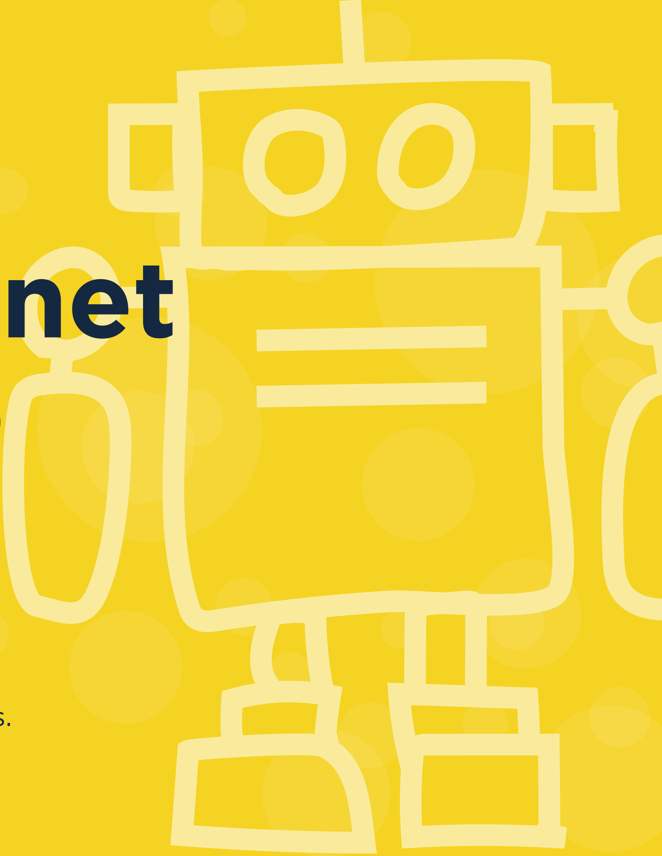
SPAMHAUS

Spamhaus Botnet Threat Update



January to June 2025

Between January and June 2025, botnet command and control (C&C) operators gained traction. Activity increased by 26%; the first increase we've observed for over 18 months. Five new malware families entered the Top 20, with Pentest frameworks continuing to dominate, owing to the ever-present Cobalt strike, and big increases from Sliver, Havoc and new entrant, DeimosC2. Meanwhile, we bid farewell to Latrodectus and Danabot, following the return of Operation Endgame 2, a takedown campaign that once again disrupted the botnet landscape!

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.

Spotlight

Operation Endgame is back!

In May 2025, a takedown operation, "Operation Endgame" 2.0 took place. This was part two of an international coalition of law enforcement agencies with one aim: to disrupt and dismantle botnet infrastructure and their operators.

Operation Endgame 2.0 targeted five malware strains including: Bumblebee, Latrodectus, Qakbot, DanaBot, Trickbot, and WarmCookie. The operation concentrated on initial access malware; a key component of cybercrime infrastructure that silently infiltrates systems before deploying ransomware.

A quick refresher of Operation Endgame

For those of you who are not overly familiar with Operation Endgame, here's a quick summary:

- In May 2024, an international law enforcement coalition coordinated the largest ever global botnet takedown.
- Seized over 100 servers and blocked more than 2,000 domains.
- Targeted IcedID, Smokeloader, SystemBC, Pikabot and Bumblebee, as well as some of the operators of the botnets.
- Seized 69 million euros in cryptocurrency from a suspect, obtained through criminal activities.
- More than ten thousand infected computer systems identified for remediation.
- Spamhaus played a key role in supporting remediation efforts of compromised accounts.

Operation Endgame Take 2

After the success of May 2024's Operation, and almost one year later, between May 19th and May 22nd 2025, Operation Endgame 2.0 announced it had dismantled key infrastructure behind malware used in ransomware attacks, targeting Bumblebee, Latrodectus, DanaBot, and WarmCookie. Indictments were also brought against individuals connected to Qakbot and Trickbot.

As a result, the operation successfully:

- Took down 300 servers worldwide, and neutralised 650 domains.

- Seized EUR 3.5 million in cryptocurrency.

- Issued international arrest warrants against 20 targets.

As a part of the remediation efforts, the Spamhaus Project once again supported the international coalition. Using data shared by authorities, we contacted email service providers, hosting companies, and other parties responsible for the compromised accounts. The only request to victims was simple: "reset your password and secure your account."

If you haven't already, we encourage providers to download their data. For more information see our Operation Endgame Remediation page.

The Endgame for Latrodectus and Danabot

The good news doesn't stop there. Following "Operation Endgame 2.0", both Latrodectus and DanaBot have dropped out of the Top 20 malware families associated with botnet C&Cs in this report!

Both malware families have a common tactic - to steal information:

- **Latrodectus** - A malware loader delivered via malicious email attachments in phishing campaigns, designed to execute commands, steal data, deploy additional malware, and maintain persistence through scheduled tasks and encrypted C&C communication.

- **DanaBot** – A modular banking trojan spread through phishing emails, designed to steal banking credentials, browser data, and personal information.

Next, we expect BumbleBee and WarmCookie to exit the Top 20 malware families associated with botnet C&Cs. Watch this space for the Botnet Threat Update, July - December 2025.

Number of botnet C&Cs observed, Jan-Jun 2025

Over the last six months, Spamhaus identified 17,258 botnet C&Cs, compared to 13,720 in the previous six months. This represents a +26% increase. From July to December 2024, the monthly average was 2,287 botnet C&Cs; this increased to 2,876 from January to June 2025.

Period	No. of Botnets	6 Month Average	% Change
Jan - Jun 2023	16,796	2,799	
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%

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 2025

United States closes in on China

Following a 54% increase in activity, the United States has narrowed the gap with China (#1), now ranking #2 for countries hosting botnet C&C servers (3,512). The difference between the two is just 21 servers, meaning the United States now hosts only 0.6% fewer botnet C&Cs than China (3,533).

With China seeing 0% change this reporting period, it may not hold the top spot for much longer. It's time for the United States to do better; this isn't a title anyone wants to claim!

New entries

Dominican Republic (#13), Seychelles (#17), Brazil (#19), Turkey (#20).

Departures

Argentina, Colombia, Korea (Republic of), Spain.

Mixed results across the globe

Only five countries had a decrease in botnet C&C servers this quarter. The most notable drops came from Bulgaria (-40%), Mexico (-25%), and Morocco (-20%).

On the flip side, several countries saw sharp increases. Germany led with an increase of +99%, followed by Singapore (+86%) and the Netherlands (+80%).

This quarter also marked the return of the Seychelles (#17) to the Top 20, last seen in Q4 2021.

Turbulent times for Finland

Botnet C&C activity in Finland has fluctuated over recent years. In Q3 2023, the country ranked #14 with a -39% decrease. The trend switched in Q4 with a +31% increase, although its position remained unchanged.

In the first half of 2024, botnet C&C activity was down by -25%, and Finland slipped into #16. However, this was followed by a +58% increase in the second half of 2024 pushing them up to #12.

Between January and June 2025, Finland has once again dropped to #15, with a -14% decrease in activity. Will this up-and-down pattern continue? Stay tuned for the next report.

Geolocation of botnet C&Cs, Jan-Jun 2025 (continued)

Bulgaria and Mexico, keep going!

In the Botnet Threat Update July - December 2024, Bulgaria saw a -24% decrease in botnet C&Cs to 544, while Mexico reported a -33% drop to 334. The good news is, the downward trend has continued this reporting period, with Bulgaria decreasing a further -40% and Mexico -25%.

Both countries are clearly making efforts to curb this malicious activity. While there's still a long way to go, it's encouraging to see consistent progress in the right direction.

Adiós, Argentina!

After a short appearance in the Top 20 in 2021, Argentina re-entered the Top 20 at #13 in the January–June 2024 report. Fortunately, this return was also brief, as Argentina has since dropped out of the Top 20 again. Here's hoping it stays out for good!

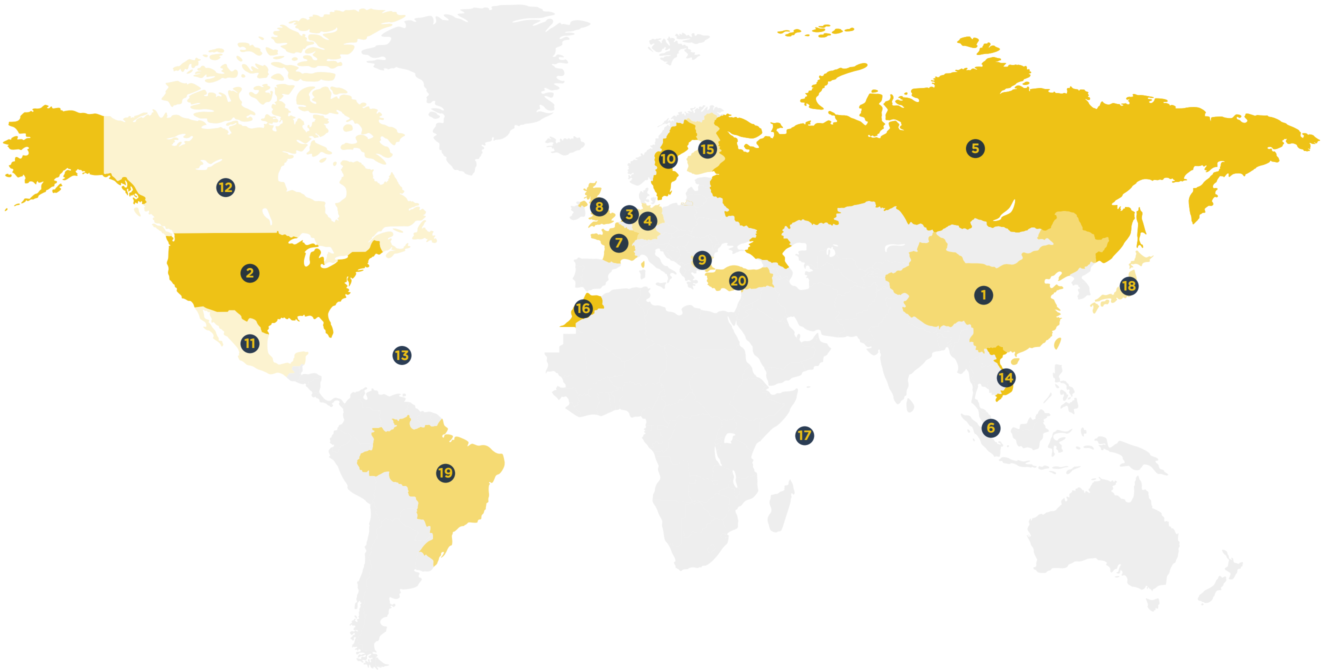
Colombia, Korea (the Republic of), and Spain also departed from the Top 20 this reporting period.

Geolocation of botnet C&Cs, Jan-Jun 2025 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Jul - Dec 2024	Jan - Jun 2025	% Change
#1	China	3,535	3,533	0%
#2	United States	2,286	3,512	54%
#3	Netherlands	782	1,406	80%
#4	Germany	657	1,307	99%
#5	Russia	1,125	1,022	-9%
#6	Singapore	382	712	86%
#7	France	279	470	68%
#8	United Kingdom	317	329	4%
#9	Bulgaria	544	327	-40%
#10	Sweden	275	284	3%

Rank	Country	Jul - Dec 2024	Jan - Jun 2025	% Change
#11	Mexico	334	251	-25%
#12	Canada	128	191	49%
#13	Dominican Rep.	-	189	New entry
#14	Vietnam	122	188	54%
#15	Finland	213	183	-14%
#16	Morocco	213	170	-20%
#17	Seychelles	-	167	New entry
#18	Japan	136	163	20%
#19	Brazil	-	154	New entry
#20	Turkey	-	146	New entry



Malware associated with botnet C&Cs, Jan-Jun 2025

Five new malware families

While these malware families are not new to the threat landscape, they're making their first appearance as a Top 20 entrant in our Botnet Threat Updates: XWorm (#9), ValleyRAT (#12), Chaos (#16), Joker (#18), and DeimosC2 (#19). Here's a quick introduction to each:

- **Xworm** is a sophisticated modular Remote Access Trojan (RAT). It first appeared in 2022 as a Malware-as-a-Service. It is designed to give cybercriminals remote, unauthorized access to infected machines, steal sensitive information, and deploy a range of malicious activity.
- **ValleyRat** is a RAT first seen in early 2023. Distributed through phishing emails or malicious downloads, it is used to provide remote attackers with unauthorized access and control over infected machines.
- **Chaos** is a ransomware that entered the threat landscape in June 2021. It is known for being a ransomware builder, allowing cybercriminals to build custom variants of ransomware without much difficulty.
- **Joker** is a well-known Android malware that exploits Google's app store to spread its malicious software. The malware acts as a credential stealer, capable of harvesting sensitive information including contact details, device data, WAP services, and SMS messages.
- **DeimosC2** is categorized as a pentest framework. Like Cobalt Strike, it is a legitimate tool designed for security testing that threat actors also use to execute malicious activities.

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.

Pentest frameworks gain popularity

Pentest Frameworks now make up 43% of all malware in the Top 20. This reporting period saw significant increases from Sliver (+138%) and Havoc (+139%), and a new entrant, DeimosC2 at #19. Cobalt Strike still remains the most prevalent pentesting framework, representing 30% of malware in the Top 20.

Remote Access Trojans (RATs) continue to rise, now accounting for 39.8% of malware associated with botnet C&Cs.

Malware associated with botnet C&Cs, Jan-Jun 2025 (continued)

Endgame for Latrodectus and Danabot

This May, saw the return of “Operation Endgame 2.0” and the takedown of several more botnets, including Latrodectus and Danabot. Consequently, these malware families have dropped out of the Top 20 malware associated with botnet C&Cs this reporting period.

Brute Ratel C4, FakeUpdates, and Stealc also departed from the Top 20 malware associated with Botnet C&Cs this reporting period.

Does Flubot still exist?

Despite 741 botnet C&C detections in the latest report, the short answer is: not really.

As we’ve explained in previous reports, FluBot relied on a “FastFlux” technique to host its botnet C&Cs. That same botnet infrastructure still serves as C&Cs for other malware families, for example, Teambot.

For consistency in our internal tracking, we continue to label the associated infrastructure as FluBot, but this is effectively hosting all kinds of other botnet C&C activity.

New entries

XWorm (#9), ValleyRAT (#12), Chaos (#16), Joker (#18), DeimosC2 (#19).

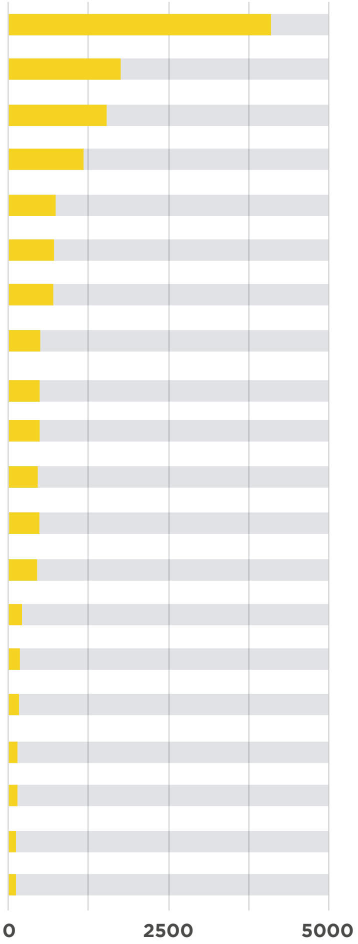
Departures

Brute Ratel C4, DanaBot, FakeUpdates, Latrodectus, Stealc.

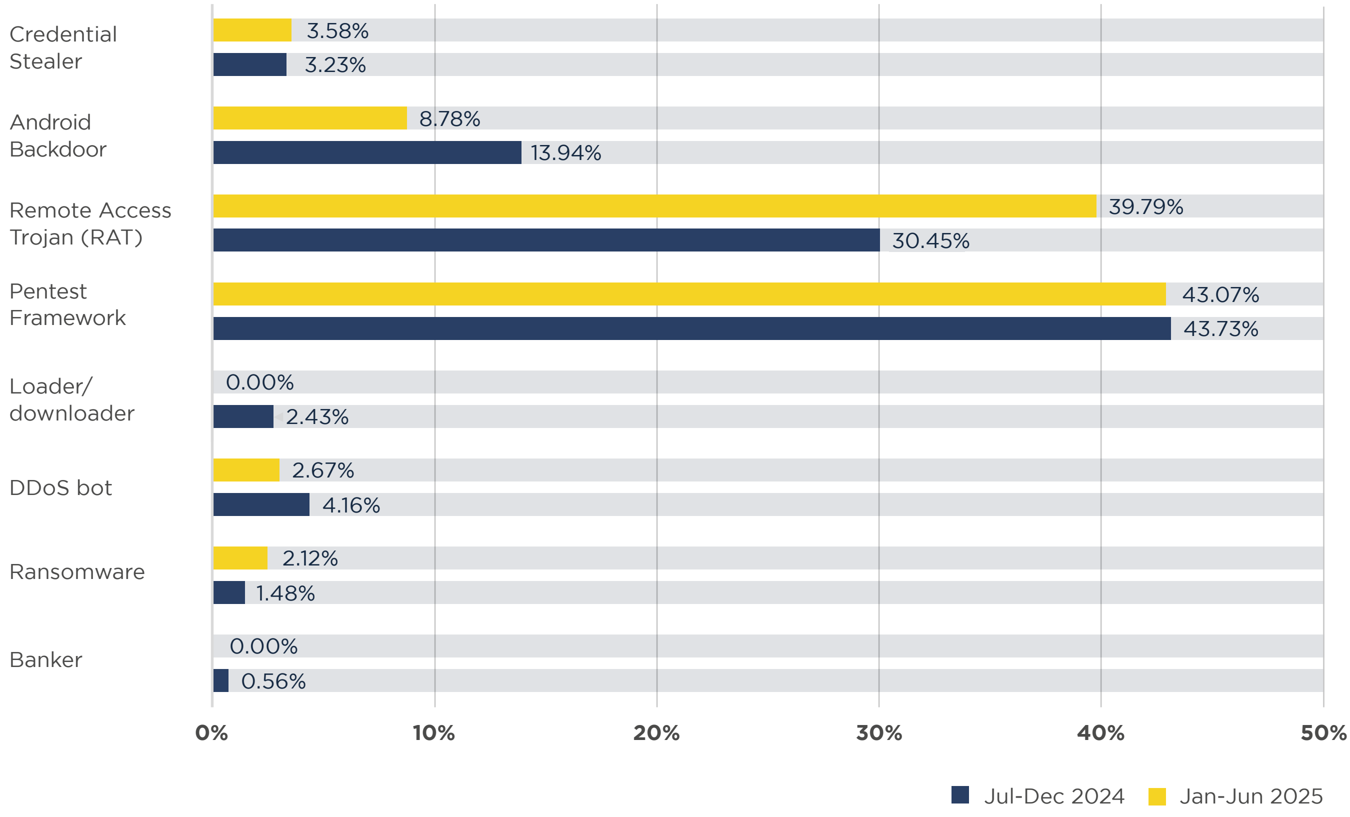
Malware associated with botnet C&Cs, Jan-Jun 2025 (continued)

Malware families associated with botnet C&Cs

Rank	Jul - Dec 2024	Jan - Jun 2025	% Change	Malware Family	Description
#1	3,737	4,107	10%	Cobalt Strike	Pentest Framework
#2	725	1,756	142%	AsyncRAT	Remote Access Trojan (RAT)
#3	1,257	1,533	22%	Remcos	Remote Access Trojan (RAT)
#4	495	1,177	138%	Sliver	Pentest Framework
#5	1,025	741	-28%	Flubot	Android Backdoor
#6	298	630	111%	DCRat	Remote Access Trojan (RAT)
#7	482	562	17%	QuasarRAT	Remote Access Trojan (RAT)
#8	192	458	139%	Havoc	Pentest Framework
#9	-	394	New entry	XWorm	Remote Access Trojan (RAT)
#10	191	382	100%	Rhadamanthys	Credential Stealer
#11	427	361	-15%	Mirai	DDoS Bot
#12	-	316	New entry	ValleyRAT	Remote Access Trojan (RAT)
#13	232	267	15%	Coper	Android Backdoor
#14	175	180	3%	Hook	Android Backdoor
#15	152	175	15%	Bianlian	Ransomware
#16	-	112	New entry	Chaos	Ransomware
#17	279	108	-61%	RedlineStealer	Remote Access Trojan (RAT)
#18	-	103	New entry	Joker	Credential stealer
#19	-	87	New entry	DeimosC2	Pentest Framework
#20	86	86	0%	NjRAT	Remote Access Trojan (RAT)



Malware type comparisons



Most abused top-level domains, Jan-Jun 2025

New entry .digital #3

The TLD .digital is operated by Identity Digital, a registry formerly known as Donuts based in the United States. This gTLD has been actively running promotions to drive registrations, with domains priced at $1.94 (at the time of writing). As is often the case, where domain prices are low, there is an increased risk of criminal activity; 534 botnet C&C servers were associated with .digital between January and June 2025.

We recommend Identity Digital works closely with its registrars to improve vetting and registration procedures, to help mitigate the risk of abuse.

More highs than lows

This report brings encouraging news for the Top 20 most abused top-level domains, with only five TLDs reporting moderate increases in abuse.

Meanwhile, eight registries achieved reductions in the number of associated botnet C&Cs using their TLDs, including .online (#18), .click (#19), and .site (#20), which all experienced reductions exceeding 65%. Additionally, seven TLDs departed from our Top 20! We'd like to thank all registries that have successfully reduced the number of associated botnet C&Cs using their TLDs.

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, between January and June 2025, **.com** had more than **155m** domains, of which 0.00147% were associated with botnet C&Cs. Meanwhile, **.digital** had approximately **157k** domains, of which 0.34022% 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.

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 2025 (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. 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

digital (#3), tech (#6), live (#11), today (#11), run (#15), cc (#16), fun (#17).

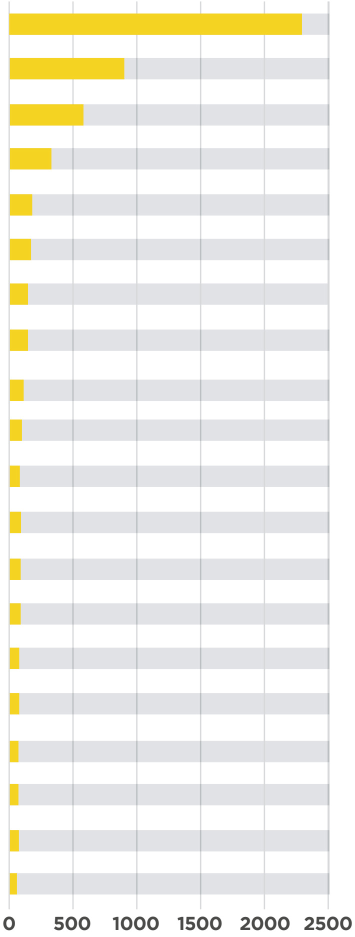
Departures

biz, buzz, cloud, cfd, monster, sbs, store.

Most abused top-level domains, Jan-Jun 2025

Top abused TLDs - number of domains

Rank	Jul - Dec 2024	Jan - Jun 2025	% Change	TLD	Type of TLD
#1	1,757	2,286	30%	com	gTLD
#2	1,514	838	-45%	top	gTLD
#3	-	534	New entry	digital	gTLD
#4	331	362	9%	xyz	gTLD
#5	230	175	-24%	net	gTLD
#6	-	164	New entry	tech	gTLD
#7	110	149	35%	info	gTLD
#8	186	147	-21%	shop	gTLD
#9	157	108	-31%	org	gTLD
#10	84	97	15%	ru	ccTLD
#11	-	80	New entry	today	gTLD
#11	-	80	New entry	live	gTLD
#13	67	78	16%	icu	gTLD
#13	91	78	-14%	cn	ccTLD
#15	-	61	New entry	run	gTLD
#16	-	60	New entry	cc	ccTLD
#17	-	50	New entry	fun	gTLD
#18	143	49	-66%	online	gTLD
#19	141	47	-67%	click	gTLD
#20	111	35	-68%	site	gTLD



Most abused domain registrars, Jan-Jun 2025

PDR steals #1...again

We have observed an enormous +268% increase of newly registered botnet C&C domains at Indian-based domain registrar, PDR, reclaiming the top spot for the second time. Registrations have more than tripled(!) from 368 in the previous six months, to 1,354 between January and June 2025.

As a result, there was a noticeable overall increase in the number of botnet C&Cs associated with registrars operating out of India, now representing 25.3%.

The situation in the US and China continues to improve

Although US domain registrars continue to dominate the Top 20, the percentage of domain registrations has decreased further this reporting period, dropping from 41.7% to 32.1%. This was largely due to decreases at GoDaddy.com (-67%), Dynadot (-53%), Spaceship, Inc. (-53%), and Namecheap (-51%).

Similarly, the percentage of domain registrations from China also fell, from 24.1% to 15.2%, placing it third, behind India. Great efforts from NiceNic (-62%) for its contribution to curbing abusive domain registrations.

Sad times for Sav

Despite 15 consecutive months reducing the number of botnet C&C operators registering through them, Sav experienced a +297% increase this reporting period, jumping eight places to #6 with 349 botnet C&C operators reported.

We hope this domain registrar can swiftly steer their ship back on course!

New entries

SPRINTNAMES-RU (#16),
Dominet (HK) Ltd (#17),
eName Technology Co., Ltd (#19),
Cloudflare (#20).

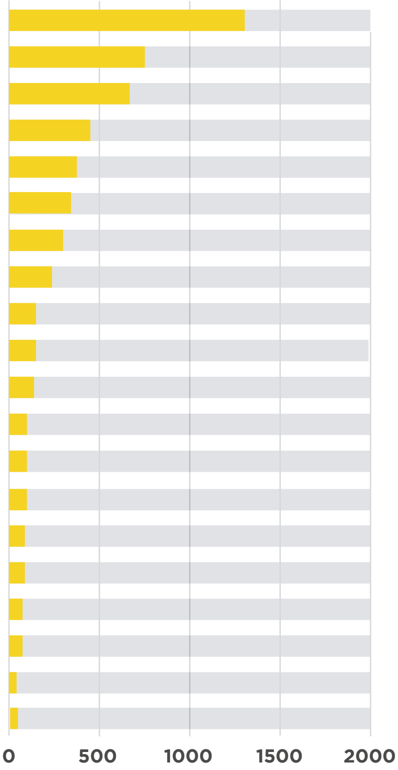
Departures

eNom, Eranet, Hosting Concepts, RU-Center.

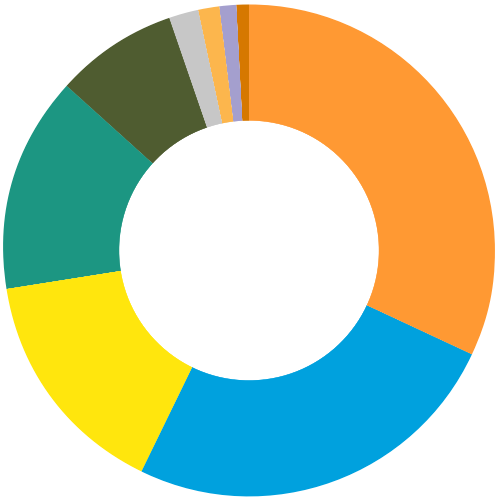
Most abused domain registrars, Jan-Jun 2025 (continued)

Most abused domain registrars - number of domains

Rank	Jul - Dec 2024	Jan - Jun 2025	% Change	Registrar	Country
#1	368	1,354	268%	PDR	India
#2	1,513	744	-51%	Namecheap	United States
#3	1,636	614	-62%	Nicenic	China
#4	164	434	165%	Gname	Singapore
#5	815	385	-53%	Dynadot Inc	United States
#6	88	349	297%	Sav	United States
#7	223	334	50%	WebNic	Singapore
#8	805	275	-66%	NameSilo	Canada
#9	159	149	-6%	Tucows	Canada
#10	437	146	-67%	GoDaddy	United States
#11	45	123	173%	Alibaba	China
#12	185	70	-62%	GMO	Japan
#13	139	65	-53%	Spaceship, Inc.	United States
#14	225	60	-73%	Hostinger	Lithuania
#15	45	53	18%	Arsys Internet, S.L. dba NICLINE.COM	Spain
#16	-	52	New entry	SPRINTNAMES-RU	Spain
#17	-	41	New entry	Dominet (HK) Limited	China
#18	60	40	-33%	REGRU	Russia
#19	-	37	New entry	eName Technology Co., Ltd.	China
#20	-	29	New entry	Cloudflare, Inc.	United States



LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Jan - Jun 2025	Jul - Dec 2024
🟧 United States	32.09%	41.68%
🟦 India	25.29%	5.13%
🟨 China	15.22%	24.14%
🟩 Singapore	14.34%	5.39%
🟫 Canada	7.92%	14.19%
⬜ Spain	1.96%	0.63%
🟧 Japan	1.31%	2.58%
🟪 Lithuania	1.12%	3.13%
🟧 Russian Federation	0.75%	1.38%
🟦 Netherlands	0%	1.76%

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

Increases across 11 networks

After 12 months of positive reductions throughout 2024, disappointingly, more than half of the Top 20 networks experienced increases over the last six months. Increases range from +2% for China-based alibaba-inc.com, to a very disappointing +78% for Romanian-based m247.com, which climbed eight places to #10.

Among the other networks included was amazon.com, which after a -19% reduction between July and December 2024, experienced a +70% increase between January and July 2025, taking them to #4.

New at #8: Who is cheapy.host?

US-based web hosting provider cheapy.host has made its debut in the Top 20 this reporting period, entering at #8 by hosting 297 newly observed botnet C&Cs.

Cheapy.host promotes itself as offering "excellence in web hosting without compromising your budget." But with a significant rise in botnet C&Cs on its network, it's clearly time to review their customer vetting processes. Having only been operating since May 2024, is cheapy.host a network we'll be seeing more of?

Thanks for your efforts to tackle botnet C&C abuse on your network

There were reductions from five networks including, colocrossing.com (-26%), uninet.net.mx (-26%), tencent.com (-24%), cloudinnovation.org (-11%), and google.com (-9%).

With a special nod to baxet.ru, limenet.io, select.ru, and telefonica.com.ar, who all dropped out of the Top 20.

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

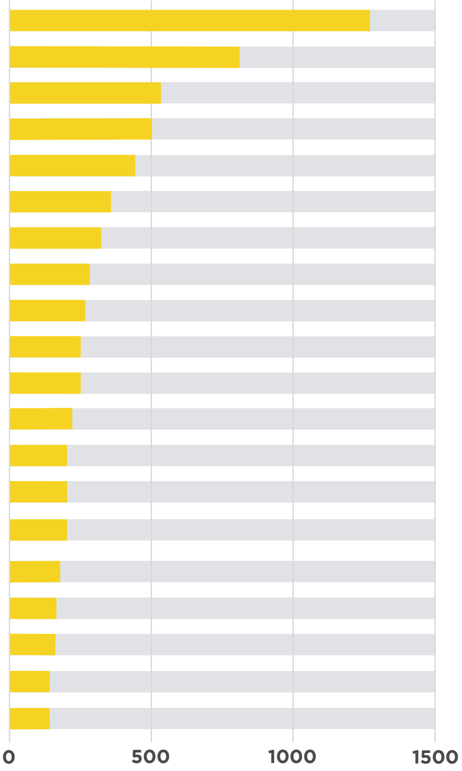
cheapy.host (#8), railnet (#17) claro.com.do (#19), ctgserver.com (#20).

Departures

baxet.ru, limenet.io, select.ru, telefonica.com.ar.

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

Rank	Jul - Dec 2024	Jan - Jun 2025	% Change	Network	Country
#1	1,269	1,291	2%	alibaba-inc.com	China
#2	1,019	774	-24%	tencent.com	China
#3	352	539	53%	digitalocean.com	United States
#4	295	502	70%	amazon.com	United States
#5	496	441	-11%	cloudinnovation.org	China
#6	249	365	47%	huawei.com	China
#7	434	323	-26%	colocrossing.com	United States
#8	-	297	New entry	cheapy.host	United States
#9	231	285	23%	neterra.net	Bulgaria
#10	151	269	78%	m247.com	Romania
#11	185	251	36%	ovh.net	France
#12	331	244	-26%	uninet.net.mx	Mexico
#13	174	222	28%	microsoft.com	United States
#14	241	220	-9%	google.com	United States
#14	184	220	20%	hetzner.com	Germany
#16	145	215	48%	contabo.de	Germany
#17	-	208	New entry	railnet	United States
#18	165	204	24%	constant.com	United States
#19	-	189	New entry	claro.com.do	Dominican Rep.
#20	-	184	New entry	ctgserver.com	China



Networks hosting the most active botnet C&Cs, Jan-Jun 2025

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs between January and June 2025. alibaba-inc.com leads this Top 20, with 277 active botnet C&Cs, followed by tencent.com with 213 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.

Increases across 9 networks

In total, the Top 20 providers with botnet C&C issues had 1,257 active botnet C&Cs on their networks between January and June 2025. Of these, three US-based providers suffered significant increases, including digitalocean.com (+366%), colocrossing.com (+230%) and amazon.com (+222%). Meanwhile, Romanian-based provider m247.com saw a +264% increase.

We call upon these network operators to quickly respond to abuse reports and work with Spamhaus to reduce the amount of botnet C&C abuse on their networks.

Large scale providers – how can we better work together

As you can see, many global names in hosting can be found in this Top 20, which is disappointing to see. We recognize the strain abuse desks are under and we want to work together with organizations to help manage abuse on their networks.

Please – reach out to Spamhaus' Community and Industry Outreach. We provide abuse reports, but we can do so much more.

New entries

railnet (#7), microsoft.com (#10), spinservers.com (#14), chinanet-idc-bj (#15), cheapy.host (#16), shuhost.com (#17), ipxo.com (#19).

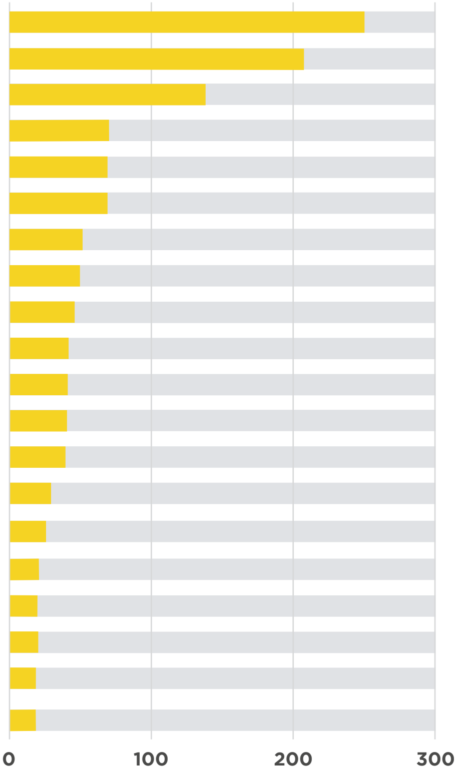
Departures

blnwx.com, changway.hk, hetzner.com, macloud.ru, neterra.net, stark-industries.solutions, ucloud.cn.

Networks hosting the most active botnet C&Cs, Jan-Jun 2025 (continued)

Total number of active botnet C&Cs per network

Rank	Jul - Dec 2024	Jan - Jun 2025	% Change	Network	Country
#1	172	277	61%	alibaba-inc.com	China
#2	85	213	151%	tencent.com	China
#3	29	135	366%	digitalocean.com	United States
#4	23	76	230%	colocrossing.com	United States
#5	23	74	222%	amazon.com	United States
#6	47	72	53%	huawei.com	China
#7	-	52	New entry	railnet	United States
#8	24	43	79%	contabo.de	Germany
#9	11	40	264%	m247.com	Romania
#10	-	36	New entry	microsoft.com	United States
#11	65	35	-46%	cloudinnovation.org	China
#12	35	34	-3%	google.com	United States
#13	18	33	83%	ctgserver.com	China
#14	-	24	New entry	spinservers.com	United States
#15	-	23	New entry	chinanet-idc-bj	China
#16	-	20	New entry	cheapy.host	United States
#17	18	18	0%	simplecarrier.net	United States
#17	-	18	New entry	shuhost.com	China
#19	18	17	-6%	ovh.net	France
#19	-	17	New entry	ipxo.com	United Kingdom



That's all for now.

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