

Spamhaus Botnet Threat Update



July to December 2024

Overall, botnet command and control (C&C) activity decreased, albeit marginally, between July and December last year by -4%. On the flip side, misuse of penetration testing frameworks increased to 43.73%, owing to increased observations of Cobalt Strike (12%) and a new entry, Brute Ratel C4.

This report sadly highlights a dominant trend - botnet C&C activity relating to China. Evidence of increased activity was seen across the Chinese-operated gTLD .top (+974%!). China also ranked #1 globally for hosting botnet C&C servers, with a 17.75% increase in activity linked to Chinese registrars. In addition, more than 60% of active listings were found on Chinese networks.

Addressing this escalating abuse will require substantial effort - we encourage registries and network operators in need of support to contact us.

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, Jul-Dec 2024

Over the last six months, Spamhaus identified 13,720 botnet C&Cs, compared to 14,248 in the previous six months. This represents a -4% decrease. From January to June 2024, the monthly average was 2,375 botnet C&Cs; this decreased to 2,287 from July to December 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%
Jul - Dec 2024	13,720	2,287	-4%



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, Jul-Dec 2024

A fleeting respite for China

Despite a -24% decrease in botnet C&C activity between January and June 2024, China unfortunately experienced a 25% increase during this reporting period. Ranking #1 for countries hosting botnet C&C servers (3535), China now hosts 35% more than its closest “competitor”, the U.S.A (2286).

Highs and Lows across the globe

Half of all regions experienced a drop in botnet C&Cs, with the most significant decreases in Mexico (-33%), France (-28%), and Bulgaria (-24%).

Meanwhile, of the countries that suffered an increase this quarter, 50% were based in Europe: Netherlands (6%), The United Kingdom (11%), Sweden (22%) Finland (58%) and Spain (new entry).

This quarter also saw a first-time entry from Morocco (#12).

Good news for Bulgaria

Between January and June 2024, Bulgaria reported a 162% increase, reaching 715 botnet C&C servers. In this reporting period, this number decreased by a respectable -24%, to 544, clearly demonstrating efforts to reduce this malicious activity. We’re pleased to see activity moving in the right direction.

Well done, Saudi Arabia!

After a -12% decrease in the last reporting period, Saudi Arabia has finally dropped off the Top 20. This is great progress; since Q3 2021, Saudi Arabia has not only been in the Top 20, but in the Top 15 countries for hosting botnet C&Cs.

Let’s hope this positive trend continues, and Saudi Arabia stays out of the Top 20.

Uruguay also departed from the Top 20 this reporting period.



New entries

Morocco (#12), Spain (#20).

Departures

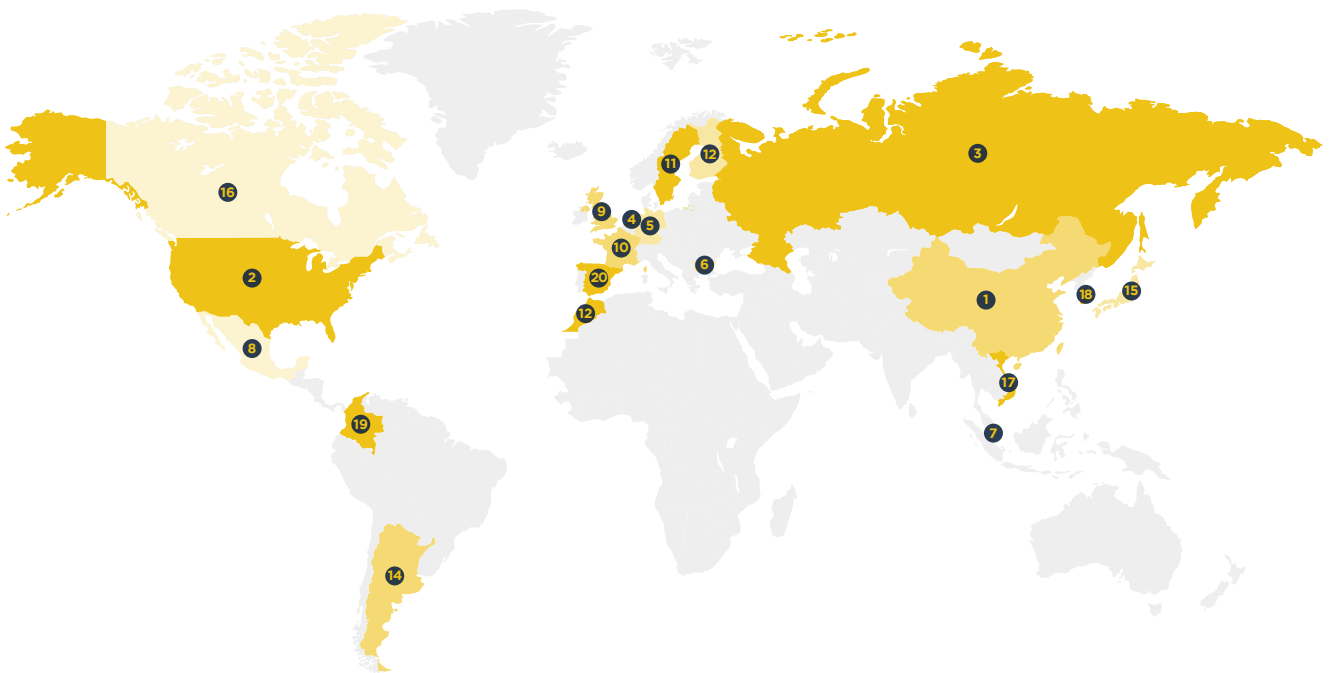
Saudi Arabia, Uruguay.

Geolocation of botnet C&Cs, Jul-Dec 2024 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Jan - Jun 2024	Jul - Dec 2024	% Change
#1	China	2,823	3,535	25%
#2	United States	2,702	2,286	-15%
#3	Russia	1,302	1,125	-14%
#4	Netherlands	737	782	6%
#5	Germany	742	657	-11%
#6	Bulgaria	715	544	-24%
#7	Singapore	332	382	15%
#8	Mexico	497	334	-33%
#9	United Kingdom	286	317	11%
#10	France	386	279	-28%

Rank	Country	Jan - Jun 2024	Jul - Dec 2024	% Change
#11	Sweden	226	275	22%
#12	Finland	135	213	58%
#12	Morocco	-	213	New entry
#14	Argentina	223	172	-23%
#15	Japan	128	136	6%
#16	Canada	144	128	-11%
#17	Vietnam	149	122	-18%
#18	Korea (Rep. of)	107	110	3%
#19	Colombia	135	107	-21%
#20	Spain	-	100	New entry



Malware associated with botnet C&Cs, Jul-Dec 2024

Cobalt Strike is on the rise... again

This report saw Cobalt Strike reach a 30 month milestone at #1 for the malware associated with the largest number of botnet C&Cs, with a 12% increase between July and December 2024.

The penetration testing tool is now associated with approximately three times more botnet C&Cs than its closest competitor, Remcos, at number two (1257).

Brute Ratel C4 debuts at #19

Brute Ratel C4 is a penetration testing framework similar to Cobalt Strike, first introduced in 2020. In 2022, a cracked version of its command and control (C&C) server leaked on underground forums, and its detection rates have significantly increased.

Ranking #19, this report highlights that Brute Ratel C4 has been frequently detected due to its use by a Latrodectus affiliate, which employs Brute Ratel C4 as a loader in their campaigns.

RATs are on the prowl

Despite significant decreases for DCRat (-59%), NjRAT (-33%), and AsyncRAT (-29%), Remote Access Trojans (RATs) remain the second most common malware type associated with botnet C&C servers, representing 30.45% during the reporting period.

RATs are 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 in this reporting period was Remcos, which saw a 72% increase between July and December 2024.



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.

Malware associated with botnet C&Cs, Jul-Dec 2024 (continued)

Android backdoors remain #3

The number of botnet C&Cs associated with Android backdoors rose to 20.01% between January and June 2024. However, over the last six months, it has decreased slightly to 13.94%. Nevertheless, Android backdoors remain the third most popular malware, due to a 152% increase in Coper (#10).

Coper malware targets Android devices by bypassing security measures, taking remote control of the device, and stealing sensitive information.

Bye, bye Qakbot!

We are delighted to report that Qakbot has finally departed from the Top 20 malware associated with botnet C&Cs!

This notorious malware first entered the charts in Q3 2022 at #4, and quickly gained momentum. However, Tuesday August 29th, 2023, the Federal Bureau of Investigation (FBI), announced that it had [taken control of the Qakbot infrastructure](#), in an International coordinated effort.

Despite the takedown efforts, Qakbot activity continued to be reported, hence its presence in reports over the past year. Will we see Qakbot again? Maybe, but only time will tell.



New entries

Stealc (#16), Brute Ratel C4 (#19), DanaBot (#20).

Departures

Bashlite, Qakbot, RisePro.

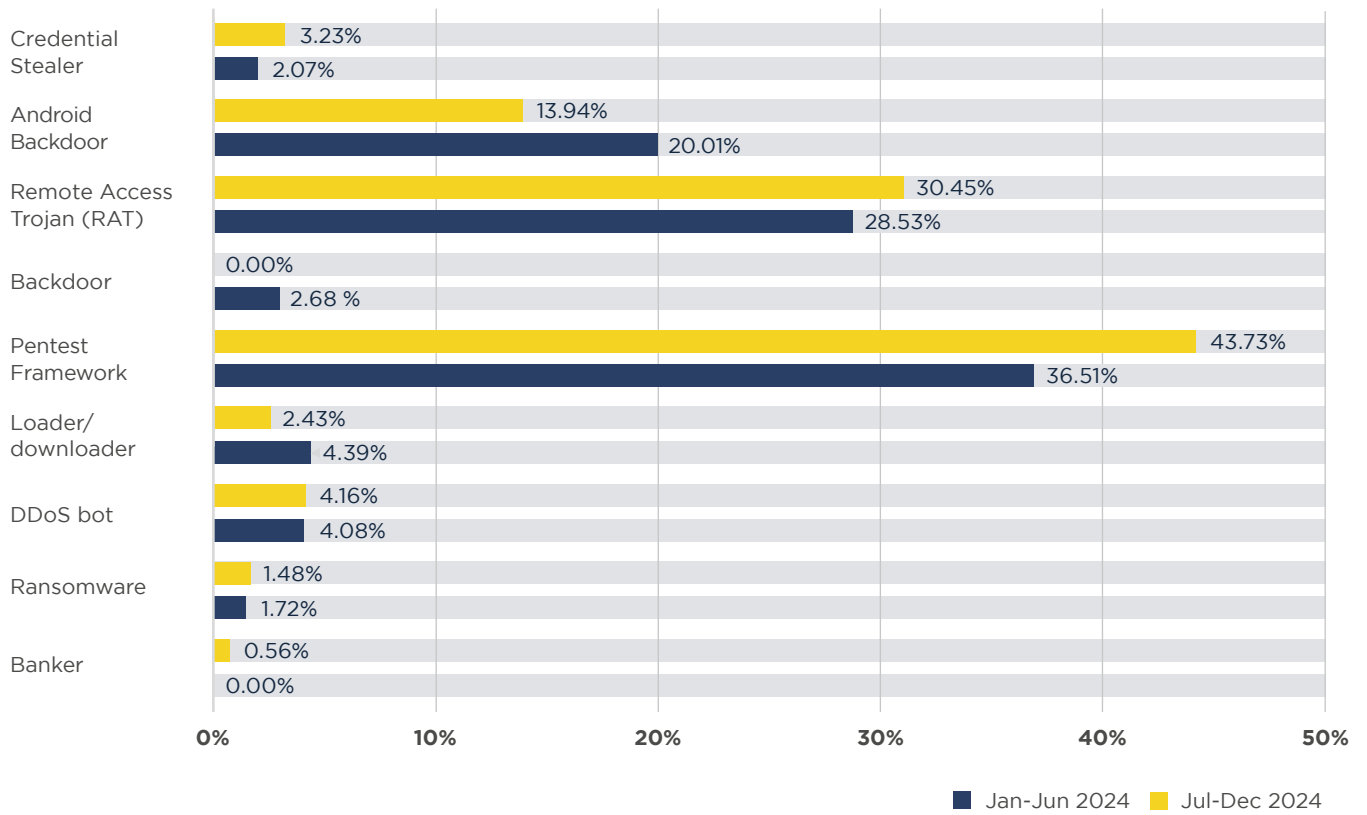
Malware associated with botnet C&Cs, Jul-Dec 2024 (continued)

Malware families associated with botnet C&Cs

Rank	Jan - Jun 2024	Jun - Dec 2024	% Change	Malware Family	Description	
#1	3,348	3,737	12%	Cobalt Strike	Pentest Framework	
#2	729	1,257	72%	Remcos	Remote Access Trojan (RAT)	
#3	1,727	1,025	-41%	Flubot	Android Backdoor	
#4	1,020	725	-29%	AsyncRAT	Remote Access Trojan (RAT)	
#5	665	495	-26%	Sliver	Pentest Framework	
#6	374	482	29%	QuasarRAT	Remote Access Trojan (RAT)	
#7	379	427	13%	Mirai	DDoS Bot	
#8	733	298	-59%	DCRat	Remote Access Trojan (RAT)	
#9	280	279	0%	RedLineStealer	Remote Access Trojan (RAT)	
#10	92	232	152%	Coper	Android Backdoor	
#11	163	192	18%	Havoc	Pentest Framework	
#12	103	191	85%	Rhadamanthys	Credential Stealer	
#13	470	175	-63%	Hook	Android Backdoor	
#14	201	168	-16%	Latrodectus	Loader/Downloader	
#15	197	152	-23%	BianLian	Ransomware	
#16	-	141	New entry	Stealc	Credential Stealer	
#17	128	86	-33%	NjRAT	Remote Access Trojan (RAT)	
#18	301	82	-73%	FakeUpdates	Loader/Downloader	
#19	-	67	New entry	Brute Ratel C4	Pentest Framework	
#20	-	58	New entry	DanaBot	Banker	

0 1000 2000 3000 4000

Malware type comparisons



Most abused top-level domains, Jul-Dec 2024

.top and .xyz

These two gTLDs have a long history of abuse, so it's not surprising to see them in the Top 3. That said, .top (#2) had a staggering 974% increase in the number of botnet C&Cs (1514) it hosted between July and December 2024! This is the third largest increase we have seen in the history of the Botnet Report.

It is surprising though to see such a significant increase, especially given that ICANN served a [breach notice to .top](#) in July 2024, which, in part, was due to DNS abuse issues.

Reductions and departures

We'd like to congratulate all the registries that manage TLDs who departed from our listings! Along with those who significantly reduced the number of associated botnet C&Cs using their TLDs, including .cfd and .site, who both saw a 70% reduction.

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, between July and December 2024, .com had more than 154m domains, of which 0.00114% were associated with botnet C&Cs. Meanwhile, .monster had approximately 50k domains, of which 0.148% were associated with botnet C&Cs. Both are in the Top 20 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.



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

click (#9), monster (#16), icu (#17), buzz (#18), biz (#20).

Departures

co, fun, space, tech, website.

Most abused top-level domains, Jul-Dec 2024 (continued)

Top abused TLDs - number of domains

Rank	Jan - Jun 2024	Jul - Dec 2024	% Change	TLD	Type of TLD
#1	2,013	1,757	-13%	com	gTLD
#2	141	1,514	974%	top	gTLD
#3	198	331	67%	xyz	gTLD
#4	224	230	3%	net	gTLD
#5	122	186	52%	shop	gTLD
#5	229	157	-31%	org	gTLD
#7	232	150	-35%	store	gTLD
#8	441	143	-68%	online	gTLD
#9	-	141	New entry	click	gTLD
#10	367	111	-70%	site	gTLD
#11	48	110	129%	info	gTLD
#12	229	108	-53%	sbs	gTLD
#13	68	91	34%	cn	ccTLD
#14	50	84	68%	ru	ccTLD
#15	60	80	33%	cloud	gTLD
#16	-	75	New entry	monster	gTLD
#17	-	67	New entry	icu	gTLD
#18	-	62	New entry	buzz	gTLD
#18	189	57	-70%	cfid	gTLD
#20	-	55	New entry	biz	ccTLD

Most abused domain registrars, Jul-Dec 2024

Huge increases at Nicenic

We have observed an enormous 757% increase of newly registered botnet C&C domains at the Chinese domain registrar, Nicenic, knocking Namecheap (US) off the top spot. These registrations have increased by more than 8 times from 191 in the previous six months, to 1636 between July and December 2024.

As a result, there was a noticeable overall increase (17.75%) in the number of botnet C&Cs associated with registrars operating out of China.

The situation in The US improves

US domain registrars continue to dominate the Top 20, though more positively, the percentage of C&C-related domain registrations decreased slightly this reporting period from 53.24% to 41.68%. This was predominantly due to Spaceship, Inc., and Sav, both experiencing a -63% decrease. Sav in particular has continued to reduce the number of botnet C&C operators registering through them for a consecutive 18 months. Keep up the great work!

More botnet C&C domains at Dynadot and WebNic.cc

Meanwhile, the situation at the US-based Dynadot and the Singapore-based registrar WebNic.cc doesn't look good. We have observed an increase of 169% in botnet C&C domains registered through Dynadot and 142% at WebNic.cc.

With some significant increases, we encourage these domain registrars to get in contact with Spamhaus to help mitigate against botnet C&C abuse.



New entries

Arsys Internet,
S.L. dba NICLINE.COM (#18),
RU-Center (#20).

Departures

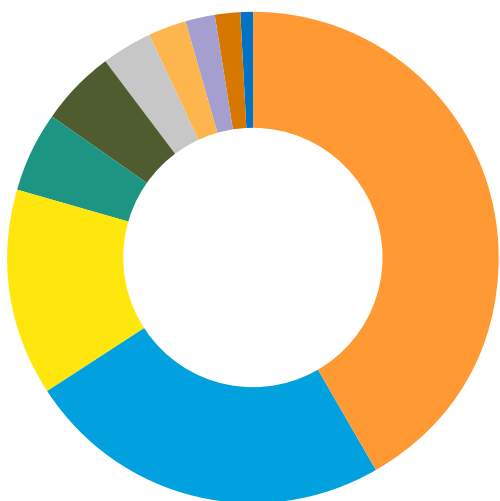
Network Solutions LLC,
Squarespace Domains.

Most abused domain registrars, Jul-Dec 2024 (continued)

Most abused domain registrars - number of domains

Rank	Jan - Jun 2024	Jul - Dec 2024	% Change	Registrar	Country
#1	191	1,636	757%	Nicenic	China
#2	1,027	1,513	47%	NameCheap	United States
#3	303	815	169%	Dynadot Inc	United States
#4	379	805	112%	NameSilo	Canada
#5	521	437	-16%	GoDaddy.com	United States
#6	394	368	-7%	PDR	India
#7	531	225	-58%	Hostinger	Lithuania
#8	92	223	142%	WebNic.cc	Singapore
#9	112	185	65%	GMO	Japan
#10	91	164	80%	Gname	Singapore
#11	151	159	5%	Tucows	Canada
#12	374	139	-63%	Spaceship, Inc.	United States
#13	78	126	62%	Hosting Concepts	Netherlands
#14	235	88	-63%	Sav	United States
#15	76	60	-21%	REGRU	Russia
#16	76	55	-28%	eNom	Russia
#17	46	52	13%	Eranet	China
#18	77	45	-42%	Alibaba	China
#18	-	45	New entry	Arsys Internet, S.L. dba NICLINE.COM	Spain
#20	-	39	New entry	RU-Center	Russia

LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Jul - Dec 2024	Jan - Jun 2024
United States	41.68%	53.24%
China	24.14%	6.39%
Canada	13.43%	12.43%
Singapore	5.39%	3.72%
India	5.13%	8.01%
Lithuania	3.13%	10.80%
Japan	2.58%	2.28%
Russia	2.15%	1.55%
Netherlands	1.76%	1.59%
Spain	0.63%	n/a

Networks hosting the most newly observed botnet C&Cs, Jul-Dec 2024

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

alibaba-inc.com #1

Despite spending years in the top five, Chinese-based e-commerce giant, Alibaba finally took the number one position. With a 43% increase in newly observed botnet C&Cs, it put to an end to Tencent's 18 month reign as the most abused network (now #2).

New entries from selectel.ru and baxet.ru

Russian Virtual Private Server (VPS) providers baxet.ru and selectel.ru have made a notable return to the Top 20 having been absent for quite some time; baxet.ru previously dropped out in Q2 2022 and selectel.ru made its comeback after an even longer absence since Q1 2021.

Decreases across 12 networks!

Yet again, we're delighted to report the number of botnet C&Cs hosted on 12 networks previously listed in the Top 20 decreased during this period, with consecutive decreases from amazon.com (-19%), constant.com (-18%), digitalocean (-18%), hetzner.com (-27%), microsoft.com (-11%) and ovh.net (-2%), with stc.com.sa dropping out of the Top 20.

Unfortunately, the same can't be said for google.com, with an 81% increase in newly observed botnet C&Cs this reporting period.



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

selectel.ru (#12), baxet.ru (#20).

Departures

petaexpress.com, stc.com.sa.

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





















Most improved and worst performers

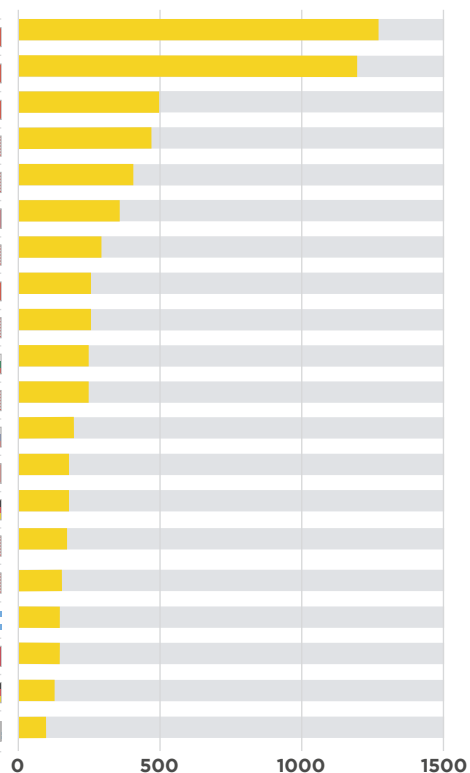
Between July and December 2024, the most improved network was US-based limenet.io with a -54% reduction in the number of newly observed botnet C&Cs on its network. Conversely, cloudinnovation.org experienced a 142% increase in newly observed botnet C&Cs.

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.

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

Rank	Jan - Jun 2024	Jul - Dec 2024	% Change	Network	Country	
#1	886	1,269	43%	alibaba-inc.com	China	
#2	976	1,019	4%	tencent.com	China	
#3	205	496	142%	cloudinnovation.org	China	
#4	214	434	103%	colocrossing.com	United States	
#5	431	352	-18%	digitalocean.com	United States	
#6	490	331	-32%	uninet.net.mx	Mexico	
#7	364	295	-19%	amazon.com	United States	
#8	215	249	16%	huawei.com	China	
#9	133	241	81%	google.com	United States	
#10	263	231	-12%	neterra.net	Bulgaria	
#11	498	229	-54%	limenet.io	United States	
#12	-	196	New entry	selectel.ru	Russia	
#13	189	185	-2%	ovh.net	France	
#14	252	184	-27%	hetzner.com	Germany	
#15	195	174	-11%	microsoft.com	United States	
#16	202	165	-18%	constant.com	United States	
#17	184	154	-16%	telefonica.com.ar	Argentina	
#18	198	151	-24%	m247.com	Romania	
#19	169	145	-14%	contabo.de	Germany	
#20	-	127	New entry	baxet.ru	Uruguay	



Networks hosting the most active botnet C&Cs, Jul-Dec 2024

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs between July and December 2024. Alibaba leads this Top 20 too with 172 active botnet C&Cs, followed by Tencent with 85 active botnet C&Cs.

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.

Network operators in China need to get on top of abuse rapidly

Over 60% of active botnet C&C listings are on networks located in China, including four new entries: cloudinnovation.org (#3), changway.hk (#10), ctgserver.com (#11), and macloud.ru (#11). We implore these operators to quickly respond to abuse reports and work with Spamhaus to reduce botnet C&C abuse on their networks.

Positive reductions across 12 networks

Excluding seven new entries and one increase in active botnet C&Cs, all remaining networks in the Top 20 either remained the same or experienced a reduction. Decreases ranged from a significant -77% from hetzner.com to -13% from ucloud.cn. Thank you to all networks for your continued efforts to prevent botnet operators hosting C&C servers on your networks. Long may this continue!



New entries

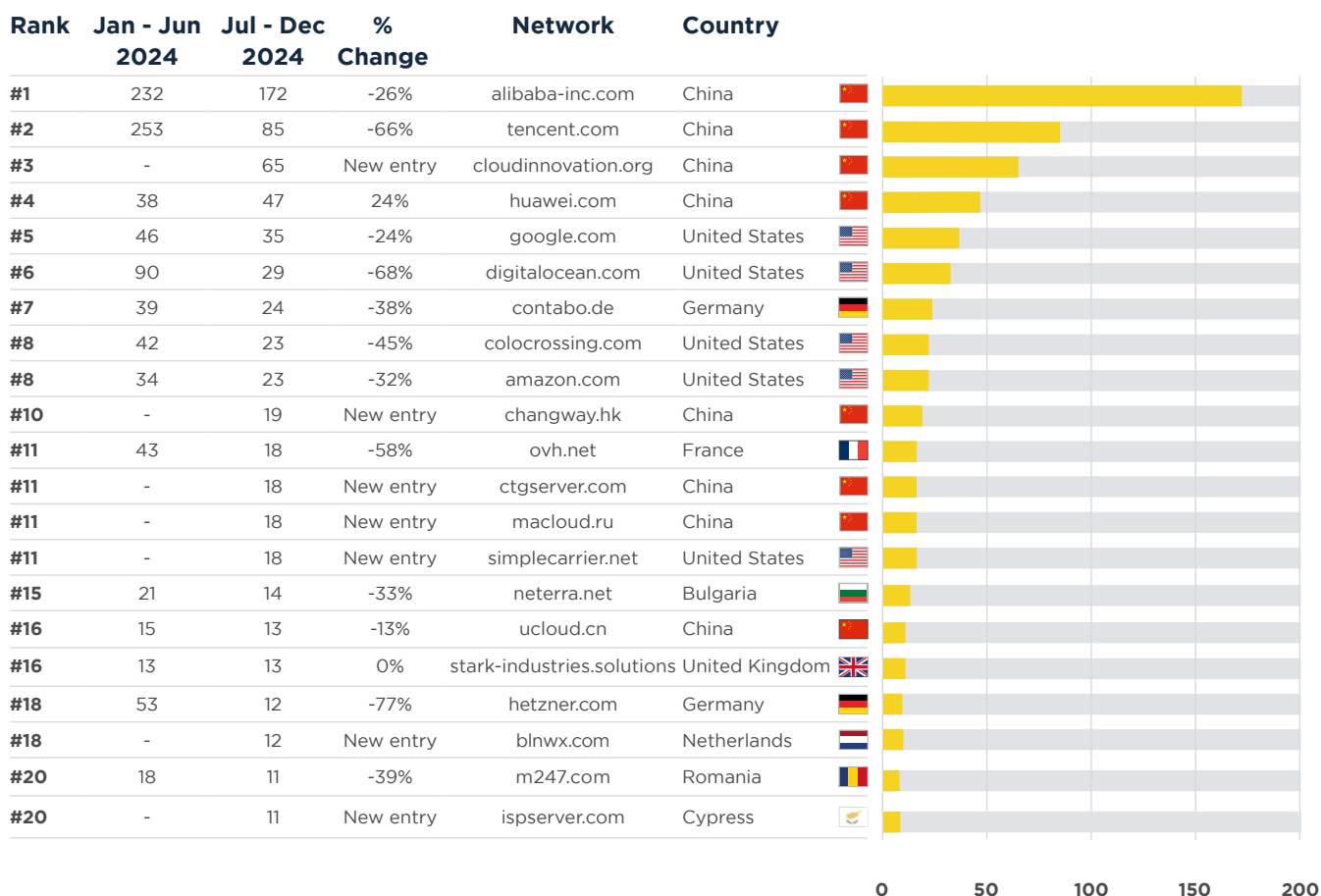
cloudinnovation.org (#3),
changway.hk (#10),
ctgserver.com (#11),
macloud.ru (#11),
simplecarrier.net (#11),
blnwx.com (#18),
ispserver.com (#20).

Departures

constant.com, itldc.com,
limenet.io, microsoft.com,
reliablesite.net, timeweb.ru.

Networks hosting the most active botnet C&Cs, Jul-Dec 2024 (continued)

Total number of active botnet C&Cs per network



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