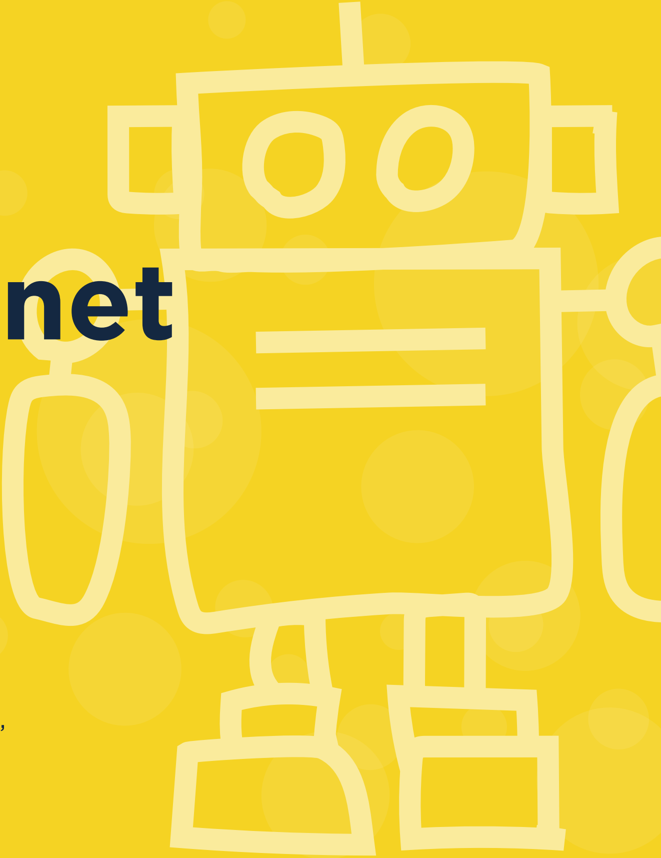
SPAMHAUS

Spamhaus Botnet Threat Update



Q4 2023

The number of botnet command and control (C&C) servers soared in Q4 2023, growing by +16%. Activity increased globally, with a significant spike in Bulgaria, but it was China, the United States, and Russia leading the pack. Along with Cobalt Strike contributing to the increase in numbers, there was a growing popularity in Remote Access Trojans (RATs), most notably QuasarRAT, which experienced a 341% increase. And finally, there's disappointing news relating to a surge in active botnet C&Cs across big-name networks.

Welcome to the Spamhaus Botnet Threat Update Q4 2023.

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

Despite the duck's demise, Pikabot and DarkGate thrive!

It's been nearly six months since the Qakbot takedown, involving an internationally coordinated effort led by the Federal Bureau of Investigation (FBI). With the infamous malware's infrastructure finally dismantled, we all took a sigh of relief. Albeit, this was short-lived. Two other malware threats - Pikabot and DarkGate - quickly emerged as new adversary favorites.

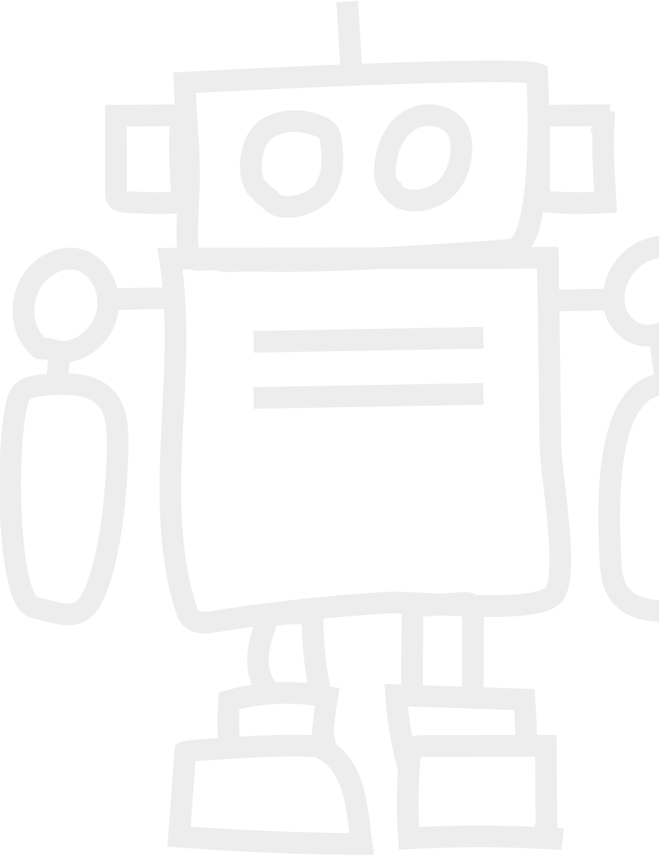
How do these threats work?

Pikabot is a backdoor, while DarkGate is a Remote Access Trojan (RAT) primarily acting as a downloader. But they have one thing in common - the ability to download, and execute, additional payloads to the infected machine. It's for this reason miscreants choose these malware families to deliver malicious files to their victims. A feature that would appeal to those whose preference was previously Qakbot.

TR Group picks Pikabot

For the notorious Conti hacker group affiliate, TR (TA577), Pikabot has become the preferred malware. For several months, Spamhaus researchers have observed a significant increase in spam from the TR group, occurring multiple times per week. So it comes as no surprise to see Pikabot enter this report as a Top 10 malware associated with botnet command and controllers (C&Cs). So what's driving this change?

It is safe to assume this change in TR's behaviour is connected to the Qakbot takedown, forcing this hacker group to switch tactics. DarkGate filled the void for a brief period before finally settling on Pikabot to conduct their weekly malicious campaigns.



Will Pikabot remain TR's default loader?

For the moment, it appears that way. Given its robustness and complexity, this malware is undoubtedly a top candidate for Qakbot's successor. Even so, let's hope its reign is brief!

Spamhaus researchers will continue to monitor insights regarding these malware's activities - keep an eye on our social media for updates.

Number of botnet C&Cs observed, Q4 2023

In Q4 2023, Spamhaus identified 8,174 botnet C&Cs compared to 7,052 in Q3 2023. This was a +16% increase quarter on quarter. The monthly average increased from 2,351 in Q3 to 2,725 botnet C&Cs per month in Q4 2023.

Quarter	No. of Botnets	Quarterly Average	% Change
Q1 2023	8,358	2,786	+23%
Q2 2023	8,438	2,813	+1%
Q3 2023	7,052	2,351	-16%
Q4 2023	8,174	2,725	+16%

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, Q4 2023

China strengthens its position

China remains in pole position, having knocked The U.S.A. off the top spot in Q3. In Q4, the number of botnets hosted in the country continued to increase by a further 35% to 2,125, showing no signs of slowing down.

The botnet superpowers return

Alongside China, The U.S.A., and Russia take the lead with significant percentage increases in botnet C&Cs - 27% and 39%, respectively. However, the award for the most significant growth in Q4 goes to Bulgaria, with a whopping 227% increase, disappointing after the previous -44% decrease in Q3.

Increases across the globe

In contrast to Q3, most geolocations experienced an increase in the number of botnet C&Cs, that is except for India (-44%), Canada (-41%), Mexico (-39%), United Kingdom (-21%) and Uruguay (-6%).

Meanwhile, South Africa and Switzerland departed from the Top 20.

New entries

Poland (#16), Turkey (#20).

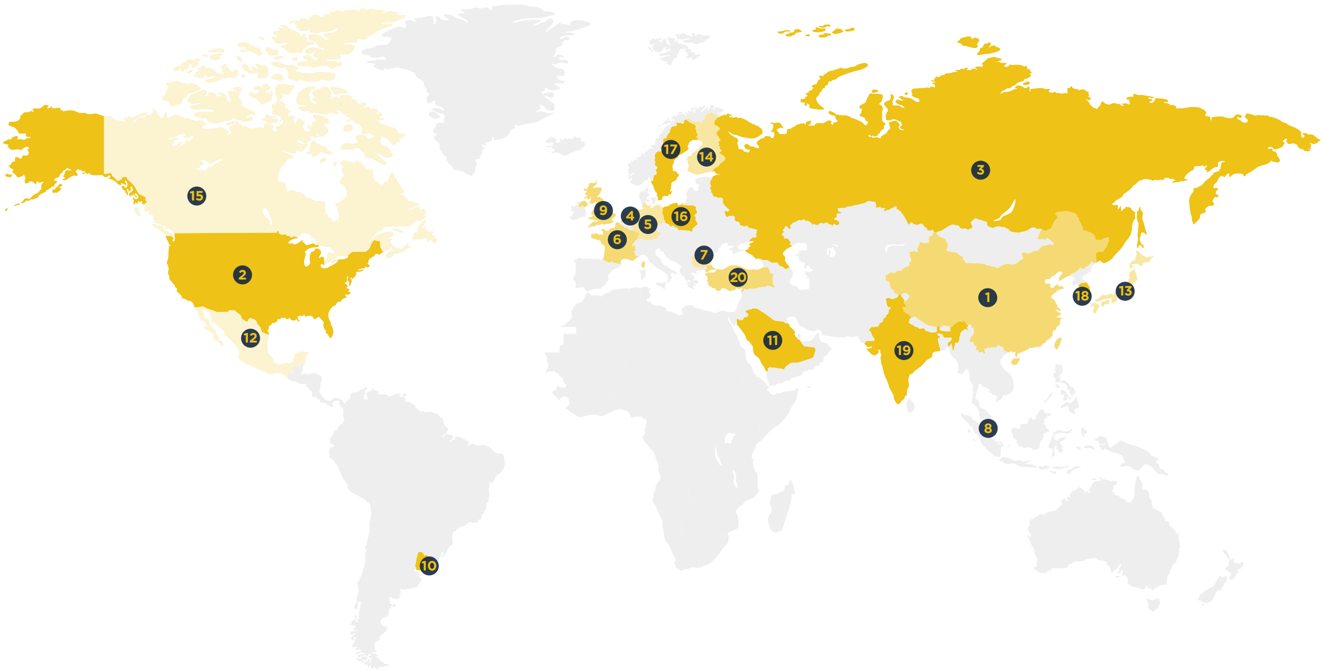
Departures

South Africa, Switzerland.

Geolocation of botnet C&Cs, Q4 2023 (continued)

Top 20 locations of botnet C&Cs

Rank	Country		Q3 2023	Q4 2023	% Change Q on Q
#1	China	🇨🇳	1570	2125	35%
#2	United States	🇺🇸	1267	1606	27%
#3	Russia	🇳🇱	441	612	39%
#4	Netherlands	🇷🇺	542	603	11%
#5	Germany	🇩🇪	378	478	26%
#6	France	🇫🇷	242	322	33%
#7	Bulgaria	🇧🇬	64	209	227%
#8	Singapore	🇸🇬	164	190	16%
#9	United Kingdom	🇬🇧	221	175	-21%
#10	Uruguay	🇺🇾	170	160	-6%
#11	Saudi Arabia	🇸🇦	153	159	4%
#12	Mexico	🇲🇽	232	141	-39%
#13	Japan	🇯🇵	70	111	59%
#14	Finland	🇫🇮	78	102	31%
#15	Canada	🇨🇦	157	92	-41%
#16	Poland	🇵🇱	-	90	New entry
#16	Sweden	🇸🇪	69	80	16%
#18	Korea (Rep. of)	🇰🇷	73	74	1%
#19	India	🇮🇳	123	69	-44%
#20	Turkey	🇹🇷	-	55	New entry



Malware associated with botnet C&Cs, Q4 2023

Cobalt Strike is on the rise

After entering its sixth quarter as the malware associated with the largest number of botnet C&Cs, Cobalt Strike maintained its usual form in Q4, with a 26% increase. The penetration testing tool is now associated with over four times more botnet C&Cs than its closest competitor, AsyncRat, at number two.

QuasarRAT climbs the charts

Speaking of Remote Access Tools – QuasarRAT experienced a significant increase (341%), moving this malware's rank from #12 to #5 in Q4. This comes as no surprise, considering that it is an open-source tool; anyone can set up a server and use it.

Penetration testing tools prevail

In Q2 and Q3, Spamhaus researchers observed an increase in the number of botnet C&Cs associated with legitimate, but abused penetration testing tools. In Q4, this trend continued with increases from 42.9% to 49.7%, meaning these penetration testing tools accounted for almost 50% of malware associated with botnet C&Cs in the Top 20.

Pika who?

Q4 saw six new malware entrants, including Pikabot at #10, associated with 198 botnet C&Cs. First seen in 2023, this backdoor malware contains several methods to avoid sandboxes, virtual machines, and other debugging techniques.

Spamhaus researchers have also observed that Pikabot appears to be the malware of choice for the well-known threat actor TA577, also known as TR.

The resurrection of Qakbot

Following the takedown of Qakbot in August 2023, and as forecasted in the Q3 report, this malware has now dropped completely from the Top 20. However, it may be too early to celebrate, given that Spamhaus researchers have detected low-volume Qakbot campaigns targeting specific business sectors seemingly 'testing the waters'.

We did say anything is possible in this industry - let's hope this isn't the resurrection of Qakbot!

What is Cobalt Strike?

Cobalt Strike is a legitimate commercial penetration testing tool that allows an attacker to deploy an "agent" on a victim's machine.

Sadly, it is extensively used by threat actors with malicious intent, for example, to deploy ransomware.

New entries

Hook (#9), Pikabot (#10), FakeUpdates (#11), Meterpreter (#14), BianLian (#17), Lumma (#18).

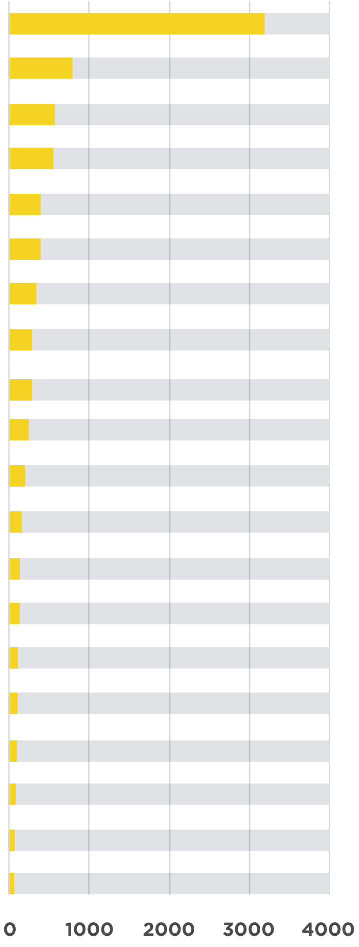
Departures

AveMaria, ISFB, NanoCore, Stealc, Tofsee, Vidar.

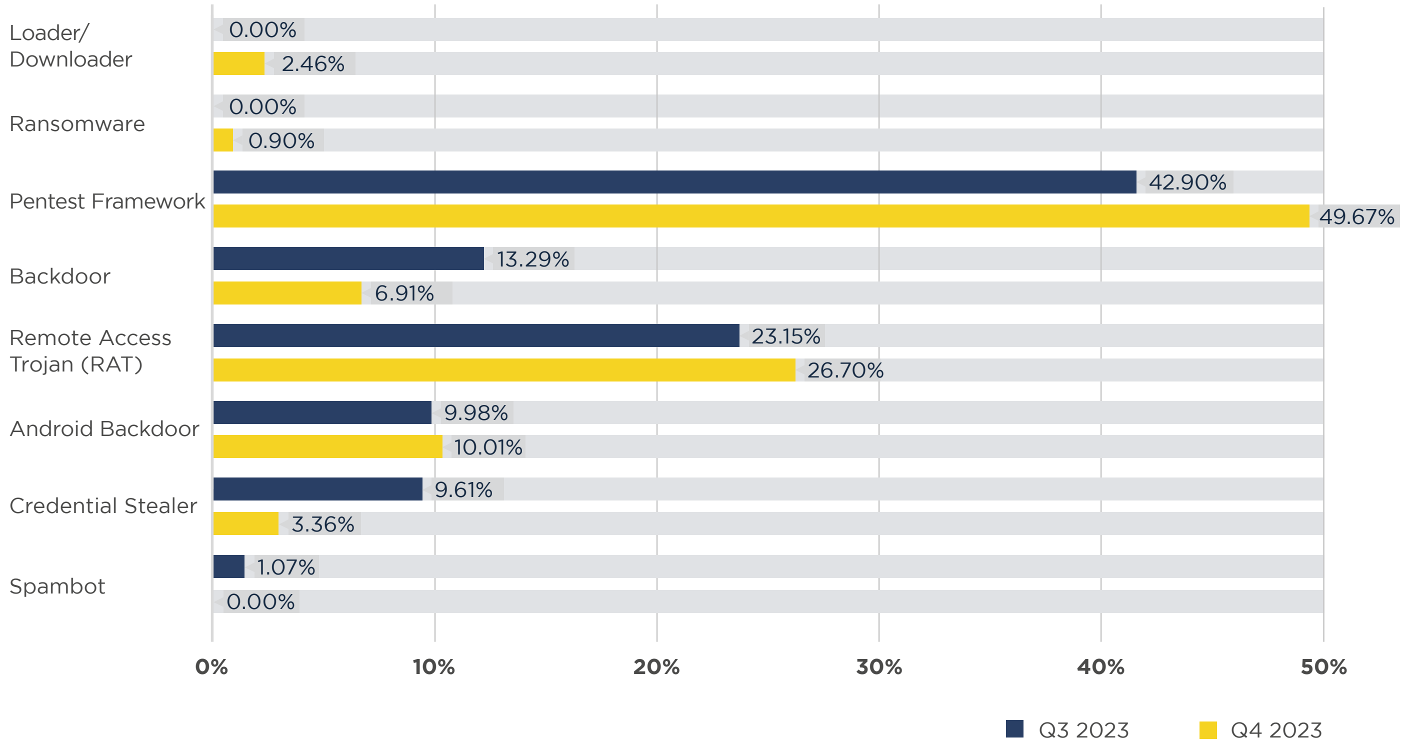
Malware associated with botnet C&Cs, Q4 2023 (continued)

Malware families associated with botnet C&Cs

Rank	Q3 2023	Q4 2023	% Change	Malware Family	Description
#1	2491	3137	26%	Cobalt Strike	Pentest Framework
#2	373	710	90%	AsyncRAT	Remote Access Trojan (RAT)
#3	285	515	81%	Sliver	Pentest Framework
#4	646	513	-21%	Flubot	Android Backdoor
#5	75	331	341%	QuasarRAT	Remote Access Trojan (RAT)
#6	341	329	-4%	Remcos	Remote Access Trojan (RAT)
#7	273	286	5%	RedLineStealer	Remote Access Trojan (RAT)
#8	197	229	16%	DCRat	Remote Access Trojan (RAT)
#9	-	223	New entry	Hook	Android Backdoor
#10	-	198	New entry	Pikabot	Backdoor
#11	-	181	New entry	FakeUpdates	Loader/downloader
#12	797	145	-82%	Qakbot	Backdoor
#13	186	111	-40%	IcedID	Credential Stealer
#14	-	88	New entry	Meterpreter	Backdoor
#15	89	78	-12%	NjRAT	Remote Access Trojan (RAT)
#16	63	77	22%	Havoc	Backdoor
#17	-	66	New entry	BianLian	Ransomware
#18	-	49	New entry	Lumma	Credential Stealer
#19	53	45	-15%	Rhadamanthys	Credential Stealer
#20	269	42	-84%	RecordBreaker	Credential Stealer



Malware type comparisons between Q3 2023 and Q4 2023



Most abused top-level domains, Q4 2023

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q4 2023, **.com** had more than 157m domains, of which 0.00076% were associated with botnet C&Cs. Meanwhile, **.pw** had approximately 17k domains, of which 0.959% were associated with botnet C&Cs. Both are in the top three of our listings. Still, one had a much higher percentage of domains related to botnet C&Cs than the other.

.pw what's going on?

Having entered the charts at #6 in Q3, abuse of .pw continued to increase this quarter, placing it at #2. While .pw might be a country code (for Republic of Palau), a significant 0.96% of their active zone files are being used for botnet C&C hosting. This is three times the amount of .hair at 0.33% - the second highest TLD exposed to abuse, based on percentage of active zone files.

Unfortunately, this is what happens with ccTLDs that are repurposed to what are effectively gTLDS – see Q3 Botnet Threat Update. To find their way out of the Top 20, the domain registry responsible needs to get a handle on registrations for this TLD, as abuse is prevalent.

Increases for .org

For the first time since Q3 2022, the gTLDs .org and .info both ranked in the top 10 most abused TLDs. Moreover, the number of newly registered botnet C&C domains observed on .org increased by 157%, from 35 to 90.

New entry at #3 for .xyz

In Q4, .xyz jumped straight back to third position, following a short break from the Top 20. Yet, it's not all doom and gloom for this registry; .makeup (#13), .beauty (#12), and .hair (#11) all experienced significant decreases of -84%, -76% and -45% respectively, following a stint in the top ten last quarter.

Let's hope it was a fleeting visit for .xyz and more decreases are on the way!

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, Q4 2023 (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

xyz (#3), fun (#5), online (#6), net (#10), store (#16), cloud (#17) icu (#18), me (#19).

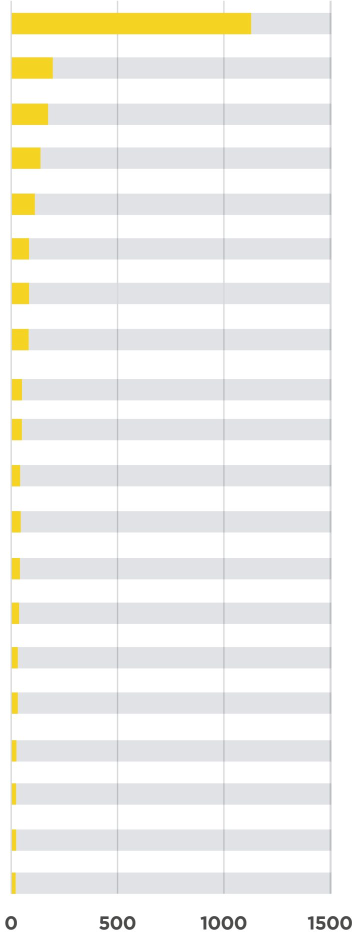
Departures

br, buzz, cn, cyou, io, rest, sbs, shop.

Most abused top-level domains, Q4 2023 (continued)

Top abused TLDs - number of domains

Rank	Q3 2023	Q4 2023	% Change	TLD	Note
#1	1904	1199	-37%	com	gTLD
#2	153	167	9%	pw	ccTLD
#3	-	144	New entry	xyz	gTLD
#4	93	124	33%	top	gTLD
#5	-	120	New entry	fun	gTLD
#6	-	93	New entry	online	gTLD
#7	35	90	157%	org	gTLD
#8	130	87	-33%	info	gTLD
#9	80	81	1%	site	gTLD
#10	-	71	New entry	net	gTLD
#11	109	60	-45%	hair	gTLD
#12	201	49	-76%	beauty	gTLD
#13	220	35	-84%	makeup	gTLD
#13	66	35	-47%	ru	ccTLD
#15	164	32	-80%	best	gTLD
#16	-	28	New entry	store	gTLD
#17	-	27	New entry	cloud	gTLD
#18	-	26	New entry	icu	gTLD
#19	-	23	New entry	me	ccTLD
#20	64	22	-66%	cfd	gTLD



Most abused domain registrars, Q4 2023

PDR steals #1

Regular readers will be used to seeing Indian-based PDR in the Top 20. However, this is the first time it has been seen here at #1. Incidentally, this is reflected in the geolocation of the most abused domain registrars, with India claiming a 20.37% slice of the pie, second to The U.S.A. at 33.55%.

That's gotta sting

Despite promising decreases in Q3, Lithuanian-based Hostinger saw a massive 271% increase in the number of botnet C&C operators registering through them, rising from 17 in Q3 to 63 in Q4.

Kudos to Cloudflare, Google and Gandi

Swift action from Cloudflare, decreasing their numbers by an impressive -68% in Q4 2023, along with Google and Gandi, who dropped out of the Top 20 entirely - great work!

Additionally, US-based, Sav, and Canadian-based, NameSilo, both improved massively in Q4. Sav's numbers plummeted by -78%, and NameSilo by -67%.

The Tucows-trend continues

Well done to Canadian-based registrar, Tucows! For a consecutive 12 months, they have continued to reduce the number of botnet C&C operators registering through them. Even though there was only a slight decrease (-3%) in Q4, every miscreant stopped counts!

New entries

Danesco (#5), GoDaddy.com (#6), Nicenic (#7), Gname.com (#11), Hosting Concepts (#12), Eranet (#17), WebNIC (#18), GMO (#19), OwnRegistrar (#19).

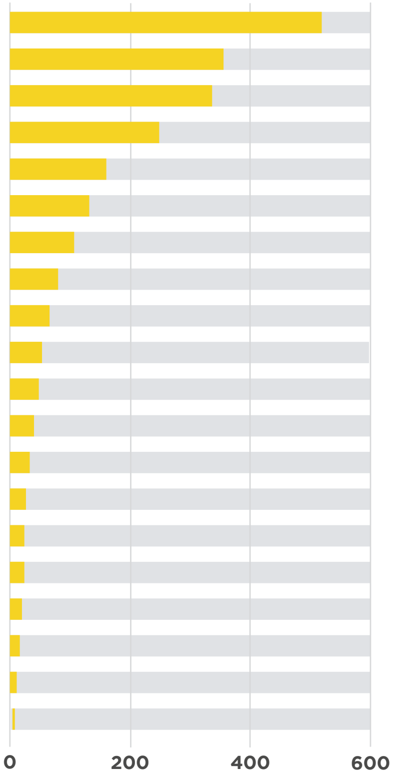
Departures

CommuniGal, DNSPod, Enom, Gandi, Google, OpenProvider, Regtime, RU-Center, Xin.

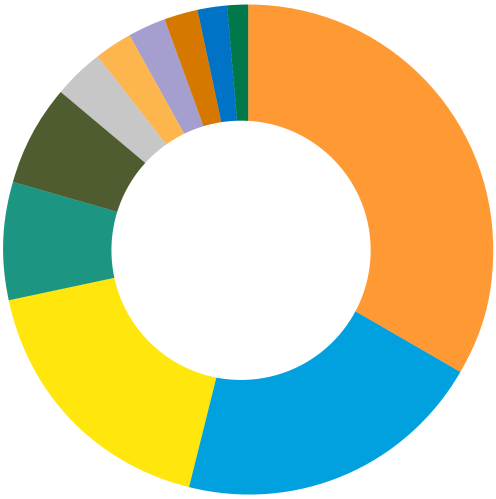
Most abused domain registrars, Q4 2023 (continued)

Most abused domain registrars - number of domains

Rank	Q3 2023	Q4 2023	% Change	Registrar	Country
#1	211	510	142%	PDR	India
#2	1162	378	-67%	NameSilo	Canada
#3	193	351	82%	NameCheap	United States
#4	1106	243	-78%	Sav	United States
#5	-	167	New entry	Danesco	Cyprus
#6	-	149	New entry	GoDaddy.com	United States
#7	-	121	New entry	Nicenic	China
#8	23	89	287%	RegRU	Russia
#9	69	67	-3%	Tucows	Canada
#10	17	63	271%	Hostinger	Lithuania
#11	-	51	New entry	Gname.com	Singapore
#12	-	48	New entry	Hosting concepts	Netherlands
#13	14	43	207%	PSI	Japan
#13	43	40	-7%	Alibaba	China
#15	123	39	-68%	CloudFlare	United States
#16	16	38	138%	Name.com	United States
#17	-	34	New entry	Eranet	China
#18	-	33	New entry	WebNIC	Malaysia
#19	-	20	New entry	OwnRegistrar	United States
#19	-	20	New entry	GMO	Japan



LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Q4 2023	Q3 2023
🟧 United States	33.55%	45.80%
🟦 India	20.37%	6.64%
🟨 Canada	17.77%	39.19%
🟩 China	7.79%	3.49%
🟩 Cyprus	6.67%	n/a
⬜ Russia	3.55%	2.49%
🟧 Lithuania	2.52%	0.54%
🟪 Japan	2.52%	0.44%
🟧 Singapore	2.04%	n/a
🟦 Netherlands	1.92%	0.63%
🟩 Malaysia	1.32%	n/a

Networks hosting the most newly observed botnet C&Cs, Q4 2023

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 13 networks

After a flurry of positive reductions in Q3, disappointingly, this quarter reported increases from 13 networks previously listed in the Top 20. Ranging from a tolerable 3% for stc.com.sa, to a deplorable 98% for constant.com!

Among the other networks included was microsoft.com, which, after a -28% reduction in Q3, experienced a 60% increase in Q4, taking them to #13.

Chinese networks dominate the top spots!

As mentioned earlier in the report, the number of botnet C&Cs hosted in China continued to rise again in Q4. Two cloud hosting providers contributing to this increase were tencent.com and alibaba-inc.com, taking the top two spots and accounting for 34% of all botnet C&Cs in our Top 20.

Nice work uninet.net.mx!

After sitting at #5 for two consecutive quarters, Q4 saw uninet.net.mx, a Mexican provider, fall to #14, with the largest percentage decrease (-39%) across all networks. Keep up the good work!

Leaving our Top 20 are...

.....bell.ca, delis.one, ielo.net, sitebgp.com, zerohost.network. Thank you for your efforts to prevent botnet operators from hosting C&C servers on your networks.

Networks and botnet C&C operators

Networks have a reasonable amount of control over operators who fraudulently sign-up for a new service.

A robust customer verification/ vetting process should occur before commissioning a service.

Where networks have a high number of listings, it highlights one of the following issues:

1. Networks are not following best practices for customer verification processes.
2. Networks are not ensuring that ALL their resellers follow sound customer verification practices.

In some of the worst-case scenarios, employees or owners of networks are directly benefiting from fraudulent sign-ups, i.e., knowingly taking money from miscreants in return for hosting their botnet C&Cs; however, thankfully, this doesn't often happen.

New entries

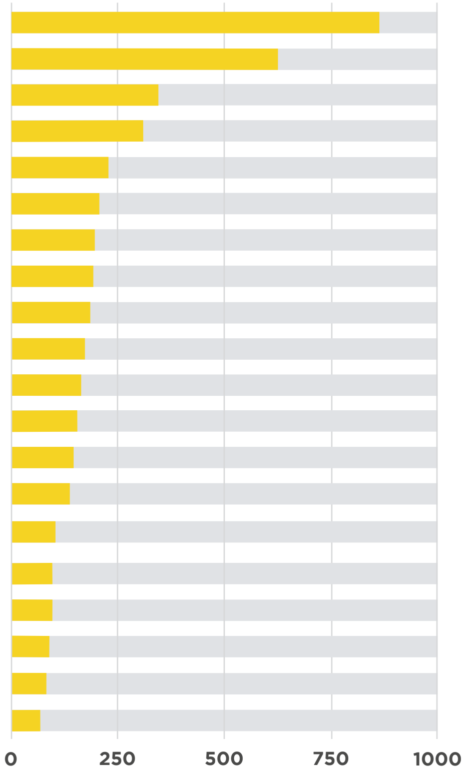
limenet.io (#9), contabo.de (#15), megalayer.net (#17), google.com (#19), linode.com (#20).

Departures

bell.ca, delis.one, ielo.net, sitebgp.com, zerohost.network.

Networks hosting the most newly observed botnet C&Cs, Q4 2023 (continued)

Rank	Q3 2023	Q4 2023	% Change	Network	Country
#1	644	837	30%	tencent.com	China
#2	398	623	57%	alibaba-inc.com	China
#3	294	321	9%	amazon.com	United States
#4	261	279	7%	digitalocean.com	United States
#5	106	210	98%	constant.com	United States
#6	104	189	82%	huawei.com	China
#7	115	170	48%	ovh.net	France
#8	160	168	5%	hetzner.com	Germany
#9	-	164	New entry	limenet.io	United States
#10	170	160	-6%	antel.net.uy	Uruguay
#11	152	157	3%	stc.com.sa	Saudi Arabia
#12	103	152	48%	neterra.net	Bulgaria
#13	89	142	60%	microsoft.com	United States
#14	229	139	-39%	uninet.net.mx	Mexico
#15	-	115	New entry	contabo.de	Germany
#16	84	108	29%	colocrossing.com	United States
#17	-	100	New entry	megalayer.net	China
#18	63	87	38%	aeza.net	Russia
#19	-	85	New entry	google.com	United States
#20	-	83	New entry	linode.com	United States



Networks hosting the most active botnet C&Cs, Q4 2023

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs at the end of Q4 2023. 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.

Big name networks miss the mark

Maybe it's not quite missing the mark, but they are certainly missing (or ignoring?) the abuse notifications we are sending to their Trust and Safety Teams.
The Top 20 providers with botnet C&C issues had 946 active botnet C&Cs on their networks in Q4. Of these, popular networks, tencent.com (#1), alibaba-inc.com (#2) digitalocean.com (#3), ovh.com (#4), and amazon.com (#5) accounted for almost 60% of the most active botnet C&Cs.

Nevertheless, it was German-based providers, contabo.com and hetzner.com that suffered the greatest increases in numbers in Q4, 142% and 135% respectively. With US-based providers, constant.com, colocrossing.com and google.com close behind with increases of 120%, 100% and 95% respectively.

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 disappoints. 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 our Industry Liaison. We provide abuse reports, but we can do so much more.

New entries

itldc.com (#13), limenet.io (#14), free-h.org (#15), linode.com (#15), aeza.net (#17), m247.com (#19).

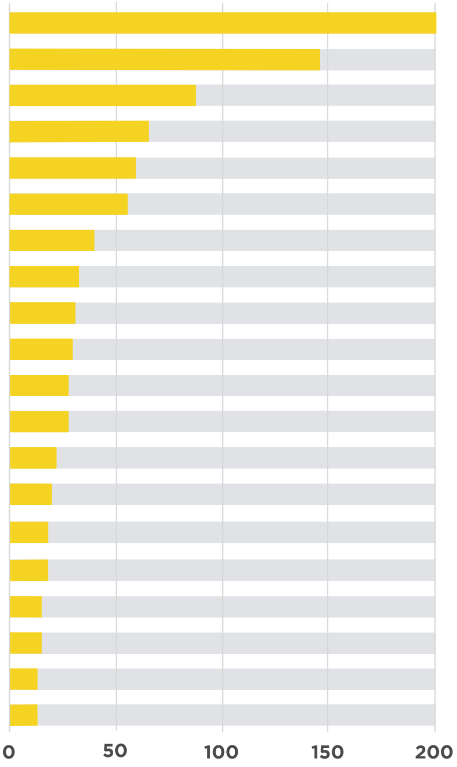
Departures

cloudflare.com, matrixllp, neterra.net, petaexpress.com, stark-industries.solutions, vdsina.ru.

Networks hosting the most active botnet C&Cs, Q4 2023 (continued)

Total number of active botnet C&Cs per network

Rank	Q3 2023	Q4 2023	% Change	Network	Country
#1	181	200	10%	tencent.com	China
#2	95	147	55%	alibaba-inc.com	China
#3	62	89	44%	digitalocean.com	United States
#4	39	67	72%	ovh.net	France
#5	38	59	55%	amazon.com	United States
#6	23	54	135%	hetzner.com	Germany
#7	22	43	95%	google.com	United States
#8	34	35	3%	huawei.com	China
#9	15	33	120%	constant.com	United States
#10	20	31	55%	microsoft.com	United States
#11	12	29	142%	contabo.de	Germany
#12	14	28	100%	colocrossing.com	United States
#13	-	21	New entry	itldc.com	United States
#14	-	18	New entry	limenet.io	United States
#15	-	17	New entry	free-h.org	France
#15	-	17	New entry	linode.com	United States
#17	-	15	New entry	aeza.net	Russia
#17	18	15	-17%	simcentric.com	China
#19	-	14	New entry	m247.com	Romania
#19	14	14	0%	quadranet.com	United States



That’s all for now. Stay safe, and we’ll see you in June 2024!