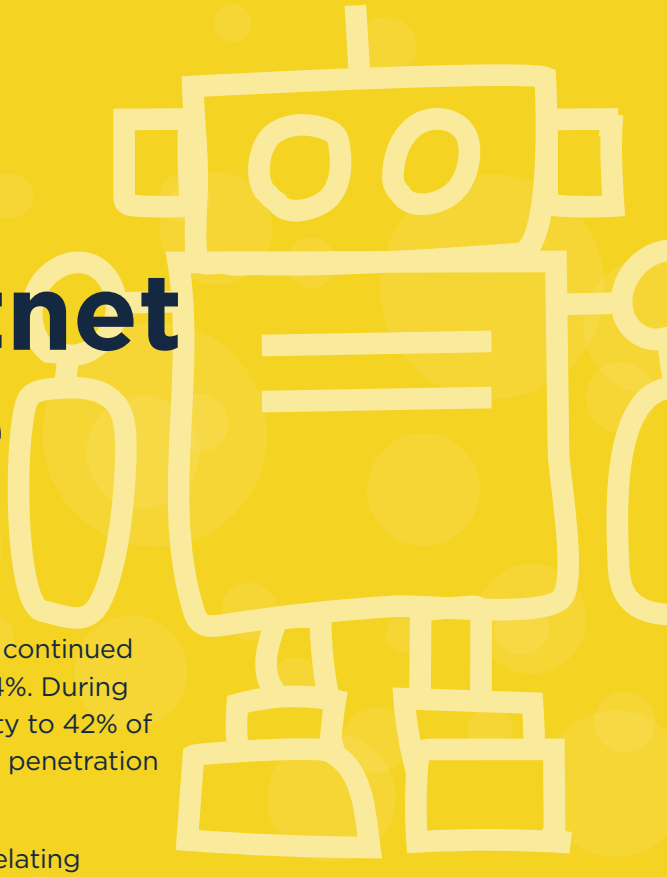
SPAMHAUS



Spamhaus Botnet Threat Update

July to December 2025

The number of botnet command and control (C&C) servers continued to rise between July and December 2025, increasing by +24%. During this period, Remote Access Trojans (RATs) grew in popularity to 42% of malware associated with observed botnet C&Cs, overtaking penetration testing frameworks as the most prevalent malware type.

This report also highlights a particularly noteworthy trend relating to botnet C&C activity linked to Russia. Domains under the Russian ccTLD (.ru), hosting botnet C&Cs increased by +3,741%, while the domain registrar REGRU experienced a whopping increase of +9,608% newly registered botnet C&C domains during the second half of 2025.

But it isn't all bad news – several large cloud network operators frequently listed in this report's Top 20 section appear to have (finally) taken action to tackle active botnet C&Cs, with numbers reducing almost across the board. Well done – we hope to see a further decrease of botnet controller activity emanating from legitimate networks in 2026!

Welcome to the Spamhaus Botnet Threat Update.

About this report

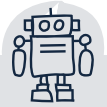
Spamhaus tracks both Internet Protocol (IP) addresses and domain names used by threat actors for hosting botnet command & control (C&C) servers. This data enables us to identify associated elements, including the geolocation of the botnet C&Cs, the malware associated with them, the top-level domains 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 2025

Over the last six months, Spamhaus identified 21,425 botnet C&Cs, compared to 17,258 in the previous six months. This represents a +24% increase. From January to June 2025, the monthly average was 2,876 botnet C&Cs; this increased to 3,571 from July to December 2025.

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%
Jan - Jun 2025	17,258	2,876	26%
Jul - Dec 2025	21,425	3,571	24%



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 2025

The United States knocks China off the top spot

The increases keep coming from networks geolocated to the United States. Between January and June 2025, the number of related botnet C&Cs increased by +54%. During this reporting period the numbers increased by a further +44%, to 5,040, knocking China off it's #1 position; a position China had held since Q3 2023.

With China seeing a -5% decrease in botnet C&Cs between July and December 2025, the United States is now hosting 1,669 more botnet controllers, considerably increasing its lead. This development once again disproves the belief that internet abuse mainly originates from non-Western jurisdictions.

New entries

Poland (#15), Colombia (#18).

Departures

Dominican Republic, Morocco.

Other increases across the globe

Only three countries saw a decrease in botnet C&C servers during this reporting period: Bulgaria (-48%), Russia (-29%), and the aforementioned China (-5%).

Conversely, several countries saw sharp increases. The Seychelles, new to the Top 20 in the January–June 2025 Botnet Threat Update, showed the largest increase at +287%, followed by the United Kingdom (+103%) and Turkey (+86%).

Seychelles surge: Shell corporations and geolocation inaccuracies

In the previous report, we identified a new entry from the Seychelles hosting 167 botnet C&C servers. Between July and December 2025, the number of botnet C&Cs located in the Seychelles increased sharply by +287% to 647, placing it at #8 in the Top 20.

Readers of our Q2 2021 Botnet Threat Update may recall eliteteam.to, a Russia-based bulletproof hosting provider purporting to be located in the Seychelles. Similarly, the current surge of botnet C&Cs geolocated to this jurisdiction stems from rogue hosting providers, such as simplecarrier.net, using offshore shell corporations for running their operations. A significant amount of botnet C&Cs geolocated to the Seychelles traces back elsewhere, such as to Hong Kong-based zillionnetwork.com or US-based, now-defunct, cheapy.host.

Geolocation of botnet C&Cs, Jul-Dec 2025 (continued)

Geolocation is far from being an exact science, and miscreants are frequently observed to deliberately forge the geolocation of their networks. From a defenders' perspective, traffic filtering based on network operators and/or Autonomous Systems (ASNs) might achieve more reliable results.

Bulgaria drops to #20!

Following a -40% decrease in the January–June 2025 Botnet Threat Update, Bulgaria, a long-standing member of this Top 20, saw a further -48% decline between July and December 2025, falling to 170 botnet C&C servers.

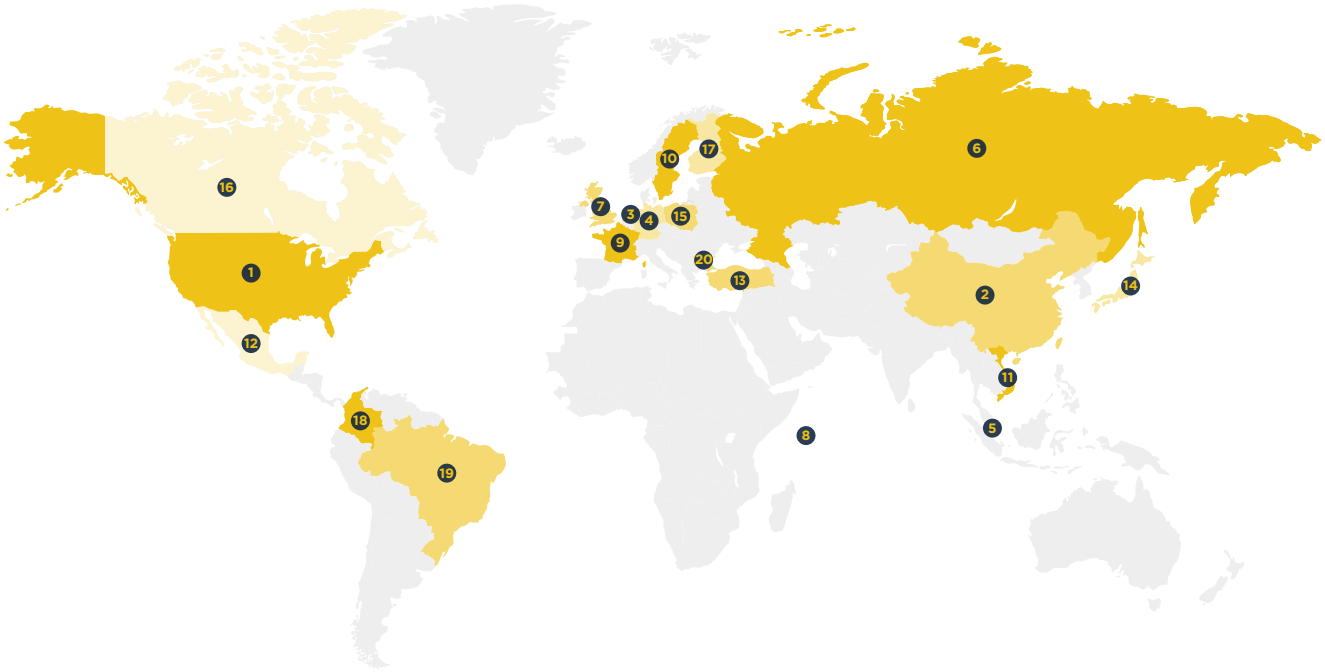
Let's hope Bulgaria will drop out of this Top 20 in 2026.

Geolocation of botnet C&Cs, Jul-Dec 2025 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Jan - Jun 2025	Jul - Dec 2025	% Change
#1	United States	3,512	5,040	44%
#2	China	3,533	3,371	-5%
#3	Netherlands	1,406	2,104	50%
#4	Germany	1,307	1,528	17%
#5	Singapore	712	1,191	67%
#6	Russia	1,022	722	-29%
#7	United Kingdom	329	667	103%
#8	Seychelles	167	647	287%
#9	France	470	533	13%
#10	Sweden	284	437	54%

Rank	Country	Jan - Jun 2025	Jul - Dec 2025	% Change
#11	Vietnam	188	321	71%
#12	Mexico	251	292	16%
#13	Turkey	146	271	86%
#14	Japan	163	269	65%
#15	Poland	-	222	New entry
#16	Canada	191	206	8%
#17	Finland	183	197	8%
#18	Colombia	-	187	New entry
#19	Brazil	154	173	12%
#20	Bulgaria	327	170	-48%



Malware associated with botnet C&Cs, Jul-Dec 2025

Remote Access Trojans: Miscreants' tool of choice

Remote Access Trojans (RATs) have overtaken penetration testing (pentesting) frameworks as the most prevalent malware type in conjunction with botnet C&Cs observed, accounting for 42% of all malware in this Top 20. Specifically, this reporting period saw noticeable increases from XWorm (+118%), Remcos (+48%), AsyncRAT (+40%), QuasarRAT (+38%), and ValleyRAT (+36%).

Despite this shift, the penetration testing framework Cobalt Strike remains the single most prevalent malware family, representing 20% of the Top 20.

Both RATs and pentesting frameworks are often used to lay the groundwork for downstream security. After initial access, threat actors may deploy second-stage malware for lateral movement within a compromised network. In addition, harvested credentials may be exfiltrated to threat actors to enable malicious logins to internet-facing services (e.g., mail servers or collaboration platforms).

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.

Aisuru on the rise

Debuting at #5, the Aisuru botnet was associated with 1,023 botnet controllers observed between July and December 2025. This botnet consists of a network of compromised Internet of Things (IoT) devices used to launch Distributed Denial-of-Service (DDoS) attacks.

First identified in August 2024, it has grown rapidly throughout 2025, with a recent shift toward abusing its bots for residential proxy activity too, as reported by KrebsOnSecurity in October. This change is in line with residential proxy networks generally gaining momentum as a major cybercrime enabler, as demonstrated by China-nexus spammers throughout 2025.

Latrodectus returns

First identified in October 2023, Latrodectus entered the Top 20 at rank #13 in our January–June 2024 Botnet Threat Update. Following its takedown by law enforcement in May 2025, it has now resurfaced, re-entering the Top 20 at rank #14, associated with 370 botnet C&Cs.

Malware associated with botnet C&Cs, Jul-Dec 2025 (continued)

Latrodectus is a Windows malware loader that was initially observed being delivered via malicious email attachments in phishing campaigns. It is designed to execute commands, steal data, deploy additional malware, and maintain persistence through scheduled tasks and encrypted C&C communication.

New entries

Aisuru (#5), Latrodectus (#14), VenomRAT (#17), PureLogs Stealer (#18), Vidar (#19).

Departures

Chaos, DeimosC2, Hook, NjRAT, RedlineStealer.

Final surge for Rhadamanthys (hopefully) and VenomRAT

In November, we saw another episode of "Operation Endgame," namely, the Europol-led takedown of infrastructure related to several major threats, including Rhadamanthys, VenomRAT, and the botnet Elysium.

Data shows how urgent this countermeasure was: Before this takedown, between July and November, activity associated with Rhadamanthys recorded a +58% rise, while VenomRAT entered the Top 20 for the first time.

Commendably, the alleged developer of VenomRAT was arrested in conjunction with this takedown. We therefore hope to see VenomRAT dropping out of the Top 20 in the upcoming Botnet Threat Update – as the case of Latrodectus illustrates, it remains to be seen whether Rhadamanthys (no related arrests have been made in the most recent Operation Endgame takedown) follows suit.

Flubot Infrastructure Reuse

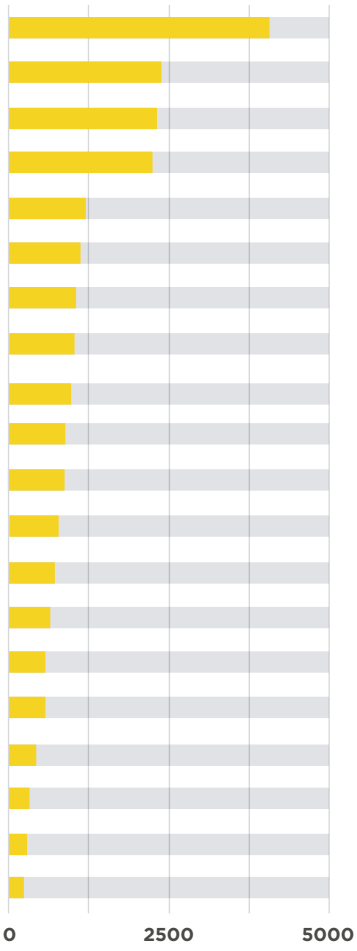
Botnet C&C activity associated with infrastructure using the same "fast flux" techniques previously observed in FluBot campaigns declined by -4% in the latter half of 2025. Despite this decrease, the activity still ranked eighth among botnet C&Cs infrastructures observed by our researchers.

As noted in previous reports, for consistency in our internal tracking, we continue to label this infrastructure as FluBot. However, it is now used to host a wide range of other botnet C&C activity.

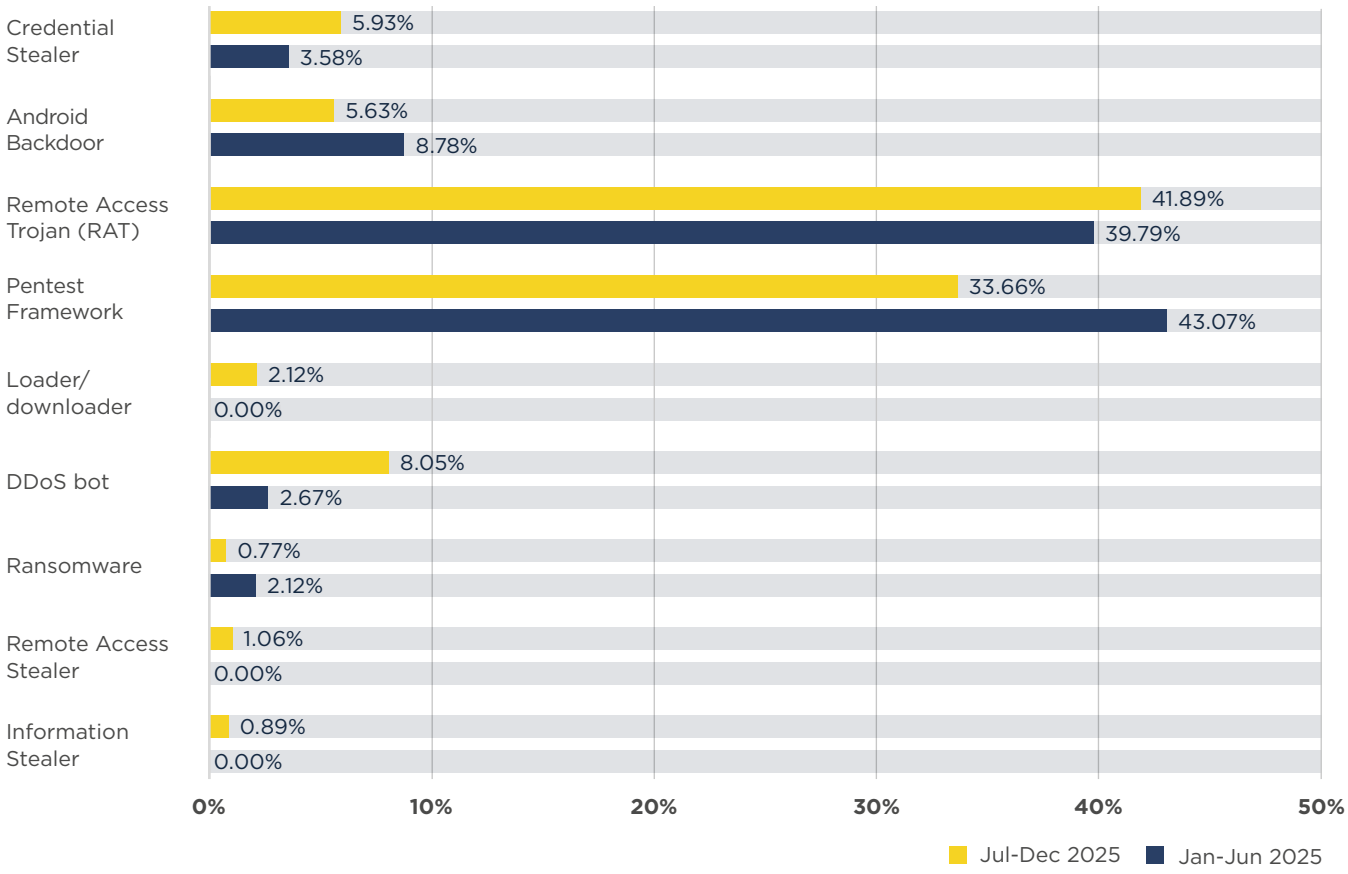
Malware associated with botnet C&Cs, Jul-Dec 2025 (continued)

Malware families associated with botnet C&Cs

Rank	Jan - Jun 2025	Jul - Dec 2025	% Change	Malware Family	Description
#1	4,107	3,451	-16%	Cobalt Strike	Pentest Framework
#2	1,756	2,467	40%	AsyncRAT	Remote Access Trojan (RAT)
#3	1,533	2,269	48%	Remcos	Remote Access Trojan (RAT)
#4	1,177	1,904	62%	Sliver	Pentest Framework
#5	-	1,023	New entry	Aisuru	DDoS Bot
#6	394	860	118%	XWorm	Remote Access Trojan (RAT)
#7	562	774	38%	QuasarRAT	Remote Access Trojan (RAT)
#8	741	710	-4%	Flubot	Android Backdoor
#9	382	604	58%	Rhadamanthys	Credential Stealer
#10	458	515	12%	Havoc	Pentest Framework
#11	630	505	-20%	DCRat	Remote Access Trojan (RAT)
#12	316	430	36%	ValleyRAT	Remote Access Trojan (RAT)
#13	361	380	5%	Mirai	DDoS Bot
#14	-	370	New entry	Latrodectus	Loader/Downloader
#15	103	279	171%	Joker	Credential Stealer
#16	267	271	1%	Coper	Android Backdoor
#17	-	185	New entry	Venom RAT	Remote Access Stealer
#18	-	155	New entry	PureLogs Stealer	Information Stealer
#19	-	151	New entry	Vidar	Credential Stealer
#20	175	135	-23%	BianLian	Ransomware



Malware type comparisons



Most abused top-level domains, Jul-Dec 2025

The trend turns

Despite encouraging decreases in the January–June 2025 Botnet Threat Update, the trend reversed in this reporting period. Only two top-level domains (TLDs), .shop (#15) and .top (#3), saw moderate declines in abuse, at -27% and -25% respectively.

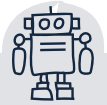
In contrast, thirteen TLDs saw increases in associated botnet C&C activity, with nine experiencing growth of +100% or more. Among these, .ru stood out with a +3,741%increase, followed by .online (+386%), .cc (+327%), .site (+280%), .org (+216%), .net (+208%), .info (+128%), .click (+106%), and .fun (+100%).

.ru serious?

As noted earlier, .ru increased by an unbelievable +3,741%, rising to 3,726 botnet C&Cs observed between July and December 2025. This increase can be attributed almost entirely to js.clearfake, a malicious JavaScript framework deployed on compromised websites, used to deceive users into downloading malware.

The .ru TLD is operated by the Coordination Center for TLD RU/РФ, the national registry for Russia's top-level domain. Over the past year, .ru had been performing reasonably well, ranking mid-table with fewer fraudulent domain registrations. This sudden spike represents a complete trend reversal, potentially due to .ru's attractiveness to miscreants, stemming from being out of direct reach to Western law enforcement.

We strongly urge the registry to work with its registrars to improve their vetting and registration controls in order to prevent further escalation of abuse.



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, Jul-Dec 2025 (continued)

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, between July and December 2025, **.com** had more than **158m** domains, of which 0.0027% were associated with botnet C&Cs. Meanwhile, **.ru** had approximately **6m** domains, of which 0.0637% were associated with botnet C&Cs. Both are in the Top 5 of our listings. Still, one had a much higher percentage of domains related to botnet C&Cs than the other.

New entries

sbs (#10), cfd (#12), asia (#13), cyou (#14), qpon (#17).

Departures

digital, live, run, tech, today.

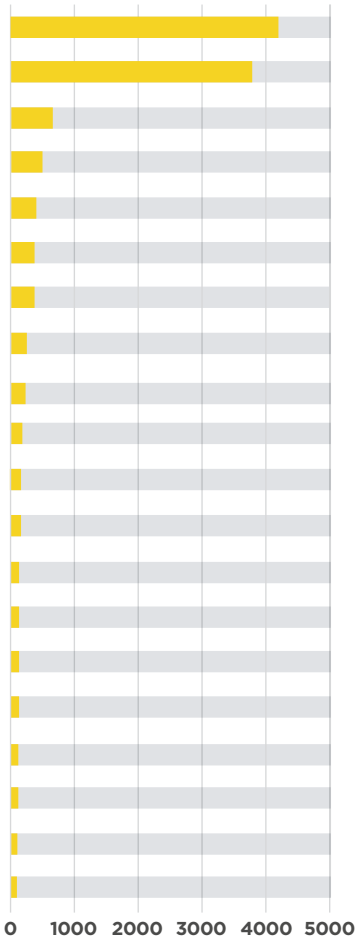
Working together with the industry for a safer internet

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, and prevented as thoroughly as possible. 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.

Most abused top-level domains, Jul-Dec 2025

Top abused TLDs - number of domains

Rank	Jan - Jun 2025	Jul - Dec 2025	% Change	TLD	Type of TLD
#1	2,286	4,287	88%	com	gTLD
#2	97	3,726	3,741%	ru	ccTLD
#3	838	627	-25%	top	gTLD
#4	175	539	208%	net	gTLD
#5	362	393	9%	xyz	gTLD
#6	108	341	216%	org	gTLD
#7	149	339	128%	info	gTLD
#8	60	256	327%	cc	ccTLD
#9	49	238	386%	online	gTLD
#10	-	172	New entry	sbs	gTLD
#11	35	133	280%	site	gTLD
#12	-	130	New entry	cfd	gTLD
#13	-	117	New entry	asia	ccTLD
#14	-	111	New entry	cyou	gTLD
#15	147	107	-27%	shop	gTLD
#16	78	106	36%	cn	ccTLD
#17	-	104	New entry	qpon	gTLD
#18	50	100	100%	fun	gTLD
#19	47	97	106%	click	gTLD
#20	78	88	13%	icu	gTLD



Most abused domain registrars, Jul-Dec 2025

REGRU powers into #1

Between July and December 2025, we observed a substantial +9,608% increase in newly registered botnet C&C domains at the Russia-based registrar REGRU, placing it at #1 for the first time. Registrations increased from 40 in the previous six months, to 3,883 during this reporting period.

Perhaps unsurprisingly, there was a notable overall increase in botnet C&Cs associated with registrars operating out of Russia, which now represent 32.2% of all observed activity.

New entries

CNOBIN INFORMATION TECHNOLOGY (#13), Name SRS (#18), Porkbun (#19).

Departures

Arsys Internet, S.L. dba NICLINE.COM, eName Technology Co., Ltd, SPRINTNAMES-RU.

Increases for many registrars

Thirteen registrars in the July-December 2025 Top 20 experienced increases in the number of botnet operators registering domains through their platforms.

Of these, six are US-based: Spaceship, Inc. (+434%), Cloudflare, Inc (+369%), Dynadot Inc. (+336%), GoDaddy.com (+253%), Namecheap (+157%) and new entrant, Porkbun, at #19 with 115 botnet C&Cs observed.

Decreases for PDR and Sav

Following a challenging first half of 2025, India-based registrar PDR saw a -76% reduction in botnet operators registering domains through its platform.

Similarly, US-based Sav is back on course with a -68% decrease, dropping to #20. In both cases, we hope not to observe another abuse surge going forward.

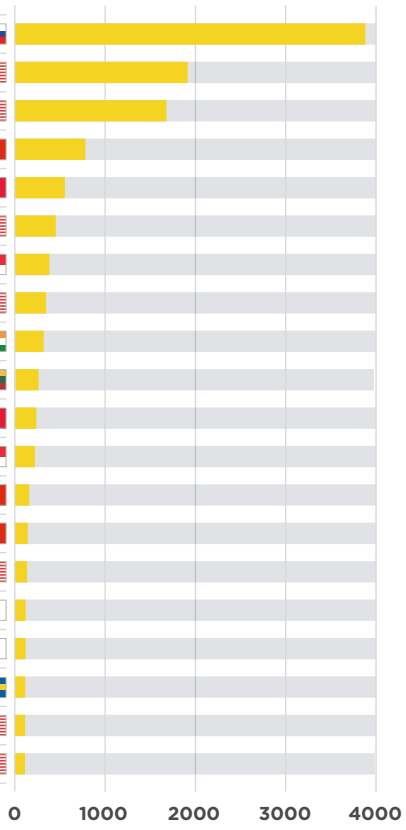
Thanks to those who've departed

Well done to Arsys Internet, S.L. dba NICLINE.COM, eName Technology Co., Ltd, and SPRINTNAMES-RU who've departed from our Top 20, and to those who have seen reductions in botnet operators registering domains
– keep up the good work!

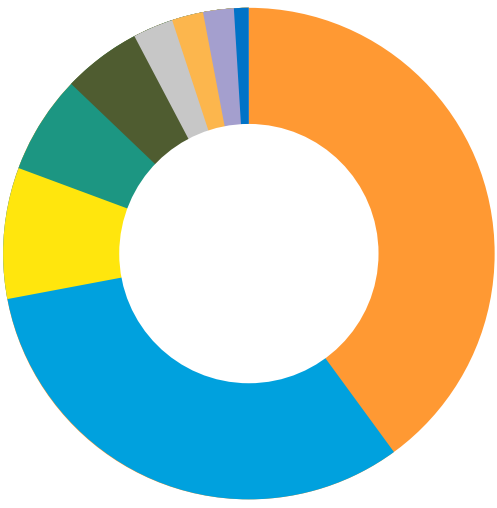
Most abused domain registrars, Jul-Dec 2025 (continued)

Most abused domain registrars - number of domains

Rank	Jan - Jun 2025	Jul - Dec 2025	% Change	Registrar	Country
#1	40	3,883	9,608%	REGRU	Russia
#2	744	1,914	157%	Namecheap	United States
#3	385	1,680	336%	Dynadot Inc	United States
#4	614	738	20%	NICENIC International Group Co.	China
#5	275	555	102%	NameSilo	Canada
#6	146	516	253%	GoDaddy.com	United States
#7	434	384	-12%	Gname	Singapore
#8	65	347	434%	Spaceship, Inc.	United States
#9	1,354	320	-76%	PDR	India
#10	60	257	328%	Hostinger	Lithuania
#11	149	238	60%	Tucows	Canada
#12	334	223	-33%	WebNic.cc	Singapore
#13	-	159	New entry	CNOBIN Information Technology	China
#14	123	144	17%	Alibaba	China
#15	29	136	369%	Cloudflare, Inc.	United States
#16	70	120	71%	GMO Internet, Inc. d/b/a Onamae.com	Japan
#17	41	120	193%	Dominet (HK) Limited	Japan
#18	-	116	New entry	Name SRS	Sweden
#19	-	115	New entry	Porkbun	United States
#20	349	111	-68%	Sav.com	United States



LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Jan - Jun 2025	Jul - Dec 2025
United States	32.09%	39.91%
Russian Federation	1.72%	32.15%
China	15.22%	8.62%
Canada	7.92%	6.57%
Singapore	14.34%	5.03%
India	25.29%	2.65%
Lithuania	1.12%	2.13%
Japan	1.31%	1.99%
Sweden	-	0.96%

Networks hosting the most newly observed botnet C&Cs, Jul-Dec 2025

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 networks, it does not reflect how quickly 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.

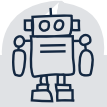
Increases continue across 6 networks

Over the past 12 consecutive months, increases in newly observed botnet C&Cs has been the dominant trend across the Top 20 networks. Notably, six networks have experienced continued increases throughout this entire period: digitalocean.com (+165%), contabo.de (+61%), m247.com (+45%), hetzner.com (+30%), microsoft.com (+18%), alibaba-inc.com (+16%), and amazon.com (+8%).

China-based network ctgserver.com, a new entrant in the January–June 2025 Botnet Threat Update, saw a +109% increase and climbed 11 places to rank #9, with 384 newly observed botnet C&Cs. Meanwhile, US-based colocrossing.com (a long-standing member of this sections' Top 20) saw a +126% increase, rising to rank #4 with 729 associated botnet C&Cs.

New entrants to the Top 20

Four new networks entered the Top 20 during this reporting period: virtualine.org (#6), as210558.net (#10), simplecarrier.net (#18), and cloudzy.com (#20). They were joined by aeza.net (#19), a recurring entrant that last appeared in the Top 20 in Q4 2023. For all of these networks, we assess they are operated for proliferating bulletproof hosting and cybercrime – consequently, they are included in our DROP and ASN-DROP lists.



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.

Networks hosting the most newly observed botnet C&Cs, Jul-Dec 2025 (continued)

Thanks for addressing botnet C&C abuse on your network

A note of recognition to claro.com.do, constant.com, and google.com who all dropped out of the Top 20 during this reporting period. In addition, reductions were observed across several networks, including huawei.com (-32%), neterra.net (-17%), ovh.net (-16%), and cheapy.host (-6%), the latter being a front company of CrazyRDP, a bulletproof hosting provider taken down by the Dutch police on November 12.

(*We assess railnet being a splinter of the virtualine.org bulletproof hosting operation, and have merged their associated numbers together in our tracking. Therefore, railnet is not a true departure.)

New entries

virtualine.org (#6), as210558.net (#10), simplecarrier.net (#18), aeza.net (#19), cloudzy.com (#20).

Departures

claro.com.do, constant.com, google.com (railnet*).

Rank	Jan - Jun 2025	Jul - Dec 2025	% Change	Network	Country
#1	1,291	1,502	16%	alibaba-inc.com	China
#2	539	1,428	165%	digitalocean.com	United States
#3	774	879	14%	tencent.com	China
#4	323	729	126%	colocrossing.com	United States
#5	502	543	8%	amazon.com	United States
#6	-	511	New entry	virtualine.org	United Kingdom
#7	441	461	5%	cloudinnovation.org	China
#8	269	390	45%	m247.com	Romania
#9	184	384	109%	ctgserver.com	China
#10	-	362	New entry	as210558.net	Germany
#11	215	346	61%	contabo.de	Germany
#12	220	285	30%	hetzner.com	Germany
#13	244	281	15%	uninet.net.mx	Mexico
#14	297	279	-6%	cheapy.host	United States
#15	222	261	18%	microsoft.com	United States
#16	365	250	-32%	huawei.com	China
#17	285	237	-17%	neterra.net	Bulgaria
#18	-	234	New entry	simplecarrier.net	United States
#19	-	214	New entry	aeza.net	Russia
#20	251	212	-16%	ovh.net	France
#20	-	212	New entry	cloudzy.com	United States

Networks hosting the most active botnet C&Cs, Jul-Dec 2025

Finally, let's review the networks that hosted the most active botnet C&Cs between July and December 2025. It's digitalocean.com leading this Top 20 with 175 active botnet C&Cs, followed by alibaba-inc.com with 150 active botnet C&Cs - both are large cloud hosting providers, equipped to do better.

Hosting providers in this ranking either have an abuse problem, or do not take the appropriate action when receiving abuse reports.

New entries

virtualine.org (#6),
optibounce.fun (#11),
neterra.net (#12),
cloudie.hk (#14),
changway.hk (#17),
bluevps.com (#17),
viettel.com.vn (#20).

Departures

cheapy.host, chinanet-idc-bj, ipxo.com, ovh.net, (railnet), simplecarrier.net.

(Some) hosting and cloud providers finally cleaning up

The second half of 2025 showed encouraging signs of progress. We saw the majority of hosting and cloud providers taking ownership of persistent botnet C&C abuse across their networks and implementing corrective measures to address these issues.

As a result, nearly all networks that appeared to be struggling with botnet C&C abuse earlier in 2025, experienced a decrease in active botnet C&C servers between July and December. These improvements were observed across all regions, from China, to the US and Europe. Well done, abuse desks – keep up the great work!

New entries and departures

As is typical for this Top 20 list, we see multiple new entries and departures each reporting period. The last six months were no exception, seeing seven different networks come and go. Some of the newcomers below you may recognize from the previous section, particularly virtualine.org, whose networks are a major abuse hotspot as this report went to press. changway.hk, an assessed front company of the "BearHost" bulletproof hosting operation, is no stranger to anti-abuse circles either.

Networks hosting the most active botnet C&Cs, Jul-Dec 2025 (continued)

Total number of active botnet C&Cs per network

Rank	Jan - Jun 2025	Jul - Dec 2025	% Change	Network	Country
#1	135	175	30%	digitalocean.com	United States
#2	277	150	-46%	alibaba-inc.com	China
#3	213	97	-54%	tencent.com	China
#4	76	87	14%	colocrossing.com	United States
#5	43	85	98%	contabo.de	Germany
#6	-	67	New entry	virtualine.org	United Kingdom
#7	74	42	-43%	amazon.com	United States
#8	33	31	-6%	ctgserver.com	China
#9	40	29	-28%	m247.com	Romania
#10	36	27	-25%	microsoft.com	United States
#11	-	26	New entry	optibounce.fun	United States
#12	-	24	New entry	neterra.net	Bulgaria
#13	18	23	28%	shuhost.com	China
#14	35	20	-43%	cloudinnovation.org	China
#14	34	20	-41%	google.com	United States
#14	-	20	New entry	cloudie.hk	China
#17	72	17	-76%	huawei.com	China
#17	-	17	New entry	changway.hk	China
#17	-	17	New entry	bluevps.com	Estonia
#20	24	14	-42%	spinservers.com	United States
#20	-	14	New entry	viettel.com.vn	Vietnam

That's all for now.

Stay safe, and we'll see you in July 2026!