Q1 2022 | Q2 2022 | % Change Q on Q |
|---|---|---|---|---|
| #11 | UAE | 47 | 51 | 9% |
| #12 | Portugal | - | 38 | New Entry |
| #13 | Ukraine | 115 | 36 | -69% |
| #14 | United Kingdom | 64 | 31 | -52% |
| #15 | Bulgaria | 62 | 28 | -55% |
| #16 | China | 38 | 25 | -34% |
| #17 | Latvia | 37 | 24 | -35% |
| #18 | Brazil | 74 | 22 | -70% |
| #19 | Switzerland | - | 19 | New Entry |
| #20 | Romania | - | 14 | New Entry |



# Malware associated with botnet C&Cs, Q2 2022

There was a reasonable amount of movement in this Top 20 in Q2, with six new entries/departures compared to only four in Q1.

## Smoke Loader doubles its infrastructure

In Q2, Smoke Loader had one of the biggest increases in botnet C&C infrastructure associated with it, and this knocked off Loki from its Q1 top spot.

Smoke Loader (aka Dofoil) is a dropper used by different threat actors, usually to provide access to infected computers on a pay-per-install model (PPI). The number of botnet C&C servers almost doubled from 59 in Q1 2022 to 117 in Q2 2022. This malware is undoubtedly on an upward trajectory, having increased by 98% in Q2!

## Remote Access Trojans (RATs) are gaining popularity

In Q2, RATs were the most popular type of malware associated with botnet C&C servers, accounting for 35% of malware. This is quite a change from Q1, where credential stealers were the most observed type of malware at 47%.

New entry SystemBC has meant that backdoor malware types have reappeared in Q2, having departed from our chart in Q1. Additionally, a newcomer to the Top 20, called Fodcha has added Distributed Denial-of-Service (DDoS) bot to our malware types.

**What is a dropper?**

This is a malicious program that facilitates the delivery and installation of malware.

**New entries**

Matanbuchs (#5), Gozi (#10), SystemBC (#15), AZORult (#16), Fodcha (#19), OrcusRAT (#20).

**Departures**

BitRAT, CoinMiner, GCleaner, njrat, Raccoon, Tofsee.

# Malware associated with botnet C&Cs, Q2 2022 (continued)

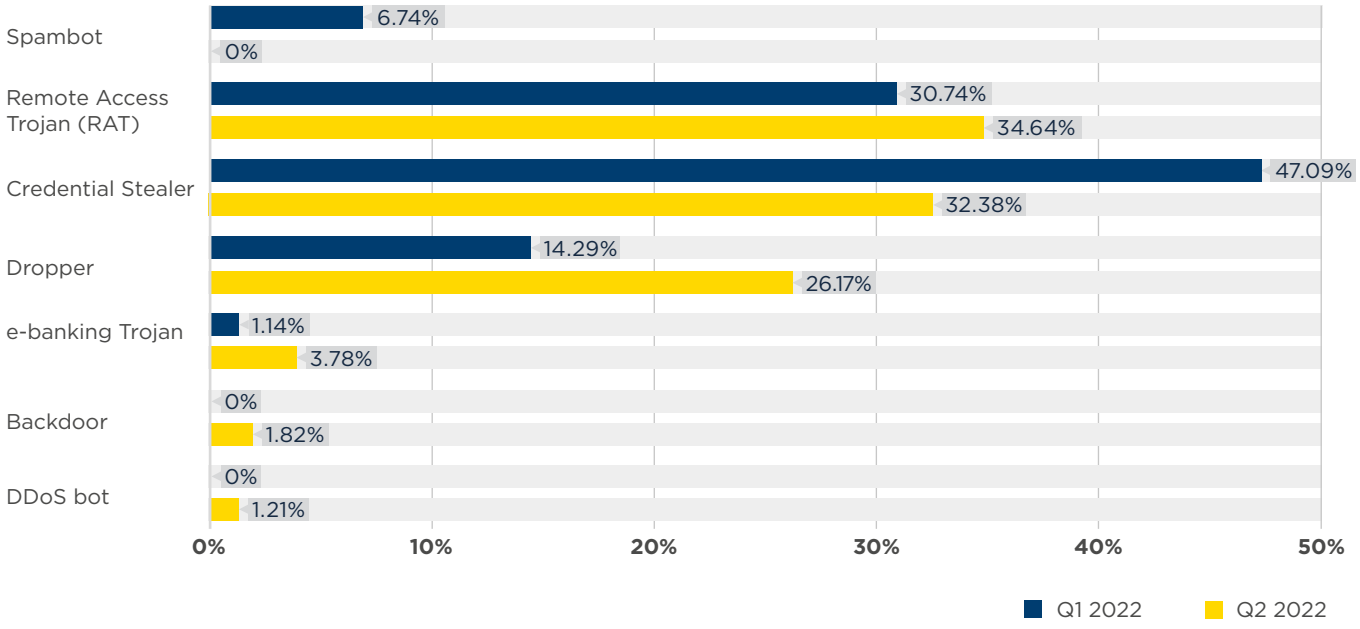
## Malware families associated with botnet C&Cs

| Rank | Q1 2022 | Q2 2022 | % Change | Malware Family | Description |
|---|---|---|---|---|---|
| **#1** | 59 | 117 | 98% | Smoke Loader | Dropper |
| **#2** | 150 | 99 | -34% | Loki | Credential Stealer |
| **#3** | 153 | 77 | -50% | RedLineStealer | Credential Stealer |
| **#4** | 74 | 71 | -4% | AsyncRAT | Remote Access Trojan (RAT) |
| **#5** | - | 56 | New Entry | Matanbuchus | Dropper |
| **#6** | 19 | 41 | 116% | AveMaria | Remote Access Trojan (RAT) |
| **#7** | 23 | 29 | 26% | Remcos | Remote Access Trojan (RAT) |
| **#8** | 12 | 27 | 125% | Vjw0rm | Remote Access Trojan (RAT) |
| **#9** | 22 | 17 | -23% | STRRAT | Remote Access Trojan (RAT) |
| **#10** | - | 16 | New Entry | Gozi | e-banking Trojan |
| **#11** | 54 | 15 | -72% | Arkei | Credential Stealer |
| **#12** | 26 | 14 | -46% | NanoCore | Remote Access Trojan (RAT) |
| **#12** | 32 | 14 | -56% | DCRat | Remote Access Trojan (RAT) |
| **#14** | 18 | 13 | -28% | Socelars | Credential Stealer |
| **#15** | - | 12 | New Entry | SystemBC | Backdoor |
| **#16** | - | 10 | New Entry | AZORult | Credential Stealer |
| **#17** | 13 | 9 | -31% | Quasar | Remote Access Trojan (RAT) |
| **#17** | 10 | 9 | -10% | DanaBot[1] | e-banking Trojan |
| **#19** | - | 8 | New Entry | Fodcha | DDoS bot |
| **#20** | - | 7 | New Entry | OrcusRAT | Remote Access Trojan (RAT) |




(1) In Q1 2022 update, DanaBot was incorrectly classified as a credential stealer.

# Malware type comparisons between Q1 2022 and Q2 2022



# Most abused top-level domains, Q2 2022

## .us drops down the Top 20

GoDaddy's .us was a new entry at #4 in Q1, so we're pleased to see a 54% decrease in the number of newly registered botnet C&C domain names associated with the TLD. Now at #12, it would be great to see this TLD drop off the Top 20 in Q3.

## .sbs departs from our charts

Spamhaus researchers have been watching .sbs with growing concern. Last year this TLD was taken over by ShortDot[1] and over the past few quarters, we've observed increasing botnet C&C abuse connected to this TLD. In Q4, it entered the Top 20 at #18 before rising to #8 in Q1. However, we're delighted that .sbs has now departed from our chart. Well done, ShortDot – we hope this continues.

## .com reverses a positive trend

Having seen a huge 75% decrease in the number of newly registered botnet C&C domain names with Verisign's TLD .com in Q1, this positive downward movement reversed in Q2, with a 134% increase.

## .cloud sees significant increases

Making its way up the Top 20 from #8 in Q1 to #3 in Q2 with a 74% increase comes ARUBA PEC S.p.A's .cloud. We hope that Italian-based ARUBA can stop the number of botnet C&C domains linked with its TLD in Q3.

## Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q2 2022, .org had more than 10.6 million domains, of which 0.0016% were associated with botnet C&Cs. Meanwhile, .tk had approximately 60,800 domains, of which 0.2814% were associated with botnet C&Cs. Both are in the top ten of our listings. Still, 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.

(1) www.spamhaus.com/resource-center/we-hope-you-keep-sbs-clean-shortdot/

# Most abused top-level domains, Q2 2022 (continued)

## Working together with the industry for a safer internet

Naturally, our preference is for no TLDs to have botnet C&Cs associated 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. Where necessary, if domain names are registered solely for distributing malware or hosting botnet C&Cs, we would like registries to suspend these domain names. We appreciate the efforts of many registries who work with us to ensure these actions are taken.

### New entries

.co (#14), .club (#17), .eu (#19), .shop (#17), .site (#20).

### Departures

.cfd, .cn, .de, .sbs, .website

## Top abused TLDs - number of domains

| Rank | Q1 2022 | Q2 2022 | % Change | TLD | Note |
|---|---|---|---|---|---|
| #1 | 913 | 2133 | 134% | com | gTLD |
| #2 | 501 | 228 | -54% | top | gTLD |
| #3 | 125 | 218 | 74% | cloud | gTLD |
| #4 | 126 | 173 | 37% | cf | ccTLD |
| #5 | 159 | 171 | 8% | tk | Originally ccTLD, now effectively gTLD |
| #6 | 115 | 168 | 46% | ml | Originally ccTLD, now effectively gTLD |
| #7 | 137 | 167 | 22% | org | gTLD |
| #8 | 192 | 121 | -37% | xyz | gTLD |
| #9 | 73 | 119 | 63% | gq | Originally ccTLD, now effectively gTLD |
| #10 | 106 | 112 | 6% | ga | Originally ccTLD, now effectively gTLD |
| #11 | 67 | 102 | 52% | info | gTLD |
| #12 | 165 | 76 | -54% | us | ccTLD |
| #13 | 53 | 57 | 8% | net | gTLD |
| #14 | - | 38 | New Entry | co | ccTLD |
| #15 | 43 | 31 | -28% | live | gTLD |
| #15 | 66 | 31 | -53% | ru | ccTLD |
| #17 | - | 25 | New Entry | club | gTLD |
| #17 | - | 25 | New Entry | shop | gTLD |
| #19 | - | 24 | New Entry | eu | ccTLD |
| #20 | - | 22 | New Entry | site | gTLD |

# Most abused domain registrars, Q2 2022

## Once again, no change at the top

Sadly, there were no changes at the top of our Top 20. NameSilo (CA) and Namecheap (US) remain in the #1 and #2 positions, respectively.

## Huge increase at Tucows

We have observed an enormous 115% increase of newly registered botnet C&C domains at the Canadian domain registrar Tucows. The number more than doubled from 87 in Q1 to 187 in Q2.

## Canadian registrars take the lead (just)

Given that NameSilo is top of the chart, and with the increases seen at Tucows, it will be no surprise that Canadian-based registrars had the highest number of botnet C&C domains registered via their services. However, while they accounted for 33.98% of domain registrations, US-based registrars were only just behind, accounting for 33.29%.

## More botnet C&C domains at GMO and PDR

The situation at the Japanese registrar GMO and the Indian-based registrar PDR doesn't look good either. We have witnessed an increase of 55% in botnet C&C domains registered through GMO and 27% at PDR.

## The situation in China improves

Some good news for China: We have seen respectable improvements across registrars based in China, with a decrease of 81% for Todaynic, 52% for NiceNic, 26% for Alibaba, and 13% for dnspod.cn. Well done!

## Reductions at Sav

In Q1, we highlighted the issues we were seeing at Sav. However, we're pleased to report that the number of botnet C&C domains registered with them has reduced by 24%. The statistics are going in the right direction; we urge Sav to keep up the momentum.

**New entries**

Launchpad (#7), OwnRegistrar (#17), Gransy (#18), Gandi (#19).

**Departures**

Ligne, WebNic.cc

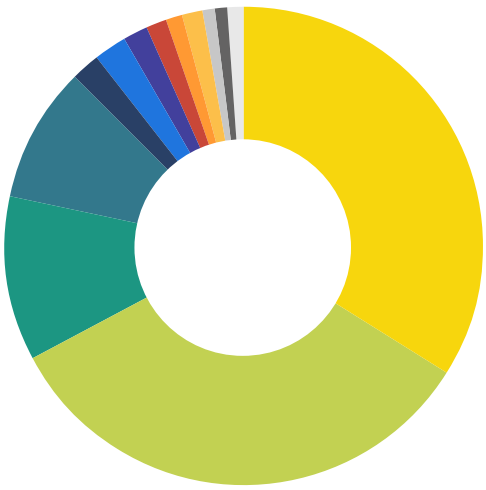
# Most abused domain registrars, Q2 2022 (continued)

## Most abused domain registrars - number of domains

| Rank | Q1 2022 | Q2 2022 | % Change | Registrar | Country |
|---|---|---|---|---|---|
| #1 | 847 | 797 | -6% | NameSilo | Canada |
| #2 | 670 | 615 | -8% | Namecheap | United States |
| #3 | 255 | 323 | 27% | PDR | India |
| #4 | 87 | 187 | 115% | Tucows | Canada |
| #5 | 266 | 128 | -52% | nicenic.net | China |
| #6 | 169 | 128 | -24% | Sav | United States |
| #7 | - | 91 | New entry | Launchpad | United States |
| #8 | 88 | 65 | -26% | Alibaba | China |
| #9 | 75 | 63 | -16% | Openprovider | Netherlands |
| #10 | 73 | 60 | -18% | RegRU | Russia |
| #11 | 96 | 59 | -39% | Porkbun | United States |
| #12 | 31 | 48 | 55% | GMO | Japan |
| #13 | 236 | 45 | -81% | Todaynic | China |
| #14 | 35 | 42 | 20% | CentralNic | United Kingdom |
| #15 | 30 | 37 | 23% | Google | United States |
| #16 | 28 | 35 | 25% | EuroDNS | Luxemberg |
| #17 | - | 34 | New entry | OwnRegistrar | United States |
| #18 | - | 33 | New entry | Gransy | Czech Republic |
| #19 | - | 28 | New entry | Gandi | France |
| #20 | 50 | 26 | -48% | Hostinger | Lithuania |
| #20 | 30 | 26 | -13% | dnspod.cn | China |
| #20 | 28 | 26 | -7% | Key Systems | Germany |




## LOCATION OF MOST ABUSED DOMAIN REGISTRARS



| Country | Q2 2022 | Q1 2022 |
|---|---|---|
| Canada | 33.98% | 29.59% |
| United States | 33.29% | 30.57% |
| India | 11.15% | 8.08% |
| China | 9.12% | 19.64% |
| Netherlands | 2.18% | 2.38% |
| Russia | 2.07% | 2.31% |
| Japan | 1.66% | 0.98% |
| United Kingdom | 1.45% | 1.11% |
| Luxemberg | 1.21% | 0.89% |
| Czech Republic | 1.14% | 0% |
| France | 0.97% | 1.14% |
| Lithuania | 0.90% | 1.58% |
| Germany | 0.90% | 0.89% |

# Networks hosting the most newly observed botnet C&Cs, Q2 2022

As usual, there were many changes in the networks hosting newly observed botnet C&Cs.

## Does this list reflect how quickly abuse is dealt with at networks?

While this Top 20 listing illustrates that there may be an issue with customer vetting processes, it doesn't reflect on the speed abuse desks deal with reported problems. See the next section in this report, "Networks hosting the most active botnet C&Cs", to view networks where abuse isn't dealt with promptly.

## Big increase in botnet C&Cs in Russia

Many Russian networks who were newcomers to our Top 20 in Q1 appear to have experienced substantial increases in the number of botnet C&Cs they are hosting on their networks in Q2. Our researchers have observed huge increases at sprinthost.ru (127%), followed by invs.ru (121%), vdsina.ru (120%), and macloud.ru (111%).

## Decrease of botnet C&Cs in LatAm

Thankfully, the situation across the LatAm region has improved, as we mentioned earlier in this report. We have observed a decrease in botnet C&C servers at antel.net.uy (-41%), claro.com.do (-34%), uninet.net.mx (-16%).

### 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 verifica-tion/ 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

timeweb.ru (#7), google.com (#10), gbnhost.com (#12), ovh.net (#13), mobily.com.sa (#15), pinvds.com (#17), mivocloud.com (#20).

### Departures

alibaba-inc.com, cloudflare.com, digitalenergy.online, gcore.lu, ihor-hosting.ru, selectel.ru, telefonica.com.br.

# Networks hosting the most newly observed botnet C&Cs, Q2 2022 (continued)

## Newly observed botnet C&Cs per network

| Rank | Q1 2022 | Q2 2022 | % Change | Network | Country |
|---|---|---|---|---|---|
| #1 | 121 | 178 | 47% | baxet.ru | Russia |
| #2 | 69 | 152 | 120% | vdsina.ru | Russia |
| #3 | 153 | 145 | -5% | stc.com.sa | Saudi Arabia |
| #4 | 62 | 137 | 121% | invs.ru | Russia |
| #4 | 163 | 137 | -16% | uninet.net.mx | Mexico |
| #6 | 63 | 133 | 111% | macloud.ru | Russia |
| #7 | - | 120 | New Entry | timeweb.ru | Russia |
| #8 | 52 | 118 | 127% | sprinthost.ru | Russia |
| #9 | 170 | 100 | -41% | antel.net.uy | Uruguay |
| #10 | - | 93 | New Entry | google.com | United States |
| #11 | 128 | 85 | -34% | claro.com.do | Dominican Rep |
| #12 | - | 75 | New Entry | gbnhost.com | Russia |
| #13 | - | 62 | New Entry | ovh.net | France |
| #14 | 54 | 61 | 13% | filanco.ru | Russia |
| #15 | - | 60 | New Entry | mobily.com.sa | Saudi Arabia |
| #16 | 63 | 59 | -6% | hostwinds.com | United States |
| #17 | - | 55 | New Entry | pinvds.com | Russia |
| #18 | 61 | 52 | -15% | ghostnet.de | Germany |
| #19 | 51 | 51 | 0% | hostsailor.com | UAE |
| #20 | - | 48 | New Entry | mivocloud.com | Moldova |

# Networks hosting the most active botnet C&Cs, Q2 2022

Hosting providers in this chart either have an abuse problem, do not take the appropriate action when receiving abuse reports, or omit to notify us when an abuse problem has been dealt with.

**New entries**

delis.one (#11), cloudflare.com (#15), dotsi.pt (#15), ovh.net (#18).

**Departures**

combahton.net, ntup.net, selectel.ru, vietserver.vn.

## Further botnet C&C servers at Google Cloud

As a new entry to this Top 20 in Q1, we have seen a hefty increase in the number of active botnet C&Cs hosted at Google Cloud throughout Q2. The numbers increased by a staggering 229%, from 24 in Q1 to 79 in Q2.

During Q3, we hope that an organization with Google's infrastructure will rapidly deal with all outstanding abuse problems. We welcome the abuse teams at Google (or any other organization) reaching out to our experts to try and resolve the issues it's facing.

## LatAm continues to struggle with active botnet C&Cs

While we have seen improvements in the number of newly observed botnet C&Cs on networks based in the LatAm region, they are still struggling to get to grips with existing botnet C&C servers. In Q2, LatAm networks hosted 61.5% of active botnet C&C servers!

## What's happening at mobily.com.sa?

In Q4, mobily.com.sa entered the Top 20. We saw a 26% increase in active botnet C&C servers on their network in Q1, which wasn't ideal. Unfortunately, in Q2, it experienced the second largest increase across all networks (176%). Given that last year this organization reported the highest top and bottom-line results since 2014[1], we urge its management to invest in its abuse team to help them tackle the issues on their network. As always, our team are on hand to help.

(1) www.zawya.com/en/press-release/etihad-etisalat-company-mobilys-net-income-for-2021-grows-368-to-sar-1-072mln-and-proposed-cash-dividends-usyg7ziz

## Networks getting to grips with botnet C&C servers

We'd like to congratulate combahton.net, ntup.net, selectel.ru, and vietserver.vn for dealing with the existing botnet C&C abuse on their networks and dropping off the Top 20 in Q2.

## Total number of active botnet C&Cs per network

| Rank | Q1 2022 | Q2 2022 | % Change | Network | Country |
|---|---|---|---|---|---|
| #1 | 501 | 636 | 27% | uninet.net.mx | Mexico |
| #2 | 422 | 561 | 33% | stc.com.sa | Saudi Arabia |
| #3 | 398 | 498 | 25% | antel.net.uy | Uruguay |
| #4 | 315 | 400 | 27% | claro.com.do | Dominican Rep |
| #5 | 198 | 219 | 11% | telefonica.com.br | Brazil |
| #6 | 83 | 105 | 27% | a1.bg | Bulgaria |
| #7 | 34 | 94 | 176% | mobily.com.sa | Saudi Arabia |
| #8 | 94 | 81 | -14% | microsoft.com | United States |
| #9 | 24 | 79 | 229% | google.com | United States |
| #10 | 65 | 71 | 9% | ielo.net | France |
| #11 | - | 64 | New Entry | delis.one | United States |
| #12 | 79 | 50 | -37% | ipjetable.net | France |
| #13 | 41 | 41 | 0% | telefonica.com.ar | Argentina |
| #14 | 29 | 35 | 21% | cableonda.net | Panama |
| #15 | - | 33 | New Entry | dotsi.pt | Portugal |
| #15 | - | 33 | New Entry | cloudflare.com | United States |
| #15 | 25 | 33 | 32% | eliteteam.to | Seychelles |
| #18 | - | 31 | New Entry | ovh.net | France |
| #19 | 24 | 29 | 21% | alexhost.md | Moldova |
| #19 | 29 | 29 | 0% | tie.cl | Chile |




That's all for now. Stay safe, and we'll see you in October!