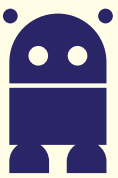
SPAMHAUS
THE SPAMHAUS PROJECT

Botnet Threat Report 2019

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 malware, location, and the hosting provider associated with botnet C&Cs.

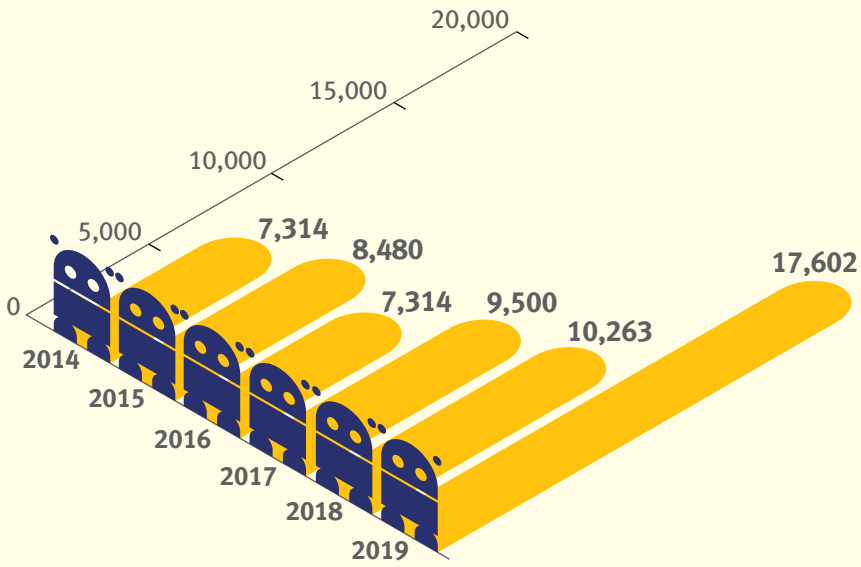
In this report, we look at key trends from 2019 and highlight the operators who are struggling with the number of botnet C&Cs associated with their particular operations. In addition, we provide insight as to what can be done to reduce global botnet threats, alongside offering some recommendations for ways that SOCs, CERTs, and CSIRTs can protect their business and users from these threats.

Contents



Number of botnet C&Cs observed in 2019

Researchers at Spamhaus Malware Labs identified and blocked 17,602 botnet C&C servers hosted on 1,210 different networks. That is an enormous 71.5% increase from the number of botnet C&Cs seen in 2018. Since 2017, the number of newly detected botnet C&Cs has almost doubled from 9,500 to 17,602.



Botnet controllers – a brief explanation

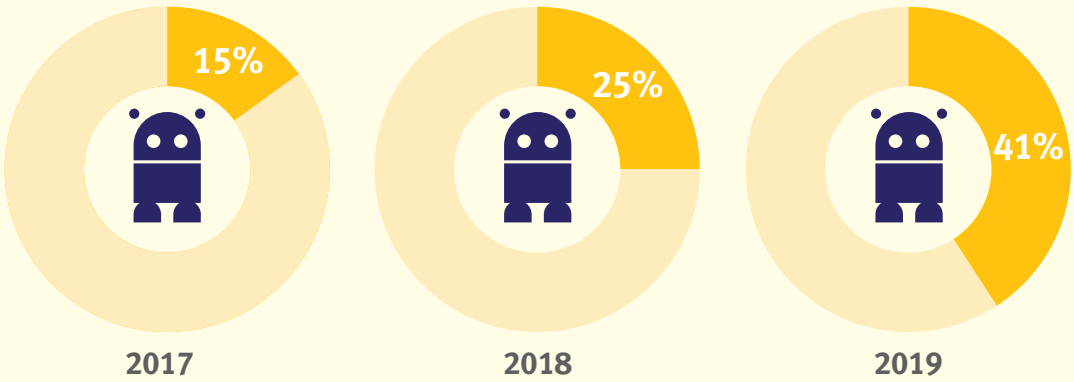
A 'botnet controller,' 'botnet C2' or 'botnet command & control' server, is commonly abbreviated to 'botnet C&C.' Fraudsters use these to both control malware infected machines and to extract personal and valuable data from malware-infected victims.

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 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.

To understand how 'popular' botnet C&Cs were as a cybercriminal's vector of choice in 2019, we reviewed the Spamhaus Block List (SBL). We looked at how many listings on this blocklist were issued for botnet C&Cs. In 2019, almost every other SBL listing issued by Spamhaus was for a botnet C&C server, another significant annual increase:

Botnet C&Cs as a percentage of all SBL listings 2017–19



Geolocation of botnet C&Cs in 2019

Russia takes the top spot: Having spent several years as the top country for hosting botnet C&Cs, the United States was knocked off its number one spot in 2019 by Russia, which experienced a 143% increase in botnet C&C traffic.

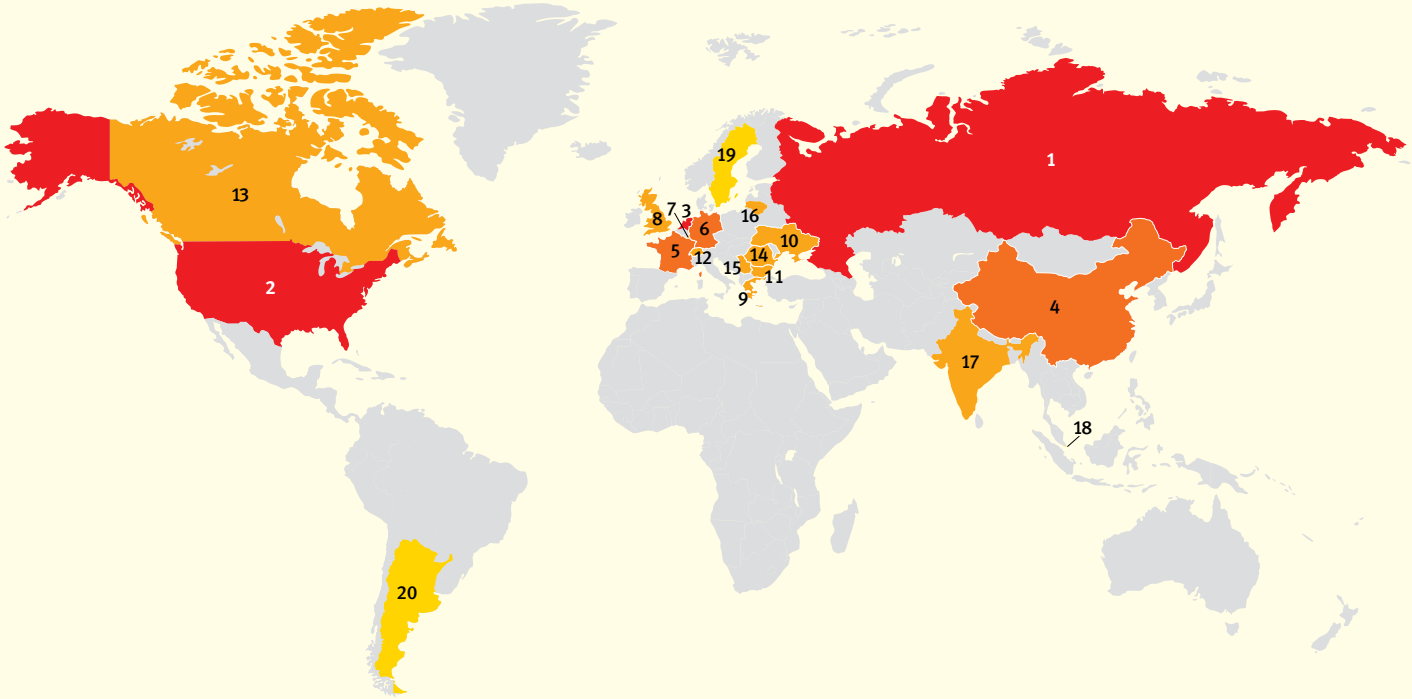
This increase doesn't surprise us. Law enforcement is less focused on internet abuse in Russia than in Western countries, and many of those providing the internet infrastructure in Russia have more lax registration procedures. Later in this report it will be shown that Russia is the most frequently recurring location of Internet Service Providers who are hosting the highest volumes of botnet C&C traffic on their networks.

China leaps up the chart: In one year, China has moved up the chart to fourth place, up from thirteenth place in 2018. It has experienced a 390% increase in the number of botnets it hosted in 2019. This percentage increase was only surpassed by Switzerland, which experienced a massive 1,119% increase from 21 in 2018, to 256 in 2019.

Departures: Chile, Italy, Malaysia, Poland, South Africa and Turkey all dropped off the Top Twenty list in 2019.

New entries: Luxemburg (#7), Greece (#9), Serbia (#15), India (#17), Sweden (#19) and Argentina (#20) were all new entries to the list in 2019.

Rank	Botnet C&Cs	Country	% change
1	4,712	Russia	+143%
2	4,007	United States	+76%
3	1,441	Netherlands	+33%
4	770	China	+390%
5	691	France	+97%
6	585	Germany	+28%
7	423	Luxembourg	—
8	401	Great Britain	+31%
9	314	Greece	—
10	300	Ukraine	+13%
11	274	Bulgaria	+57%
12	256	Switzerland	+1,119%
13	245	Canada	+5%
14	243	Romania	+63%
15	157	Serbia	—
16	117	Lithuania	–34%
17	114	India	—
18	97	Singapore	–20%
19	96	Sweden	—
20	94	Argentina	—



Malware associated with botnet C&Cs in 2019

In 2019, some malware families almost completely disappeared, while others evolved.

Credential Stealers: Nearly 60% of the newly detected botnet C&Cs in 2019 were associated with credential stealers.

Lokibot not only remained in the #1 position but also increased its number of associated botnet C&Cs by 74%, compared to 2018 figures. Fellow credential stealer AZORult joined Lokibot at the top of the chart, in the #2 position.

Emotet + TrickBot: In 2019, we observed an increase in Emotet and TrickBot malspam campaigns and infections. Traditionally, these two malware families have been used by miscreants to commit ebanking fraud. However, over the past two years, we have seen threat actors moving away from the traditional ebanking fraud model to a Pay-Per-Install (PPI) model. In 2019, Emotet and TrickBot were extremely active, predominantly with Emotet either propagating itself, or being used to drop additional ransomware i.e.TrickBot.

Remote Access Tools (RATs): In addition to credential stealers and droppers, RATs were the second highest malware family, accounting for 19% of botnet C&Cs.

In 2018 we reported that a large amount of RAT botnet C&C infrastructure was associated with Adwind/Jbifrost, but in 2019 this particular RAT reduced by 78%. It was quickly replaced with NanoCore, which increased by 181% in 2019 and rose to #3 spot on our chart.

Another RAT that disappeared in 2019 was ImminentRAT, which was taken down by the Australian Federal Police (AFP) in 2019.[1]

New entries: Credential stealers: Predator Stealer (#9), KPOTStealer (#12) and HawkEye (18), RATs: QuasarRAT (#16), ebanking Trojan: Dridex (#17) and IcediD (#19).

Loki

2018	2019
2,347	4,075

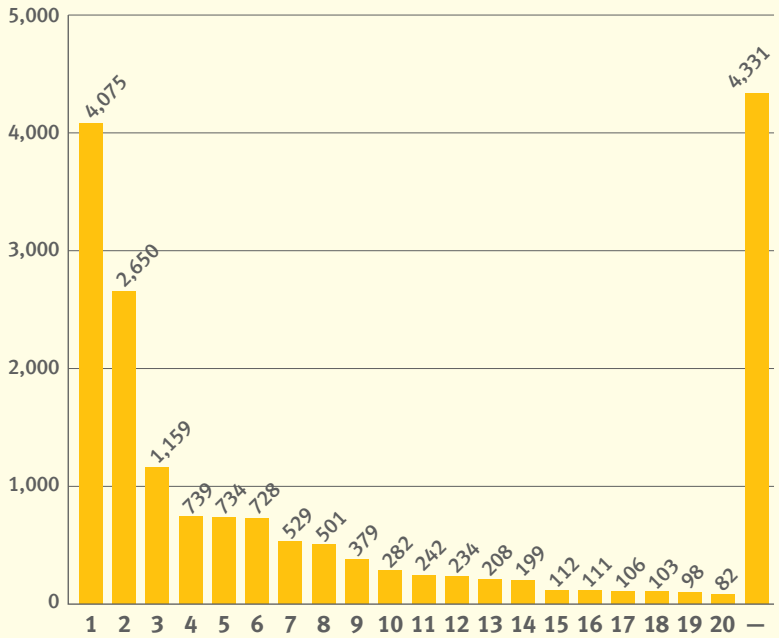
TrickBot

2018	2019
241	734

NanoCore

2018	2019
322	1,159

Malware families associated with 2019 botnet C&C listings



Rank	Malware	Note	% change
1	Lokibot	Credential Stealer	+74%
2	AZORult	Credential Stealer	+190%
3	NanoCore	Remote Access Tool (RAT)	+181%
4	Pony	Dropper/Credential Stealer	–23%
5	TrickBot	e-banking trojan	+173%
6	Gozi	e-banking trojan	+76%
7	Emotet	Dropper/Backdoor	–23%
8	RemocsRAT	Remote Access Tool (RAT)	+147%
9	Predator Stealer	Credential Stealer	—
10	Adwind/JBifrost	Remote Access Tool (RAT)	–78%
11	NetWire	Remote Access Tool (RAT)	+98%
12	KPOTStealer	Credential Stealer	—
13	ArkeiStealer	Credential Stealer	+197%
14	NjRAT	Remote Access Tool (RAT)	+290%
15	AgentTesla	KeyLogger/Credential Stealer	–4%
16	QuasarRAT	Remote Access Tool (RAT)	—
17	Dridex	e-banking trojan	—
18	HawkEye	Credential Stealer	—
19	IcedID	e-banking trojan	—
20	CoinMiner	Various crypto currency miners	–8%
—	Others	Other malware families	—

Number of botnet C&C domain names registered in 2019

The number of domain name registrations for botnet C&C hosting in 2019 dropped 71% to 20,342. Our experts believe there are two reasons for this:

1. **Domain name generation algorithms (DGAs)** were commonly used by cybercriminals to make their botnet C&C infrastructure more resilient against takedown efforts and seizures conducted by law enforcement agencies or IT researchers. However, in 2019, we saw a 42% reduction in their use.

   DGA's evidently have become less interesting and reliable to those using them. In our opinion the main drivers for this are combined industry efforts, easier wholesale blocking of DGA registrations and the increased availability of peer-to-peer (P2P) communication mechanisms. These days DGAs have mostly become a fallback mechanism.

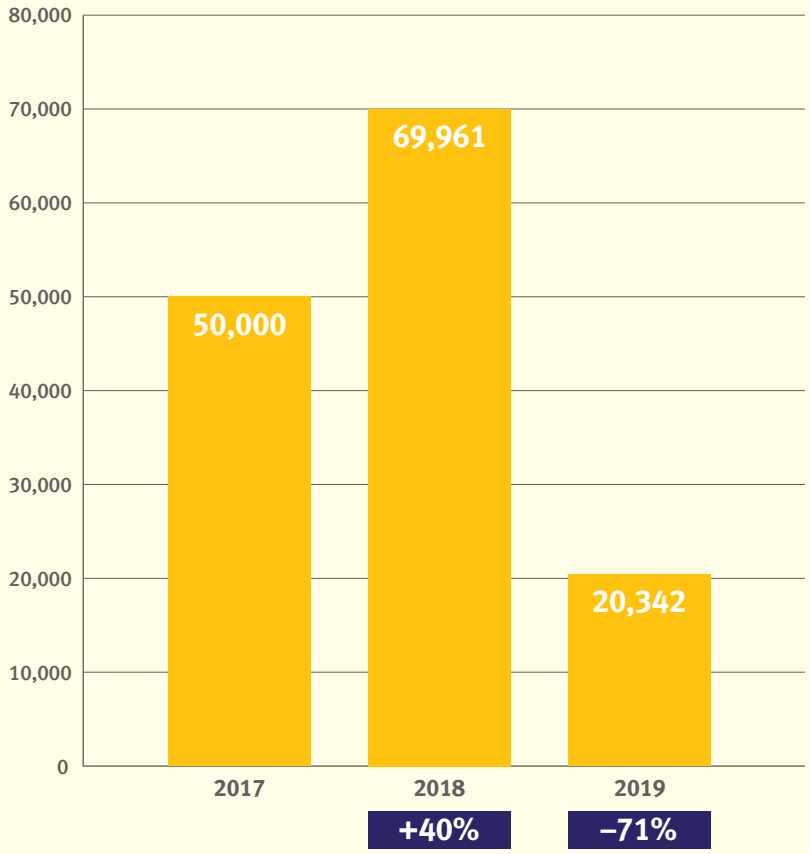
2. **There is a large supply of compromised websites.** The numbers we are including in this report exclude hijacked domain names, which are domains that are owned by non-cybercriminals that were used without permission, and domains on 'free sub-domain' provider services. Given the plentiful supply of these compromised websites it makes more sense for cybercriminals to utilize these domain names, rather than purchase new ones. From a financial perspective these domain names are free, also there is no paper trail, which in turn protects the identity of the cybercriminal.

The importance of domain names:

Cybercriminals prefer to use a domain name registered exclusively to host the botnet C&C.

A dedicated domain name allows them to fire up a new virtual private server (VPS), load the botnet C&C kit, and immediately be back in contact with their botnet after their (former) hosting provider shuts down their botnet C&C server. Not having to change the configuration of each infected computer (bot) on the botnet is a major advantage.

Domain name registrations for botnet C&C hostings 2017–19



Most abused top-level domains in 2019

Except for .ru & .com, all the TLDs that appeared on our 2018 listings saw a significant reduction in the number of botnet C&Cs associated with them. We assume that part of the reason is due to the reduction, as mentioned above, in domain registrations for botnet C&Cs. We'd also like to hope that these registries have taken positive steps to remove bad domains from their TLDs.

.com & .net: These top two TLDs accounted for approximately 50% of the botnet C&Cs in 2019. Taking into account the sheer size of both these zones, the diversity of the .com and .net registrar ecosystem and the somewhat complicated situation around abuse policies (see the recent discussions at ICANN trying to define 'DNS Abuse')[2], we do not see this changing anytime soon.

Global Registry Services Ltd: Eight top-level domains (TLDs) dropped off the most abused TLD Top 20 list in 2019. Six of those eight are managed by Global Registry Services Ltd, who have clearly made a concerted effort to clean up their TLDs.

New entries: .net (#2), .cm (#6), .org (#10), .eu (#14), icu (#16), su (#17), site (#18) & name (#20) have all made it onto the Top 20 list in 2019.

.bit: In our 2018 *Botnet Threat Report*, we raised concerns about the increase of botnet C&C domain names hosted on the decentralized TLD .bit. In Q2 2019, OpenNIC voted to drop .bit from their resolvers[3]. As a result, any botnet that relied on OpenNIC to resolve .bit stopped functioning, leading to the number of botnet C&C domains within .bit dropping to almost zero.

.pw: This TLD topped the rankings in 2018; however, we observed a 92% reduction in the amount of botnet C&Cs associated with .pw in 2019, dropping it down to #5.

Top-level domains (TLDs) – a brief overview

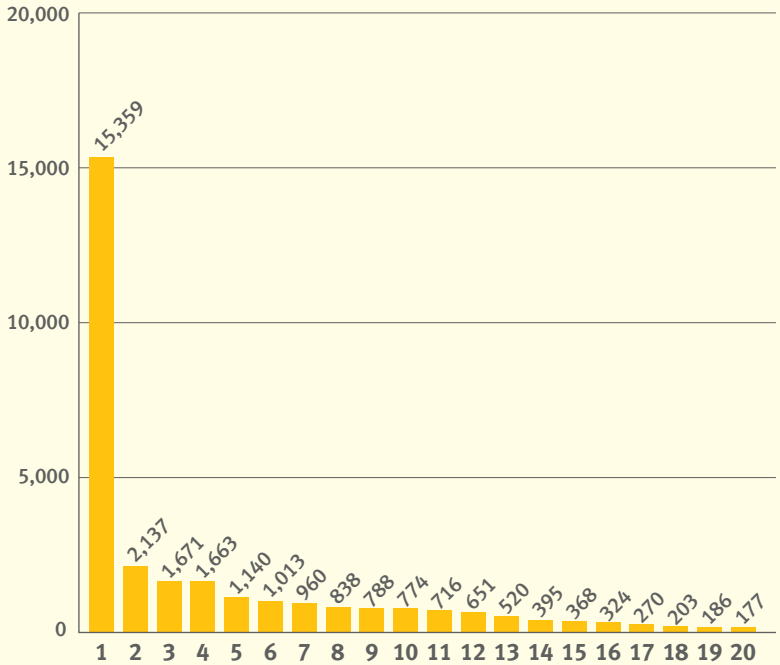
There are several different top-level domains including:

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	% change
1	com	gTLD	+30%
2	net	gTLD	—
3	ru	ccTLD of Russia	+41%
4	info	gTLD	–1%
5	pw	ccTLD of Palau	–92%
6	cm	originally ccTLD, now effectively gTLD	—
7	top	gTLD	–90%
8	tk	originally ccTLD, now effectively gTLD	–86%
9	ga	originally ccTLD, now effectively gTLD	–68%
10	org	gTLD	—
11	xyz	gTLD	–87%
12	cf	originally ccTLD, now effectively gTLD	–70%
13	ml	originally ccTLD, now effectively gTLD	–90%
14	eu	ccTLD of European Union	—
15	gq	originally ccTLD, now effectively gTLD	–83%
16	icu	gTLD	—
17	su	ccTLD of Soviet Union	—
18	site	gTLD	—
19	club	gTLD	–86%
20	name	gTLD	—

Most abused domain registrars in 2019

Cybercriminals need to find a sponsoring registrar to get a botnet C&C domain name registered. Registrars can't easily detect all fraudulent registrations or registrations of domains for criminal use before these domains go live. However, the 'life span' of criminal domains on legitimate, well-run, registrars tends to be quite short.

Namecheap was (again) the most abused registrar: Around 25% of all botnet C&C domain names were registered through this US-based registrar. It's the third consecutive time that Namecheap has held the pole position in our annual ranking of most abused domain registrars.

Key-Systems used for fast flux hosting: In 2019, we saw an increase of fraudulent domain registrations with Key-Systems. A key point to note is that many of the C&C domains that were hosted on fast flux networks were registered through this particular registrar.

Hosting Concepts used for bulletproof hosting: The new bulletproof hosting outfit Spamhaus identified in the latter half of 2019[4] has been heavily utilising this registrar for registering botnet C&C domains for their customers. As a result, this Dutch registrar made it onto our chart for the first time.

Alpnames shut down by ICANN: In March 2019, ICANN shut down this Gibraltar based domain registrar. As a result, the number of newly registered botnet C&Cs domain names at this registrar dropped down to zero.

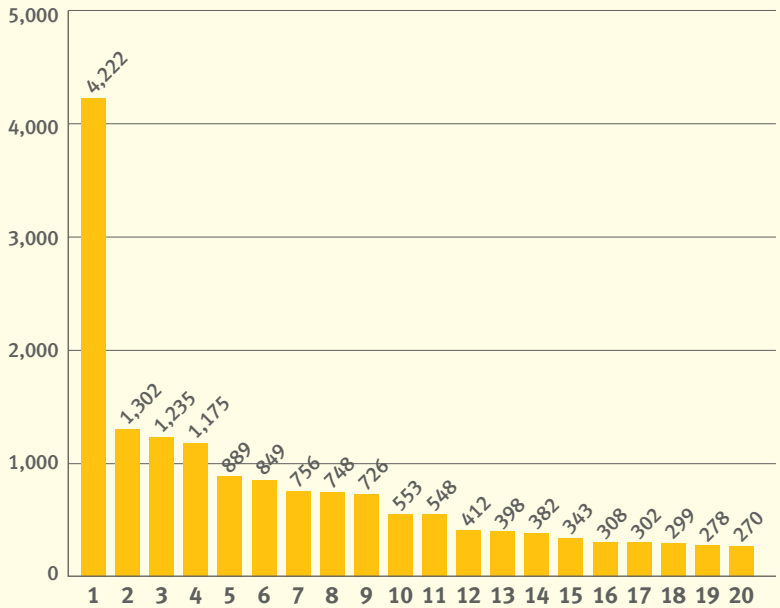
New entries: Key Systems (#5), WebNic.cc (#6), Hosting Concepts (#8), 55hl.com (#9), Hostinger (#13), GMO (#14).

Departures: Out of the five domain registrars that dropped off the Top Twenty list in 2019 (excluding Alpnames), four were based in the United States: Enom, Network Solutions (aka web.com), Register.com & Tucows.

Fast flux

Botnets use this DNS technique to obscure phishing sites, or domains for downloading malware. This is done by placing the phishing or malware behind an ever-changing network of compromised hosts, which act as proxies.

Fraudulent domain name registrations



Rank	Registrar	Country	% change
1	Namecheap	United States	–89%
2	RegRU	Russia	–10%
3	PDR	India	–91%
4	NameSilo	United States	+54%
5	Key Systems	Germany	—
6	WebNic.cc	Singapore	—
7	west263.com	China	+160%
8	Hosting Concepts	Netherlands	—
9	55hl.com	China	—
10	NameBright (aka DropCatch)	United States	+216%
11	CentralNic	Great Britain	+114%
12	RU-Center	Russia	+159%
13	Hostinger	Lithuania	—
14	GMO	Japan	—
15	Eranet International	China	+214%
16	OnlineNIC	China	+84%
17	Arsys	Spain	+14%
18	Xi Net	China	–18%
19	Alibaba	China	–86%
20	R01	Russia	+42%

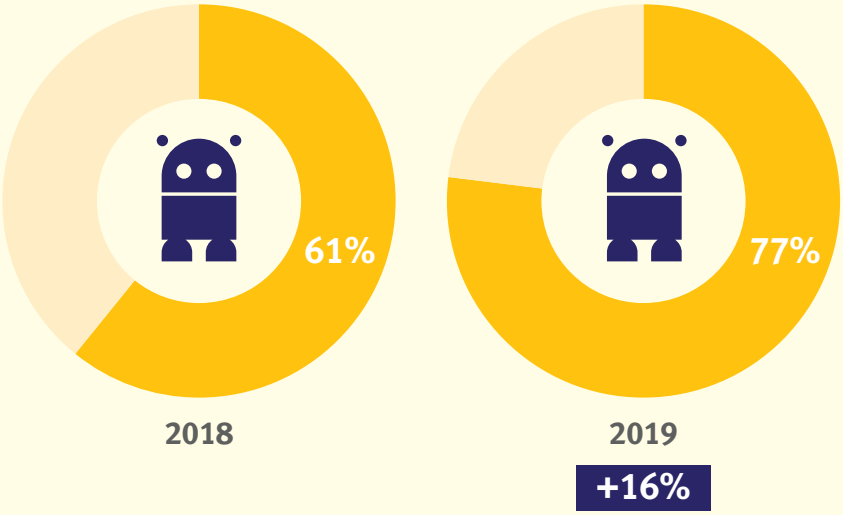
New bulletproof hosting operator increased number of botnet C&Cs in 2019

From all of the botnet C&Cs Spamhaus observed in 2019, 77% were as a result of fraudulent sign-ups, compared to 61% in 2019. This 16% increase, we believe, can be attributed to the new bulletproof hosting operation we previously mentioned.[5] This new set-up operates with a new modus operandi, providing its clients with significant benefits over previous bulletproof hosting models.

What is a 'fraudulent sign-up'?

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

Fraudulent sign-ups 2018–19



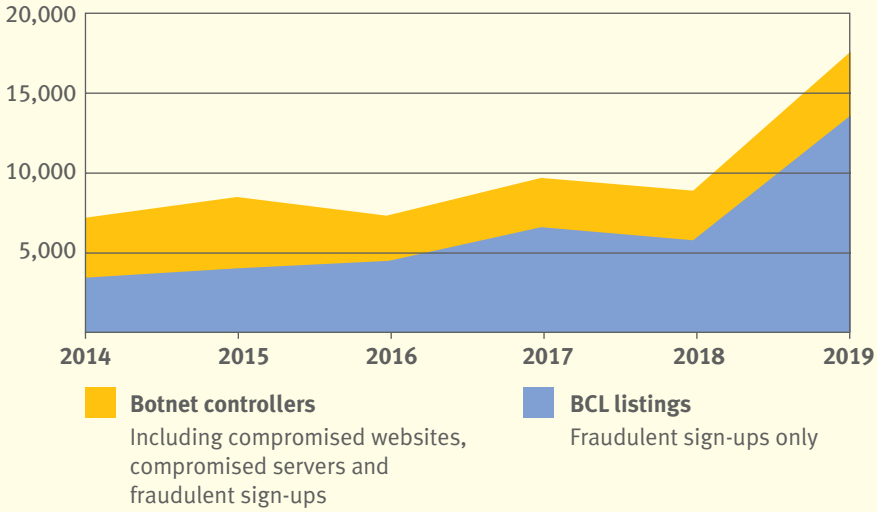
Botnet C&Cs resulting from fraudulent sign-ups in 2019

When a botnet C&C is noted to be the result of a fraudulent sign-up, it is subject to a listing on the Spamhaus Botnet C&C List (BCL). The graph below shows the overall number of botnet C&C listings versus the number of botnet C&C listings on the BCL between 2014–2019.

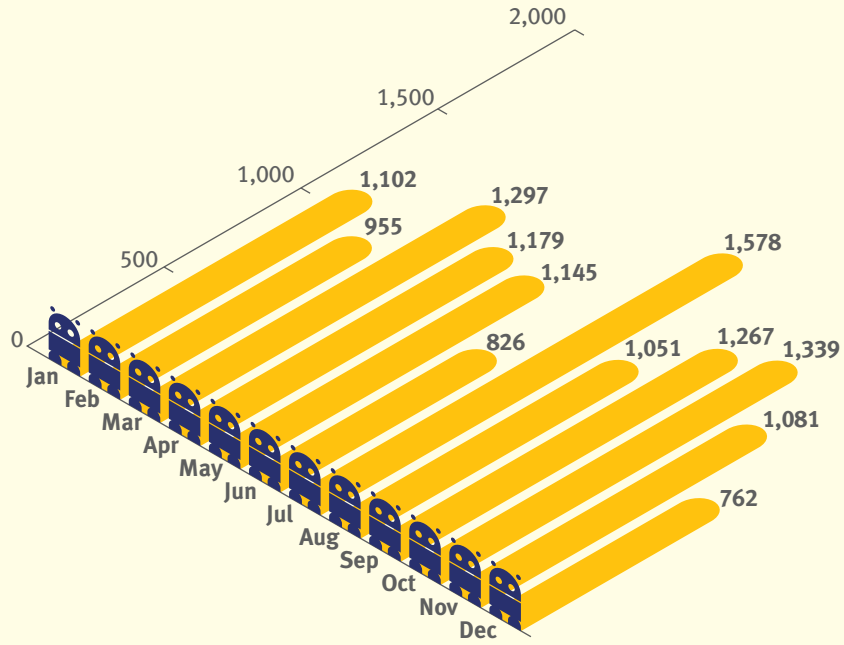
In 2019, we averaged approximately 1,130 BCL listings per month. This is more than double the average in 2018 (530 per month).

With the above mentioned new bulletproof hosting operation, we feel confident that the number of fraudulent sign-ups at hosting providers will increase in 2020 unless hosting providers implement more robust customer verification processes.

Total of newly detected botnet C&C listings vs newly detected BCL listings 2014–2019



Spamhaus Botnet C&C Listings (BCL) per month



How to utilize the BCL

This is a 'drop all traffic' list intended for use by networks to null route traffic to and from botnet C&Cs. These IP addresses host no legitimate services or activities, so they can be directly blocked on both ISP and corporate networks without the risk of affecting legitimate traffic. Infected computers that may be present on their networks are effectively rendered harmless.

The dark side of the Internet

These statistics exclude botnet C&Cs hosted on the dark web (like Tor). The use of such anonymization networks by botnet operators started becoming more popular in 2016. This popularity is more than likely driven by the fact that the location of the botnet C&C is unidentifiable; making the takedown of a server almost impossible. This trend has continued into 2019. However, a vast amount of the botnet C&Cs detected by Spamhaus Malware Labs in 2019 were still hosted on the clear web.

For anonymization services like Tor, we recommend a whitelist approach: In general, block access to anonymization services except for those users who need it (opt-in).

ISPs hosting botnet C&Cs in 2019

Before we reveal which hosting ISPs had the largest number of botnet C&Cs on their networks in 2019, it is essential to understand some key points:

Preventing Botnet C&Cs on compromised servers or websites: It can be difficult for an ISP or hosting provider to do this since these are often under the control of the customer. Many servers and websites are running outdated software, making them vulnerable to attacks from the internet. We have seen that some of the more proactive ISPs and hosting providers are now using newer tools and methods to track down outdated software and monitor botnet C&C traffic. Of course, blocking traffic to known botnet C&Cs is a good start.

Preventing Botnet C&Cs on servers used solely for hosting a botnet C&C: ISPs have far more control in this situation since when a new customer tries to sign-up, a customer verification/vetting process should take place before commissioning the service. Where ISPs have a high number of BCL listings (botnet C&Cs hosted on servers solely for that purpose, i.e., a fraudulent sign-up) it highlights one of the following issues:

1. ISPs are not following best practices for customer verification processes.
2. ISPs are not ensuring that ALL their resellers are following sound customer verification practices.
3. Employees or owners of ISPs are directly benefiting from fraudulent sign-ups, i.e., knowingly taking money from miscreants in return for hosting their botnet C&Cs.

The larger the ISP, the larger the volumes of abuse. While it may seem obvious, it's important to remember that due to their increased hosting capabilities, the bigger ISPs and hosting providers have a higher volume of poorly patched servers and websites on their network.

Outdated software makes for an easy target

It is a simple task for a cybercriminal to scan the internet for servers or websites that are running outdated or vulnerable software. Some of the most popular open source content management systems (CMS) like WordPress, Joomla, Typo3 or Drupal are especially popular targets, due to the high number of poorly maintained installations of these packages.

Proxy nodes

Botnet operators do not only use hosting providers and anonymization services to host their botnet infrastructure. Spamhaus Malware Labs has also seen an increase of malware-infected machines (bots) that cybercriminals turn into a proxy node.

In doing so, these bots become a part of the botnet infrastructure and are used to relay botnet C&C communications from other infected machines to the real botnet controller. While this is not a new technique that has appeared in 2018, malware families like Qadars, Quakbot, and others have been using this approach for several years; we have observed a substantial increase of Heodo/Emotet infected machines that have become a part of the Heodo/Emotet botnet infrastructure.

It is worth noting that if you think that your internet connection is suddenly running more slowly than expected, then your computer could potentially be infected and be acting as a proxy for a botnet operation.

Total botnet C&C hosting numbers by ISP, including compromised websites, compromised servers and fraudulent sign-ups

Rank	C&Cs	Network	Country	% change
1	1,581	cloudflare.com	United States	+125%
2	629	alibaba-inc.com	China	+240%
3	507	ovh.com	France	+42%
4	483	simplecloud.ru	Russia	+2,741%
5	407	ispserver.com	Russia	+267%
6	338	reg.ru	Russia	+412%
7	319	timeweb.ru	Russia	+187%
8	287	mtw.ru	Russia	+101%
9	265	fos-vpn.org	Seychelles	—
10	262	colocrossing.com	United States	+264%
11	247	marosnet.ru	Russia	+1,444%
12	244	stajazk.ru	Russia	+495%
13	232	selectel.ru	Russia	–15%
14	222	m247.ro	Romania	+500%
15	201	spacenet.ru	Russia	+3,250%
16	200	leaseweb.com	Netherlands	+74%
17	172	endurance.com	United States	+251%
18	171	mchost.ru	Russia	+76%
19	171	itos.biz	Russia	+235%
20	171	hetzner.de	Germany	+131%

Botnet C&C hosting numbers by ISP, as a result of fraudulent sign-ups only (BCL)

Rank	C&Cs	Network	Country	% change
1	1,581	cloudflare.com	United States	+125%
2	626	alibaba-inc.com	China	+284%
3	476	simplecloud.ru	Russia	+3,073%
4	432	ovh.net	France	+89%
5	397	ispserver.com	Russia	+493%
6	357	reg.ru	Russia	+693%
7	280	mtw.ru	Russia	+264%
8	265	fos-vpn.org	Seychelles	—
9	257	timeweb.ru	Russia	+289%
10	244	stajazk.ru	Russia	+495%
11	233	colocrossing.com	United States	+276%
12	233	marosnet.ru	Russia	+1,453%
13	224	selectel.ru	Russia	–6%
14	219	m247.ro	Romania	+526%
15	194	spacenet.ru	Russia	+3,133%
16	171	itos.biz	Russia	+375%
17	160	leaseweb.com	Netherlands	+86%
18	158	mchost.ru	Russia	+95%
19	158	netangels.ru	Russia	—
20	156	greenvps.net	Russia	—

Cloudflare – the top botnet C&C hosting network: Cloudflare is a Content Delivery Network (CDN) provider from the US. While they do not directly host any content, they provide services to botnet operators, masking the actual location of the botnet controller and protecting it from DDoS attacks.

Many cybercriminals sign-up for Cloudflare's free plan with the sole purpose of using it exclusively for hosting a botnet C&C. Usually, such a listing would be placed on our BCL; however, because the hosting of the botnet C&C is on a Cloudflare shared IP address, it is placed on the SBL. In this extraordinary circumstance, we have chosen to list the same figures in both charts.

New entries: simplecloud.ru (BCL #3), ovh.net (BCL #4), reg.ru (BCL #6), fos-vpn.org (BCL #8), stajazk.ru (BCL #10), marosnet.ru (BCL #12), m247.ro (BCL #14), spacenet.ru (BCL #15), itos.biz (BCL #16), netangels.ru (BCL #19), greenvps.net (BCL #20) are all newcomers to our Top Twenty BCL rankings. It is interesting to note that out of these eleven ISPs with botnet C&Cs on their network as a result of fraudulent sign-ups, 73% are Russian based.

ISPs with only BCL listings: Newcomers greenvps.net and netangles.ru are the only networks that we have seen with botnet C&C listings on the BCL alone. We weren't able to find a single compromised server or website that was abused for botnet C&C hosting on any of these networks, signaling that all the sign-ups on these two networks were fraudulent.

Recurring entries: Unfortunately, with the exception of selectel.ru, all the ISPs listed on our 2018 Top Twenty BCL list saw a significant increase in the amount of botnet C&Cs on their networks as a result of fake registrations in 2019.

Departures: gerber-edv.net & anmaxx.net: We suspect both have been rebranded, and swiftway.net has disappeared. Meanwhile the following companies appear to be successfully trading, and therefore we assume have appropriately dealt with the botnet C&C abuse on their networks; iliad.fr, morene.host, neohost.com.ua, dataclub.biz, hostsailor.com, eksenbilisim.com.tr, digitalocean.com, choopa.com, melbicom.net, zare.com, and tencent.com.

Conclusion

East/West Divide: On reading this report the divide between East and West is obvious, with the East lagging behind the West, both in terms of robust sign-up procedures, and in enforcement focused on taking down cybercriminal activity. Criminals will always follow the path of least resistance, be that registering their domain with a Chinese registrar or using a Russian ISP, neither of which follow rigorous sign-up processes.

Emotet & Trickbot: Our researchers have noted a huge increase in the number of Emotet and TrickBot malspam campaigns and infections. Despite having a 'holiday'[6] in June, July and August, Emotet ramped up its activity towards the end of last year.[7] Emotet's behavior and characteristics are constantly changing to make it more and more dangerous.

DGA usage is dropping. This is good news, and illustrates that with a combined effort from the industry, positive changes can be made.

New botnet bulletproof hosting operator: We do have concerns in regard to the appearance of this operator. Worryingly, the set-up for cybercriminals is more cost-effective, less risky, and provides greater agility when compared with that of 'conventional' bulletproof hosting, making it easier for them to host all kinds of badness. It is crucial that hosting providers across the globe stop allowing customers to fraudulently sign up for services. Otherwise, the 16% increase in botnet C&Cs associated with fraudulent sign-ups in 2019 will continue to rise in 2020.

Compromised websites: We have seen a shift to cybercriminals using compromised website domain names for their botnet C&Cs, rather than buying their own domains. This adds complexity to take downs. Therefore, it is imperative that everyone who runs a website ensures theirs is secure.

Recommended precautionary actions

In such a rapidly changing environment a flexible and swift (if not automated) approach is required by those who protect networks and users. In addition to current security measures that are currently implemented, based on the botnet C&C threats observed in 2019, we recommend the additional following precautionary actions:

- Choose your internet infrastructure providers, e.g. registrars and ISPs, wisely. Picking providers with poor reputation can have serious consequences for business operations. 'Cheap' should rarely be a deciding factor in a business decision making process.
- Authentication logs should be monitored to determine what regular traffic looks like so when anomalies occur, they will be obvious. If possible, do not allow authentication to a network via multiple points to keep protection needs simple.
- To combat threats from botnet C&Cs utilizing dTLDs look to Border Gateway Protocol data feeds that automatically block connections to IP addresses associated with botnet C&Cs.
- To avoid websites being hacked by cybercriminals to host a botnet C&C, always ensure the installed CMS, such as WordPress or Typo3, including any installed 3rd party plugins, are up-to-date.
- When operating a server, ensure that the operating system (OS) is up to date and any installed software such as Apache2 or PHP is running with the latest security patches.
- Block access to cryptocurrency mining pools by default, and provide users who require access with the ability to 'opt-in.'
- Block traffic to anonymization services like Tor by default, and provide users who require access with the ability to 'opt-in.'
- Avoid your server being one of the many that are compromised on a daily basis as a result of brute force or stolen SSH passwords. Use SSH key authentication whenever possible or deploy two-factor authentication (2FA).

About Spamhaus

The Spamhaus Project is a non-profit organization dedicated to making the internet a better place for everyone. We have been producing industry leading threat intelligence datasets for over two decades. These datasets protect three billion end users against malicious activity including spam, malware and phishing.

As the internet continues to become ever more integrated in our day-to-day lives, so do the threats related to malicious activities. The process of identifying bad behaviors is constantly evolving, with cybercriminals rapidly developing new ways of targeting users.

Spamhaus works together with the wider internet community, including network operators to define what acceptable and appropriate behavior looks like online. We then shine a light on behavior that doesn't meet these policies. We identify and list internet infrastructure, for example an IP address, which is either currently exhibiting bad behavior or, based on our experience, is likely to do so. Our datasets are used to protect users from infrastructure which show malicious intent. Additionally, our data can provide users with deeper insights, enabling them to rapidly investigate and remediate incidents.

A broad community of organizations, network operators and individuals share their data with us to help improve the quality and reliability of our datasets. An experienced team of security researchers use heuristics, machine learning and manual investigations to carefully analyze, score and list infrastructure entities. Our community-led approach, impartiality and dedication has led us to become trusted by Internet Service Providers (ISPs), Email Service Providers (ESPs), enterprise business and law enforcement, among others.

References

1 https://www.europol.europa.eu/newsroom/news/international-crackdown-rat-spyware-which-takes-total-control-of-victims%E2%80%99-pcs].
2 https://66.schedule.icann.org/meetings/1116759
3 https://www.spamhaus.org/news/article/785/spamhaus-botnet-threat-update-q2-2019
4 https://www.spamhaus.org/news/article/792/bulletproof-hosting-theres-a-new-kid-in-town
5 https://www.spamhaus.org/news/article/792/bulletproof-hosting-theres-a-new-kid-in-town
6 https://www.spamhaus.org/news/article/789/spamhaus-botnet-threat-update-q3-2019
7 https://www.spamhaus.org/news/article/791/estimating-emotets-size-and-reach