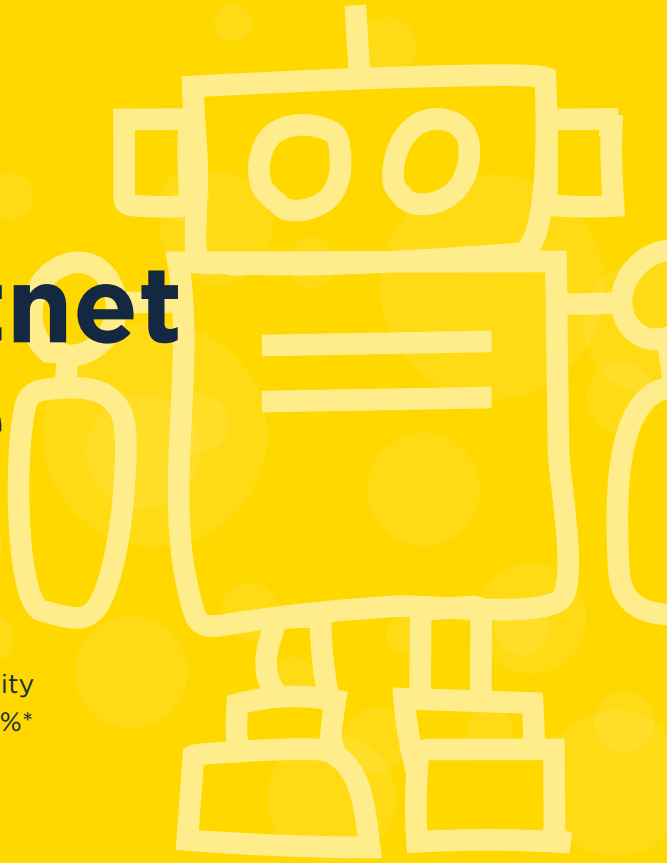
SPAMHAUS



# Spamhaus Botnet Threat Update

## Q2 2020

The pandemic certainly didn't put the brakes on botnet operators in Q2 2020. After the welcome decrease in activity at the end of Q1, the research team tracked and listed a 29%* increase in the number of botnet Command & Controllers (C&Cs) this quarter.

This increased activity is highlighted across most of our Top 20 lists, with extensive changes, including numerous new entries and departures...it's never a dull moment in the botnet ecosphere.

**Welcome to the Spamhaus Botnet Threat Update Q2 2020.**

## What are botnet 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 to 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, ransomware, launch DDoS attacks, commit e-banking fraud, click-fraud or to mine cryptocurrencies such as Bitcoin.

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

Spotlight

# Highlighting networks with the most active botnet C&Cs

Historically, our Quarterly Botnet Threat Updates have focused on newly observed botnet Command and Controllers (C&Cs). In doing so, we can clearly illustrate the quality of a network's customer vetting process and security mechanisms; however, it doesn't provide insight into how particular networks handle abuse reports.

Additionally, purely counting new botnet C&Cs enables "bulletproof" hosting companies to evade listings in our Botnet Threat Updates; they don't take down botnet C&Cs on their network. Therefore, fewer new ones appear.

To address this problem, we will now be including in this Update, statistics on those networks hosting the highest total number of active botnet C&Cs.

To produce these figures, we review the number of total unresolved botnet C&C listings detailed on the Spamhaus Blocklist (SBL) per network. Realtime data on these statistics can be accessed 24/7 on the Spamhaus website: www.spamhaus.org/statistics/networks/

### What is bulletproof hosting?

Bulletproof hosting companies provide domain or web hosting services that enable their customers to upload and/or distribute material that would not be accepted among legitimate providers.

Further details on how they operate can be found here: www.spamhaus.org/news/article/792/bulletproof-hosting-theres-a-new-kid-in-town

# Number of botnet C&Cs observed, Q2 2020

In the second quarter of 2020, Spamhaus Malware Labs identified a total of 3,559 new botnet Command & Control servers (C&Cs). Out of this total number, 2,701 were under the direct control of miscreants i.e., as a result of a fraudulent sign-up.

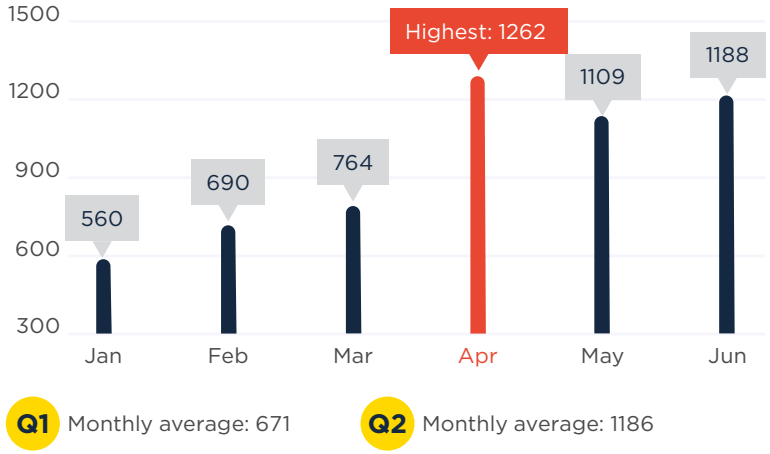
After the first quarter of this year, there was a 57% decrease in newly observed botnet C&Cs with malicious control - extremely positive. At the end of this quarter, figures unfortunately swung back in the opposite direction, with a 29%* increase.

Spamhaus Malware Labs has also identified that, over the past few months, botnet C&Cs appear to be staying active for an increased duration i.e., it's taking longer for them to be shutdown.

**What is a 'fraudulent sign-up'?**

This is where a miscreant is using a fake, or stolen identity to sign-up for a service, usually a Virtual Private Server (VPS) or a dedicated server, for the sole purpose of using it for hosting a botnet C&C.

**Number of new botnet C&Cs detected by Spamhaus since the beginning of 2020:**




**Q1** Monthly average: 671

**Q2** Monthly average: 1186

*Data updated since original publication to ensure parity of figures - comparing new botnet Command & Control servers (C&Cs) under the direct control of miscreants: 2,014 in Q1 and 2,701 in Q2.

# Geolocation of botnet C&Cs in Q2, 2020

Let's take a more in-depth look at where in the world these botnet C&Cs were hosted. Given the increase in the total number of new botnet C&Cs, it's not surprising that all countries, except China, had an uptick in the number of botnet C&Cs they were hosting. However, there are some newcomers to the chart, while other countries improved and left the Top 20 listing.

## Top 10 locations of botnet C&Cs

| Rank | Country | Q2 2020 | % Change Q on Q |
|---|---|---|---|
| #1 | United States | 896 | 7% |
| #2 | Russia | 812 | 32% |
| #3 | Netherlands | 337 | 61% |
| #4 | Germany | 185 | 7% |
| #5 | Singapore | 131 | 157% |
| #6 | France | 108 | 35% |
| #7 | Great Britain | 89 | 37% |
| #8 | China | 74 | -15% |
| #9 | Bulgaria | 72 | 38% |
| #10 | Hungary | 70 | New Entry |

### Significant increases

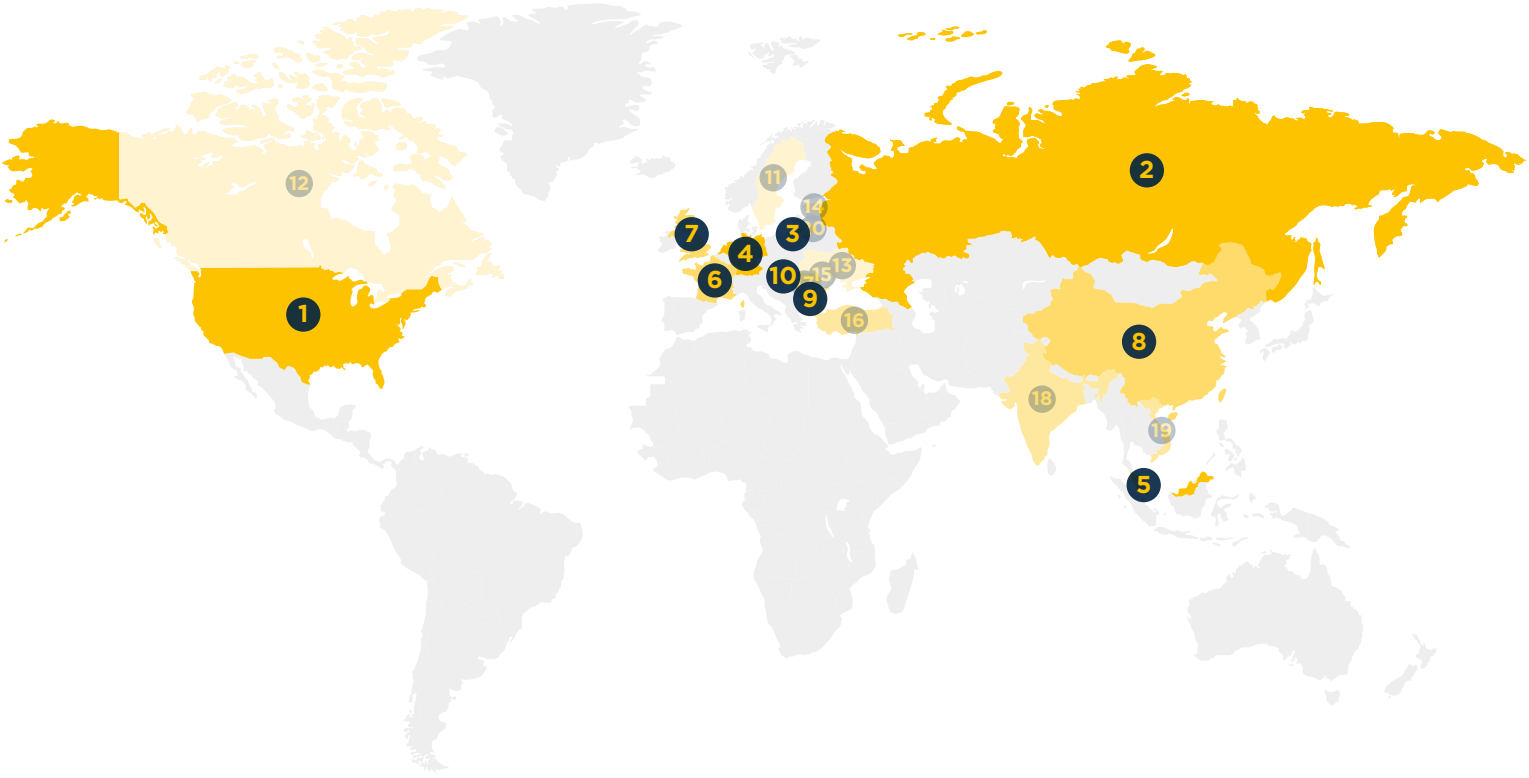
Russia is making a strong bid to take the top spot back from the USA; it increased its listing numbers by 198 botnet C&Cs quarter on quarter. Nonetheless, Singapore had the highest percentage increase of 157%, taking it from #9 in Q1 to #5 in Q2.

### New entries

#10 Hungary, #14 Estonia, #18 India and #20 Lithuania – Hungary was the highest newcomer to the Top 20 list with 70 newly detected botnet C&Cs.

### Departures

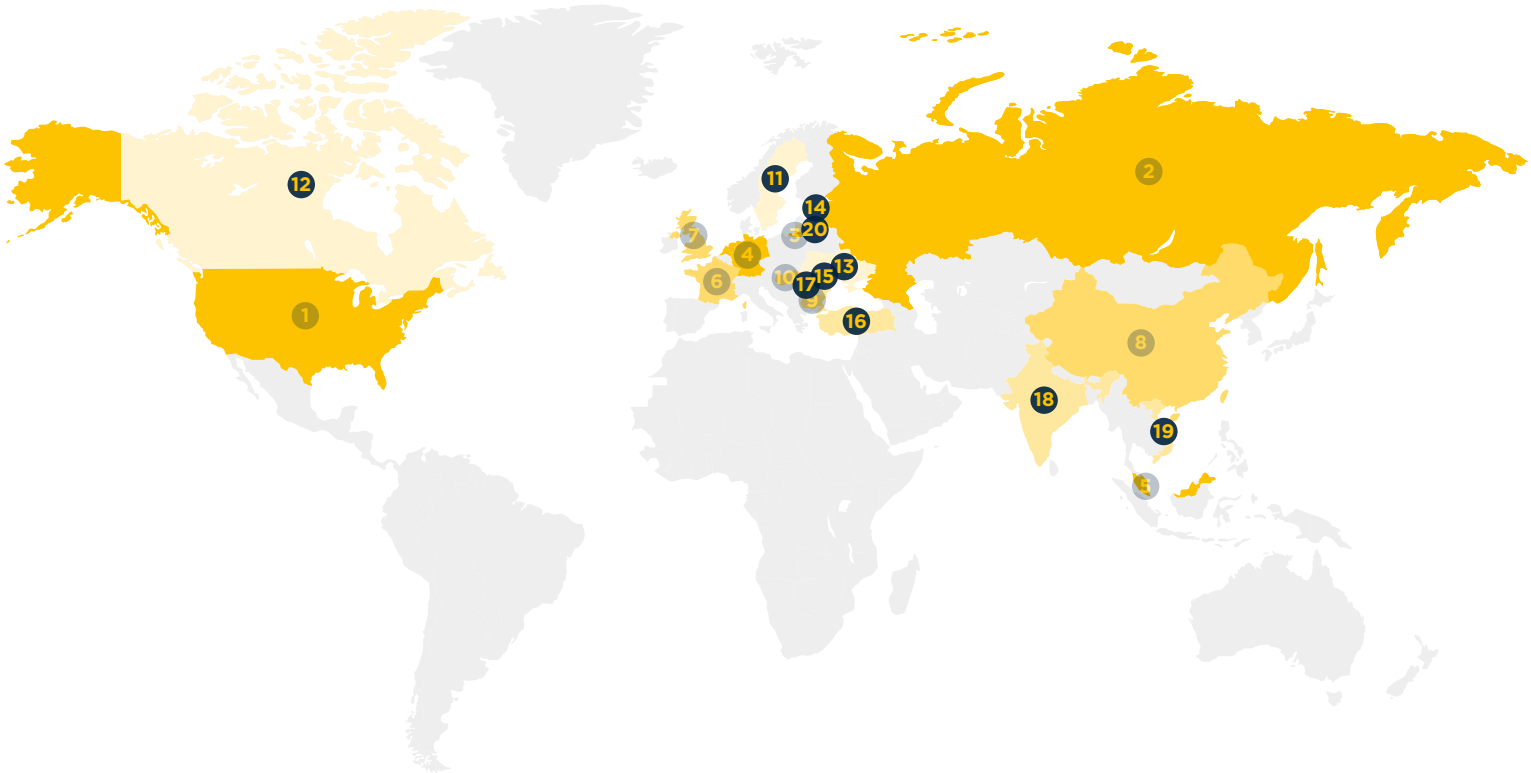
Hong Kong, Malaysia, Luxembourg and Switzerland – all these countries improved and dropped off the Top 20 List. Well done!



# Geolocation of botnet C&Cs in Q2, 2020 (continued)

## Top 11-20 locations of botnet C&Cs

| Rank | Country | Q2 2020 | % Change Q on Q |
|---|---|---|---|
| #11 | Sweden | 59 | 136% |
| #12 | Canada | 53 | 56% |
| #13 | Ukraine | 50 | 92% |
| #14 | Estonia | 46 | New Entry |
| #15 | Moldova | 45 | 105% |
| #16 | Turkey | 44 | 100% |
| #17 | Romania | 39 | 63% |
| #18 | India | 37 | New entry |
| #19 | Vietnam | 29 | 45% |
| #20 | Lithuania | 29 | New entry |



# Malware associated with botnet C&Cs, Q2 2020

## Credential Stealers

The high volume of credential stealers we had previously reported in 2019 continued into Q2, 2020.

While we have seen a decrease in malware activity linked to **Lokibot** (#1 in Q1) and **AZORult** (#2 in Q1), we have seen a substantial increase in the amount of spam emails distributing another credential stealer: **AgentTesla**. In Q2, we saw a rise of 772% in the number of botnet C&Cs associated with this malware family between Q1 & Q2. Let's be honest – that's one behemoth increase!

## QNodeService

A malware family that is new on the scene is **QNodeService**. It first appeared in March 2020[1], and acts as a download for a malicious script written in the JavaScript framework **Node.js**.

Looking at our records, it seems that **QNodeService** is the very first malware-as-a-service that is using **Node.js**. Using Java + JavaScript comes with a handful benefits from a threat actor's perspective, including poor AV detection rates and multi-OS support.

## Emotet

With no activity tracked for **Emotet** in Q2, it dropped off the Top 20 list. However, at the time of writing this report, we have seen **Emotet**'s malspam campaigns fire up, so we suspect **Emotet** will be reappearing in Q3.

### What are Credential Stealers?

This kind of malware is used by bad actors to steal personal information from a victim's computer, including key strokes (key logging functionality), session cookies, email addresses, and also credentials to various online services, such as email and File Transfer Protocol (FTP).

### New entries

#3 RedLineStealer, #9 DanaBot, #12 IcedID, #13 AveMaria, #16 QNodeService, #20 Zloader

### Departures

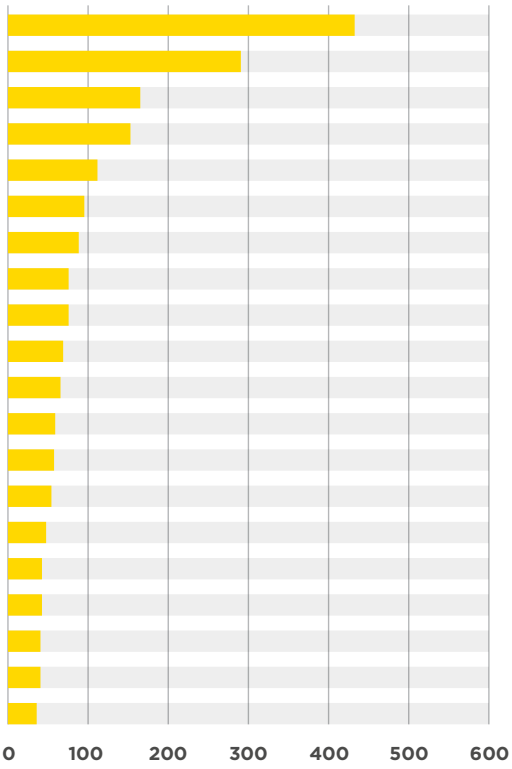
Emotet, HawkEye, PredatorStealer, QuasarRAT, RevengeRAT, TrickBot

[1]https://blog.trendmicro.com/trendlabs-security-intelligence/qnodeservice-node-js-trojan-spread-via-covid-19-lure/

# Malware associated with botnet C&Cs, Q2 2020 (continued)

## Malware families associated with botnet C&Cs

| Rank | Q2 2020 | % Change Q on Q | Malware Family | Description |
|---|---|---|---|---|
| #1 | 436 | 772% | AgentTesla | Credential Stealer |
| #2 | 290 | -46% | Lokibot | Credential Stealer |
| #3 | 169 | New entry | RedLineStealer | Credential Stealer |
| #4 | 156 | 51% | NanoCore RAT | Remote Access Tool (RAT) |
| #5 | 112 | -27% | Gozi | e-banking Trojan |
| #6 | 98 | -5% | AZORult | Credential Stealer |
| #7 | 92 | 1% | RemcosRAT | Remote Access Tool (RAT) |
| #8 | 74 | 23% | njrat | Remote Access Tool (RAT) |
| #9 | 74 | New entry | DanaBot | Credential Stealer |
| #10 | 69 | 17% | ArkeiStealer | Credential Stealer |
| #11 | 67 | 63% | KPOTStealer | Credential Stealer |
| #12 | 62 | New entry | IcedID | e-banking Trojan |
| #13 | 61 | New entry | AveMaria | Remote Access Tool (RAT) |
| #14 | 55 | -18% | Adwind | Remote Access Tool (RAT) |
| #15 | 51 | 21% | NetWire | Remote Access Tool (RAT) |
| #16 | 47 | New entry | QNodeService | Remote Access Tool (RAT) |
| #17 | 47 | 57% | RaccoonStealer | Credential Stealer |
| #18 | 46 | -4% | Pony | Credential Stealer |
| #19 | 45 | 105% | AsyncRAT | Remote Access Tool (RAT) |
| #20 | 43 | New entry | Zloader | Loader |



# Most abused top-level domains, Q2 2020

Here are the top-level domains (TLDs) chosen most frequently by botnet operators to host their infrastructure on. There have been significant changes in these between the two quarters, with six new entries and one meteoric rise.

## .top & .gq

Having sat in the lower part of the Top 20 List in Q1, **.top** has seen an extraordinary 530% increase in Q2 to take it into second place, behind **.com**. Another TLD which has seen huge increases between the two quarters is **.gq**, with a 316% increase.

## .pw

With a 91% decrease in associated botnet traffic **.pw** has dropped from #3 in Q1, to #20 in Q2.

## .de & .eu

The country code top-level domain (ccTLD) of Germany, **.de**, has been listed for the first time in our Top 20 list.

### Top-level domains (TLDs) – a brief overview

There are several different top-level domains including:

**Generic TLDs (gTLDs)** – can be used by anyone

**Country code TLDs (ccTLDs)** – some have restricted use within a particular country or region; however, others are licensed for general use giving the same functionality of gTLDs

**Decentralized TLDs (dTLDs)** – independent top-level domains that are not under the control of ICANN

### New entries

Entering the charts, and not for the first time, generic top-level domain (gTLD) .club comes back at #6. Other new entries in Q2, 2020 are #8 .de , #11 .eu, #15 .uz, #17 .ai, #18 .cc

### Departures

Having ranked #2 last quarter with 1,151 botnet C&Cs, .la has dropped off the Top 20 list in Q2, 2020. Also dropping out of these rankings are .tw, .in, .top, .me, .site. Great work!

# Most abused top-level domains, Q2 2020 (continued)

## Top abused TLDS - number of domains

| Rank | Q2 2020 | % Change Q on Q | TLD | Note |
|---|---|---|---|---|
| #1 | 5059 | 54% | com | gTLD |
| #2 | 617 | 530% | top | gTLD |
| #3 | 453 | 316% | gq | Originally ccTLD, now effectively gTLD |
| #4 | 306 | 10% | xyz | gTLD |
| #5 | 206 | 8% | net | gTLD |
| #6 | 198 | New entry | club | gTLD |
| #7 | 172 | 33% | info | gTLD |
| #8 | 170 | New entry | de | ccTLD of Germany |
| #9 | 147 | -9% | tk | Originally ccTLD, now effectively gTLD |
| #10 | 146 | -15% | ga | Originally ccTLD, now effectively gTLD |
| #11 | 111 | New entry | eu | ccTLD of Europe |
| #12 | 102 | -4% | ru | ccTLD of Russia |
| #13 | 98 | -32% | cf | Originally ccTLD, now effectively gTLD |
| #14 | 94 | -43% | ml | Originally ccTLD, now effectively gTLD |
| #14 | 94 | New entry | uz | ccTLD of Uzbekistan |
| #16 | 92 | -22% | kr | ccTLD of Korea |
| #17 | 91 | New entry | ai | ccTLD of Anguilla |
| #18 | 63 | New entry | cc | gTLD |
| #19 | 57 | -46% | org | gTLD |
| #20 | 50 | -91% | pw | ccTLD of Palau |

# Most abused domain registrars, Q2 2020

When setting up a botnet C&C infrastructure, threat actors need to decide who they are going to register their domain with. Registrars can't easily detect fraudulent sign-ups; however, domains used for botnet C&Cs don't tend to have a long lifespan with well-run registrars.

## Namcheap

The US-based domain registrar **Namecheap** has been in the #1 spot for a significant length of time.

## Enom

Entering the Top 20 at #2, **Enom** had 419 botnet C&Cs operating on domains registered to it in Q2.

## Highest climbers

**NameSilo** had a 90% increase in the number of botnet C&Cs operating on domains registered through them in Q2, taking them to #3 on the Top 20 List. However, with an even more considerable increase of 202%, was **Alibaba**, moving up #11 in Q1 to #4 in Q2.

### New entries

#2 Enom (US), #10 OnlineNic (CH), #13 Bizcn (CH), #16 Megazone (KR), #18 OVH (FR)

### Departures

EuroDNS (LU), Arsys (ES), Nom IQ (LV), Hostinger (LT) 1API (DE)

# Most abused domain registrars, Q2 2020 (continued)

## Most abused domain registrars - number of domains

| Rank | Q2 2020 | % Change Q on Q | Registrar | Country |
|---|---|---|---|---|
| #1 | 763 | 22% | Namecheap | United States |
| #2 | 419 | New entry | Enom | United States |
| #3 | 304 | 90% | NameSilo | United States |
| #4 | 299 | 202% | Alibaba | China |
| #5 | 276 | -10% | PDR | India |
| #6 | 275 | -1% | WebNic.cc | Singapore |
| #7 | 263 | -35% | Key-Systems | Germany |
| #8 | 204 | 49% | Eranet International | China |
| #9 | 178 | -31% | west263.com | China |
| #10 | 161 | New entry | OnlineNic | China |
| #11 | 137 | -22% | Hosting Concepts | Netherlands |
| #12 | 124 | -41% | RegRU | Russia |
| #13 | 95 | New entry | Bizcn | China |
| #14 | 87 | 43% | Tucows | United States |
| #15 | 84 | 20% | 55hl.com | China |
| #16 | 84 | New entry | Meagazone | Korea |
| #17 | 80 | 45% | CentralNic | United Kingdom |
| #18 | 71 | New entry | OVH | France |
| #19 | 55 | -44% | NameBright/DropCatch | United States |
| #20 | 49 | 48% | Xin Net | China |

# Networks hosting the most newly observed botnet C&Cs, Q2 2020

The hosting landscape is fast-moving. You only have to regularly look at "The World's Worst Spam Support ISPs"[2] on The Spamhaus Project's website to understand the changing environment. It is therefore not surprising that there were multiple changes in our Top 20 listings: 6 networks dropped off our charts, resulting in 6 newcomers!



## selectel.ru

This Russian based hosting company has been present in the Top 20 for a long time. However, the situation deteriorated in Q2; we witnessed a 194% increase in new botnet C&Cs on their network. As a result, **selectel.ru** has knocked cloudflare.com off their #1 spot.

## cloudflare.com

We are delighted to see that the US CDN provider **Cloudflare** improved their abuse situation in Q2, by reducing the number of botnet C&Cs operating on their network by 50%. This is a great effort – and we're looking forward to seeing this reduce further in the forthcoming quarter.

## namecheap.com

**Namecheap**, as detailed earlier in this report, is the most abused domain registrar when it comes to botnet C&Cs. Sadly, **Namecheap** also managed to get into the Top 10 list of Networks hosting the most botnet C&Cs in Q2.

## tencent.com

The Chinese cloud service provider **Tencent** was heavily abused by threat actors over the past two years for hosting botnet C&Cs. We are very pleased to see that **Tencent** dropped out of our Top 20 list in Q2.

We hope that this will be a signal to their rival, **Alibaba**, also to improve. Unfortunately, we haven't seen much sign of this yet.

[2]https://www.spamhaus.org/statistics/networks/

# Networks hosting the most newly observed botnet C&Cs, Q2 2020 (continued)

## Newly observed botnet C&Cs per network

| Rank | Q2 2020 | % Change Q on Q | Network | Country |
|---|---|---|---|---|
| #1 | 259 | 194% | selectel.ru | Russia |
| #2 | 159 | -50% | cloudflare.com | United States |
| #3 | 158 | -9% | alibaba-inc.com | China |
| #4 | 132 | 100% | ovh.net | France |
| #5 | 113 | New entry | ghlc.biz | United Kingdom |
| #6 | 111 | 109% | endurance.com | United States |
| #7 | 76 | New entry | maxko.org | Croatia |
| #8 | 69 | New entry | namecheap.com | United States |
| #9 | 59 | 69% | digitalocean.com | United States |
| #10 | 58 | 35% | colocrossing.com | United States |
| #11 | 55 | 8% | itldc.com | Ukraine |
| #11 | 55 | 25% | ispserver.com | Russia |
| #13 | 53 | 51% | leaseweb.com | Netherland |
| #14 | 52 | 79% | m247.ro | Romania |
| #14 | 52 | New entry | inter-cloud.tech | Ukraine |
| #16 | 51 | 104% | hetzner.de | Germany |
| #17 | 50 | 16% | google.com | United States |
| #18 | 49 | New entry | pq.hosting | Moldova |
| #19 | 48 | New entry | vitox.eu | Netherlands |
| #19 | 48 | 2% | baxet.ru | Russia |




## Russian hosting providers improved

We were pleased to observe that a handful of Russian based hosting providers, including **mgnhost.ru**, **firstbyte.ru** and **best-hoster.ru**, improved their fight against abuse, resulting in a lower number of new botnet C&Cs on their networks. As a result, these dropped off the Top 20 list.

### New entries

#5 ghlc.biz, #7 maxko.org, #8 namecheap.com, #14 inter-cloud.tech, #18 pq.hosting, #19 vitox.eu

### Departures

dataclub.biz, mgnhost.ru, firstbyte.ru, best-hoster.ru, tencent.com, fos-vpn.org

# Networks hosting the most active botnet C&Cs, Q2 2020

As mentioned in the "Spotlight" section of this Update, we are going to be listing network operators with the highest total number of active botnets on their network i.e., not only botnets Spamhaus has seen for the first time this quarter.

## ghlc.biz

This network, according to RIPE location in the UK, was hosting more than 300 active botnet C&Cs by the end of Q2. This network shows little interest in acting upon abuse reports, which in turn enables botnet C&Cs to remain online. Consequently, we currently consider this network as "bulletproof" and have added it to the Spamhaus Do not Route Or Peer (DROP)[3] List, advising our users not to accept any traffic to or from this network.

## inter-cloud.tech

The situation at **inter-cloud.tech** is similar to **ghlc.biz**. This network rarely takes positive actions in relation to abuse reports, allowing botnet C&Cs to remain on their network. As a result, their network ranges (prefixes) are also listed on Spamhaus DROP.

## fink.org

At the end of Q2, we calculated there close to 100 active botnet C&Cs on this network, mostly associated with Remote Access Tools (RATs).

## Cloud providers

Surprisingly, the two cloud providers **Microsoft** (Azure) and **Google** (Compute Engine) are hosting, compared to others, a large number of active botnet C&Cs.

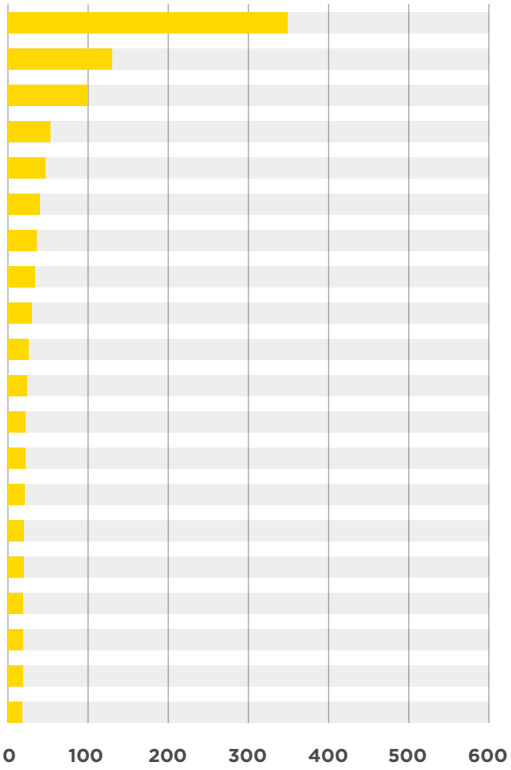
Our experience has shown that getting a response from them on abuse reports is sometimes difficult. This illustrates one of the reasons why they have a large number of active botnet C&Cs in their network.

[3]https://www.spamhaus.org/drop/

# Networks hosting the most active botnet C&Cs, Q2 2020 (continued)

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

| Rank | Botnet C&Cs | Network | Country |
|---|---|---|---|
| #1 | 349 | ghlc.biz | Russia |
| #2 | 130 | inter-cloud.tech | Ukraine |
| #3 | 99 | fink.org | Switzerland |
| #4 | 53 | digitalocean.com | United States |
| #5 | 47 | combahton.net | Germany |
| #6 | 40 | endurance.com | United States |
| #7 | 36 | mail.ru | Russia |
| #8 | 34 | google.com | United States |
| #9 | 30 | microsoft.com | United States |
| #10 | 26 | claro.com.co | Colombia |
| #11 | 24 | ipjetable.net | France |
| #12 | 22 | pointtoserver.com | Hong Kong |
| #12 | 22 | eurobyte.ru | Russia |
| #14 | 21 | inmotionhosting.com | United States |
| #15 | 20 | dtln.ru | Russia |
| #15 | 20 | avguro.com | Russia |
| #17 | 19 | invs.ru | Russia |
| #17 | 19 | cnt.gob.ec | Ecuador |
| #17 | 19 | une.net.co | Colombia |
| #20 | 18 | volumedrive.com | United States |




**We look forward to seeing you in October, with Q3's update. Stay safe.**

*Data updated since original publication to ensure parity of figures - comparing new botnet Command & Control servers (C&Cs) under the direct control of miscreants: 2,014 in Q1 and 2,701 in Q2.