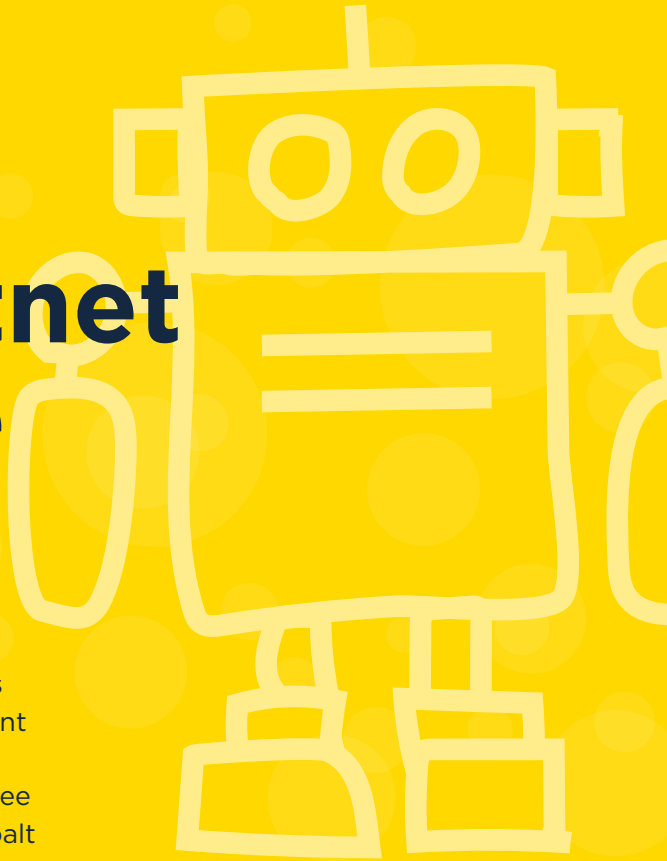
SPAMHAUS



Spamhaus Botnet Threat Update

Q3 2022

Well, Q3 was a busy quarter. There was no vacation for botnet C&Cs this year. With a 38% increase in botnet C&Cs detected by the research team, there was a lot of movement across all the charts with multiple new entries. There is a strong Chinese element felt throughout this report as we see a vast amount of botnet C&Cs out of China relating to Cobalt Strike – a legitimate penetration testing tool being used for nefarious purposes.

Welcome to the Spamhaus Botnet Threat Update Q3 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

Initial Access Brokers – are they selling access to your network?

Initial Access Brokers (IABs) have been one of the top threats over the past years. But what are they, and why are they so dangerous?

An explanation

The term “Initial Access Brokers” refers to threat actors who usually operate in groups, trying to breach corporate networks. They use various tactics, techniques, and procedures (TTPs) to achieve their goals.

Ways IABs operate

One of their preferred TTPs is to spread malware via opportunistic or targeted malspam campaigns. For this purpose, brokers either develop their own piece of malware or rent access to Malware-as-a-Service (MaaS) botnets. The list of malware families known to be used by such brokers is long: Emotet, IcedID, Dridex, Qakbot, and many more. One of the most recent emerging threats used by such brokers is BumbleBee. You can read more about the rise of BumbleBee in this update.

However, malware isn't the only way these IABs enter your corporate network. Another tactic is to exploit exposed software or devices connected to the internet. Brokers focus on known software vulnerabilities that potential victims have failed to patch (e.g., Microsoft Exchange Servers). Alternatively, they'll use brute force attacks where weak credentials are employed, e.g., for remote access.

And after they've breached your network...?

Initially, the broker will try to identify which network they have penetrated. Important information for the attackers to ascertain is the organization's country and sector along with its size, e.g., the number of employees & revenue.

Armed with a good understanding of the value attached to the "asset", the broker will then engage with potential buyers to see who wants to purchase access to the victim's network.

And then?

What happens from this point forwards wholly depends on the buyer. They may not use the access immediately. On the other hand, the buyer may immediately conduct reconnaissance and lateral movement as soon as they have access, which may lead to full encryption of the victim's network with ransomware within just a couple of hours.

How can you protect against IABs?

While this may sound scary, there are simple ways to protect yourself from this kind of threat.

1. Watch out for indicators of potential compromise on the network level and your endpoints.
2. Secure any remote access with multi-factor authentication (MFA).
3. Deploy critical security patches as soon as possible, once they are released.

This may sound like security 101, but breaches regularly occur because organizations do not follow these best common practices.

Number of botnet C&Cs observed, Q3 2022

In Q3 2022, Spamhaus identified 4,331 botnet C&Cs compared to 3,141 in Q2 2022. This was a 38% increase quarter on quarter. The monthly average increased from 1,047 in Q2 to 1,444 botnet C&Cs per month in Q3.

Quarter	No. of Botnets	Quarterly Average	% Change
Q4, 2021	3,271	1,090	+23%
Q1, 2022	3,538	1,179	+8%
Q2, 2022	3,141	1,047	-11%
Q3, 2022	4,331	1,444	+38%

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, Q3 2022

Botnet C&C boom in China

The number of newly observed botnet C&C servers in China went through the roof last quarter - we recorded a 3884% increase in botnet C&C activity in China. That's more than 900 additional botnet C&Cs than we saw in Q2. Most of the activity in this region was related to misuse of the legitimate penetration testing tool, Cobalt Strike.

Increase in botnet C&C activity in central Europe and North America

We saw an increase in botnet C&C activity across central Europe, including Switzerland (+126%), United Kingdom (+116%), Germany (+57%), France (+54%) and Netherlands (+36%). Meanwhile, the United States experienced a 140% increase in botnet C&Cs, and Canada was a new entry at #11.

Improvements across Eastern Europe

An interesting observation for Q3 is that overall, many Eastern European countries experienced a decrease in the numbers of botnet C&Cs, e.g., Bulgaria, Latvia, Moldova, Romania and Ukraine. As a result, these countries all departed from our quarterly ranking. Nice work!

Significant decrease in Russia

One surprise in Q3 was a significant decrease in the number of newly observed botnet C&Cs in Russia. The number fell by 891, from 1254 botnet C&Cs in Q2 to only 363 in Q3. That's reduced by almost three quarters (-71%).

Improvements continue across the LatAm region

With the exception of Brazil, the situation in LatAm countries continues to improve in Q3, as it has done since the beginning of the year. The Dominican Republic (-44%) and Mexico (-24%), both experienced a reduction in the number of botnet C&Cs. Let's hope they drop off the Top 20 in Q4, just as Uruguay did in Q2.

New entries

Singapore (#9), Canada (#11), Japan (#12), Republic of Korea (#13), Finland (#15), Lithuania (#16), India (#18), Czech Republic (#19).

Departures

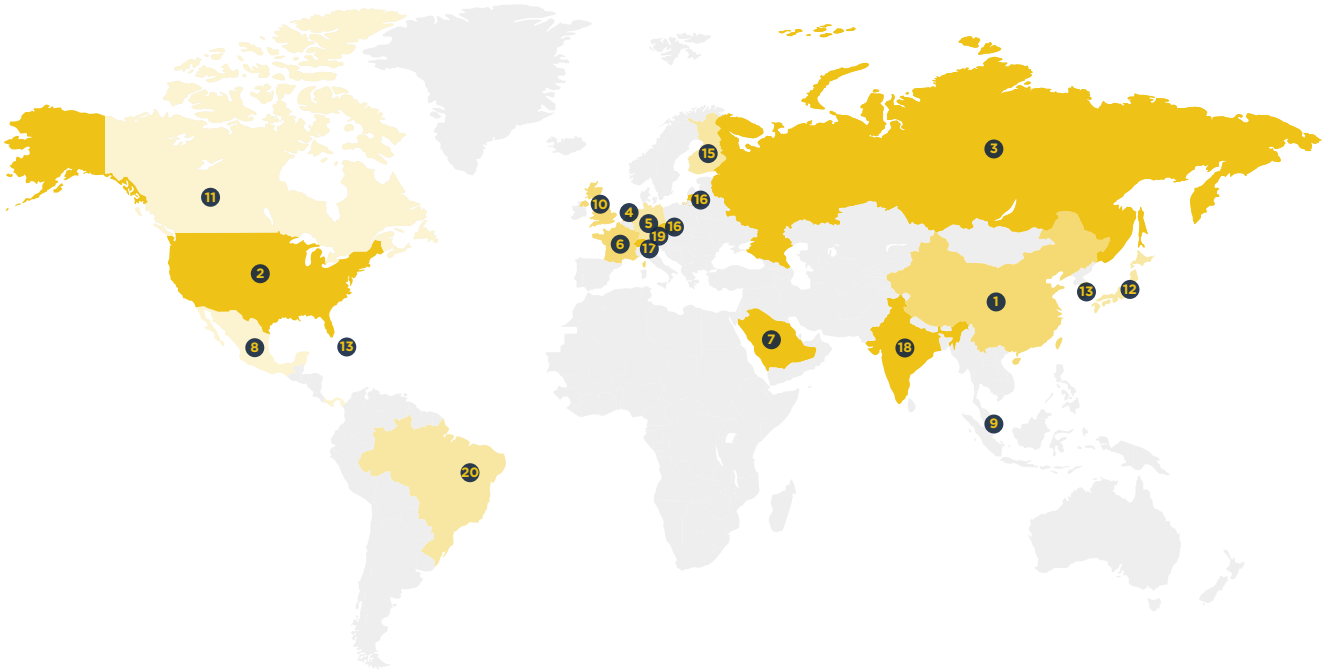
Bulgaria, Latvia, Moldova, Portugal, Romania, Ukraine, Arab Emirates, Uruguay.

Geolocation of botnet C&Cs, Q3 2022 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Q2 2022	Q3 2022	% Change Q on Q
#1	China	25	996	3884%
#2	United States	384	922	140%
#3	Russia	1254	363	-71%
#4	Netherlands	216	293	36%
#5	Germany	159	249	57%
#6	France	78	120	54%
#7	Saudi Arabia	205	110	-46%
#8	Mexico	137	104	-24
#9	Singapore	-	96	New Entry
#10	United Kingdom	31	67	116%

Rank	Country	Q2 2022	Q3 2022	% Change Q on Q
#11	Canada	-	52	New Entry
#12	Japan	-	50	New Entry
#13	Korea	-	48	New Entry
#13	Dominican Rep	85	48	-44%
#15	Finland	-	47	New Entry
#16	Lithuania	-	44	New Entry
#17	Switzerland	19	43	126%
#18	India	-	42	New Entry
#19	Czech Republic	-	33	New Entry
#20	Brazil	22	29	32%



Malware associated with botnet C&Cs, Q3 2022

Cobalt Strike strikes!

We have previously reported on Cobalt Strike - sadly, despite being a legitimate tool, Cobalt Strike is extensively used by threat actors with malicious intent, for example, to deploy ransomware. Last quarter, we identified almost 2,000 new Cobalt Strike botnet C&Cs, making it the most dominant threat in Q3.

What is Cobalt Strike?

Cobalt Strike is a legitimate commercial penetration testing tool that allows an attacker to deploy an "agent" on a victim's machine.

RedLineStealer C&Cs go through the roof

RedLineStealer has been present in our Top 20 for years. However, the number of newly observed C&Cs associated with RedLineStealer exploded in Q3 by 409%, from 77 to 392. RedLine is one of the most successful credential stealers, sold as Malware-as-a-Service (MaaS) on the dark web.

RATs and more RATs!

Remote Access Trojans (RATs) have always been very popular among threat actors - in Q3, they accounted for 35% of all botnet C&Cs. Increases occurred across almost all of the popular RATs that criminals are currently selling on the dark web, including DCRat with 521% (#10), NanoCore with 264% (#15) and Remcos with 200% (#10).

Hello, BumbleBee!

Heard about BumbleBee before? If not, keep reading! BumbleBee is a backdoor that provides threat actors access to the victim's machine. Like Emotet and IcedID, BumbleBee acts as an Initial Access Broker, selling access to compromised corporate networks on the dark web that often leads to ransomware. In Q3, BumbleBee eclipsed all its competitors, including Emotet. We suggest you keep a close eye on this threat over the coming months!

Malware associated with botnet C&Cs, Q3 2022 (continued)

Emotet

Since we've mentioned Emotet, we thought some readers might wonder if its appearance in the Top 20 means this malware is back up and running following its takedown in January 2021. The truth is that while our researchers are observing botnet C&Cs firing, we haven't seen Emotet activity for some time i.e., the house door may be open, but no one is home.

Flubot labeling

Although FluBot's activity decreased massively in the second half of 2022, we continue to see a high number of newly observed botnet C&Cs associated with it. As we've mentioned in previous updates, this is because Flubot is using a technique called "FastFlux" to host its botnet C&Cs. The same botnet infrastructure also serves as C&Cs for other malware families, such as TeamBot. To make our internal tracking of this threat easier, we continue to label the associated infrastructure as "FluBot."

New entries

Cobalt Strike (#1), Flubot (#3), Qakbot (#4), RecordBreaker (#5), Bumblebee (#6), Emotet (#7), NjRAT (#8), Tofsee (#13), Dridex (#16), NetWire (#18).

Departures

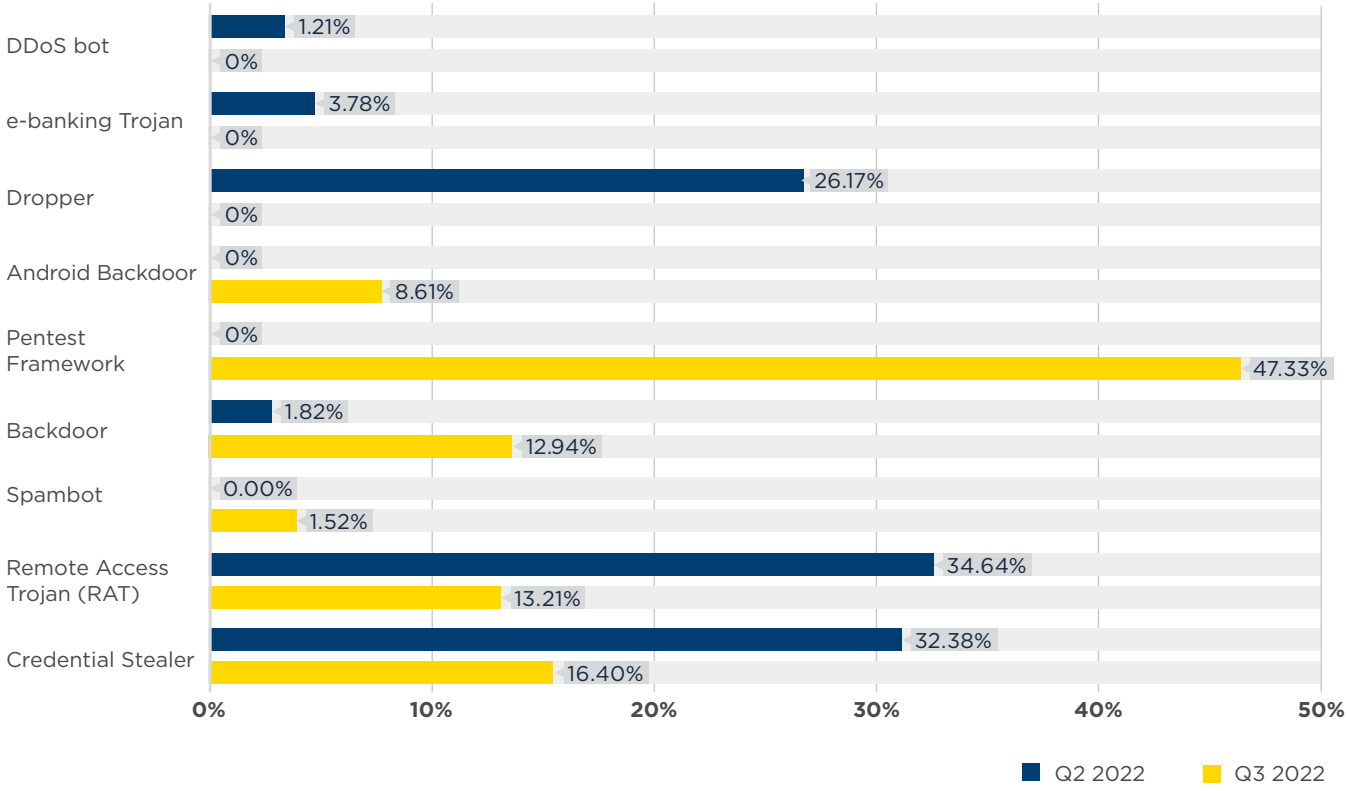
AZORult, DanaBot, Fodcha, Gozi, Matanbuchus, OrcusRAT, Quasar, Smoke Loader, STRRAT, SystemBC.

Malware associated with botnet C&Cs, Q3 2022 (continued)

Malware families associated with botnet C&Cs

Rank	Q2 2022	Q3 2022	% Change	Malware Family	Description
#1	-	1902	New Entry	Cobalt Strike	Pentest Tool
#2	77	392	409%	RedLineStealer	Credential Stealer
#3	-	346	New Entry	Flubot	Android Backdoor
#4	-	213	New Entry	Qakbot	Backdoor
#5	-	154	New Entry	RecordBreaker	Credential Stealer
#6	-	152	New Entry	Bumblebee	Backdoor
#7	-	112	New Entry	Emotet	Backdoor
#8	-	97	New Entry	NjRAT	Remote Access Trojan (RAT)
#9	71	89	25%	AsyncRAT	Remote Access Trojan (RAT)
#10	14	87	521%	DCRat	Remote Access Trojan (RAT)
#10	29	87	200%	Remcos	Remote Access Trojan (RAT)
#12	41	67	63%	AveMaria	Remote Access Trojan (RAT)
#13	-	61	New Entry	Tofsee	Spambot
#14	15	58	287%	Arkei	Credential Stealer
#15	14	51	264%	NanoCore	Remote Access Trojan (RAT)
#16	-	43	New Entry	Dridex	Backdoor
#17	99	35	-65%	Loki	Credential Stealer
#18	-	28	New Entry	NetWire	Remote Access Trojan (RAT)
#19	27	25	-7%	Vjw0rm	Remote Access Trojan (RAT)
#20	13	20	54%	Socelars	Credential Stealer

Malware type comparisons between Q2 2022 and Q3 2022



Most abused top-level domains, Q3 2022

Freenom continues to dominate our Top 20

While a few of the TLDs operated by Freenom improved over the last quarter, others had marked increases in the number of new botnet C&Cs associated with them. TLDs gq, tk, ga, ml, cf are all operated by Freenom and appear too frequently in the Top 20. Come on, Freenom – you can do better.

Increase in botnet C&Cs hosted on LatAm TLDs

When it comes to the LatAm region, both ccTLD .co (#13) and .br (#20) both experienced significant increases in botnet C&Cs associated with their TLDs in Q3.

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q3 2022, .com had more than 150 million domains, of which 0.001% were associated with botnet C&Cs. Meanwhile, .ga had approximately 6,500 domains, of which 3.263% 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, Q3 2022 (continued)

Working together with the industry for a safer internet

Naturally, our preference is for no TLDs to have botnet C&Cs linked 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 greatly appreciate the efforts of many registries who work with us to ensure these actions are taken.

New entries

.cyou (#11), .online (#14), .fun (#19), .br(#20).

Departures

.club, .eu, .live, .site

Top abused TLDs - number of domains

Rank	Q2 2022	Q3 2022	% Change	TLD	Note
#1	2133	1674	-22%	com	gTLD
#2	168	442	163%	ml	Originally ccTLD, now effectively gTLD
#3	228	244	7%	top	gTLD
#4	112	213	90%	ga	Originally ccTLD, now effectively gTLD
#5	218	181	-17%	cloud	gTLD
#6	171	139	-19%	tk	Originally ccTLD, now effectively gTLD
#7	121	134	11%	xyz	gTLD
#8	167	117	-30%	org	gTLD
#9	102	101	-1%	info	gTLD
#10	173	85	-51%	cf	Originally ccTLD, now effectively gTLD
#11	-	84	New Entry	cyou	gTLD
#11	76	84	11%	us	ccTLD
#13	38	78	105%	co	ccTLD
#14	-	73	New Entry	online	gTLD
#15	57	71	25%	net	gTLD
#16	31	59	90%	ru	ccTLD
#17	119	56	-53%	gq	ccTLD
#18	25	52	108%	shop	gTLD
#19	-	49	New Entry	fun	gTLD
#20	-	47	New Entry	br	ccTLD

Most abused domain registrars, Q3 2022

Kudos to Key Systems and PDR

The German-based domain registrar Key Systems and Indian-based PDR have both improved massively. PDR's numbers have dropped by 46%, and Key Systems has completely dropped off the Top 20. Other departures are CentralNic, dnspod.cn, Gransy, Launchpad, and OwnRegistrar. Well done to you all!

Russian domain registrars on the rise (again)

We have seen an increase in fraudulent domain registrations across Russian-based domain registrars, specially RegRU (+50%) and Ru-Center (new entry). We hope that the situation at these two registrars will improve in the coming quarter.

Ups and downs at NameSilo and Namecheap

The two North American domain registrars, NameSilo (CA) and Namecheap (US), continue to lead our quarterly ranking. While the number of newly observed botnet C&C domains registered through their services improved in Q2, the situation worsened in Q3 with an increase of 18% and 5%, respectively. We suspect (sadly) that both will continue to lead our ranking in Q4.

New entries

Name.com (#16), NameBright (#19), RU-Center (#20).

Departures

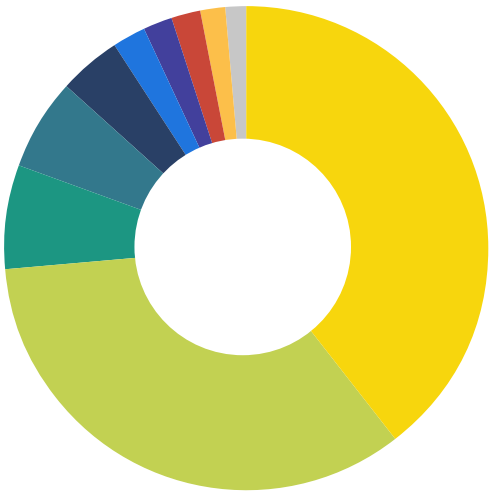
CentralNic, dnspod.cn, Gransy, Key Systems, Launchpad, OwnRegistrar.

Most abused domain registrars, Q3 2022 (continued)

Most abused domain registrars - number of domains

Rank	Q2 2022	Q3 2022	% Change	Registrar	Country
#1	797	937	18%	NameSilo	Canada
#2	615	644	5%	Namecheap	United States
#3	323	173	-46%	PDR	India
#4	187	166	-11%	Tucows	Canada
#5	128	105	-18%	Sav	United States
#6	128	103	-20%	Nicenic	China
#7	60	90	50%	RegRU	Russia
#8	48	62	29%	GMO	Japan
#8	65	62	-5%	Alibaba	China
#10	59	61	3%	Porkbun	United States
#11	26	58	123%	Hostinger	Lithuania
#12	28	55	96%	Gandi	France
#13	37	51	38%	Google	United States
#14	63	47	-25%	OpenProvider	Netherlands
#15	34	35	3%	OwnRegistrar	United States
#16	-	33	New entry	Name.com	United States
#17	35	32	-9%	EuroDNS	Luxembourg
#18	45	30	-33%	Todaynic	China
#19	-	26	New entry	NameBright	United States
#20	-	25	New entry	RU-Center	Russia

LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Q3 2022	Q2 2022
Canada	39.46%	33.98%
United States	34.17%	33.29%
China	6.98%	9.12%
India	6.19%	11.15%
Russia	4.11%	2.07%
Japan	2.22%	1.66%
Lithuania	2.08%	0.90%
France	1.97%	0.97%
Netherlands	1.68%	2.18%
Luxembourg	1.14%	1.21%
United Kingdom	-	1.45%
Czechia	-	1.14%
Germany	-	0.90%

Networks hosting the most newly observed botnet C&Cs, Q3 2022

There was even more movement than usual in Q3 among the Top 20 networks hosting the largest number of botnet C&Cs. With 15 new entries and departures, there's plenty to catch up on...

Does this list reflect how quickly networks deal with abuse?

While this Top 20 listing illustrates that there may be an issue with customer vetting processes at the named network, 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.

Chinese networks skyrocket to the top!

As mentioned earlier, the number of botnet C&Cs hosted in China soared in Q3! Two cloud hosting providers contributing to this increase were Tencent and Alibaba, taking the top two spots in our Top 20.

A disappointing reappearance from Hetzner

If you are one of our regular readers, Hetzner will undoubtedly ring bells. Many moons ago, Hetzner was a favorite among threat actors for hosting botnet C&Cs.

Thankfully, Hetzner managed to address these abuse problems and as a result didn't appear in our Top 20 for some time... until now. We are disappointed to see that Hetzner is evidently struggling with botnet C&C abuse; and we desperately hope this is just a "blip" and they can rapidly rectify these issues.

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.

Networks hosting the most newly observed botnet C&Cs, Q3 2022 (continued)

Threat actors love western cloud providers

Western cloud providers are cheap and reliable. Sadly, this results in their infrastructure being a favorite place for threat actors to host their botnet C&Cs.

Many western network brands appeared in last quarter's Top 20 including; Amazon (#3), DigitalOcean (#4), Hetzner (#6), OVH (#7), Microsoft (#13), Leaseweb (#14) and ColoCrossing (#17).

We believe these operators should set an example across the industry in preventing malicious customers from signing up to host botnet C&Cs on their networks.

Delis LLC - a new bulletproof hoster in town?

One of our newcomers in Q3 was the Dutch hosting provider delis.one. Their website address doesn't even serve up a functioning website, which immediately raises a red flag. Therefore, it will come as no surprise that they entered the Top 20 at #5. Have we sniffed out a new bulletproof hosting company? We are sure that time will reveal all.

New entries

tencent.com (#1), alibaba-inc.com (#2), amazon.com (#3), digitalocean.com (#4), delis.one (#5), hetzner.com (#6), choopa.com (#9), frantech.ca (#11), m247.ro (#12), microsoft.com (#13), leaseweb.com (#14), huawei.com (#15), colocrossing.com (#17), baidu.com (#18), lethost.co (#20)

Departures

antel.net.uy, baxet.ru, filanco.ru, gbnhost.com, ghostnet.de, google.com, hostsailor.com, hostwinds.com, invs.ru, macloud.ru, mivocloud.com, mobily.com.sa, pinvds.com, sprinthost.ru, timeweb.ru

Networks hosting the most newly observed botnet C&Cs, Q3 2022 (continued)

Newly observed botnet C&Cs per network

Rank	Q2 2022	Q3 2022	% Change	Network	Country
#1	-	509	New Entry	tencent.com	China
#2	-	248	New Entry	alibaba-inc.com	China
#3	-	197	New Entry	amazon.com	United States
#4	-	166	New Entry	digitalocean.com	United States
#5	-	134	New Entry	delis.one	Netherlands
#6	-	114	New Entry	hetzner.com	Germany
#7	62	112	81%	ovh.net	France
#8	137	99	-28%	uninet.net.mx	Mexico
#9	-	90	New Entry	choopa.com	United States
#10	145	81	-44%	stc.com.sa	Saudi Arabia
#11	-	65	New Entry	frantech.ca	Canada
#12	-	59	New Entry	m247.ro	Romania
#13	-	53	New Entry	microsoft.com	United States
#14	-	51	New Entry	leaseweb.com	Netherlands
#15	-	50	New Entry	huawei.com	China
#16	85	48	-44%	claro.com.do	Dominican Rep
#17	-	44	New Entry	colocrossing.com	United States
#18	-	41	New Entry	baidu.com	China
#19	152	39	-74%	vdsina.ru	Russia
#20	-	34	New Entry	lethost.co	Russia

Networks hosting the most active botnet C&Cs, Q3 2022

Finally, let's review the networks that hosted the largest number of active botnet C&Cs at the end of Q3 2022. Hosting providers in this ranking either have an abuse problem, do not take the appropriate action when receiving abuse reports, or omit to notify us when they have dealt with an abuse problem.

Chinese cloud providers leading this ranking (too)

Given the amount of newly observed botnet C&Cs hosted in China in Q3, it is not a big surprise that China is leading this ranking too. Tencent and Alibaba were hosting the most active botnet C&Cs by the end of Q3.

Good news for Microsoft and Cloudflare

We are delighted to see that the number of active botnet C&Cs has improved at both Microsoft (Azure) and Cloudflare. Both dramatically decreased botnet C&C numbers hosted on their services by -80% (Microsoft) and -58% (Cloudflare). Well done, and keep up the great work on dealing with abuse reports quickly and effectively!

New entries

tencent.com (#1), alibaba-inc.com (#2), digitalocean.com (#3), amazon.com (#4), frantech.ca (#7), hetzner.com (#8), choopa.com (#9), colocrossing.com (#10), huawei.com (#10), leaseweb.com (#10), baidu.com (#13), contabo.de (#15), hivelocity.net (#15), skbroadband.com (#17), 1ue.com (#19), combahton.net (#19).

Departures

a1.bg, alexhost.md, antel.net.uy, cableonda.net, claro.com.do, dotsi.pt, eliteteam.to, google.com, ielo.net, ipjetable.net, mobily.com.sa, stc.com.sa, telefonica.com.ar, telefonica.com.br, tie.cl, uninet.net.mx

Rank	Q2 2022	Q3 2022	% Change	Network	Country
#1	-	183	New Entry	tencent.com	China
#2	-	91	New Entry	alibaba-inc.com	China
#3	-	87	New Entry	digitalocean.com	United States
#4	-	85	New Entry	amazon.com	United States
#5	64	49	-23%	delis.one	Netherlands
#6	31	32	3%	ovh.net	France
#7	-	30	New Entry	frantech.ca	Canada
#8	-	24	New Entry	hetzner.com	Germany
#9	-	18	New Entry	choopa.com	United States
#10	-	17	New Entry	huawei.com	China
#10	-	17	New Entry	colocrossing.com	United States
#10	-	17	New Entry	leaseweb.com	Netherlands
#13	-	16	New Entry	baidu.com	China
#13	81	16	-80%	microsoft.com	United States
#15	-	15	New Entry	contabo.de	Germany
#15	-	15	New Entry	hivelocity.net	United States
#17	-	14	New Entry	skbroadband.com	South Korea
#17	33	14	-58%	cloudflare.com	United States
#19	-	13	New Entry	1ue.com	China
#19	-	13	New Entry	combahton.net	Germany

That's all for now. Stay safe and see you in January 2023!