SPAMHAUS
THE SPAMHAUS PROJECT

Botnet Threat Update
Q1–2020

In the past quarter, the number of botnet Command & Controllers (C&Cs) associated with fraudulent sign-ups, reduced by 57%. Good news, we hope. However, a new malware has burst onto the scene and is making the most of one particular cloud operator's infrastructure. Last but not least, it's all changed (again) when it comes to the country that hosted more botnet C&Cs than any other.

Welcome to the Spamhaus Botnet Threat Update Q1 2020.

Spotlight

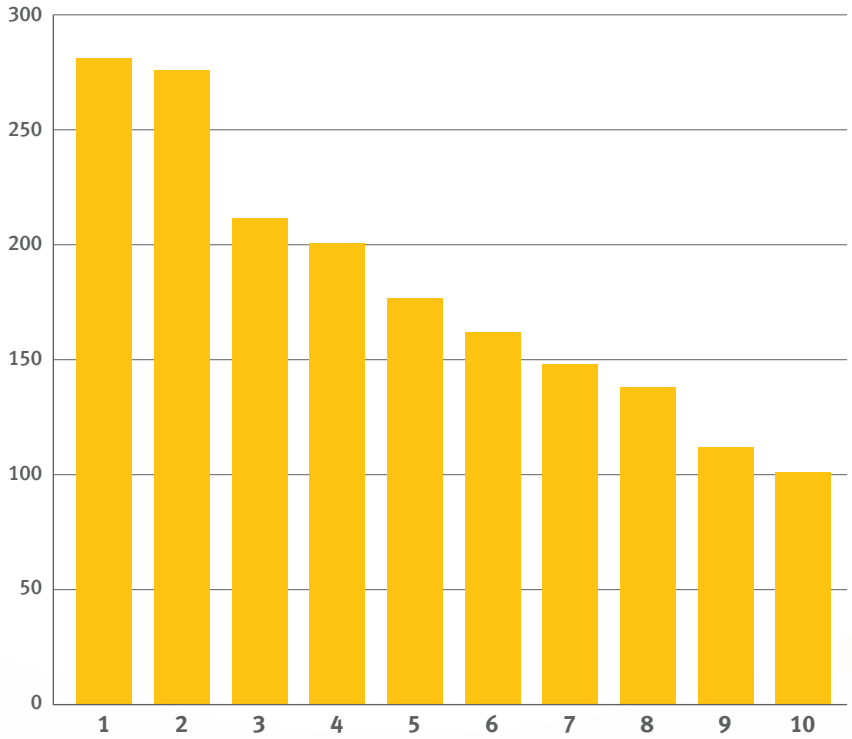
Raccoon Stealer

At the end of 2019, a newcomer joined the cyber threat landscape: Raccoon Stealer. This piece of malware is usually delivered to the end-user through spam campaigns, dropper, or exploit kits by malware that is already present on the victim's machine.

Raccoon Stealer is a credential and information stealer that runs on MS Windows. However, it is also being used by threat actors to install additional malware. What makes Raccoon Stealer rather unique is where its botnet C&Cs are hosted: on the Google Cloud.

We discovered the first instance of Raccoon Stealer on November 19, 2019. Since then, we have identified several dozen new Raccoon Stealer C&Cs – all of them hosted on the Google Cloud. But why would a threat actor use Google to host their botnet infrastructure? To answer this question, let's have a look at Spamhaus' "World's worst spam support ISPs".

The world's worst spam support ISPs – number of known spam issues



Rank	ISP	No of spam issues
1	htu.cc	281
2	google.com	276
3	chinanet-js	211
4	chinanet-ha	200
5	zzidc.com	176
6	fos-vpn.org	161
7	chinanet-zj	147
8	chinanet-hb	137
9	digitalocean.com	111
10	chinaccs.cn	100

https://www.spamhaus.org/statistics/networks/

In Q1 2020, Spamhaus listed Google as the second-worst Internet Service Provider (ISP), in regards to spam support. The reason for this poor ranking is simple: Google takes a long time to handle abuse reports regarding spammer or phishing sites. In addition to this, it also takes a long time to handle abuse reports relating to botnet C&Cs hosted on their Cloud (Google Compute Engine).

At the time of publishing this update, many abuse reports remain unanswered. This provides a perfect environment for the bad actors abusing Google's infrastructure to host malicious and harmful content, which is something the operator of Raccoon Stealer quickly noticed. Why bother looking for a shady and expensive bulletproof hosting provider when you can host your botnet infrastructure reliably and at minimal cost at Google?

Large Cloud operators can dramatically reduce the amount of badness on the internet by monitoring infrastructure for abuse, and where it's reported taking rapid action to remediate. Earlier this year, we highlighted the efforts of Amazon Webs Services (AWS)[1], who blocked port 25 outbound, resulting in a huge reduction of spam. Where a concerted effort is made, positive outcomes follow.

Botnet controllers – a brief explanation

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 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.

[1] https://www.spamhaus.org/news/article/794/amazon-web-services-thwarting-spam-with-a-decade-old-best-practice

Number of botnet C&Cs observed, Q1 2020

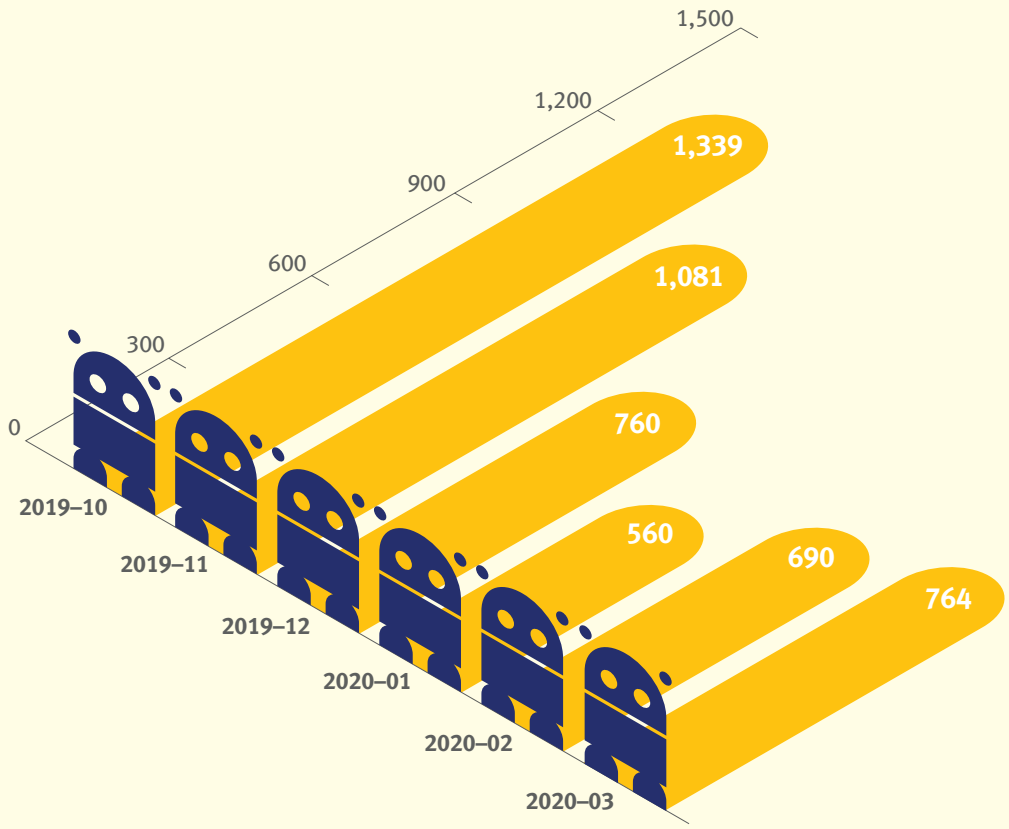
In the first quarter of 2020, Spamhaus Malware Labs identified a total number of 2,738 new botnet Command & Controllers (C&Cs). Out of these, 2,014 (average 671 per month) were under the direct control of miscreants i.e. as a result of a fraudulent sign-up. That's a decrease of 57% compared to Q4 2019. This is welcome news for internet users, following the significant increases throughout 2019.

The reason for this decrease is currently unproven. Having said that, we believe it could be partially related to a VPN provider who refuses to take action on abuse reports and is failing to shut down traffic from existing botnet C&Cs. If botnet C&Cs, which have been detected and reported, are allowed to continue to operate, there is no reason why miscreants should spin up new ones.

The drop in the number of newly registered botnet C&Cs we observed and blocked started to fall in December 2019, as the following chart indicates:

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.



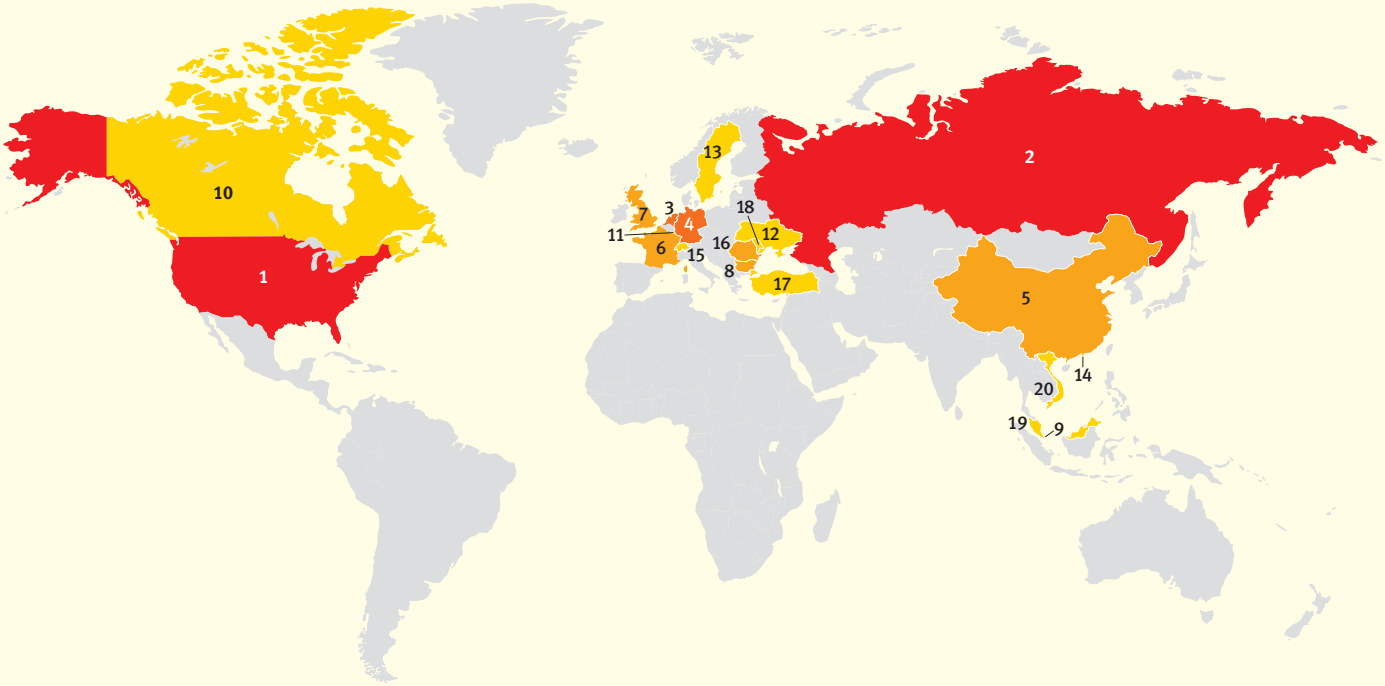
Botnet controller listings per month

Geolocation of botnet C&Cs in Q1 2020

USA is back on top: In Q4 2019, Russia took the top spot from the United States (US). However, in Q1 2020, the US has returned to the #1 spot, accounting for approximately 35% of botnet C&C traffic.

Departures: Lithuania, Serbia, Cyprus, Greece and India.

New entries: Sweden (#13), Hong Kong (#14), Turkey (#17), Malaysia (#19) and Vietnam (#20).



Rank	Botnet controllers	Country
1	841	USA
2	614	Russia
3	209	Netherlands
4	173	Germany
5	87	China
6	80	France
7	65	Great Britain
8	52	Bulgaria
9	51	Singapore
10	34	Canada

Rank	Botnet controllers	Country
11	27	Luxembourg
12	26	Ukraine
13	25	Sweden
14	25	Hong Kong
15	25	Switzerland
16	24	Romania
17	22	Turkey
18	22	Moldova
19	21	Malaysia
20	20	Vietnam

Malware associated with botnet C&Cs, Q1 2020

Credential Stealers & RATs: A vast majority of newly detected botnet C&Cs in Q1 2020 were either associated with Remote Access Tools (RATs) or credential stealers. There were only a few exceptions in our top 20 list: Gozi (e-banking Trojan), TrickBot and Emotet (both Droppers/Backdoors).

Lokibot: In Q4 2019, Lokibot's activity reduced; nonetheless, we saw a 33% increase in newly observed Lokibot C&Cs, from 403 in Q4 2019, to 535 in Q1 2020. Lokibot has held the #1 position on our Top Twenty list for over two years now!

AZORult: While we have seen a decrease in botnet activity associated with AZORult, it remained the second largest threat in Q1 2020.

NanoCore and Remcos: These two malware families appear to be fighting for dominance in the RAT market. While Remcos has never recorded more newly detected botnet C&Cs than NanoCore, the margin separating these two RATs is becoming smaller.

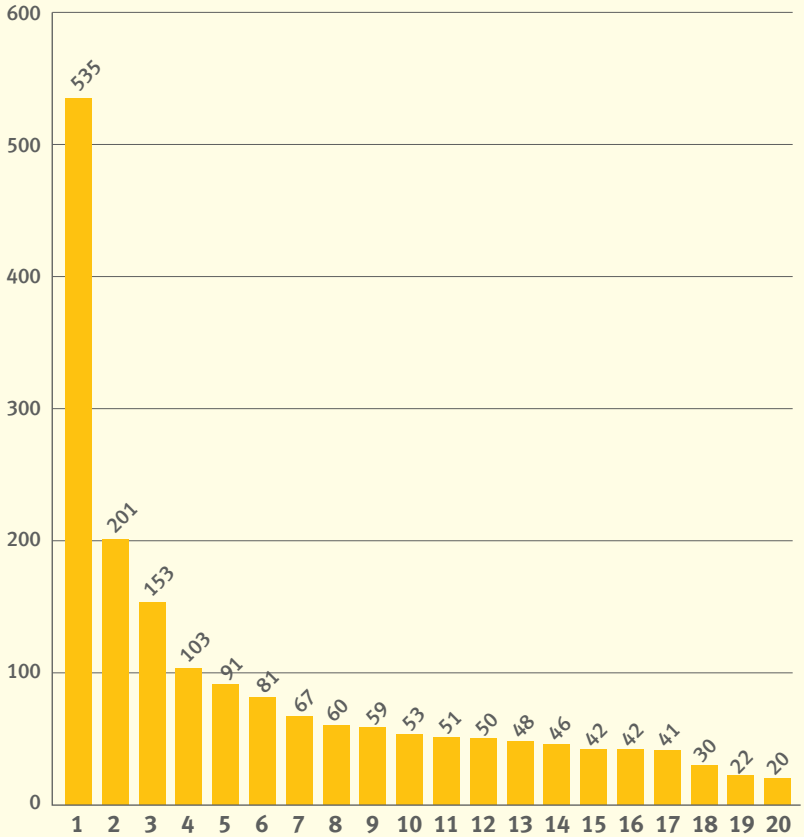
Emotet

Emotet is a former e-banking Trojan that targeted e-banking customers globally. In 2018 Emotet ceased its e-banking fraud activities and started to offer infected computers on a 'Pay-Per-Install' model. Throughout 2019 Emotet became one of the most dangerous botnets and is still considered so in 2020.

AZORult

AZORult is a credential stealer crimeware kit sold on underground hacker sites. It not only attempts to harvest and exfiltrate credentials from various applications such as web browsers, but additionally tries to steal address books from email clients.

Malware families associated with botnet C&Cs



Rank	Malware	Note
1	Lokibot	Credential Stealer
2	AZORult	Credential Stealer
3	Gozi	e-banking Trojan
4	NanoCore	Remote Access Tool (RAT)
5	RemcosRAT	Remote Access Tool (RAT)
6	Emotet	Dropper/Backdoor
7	Adwind	Remote Access Tool (RAT)
8	njrat	Remote Access Tool (RAT)
9	ArkeiStealer	CredentialStealer
10	QuasarRAT	Remote Access Tool (RAT)
11	TrickBot	Dropper/Backdoor
12	AgentTesla	Credential Stealer
13	Pony	Credential Stealer
14	PredatorStealer	Credential Stealer
15	NetWire	Remote Access Tool (RAT)
16	HawkEye	Credential Stealer
17	KPOTStealer	Credential Stealer
18	RaccoonStealer	Credential Stealer
19	AsyncRAT	Remote Access Tool (RAT)
20	RevengeRAT	Remote Access Tool (RAT)

Most abused top-level domains, Q1 2020

.la: The most significant change in this Top Twenty list is the appearance of country code top-level domain (ccTLD) .la (Laos). Not only did .la make its way onto the chart, but it also entered at #2!

.com: Throughout 2019, we reported that the vast majority of botnet C&C domains were registered in the generic top-level-domain (gTLD) .com. This trend continued in Q1 2020 with .com accounting for approximately 45% of the top-level botnet C&C domains.

.pw & .xyz: These two TLDs have appeared in the Top Twenty for over a year, although there was a significant increase in the number of botnet C&C domain registrations associated with these TLDs in Q1 2020, placing them at #3 & #4 respectively.

Top-level domains (TLDs) – a brief overview

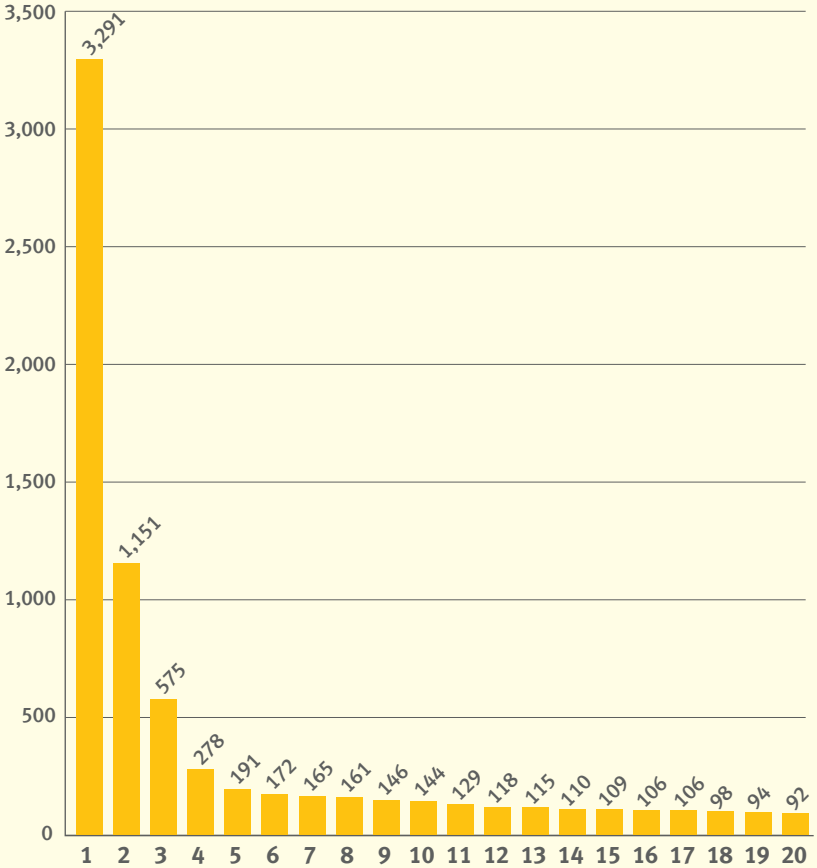
There are several different top-level domains including:

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

Top abused TLDs – number of domains



Rank	TLD	Note
1	com	
2	la	
3	pw	
4	xyz	
5	net	
6	ga	
7	ml	
8	tk	
9	tw	
10	cf	
11	info	
12	kr	
13	in	
14	uz	
15	gq	
16	ru	
17	org	
18	top	
19	me	
20	site	

Most abused domain registrars, Q1 2020

Namecheap: The USA based domain registrar 'Namecheap' continued to be the favorite place for malware authors to register their botnet C&C domains.

Key Systems: German based 'Key Systems' became the domain registrar with the second largest number of newly registered botnet C&C domains in Q1 2020. This registrar only appeared on the Top Twenty List in Q3 2019, illustrating how quickly miscreants take advantage of weak vetting processes.

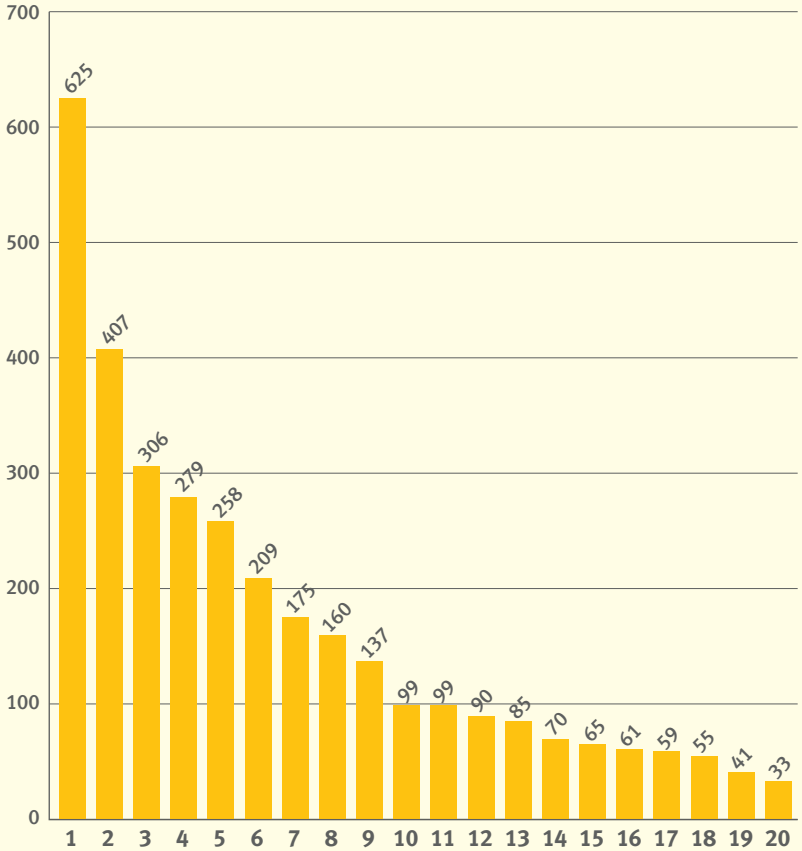
Hosting Concepts: Last year, this Dutch domain registrar was responsible for a large number of botnet C&C domain registrations, particularly relating to bulletproof hosting. We are pleased to see that it appears Hosting Concepts is improving its registration processes, dropping from #3 in Q4 2020 to #7 in Q1 2020.

Poor processes leave operators open to abuse

To register a domain name, a botnet operator must choose a domain registrar. Domain registrars play a crucial role in fighting abuse in the domain landscape: they not only vet the domain registrant (customer) but also have the ability to suspend or delete domain names.

Unfortunately, many domain registrars do not have a robust customer vetting process, leaving their service open to abuse.

Most abused domain registrars – number of domains



Rank	Registrar	Country
1	Namecheap	United States
2	Key Systems	Germany
3	PDR	India
4	WebNic.cc	Singapore
5	west263.com	China
6	RegRU	Russia
7	Hosting Concepts	Netherlands
8	NameSilo	United States
9	Eranet International	China
10	NameBright/DropCatch	United States
11	Alibaba/HiChina/net.cn	China
12	EuroDNS	??
13	Arsys	Spain
14	55hl.com	China
15	Nom IQ	??
16	Tucows	United States
17	Hostinger	Lithuania
18	CentralNic	United Kingdom
19	1API	Germany
20	Xin Net	China

Internet Service Providers (ISPs) hosting botnet C&Cs, Q1 2020

Compared to Q4 2019, there was little change in the hosting provider landscape. The usual suspects were still present in Top Twenty, including Cloudflare (US), Google (US), OVH (FR) and Hetzner (DE). It would appear that these big players in the Cloud hosting market did little to improve the situation.

Cloudflare: We continue to see cloudflare.com, a US-based content delivery network (CDN) provider, being one of the preferred options by cybercriminals to host botnet C&C servers. This trend has been evident since 2018.

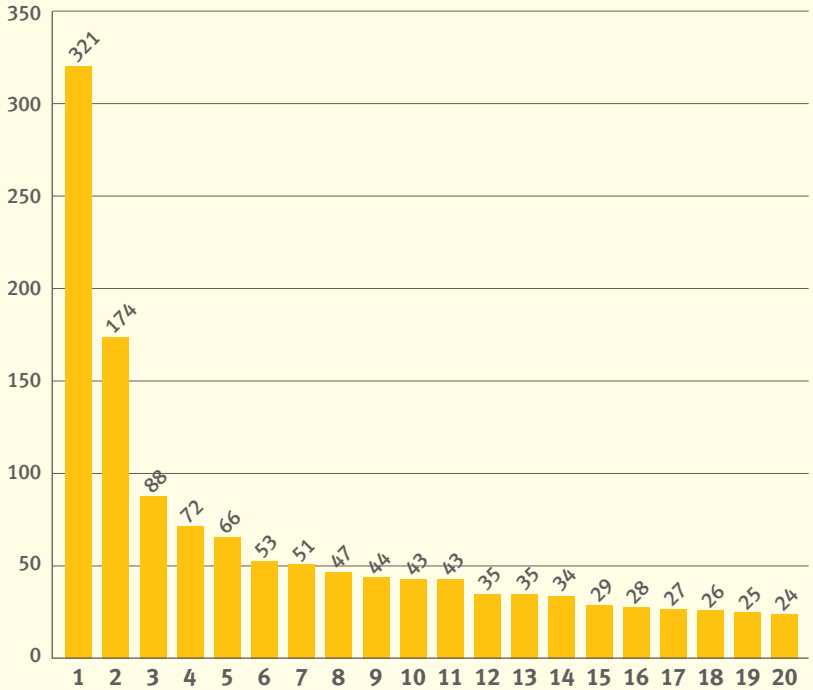
In Q4 2019, Alibaba knocked Cloudflare off the #1 spot, but Cloudflare is back as the leader in Q1 2020, with more than 300 botnet C&Cs on their network.

Disappointingly, we have still not seen any visible attempts from Cloudflare to battle the ongoing abuse on their network regarding botnet hosting and other hostile infrastructure.

Cloudflare

While Cloudflare does not directly host any content, it provides services to botnet operators, masking the actual location of the botnet controller and protecting it from DDoS attacks.

Botnet C&Cs per ISP



Rank	Network	Country
1	cloudflare.com	United States
2	alibaba-inc.com	China
3	selectel.ru	Russia
4	fos-vpn.org	Germany
5	ovh.net	France
6	endurance.com	United States
7	itldc.com	Ukraine
8	baxet.ru	Russia
9	ispserver.com	Russia
10	colocrossing.com	United States
11	google.com	United States
12	leaseweb.com	Netherlands
13	digitalocean.com	United States
14	tencent.com	China
15	m247.ro	Romania
16	best-hoster.ru	Russia
17	firstbyte.ru	Russia
18	mgnhost.ru	Russia
19	hetzner.de	Germany
20	dataclub.biz	United Kingdom

We look forward to seeing you in July when we'll be providing you with Quarter 2's update.