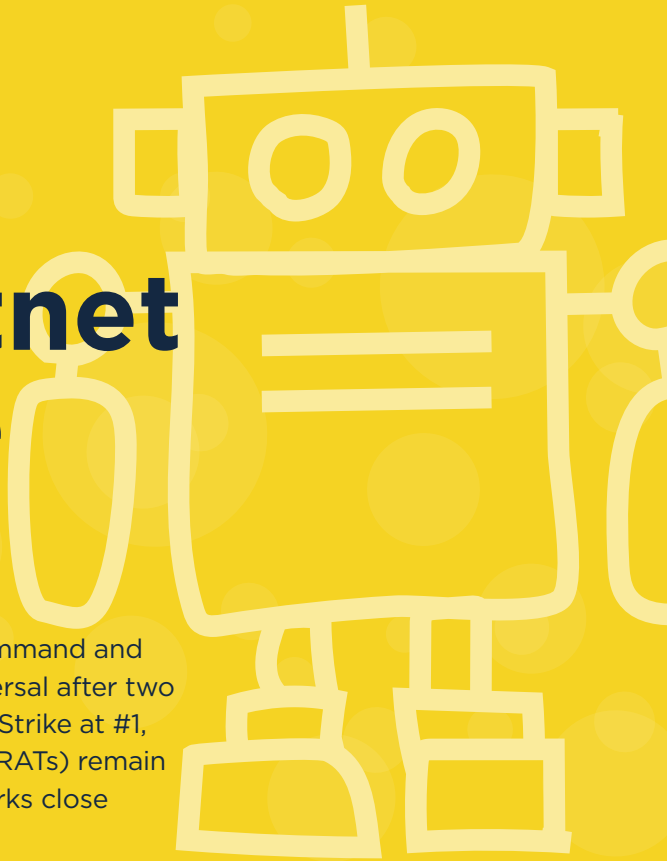
SPAMHAUS



Spamhaus Botnet Threat Update

January to June 2026

Between January and June 2026, the number of botnet command and control (C&C) servers fell sharply by -30%, a significant reversal after two consecutive periods of growth. Sliver has overtaken Cobalt Strike at #1, with Cobalt Strike dropping -68%. Remote Access Trojans (RATs) remain the dominant malware type at 46.1%, with pentest frameworks close behind at 38.6%.

In the domain space, the ccTLD .cn surged +771% to claim #3 in the most abused TLD table. Meanwhile, India-based registrar PDR saw a +901% increase in domains associated with botnet C&Cs.

But not all news is bad. REGRU delivered an impressive -90% reduction, and several major networks showed meaningful improvements in active botnet C&C numbers.

Welcome to the Spamhaus Botnet Threat Update.

About this report

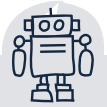
Spamhaus tracks both Internet Protocol (IP) addresses and domain names used by threat actors for hosting botnet command & control (C&C) servers. This data enables us to identify associated elements, including the geolocation of the botnet C&Cs, the malware associated with them, the top-level domains 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 2026

Between January and June 2026, Spamhaus identified 14,952 botnet C&Cs, a -30% decrease compared to the 21,425 observed in the previous period (July–December 2025). The monthly average fell from 3,571 to 2,492, bringing total activity back to levels last seen in the first half of 2024. After two consecutive periods of significant increase (+26% and +24%), this is the sharpest decline since 2023.

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%
Jan - Jun 2026	14,952	2,492	-30%



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 2026

The US holds on

The United States retains the top spot for the sixth consecutive period, but numbers of botnet C&Cs reduced from 5,040 to 4,244 (-16%). The Netherlands climbs to #2 (1,595 detections), despite a -24% decrease, while Germany remains at #4 (1,170 detections), both solidifying their roles as major hosting hubs for malicious infrastructure.

Botnet C&Cs decline across the globe...

... predominantly in the East. China dropped sharply from 3,371 to 1,409 C&Cs (-58%), falling from #2 to #3, a downward trend seen over multiple reporting periods. Singapore had a -46% decline (1,191 to 645), and Vietnam fell from 321 to 174 (-46%). The steepest single reduction in botnet C&Cs belongs to the Seychelles, which plunged from 647 to 209 (-68%), sliding from #8 to #14. Russia also continued its decline, dropping from 722 to 471 (-35%). France, by contrast, held almost perfectly steady: 533 to 525 (-2%).

Five new countries...

... enter the Top 20 this period: Cyprus (#9), Moldova (#12), Latvia (#15), Switzerland (#18), and the United Arab Emirates (#20). Their entry reflects the increasingly distributed nature of hosting abuse. Finland (+29%) and Canada (+6%) were the only countries to record meaningful increases. Meanwhile, Brazil, Bulgaria, Colombia, Mexico, and Poland all exited to the Top 20.

Geolocation Caveat:
Country rankings reflect where C&C servers are hosted, not where the operators are located. Threat actors routinely exploit jurisdictional complexity as part of their operational security.

New entries

Cyprus (#9) Moldova (#12), Latvia (#15), Switzerland (#18), United Arab Emirates (#20).

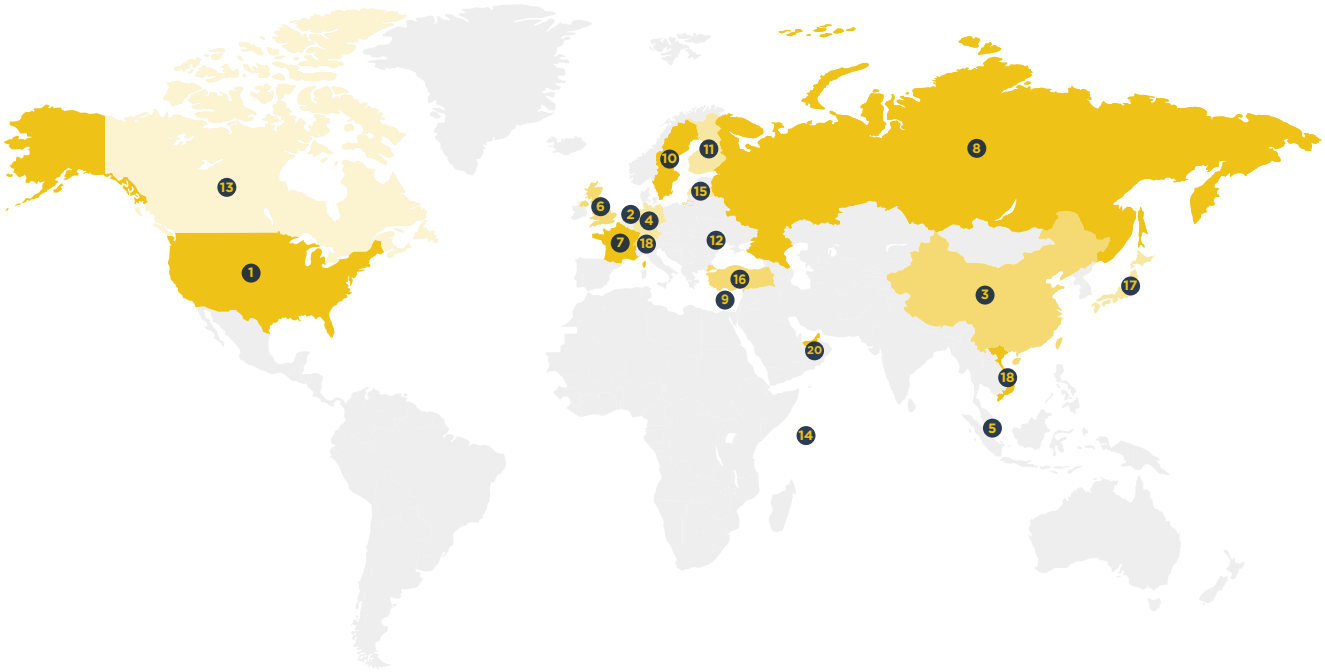
Departures

Brazil, Bulgaria, Columbia, Mexico, Poland.

Geolocation of botnet C&Cs, Jan-Jun 2026 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Jul - Dec 2025	Jan - Jun 2026	% Change
#1	United States	5,040	4,244	-16%
#2	Netherlands	2,104	1,595	-24%
#3	China	3,371	1,409	-58%
#4	Germany	1,528	1,170	-23%
#5	Singapore	1,191	645	-46%
#6	United Kingdom	667	539	-19%
#7	France	533	525	-2%
#8	Russia	722	471	-35%
#9	Cyprus	-	286	New entry
#10	Sweden	437	264	-40%
#11	Finland	197	254	+29%
#12	Moldova	-	231	New entry
#13	Canada	206	219	+6%
#14	Seychelles	647	209	-68%
#15	Latvia	-	188	New entry
#16	Turkey	271	187	-31%
#17	Japan	269	175	-35%
#18	Vietnam	321	174	-46%
#18	Switzerland	-	174	New entry
#20	UAE	-	143	New entry



Malware associated with botnet C&Cs, Jan-Jul 2026

Sliver dethrones Cobalt Strike

Sliver - an open-source, cross-platform penetration testing framework - has taken the #1 position from Cobalt Strike. Between January and June 2026 it climbed from 1,904 to 3,008 detections (+58%), while Cobalt Strike fell from 3,451 to 1,110 (-68%), dropping from #1 to #4. This is the largest percentage decline for Cobalt Strike since Spamhaus began tracking it. Whether this reflects successful disruption efforts, a tactical shift by threat actors, or both, the scale of the change is hard to ignore. Nevertheless, Cobalt Strike remains in the Top 20 and is still a significant threat.

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.

RATs and pentest frameworks dominate

Pentest framework malware grew from 33.7% to 38.6% of the Top 20. Combined, Sliver, Cobalt Strike, Havoc, and new entrant DeimosC2 account for 4,577 of the 12,022 detections across the Top 20 families. Remote Access Trojans (RATs) remain the largest malware type at 46.1% (up from 41.9%), led by AsyncRAT (#2), Remcos (#3), and DCRat (#6). Between them, RATs and pentest frameworks account for more than 84% of all Top 20 C&C activity.

Flubot makes an exit

Flubot, which had maintained a presence in the Top 20 has now departed entirely. As we've discussed in previous publications, FluBot used 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.

Malware associated with botnet C&Cs, Jan-Jun 2026 (continued)

... Five new malware families

PureRAT (#11): A commercially available .NET-based RAT first observed circulating on underground forums in 2023. PureRAT offers buyers a range of features including keylogging, screen capture, remote desktop access, credential harvesting, and file management. It is typically distributed via phishing emails disguised as business documents and includes anti-analysis features to avoid detection.

Tofsee (#15): A spambot first identified around 2013 and also known as Gheg. Tofsee primarily operates as a spam distribution platform but also has secondary capabilities for credential stealing and malware download. Despite its age, it continues to evolve and maintain an active infrastructure.

DeimosC2 (#18): An open-source C2 framework written in Go that supports multiple communication protocols. Like Sliver, DeimosC2 was originally developed as a legitimate red team tool, but has been adopted by malicious actors for post-exploitation command and control operations.

Socks5Systemz (#19): A backdoor that has been operating since at least 2016, primarily used to establish persistent, covert access to compromised systems. Once installed, it converts infected machines into SOCKS5 proxies, effectively renting out compromised systems to other threat actors seeking to anonymise their traffic.

NetSupportManagerRAT (#20): While technically this is a legitimate Remote Monitoring and Management (RMM) tool, attackers often hijack it to control computers without permission - hence it's frequently referred to as NetSupportManagerRAT. By leveraging genuine software, it evades detection, and it has been deployed in a range of campaigns, most notably through fake browser update lures.

New entries

PureRAT (#11), Tofsee (#15), DeimosC2 (#18), Socks5Systemz (#19), NetSupportManagerRAT (#20).

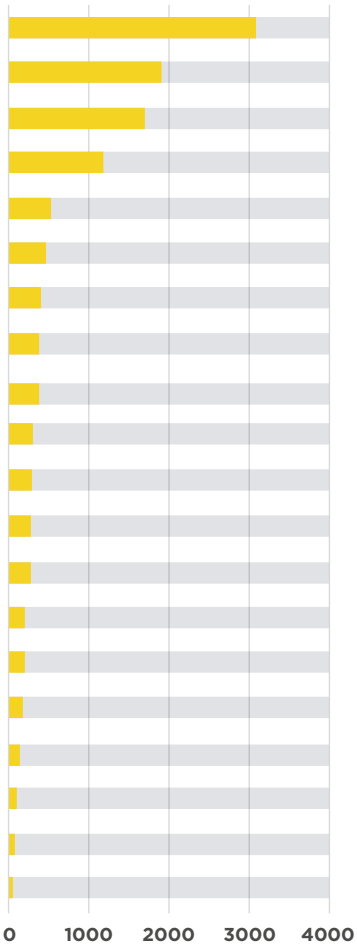
Departures

BianLian, Flubot, Latrodectus, PureLogs Stealer, and Rhadamanthys.

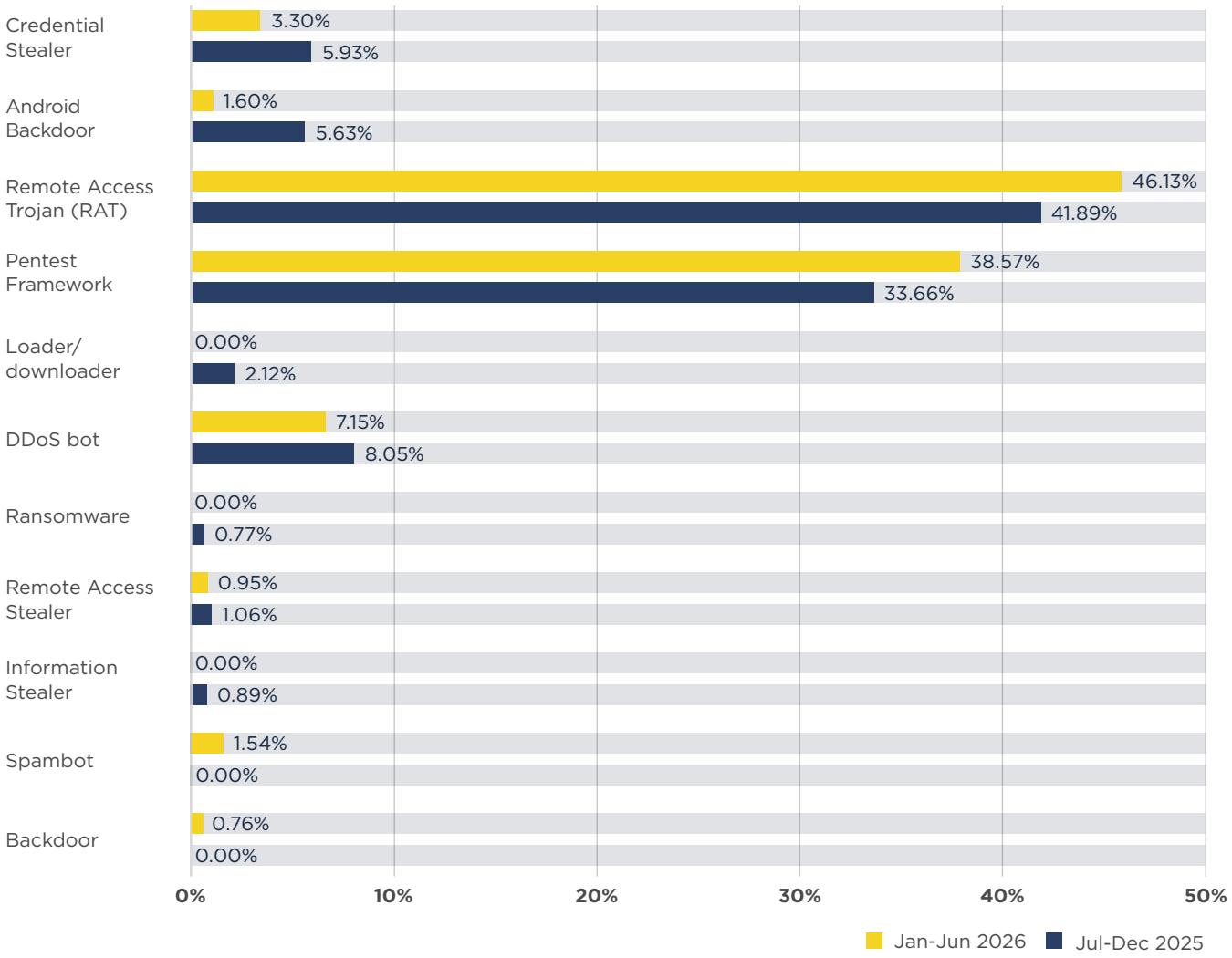
Malware associated with botnet C&Cs, Jan-Jun 2026 (continued)

Malware families associated with botnet C&Cs

Rank	Jul - Dec 2025	Jan - Jul 2026	% Change	Malware Family	Description
#1	1904	3008	+58%	Sliver	Pentest Framework
#2	2467	1951	-21%	AsyncRAT	RAT
#3	2269	1717	-24%	Remcos	RAT
#4	3451	1110	-68%	Cobalt Strike	Pentest Framework
#5	1023	594	-42%	Aisuru	DDoS Bot
#6	505	447	-11%	DCRat	RAT
#7	774	378	-51%	QuasarRAT	RAT
#8	515	357	-31%	Havoc	Pentest Framework
#9	430	356	-17%	ValleyRAT	RAT
#10	860	289	-66%	XWorm	RAT
#11	-	271	New entry	PureRAT	RAT
#12	380	254	-33%	Mirai	DDoS Bot
#13	151	247	+64%	Vidar	Credential Stealer
#14	271	190	-30%	Coper	Android Backdoor
#15	-	183	New entry	Tofsee	Spambot
#16	279	145	-48%	Joker	Credential Stealer
#17	185	113	-39%	Venom RAT	Remote Access Stealer
#18	-	102	New entry	DeimosC2	Pentest Framework
#19	-	90	New entry	Socks5Systemz	Backdoor
#20	-	65	New entry	NetSupportManagerRAT	RAT



Malware type comparisons



Most abused top-level domains, Jan-Jun 2026

Divergence at the top: .cn vs .ru

The Russian ccTLD, .ru, fell from 3,726 to just 630 botnet C&Cs (-83%), a direct reversal of the spike seen in the previous period when .ru was driven to #2 by js.clearfake campaign activity. Meanwhile .cn surged from 106 to 923 botnet C&Cs (+771%), jumping from #16 to #3. Whether this reflects a shift in registrant behaviour, a specific campaign cluster moving to .cn registered domains, or changes in registry vetting practices is worth investigating.

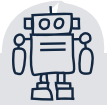
The .com surge dominates

At the top of the table, .com more than doubled from 4,287 to 9,285 (+117%) botnet C&Cs, consolidating its position at #1. However, this volume should be interpreted in context: with more than 158 million active domains, .com's botnet C&C concentration rate remains extremely low (around 0.006% of registered domains). The same caveat applies to .net (#4) and .org (#8).

New gTLDs signal opportunistic registration patterns

Six TLDs enter the Top 20 for the first time this period, all with notable concentration rates relative to their zone file sizes: .io (#7), .digital (#9), .lat (#12), .garden (#14), .lol (#15) and .tv (#18) - the Tuvalu ccTLD, frequently used for commercial purposes globally rather than by Tuvaluan registrants, and has historically attracted abuse.

The .icu gTLD grew +155% to 224 botnet C&C detections (#19), while .fun rose +118% to 218 (#20). Together, the influx of new gTLDs into the Top 20 reflects a pattern of botnet operators cycling across low-cost, high-volume registration options.



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, Jan-Jun 2026 (continued)

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.

New entries

io (#7), digital (#9), lat (#12), garden (#14), lol (#15), tv (#18).

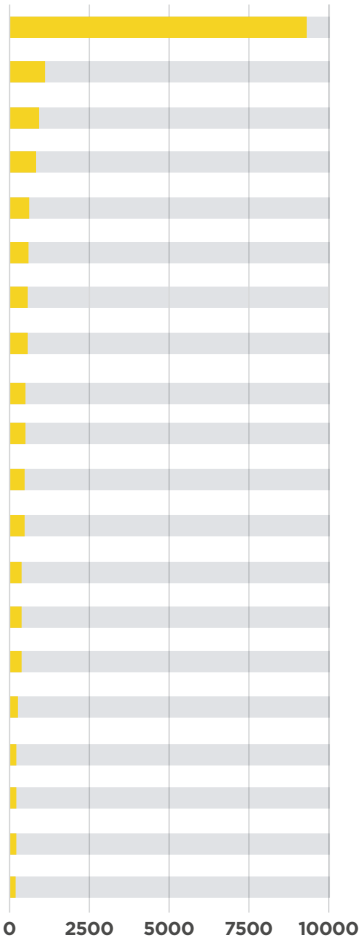
Departures

asia, cfd, click, qpon, sbs, shop.

Most abused top-level domains, Jan-Jun 2026

Top abused TLDs - number of domains

Rank	Jul - Dec 2025	Jan - Jun 2026	% Change	TLD	Type of TLD
#1	4287	9285	+117%	com	gTLD
#2	627	1126	+80%	top	gTLD
#3	106	923	+771%	cn	ccTLD
#4	539	826	+53%	net	gTLD
#5	3726	630	-83%	ru	ccTLD
#6	393	622	+58%	xyz	gTLD
#7	-	565	New entry	io	ccTLD
#8	341	555	+63%	org	gTLD
#9	-	498	New entry	digital	gTLD
#10	256	492	+92%	cc	ccTLD
#11	339	467	+38%	info	gTLD
#12	-	460	New entry	lat	gTLD
#13	111	388	+250%	cyou	gTLD
#14	-	372	New entry	garden	gTLD
#15	-	369	New entry	lol	gTLD
#16	238	259	+9%	online	gTLD
#17	133	236	+77%	site	gTLD
#18	-	227	New entry	tv	ccTLD
#19	88	224	+155%	icu	gTLD
#20	100	218	+118%	fun	gTLD



Most abused domain registrars, Jan-Jun 2026

PDR's extraordinary surge

PDR, an India-based registrar operating under the PublicDomainRegistry brand, exploded from 320 to 3,204 botnet C&C associated domains, rocketing from #9 to #2. This level of growth strongly suggests PDR has become a newly favoured platform for botnet operators, possibly due to permissive registration policies, weak KYC (Know Your Customer) processes, or promotional incentives.

Sav.com (#6) is another standout registrar that appears to have attracted significant malicious registrant activity in a short window, with an increase of +850%. We urge PDR and Sav.com to engage with Spamhaus directly to better understand the scope of abuse on their platform.

An unwelcome return to the top

Namecheap (+126%) displaces REGRU to reclaim the #1 position it has held in previous reports. Dynadot (#3) and Nicenic International Group (#4) both saw significant increases of +43% and +105% respectively. GoDaddy (#5) reappears with a sharp rise of +122%. As one of the world's largest registrars, GoDaddy has both the means and the obligation to do more.

REGRU's dramatic improvement

The best news this reporting period belongs to REGRU, the Russian registrar that previously held the #1 position with 3,883 botnet C&Cs associated with its domains. Between January and June 2026 it fell to #12 with a -90% reduction. This is a welcome improvement, and whatever steps REGRU has taken to address abuse on its platform deserve acknowledgement. Keep up the good work.

New entrants to the Top 20

Four registrars enter the Top 20 this period: China-based Wanshangyunji (Chengdu) Technology Co., Ltd. (#11), US-based Global Domain Group LLC (#13), plus Netherlands-based Realtime Register B.V. (#18) and Hosting Concepts B.V. (#19). Meanwhile, Hostinger (#9) continues to grow its presence with a +178% increase.

New entries

Wanshangyunji (Chengdu) Technology Co., Ltd. (#11), Global Domain Group LLC (#13), Realtime Register B.V. (#18), Hosting Concepts B.V. (#19).

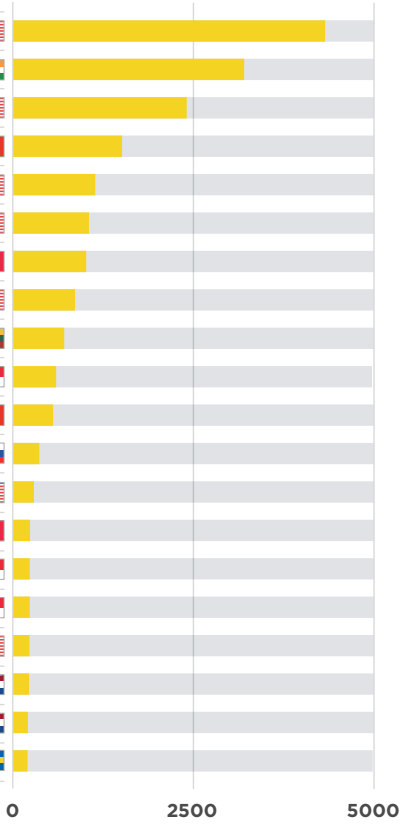
Departures

Alibaba, CNOBIN INFORMATION TECHNOLOGY, Dominet (HK) Limited, GMO Internet, Inc. d/b/a Onamae.

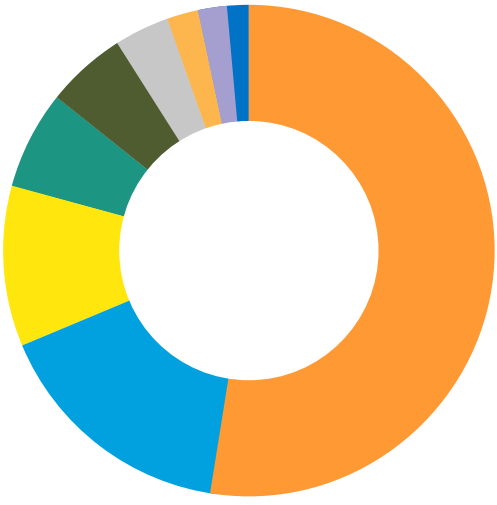
Most abused domain registrars, Jul-Dec 2025 (continued)

Most abused domain registrars - number of domains

Rank	Jan - Jun 2025	Jan - Jun 2026	% Change	Registrar	Country
#1	1914	4331	+126%	Namecheap	United States
#2	320	3204	+901%	PDR	India
#3	1680	2409	+43%	Dynadot Inc	United States
#4	738	1514	+105%	Nicenic International Group Co.	China
#5	516	1144	+122%	GoDaddy.com	United States
#6	111	1055	+850%	Sav.com	United States
#7	555	1034	+86%	NameSilo	Canada
#8	347	862	+148%	Spaceship, Inc.	United States
#9	257	715	+178%	Hostinger	Lithuania
#10	384	600	+56%	Gname	Singapore
#11	-	559	New entry	Wanshangyunji (Chengdu) Technology Co., Ltd.	China
#12	3883	369	-90%	REGRU	Russia
#13	-	296	New entry	Global Domain Group LLC	United States
#14	238	239	0%	Tucows	Canada
#15	223	235	+5%	WebNic.cc	Singapore
#16	136	231	+70%	Cloudflare, Inc.	Singapore
#17	115	220	+91%	Porkbun	United States
#18	-	211	New entry	Realtime Register B.V.	Netherlands
#19	-	200	New entry	Hosting Concepts B.V.	Netherlands
#20	116	198	+71%	Name SRS	Sweden



LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Jul - Dec 2025	Jan - Jun 2026
United States	39.91%	52.57%
India	2.65%	16.33%
China	8.62%	10.56%
Canada	6.57%	6.49%
Singapore	5.03%	5.43%
Lithuania	2.13%	3.64%
Netherlands	-	2.09%
Russia	32.15%	1.88%
Sweden	0.96%	1.01%

Networks hosting the most newly observed botnet C&Cs, Jan-Jun 2026

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.

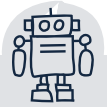
DigitalOcean takes #1

DigitalOcean has moved into the top position for newly observed C&Cs with 1,017 detections (-29%). Its continued presence across multiple consecutive reports points to a systemic rather than incidental problem.

Stark Industries arrives at #2...

...with 931 newly observed C&Cs, the most significant new entry. Stark Industries Solutions is a bulletproof hosting provider nominally registered in the United Kingdom but widely assessed to be operated for, and by, Russian-affiliated threat actors. It has been associated with DDoS infrastructure, state-sponsored intrusion campaigns, and broader cybercriminal activity. Its debut at #2 in this table is deeply concerning. Stark Industries Solutions is included in Spamhaus's DROP and ASN-DROP lists, and network operators are strongly encouraged to treat traffic to and from this ASN accordingly.

Cloudzy.com also enters the Top 20 at #9 with 291 newly observed C&Cs. Cloudzy has previously been assessed by threat intelligence researchers as a provider that knowingly or recklessly hosts malicious infrastructure.



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, Jan-Jun 2026 (continued)

Broad declines among major providers

Several major networks showed meaningful improvements this period. Tencent reduced newly observed botnet C&Cs from 879 to 302 (-66%), Alibaba from 1,502 to 588 (-61%), and cloudinnovation.org from 461 to 217 (-53%). Amazon also fell from 543 to 335 (-38%), and Microsoft from 261 to 172 (-34%). Meanwhile, contabo.de (+8%) and neterra.net (+13%) were the only networks to see increases.

While all of these organisations remain in the Top 20, their scale means even modest numbers represent significant impact, and the direction of travel is positive. Thanks for your efforts and keep up the great work.

New entrants globaltelehost.com (#18) and ghostynetworks.com (#19) are both providers with limited public profiles and their appearance in the Top 20 are worth monitoring.

New entries

stark-industries.solutions (#2), cloudzy.com (#9), globaltelehost.com (#18), ghostynetworks.com (#19).

Departures

cheapy.host, huawei.com, simplecarrier.net, uninet.net.mx.

Rank	Jul - Dec 2025	Jan - Jun 2026	% Change	Network	Country
#1	1428	1017	-29%	digitalocean.com	United States
#2	-	931	New entry	stark-industries.solutions	United Kingdom
#3	729	589	-19%	colocrossing.com	United States
#4	1502	588	-61%	alibaba-inc.com	China
#5	511	382	-25%	virtualine.org	United Kingdom
#6	346	374	+8%	contabo.de	Germany
#7	543	335	-38%	amazon.com	United States
#8	879	302	-66%	tencent.com	China
#9	-	291	New entry	cloudzy.com	United States
#10	362	273	-25%	as210558.net	Germany
#11	237	268	+13%	neterra.net	Bulgaria
#12	285	260	-9%	hetzner.com	Germany
#13	384	219	-43%	ctgserver.com	China
#14	461	217	-53%	cloudinnovation.org	China
#15	390	213	-45%	m247.com	Romania
#16	214	204	-5%	aeza.net	Russia
#17	261	172	-34%	microsoft.com	United States
#18	-	166	New entry	globaltelehost.com	Canada
#19	-	161	New entry	ghostynetworks.com	United States
#20	212	155	-27%	ovh.net	France

Networks hosting the most active botnet C&Cs, Jan-Jun 2026

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs between January and June 2026. Hosting providers in this ranking either have an abuse problem, or do not take the appropriate action when receiving abuse reports.

Positive reductions across 9 networks...

Between January and June 2026, only two networks saw increases in active botnet C&C: cloudinnovation.org (+30%), and Google (10%)

DigitalOcean (#1) reduced active botnet C&Cs by -56% to 77. Meanwhile, contabo.de showed the most significant improvement, dropping from 85 to just 14 active botnet C&Cs (-84%), and virtualine.org fell from 67 to 16 (-76%). Tencent (#5) also showed meaningful improvement with a -64% reduction. Nine networks from the previous period also exited the Top 20 entirely.

Thank you to all networks for your continued efforts, and we hope not to see another surge!

An unusually fast accumulation

Cloudzy.com enters the active table at #9, accumulating botnet C&C infrastructure within the same period it appeared in the newly observed table.

Please get in touch

Spamhaus encourages all networks appearing in this table to reach out proactively. Abuse desks are under enormous pressure, and we know that acting on every report is resource intensive. However, we can offer more than just abuse notifications. Working together, we can help prioritise and resolve the most impactful infrastructure faster.

New entries

vpsdedicated.net (#3), hosterdaddy.com (#7), cloudzy.com (#9), ghostynetworks.com (#11), ncck.com (#13), 1gservers.com (#15), as214351.com (#15), hetzner.com (#18), fibacloud.com (#19)

Departures

bluevps.com, changway.hk, cloudie.hk, colocrossing.com, huawei.com, neterra.net, optibounce.fun, shuhost.com, spinservers.com.

Networks hosting the most active botnet C&Cs, Jan-Jun 2026 (continued)

Total number of active botnet C&Cs per network

Rank	Jul - Dec 2025	Jan - Jun 2026	% Change	Network	Country
#1	175	77	-56%	digitalocean.com	United States
#2	150	71	-53%	alibaba-inc.com	China
#3	-	42	New entry	vpsdedicated.net	Slovenia
#4	42	41	-2%	amazon.com	United States
#5	97	35	-64%	tencent.com	China
#6	20	26	+30%	cloudinnovation.org	China
#7	27	25	-7%	microsoft.com	United States
#7	-	25	New entry	hosterdaddy.com	France
#9	31	24	-23%	ctgserver.com	China
#9	-	24	New entry	cloudzy.com	United States
#11	20	22	+10%	google.com	United States
#11	-	22	New entry	ghostynetworks.com	United States
#13	-	20	New entry	ncck.com	Netherlands
#14	29	19	-34%	m247.com	Romania
#15	-	17	New entry	1gservers.com	United States
#15	-	17	New entry	as214351.com	United Kingdom
#17	67	16	-76%	virtualine.org	United Kingdom
#18	-	15	New entry	hetzner.com	Germany
#19	85	14	-84%	contabo.de	Germany
#19	-	14	New entry	fibacloud.com	United States

That's all for now - stay safe!