SPAMHAUS
THE SPAMHAUS PROJECT

Botnet Threat Update
Q1–2019

Welcome to the first quarterly update of 2019

In the first three months of this year, Spamhaus Malware Labs have observed significant changes in the malware that's associated with botnet Command & Control (C&C) servers, most notably a preference for cybercriminals to utilize crimeware kits.

Meanwhile '.com' & '.UK' are leading the way when it comes to the top-level domains (TLDs) that are associated with botnet C&Cs. However, there's no change when it comes to most abused hosting provider: Cloudflare.

Spotlight

This quarter we're putting the spotlight on a single bulletproof hosting outfit.

Since January, we have seen an upswing in the number of fraudulent domain name registrations in the ccTLD spaces '.UG' (Uganda) and '.NG' (Nigeria).

While both ccTLDs have had an increase in the number of fraudulent domain name registrations, '.UG' has gone through the roof. In February 2019, 35% of all domain names within '.UG' that Spamhaus Malware Labs observed were registered for the sole purpose of hosting a botnet controller (C&C).

Who is responsible for this massive increase of fraudulent domain name registrations in the African domain namespace? During our investigation, we discovered that a single bulletproof hosting outfit is connected to these domain registrations which is selling its services on underground sites and the dark web.

The setup is simple: They register a '.UG' domain name for their customer with the operator 'i3c.co.ug' and use a Chinese based DNS provider 'DNSPod' (Tencent). From a cybercriminal's perspective, this has a big advantage: Both i3c.co.ug and DNSPod are exceptionally slow to investigate abuse reports, that's if they are investigated at all. This makes a cybercriminal's botnet C&C infrastructure almost 100% bulletproof to takedown requests.

Spamhaus is trying to work together with both i3c.co.uh and DNSPod to resolve this issue. While communication between these operators can be challenging these efforts are starting to pay off, with the percentage of fraudulent domain registrations within ccTLD '.UG' reducing from 35% to 29%.

Looking for the path of least resistance

Once Spamhaus identifies a botnet C&C, in addition to listing the entity across our range of services, we typically send takedown requests to the relevant domain registry, registrar and network owner.

Needless to say, this has a substantial negative impact on a cybercriminal's operations. Therefore, it is no surprise that spammers, phishers and botnet operators alike, are constantly looking for new ways to increase the uptime of their botnet C&C infrastructure to ensure that their operation is running smoothly.

Number of botnet C&Cs observed in 2019

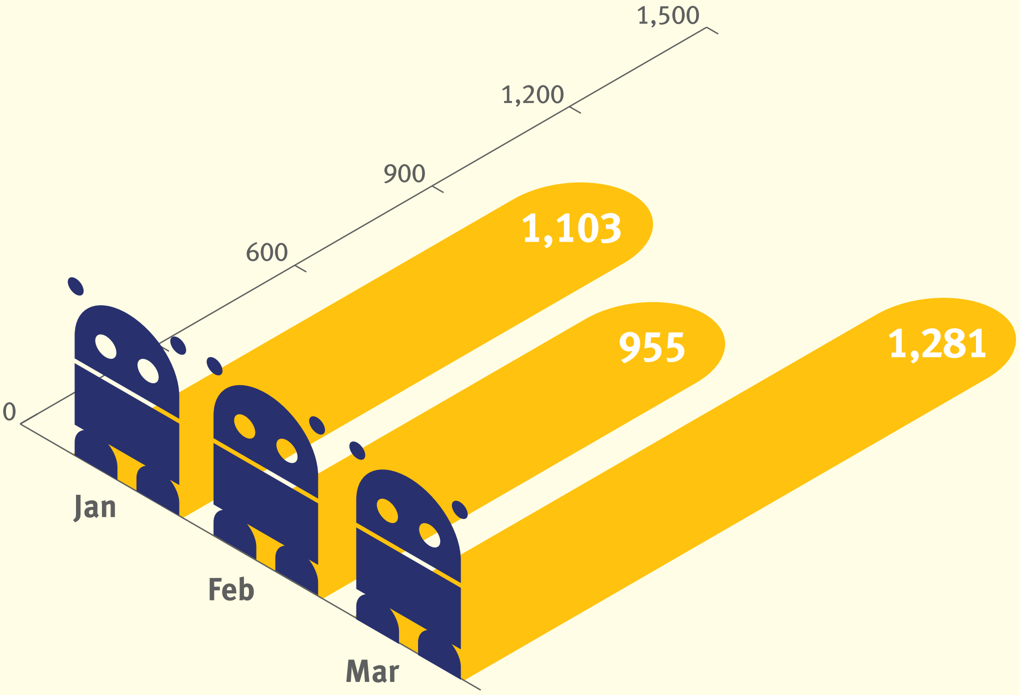
When we look at the number of newly detected botnet Command & Controllers (C&C), as a result of fraudulent sign-ups, it is evident that the upward trend detected in 2018 is continuing into 2019.

In 2018 the number of botnet C&Cs identified from fraudulent sign-ups lifted 176% from 276 per month in January to 762 per month in December. The monthly average across 2018 was 530 botnet controller listings (BCL) per month.

In this quarter we have observed another significant step-up in numbers across the first three months of this year. The number of newly detected botnet C&Cs reached 1,281 in March 2019, an additional 519 botnet C&Cs compared to December 2018's figures. Meanwhile, the monthly average in 2019 has increased by 110% to 1,113 per month.

What is a 'fraudulent sign-up'?

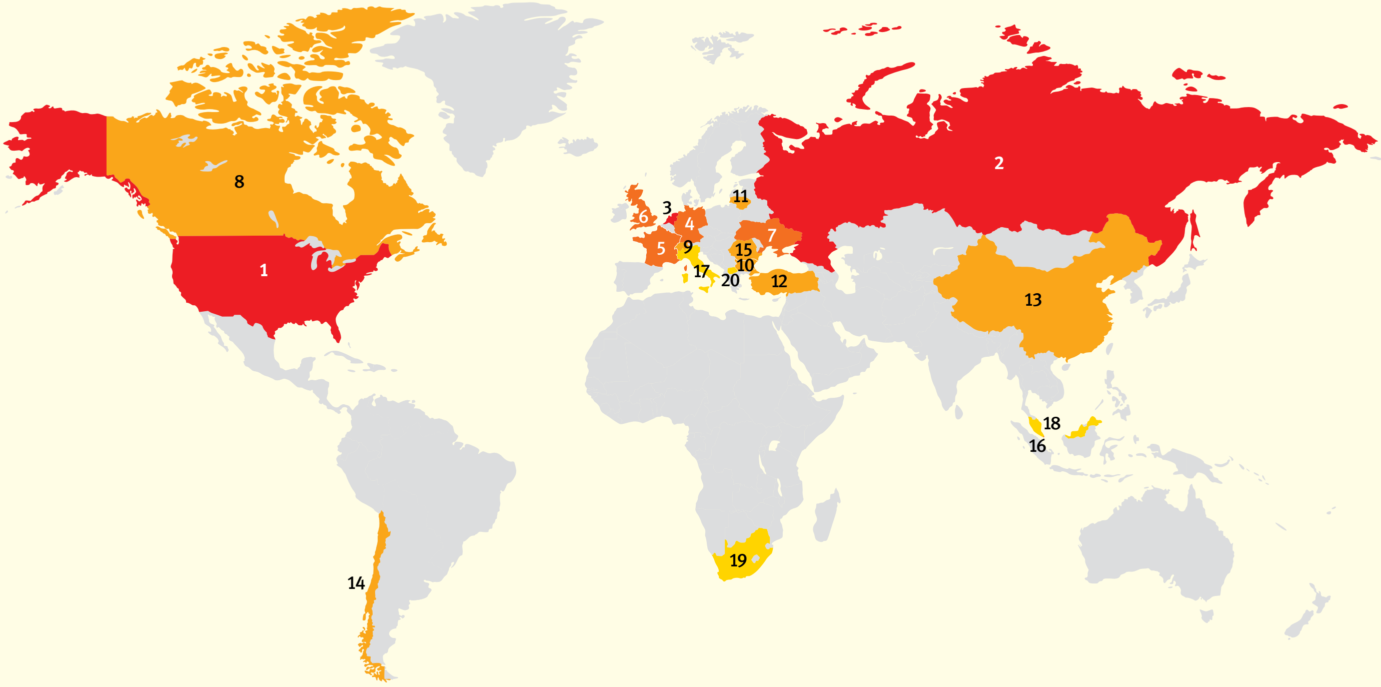
This is where a miscreant is using a fake, or stolen identity, to sign-up for a service, usually a VPS or a dedicated server, for the sole purpose of using it for hosting a botnet C&C.



Botnet controller listings per month

Geolocation of botnet C&Cs in Q1 2019

There has been no change in the location of botnet C&C traffic. The number one geolocation for botnet C&Cs remains the United States, followed by Russia and the Netherlands:



Rank	Botnet controllers	Country
1	2,275	USA
2	1,914	Russia
3	1,054	Netherlands
4	452	Germany
5	350	France
6	298	UK
7	259	Ukraine
8	224	Canada
9	211	Switzerland
10	175	Bulgaria

Rank	Botnet controllers	Country
11	169	Lithuania
12	163	Turkey
13	149	China
14	143	Chile
15	140	Romania
16	121	Singapore
17	101	Italy
18	95	Malaysia
19	94	South Africa
20	91	North Macedonia

Malware associated with botnet C&Cs, Q1 2019

We have identified substantial changes in the malware that is associated with botnet C&Cs across the first quarter of 2019. Most pertinent is the increase in the popularity of crimeware kits, which enable individuals with no previous coding experience to create, customize and distribute malware.

AZORult: Throughout 2018 a total of 915 botnet C&Cs associated with AZORult were identified and blocked by our researchers. This averages out at 76 botnet C&C per month. In the first three months of this year, 1,155 botnet C&Cs have been identified. This takes 2019's monthly average to 385 botnet C&Cs, which is a whopping 407% increase.

Crimeware kits: Lokibot (#1) and AZORult (#2) botnet C&Cs account for 64% of all botnet traffic in Q1. There is a growth in popularity of crimeware kits, indicating that cybercrime is becoming increasingly 'commoditized'. This commoditization wouldn't occur without the right kind of demand and platform. Does this point to the cybercrime market growing in sophistication, driven by the increasing opportunities the dark web presents?

JBifrost: Numbers associated with this Remote Access Tool (RAT) in 2018 proliferated, seeing it take the #2 spot, however in Q1 2019 it has moved down 4 places to #6.

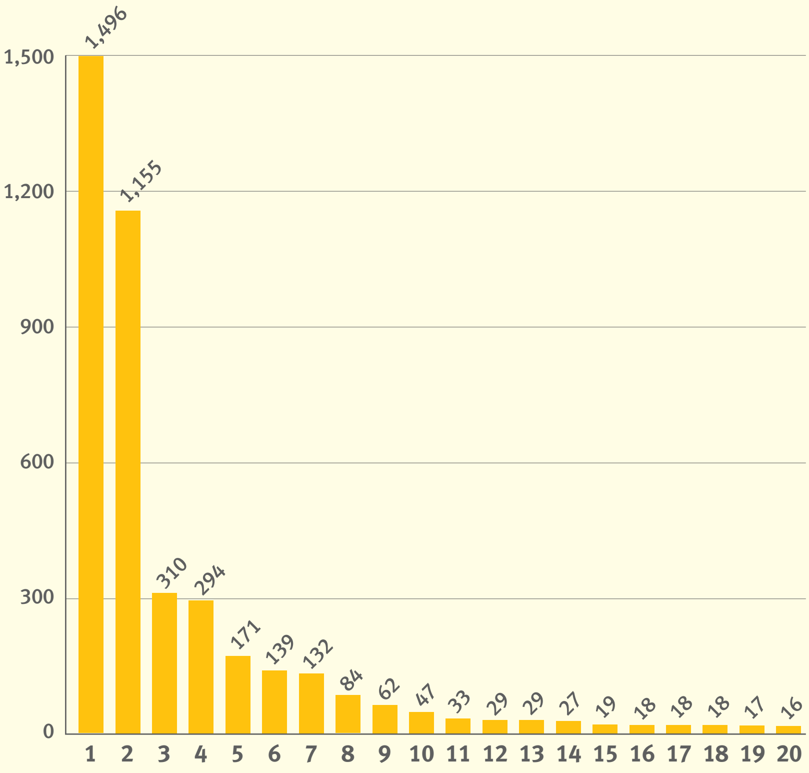
AZORult

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.

JBifrost

JBifrost, also known as Adwind, is a Remote Access Tool (RAT) based on Java. Java is a cross-platform environment which allows JBifrost to not only run on computers running the Windows operating system but also macOS and Android.

Malware families associated with botnet C&C listings Q1 2019



Rank	Malware	Note
1	Lokibot	Credential Stealer
2	AZORult	Credential Stealer
3	Pony	Dropper/Credential Stealer
4	NanoCore	Remote Access Tool (RAT)
5	RemcosRAT	Remote Access Tool (RAT)
6	JBifrost	Remote Access Tool (RAT)
7	Gozi	e-banking Trojan
8	ArkeiStealer	Credential Stealer
9	NetWire	Remote Access Tool (RAT)
10	Neurevt	e-banking Trojan
11	njrat	Remote Access Tool (RAT)
12	PredatorStealer	Credential Stealer
13	ImminentRAT	Remote Access Tool (RAT)
14	KPOTStealer	Credential Stealer
15	TinyNuke	Credential Stealer
16	RevCodeRAT	Remote Access Tool (RAT)
17	Gootkit	e-banking Trojan
18	IcedID	e-banking Trojan
19	OrcusRAT	Remote Access Tool (RAT)
20	Redosdru	Remote Access Tool (RAT)

Most abused top-level domains, Q1 2019

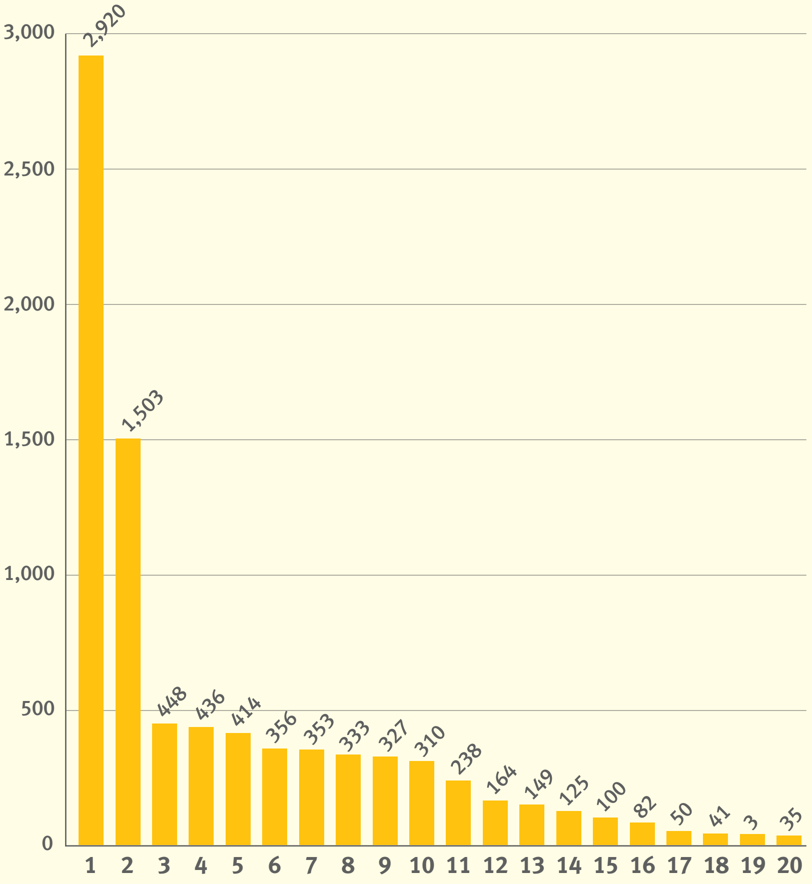
In addition to the issues that featured in our ‘Spotlight’, there has been lots of change for the top-level domains (TLDs) that are being used to host botnet C&Cs. Perhaps most interesting is that the top 2 entries are for well-known TLDs: ‘.com’ & ‘.uk’, particularly ‘.uk’ which has also seen a significant amount of shoeshow spamming activity in the past few months, as featured here.

How cybercriminals protect against takedowns

To make botnet C&Cs more resilient against takedowns cybercriminals usually register a dedicated domain name for hosting the botnet C&C.

When the hosting provider takes down the botnet C&C, the botnet operator can easily change the DNS A record to a different server.

Top abused TLDs – number of domains



Rank	TLD	Note
1	com	gTLD
2	uk	ccTLD of United Kingdom
3	tk	originally ccTLD, now effectively gTLD
4	net	gTLD
5	ga	originally ccTLD, now effectively gTLD
6	cf	originally ccTLD, now effectively gTLD
7	pw	ccTLD of Palau
8	info	gTLD
9	ru	ccTLD
10	cm	ccTLD of Cameroon
11	ml	originally ccTLD, now effectively gTLD
12	gq	originally ccTLD, now effectively gTLD
13	xyz	gTLD
14	org	gTLD
15	ug	ccTLD of Uganda
16	icu	gTLD
17	top	gTLD
18	website	gTLD
19	host	gTLD
20	su	ccTLD of Soviet Union

Most abused domain registrars, Q1 2019

Namecheap has been knocked off its top spot by Register.com, which has moved up the ranks to #1 from #10 this quarter. Namecheap accounted for 65% of all domain registrations for botnet C&Cs in 2018 and now only accounts for 15%. We hope this is due to instigating a more vigorous vetting process, and not just a result of Namecheap not running any promotions in the past quarter.

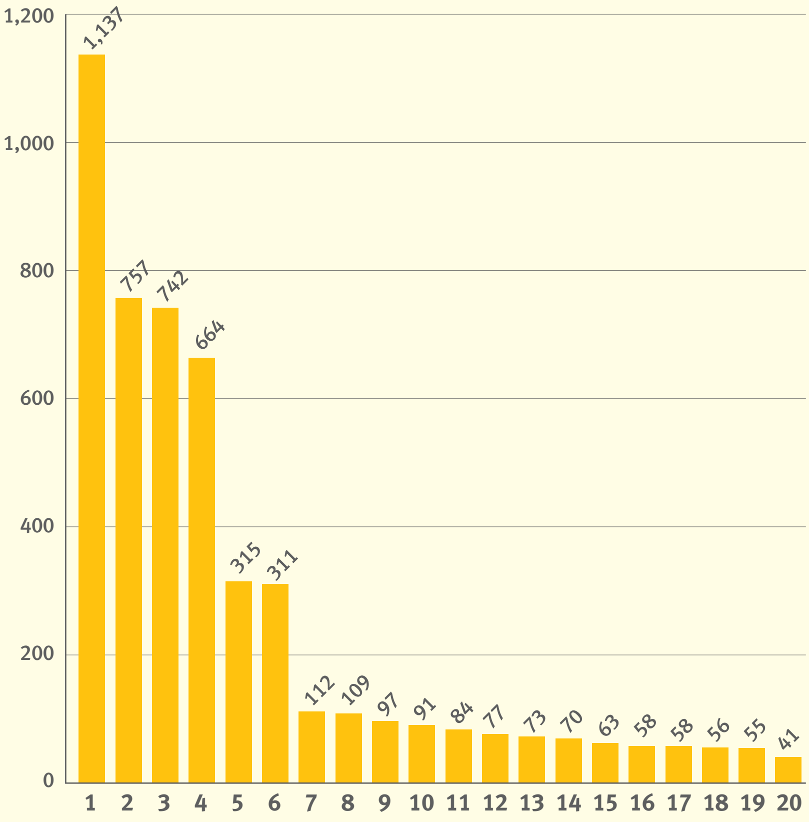
Register.com have 22% of the total domains used for botnet C&Cs registered through them in Q1 2019, compared to 0.55% across 2018.

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	Register.com	United States	🇺🇸
2	Namecheap	United States	🇺🇸
3	Network Solutions (aka web.com)	United States	🇺🇸
4	PDR	India	🇮🇳
5	RegRu	Russia	🇷🇺
6	NameSilo	United States	🇺🇸
7	GMO	Japan	🇯🇵
8	Arsys	Spain	🇪🇸
9	CentralNic	United Kingdom	🇬🇧
10	ENom	United States	🇺🇸
11	RU-Center	Russia	🇷🇺
12	Hostinger	Lithuania	🇱🇹
13	WebNic.cc	Singapore	🇸🇬
14	Eranet International	China	🇨🇳
15	Xin Net	China	🇨🇳
16	NameBright/DropCatch	United States	🇺🇸
17	Tucows	United States	🇺🇸
18	R01	Russia	🇷🇺
19	Alibaba (aka HiChina/net.cn)	China	🇨🇳
20	OnlineNIC	United States	🇺🇸

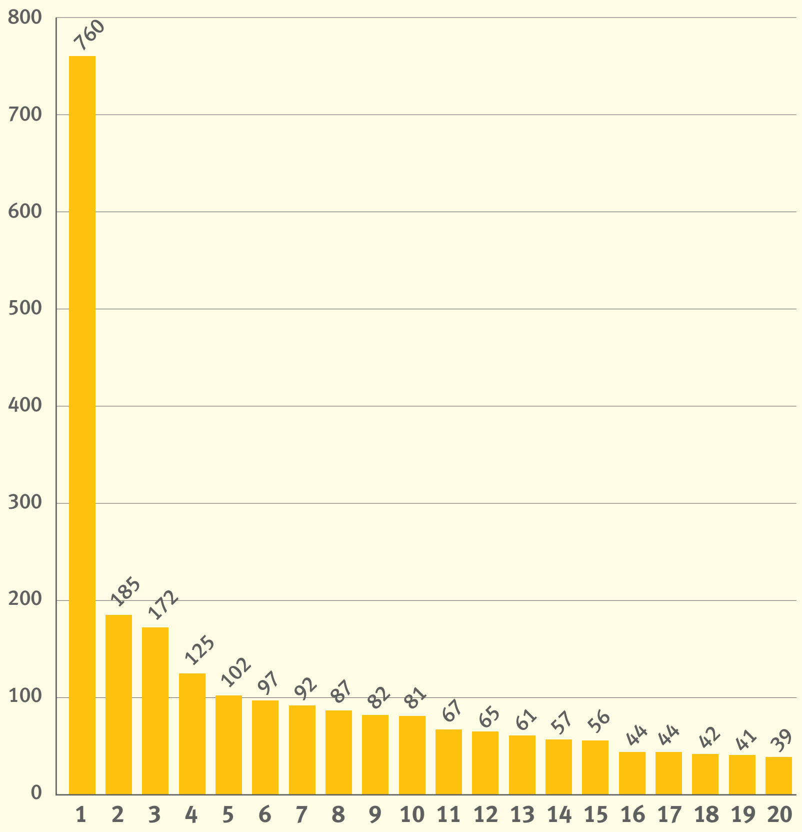
ISPs hosting botnet C&Cs, Q1 2019

What hasn't changed in Q1 2019 compared to 2018 is the preferred place that miscreants choose to host their botnet C&Cs: The US-based CDN provider Cloudflare. Cloudflare is followed some way behind by three Russian based hosting providers called Stajazk, Timeweb and Reg.ru.

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.

Total botnet C&C hosting numbers by ISP



Rank	Network	Country
1	cloudflare.com	United States
2	stajazk.ru	Russia
3	timeweb.ru	Russia
4	reg.ru	Russia
5	ovh.net	France
6	mchost.ru	Russia
7	melbicom.ru	Russia
8	simplecloud.ru	Russia
9	iliad.fr	France
10	mtw.ru	Russia
11	greenvps.net	Russia
12	m247.ro	Romania
13	alibaba-inc.com	China
14	fos-vpn.org	Seychelles
15	rivavpn.com	United States
16	well-web.net	Russia
17	skyvps.ru	Russia
18	gerber-edv.net	Bulgaria
19	select.ru	Russia
20	dataclub.biz	Belize

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

www.spamhaus.org @spamhaus

SPAMHAUS
THE SPAMHAUS PROJECT