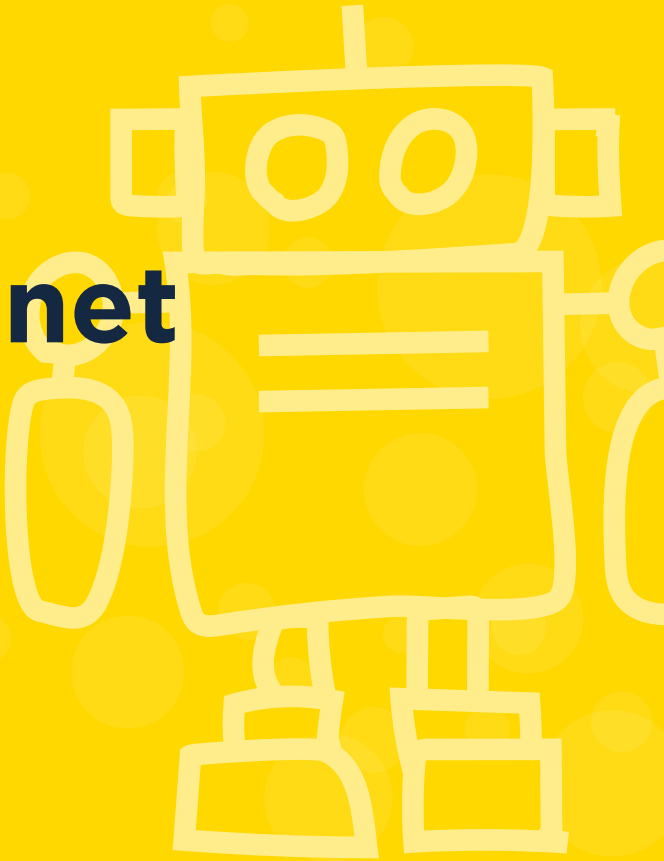
SPAMHAUS

Spamhaus Botnet Threat Update



Q4 2021

Q4 saw a 23% rise in the number of new botnet command and controllers (C&Cs) identified by our research team. Despite this increase, our researchers are aware of botnet C&C activity they cannot track due to communications being made via DNS over HTTPS (DoH). This is worrying and certainly tilts the scales in the cybercriminals' favor.

Welcome to the Spamhaus Botnet Threat Update Q4 2021.

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, and 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

The issues of DNS over HTTPS (DoH)

Remember FluBot & TeamBot from Q3?

Last quarter, we reported "an explosion in backdoor malware" due to FluBot & TeamBot. In Q4, from the perspective of botnet C&C infrastructure Spamhaus observed, this malware family completely disappeared. However, this doesn't mean they weren't active. That is far from the truth – they were active!

Why are they not being detected by Spamhaus?

This malware isn't appearing in our listings because those miscreants responsible for them have changed their operating procedures. Instead of making C&C communications using traditional HTTPS protocol, they use DNS over HTTPS (DoH) and abuse large DoH providers, including Google and Alibaba.

Preventing abuse on the internet gets harder

While DoH was heralded with fanfares and touted as the next best security development of the internet, some security professionals (including Spamhaus) sighed as they realized the good guys would lose even more visibility over what the bad guys were doing. And by "even more," we refer to other issues like losing visibility of WHOIS data.[1]

(1) www.spamhaus.org/news/article/775/how-has-gdpr-affected-spam

Why is DoH an issue?

DoH encrypts DNS traffic, making a resource private and secure that previously has always been public (unencrypted). You may be thinking that this has to be a good thing, however as you can see, in this circumstance, our researchers have no visibility of FluBot & TeamBot's DNS requests. Consequently, we can't list the IP addresses, and therefore this data can't be used to protect users. While DoH is meant to be protecting the internet community, it is also enabling cybercriminals. It's a double-edged sword.

Not only does DoH make hunting down miscreants even more challenging, but it also means that security products based around DNS monitoring and filtering could be less effective, which is far from ideal. Security issues are compounded due to major DoH providers not filtering harmful DNS resolutions of botnet, phishing or malware domains.

Number of botnet C&Cs observed, Q4 2021

In Q4 2021, Spamhaus identified 3,271 botnet C&Cs compared to 2,656 in Q3 2021. This was a 23% increase quarter on quarter. The monthly average increased from 885 in Q3 to 1,090 botnet C&Cs per month in Q4.

Quarter	No. of Botnets	Quarterly Average	% Change
Q1	1660	553	24%
Q2	1462	487	-12%
Q3	2656	885	82%
Q4	3271	1090	23%

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 2021

Russia continues with significant increases

We reported last quarter that the number of botnet C&Cs in Russia had increased dramatically. However, this quarter saw even bigger increases:

- Q1 to Q2 – 19% increase
- Q2 to Q3 – 64% increase
- Q3 to Q4 – 124% increase

In Q4, almost 30% of botnet C&C servers were located in Russia.

New entries

Ukraine (#12), Bulgaria (#15), Seychelles (#17), Hong Kong (#18).

Departures

Korea, Switzerland, Argentina, Vietnam.

LatAm presence continues

Several countries from Latin America (LatAm) were new entries in Q3 and remained in the Top 20 in Q4, including Mexico, Dominion Republic, Brazil, and Uruguay. Uruguay had the largest percentage increase (181%) of all geos in Q4.

Ups and downs across Europe

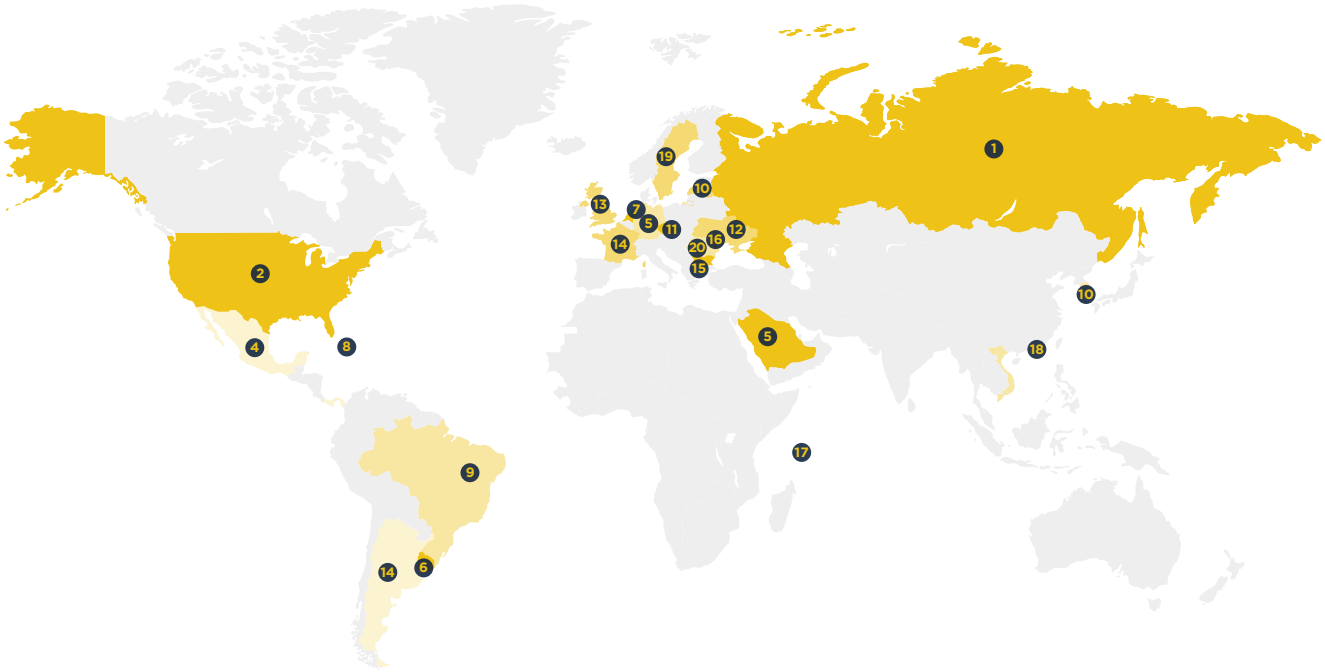
After continuing increases across various European countries, we're pleased to report that several have reduced numbers; the Netherlands, France, Sweden and Romania. Meanwhile, Switzerland has dropped off the Top 20 List completely. However, Germany has moved into third place with a 35% increase, and Great Britain has experienced a 56% increase.

Geolocation of botnet C&Cs, Q4 2021 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Q3 2021	Q4 2021	% Change Q on Q
#1	Russia	381	854	124%
#2	United States	301	384	28%
#3	Germany	170	230	35%
#4	Mexico	182	186	2%
#5	Saudi Arabia	117	180	54%
#6	Uruguay	63	177	181%
#7	Netherlands	273	164	-40%
#8	Dominican Rep	96	110	15%
#9	Brazil	86	92	7%
#10	Latvia	58	69	19%

Rank	Country	Q3 2021	Q4 2021	% Change Q on Q
#11	Czech Republic	40	66	65%
#12	Ukraine	-	64	New Entry
#13	United Kingdom	39	61	56%
#14	France	123	60	-51%
#15	Bulgaria	-	56	New Entry
#16	Moldova	49	50	2%
#17	Seychelles	-	34	New Entry
#18	Hong Kong	-	28	New Entry
#19	Sweden	38	26	-32%
#20	Romania	33	24	-27%



Malware associated with botnet C&Cs, Q4 2021

Credential stealers were the most prevalent malware type associated with Botnet C&Cs in Q4. This doesn't come as a surprise, given that the top two malware listed, RedLine & Loki, are both Credential Stealers.

GCleaner emerging

We saw a considerable uptick in GCleaner activity, leading to it being placed at #4, despite being a newcomer to the Top 20. GCleaner is similar to Smoke Loader in its modus operandi, and it is utilized in a Pay-Per-Install (PPI) model, dropping other malware on already infected hosts. While this malware threat has been around for some time, it is the first time that GCleaner has made it onto our Top 20 listings.

FluBot/TeamBot disappear

As discussed in our Spotlight section, this malware that had the #1 spot last quarter has disappeared from our listings; however, it is still operational having switched across to using DoH.

New entries

GCleaner (#4), DCRat (#10), Arkei (#14), TrickBot (#15), Socelars(#16).

Departures

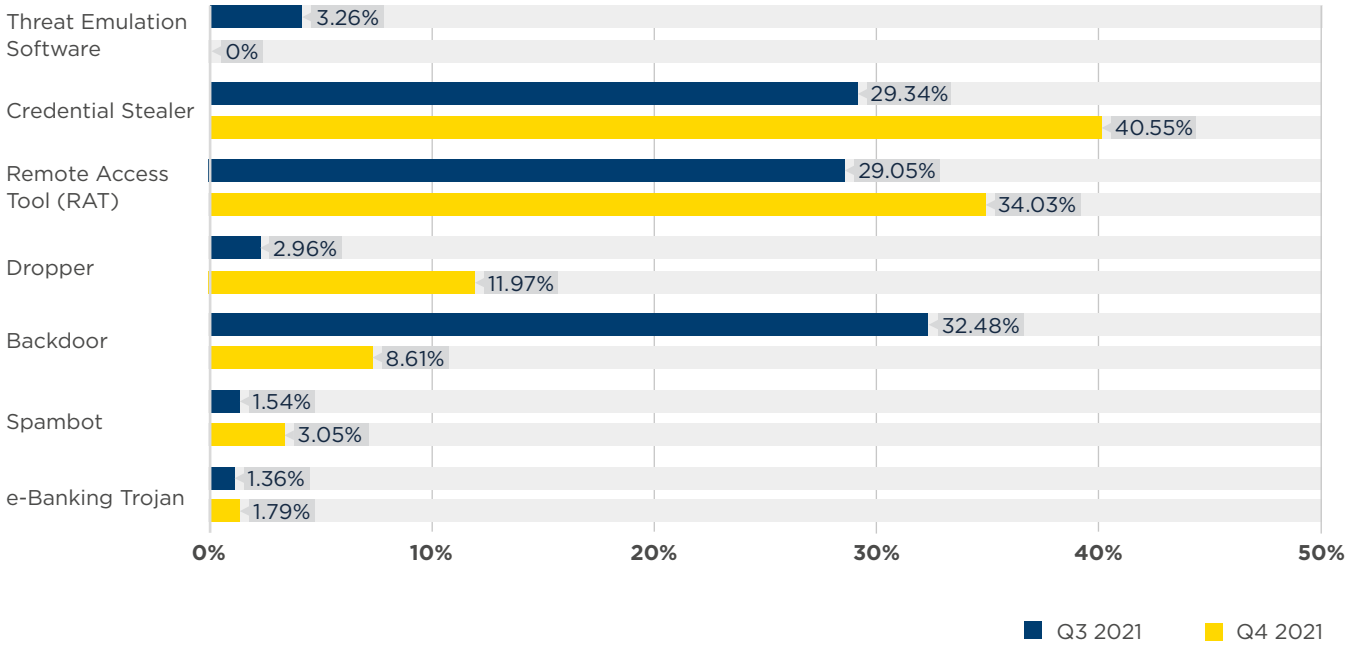
FluBot/TeamBot, AveMaria, ServHelper, QuasarRAT, AgentTesla.

Malware associated with botnet C&Cs, Q4 2021 (continued)

Malware families associated with botnet C&Cs

Rank	Q3 2021	Q4 2021	% Change	Malware Family	Description
#1	210	164	-22%	RedLine	Credential Stealer
#2	108	102	-6%	Loki	Credential Stealer
#3	121	91	-25%	AsyncRAT	Remote Access Tool (RAT)
#4	-	86	New Entry	GCleaner	Dropper
#5	93	75	-19%	Raccoon	Credential Stealer
#6	43	65	51%	Vjw0rm	Remote Access Tool (RAT)
#7	41	43	5%	CryptBot	Backdoor
#8	136	37	-73%	BitRAT	Remote Access Tool (RAT)
#9	71	36	-49%	NjRAT	Remote Access Tool (RAT)
#10	-	32	New Entry	DCRat	Remote Access Tool (RAT)
#11	26	29	12%	Tofsee	Spambot
#11	40	29	-28%	Remocs	Remote Access Tool (RAT)
#13	50	28	-44%	Smoke Loader	Dropper
#14	-	27	New Entry	Arkei	Credential Stealer
#15	-	21	New Entry	TrickBot	Backdoor
#16	-	18	New Entry	Socelars	Credential Stealer
#16	55	18	-67%	CobaltStrike	Backdoor
#18	23	17	-26%	Gozi	E-banking Trojan
#18	37	17	-54%	NanoCore	Remote Access Tool (RAT)
#18	30	17	-43%	STRRAT	Remote Access Tool (RAT)

Malware type comparisons between Q4 and Q3 2021



Most abused top-level domains, Q4 2021

A new entry at #4

We don't often see new TLD entries within the top five of this Botnet C&C Top 20; however, .xxx, an adult TLD, run by registry ICM, has entered at #4. With less than 10,000 active domains but a total of 223 domains associated with botnet C&C activity in Q4 we can only assume that there are problems.

.de reappears

The ccTLD de (Germany) re-entered our quarterly ranking at #20, having dropped off the Top 20 in Q2.

Reductions and departures

We'd like to congratulate all the registries that manage TLDs who departed from our listings along with those who significantly reduced the number of associated botnet C&Cs using their TLDs, including .buzz and .net, who both saw an 80% reduction.

Q3 data inaccuracy

Apologies to Verisign for an error in our Q3 2021 statistic for .com. We misreported the number of botnet C&Cs for the TLD, and the correct figure was 3,730. Various issues led to this error, but we are pleased to confirm that we have worked with Verisign to rectify these.

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q4 2021, .net had more than 13 million active domain zones, of which 0.00103% were associated with botnet C&Cs. Meanwhile, .xxx had just over 9,000 active domains, of which 2.4% were associated with botnet C&Cs. Both are in the top ten of our listings, but one had a much higher percentage of active domains associated with botnet C&Cs than the other.

Top-level domains (TLDs) a brief overview

There are several different top-level domains including:

Generic TLDs (gTLDs)
These can be used by anyone.

Country code TLDs (ccTLDs)
Some ccTLDs have restricted use within a particular country or region; however, others are licensed for general use giving them the same functionality of gTLDs.

Decentralized TLDs (dTLDs)
Independent top-level domains that are not under the control of ICANN.

Working together with the industry for a safer internet

Naturally, our preference is for no TLDs to have botnet C&Cs associated 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 with the sole purpose of distributing malware or hosting botnet C&Cs, we would like registries to suspend these domain names. We appreciate the efforts of many registries who work with us to ensure these actions are taken, including .xyz and .top.

New entries

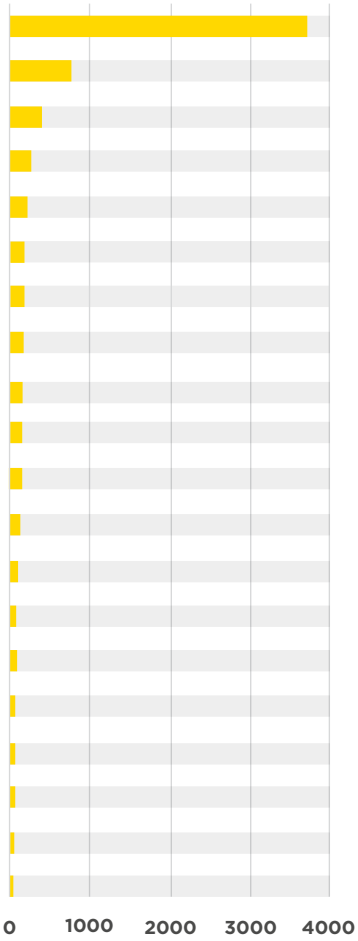
xxx (#4), site (#14), one (#15), gq (#16), sbs (#18), de (#20).

Departures

cn, su, club, eu, co, monster.

Top abused TLDs - number of domains

Rank	Q3 2021	Q4 2021	% Change	TLD	Note
#1	3730	3719	-0.2%	com	gTLD
#2	829	715	-14%	top	gTLD
#3	833	396	-52%	xyz	gTLD
#4	-	223	New Entry	xxx	gTLD
#5	132	143	8%	ga	Originally ccTLD, now effectively gTLD
#6	665	136	-80%	net	gTLD
#7	330	133	-60%	ru	ccTLD
#8	183	122	-33%	tk	Originally ccTLD, now effectively gTLD
#9	265	116	-56%	org	gTLD
#10	538	108	-80%	buzz	gTLD
#11	178	103	-42%	info	gTLD
#12	98	97	-1%	cf	Originally ccTLD, now effectively gTLD
#13	123	87	-29%	ml	Originally ccTLD, now effectively gTLD
#14	-	75	New Entry	site	gTLD
#15	-	70	New Entry	one	gTLD
#16	-	56	New Entry	gq	Originally ccTLD, now effectively gTLD
#17	82	52	-37%	cloud	gTLD
#18	-	51	New Entry	sbs	gTLD
#19	170	45	-74%	br	ccTLD
#20	-	44	New Entry	de	ccTLD



Most abused domain registrars, Q4 2021

Overall, we saw a decrease in fraudulent domain registrations in Q4 2021, which is positive news. But some countries' registrars are still clearly struggling.

United States based registrars

Registrars in the US had the most fraudulent botnet C&C registrations in Q4, overtaking China & Canada from Q3.

German based registrars

There was a noticeable increase (136%) in the number of botnet C&Cs associated with registrars operating out of Germany. This was due to Key Systems experiencing a 74% increase and 1API re-entering our charts at #12, having dropped off the Top 20 in Q2.

Atak

This domain registrar appeared for the first time in our rankings. Atak operates out of Turkey and hasn't responded to any of our abuse reports to date. We have therefore filed a complaint against Atak with ICANN's policy enforcement. It is imperative that everyone who is part of the internet ecosphere work together to protect internet users.

Nicenic.net (China) & PDR (India)

These registrars experienced significant increases in the number of botnet C&C domains registered through them in Q4. However, while registrations are increasing for PDR their response times to abuse reports are excellent.

Thank you to those who've departed from our listings

Last quarter we highlighted that CentralNic, West263, and Network Solutions had all experienced considerable increases in the number of newly registered botnet C&C domains. In Q4, all three of these registrars, along with eName, Xin Net, 22net, and OVH, departed from our Top 20 this quarter, so we'd like to applaud all their efforts in preventing fraudulent registrations.

Registrars and botnet C&C operators

Cybercriminals need to find a sponsoring registrar to register a botnet C&C domain name. Registrars can't easily detect all fraudulent registrations before these domains go live. However, the 'life span' of criminal domains on a legitimate, well-run registrar tends to be relatively short.

New entries

1API (#12), Beget (#14), Sav.com (#15), Hostinger (#16), Atak (#18), Naunet (#19), EuroDNS (#20), Mat Bao Corporation (#20).

Departures

eName, CentralNic, Network Solutions, Xin Net, west263.com, 22net, OVH.

Most abused domain registrars, Q3 2021 (continued)

Most abused domain registrars - number of domains

Rank	Q3 2021	Q4 2021	% Change	Registrar	Country
#1	1568	988	-37%	NameSilo	United States
#2	1267	718	-43%	Namecheap	Canada
#3	209	536	156%	nicenic.net	China
#4	169	433	156%	PDR	India
#5	188	328	74%	Key Systems	Germany
#6	154	272	77%	WebNic.cc	Singapore
#7	1217	201	-83%	Alibaba	China
#8	165	197	19%	Openprovider	Netherlands
#9	189	135	-29%	Eranet International	China
#10	403	127	-68%	Tucows	Canada
#11	475	124	-74%	RegRU	Russia
#12	-	115	New Entry	1API	Germany
#13	403	80	-80%	Porkbun	United States
#14	-	68	New Entry	Beget LLC	Russia
#15	-	66	New Entry	Sav.com	United States
#16	-	57	New Entry	Hostinger	Lithuania
#17	214	54	-75%	dnspod.cn	China
#18	-	51	New Entry	Atak	Turkey
#19	-	49	New Entry	NauNet	Russia
#20	-	48	New Entry	Mat Bao Corporation	Vietnam
#20	-	48	New Entry	EuroDNS	Luxemberg

LOCATION OF MOST ABUSED DOMAIN REGISTRARS

Country	Botnets	%
United States	1134	24.15%
China	926	19.72%
Canada	845	18.00%
Germany	443	9.44%
India	433	9.22%
Singapore	272	5.79%
Russia	241	5.13%
Netherlands	197	4.20%
Lithuania	57	1.21%
Turkey	51	1.09%
Luxemberg	48	1.02%
Vietnam	48	1.02%
Total	**4695**	

Networks hosting the most newly observed botnet C&Cs, Q4 2021

As usual, there were many changes in the networks hosting newly observed botnet C&Cs.

Does this list reflect how quickly abuse is dealt with at networks?

While this Top 20 listing illustrates that there may be an issue with customer vetting processes, it doesn't reflect on the speed abuse desks deal with reported issues. See "Networks hosting the most active botnet C&Cs" to view networks where abuse isn't dealt with promptly.

A mixed bag

Uninet.net.mx (#1), serverion.com (#5) and cloudflare.com (#9) – all three appear within the Top 10 of our listings, but there are big differences between them.

Uninet is a telecom and network operator in Mexico. All newly hosted botnet C&Cs we identified in their IP space resulted from compromised customer equipment.

Serverion is a hosting company based in the Netherlands. All botnet C&Cs we identified on their network in Q4 resulted from fraudulent sign-ups.

Last but not least, we have Cloudflare who is not hosting any content rather providing a reverse proxy service and DDoS protection to botnet C&Cs, hiding their actual location.

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, this doesn't often happen, thankfully.

New entries

selectel.ru (#10), timeweb.ru (#12), firstbyte.ru (#13), pinvds.com (#15), ihor-hosting.ru (#18), itldc.com (#19), m247.ro (#20).

Departures

ipjetable.net, pq.hosting, ovh.com, mivocloud.com, telefonica.com.ar, uplus.co.kr, mgnhost.ru.

Networks hosting the most newly observed botnet C&Cs, Q4 2021 (continued)

Newly observed botnet C&Cs per network

Rank	Q3 2021	Q4 2021	% Change	Network	Country
#1	177	187	6%	uninet.net.mx	Mexico
#2	33	182	452%	alibaba-inc.com	China
#3	63	175	178%	antel.net.uy	Uruguay
#4	105	168	60%	stc.com.sa	Saudi Arabia
#5	115	116	1%	serverion.com	Netherlands
#6	95	110	16%	claro.com.do	Dominican Rep
#7	58	85	47%	telefonica.com.br	Brazil
#8	44	80	82%	baxet.ru	Russia
#9	68	72	6%	cloudflare.com	United States
#10	-	63	New entry	selectel.ru	Russia
#11	44	51	16%	nano.lv	Latvia
#12	-	49	New entry	timeweb.ru	Russia
#13	-	48	New entry	firstbyte.ru	Russia
#13	33	48	45%	hostwinds.com	United States
#15	-	47	New entry	pinvds.com	Russia
#16	89	39	-56%	privacyfirst.sh	Germany
#17	51	38	-25%	hetzner.de	Germany
#18	-	36	New entry	ihor-hosting.ru	Russia
#19	-	35	New entry	itldc.com	Ukraine
#20	-	34	New entry	m247.ro	Romania

Networks hosting the most active botnet C&Cs, Q4 2021 (continued)

Finally, let's review the networks that hosted the largest number of active botnet C&Cs at the end of 2021. Hosting providers who appear in this ranking either have an abuse problem, do not take the appropriate action when receiving abuse reports, or omit to notify us when an abuse problem has been dealt with.

New entries

al.bg (#8), mobily.com.sa (#12), ielo.net (#13), google.com (#16), combahton.net (#16).

Departures

serverion.com, uplus.co.kr, hostry.com, skbroadband.com, claro.com.co.

Network operators in LatAm region need to get on top of abuse rapidly

Over 60% of active botnet C&C listings are on networks located in the LatAm region. We implore these operators to quickly respond to abuse reports and work with Spamhaus to reduce botnet C&C abuse on their networks.

Total number of active botnet C&Cs per network (as per 31st of December 2021)

Rank	Q3 2021	Q4 2021	% Change	Network	Country
#1	185	389	110%	uninet.net.mx	Mexico
#2	119	296	149%	stc.com.sa	Saudi Arabia
#3	68	257	278%	antel.net.uy	Uruguay
#4	97	204	110%	claro.com.do	Dominican Rep
#5	63	146	132%	telefonica.com.br	Brazil
#6	79	94	19%	microsoft.com	United States
#7	99	91	-8%	ipjetable.net	France
#8	-	60	New Entry	a1.bg	Bulgaria
#9	41	41	0%	telefonica.com.ar	Argentina
#10	29	29	0%	tie.cl	Chile
#10	32	29	-9%	vietserver.vn	Vietnam
#12	-	27	New Entry	mobily.com.sa	Saudi Arabia
#13	-	25	New Entry	ielo.net	France
#14	21	24	14%	clouvider.net	United Kingdom
#15	24	22	-8%	ovpn.com	Sweden
#16	22	21	-5%	charter.com	United States
#16	-	21	New Entry	google.com	United States
#16	21	21	0%	algartelecom.com.br	Brazil
#16	21	21	0%	une.net.co	Colombia
#16	-	21	New Entry	combahton.net	Germany