

Spamhaus Botnet Threat Update



Q1 2023

The number of botnet command and control (C&C) servers continued to escalate in the first quarter of 2023 by +23%. Across Europe, activity increased, but as per the norm, the United States, China, and Russia led the way. In addition to Cobalt Strike and Qakbot contributing to the increase in numbers, there was a growing popularity in credential stealers, none more so than that of RecordBreaker, which experienced a massive 899% surge. Last but not least, there's disappointing news relating to active botnet C&Cs which remain persistent across various networks.

Welcome to the Spamhaus Botnet Threat Update Q1 2023.

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, 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.



Number of botnet C&Cs observed, Q1 2023

In Q1 2023, Spamhaus identified 8,358 botnet C&Cs compared to 6,775 in Q4 2022. This was a +23% increase quarter on quarter. The monthly average increased from 2,258 in Q4 to 2,786 botnet C&Cs per month in Q1 2023.

Quarter	No. of Botnets	Quarterly Average	% Change
Q2 2022	3,141	1,047	-11%
Q3 2022	4,331	1,444	+38%
Q4 2022	6,775	2,258	+56%
Q1 2023	8,358	2,786	+23%



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, Q1 2023

The U.S.A., China, and Russia remain the botnet superpowers

There was no change this quarter in the top three countries listed. While the U.S.A and China experienced minimal percentage changes, +8% and -4%, respectively, Russia witnessed a sizable 62% increase in botnet C&Cs. However, the award for the most significant growth in Q4 goes to Switzerland, with a whopping 169% surge.

Increases across Europe

Another quarter – another set of increases across Europe relating to botnet C&C activity. This quarter, every new Top 20 entry is based in Europe: Sweden (#17), Austria (#19), and Lithuania (#20).

Meanwhile, of the countries listed that suffered an uplift in botnet C&Cs this quarter, over 50% were based in Europe.

Is Saudi Arabia finally improving?

Since Q4 2021, Saudi Arabia has not only been in the Top 20, but in the Top 10 countries for hosting botnet C&Cs... until Q1 2023. With a -38% decrease, it has finally dropped out of the Top 10 to #14. Let's hope this trend continues, and it drops off the listings entirely.



New entries











Sweden (#17), Austria (#19) and Lithuania (#20).











Departures

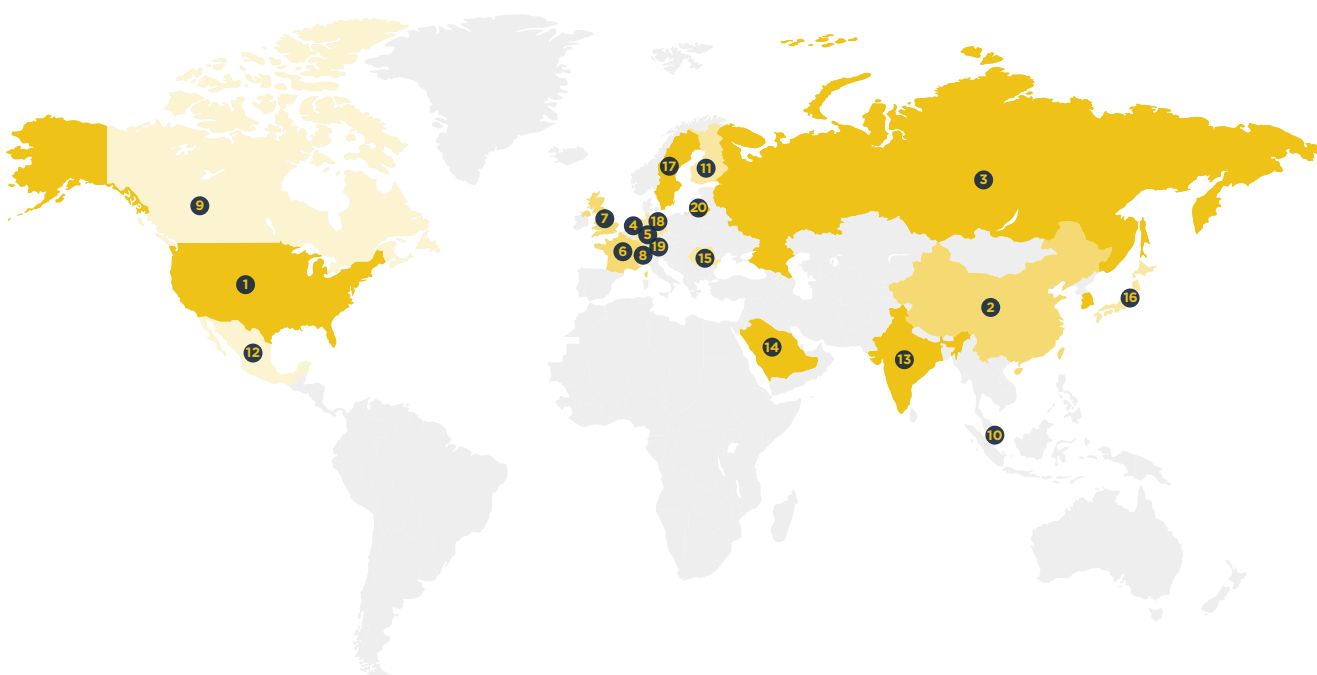
Korea (the Republic of), Spain, Venezuela (Bolivarian Republic of).

Geolocation of botnet C&Cs, Q1 2023 (continued)

Top 20 locations of botnet C&Cs

Rank	Country		Q4 2022	Q1 2023	% Change Q on Q
#1	United States		1713	1857	8%
#2	China		1033	993	-4%
#3	Russia		500	811	62%
#4	Netherlands		467	683	46%
#5	Germany		391	609	56%
#6	France		227	319	41%
#7	United Kingdom		165	249	51%
#8	Switzerland		61	164	169%
#9	Canada		148	154	4%
#10	Singapore		125	152	22%

Rank	Country		Q4 2022	Q1 2023	% Change Q on Q
#11	Finland		72	135	88%
#12	Mexico		140	127	-9%
#13	India		75	115	53%
#14	Saudi Arabia		182	113	-38%
#15	Bulgaria		77	109	42%
#16	Japan		67	101	51%
#17	Sweden		-	100	New entry
#18	Poland		71	92	30%
#19	Austria		-	70	New entry
#20	Lithuania		-	61	New entry



Malware associated with botnet C&Cs, Q1 2023

Cobalt Strike and Qakbot remain prevalent

In Q1, Cobalt Strike remained in the #1 spot for a third quarter. This malware was associated with 160% more botnet C&Cs than its closest rival, the backdoor [Initial Access Broker](#), Qakbot.

A surge in credential stealers

The number of botnet C&Cs associated with credential stealers amounted to only 5.79% of listings in Q4 2022; however, this quarter, that percentage rose to 22.47%.

One of the key contributors to this increase was RecordBreaker. This malware experienced a remarkable 899% rise in listings, jettisoning it from #15 in Q4 2022 to #3 in Q1 2023. Evidently, RecordBreaker is benefiting from the code boost it received in 2022.

Tofsee spambot - a consistent listing

Over the past few years, it's a rarity for Tofsee not to appear in the Top 20. This quarter we saw a slight reduction (-12%) in its number of listings, taking it from #12 to #18 this quarter.

To discover how to protect against this malware, read the blog posts recently published by our malware specialists focusing on two malware vaccines and a network-based kill switch:

1. [Binary file vaccine](#)
2. [InMemoryConfig store vaccine](#)
3. [Network-based kill switch](#)

FluBot labeling

FluBot continues to decrease (-13%) its activity in 2023; however, our researchers are still observing it as the sixth most popular threat associated with botnet C&Cs. As we've mentioned in previous updates, Flubot is using a "FastFlux" technique 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."



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.

Sadly, it is extensively used by threat actors with malicious intent, for example, to deploy ransomware.



New entries

IcedID (#7), Sliver (#8), ISFB (#10), Rhadamanthys (#13), Aurora Stealer (#15), Vidar (#16).

Departures

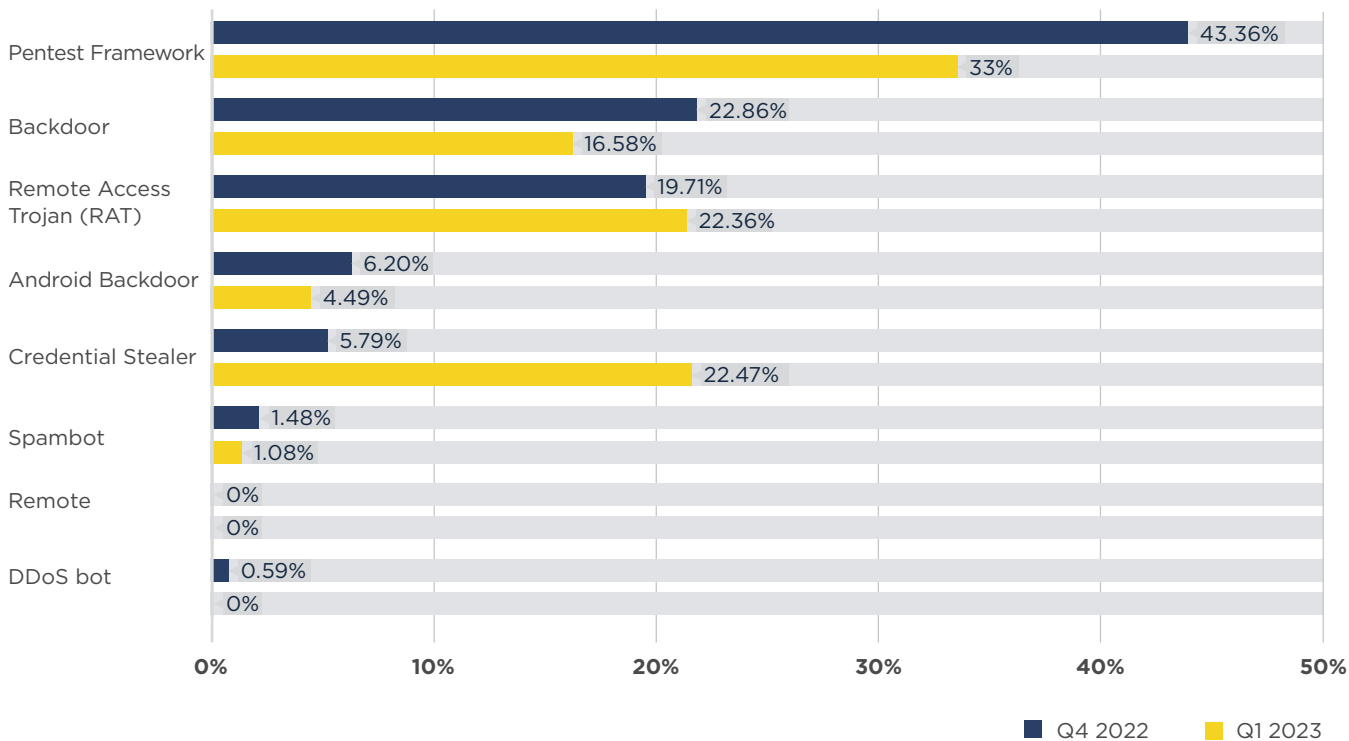
Arkei, Dridex, Loki, NanoCore, RecordStealer, VjwOrm.

Malware associated with botnet C&Cs, Q1 2023 (continued)

Malware families associated with botnet C&Cs

Rank	Q4 2022	Q1 2023	% Change	Malware Family	Description
#1	2657	2182	-18%	Cobalt Strike	Pentest Framework
#2	1020	969	-5%	Qakbot	Backdoor
#3	89	889	899%	RecordBreaker	Credential Stealer
#4	497	417	-16%	RedLineStealer	Remote Access Trojan (RAT)
#5	90	380	322%	AsyncRAT	Remote Access Trojan (RAT)
#6	380	332	-13%	Flubot	Android Backdoor
#7	-	321	New entry	IcedID	Credential Stealer
#8	-	256	New entry	Sliver	Pentest Framework
#9	89	254	185%	Remcos	Remote Access Trojan (RAT)
#10	-	194	New entry	ISFB	Remote Access Trojan (RAT)
#11	121	185	53%	DCRat	Remote Access Trojan (RAT)
#12	245	175	-29%	Bumblebee	Backdoor
#13	-	168	New entry	Rhadamanthys	Credential Stealer
#14	177	155	-12%	NjRAT	Remote Access Trojan (RAT)
#15	-	143	New entry	Aurora Stealer	Credential Stealer
#16	-	83	New entry	Vidar	Credential Stealer
#17	100	81	-19%	Emotet	Backdoor
#18	91	80	-12%	Tofsee	Spambot
#19	120	67	-44%	AveMaria	Remote Access Trojan (RAT)
#20	47	56	19%	Amadey	Credential Stealer

Malware type comparisons between Q4 2022 and Q1 2023



Most abused top-level domains, Q1 2023

Freenom's troubles equate to a positive change

At the end of last year, we reported that some of the Freenom TLDs (.ga & .ml) were experiencing significant reductions in the number of associated botnet C&C registrations. This quarter all of Freenom's TLDs (.cf, .ga, .gq, .ml, .tk) have dropped out of the Top 20.

We'd love to say that's because they started to take abuse on their TLDs seriously, but given their history, we know that's extremely unlikely. Instead, the truth lies in the legal actions taken by a social giant...

In March of this year, [Freenom was sued by Meta, alleging cybersquatting violations and trademark infringement](#), and for some time, the registry hasn't been accepting new domain registrations.

As we have always stated, botnet operators look for the path of least resistance – where infrastructure is cheap, or ideally free, and registration processes devoid of verification. We're delighted to see these TLDs dropping off our rankings.

The question is, "Who are those miscreants now turning to for botnet C&C domain registrations?"

Unbelievable increases

Both .us, the ccTLD run by Registry Services LLC, and .me, the one-time ccTLD now run as a gTLD by DoME n.d.o.o, have experienced some of the highest percentage increases quarter-on-quarter that we've witnessed since we began compiling the Botnet Update. In Q1 2023, .us experienced a +1,569% increase, and .me a +1,497% increase!!!

Is this just a coincidence that following Freenom's "freeze" on new domain registrations, we see other registries experience unprecedented increases in domains associated with botnet C&Cs?

We urge both registries to review their registration processes and that of their affiliated registrars.



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.

Most abused top-level domains, Q1 2023 (continued)

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q1 2023, **.net** had more than 13m domains, of which 0.001% were associated with botnet C&Cs. Meanwhile, **.us** had approximately 220k domains, of which 0.393% 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.

Working together with the industry for a safer internet

Naturally, we prefer 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

site (#6), website (#10), space (#13), one (#13), click (#16), cn (#17), cyou (#18), fun (#19).

Departures

br, cf, cfd, de, ga, gq, ml, tk.

Most abused top-level domains, Q1 2023 (continued)

Top abused TLDs - number of domains

Rank	Q4 2022	Q1 2023	% Change	TLD	Note
#1	2184	2736	25%	com	gTLD
#2	190	1094	476%	top	gTLD
#3	52	868	1569%	us	ccTLD
#4	152	541	256%	ru	ccTLD
#5	29	463	1497%	me	Originally ccTLD, now effectively gTLD
#6	-	318	New entry	site	gTLD
#7	46	252	448%	online	gTLD
#8	114	242	112%	org	gTLD
#9	68	174	156%	net	gTLD
#10	-	162	New entry	website	gTLD
#11	37	145	292%	info	gTLD
#12	84	131	56%	shop	gTLD
#13	-	104	New entry	space	gTLD
#13	-	104	New entry	one	gTLD
#15	220	103	-53%	xyz	gTLD
#16	-	92	New entry	click	gTLD
#17	-	90	New entry	cn	ccTLD
#18	-	76	New entry	cyou	gTLD
#19	-	73	New entry	fun	gTLD
#20	160	69	-57%	cloud	gTLD

Most abused domain registrars, Q1 2023

NameSilo is back in pole position

After briefly being knocked off its top spot at the end of last year by Tucows, NameSilo is back to its #1 position (sadly). In Q1, it saw a 409% growth in the number of fraudulent domain registrations for botnet C&Cs, compared to the previous quarter.

We guess that the only good news for NameSilo in this data is the fact that its percentage increase was surpassed by three other registrars: West263 (1448%), Google (723%) and Hostinger (411%).

Nice work Tucows

As touched on above, Tucows had a dreadful time regarding the number of botnet C&C registrations at the end of last year, with 597 in Q4 2022. We're delighted to report that at the end of Q1 2023, these numbers had reduced by 75% taking them to 149, dropping them down the Top 20 from #1 to #11.

Keep on slashing those numbers Tucows.



New entries

OwnRegistrar (#8), Xin (#12), R01 (#15).

Departures

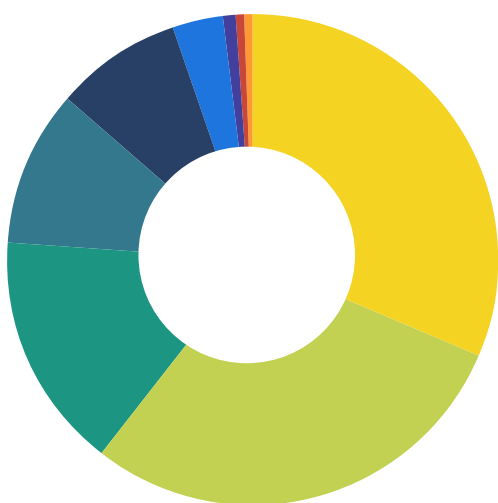
Gransy, InterNetworX, Todaynic.

Most abused domain registrars, Q1 2023 (continued)

Most abused domain registrars - number of domains

Rank	Q4 2022	Q1 2023	% Change	Registrar	Country
#1	414	2109	409%	NameSilo	Canada
#2	554	1152	108%	Namecheap	United States
#3	190	626	229%	RegRU	Russia
#4	168	613	265%	PDR	India
#5	31	480	1448%	West263	China
#6	48	395	723%	Google	United States
#7	75	375	400%	Nicenic	China
#8	-	297	New entry	OwnRegistrar	United States
#9	46	235	411%	Hostinger	Lithuania
#10	103	165	60%	Sav	United States
#11	597	149	-75%	Tucows	Canada
#12	-	108	New entry	Xin	China
#13	100	91	-9%	Alibaba	China
#14	56	74	32%	Porkbun	United States
#15	-	55	New entry	RO1	Russia
#16	23	48	109%	Name.com	China
#17	23	46	100%	RU-Center	Russia
#18	57	45	-21%	GMO	Japan
#19	42	43	2%	Gandi	France
#20	49	36	-27%	Openprovider	Netherlands

LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Q1 2023	Q4 2022
Canada	31.62%	37.07%
United States	29.17%	28.75%
China	15.43%	8.58%
Russia	10.18%	7.81%
India	8.58%	6.16%
Lithuania	3.29%	1.69%
Japan	0.63%	2.09%
France	0.60%	1.54%
Netherlands	0.50%	1.80%

Networks hosting the most newly observed botnet C&Cs, Q1 2023

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 that 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.

No sooner do they leave than they return

Unfortunately, having departed from the Top 20 in Q4 2022, m247.com (alternatively known as m247.ro) and colocrossing.com have returned to #12 and #20, respectively.



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 verification/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.



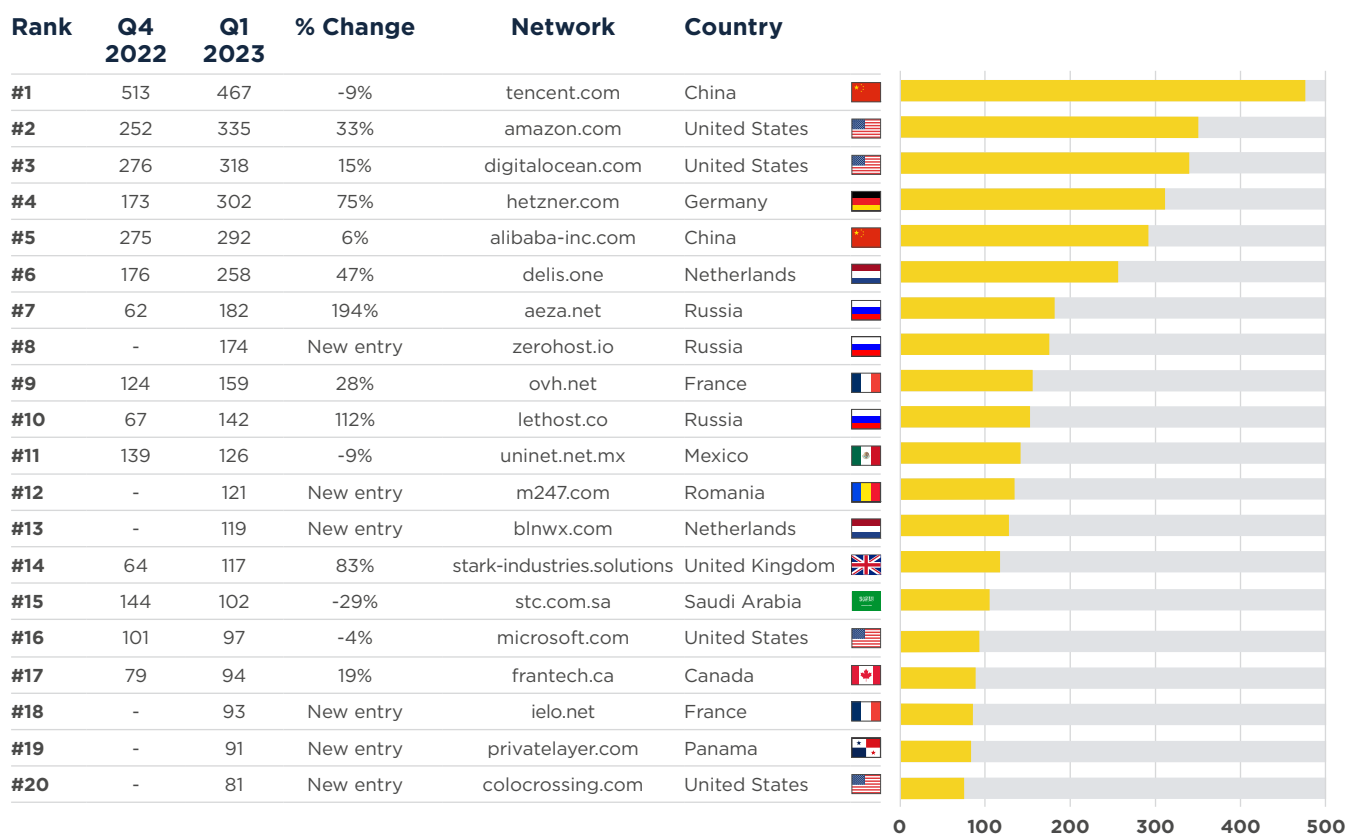
New entries

zerohost.io (#8), m247.com (#12), blnwx.com (#13), ielo.net (#18), privatelayer.com (#19), colocrossing.com (#20).

Departures

baxet.ru, charter.com, choopa.com, cloudflare.com, leaseweb.com pangintl.com.

Networks hosting the most newly observed botnet C&Cs, Q1 2023 (continued)



Networks hosting the most active botnet C&Cs, Q1 2023

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs at the end of Q1 2023. 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.

Let's start with the good news

We want to congratulate all those operators who have addressed those botnet C&C servers that have been persistent on their networks; baidu.com, comcast.net, google.com, huawei.com, ispserver.com, and skybroadband.com. Excellent work!

But what is going on elsewhere in the industry?

At the end of last year, we announced how impressed we were with the majority of network operators who were cleaning up their operations of active botnet C&Cs. This was particularly notable given that this period included Black Friday and the Holiday Season - notorious times for online abuse.

BUT, in the first quarter of this year - except for tencent.com, which decreased the number of botnet C&Cs it hosted by -12% - every previously listed network has experienced increases. In fact, 7 out of the 13 operators we're referring to doubled, and one tripled, the number of active botnet controllers on their networks.



New entries

zerohost.io (#6), blnwx.com (#12), constant.com (#12), m247.com (#14), contabo.de (#19), linode.com (#19).

Departures

baidu.com, comcast.net, google.com, huawei.com, ispserver.com, skybroadband.com.

Networks hosting the most active botnet C&Cs, Q1 2023 (continued)

What has happened?

Did your abuse teams not come back from their vacation, or considering the current economic climate, are cuts being made to these teams? Alternatively, in the scramble for a quick buck, are verification methods at the sales end of the process being relaxed, allowing the dross to swarm in? Although, if the latter were the case, we would expect significant increases in newly observed botnet C&Cs.

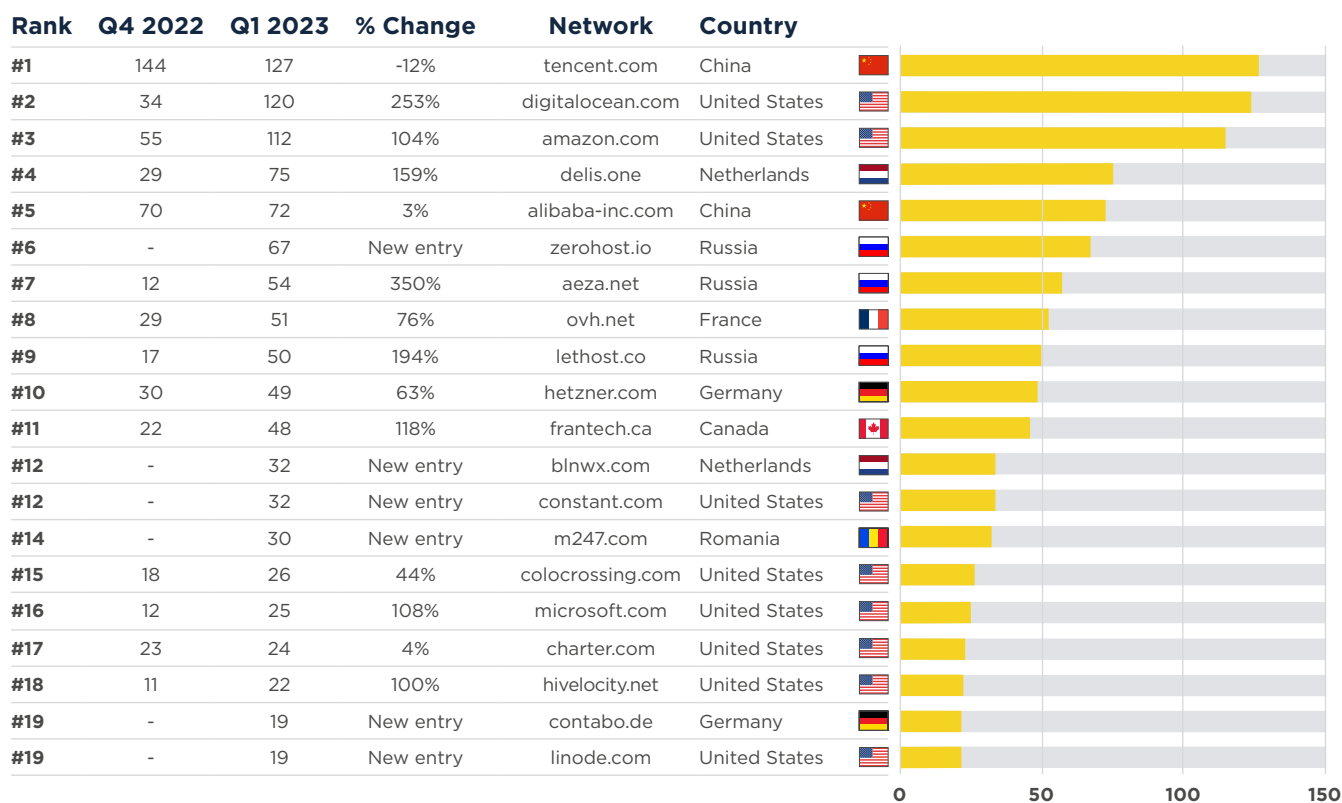
We'd like to hear from you.

We'd like to understand the challenges of dealing with this abuse:

- aeza.net (+350%)
- digitalocean.com (+253%)
- lethost.co (+194%)
- delis.one (+159%)
- frantech.ca (+118%)
- microsoft.com (+108%)
- amazon.com (+104%)
- hivelocity.net (+100%)
- ovh.net (+76%)
- hetzner.com (+63%)
- colocrossing.com (+44%)
- charter.com (+4%)
- alibaba-inc.com (+3%)

Networks hosting the most active botnet C&Cs, Q1 2023 (continued)

Total number of active botnet C&Cs per network



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