

Spamhaus Botnet Threat Update



January to June 2024

Overall, botnet command and control (C&C) activity decreased slightly between January and June this year by -6%. Misuse of the penetration testing framework Cobalt Strike also declined by -41%. Meanwhile, the popularity of android backdoors were on the rise, with new entries from Hook and Coper.

One of the most positive developments was that three well-known global network operators have taken action to address active botnet C&Cs.

Welcome to the Spamhaus Botnet Threat Update.

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, Jan-Jun 2024

Over the last six months, Spamhaus identified 14,248 botnet C&Cs, compared to 15,226 in the previous six months. This represents a -6% decrease. From July to December 2023, the monthly average was 2,538 botnet C&Cs; this decreased to 2,375 from January to June 2024.

Period	No. of Botnets	6 Month Average	% Change
Jul - Dec 2023	15,226	2,538	-9%
Jan - Jun 2024	14,248	2,375	-6%



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, Jan-Jun 2024

Improvements for China

...but this improvement is far from enough. Despite a -24% decrease in botnet C&C activity between January and June 2024, China was still hosting more botnet C&Cs (2,823) than any other country. Nevertheless, let's hope this downtrend continues.

Decreases across the globe

Most regions, including the aforementioned China (-24%), experienced a decrease in the number of botnet C&Cs, with the exception of Bulgaria (+162%), Sweden (+52%), Mexico (+33%) and Russia (+24%). Meanwhile, India, Poland and Switzerland departed from the Top 20.

What's happening in Bulgaria?

After reporting a +227% increase in Q4 2023, Bulgaria shows no signs of curtailing this malicious activity. The number of botnet C&Cs hosted in the country continued to increase, reaching 715, placing them at #6 in this Top 20.

Highs and lows for Latin America

New entrants Argentina and Colombia joined the Top 20 rankings at #13 and #16, respectively. Meanwhile, Mexico advanced five places to #7, with a +33% increase, reaching 497 botnet C&Cs. However, there is some positive news: Uruguay dropped to #19 with a respectable -64% decrease, from 330 to 118.



New entries

Argentina (#13), Vietnam (#14), Colombia (#16).









Departures

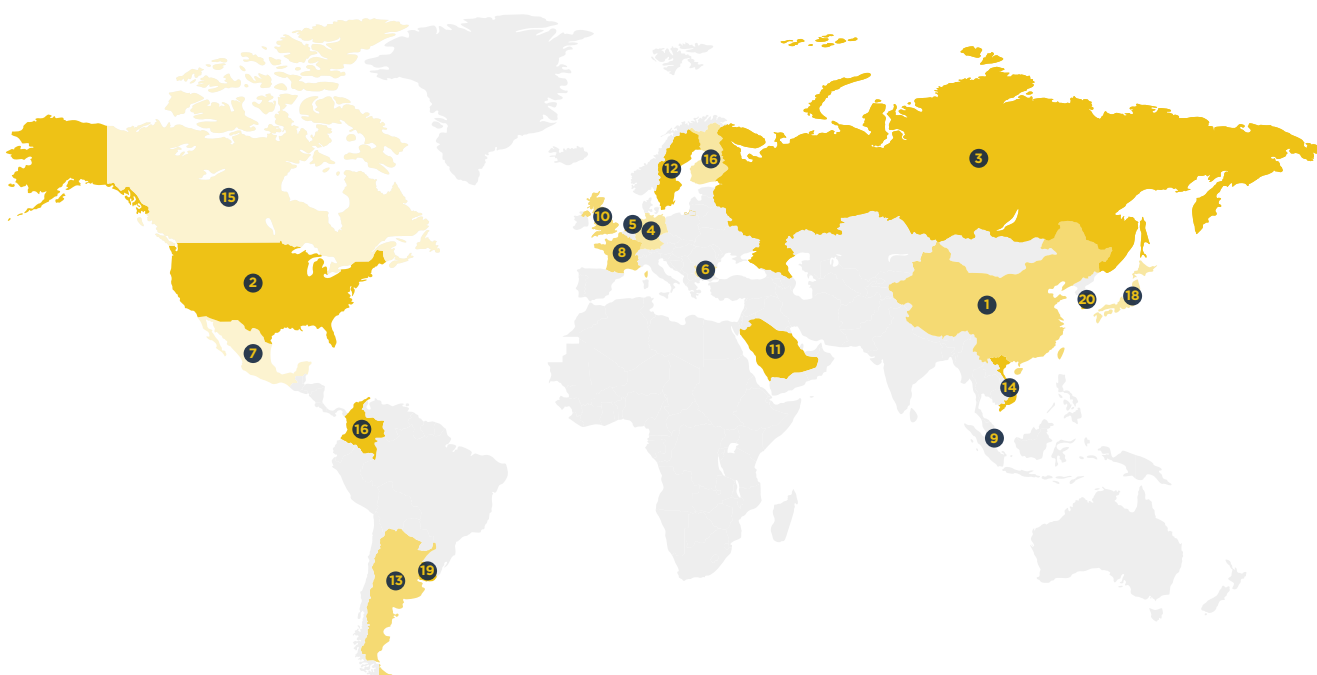
India, Poland, Switzerland.

Geolocation of botnet C&Cs, Jan-Jun 2024 (continued)

Top 20 locations of botnet C&Cs

Rank	Country		Jul - Dec 2023	Jan - Jun 2024	% Change
#1	China		3,695	2,823	-24%
#2	United States		2,873	2,702	-6%
#3	Russia		1,053	1,302	24%
#4	Germany		856	742	-13%
#5	Netherlands		1,145	737	-36%
#6	Bulgaria		273	715	162%
#7	Mexico		373	497	33%
#8	France		564	386	-32%
#9	Singapore		354	332	-6%
#10	United Kingdom		396	286	-28%

Rank	Country		Jul - Dec 2023	Jan - Jun 2024	% Change
#11	Saudi Arabia		312	246	-21%
#12	Sweden		149	226	52%
#13	Argentina		-	223	New entry
#14	Vietnam		-	149	New entry
#15	Canada		249	144	-42%
#16	Finland		180	135	-25%
#16	Colombia		-	135	New entry
#18	Japan		181	128	-29%
#19	Uruguay		330	118	-64%
#20	Korea (Rep. of)		147	107	-27%



Malware associated with botnet C&Cs, Jan-Jun 2024

Cobalt Strike

While the number of botnet C&Cs associated with Cobalt Strike decreased by -41%, this malware remained in the #1 spot for another six months. Furthermore, it was associated with 93% more botnet C&Cs than its closest contender, Flubot, at #2.

Is Flubot not dead?

As we've discussed in previous publications, FluBot uses 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 easier, we continue to label the associated infrastructure as FluBot, but this is effectively hosting all kinds of other botnet C&C badness.

RATs are on the rise

Remote Access Trojans (RATs), accounting for 28.53% of malware, were the second most popular type associated with botnet C&C servers. This malware type is designed to enable attackers to control an infected computer remotely. Once the RAT is operating, the attacker can send commands to the compromised system to receive data in response. The most prevalent RAT this reporting period was DCRat, which saw a +72% increase between January and June 2024.

Android backdoors increase in popularity

The number of botnet C&Cs associated with android backdoors amounted to only 8.58% between July and December 2023; however, over the last six months that percentage rose to 20.01%. This is partially due to new entrants Hook (#7) and Coper (#19), but is predominantly comprised of Flubot associated infrastructure.

Endgame for IcedID and Pikabot

This May we saw "[Operation Endgame](#)" and the takedown of several botnets, including IcedID and Pikabot. Therefore, it will come as no surprise to see these malware families drop out of the Top 20 malware associated with botnet C&Cs this reporting period. Great to see onward impact from this global operation!



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

Hook (#7), Mirai (#8), Latrodectus (#13), BianLian (#14), RisePro (#16), Coper (#19), Bashlite (#20).

Departures

IcedID, ISFB, Meterpreter, Pikabot, RecordBreaker, Stealc, Tofsee.

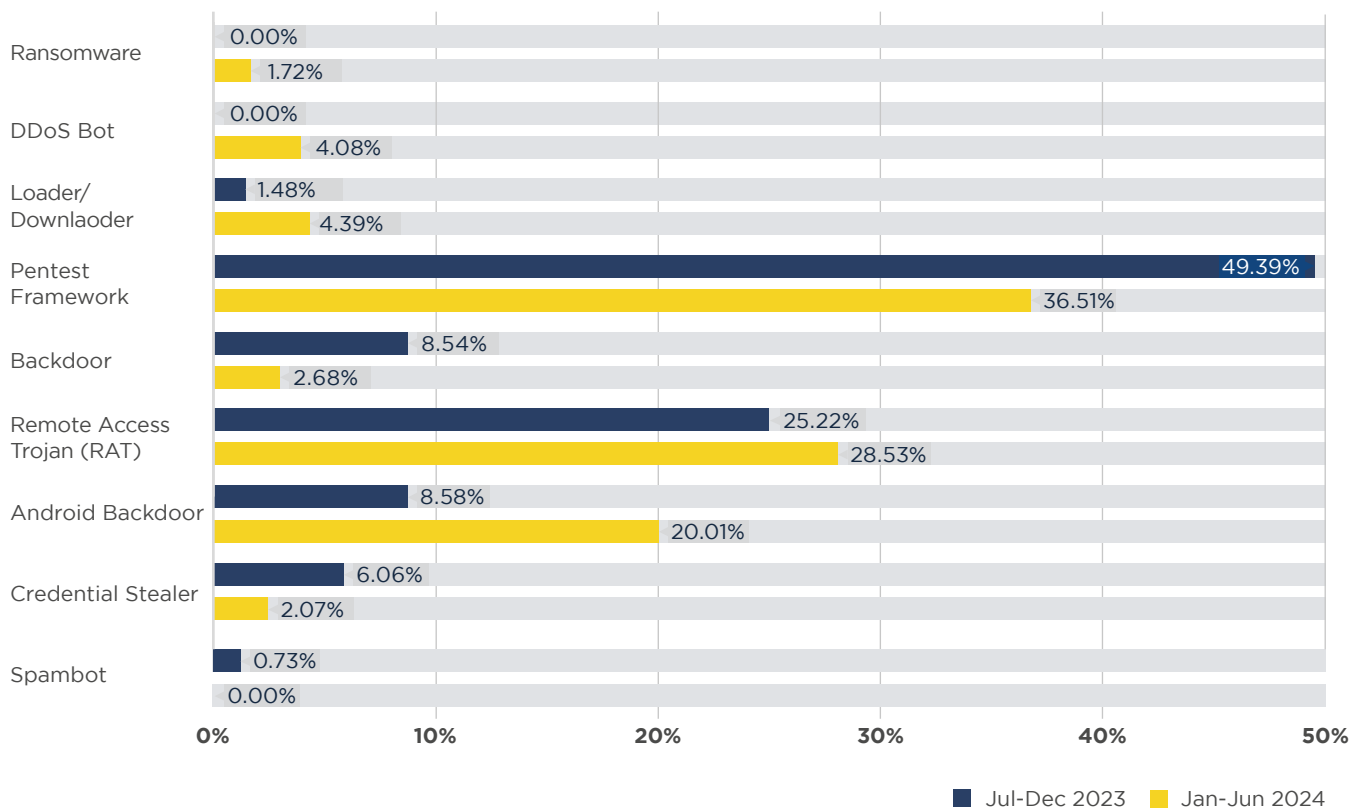
Malware associated with botnet C&Cs, Jan-Jun 2024 (continued)

Malware families associated with botnet C&Cs

Rank	Jul - Dec 2023	Jan - Jun 2024	% Change	Malware Family	Description	
#1	5,628	3,348	-41%	Cobalt Strike	Pentest Framework	
#2	1,159	1,727	49%	Flubot	Android Backdoor	
#3	1,083	1,020	-6%	AsyncRAT	Remote Access Trojan (RAT)	
#4	426	733	72%	DCRat	Remote Access Trojan (RAT)	
#5	670	729	9%	Remcos	Remote Access Trojan (RAT)	
#6	800	665	-17%	Sliver	Pentest Framework	
#7	-	470	New entry	Hook	Android Backdoor	
#8	-	379	New entry	Mirai	DDoS Bot	
#9	406	374	-8%	QuasarRAT	Remote Access Trojan (RAT)	
#10	942	307	-67%	Qakbot	Backdoor	
#11	200	301	51%	FakeUpdates	Loader/Downloader	
#12	559	280	-50%	RedLineStealer	Remote Access Trojan (RAT)	
#13	-	201	New entry	Latrodectus	Loader/Downloader	
#14	-	197	New entry	BianLian	Ransomware	
#15	140	163	16%	Havoc	Pentest Framework	
#16	-	134	New entry	RisePro	Credential Stealer	
#17	167	128	-23%	NjRAT	Remote Access Trojan (RAT)	
#18	98	103	5%	Rhadamanthys	Credential Stealer	
#19	-	92	New entry	Coper	Android Backdoor	
#20	-	88	New entry	Bashlite	DDoS Bot	

0 1000 2000 3000 4000

Malware type comparisons



Most abused top-level domains, Jan-Jun 2024

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, between January and June 2024, **.com** had more than 155m domains, of which 0.00129% were associated with botnet C&Cs. Meanwhile, **.sbs** had approximately 721k domains, of which 0.03172% were associated with botnet C&Cs. Both are in the top five of our listings. Still, one had a much higher percentage of domains related to botnet C&Cs than the other.

.sbs in at #5

After a fleeting visit in Q3 2023, generic top-level domain (gTLD), **.sbs**, owned by Shortdot, shot back into the Top 20 at #5 with a +252% increase. With [prices starting as low as \\$0.90](#) (at the time of writing), it's no surprise this gTLD is a botnet hotbed. Clearly, this TLD is still not living up to its value proposition "where people cultivate unbiased mindsets" and "public interest agendas meet meaningful actions."

Increases for .online

Having re-entered the charts in Q4 2023, Radix-owned gTLD, **.online**, increased by +280% between January and June 2024, ranking #2 in the Top 20 most abused top-level domains. Another TLD owned by the same registry, **.store**, also entered the Top 20 this period at #4, with 232 newly registered botnet C&C domains observed on it.

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.



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.



New entries

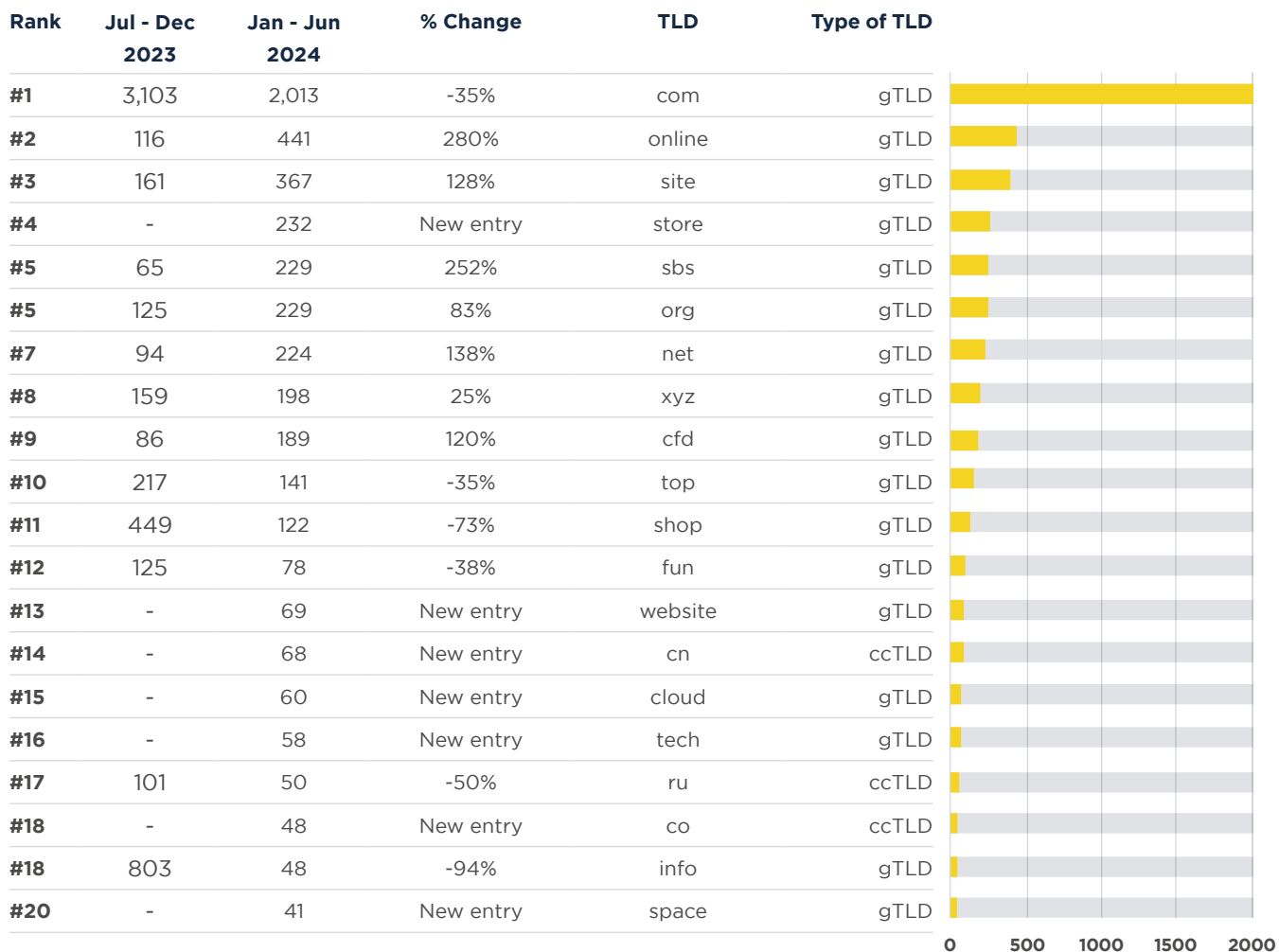
store (#4), website (#13), cn (#14), cloud (#15), tech (#16), co (#18), space (#20).

Departures

beauty, best, buzz, hair, makeup, pw, rest.

Most abused top-level domains, Jan-Jun 2024 (continued)

Top abused TLDs - number of domains



Most abused domain registrars, Jan-Jun 2024

Namecheap #1

Despite spending years in the top five, US-based Namecheap finally took the number one position, with a disappointing +89% increase. Meanwhile, NameSilo improved massively, with a -75% reduction dropping to #5 for the first time ever.

US domain registrars dominate the Top 10

We have seen an increase in new entrants and the overall number of domain registrations across US-based domain registrars in the Top 10, including: GoDaddy (+250%), Namecheap (+89%), Dynadot Inc. (new entry), and Spaceship Inc. (new entry). We hope that the situation in this region will improve before the next report publication.

Huge increases at Hostinger

We have observed an enormous +564% increase of newly registered botnet C&C domains at the Lithuanian-based registrar, Hostinger, rising from 80 between July December 2023, to 531 between January and June 2024. Now ranking #2 in the Top 20, we hope this domain registrar can stop this increase in malicious domain registrations, and fast.

Tucows' downward trend turns

After 12 months of reductions in the number of botnet C&C operators registering through them, Tucows experienced an +11% increase during this period. Sadly, this placed Tucows straight back in the Top 10.

Sav getting savvy to abuse?

In Q2 2023, we reported issues we were seeing at US-based registrar, Sav. However, we're pleased to share that the number of botnet C&C domains registered with Sav has reduced by an impressive -83%. Great work Sav, long may the decreases continue!



New entries

Spaceship, Inc. (#6),
Dynadot Inc (#7),
GMO (#11), WebNic.cc (#12),
Squarespace Domains (#14),
eNom (#15), Hosting Concepts (#16),
Network Solutions, LLC (#19).

Departures

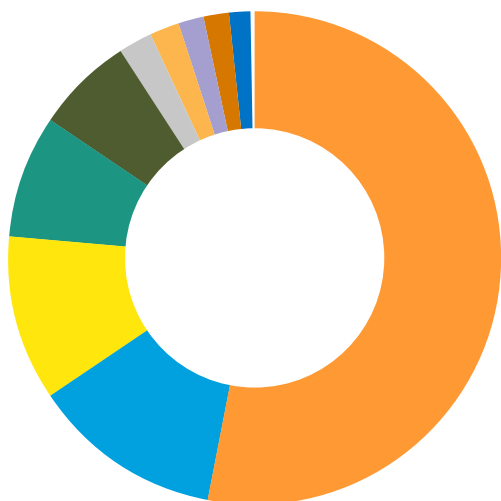
Cloudflare,
CommuniGal Communication Ltd,
Danesco Trading Ltd,
Hosting Concepts B.V., Name.com,
PSI, RU-Center, Xin Net.

Most abused domain registrars, Jan-Jun 2024 (continued)

Most abused domain registrars - number of domains

Rank	Jul - Dec 2023	Jan - Jun 2024	% Change	Registrar	Country
#1	544	1,027	89%	Namecheap	United States
#2	80	531	564%	Hostinger	Lithuania
#3	149	521	250%	GoDaddy.com	United States
#4	721	394	-45%	PDR	India
#5	1,540	379	-75%	NameSilo	Canada
#6	-	374	New entry	Spaceship, Inc.	United States
#7	-	303	New entry	Dynadot Inc	United States
#8	1,349	235	-83%	Sav	United States
#9	127	191	50%	Nicenic	China
#10	136	151	11%	Tucows	Canada
#11	-	112	New entry	GMO	Japan
#12	-	92	New entry	WebNic.cc	Virgin Islands
#13	52	91	75%	Gname	Singapore
#14	-	90	New entry	Squarespace Domains	United States
#15	-	81	New entry	eNom	Canada
#16	-	78	New entry	Hosting Concepts	Netherlands
#17	83	77	-7%	Alibaba	China
#18	121	76	-37%	RegRU	Russia
#19	-	68	New entry	Network Solutions, LLC	United States
#20	34	46	35%	Eranet	China

LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Jan - Jun 2024	Jul - Dec 2023
United States	53.24%	36.84%
Canada	12.43%	27.34%
Lithuania	10.80%	1.31%
India	8.01%	11.76%
China	6.39%	4.83%
Japan	2.28%	0.93%
Virgin Islands	1.87%	n/a
Singapore	1.85%	0.85%
Netherlands	1.59%	n/a
Russia	1.55%	2.77%

Networks hosting the most newly observed botnet C&Cs, Jan-Jun 2024

As usual, there were many changes in the networks hosting newly observed botnet C&Cs.

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.

Decreases across 11 networks!

After a disappointing Q4 2023, we're thrilled to report the number of botnet C&Cs hosted on 11 networks previously listed in the Top 20 declined during this reporting period. Decreases ranged from a significant -41% with amazon.com to a token -1% with google.com. Even tencent.com, perpetually in the top spot, experienced a -34% reduction from 1481 to 976!

A note of recognition...

...for excellent work! aeza.net, antel.net.uy, ielo.net, sitebgp.com, and zerohost.network all dropped out of the Top 20 networks hosting the most newly observed botnet C&Cs. Thank you for addressing this abuse on your networks.



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.



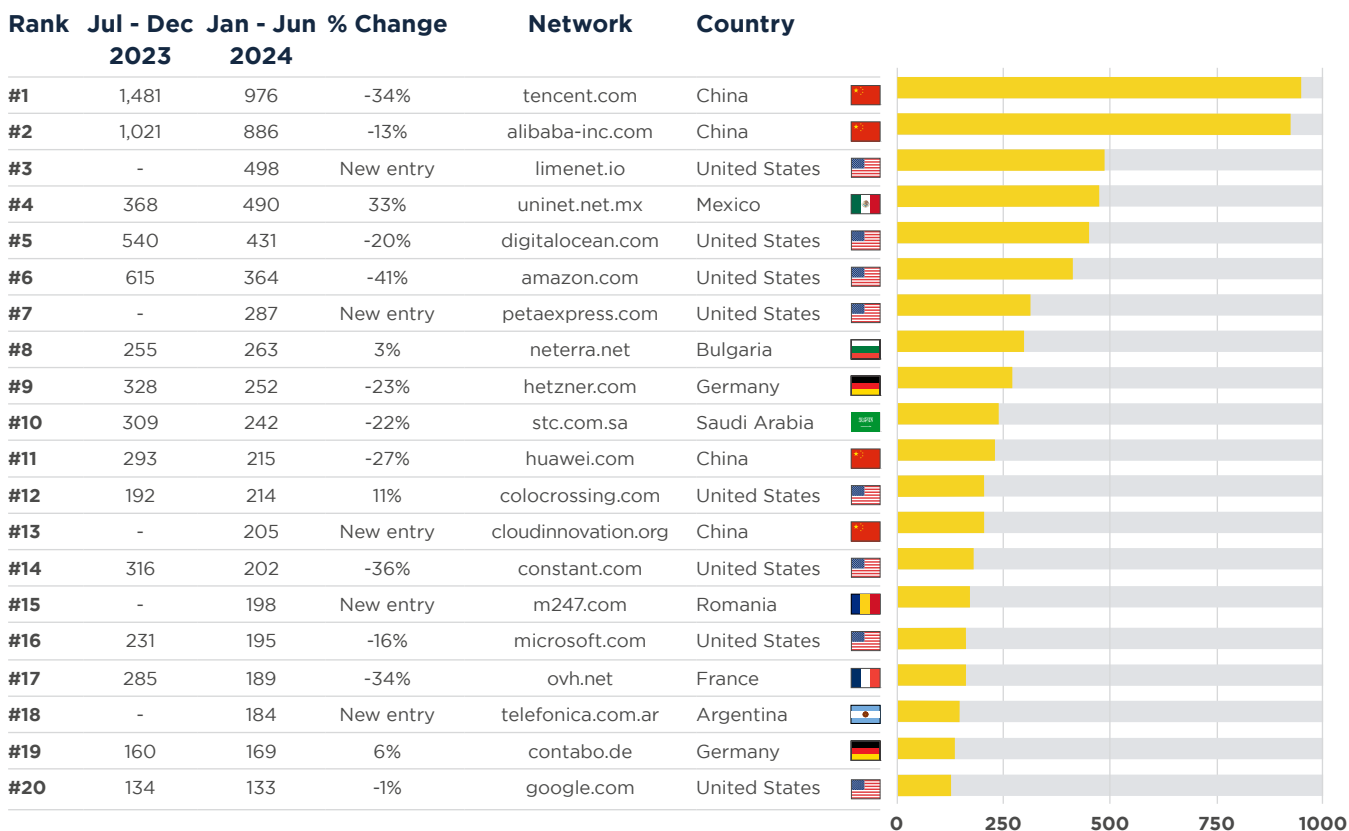
New entries

limenet.io (#3), petaexpress.com (#7), cloudinnovation.org (#13), m247.com (#15), telefonica.com.ar (#18).

Departures

aeza.net, antel.net.uy, ielo.net, sitebgp.com, zerohost.network.

Networks hosting the most newly observed botnet C&Cs, Jan-Jun 2024 (continued)



Networks hosting the most active botnet C&Cs, Jan-Jun 2024

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs between January and June 2024. 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 providers host lion's share of active C&Cs

Over the past 12 months, tencent.com (#1) and alibaba-inc.com (#2) have maintained their positions hosting the most active botnet C&Cs. From January to June 2024, there was a continued upward trend, with a +27% increase for tencent.com and a +58% increase for alibaba-inc.com. Given the ongoing growth of newly observed botnet C&Cs hosted in China, it's hardly surprising these providers account for almost 50% of networks hosting the most active botnet C&Cs.

But the good news is...

Three major networks, previously highlighted in Q4 2023 for having a potential abuse problem or for failing to take appropriate action to address botnet C&C servers on their network, have made significant improvements. Congratulations to, amazon.com (-42%), ovh.net (-36%), and microsoft.com (-26%). Long may this continue!



New entries

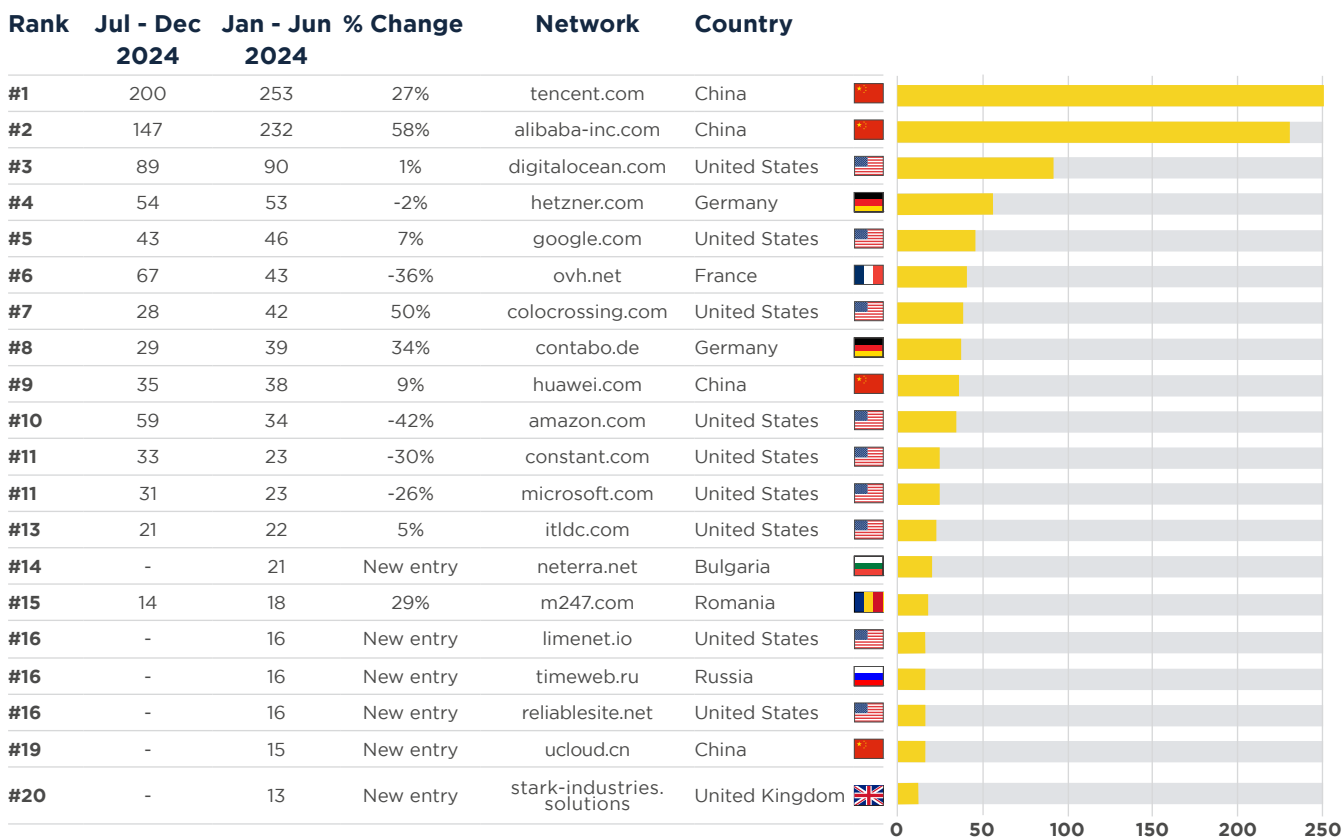
neterra.net (#14), limenet.io (#16), reliablesite.net (#16), timeweb.ru (#16), ucloud.cn (#19), stark-industries.solutions (#20).

Departures

aeza.net, free-h.org, linode.com, quadranet.com, simcentric.com, uplus.co.kr.

Networks hosting the most active botnet C&Cs, Jan-Jun 2024 (continued)

Total number of active botnet C&Cs per network



That's all for now. Stay safe, and we'll see you in Jan 2025!