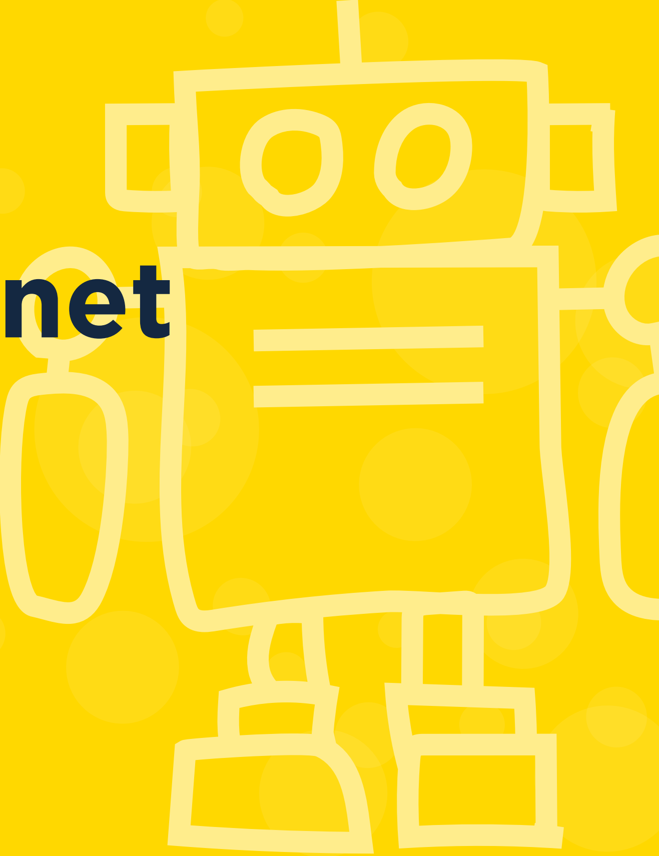
SPAMHAUS

Spamhaus Botnet Threat Update



Q2 2021

This quarter, the Spamhaus researchers have observed a 12% reduction in newly observed botnet command and controllers (C&Cs), which is good news. However, it's not good news for everyone; more than one industry-leading provider is suffering under the weight of active botnet C&Cs on their networks.

Welcome to the Spamhaus Botnet Threat Update Q2 2021.

What are botnet 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 to 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 to 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.

Spotlight

The Emotet story continues

Yes, we know – we're still discussing Emotet, despite its takedown in January. This is because the Emotet narrative didn't end the moment it was taken down. Far from it.

As a result of the way Emotet proliferated, through thread hijacking, millions of email accounts were left compromised and open to further exploitation by other malware and ransomware.

Spamhaus has spent the past quarter working with the FBI to assist with remediation efforts and reach out to those affected. To give you an understanding of the scale of the operation, here are some numbers:

- 1.3 million compromised email accounts
- 22,000 unique domains
- 3,000 networks

Our team has been busy contacting the relevant abuse desks, trust and safety departments, and end-users, providing them with remediation data and instructions on how to safeguard these compromised accounts.

We're delighted to report that over 60% of those 1.3 million accounts have now been secured. It goes to show that we all have a role to play in making the internet a safer place.

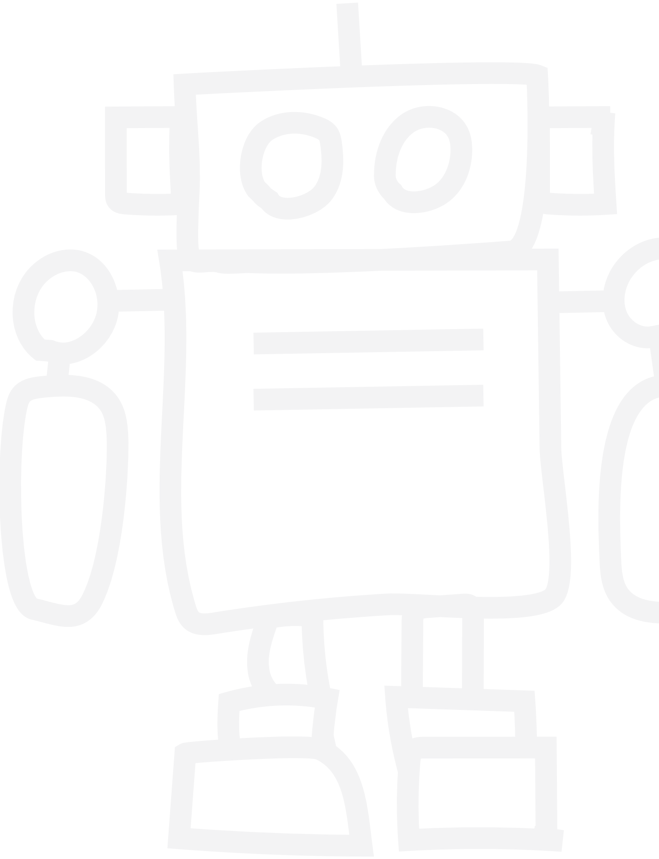
What is thread hijacking?

This is where miscreants use their victim's existing email conversations (threads) to spread malicious links or attachments to new victims.

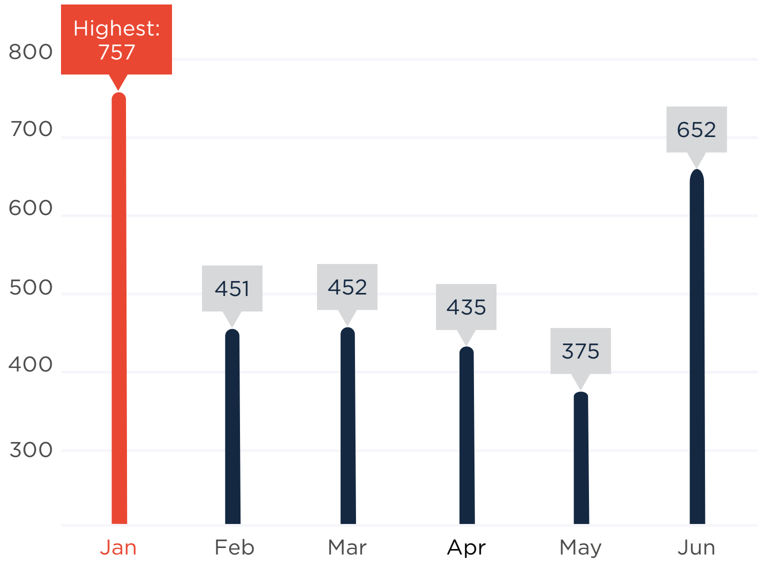
An attacker can be far more convincing and fool further victims into clicking on harmful links or downloading files by replying to an existing email thread.

Number of botnet C&Cs observed, Q2 2021

Here’s an overview of the number of newly observed botnet Command & Control servers (C&Cs) in Q2 2021. Spamhaus Malware Labs identified **1,462 botnet C&Cs** compared to 1,660 in Q1 2021. This was a **decrease** of **12%**. The monthly average dropped from 553 per month in Q1 to 487 botnet C&Cs per month in Q2.



Number of new botnet C&Cs detected by Spamhaus in 2021:



Q1 Monthly average: 553

Q2 Monthly average: 487

Geolocation of botnet C&Cs, Q2 2021

We saw multiple changes in the geo-locations that cybercriminals used to set up new botnet C&C servers, particularly at the lower end of our Top 20 listings, where there was a raft of new entries.

Decreases across Latin America

There was a noticeable decrease in Latin American countries hosting botnet C&Cs, with Argentina and Colombia dropping off the Top 20 list and Brazil seeing a 40% decrease. The only exception to this was Panama which was a new entry at #13.

Continued increases across Europe

Once again, we witnessed an increase in the number of European countries entering the Top 20. This included the Czech Republic, Poland, and Finland. Meanwhile, Germany, France, Latvia, and United Kingdom all saw increases in botnet C&Cs.

New entries

Czech Republic (#11), Panama (#13), Malaysia (#15), Poland (#15), Finland (#17), Vietnam (#18).

Departures

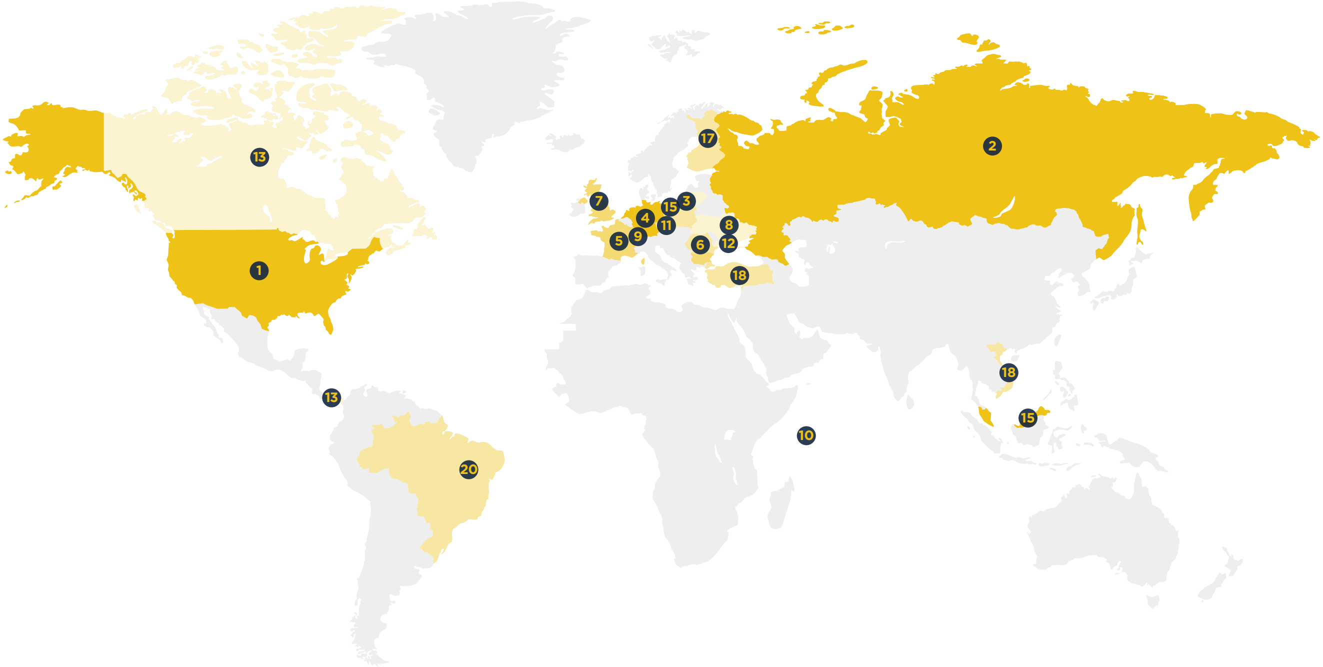
China, Sweden, Hong Kong, Argentina, Colombia, Singapore.

Geolocation of botnet C&Cs, Q2 2021 (continued)

Top 20 locations of botnet C&Cs

New entry

Rank	Country	Q1 2021	Q2 2021	% Change Q on Q
#1	United States	338	281	-17%
#2	Russia	195	233	19%
#3	Netherlands	207	168	-19%
#4	Germany	99	117	18%
#5	France	71	92	30%
#6	Latvia	31	84	171%
#7	United Kingdom	49	57	16%
#8	Ukraine	22	44	100%
#9	Switzerland	59	41	-31%
#10	Seychelles	29	38	31%
#11	Czech Republic	-	31	New entry
#12	Moldova	29	29	0%
#13	Panama	-	16	New entry
#13	Canada	26	16	-38%
#15	Malaysia	-	15	New entry
#15	Poland	-	15	New entry
#17	Finland	-	14	New entry
#18	Vietnam	-	13	New entry
#18	Turkey	25	13	-48%
#20	Brazil	20	12	-40%



Malware associated with botnet C&Cs, Q2 2021

Let's start with the good news. After the laudable Emotet botnet takedown in Q1 2021, we are pleased to report that no activity from Emotet has been observed.

Dropper popularity increasing

In Q2 there was a shift away from credential stealers and remote access tools (RATs) to droppers.

Raccoon rapidly reaches #1

Raccoon only made its first appearance in our Top 20 last quarter at #8. In Q2, it's flown up the charts to take pole position.

Credential stealers for sale

Not only is the aforementioned credential stealer, Raccoon, available for purchase on the dark web, but so are the likes of RedLine and Oski, which were new entries to our charts this quarter. Given the ease of access, it comes as no surprise to see the popularity of these malware growing.

What is a dropper?

Droppers conceal code to enable malware to escape detection by virus scanners i.e. it silently drops the malware onto the targeted system.

New entries

Oski (#7), Tofsee (#11), STRRAT (#15), CryptBot (#16), CobaltStrike (#17), ServHelper (#18), IcedID (#18).

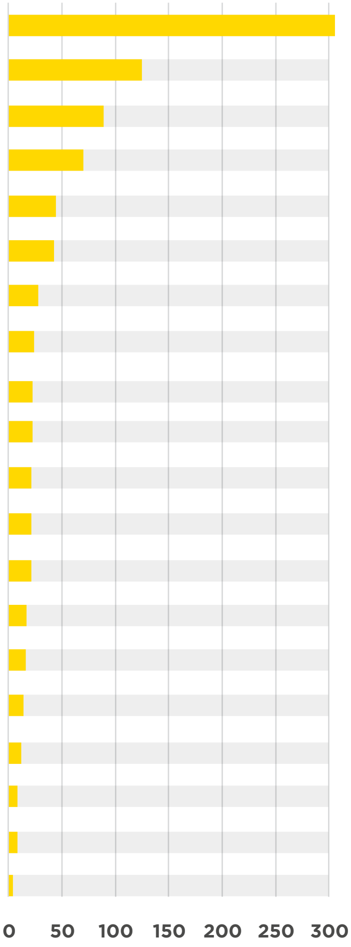
Departures

Emotet, NetWire, AveMaria, FickerStealer, AZORult, TriumpLoader, Hancitor

Malware associated with botnet C&Cs, Q2 2021 (continued)

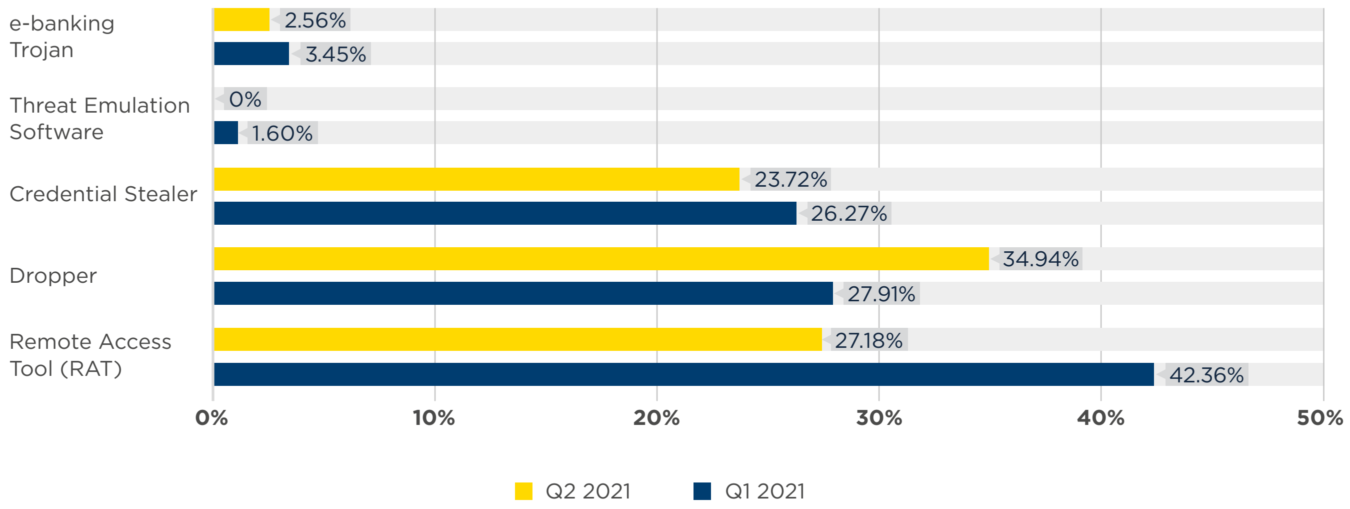
Malware families associated with botnet C&Cs

Rank	Q1 2021	Q2 2021	% Change	Malware Family	Description
#1	45	302	571%	Raccoon	Dropper
#2	55	123	124%	RedLine	Remote Access Tool (RAT)
#3	69	83	20%	AsyncRAT	Credential Stealer
#4	83	66	-20%	Loki	Remote Access Tool (RAT)
#5	38	43	13%	Gozi	Remote Access Tool (RAT)
#6	33	42	27%	BitRAT	Credential Stealer
#7	-	28	New entry	Oski	Remote Access Tool (RAT)
#8	18	26	44%	Vjw0rm	Credential Stealer
#9	36	24	-33%	NjRAT	Credential Stealer
#9	124	24	-81%	RemcosRAT	e-banking Trojan
#11	68	23	-66%	NanoCore	Remote Access Tool (RAT)
#11	55	23	-58%	AgentTesla	Remote Access Tool (RAT)
#11	-	23	New entry	Tofsee	Remote Access Tool (RAT)
#14	39	19	-51%	Arkei	Remote Access Tool (RAT)
#15	-	17	New entry	STRRAT	Credential Stealer
#16	-	16	New entry	CryptBot	Credential Stealer
#17	-	15	New entry	CobaltStrike	Threat Emulation Software*
#18	-	14	New entry	ServHelper	Credential Stealer
#18	-	14	New entry	IcedID	Dropper
#20	18	11	-39%	QuasarRAT	Dropper



* Updated 15 Oct 2021 | CobaltStrike was reported as being a Remote Access Tool when this report was originally published. We have updated to reflect it is Threat Emulation Software.

Malware type comparisons between Q1 and Q2 2021



Most abused top-level domains, Q2 2021

.com

For Q2 2021, the gTLD .com once again made it at the top of our ranking. Moreover, the number of newly registered botnet C&C domains observed on .com increased by 166%, from 1,549 to 4,113!

.xyz

With a vast 114% upsurge this quarter, it comes as no surprise that gTLD .xyz has replaced gTLD .top in the #2 spot.

Country code TLDs

Only two new ccTLDs were new to the Top 20 this quarter, with .br entering at #5 and .cn at #12. Meanwhile, three ccTLDs improved their reputation and departed the list; .us, .de & .la

Top-level domains (TLDs) – a brief overview

There are several different top-level domains including:

Generic TLDs (gTLDs) – can be used by anyone

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

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

New entries

buzz (#3), br (#5), VIP (#6), cloud (#10), cn (#12), online (#16), live (#17).

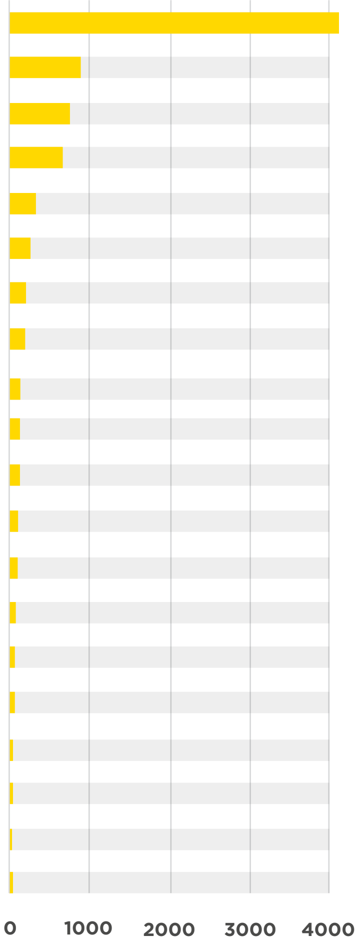
Departures

me, biz, cc, us, la, co, de.

Most abused top-level domains, Q2 2021 (continued)

Top abused TLDs - number of domains

Rank	Q1 2021	Q2 2021	% Change	TLD	Note
#1	1549	4113	166%	com	gTLD
#2	345	739	114%	xyz	gTLD
#3	-	662	New entry	buzz	gTLD
#4	622	607	-2%	top	gTLD
#5	-	208	New entry	br	ccTLD
#6	-	175	New entry	vip	gTLD
#7	83	157	89%	org	gTLD
#8	114	151	32%	ru	ccTLD
#9	72	146	103%	net	gTLD
#10	-	141	New entry	cloud	gTLD
#11	124	140	13%	tk	Originally ccTLD, now effectively gTLD
#12	-	139	New entry	cn	ccTLD
#12	108	116	7%	eu	ccTLD
#14	121	106	-12%	ga	Originally ccTLD, now effectively gTLD
#15	106	104	-2%	ml	Originally ccTLD, now effectively gTLD
#16	-	86	New entry	online	gTLD
#17	-	81	New entry	live	gTLD
#18	51	80	57%	su	ccTLD
#19	46	78	70%	info	gTLD
#20	82	73	-11%	cf	ccTLD



Most abused domain registrars, Q2 2021

After many years with no change at the top of our registrar reputation rankings, we finally have some movement!

NameSilo

We saw an enormous 594% increase of newly registered botnet C&C domains at the Canadian domain registrar NameSilo, knocking Namecheap off their #1 ranking. This was quite a feat considering that NameCheap saw a 52% increase in newly registered botnet C&C domains. These are huge numbers!*

Germany and China

It was not only US and Canadian-based registrars who saw significant increases in Q2. The two German-based domain registrars, Key Systems (56%) and 1API (254%), also experienced growth in the number of botnet domains registered through their services, as did almost all the Chinese registrars listed below, including eName Technology who entered our Top 20 at #3.

New entries

eName Technology (#3), Arsys (#5), Xin Net (#10), CentralNic (#11), Network Solutions (#14).

Departures

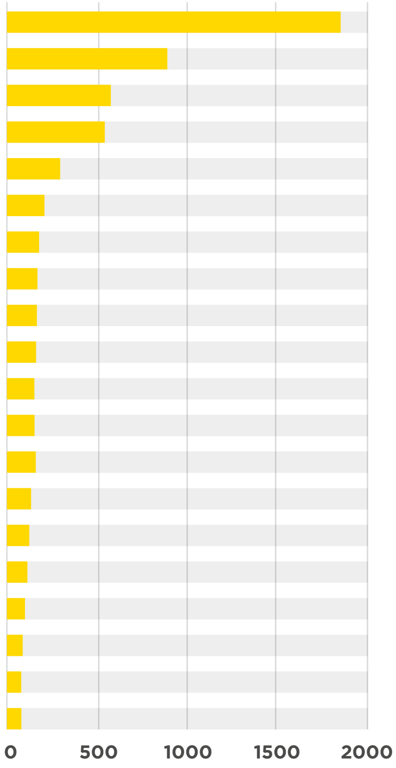
101 Domains, Bizcn, OnlineNIC, OVH, NameBright.

* Updated 15 Oct 2021 | NameSilo and Tucows were reported as being US-based providers when this report was originally published. We have updated to reflect they are based in Canada.

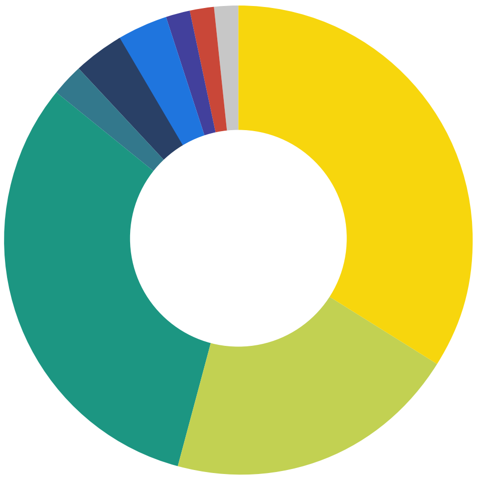
Most abused domain registrars, Q2 2021 (continued)

Most abused domain registrars - number of domains

Rank	Q1 2021	Q2 2021	% Change	Registrar	Country
#1	259	1797	594%	NameSilo	Canada* 🇨🇦
#2	628	955	52%	Namecheap	United States 🇺🇸
#3	-	526	New entry	eName Technology	China 🇨🇳
#4	85	504	493%	Alibaba	China 🇨🇳
#5	-	237	New entry	Arsys	Spain 🇪🇸
#6	384	215	-44%	Eranet International	China 🇨🇳
#7	72	188	161%	PDR	India 🇮🇳
#8	238	135	-43%	RegRU	Russia 🇷🇺
#9	33	134	306%	HiChina	China 🇨🇳
#10	-	125	New entry	Xin Net	China 🇨🇳
#11	-	112	New entry	CentralNic	United Kingdom 🇬🇧
#12	26	110	323%	22net	China 🇨🇳
#12	29	110	279%	Tucows	Canada* 🇨🇦
#14	-	101	New entry	Network Solutions	United States 🇺🇸
#15	28	99	254%	1API	Germany 🇩🇪
#16	59	92	56%	Key Systems	Germany 🇩🇪
#17	56	91	63%	WebNic.cc	Singapore 🇸🇬
#18	35	89	154%	Name.com	United States 🇺🇸
#19	50	80	60%	west263.com	China 🇨🇳
#20	116	73	-37%	55hl.com	China 🇨🇳



LOCATION OF MOST ABUSED DOMAIN REGISTRARS



	Country	Botnets	%
🟨	Canada*	1907	33.03%
🟩	United States	1145	19.83%
🟩	China	1767	30.6%
🟦	Spain	237	2.3%
🟦	Germany	191	3.3%
🟦	India	188	3.3%
🟪	Russia	135	1.6%
🟥	United Kingdom	112	1.6%
⬜	Singapore	91	1.6%
	Total	5773	

* Updated 15 Oct 2021 | Two registrars (NameSilo & Tucows) were reported as being US-based providers when this report was originally published. We have updated the text and data to reflect they are based in Canada.

Networks hosting the most newly observed botnet C&Cs, Q2 2021

There is always lots of change in those hosting the most newly observed botnet C&Cs. This quarter was no exception.

Bulletproof hosting operation

In Q2, one of the most extensive bulletproof hosting operations moved from Amazon to DigitalOcean. As a result, the amount of newly observed botnet C&Cs at Amazon rapidly decreased. Conversely, there was a sudden increase in new botnet C&Cs hosted at DigitalOcean.

Microsoft.com

We have seen microsoft.com (US) enter the Top 20. We have observed them hosting a significant amount of Vjw0rm and BitRAT botnet C&C infrastructure.

New entries

nano.lv (#6), mgnhost.ru (#8), baxet.ru (#10), ipjetable.net (#11), digitalocean.com (#12), internet.it (#14), hostsailor.com (#16), microsoft.com (#17), m247.ro (#8), offshoreracks.com (#19), mivocloud.com (#19).

Departures

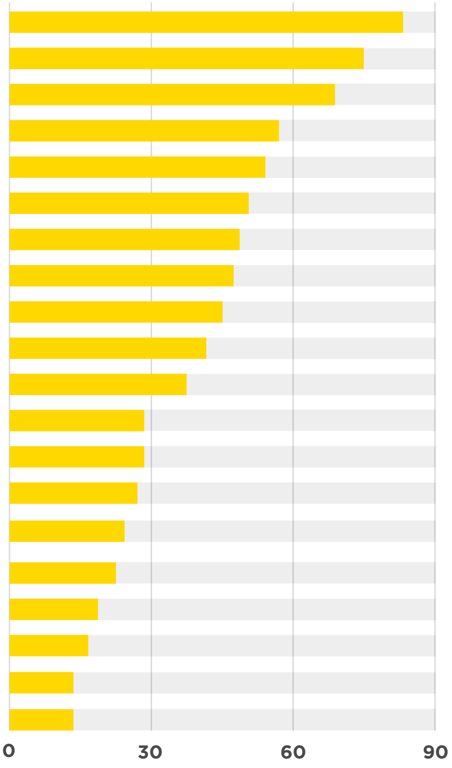
intersec.host, amazon.com, endurance.com, choopa.com, combahton.net, leaseweb.com, linode.com, ispserver.com colocrossing.com, dedipath.com, msk.host.

[2]https://www.spamhaus.org/statistics/networks/

Networks hosting the most newly observed botnet C&Cs, Q2 2021 (continued)

Newly observed botnet C&Cs per network

Rank	Q1 2021	Q2 2021	% Change	Network	Country
#1	35	82	134%	pq.hosting	Russia
#2	53	74	40%	google.com	United States
#3	21	68	224%	serverion.com	Netherlands
#4	51	56	10%	ovh.com	France
#5	23	53	130%	itldc.com	Ukraine
#6	-	49	New Entry	nano.lv	Latvia
#7	131	48	-63%	privacyfirst.sh	Germany
#8	-	47	New Entry	mgnhost.ru	Russia
#9	19	46	142%	hetzner.de	Germany
#10	-	40	New Entry	baxet.ru	Russia
#11	-	35	New Entry	ipjetable.net	France
#12	45	29	-36%	cloudflare.com	United States
#12	-	29	New Entry	digitalocean.com	United States
#14	-	28	New Entry	Internet.it	Russia
#15	26	26	0%	alibaba-inc.com	China
#16	-	25	New Entry	hostsailor.com	U. Arab Emirates
#17	-	22	New Entry	microsoft.com	United States
#18	-	21	New Entry	m247.ro	Romania
#19	-	16	New Entry	offshoreracks.com	Panama
#19	-	16	New Entry	mivocloud.com	Moldova



Networks hosting the most active botnet C&Cs, Q2 2021

Finally, let's take a look at the networks that hosted a large number of active botnet C&Cs in Q2 2021. Hosting providers who appear in this ranking either have an abuse problem or do not take the appropriate action when they receive abuse reports.

Eliteteam.to

This is a bulletproof hosting company purporting to be located in the Seychelles. In reality, they more than likely operate out of Russia.

Microsoft.com and google.com

It is evident that Microsoft is struggling with the amount of abuse generated on its Azure cloud platform. Likewise, google.com is equally besieged with abuse reports.

Well done to the departures!

We want to acknowledge all those who have departed from this list – it's good to see the number of active botnet C&Cs reducing on your network. Nice work!

!

New entries

m247.ro (#12), eliteteam.to (#13), mgnhost.ru (#13), unusinc.com (#17).

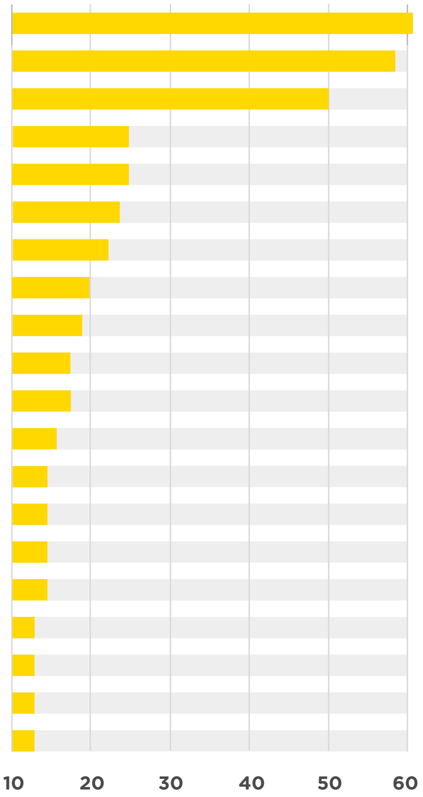
Departures

mail.ru, digitalocean.com, eurobyte.ru, telstra.com.

Networks hosting the most active botnet C&Cs, Q2 2021 (continued)

Total number of active botnet C&Cs per network

Rank	Q4 2020	Q1 2021	% Change	Network	Country
#1	33	61	85%	ipjetable.net	France
#2	48	58	21%	microsoft.com	United States
#3	43	50	16%	google.com	United States
#4	23	23	0%	ttnet.com.tr	Turkey
#4	21	23	10%	vietserver.vn	Vietnam
#6	22	21	-5%	charter.com	United States
#6	21	21	0%	inmotionhosting.com	United States
#8	17	20	18%	ovpn.com	Sweden
#9	18	18	0%	clouvider.net	United Kingdom
#10	12	17	42%	hostry.com	Cyprus
#10	17	17	0%	une.net.co	Colombia
#12	-	15	New Entry	m247.ro	Romania
#13	17	13	-24%	datawire.ch	Switzerland
#13	-	13	New Entry	eliteteam.to	Seychelles
#13	13	13	0%	mtnnigeria.net	Nigeria
#13	-	13	New Entry	mgnhost.ru	Russia
#17	18	12	-33%	claro.com.co	Colombia
#17	12	12	0%	kornet.net	South Korea
#17	14	12	-14%	chinanet-js	China
#17	-	12	New Entry	unusinc.com	United States



That's all for now.

Stay safe and see you in October!