SPAMHAUS

Spamhaus Botnet Threat Update

Q2 2023

The number of botnet command control (C&C) servers plateaued in Q2 of this year, with a minimal +1% increase. Nevertheless, given the +23% increase in Q1, it would have been good to have seen numbers decrease.

The misuse of the legitimate penetration testing tool Cobalt Strike remains a top threat, and our researchers are not seeing a reduction in active botnet C&Cs across hosting providers whose increases in Q1 were abnormally high.

Welcome to the Spamhaus Botnet Threat Update Q2 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.

Number of botnet C&Cs observed, Q2 2023

In Q2 2023, Spamhaus identified 8,438 botnet C&Cs compared to 8,358 in Q1 2023. This was a +1% increase quarter on quarter. The monthly average increased from 2,786 in Q1 to 2,813 botnet C&Cs per month in Q2 2023.

Quarter	No. of Botnets	Quarterly Average	% Change
Q3 2022	4,331	1,444	+38%
Q4 2022	6,775	2,258	+56%
Q1 2023	8,358	2,786	+23%
Q2 2023	8,438	2,813	+1%

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, Q2 2023

The Americas are on the rise (again)

The United States has topped the charts for the past four quarterly reports, and this quarter is no exception. In this Q2 Top 20, the US hosted 37% of all botnet C&Cs observed by our researchers. However, their increase against last quarter's numbers was a minimal +4%, unlike Mexico, which experienced a +130% increase, along with Canada, which had a +41% increase.

Decreases across Europe

Having reported increases across European countries hosting botnet C&Cs for the past year, there was finally a reduction in Q2. Almost every country that experienced decreases in our Top 20 was European, with Switzerland (-45%), the Netherlands (-26%), and Germany (-24%) all experiencing meaningful reductions.

New entries

Korea (the Republic of) (#18), Italy (#20).

Departures

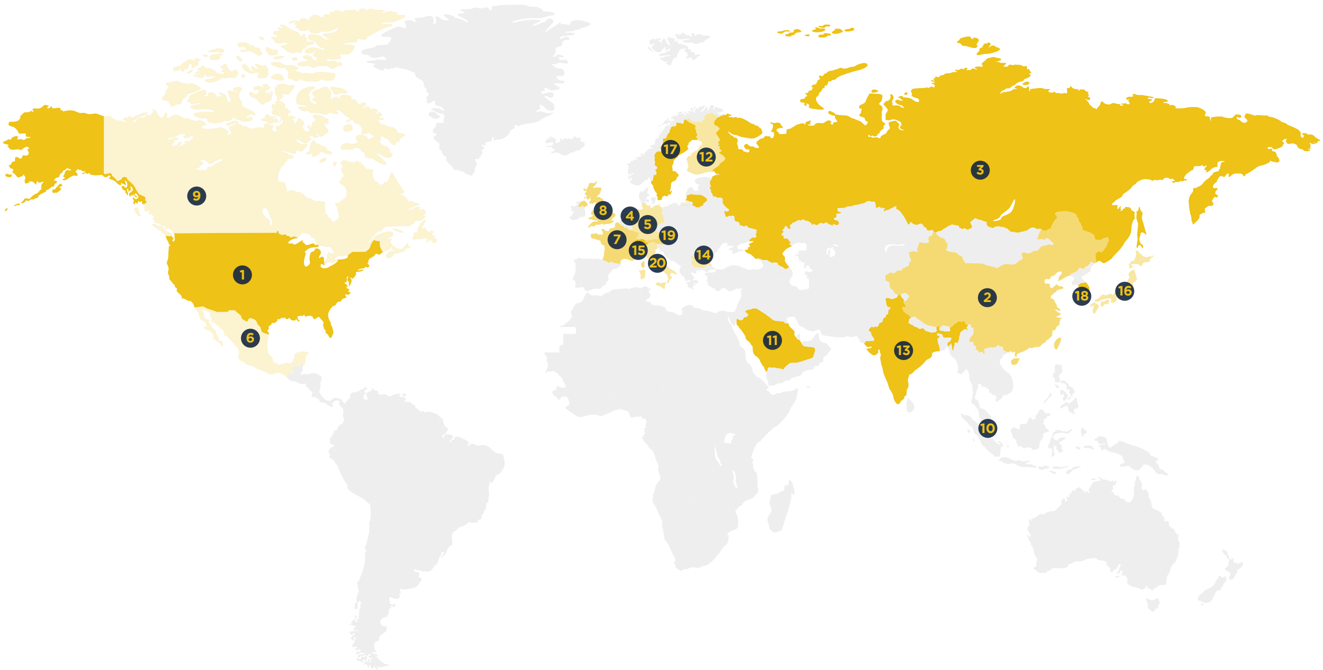
Lithuania, Poland.

Geolocation of botnet C&Cs, Q2 2023 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Q1 2023	Q2 2023	% Change Q on Q
#1	United States	1857	1935	4%
#2	China	993	1333	34%
#3	Russia	811	667	-18%
#4	Netherlands	683	503	-26%
#5	Germany	609	465	-24%
#6	Mexico	127	292	130%
#7	France	319	288	-10%
#8	United Kingdom	249	243	-2%
#9	Canada	154	217	41%
#10	Singapore	152	153	1%

Rank	Country	Q1 2023	Q2 2023	% Change Q on Q
#11	Saudi Arabia	113	135	19%
#12	Finland	135	128	-5%
#13	India	115	121	5%
#14	Bulgaria	109	114	5%
#15	Switzerland	164	91	-45%
#16	Japan	101	90	-11%
#17	Sweden	100	87	-13%
#18	Korea (Rep. of)	-	79	New entry
#19	Austria	70	76	9%
#20	Italy	-	71	New entry



Malware associated with botnet C&Cs, Q2 2023

Cobalt Strike and Qakbot remain prevalent

Anyone with a keen eye will note that this is the same headline from Q1, meaning that this is now the fourth quarter Cobalt Strike has been in the #1 spot. However, the gap is closing between its nearest rival, Qakbot. In Q1, Cobalt Strike was associated with +160% more malware than Qakbot. However, this quarter the difference was "only" +85% more.

Is FluBot still operational?

Europol announced in June 2022 that FluBot had been taken down, so you may be questioning why we are showing an 80% increase in the number of botnet C&Cs associated with this malware?

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.

Misuse of penetration testing test tools is on the rise

Given the prevalence of Cobalt Strike, it will come as no surprise that malware related to penetration testing tools account for the largest percentage of associated botnet C&Cs. The situation was exacerbated in Q2 by Sliver, which moved up the chart two places, with a +41% increase.

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

QuasarRAT (#12), Havoc (#14), Hydra (#18).

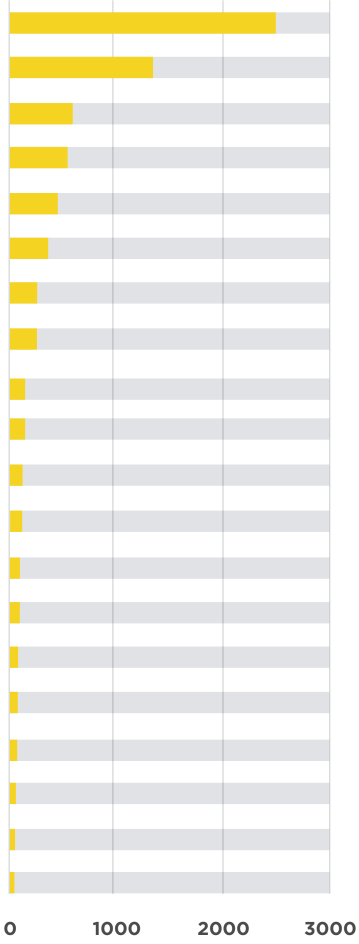
Departures

Amadey, Emotet, Vidar.

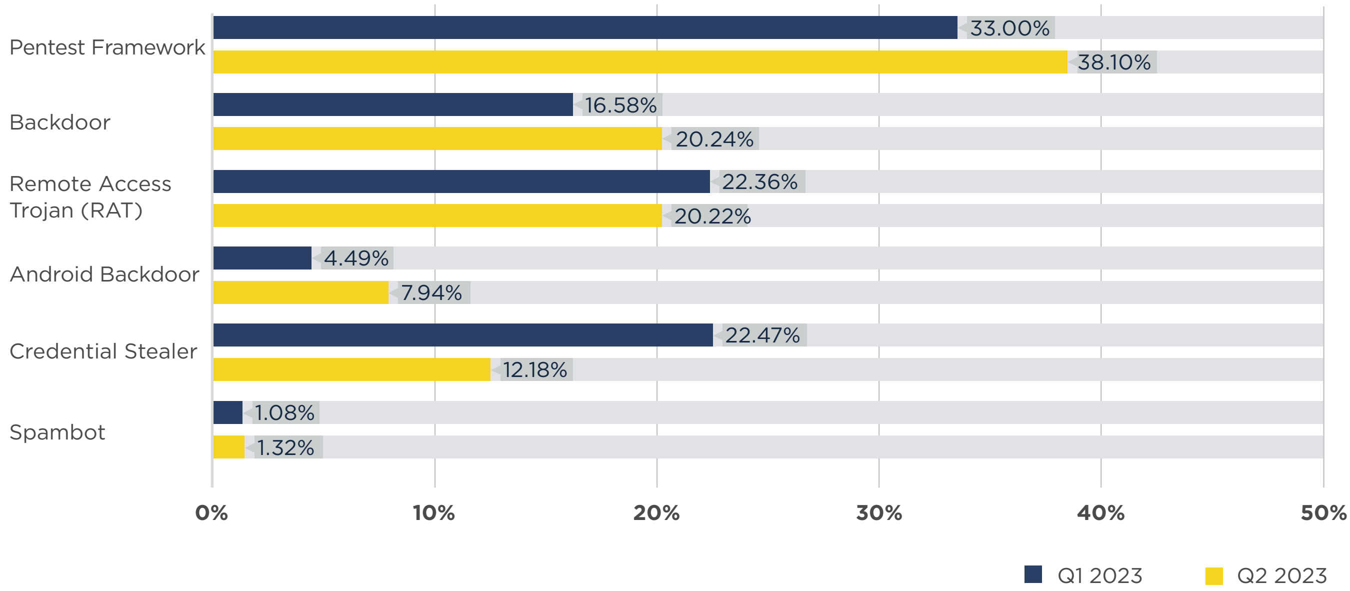
Malware associated with botnet C&Cs, Q2 2023 (continued)

Malware families associated with botnet C&Cs

Rank	Q1 2023	Q2 2023	% Change	Malware Family	Description
#1	2182	2501	15%	Cobalt Strike	Pentest Framework
#2	969	1349	39%	Qakbot	Backdoor
#3	332	596	80%	Flubot	Android Backdoor
#4	889	548	-38%	RecordBreaker	Credential Stealer
#5	380	456	20%	AsyncRAT	Remote Access Trojan (RAT)
#6	256	361	41%	Sliver	Pentest Framework
#7	417	258	-38%	RedLineStealer	Remote Access Trojan (RAT)
#8	254	254	0%	Remcos	Remote Access Trojan (RAT)
#9	321	206	-36%	IcedID	Credential Stealer
#10	194	145	-25%	ISFB	Remote Access Trojan (RAT)
#11	185	132	-29%	DCRat	Remote Access Trojan (RAT)
#12	-	113	New entry	QuasarRAT	Remote Access Trojan (RAT)
#13	80	99	24%	Tofsee	Spambot
#14	-	98	New entry	Havoc	Backdoor
#15	155	82	-47%	NjRAT	Remote Access Trojan (RAT)
#16	67	79	18%	AveMaria	Remote Access Trojan (RAT)
#17	175	73	-58%	Bumblebee	Backdoor
#18	-	61	New entry	Hydra	Credential Stealer
#19	143	53	-63%	Aurora Stealer	Credential Stealer
#20	168	47	-72%	Rhadamanthys	Credential Stealer



Malware type comparisons between Q1 2023 and Q2 2023



Most abused top-level domains, Q2 2023

The TLD botnet landscape after Freenom's issues

Last quarter we reported on the Freenom effect; whereby malicious operators were moving to the next best thing to free domain names - the cheapest ones available.

In Q1, researchers witnessed huge increases, i.e., +1,569% for .us, which we attributed to the Freenom effect. In Q2, the botnet C&C TLD landscape settled down somewhat. The largest increase experienced was +133% for .cloud, run by ARUBA PEC SpA, one of the largest domain registries in Europe. This placed the TLD at #5, up from #20 in Q1.

New entry at #2 for .rest

New entrant .rest is run by Punto 2012, a Mexican-based registry running gTLDs for restaurants and bars. We suspect the restaurant industry focused gTLD has been running a promotion to drive domain registrations. As we all know, where cheap domains prevail, criminal activity will follow.

We recommend Punto 2012 work with its registrars to improve vetting and registration processes.

Botnet operators Cyou

ShortDot registry had 161 botnet C&Cs using its TLD, .cyou, in Q2. This is a large increase of 112% quarter on quarter. No doubt this is because .cyou domains are available for next to nothing (at the time of publication, we've found them available for $2.55 for the first year).

Meanwhile, ShortDot's .cfd (ClothingFashionDesign) is a new entry at #18 to the Top 20 in Q2. We questioned a while ago, when ShortDot took over the operation of TLD .sbs, if increased registrations need to lead to increased abuse.

Top-level domains (TLDs) a brief overview

There are a couple of different top-level domains (TLDs) including:

Generic TLDs (gTLDs) - these are under ICANN jurisdiction. Some TLDs are open i.e. can be used by anyone e.g., .com, some have strict policies regulating who and how they can be used e.g., .bank, and some are closed e.g., .honda.

Country code TLDs (ccTLDs) - typically these relate to a country or region. Registries define the policies relating to these TLDs; some allow registrations from anywhere, some require local presence, and some license their namespace wholesale to others.

Most abused top-level domains, Q2 2023 (continued)

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q2 2023, **.com** had more than 159m domains, of which 0.001% were associated with botnet C&Cs. Meanwhile, **.rest** had approximately 38k domains, of which 0.627% were associated with botnet C&Cs. Both are in the top ten of our listings. Still, one had a much higher percentage of domains related to botnet C&Cs than the other.

New entries

rest (#2), beauty (#10), br (#11), makeup (#17), cfd (#18), io (#19).

Departures

click, fun, one, online, space, website.

Working together with the industry for a safer internet

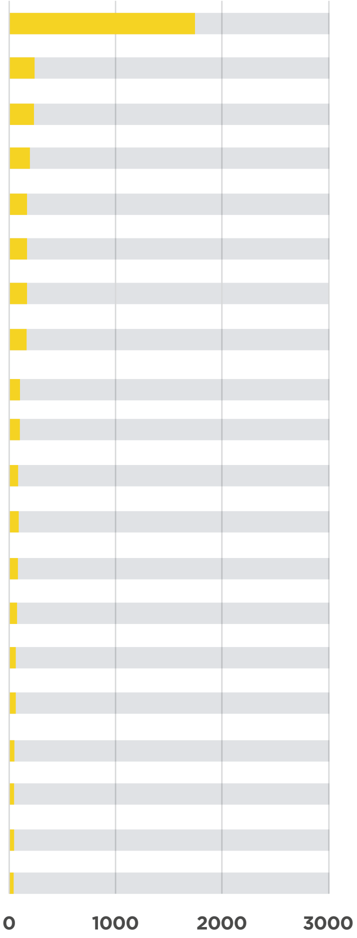
Naturally, we prefer no TLDs to have botnet C&Cs linked with them, but we live in the real world and understand there will always be abuse.

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.

Most abused top-level domains, Q2 2023 (continued)

Top abused TLDs - number of domains

Rank	Q1 2023	Q2 2023	% Change	TLD	Note
#1	2736	1741	-36%	com	gTLD
#2	-	238	New entry	rest	gTLD
#3	131	226	73%	shop	gTLD
#4	541	188	-65%	ru	ccTLD
#5	69	161	133%	cloud	gTLD
#5	76	161	112%	cyou	gTLD
#5	1094	161	-85%	top	gTLD
#8	90	157	74%	cn	ccTLD
#9	868	95	-89%	us	ccTLD
#10	-	94	New entry	beauty	gTLD
#11	-	90	New entry	br	ccTLD
#12	145	85	-41%	info	gTLD
#13	242	80	-67%	org	gTLD
#14	103	72	-30%	xyz	gTLD
#15	174	60	-66%	net	gTLD
#16	318	50	-84%	site	gTLD
#17	-	47	New entry	makeup	gTLD
#18	-	44	New entry	cfd	gTLD
#19	-	40	New entry	io	ccTLD
#19	463	40	-91%	me	ccTLD



Most abused domain registrars, Q2 2023

Sav suffer significant increases

Having stayed out of the top three, Q2 saw Sav experience an eye-watering 408% increase, placing them at #2. Positioned at the cheaper end of the market, they focus on pseudo-TLDs. Unlike standard TLDs they allow registration of subdomains beneath actual domains. Due to the absence of ICANN fees, these domains can be offered at a lower price. Our researchers suspect that, with Freenom's no longer endless supply of domains, registrars such as Sav promoting cheap prices are inevitably attracting abusive operators.

Namecheap starts to drop down the leaderboard

Having spent years in second place in the Top 20, Namecheap started to experience improvements in Q2, when it dropped to #3 with a -66% decrease in the number of domain names registered by botnet C&C operators. There were also significant decreases for Hostinger (-86%), Google (-85%), and Nicenic (-80%). Nice work!

Hats off to Tucows

For Canadian-based Tucows, the downward trend continues. After holding the top spot in Q4 2022 with 597 domains, Tucows has turned it around over the last six months. Dropping an impressive -75% in Q1 of this year, followed by a further -40% in Q2, with 90 domains associated with botnet C&Cs. Long may the decreases continue!

New entries

InterNetworX (#8), Enom (#17), 101Domain (#18), Todaynic (#19).

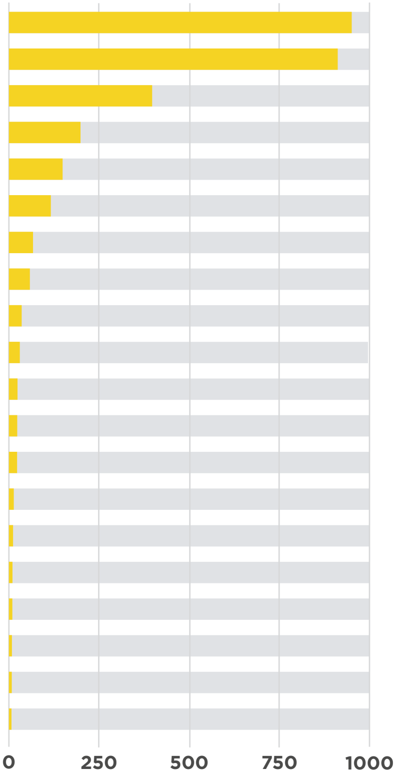
Departures

GMO, OwnRegistrar, R01, west263.com.

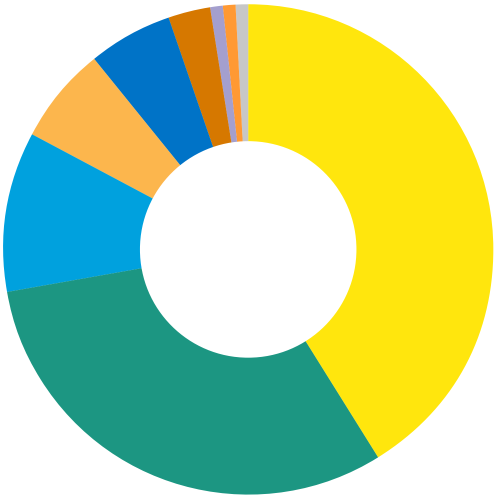
Most abused domain registrars, Q2 2023 (continued)

Most abused domain registrars - number of domains

Rank	Q1 2023	Q2 2023	% Change	Registrar	Country
#1	2109	919	-56%	NameSilo	Canada
#2	165	838	408%	Sav	United States
#3	1152	388	-66%	Namecheap	United States
#4	626	201	-68%	RegRU	Russia
#5	613	183	-70%	PDR	India
#6	108	168	56%	Xin	China
#7	149	90	-40%	Tucows	Canada
#8	-	89	New entry	InterNetworX	Germany
#9	375	76	-80%	Nicenic	China
#10	91	60	-34%	Alibaba	China
#11	395	58	-85%	Google	United States
#12	74	57	-23%	Porkbun	United States
#13	235	34	-86%	Hostinger	Lithuania
#14	43	29	-33%	Gandi	France
#15	48	25	-48%	Name.com	United States
#16	36	24	-33%	Openprovider	China
#17	-	21	New entry	ENom	Canada
#18	-	20	New entry	101Domain	Ireland
#19	-	18	New entry	Todaynic	China
#20	46	14	-70%	RU-Center	Russia



LOCATION OF MOST ABUSED DOMAIN REGISTRARS



	Country	Q2 2023	Q1 2023
🟨	United States	41.24%	29.17%
🟩	Canada	31.10%	31.62%
🟦	China	10.45%	15.43%
🟧	Russia	6.49%	10.18%
🟦	India	5.53%	8.58%
🟫	Germany	2.69%	n/a
🟪	Lithuania	1.03%	3.29%
🟧	France	0.88%	0.60%
⬜	Ireland	0.60%	n/a

Networks hosting the most newly observed botnet C&Cs, Q2 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.

Same providers, different ranks, but tencent.com remains #1

Usually, we see a reasonable amount of fluctuation in the names of network providers hosting botnet C&C infrastructure. However, in Q2, there were only three new entries; constant.com (#12), bt.com (#16), and huawei.com (#17). Sadly, tencent.com remains top of the leaderboard, with an increase of +27% quarter on quarter, taking it to 593 botnet C&Cs in Q2.

Uninet.net.mx is evidently struggling

Q2 saw uninet.net.mx, a Mexican provider, rising from #11 to #5, with the largest percentage increase (+128%) across all networks. We strongly recommend that providers experiencing significant increases relating to botnet C&Cs being hosted on their networks make their registration and vetting procedures more robust.

Thank you for addressing botnet C&C abuse on your network

A note of recognition to frantech.ca, privatelayer.com, and stark-industries.solutions, who all dropped out of the Top 20 in Q2. There were also significant reductions at hetzner.com (-33%), m247.com (-29%), and blnwx.com (-29%). Well done!

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

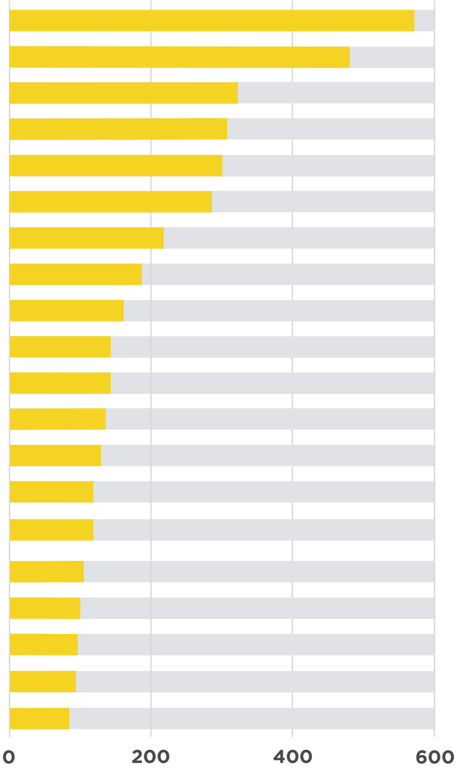
constant.com (#12), bt.com (#16), huawei.com (#17).

Departures

frantech.ca, privatelayer.com, stark-industries.solutions.

Networks hosting the most newly observed botnet C&Cs, Q2 2023 (continued)

Rank	Q1 2023	Q2 2023	% Change	Network	Country
#1	467	593	27%	tencent.com	China
#2	292	448	53%	alibaba-inc.com	China
#3	335	308	-8%	amazon.com	United States
#4	258	294	14%	delis.one	Netherlands
#5	126	287	128%	uninet.net.mx	Mexico
#6	318	270	-15%	digitalocean.com	United States
#7	302	202	-33%	hetzner.com	Germany
#8	182	177	-3%	aeza.net	Russia
#9	159	163	3%	ovh.net	France
#10	174	141	-19%	zerohost.io	Russia
#11	102	132	29%	stc.com.sa	Saudi Arabia
#12	-	125	New entry	constant.com	United States
#13	97	124	28%	microsoft.com	United States
#14	142	110	-23%	lethost.co	Russia
#15	81	95	17%	colocrossing.com	United States
#16	-	91	New entry	bt.com	United Kingdom
#17	-	90	New entry	huawei.com	China
#18	121	86	-29%	m247.com	Romania
#19	119	85	-29%	blnwx.com	Netherlands
#20	93	84	-10%	ielo.net	France



Networks hosting the most active botnet C&Cs, Q2 2023

Finally, let's review the networks that hosted the most significant number of active botnet C&Cs at the end of Q2 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.

At least the huge increases have ceased...

Last quarter we reported an alarming number of increases relating to networks hosting active botnet C&Cs. Eight network providers experienced triple-figure increases.

Thankfully the largest increase in Q2 was 49% (alibaba-inc.com). Disappointingly, we didn't witness triple-figure decreases, meaning there are still far too many active botnet C&Cs on networks, i.e., providers are still taking too long to deal with abuse reports.

The scale of the problem at the top of the chart

The Top 20 providers who are not quickly resolving botnet C&C issues had 899 active botnet C&Cs on their networks in Q2. Of these, tencent.com (#1), alibaba-inc.com (#2), amazon.com (#3), and digitalocean.com (#4) account for just under 50% of this total.

Admittedly, US-based providers amazon.com and digitalocean.com saw reductions in numbers in Q2, -28% and -33% respectively, which we applaud. Unfortunately, both Chinese-based networks, tencent.com and alibaba-inc.com, saw increases of 37% and 49%, respectively.

New entries

servinga.com (#9), waicore.com (#12), huawei.com (#12), oracle.com (#16), hostwinds.com (#16), google.com (#18), uplus.coo.kr (#18).

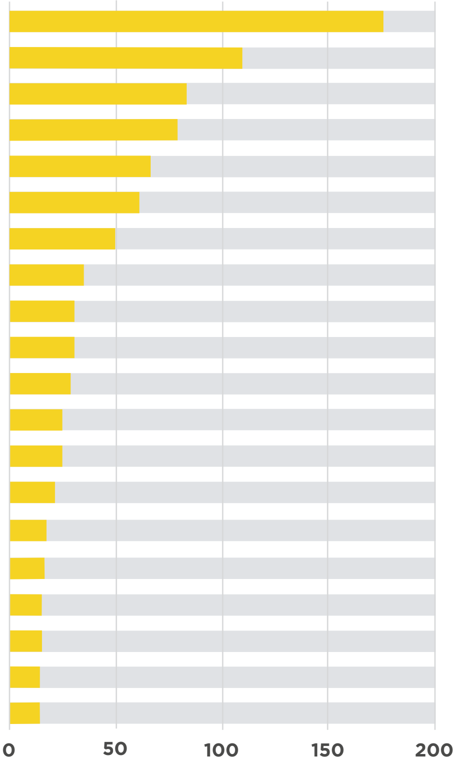
Departures

aeze.net, blnwx.com, charter.com, frantech.ca, hivelocity.net, lethost.co, linode.com.

Networks hosting the most active botnet C&Cs, Q2 2023 (continued)

Total number of active botnet C&Cs per network

Rank	Q1 2022	Q1 2023	% Change	Network	Country
#1	127	174	37%	tencent.com	China
#2	72	107	49%	alibaba-inc.com	China
#3	112	81	-28%	amazon.com	United States
#4	120	80	-33%	digitalocean.com	United States
#5	51	60	18%	ovh.net	France
#6	75	56	-25%	delis.one	Netherlands
#7	49	50	2%	hetzner.com	Germany
#8	25	34	36%	microsoft.com	United States
#9	-	33	New entry	servinga.com	Germany
#9	32	33	3%	constant.com	United States
#11	26	26	0%	colocrossing.com	United States
#12	-	24	New entry	waicore.com	Belarus
#12	-	24	New entry	huawei.com	China
#14	19	22	16%	contabo.de	Germany
#14	67	22	-67%	zerohost.io	Russia
#16	30	19	-37%	m247.com	Romania
#17	-	14	New entry	oracle.com	United States
#17	-	14	New entry	hostwinds.com	Luxembourg
#19	-	13	New entry	google.com	United States
#19	-	13	New entry	uplus.co.kr	Korea (Rep. of)



That's all for now. Stay safe, and see you in October 2023!