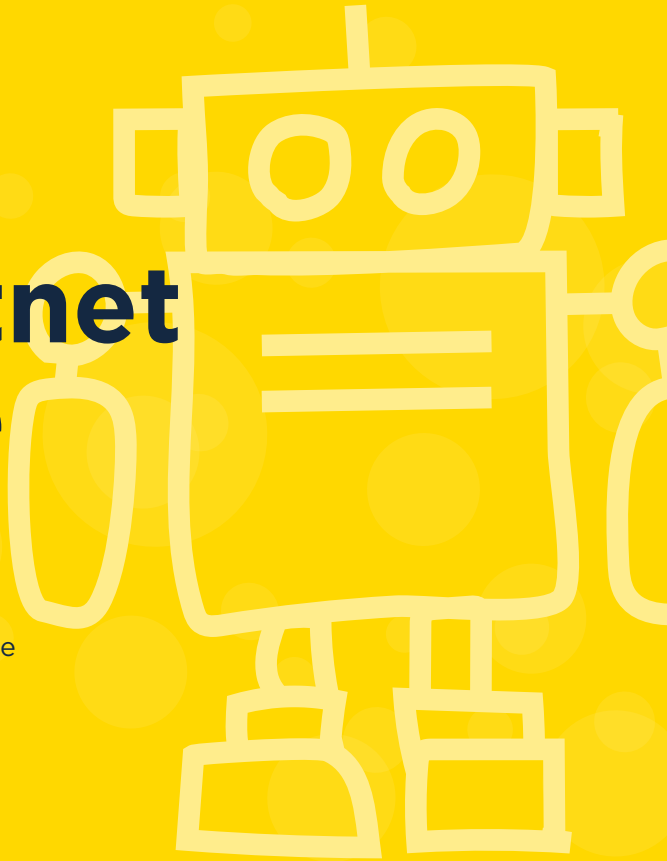
SPAMHAUS

Spamhaus Botnet Threat Update



Q1 2022

In the first quarter of 2022, there was a modest 8% increase in the number of new botnet command and controllers (C&Cs) identified by our research team. Positives such as the demise of TrickBot were countered by the continuing inability of network operators in LatAm to deal effectively with active abuse reports. Meanwhile, there was a disproportionate amount of abuse where registries and registrars apply cheap and free business models.

Welcome to the Spamhaus Botnet Threat Update Q1 2022.

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

Freenom – when free domains become a problem

Something for nothing

We all love it when we don't have to pay for a service we use. Freenom, a domain registration service located in the Netherlands, offer just that - they provide some domain registration services for free. In fact, according to Freenom's website[1], "Freenom is the world's first and only free domain provider".

Sounds great, doesn't it? From our point of view, the answer is a resounding "No" because, unfortunately, free services do not tend to attract purely legitimate users and businesses. Instead, they usually attract less desirable users, and those kinds of users bring with them a whole load of badness, i.e. abuse.

The problematic top-level domains

Freenom operates (via agreements with the relevant registry[2]) the following five country code top-level domains (ccTLDS):

- .tk (ccTLD of Tokelau)
- .ml (ccTLD of Mali)
- .ga (ccTLD of Gabon)
- .cf (cc TLD of Central African Republic)
- .gq (cc TLD of Equatorial Guinea)

(1) www.freenom.com/en/freeandpaiddomains.html
(2) domainincite.com/17468-freenom-ads-gq-to-free-african-cctld-roster

While domain registrants will commonly use ccTLDs for their applicable country, these five ccTLDs operated by Freenom, to all intents and purposes, became general top-level domains (gTLDs), primarily being used outside their country.

Where's the abuse?

As you will see when reading through our report, all five Freenom TLDs made it into our quarterly ranking of the most abused TLDs used in domain registrations for botnet C&Cs.

A more detailed review of our data reveals that the majority of fraudulent domain registrations within Freenom's TLDs are not linked to highly advanced and sophisticated threat actors, but users of freely available crimeware kits that they have bought for a few bucks on the dark web. These somewhat "amateur" threat actors do not have the same financial resources as more "professional" cybercriminals. Therefore, it is no surprise that they try to (ab)use services that are available for free – such as Freenom offers.

The abuse goes beyond botnet C&Cs

Last year, PhishLabs published a report on Breaking down phishing site TLDs and certificate abuse[1]. This highlighted that out of the Top 10 most abused TLDs, seven were ccTLDs, and out of that seven (yes - you've guessed it), five were the above ccTLDs that users can register for free through Freenom.

(1) www.phishlabs.com/blog/breaking-down-phishing-site-tlds-and-certificate-abuse-in-q1/

Meanwhile, if you take a look at the Top 10 most abused TLDs[1], which determines the "badness" of a TLD, all five of Freenom's TLDs make an appearance.

The 10 Most Abused Top Level Domains

As of 14 April 2022 the TLDs with the worst reputations for spam operations are:

Rank	Domain	Badness Index	Domains seen	Bad domains	%
#1	.cn	3.82	135,203	47,939	35.5%
#2	.surf	3.60	3,182	1,557	48.9%
#3	.gq	2.94	8,976	3,259	36.3%
#4	.ga	2.87	13,717	4,661	34.0%)
#5	.cf	2.72	12,431	4,071	32.7%
#6	.tk	2.38	36,192	9,411	26.0%
#7	.ml	2.32	21,396	5,732	26.8%
#8	.work	2.01	34,974	7,830	22.4%
#9	.top	1.79	75,593	14,177	18.8%
#10	.cam	1.56	7,782	1,642	21.1%

It's evident that where there's a freebie, there's abuse!

(1) www.spamhaus.org/statistics/tlds/

Number of botnet C&Cs observed, Q1 2022

In Q1 2022, Spamhaus identified 3,538 botnet C&Cs compared to 3,271 in Q4 2021. This was an 8% increase quarter on quarter. The monthly average increased from 1,090 in Q4 to 1,179 botnet C&Cs per month in Q1.

Quarter	No. of Botnets	Quarterly Average	% Change
Q2, 2021	1462	487	-12%
Q3, 2021	2656	885	+82%
Q4, 2021	3271	1090	+23%
Q1, 2022	3538	1179	+8%

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, Q1 2022

A year of increases for Russia

For the past year, the number of botnet C&Cs in Russia has continued to increase, quarter on quarter:

- 2021 Q1 to Q2 – 19% increase
- 2021 Q2 to Q3 – 64% increase
- 2021 Q3 to Q4 – 124% increase
- 2021 Q4 to 2022 Q1 – 24% increase

In Q1, approximately one-third of all botnet C&C servers that our researchers observed were located in Russia.

New entries

United Arab Emirates (#15), Estonia (#16).

Departures

Sweden, Romania.

Increase in Botnet C&Cs hosted in the West

Besides the continuing increase of botnet C&Cs hosted in Russia, we have also noticed an increase in hosting across the West, notably in the Ukraine (+80%), France (+23%), United States (+20%), the Netherlands (+16%), and Estonia (newcomer). The increase in the Ukraine isn't surprising given the ongoing conflict – miscreants are one of the first to find vulnerabilities, and profit.

Marginal improvements in LatAm

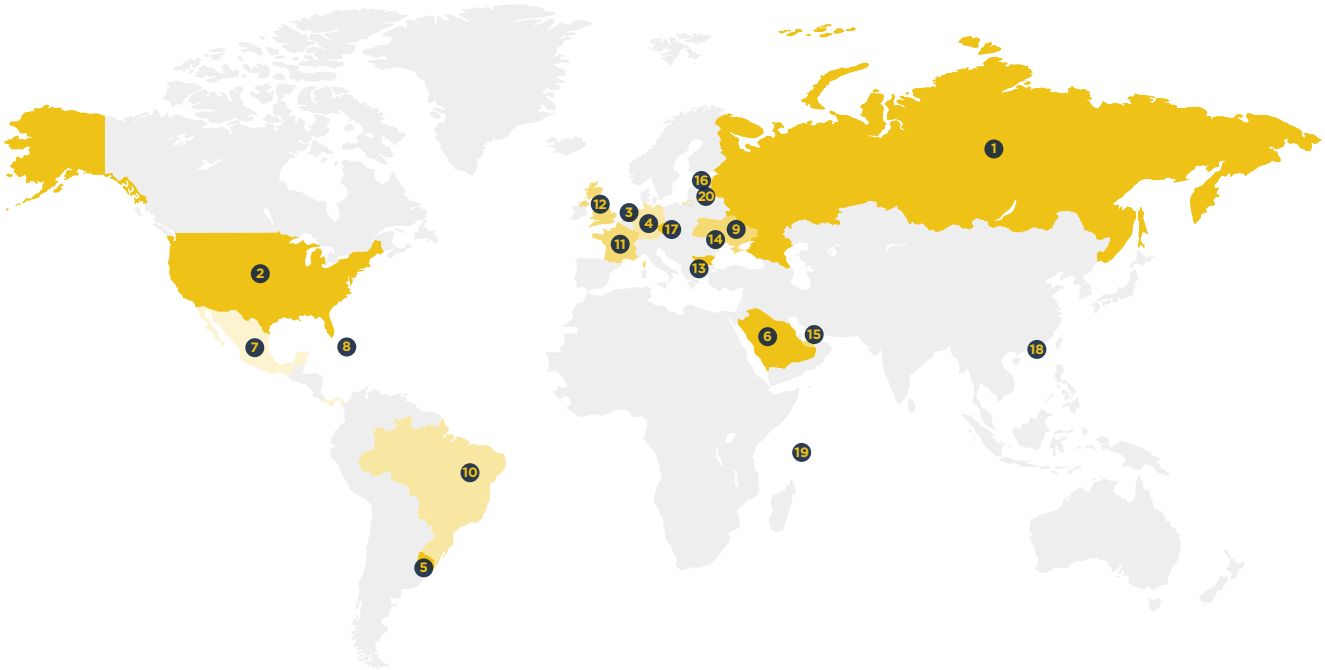
At the end of 2021, LatAm countries experienced a significant increase in botnet C&Cs they were hosting. This quarter saw a slight reduction in these numbers; Uruguay (-4%), Mexico (-12%), Brazil (-20%), with the exception of the Dominican Republic, which experienced a 16% increase. There is significant room for improvement across this region when handling abuse.

Geolocation of botnet C&Cs, Q1 2022 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Q4 2021	Q1 2022	% Change Q on Q
#1	Russia	854	1059	24%
#2	United States	384	461	20%
#3	Netherlands	164	191	16%
#3	Germany	230	191	-17%
#5	Uruguay	177	170	-4%
#6	Saudi Arabia	180	163	-9%
#6	Mexico	186	163	-12%
#8	Dominican Rep	110	128	16%
#9	Ukraine	64	115	80%
#10	France	60	74	23%

Rank	Country	Q4 2021	Q1 2022	% Change Q on Q
#10	Brazil	92	74	-20%
#12	United Kingdom	61	64	5%
#13	Bulgaria	56	62	11%
#14	Moldova	50	54	8%
#15	UAE	-	47	New Entry
#16	Estonia	-	45	New Entry
#17	Czech Republic	66	40	-39%
#18	Hong Kong	28	38	36%
#19	Seychelles	34	37	9%
#19	Latvia	69	37	-46%



Malware associated with botnet C&Cs, Q1 2022

Spoiler alert! There was no change at the top of quarterly malware charts - RedLine and Loki, both credential stealers, stayed at the top of our chart.

Malware as a service

While we have seen a small decrease in the number of RedLine botnet C&C servers, our researchers have detected a 47% increase in Loki ones. Both are being sold on the dark web as "crimeware" kits, allowing anyone who buys one to operate their own malware operation.

Farewell, TrickBot!

For many years, TrickBot was one of the major botnets, constantly in and out of our Top 20 listings. Initially, it was an ebanking Trojan; however, it evolved into a dropper, providing cybercriminals with initial access to corporate networks. In this role, TrickBot heavily targeted the U.S. economy and was responsible for cyber-attacks against hundreds of American companies.

In 2020, TrickBot managed to survive takedown attempts by both Microsoft and the US Cyber Command[1]. Now in Q1 2022, TrickBot suddenly vanished from the malware threat landscape. Security researchers confirmed in a tweet[2] that the notorious TrickBot malware gang had both its operation and infrastructure shutdown. Farewell, TrickBot – we won't miss you!

Tofsee, Smoke Loader and Arkei continue to gain popularity

In 2021 all three of the above malware entered our Top 20 and over the past quarter, they all experienced increases of 100% and more!

What is a credential stealer?

Cybercriminals use these to harvest sensitive information, e.g. log-in details, from a victim's machine.

New entries

AveMaraia (#14), Quasar (#17), CoinMiner (#18), DanaBot (#20).

Departures

CobaltStrike, CryptBot, Gozi, TrickBot.

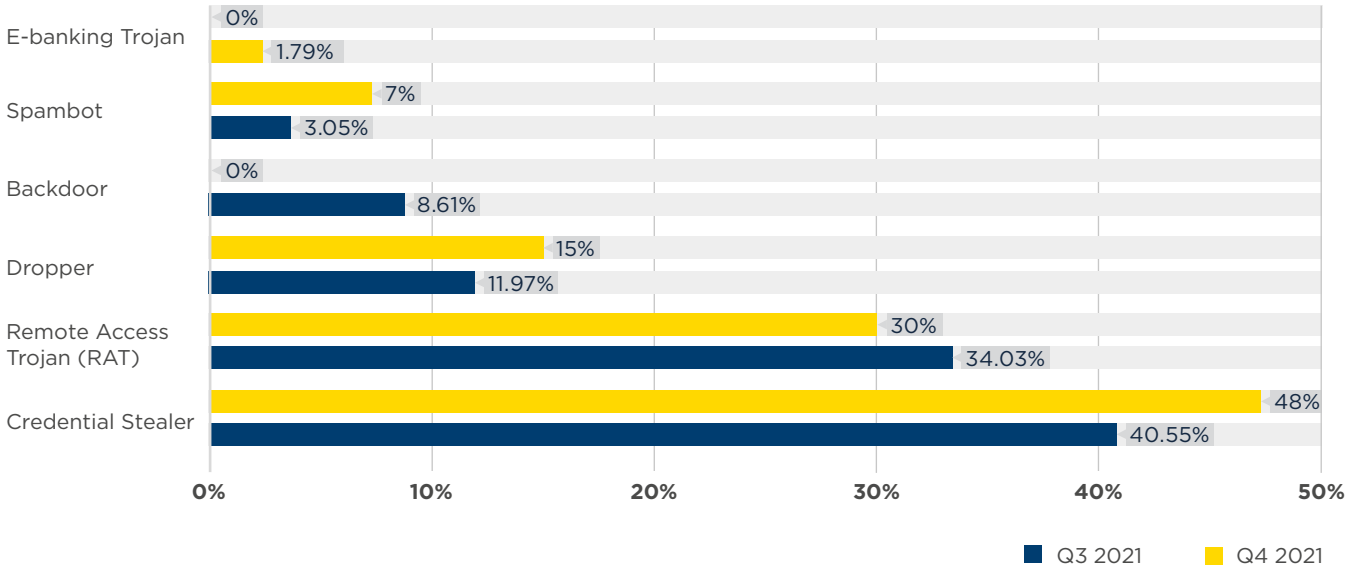
(1) www.cyberscoop.com/trickbot-takedown-cyber-command-microsoft/
(2) twitter.com/VK_Intel/status/1496944228135493638

Malware associated with botnet C&Cs, Q1 2022 (continued)

Malware families associated with botnet C&Cs

Rank	Q4 2022	Q4 2021	% Change	Malware Family	Description
#1	164	153	-7%	RedLine	Credential Stealer
#2	102	150	47%	Loki	Credential Stealer
#3	91	74	-19%	AsyncRAT	Remote Access Trojan (RAT)
#4	86	66	-23%	GCleaner	Dropper
#5	29	59	103%	Tofsee	Spambot
#5	28	59	111%	Smoke Loader	Dropper
#7	27	54	100%	Arkei	Credential Stealer
#8	75	37	-51%	Raccoon	Credential Stealer
#9	32	32	0%	DCRat	Remote Access Trojan (RAT)
#10	17	26	53%	NanoCore	Remote Access Trojan (RAT)
#11	29	23	-21%	Remcos	Remote Access Trojan (RAT)
#12	17	22	29%	STRRAT	Remote Access Trojan (RAT)
#13	36	20	-44%	NjRAT	Remote Access Trojan (RAT)
#14	-	19	New Entry	AveMaria	Remote Access Trojan (RAT)
#15	18	18	0%	Socelars	Credential Stealer
#16	37	16	-57%	BitRAT	Remote Access Trojan (RAT)
#17	-	13	New Entry	Quasar	Remote Access Trojan (RAT)
#18	65	12	-82%	Vjw0rm	Remote Access Trojan (RAT)
#18	-	12	New Entry	CoinMiner	Cryptocurrency miner
#20	-	10	New Entry	DanaBot	Credential Stealer

Malware type comparisons between Q4 2021 and Q1 2022



Most abused top-level domains, Q1 2022

Most abused top-level domains, Q1 2022

Unsurprisingly, there has been no change at the top of our quarterly ranking - gTLD .com continues to be the preferred TLD for malware authors and botnet operators to use for registering their domain names.

Meanwhile, the Chinese operated gTLD .top stays at #2 in our charts. There was some improvement in Q1, with a 30% reduction in the number of newly observed botnet C&C domains. However, .top still had well over double the number of domains associated with botnet C&Cs than .xyz at #3.

A new entry at #4

This quarter .us entered the Top 20 straight in at #4. We can only hope that GoDaddy, who is responsible for .us, can follow in the steps of .buzz which entered our chart at #3 one year ago, but dropped out of the ranking this quarter. Thank you for addressing the abuse associated with your TLD, dotStrategy – it's time to follow suit, GoDaddy!

Departures

Speaking of departures, we'd like to congratulate all those registries that manage TLDs who departed from our listings, including ICM, which is responsible for .xxx. This TLD entered the Top 20 in Q4 2021 at #4, but it exited our listings this quarter.

Verisign's .com & .net see significant decreases

Both of Verisign's TLDs, .com and .net had the largest decreases in Q1; -75% and -61% respectively. These were closely followed by .xyz who experienced a -52% decrease. Nice work all round! Keep those figures reducing.

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.

Most abused top-level domains, Q1 2022 (continued)

.tk, .cf, .ml, .ga and .gq

In this quarter's "Spotlight" we discussed the issues with these five ccTLDs, which are now operated by Freenom. They continue to pose a severe threat to internet users and businesses. In Q1 2022, we have in total identified 579 botnet C&C domains registered in Freenom's domain name space. That's a lot!

Fraudulent domain registrations in .sbs and .cloud more than doubled

The number of fraudulent domain registrations observed by Spamhaus in the two gTLDs .sbs and .cloud more than doubled in Q1 2022; 145% (.sbs) and 140% (.cloud).

Last year, we raised concerns about activities our researchers had started to observe relating to .sbs[1]. Unfortunately, this message appears to have fallen on deaf ears. We urge the corresponding registries, ShortDot and Aruba PEC SpA, to take meaningful measures to reduce the number of botnet C&C domains registered in their domain name space.

Interpreting the data

Registries with a greater number of active domains have greater exposure to abuse. For example, in Q1 2022, .de had more than 6.3 million active domain zones, of which 0.00093% were associated with botnet C&Cs. Meanwhile, .sbs had just over 30,000 active domain zones, with 0.42% associated with botnet C&Cs. Both are in the Top 20 of our listings. Still, one had a much higher percentage of active domains related to botnet C&Cs than the other.

New entries

.us (#4), .website (#13), .cn (#18), .live (#19), .cfd (#20)

Departures

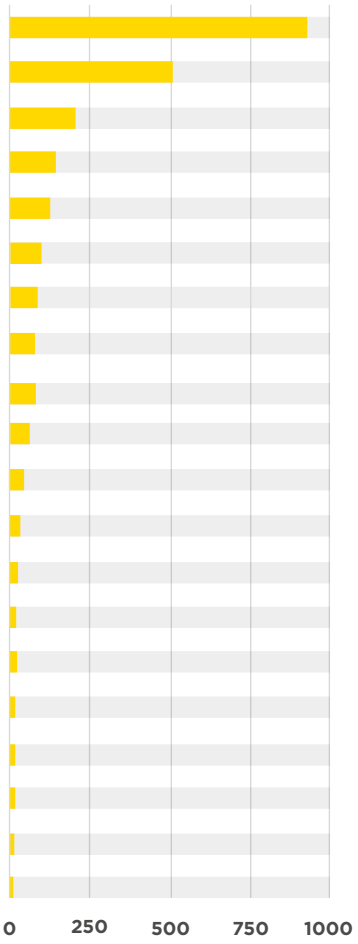
.br, .buzz, .one, .site, .xxx

(1) www.spamhaus.com/resource-center/we-hope-you-keep-sbs-clean-shortdot/

Most abused top-level domains, Q1 2022 (continued)

Top abused TLDs - number of domains

Rank	Q4 2021	Q1 2022	% Change	TLD	Note
#1	3719	913	-75%	com	gTLD
#2	715	501	-30%	top	gTLD
#3	396	192	-52%	xyz	gTLD
#4	-	165	New Entry	us	gTLD
#5	122	159	30%	tk	Originally ccTLD, now effectively gTLD
#6	116	137	18%	org	gTLD
#7	97	126	30%	cf	Originally ccTLD, now effectively gTLD
#8	51	125	145%	sbs	gTLD
#8	52	125	140%	cloud	gTLD
#10	87	115	32%	ml	Originally ccTLD, now effectively gTLD
#11	143	106	-26%	ga	Originally ccTLD, now effectively gTLD
#12	56	73	30%	gq	Originally ccTLD, now effectively gTLD
#13	-	70	New Entry	website	gTLD
#14	103	67	-35%	info	gTLD
#15	133	66	-50%	ru	ccTLD
#16	44	59	34%	de	ccTLD
#17	136	53	-61%	net	gTLD
#18	-	45	New Entry	cn	ccTLD
#19	-	43	New Entry	live	gTLD
#20	-	42	New Entry	cfd	gTLD



Most abused domain registrars, Q1 2022

No changes at the top

Sadly, we have seen no changes at the top of this chart. With NameSilo and Namecheap holding onto the #1 and #2 spots.

However, the United States has just edged past Canada (with less than a 1% lead) to be the country where the most abused domain registrars are located.

Google enters the Top 20

We are exceptionally disappointed to see Google enter this list for the first time, with a new entry at #16. We hope that this is just a temporary "visit" and that Google takes robust action to reduce the number of domain registrations for botnet C&Cs that they are allowing to take place.

What's happening at Sav?

In Q1, Sav experienced a 156% increase, from 66 botnet C&C domain name registrations to 169, propelling it to #6. Recently Sav reported it had doubled the number of domains under its management to two million in just six months[1]. The number of domains registered for botnet C&C abuse more than doubled last quarter. Does exponential growth have to bring exponential abuse? We don't think so.

Registrars improving

It's not all bad news. In Q1, we have seen six registrars depart from our Top 20, along with improvements at thirteen domain registrars, including Key Systems (-91%), WebNic (-90%), and Openprovider (-62%). Well done to all registrars who've departed from our listings, and nice work to those who have seen reductions in domain registrations, but there is still quite a way to go!

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

Todaynic (#5), Ligne (#13), CentralNic (#14), GMO (#15), Google (#16).

Departures

1API, Atak, Beget LLC, Eranet International, Mat Bao Corp, NauNet.

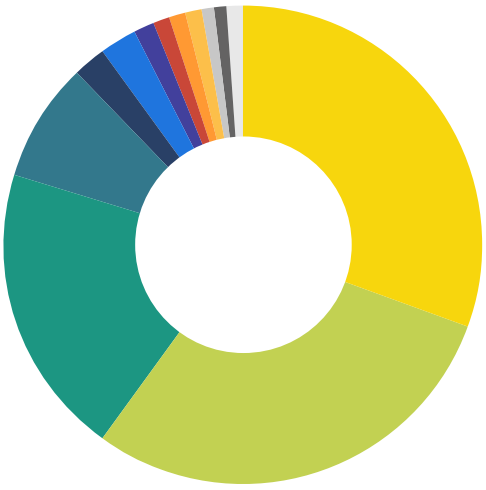
(1) www.dnjournal.com/archive/lowdown/2022/dailyposts/20220409.htm

Most abused domain registrars, Q1 2022 (continued)

Most abused domain registrars - number of domains

Rank	Q4 2021	Q1 2022	% Change	Registrar	Country
#1	988	847	-14%	NameSilo	Canada
#2	718	670	-7%	Namecheap	United States
#3	536	266	-50%	nicenic.net	China
#4	433	255	-41%	PDR	India
#5	-	236	New Entry	Todaynic	China
#6	66	169	156%	Sav	United States
#7	80	96	20%	Porkbun	United States
#8	201	88	-56%	Alibaba	China
#9	127	87	-31%	Tucows	Canada
#10	197	75	-62%	Openprovider	Netherlands
#11	124	73	-41%	RegRU	Russia
#12	57	50	-12%	Hostinger	Lithuania
#13	-	36	New Entry	Ligne	France
#14	-	35	New Entry	CentralNic	United Kingdom
#15	-	31	New Entry	GMO	Japan
#16	-	30	New Entry	Google	United States
#16	54	30	-44%	dnspod.cn	China
#18	328	28	-91%	Key Systems	Germany
#18	48	28	-42%	EuroDNS	Luxemberg
#20	272	27	-90%	WebNic.cc	Singapore

LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Q4 2021	Q1 2022
United States	20.43%	30.57%
Canada	26.37%	29.59%
China	18.70%	19.64%
India	10.24%	8.08%
Netherlands	4.66%	2.38%
Russia	2.93%	2.31%
Lithuania	1.35%	1.58%
France	0.00%	1.14%
United Kingdom	0.00%	1.11%
Japan	0.00%	0.98%
Germany	7.76%	0.89%
Luxemberg	1.14%	0.89%
Singapore	6.43%	0.86%

Networks hosting the most newly observed botnet C&Cs, Q1 2022

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.

Many newcomers from Russia

One of the things you will quickly notice when reading through our most recent Top 20 is the number of Russian new entries.

In Q1 2022, six out of the eight newcomers were hosting providers located in Russia. Combined they hosted more than 39% of the total number of botnet C&Cs – over three times the number hosted in Q4 2021.

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

vdsina.ru (#7), macloud.ru (#9), digitalenergy.online (#12), invs.ru (#12), ghostnet.de (#14), filanco.ru (#15), gcore.lu (#16), sprinthost.ru (#17), hostsailor.com (#18).

Departures

firstbyte.ru, hetzner.de, itldc.com, m247.ro, nano.lv, pinvds.com, privacyfirst.sh, serverion.com, timeweb.ru

Networks hosting the most newly observed botnet C&Cs, Q1 2022 (continued)

Newly observed botnet C&Cs per network

Rank	Q4 2021	Q1 2022	% Change	Network	Country
#1	175	170	-3%	antel.net.uy	Uruguay
#2	187	163	-13%	uninet.net.mx	Mexico
#3	168	153	-9%	stc.com.sa	Saudi Arabia
#4	110	128	16%	claro.com.do	Dominican Rep
#5	80	121	51%	baxet.ru	Russia
#6	182	95	-48%	alibaba-inc.com	China
#7	-	69	New Entry	vdsina.ru	Russia
#7	85	69	-19%	telefonica.com.br	Brazil
#9	-	63	New Entry	macloud.ru	Russia
#9	48	63	31%	hostwinds.com	United States
#9	63	63	0%	selectel.ru	Russia
#12	-	62	New Entry	digitalenergy.online	Russia
#12	-	62	New Entry	invs.ru	Russia
#14	-	61	New Entry	ghostnet.de	Germany
#15	-	54	New Entry	filanco.ru	Russia
#16	-	53	New Entry	gcore.lu	Luxembourg
#17	-	52	New Entry	sprinthost.ru	Russia
#18	-	51	New Entry	hostsailor.com	UAE
#18	36	51	42%	ihor-hosting.ru	Russia
#20	72	49	-32%	cloudflare.com	United States

Networks hosting the most active botnet C&Cs, Q1 2022

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

cableonda.net (#12), eliteteam.to (#15), ntup.net (#15), alexhost.md (#17), selectel.ru (#19).

Departures

algartelecom.com.br, charter.com, clouvider.net, ovpn.com, une.net.co.

LatAm network operators continue to struggle with abuse

As previously reported in the last Botnet Update, operators within the LatAm region are struggling to respond to abuse reports promptly. In Q1 2022, this region continued to be accountable for hosting over 60% of active botnet C&Cs, with four out of the top five hosting companies located in LatAm.

Spamhaus urges these operators to work together with us to help address abuse on their networks.

Total number of active botnet C&Cs per network

Rank	Q4 2021	Q1 2022	% Change	Network	Country
#1	389	501	29%	uninet.net.mx	Mexico
#2	296	422	43%	stc.com.sa	Saudi Arabia
#3	257	398	55%	antel.net.uy	Uruguay
#4	204	315	54%	claro.com.do	Dominican Rep
#5	146	198	36%	telefonica.com.br	Brazil
#6	94	94	0%	microsoft.com	United States
#7	60	83	38%	a1.bg	Bulgaria
#8	91	79	-13%	ipjetable.net	France
#9	25	65	160%	ielo.net	France
#10	41	41	0%	telefonica.com.ar	Argentina
#11	27	34	26%	mobily.com.sa	Saudi Arabia
#12	29	29	0%	tie.cl	Chile
#12	-	29	New Entry	cableonda.net	Panama
#14	29	28	-3%	vietserver.vn	Vietnam
#15	-	25	New Entry	eliteteam.to	Seychelles
#15	-	25	New Entry	ntup.net	Russia
#17	21	24	14%	google.com	United States
#17	-	24	New Entry	alexhost.md	Moldova
#19	-	23	New Entry	selectel.ru	Russia
#20	21	22	5%	combahton.net	Germany

That's all for now. Stay safe, and we'll see you in July!