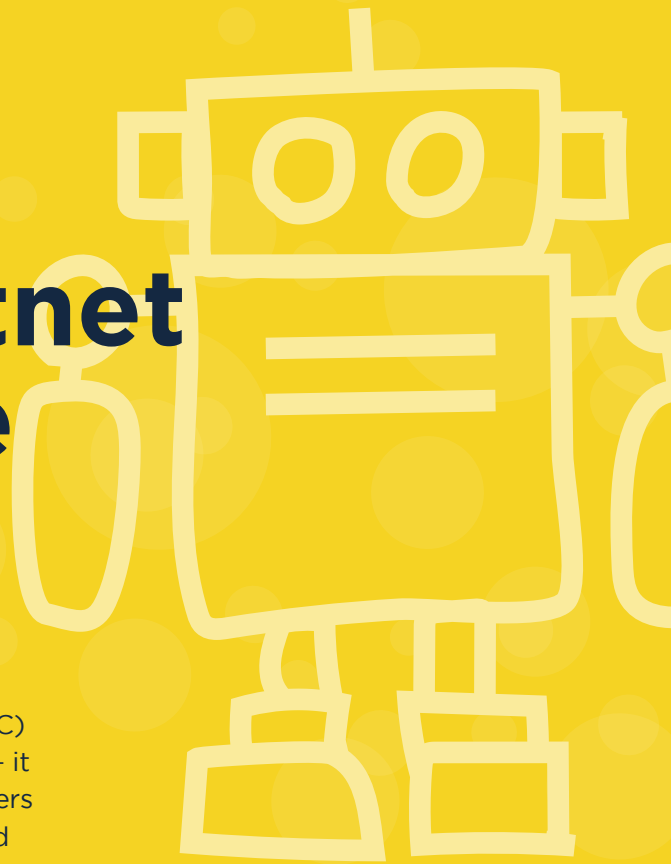


Spamhaus Botnet Threat Update



Q3 2023

The big news of Q3 was the takedown of Qakbot, aka “Operation Duck Hunt”. Was this the driver of the -16% reduction in the number of botnet command & control (C&C) servers our threat hunters observed in Q3? It’s hard to say – it certainly was a contributing factor, however this report covers the traditional Western summer holiday months i.e. July and August, and bad actors take holidays too!

Welcome to the Spamhaus Botnet Threat Update Q3 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

A sitting duck? Qakbot's demise

In Q3 a takedown operation, called “Duck Hunt” occurred, taking control of Qakbot’s infrastructure, and metaphorically shooting down this malevolent malware.

Qakbot refresher

For those of you who are not overly familiar with the Qakbot malware, here are some key points to digest:

- Qakbot was Bad, with a capital B, and seen as one of the most significant threats to corporate networks.
- In 2022, every fourth malware site shared by contributors to abuse.ch’s [URLHaus platform](#) was associated with Qakbot – this malware was prolific.
- Qakbot’s usual modus operandi was in providing initial access to a network for groups to then deploy ransomware, such as Conti, ProLock, Egregor and REvil.
- Investigators have found evidence that, between October 2021 and April 2023, Qakbot administrators received fees corresponding to approximately \$58 million in ransoms paid by victims.

The takedown

On Tuesday August 29th, 2023, the Federal Bureau of Investigation (FBI), coordinating an international group of law enforcement authorities, announced that it had taken control of the Qakbot infrastructure.

In a cunning move, through Bureau-controlled servers, the FBI instructed infected computers to download an uninstaller file. This uninstaller, specifically created to remove Qakbot malware, untethered infected computers from the botnet and prevented the installation of any additional malware.

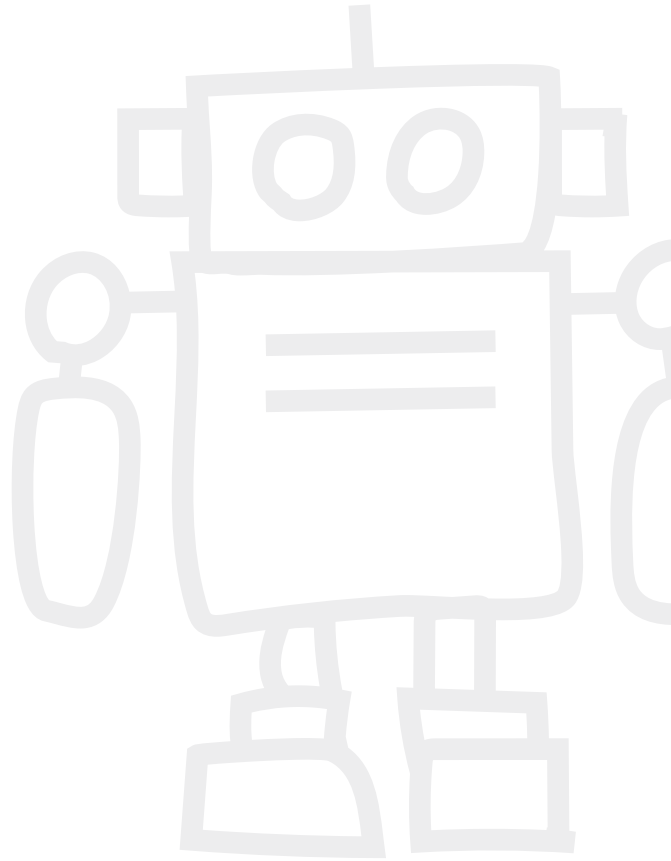
It takes a community to keep the internet safe

As part of the remediation efforts, The Spamhaus Project was more than happy to be able to assist the FBI and the international coalition. Through data shared by these entities, we were able to contact email service providers, hosting companies, and other parties responsible for email accounts that had been compromised by Qakbot. The request was a simple one “please secure the accounts in question via a simple password reset.”

Out of the 6.3 million email addresses that had been shared with Spamhaus by the FBI, approximately 50% were downloaded for remediation.

Will the duck remain down?

Who knows. Given that the perpetrators behind Qakbot haven't been arrested, we may well see it rise from the ashes. Nonetheless, we applaud the work that this cross-border coalition, led by the FBI, has done – as ever it highlights that it takes a global community to make the internet a safer place.



Number of botnet C&Cs observed, Q3 2023

In Q3 2023, Spamhaus identified 7,052 botnet C&Cs compared to 8,438 in Q2 2023. This was a -16% decrease quarter on quarter. The monthly average reduced from 2,813 in Q2 to 2,351 botnet C&Cs per month in Q3 2023.

Quarter	No. of Botnets	Quarterly Average	% Change
Q4 2022	6,775	2,258	+56%
Q1 2023	8,358	2,786	+23%
Q2 2023	8,438	2,813	+1%
Q3 2023	7,052	2,351	-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, Q3 2023

China knocks the US off pole position

Those increases keep coming for China. In Q2, the number of botnets hosted in the country increased by 34%. Last quarter the numbers increased by a further 18%, to 1,570, knocking the US off its #1 position; a position the US had held for a year.

Decreases across the globe

Except for the previously mentioned China, along with Saudi Arabia (+13%), the Netherlands (+8%), Singapore (+7%) and India (2%), all other regions experienced a decrease in the number of botnet C&Cs. Meanwhile, Austria and Italy departed from the Top 20.

A special mention to Bulgaria that almost halved the number of botnets it was hosting in Q3, with a -44% decrease.



New entries

Uruguay (#9), South Africa (#20).











Departures











Austria, Italy.

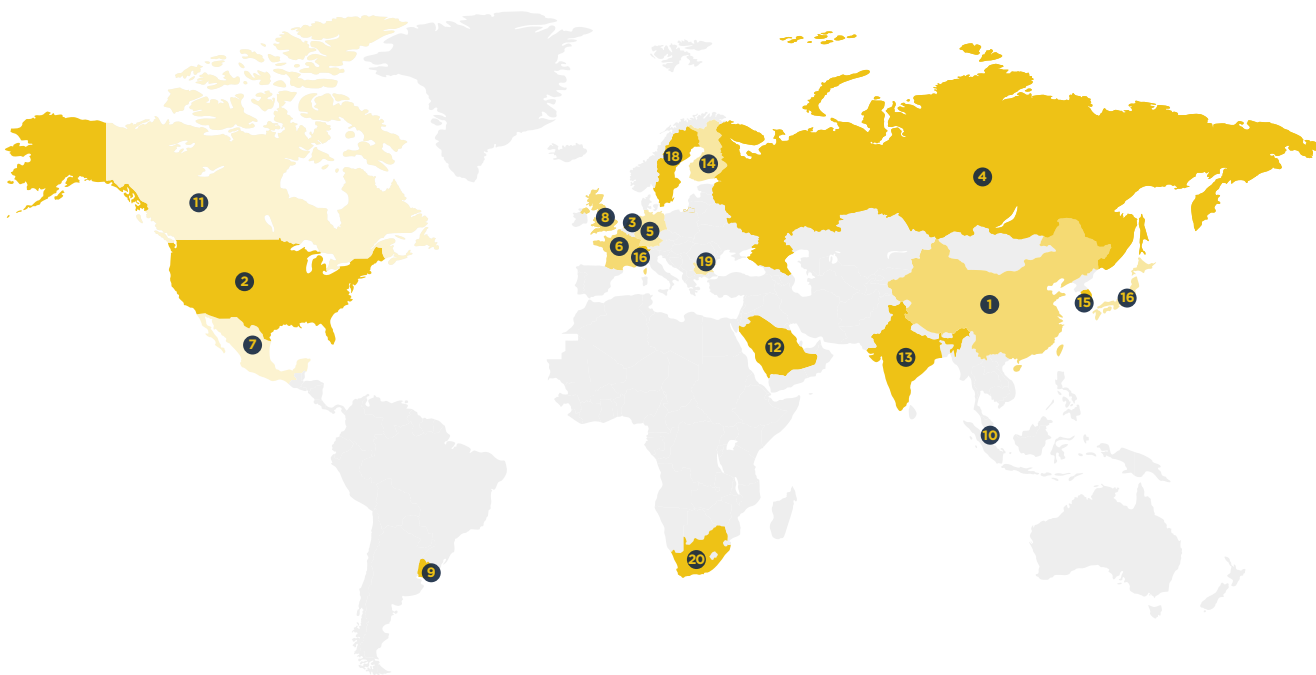
Geolocation of botnet C&Cs, Q3 2023

(continued)

Top 20 locations of botnet C&Cs

Rank	Country		Q2 2023	Q3 2023	% Change Q on Q
#1	China		1333	1570	18%
#2	United States		1935	1267	-35%
#3	Netherlands		503	542	8%
#4	Russia		667	441	-34%
#5	Germany		465	378	-19%
#6	France		288	242	-16%
#7	Mexico		292	232	-21%
#8	United Kingdom		243	221	-9%
#9	Uruguay		-	170	New entry
#10	Singapore		153	164	7%

Rank	Country		Q2 2023	Q3 2023	% Change Q on Q
#11	Canada		217	157	-28%
#12	Saudi Arabia		135	153	13%
#13	India		121	123	2%
#14	Finland		128	78	-39%
#15	Korea (Rep. of)		79	73	-8%
#16	Japan		90	70	-22%
#16	Switzerland		91	70	-23%
#18	Sweden		87	69	-21%
#19	Bulgaria		114	64	-44%
#20	South Africa		-	62	New entry



Malware associated with botnet C&Cs, Q3 2023

Still no change with Cobalt Strike

Whilst the number of botnet C&Cs associated with Cobalt Strike barely fluctuated in Q3, this penetration testing tool remained, for the fifth quarter, associated with the largest number of botnet C&Cs. So prevalent is the issue that Cobalt Strike is associated with three times more botnet C&Cs than its closest competitor, Qakbot, at #2.

How are penetration testing test tools being used by bad actors?

In Q2, we reported that an increasing number of botnet C&Cs were associated with abused legitimate penetration testing tools. In Q3, there were further increases from 39.1% to 42.9%. The likes of Cobalt Strike are used by miscreants as a lateral movement tool from various loaders, for example, Bumblebee and IcedID.

Qakbot's demise

As we've discussed in the Spotlight section, Qakbot was taken down in August this year. Therefore, it will come as no surprise to see the -41% decrease in numbers associated with this malware. Hopefully, next quarter's report will see this malware drop off the Top 20 entirely... unless there is a resurrection, and in this industry, anything is possible!



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

Stealc (#13), Vidar (#19), Nanocore (#20).

Departures

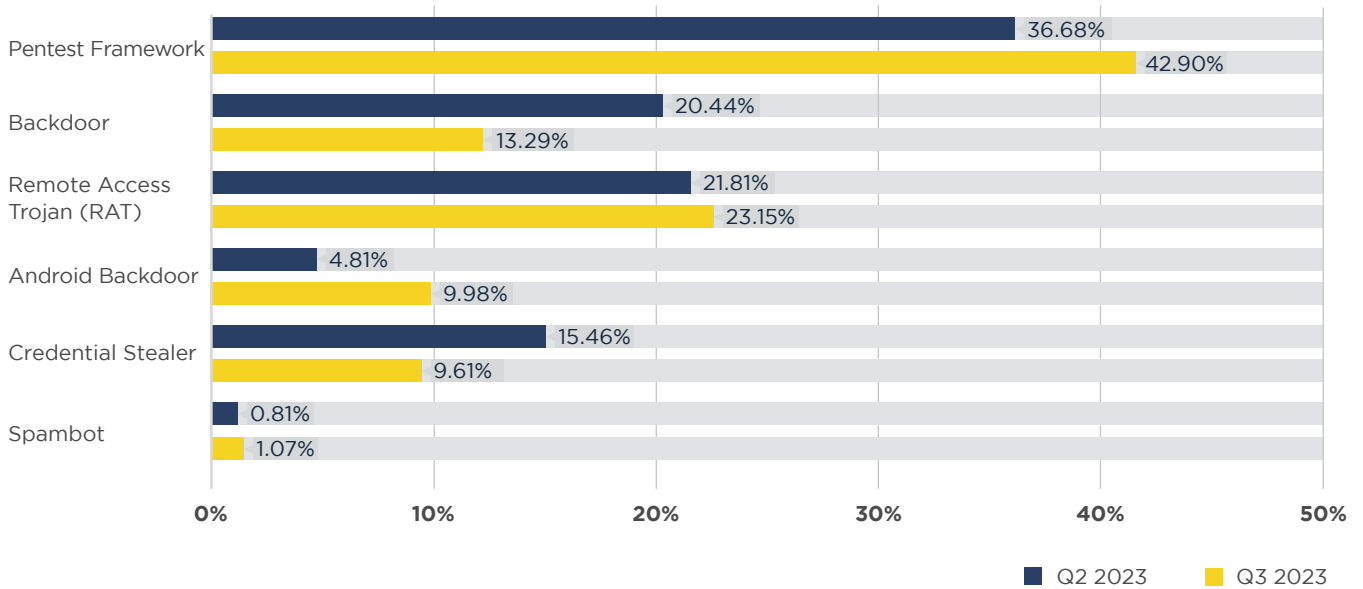
Aurora Stealer, Bumblebee, Hydra.

Malware associated with botnet C&Cs, Q3 2023 (continued)

Malware families associated with botnet C&Cs

Rank	Q2 2023	Q3 2023	% Change	Malware Family	Description	
#1	2501	2491	0%	Cobalt Strike	Pentest Framework	
#2	1349	797	-41%	Qakbot	Backdoor	
#3	596	646	8%	Flubot	Android Backdoor	
#4	456	373	-18%	AsyncRAT	Remote Access Trojan (RAT)	
#5	254	341	34%	Remcos	Remote Access Trojan (RAT)	
#6	361	285	-21%	Sliver	Pentest Framework	
#7	258	273	6%	RedLineStealer	Remote Access Trojan (RAT)	
#8	548	269	-51%	RecordBreaker	Credential Stealer	
#9	132	197	49%	DCRat	Remote Access Trojan (RAT)	
#10	206	186	-10%	IcedID	Credential Stealer	
#11	82	89	9%	NjRAT	Remote Access Trojan (RAT)	
#12	113	75	-34%	QuasarRAT	Remote Access Trojan (RAT)	
#13	-	73	New entry	Stealc	Credential Stealer	
#14	99	69	-30%	Tofsee	Spambot	
#14	145	69	-52%	ISFB	Remote Access Trojan (RAT)	
#16	98	63	-36%	Havoc	Backdoor	
#17	47	53	13%	Rhadamanthys	Credential Stealer	
#18	79	48	-39%	AveMaria	Remote Access Trojan (RAT)	
#19	-	41	New entry	Vidar	Credential Stealer	
#20	-	33	New entry	NanoCore	Remote Access Trojan (RAT)	

Malware type comparisons between Q2 2023 and Q3 2023



Most abused top-level domains, Q3 2023

It's all about the looks

In Q3, it was evident that there was a pattern in the abuse of beauty-related TLDs. With .makeup, .beauty, and .hair all in the Top 10 list, we assume that a special offer run by the registry .xyz was too much of a lure for bad actors to purchase these domains for their botnet C&Cs. Nevertheless, it's not all bad news for this registry; .xyz itself dropped out of the Top 20, which we congratulate.

New ccTLD entry

Having seen a plethora of country code TLDs depart from the Top 20, following Freenom's demise, it's disappointing to see a new entry to the charts: .pw.

Originally, this ccTLD was reserved for the residents of Palau, an island country found in the Pacific Ocean. However, now it's commonly used to represent 'Professional Web' and available for use by anyone. As it happens with many ccTLDs that are repurposed to what are effectively gTLDs, they find their way onto our Top 20. As prices are dropped, those wishing to burn through domains i.e. cybercriminals, look for the cheapest domains available.

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q3 2023, .ru had more than 5 million domains, of which 0.001% were associated with botnet C&Cs. Meanwhile, .pw had approximately 13,000 domains, of which 1.16% were associated with botnet C&Cs. Both are in the top twenty 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, Q3 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

best (#5), pw (#6), hair (#8),
buzz (#11), sbs (#14).

Departures

cloud, me, net, us, xyz.

Most abused top-level domains, Q3 2023 (continued)

Top abused TLDs - number of domains

Rank	Q2 2023	Q3 2023	% Change	TLD	Note	
#1	1741	1904	9%	com	gTLD	
#2	226	449	99%	shop	gTLD	
#3	47	220	368%	makeup	gTLD	
#4	94	201	114%	beauty	gTLD	
#5	-	164	New entry	best	gTLD	
#6	-	153	New entry	pw	ccTLD	
#7	85	130	53%	info	gTLD	
#8	-	109	New entry	hair	gTLD	
#9	161	93	-42%	top	gTLD	
#10	50	80	60%	site	gTLD	
#11	-	70	New entry	buzz	gTLD	
#12	188	66	-65%	ru	ccTLD	
#13	44	64	45%	cf	gTLD	
#14	-	55	New entry	sbs	gTLD	
#14	238	55	-77%	rest	gTLD	
#16	161	47	-71%	cyou	gTLD	
#17	80	35	-56%	org	gTLD	
#17	157	35	-78%	cn	ccTLD	
#19	90	34	-62%	br	ccTLD	
#20	40	32	-20%	io	ccTLD	

Most abused domain registrars, Q3 2023

Cloudflare enters at #5

Regular readers will be used to seeing Cloudflare regularly enter and depart our network-focused charts. However, this is the first time that the Domain Registrar (“with no-markup pricing”), has been in the most abused domain registrars Top 20, entering at #5. Having established itself as a “Registrar for Everyone” in September 2023, we hope this new entry isn’t a taste of things to come.

RU-Center, Sav and NameSilo still on the rise

Having experienced a significant +408% increase in Q2, at least in Q3 Sav only witnessed a +32% increase, placing them at #2. Instead, it was RU-Center’s turn to have huge increases (+221%) in the number of domain names registered by botnet C&C operators in Q3. Meanwhile, (disappointingly), NameSilo continues it’s upward trajectory making it past the 1,000 marker, and steadfastly holding onto its #1 spot.

Decreases for many registrars

Eleven out of the fifteen registrars listed in Q2’s Top 20, saw decreases in the number of botnet C&C operators registering through them. It’s good news to see operators like Google (-71%), Gandi (-59%), Hostinger (-50%), and Namecheap (-50%), continue to drop down the chart, quarter on quarter.

The Tucows-trend

They are on a roll! For a third consecutive quarter, Canadian-based Tucows continues to see reductions in its numbers. Now at 69 domains, it’s a further 23% decrease.



New entries





















Cloudflare (#5), DNSPod (#11), PSI (#16), CommuniGal (#18), Regtime (#20).

Departures

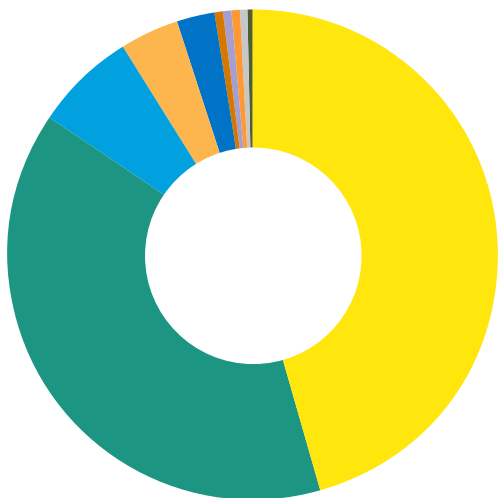
101Domain, InterNetworX, Nicenic, Porkbun, Todaynic.











Most abused domain registrars, Q3 2023 (continued)

Most abused domain registrars - number of domains

Rank	Q2 2023	Q3 2023	% Change	Registrar	Country	
#1	919	1162	26%	NameSilo	Canada	
#2	838	1106	32%	Sav	United States	
#3	183	211	15%	PDR	India	
#4	388	193	-50%	Namecheap	United States	
#5	-	123	New entry	Cloudflare	United States	
#6	90	69	-23%	Tucows	Canada	
#7	168	46	-73%	Xin	China	
#8	14	45	221%	RU-Center	Russia	
#9	60	43	-28%	Alibaba	China	
#10	201	23	-89%	RegRU	Russia	
#11	-	22	New entry	DNSPod	China	
#12	24	20	-17%	Openprovider	Netherlands	
#13	34	17	-50%	Hostinger	Lithuania	
#13	58	17	-71%	Google	United States	
#15	25	16	-36%	Name.com	United States	
#16	-	14	New entry	PSI	Japan	
#16	21	14	-33%	ENom	China	
#18	-	13	New entry	CommuniGal	Israel	
#19	29	12	-59%	Gandi	France	
#20	-	11	New entry	Regtime	Russia	

LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Q3 2023	Q2 2023
 United States	45.80%	35.75%
 Canada	38.75%	29.50%
 India	6.64%	6.07%
 China	3.93%	11.71%
 Russia	2.49%	13.10%
 Netherlands	0.63%	0.42%
 Lithuania	0.54%	2.29%
 Japan	0.44%	0.60%
 Israel	0.41%	n/a
 France	0.38%	0.54%

Networks hosting the most newly observed botnet C&Cs, Q3 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.

Tencent.com still out front

Once again, tencent.com remained at #1 in Q3, hosting over +47% more botnet C&Cs than alibaba-inc.com, who sat at #2. It has been over a year since tencent.com have held the top spot. And with a +9% increase quarter-on-quarter, it doesn't look like they're heading in the direction of reducing numbers of botnet C&Cs on their network any time soon.

Positive reductions across 12 networks

Q3 witnessed reductions from 12 networks previously listed in the Top 20, for the number of botnet C&Cs being hosted on their networks. Ranging from a meagre -3% with digitalocean.com, through to a very respectable -69% with delis.one. Even uninet.net.mx who flew up the Top 20 in Q2, experienced a -20% reduction from 287 in Q2 to 229 in Q3. Thank you all for your efforts to prevent botnet operators 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.



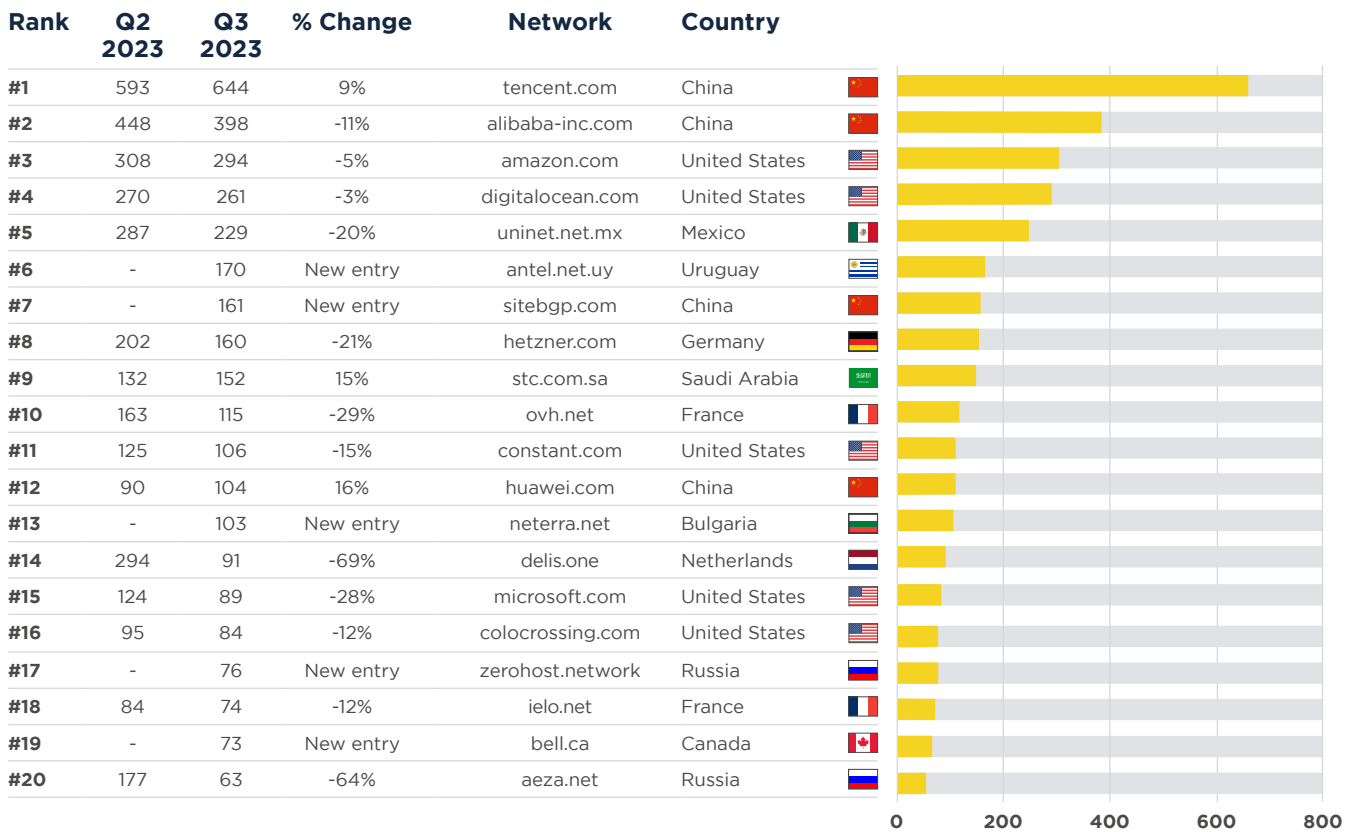
New entries

antel.net.uy (#6), sitebgp.com (#7), neterra.net (#13), zerohost.network (#17), bell.ca (#19).

Departures

blnwx.com, bt.com, lethost.co, m247.com, zerohost.io.

Networks hosting the most newly observed botnet C&Cs, Q3 2023 (continued)



Networks hosting the most active botnet C&Cs, Q3 2023

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs at the end of Q3 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.

New entries and departures

As we've become accustomed to with this Top 20 list, we regularly see multiple new entries and departures. Last quarter was no exception, seeing eight different networks come and go.

Large scale providers – how can we better work together

Some of the global names in hosting can be found in this Top 20, which disappoints us. 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 us. We provide abuse reports, but we can do so much more.



New entries

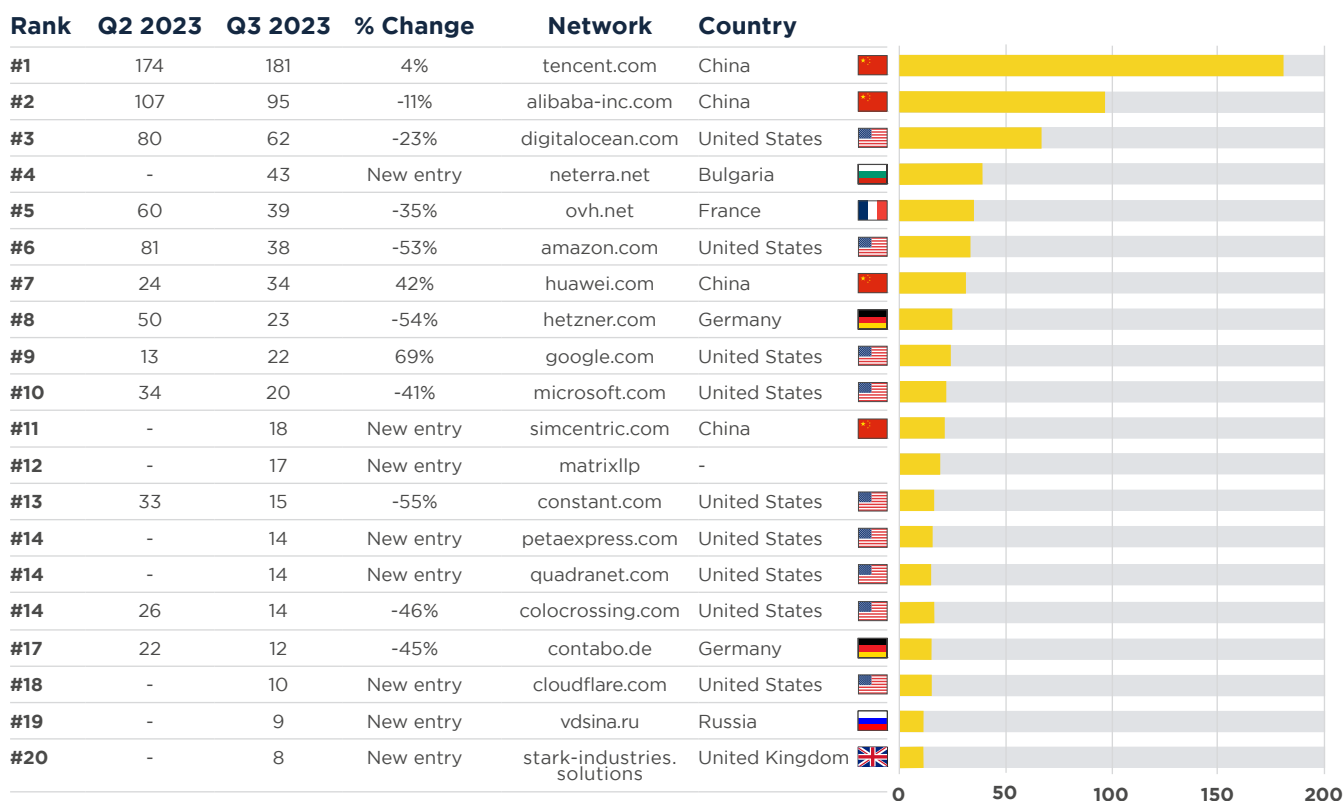
neterra.net (#4),
simcentric.com (#11), matrixllp (#12),
petaexpress.com (#13),
quadranet.com (#13),
cloudflare.com (#17), vdsina.ru (#18),
stark-industries.solutions (#19).

Departures

delis.one, hostwinds.com, m247.com,
oracle.com, servinga.com, uplus.co.kr,
waicore.com, zerohost.io

Networks hosting the most active botnet C&Cs, Q3 2023 (continued)

Total number of active botnet C&Cs per network



That's all for now. Stay safe, and see you in January 2024!