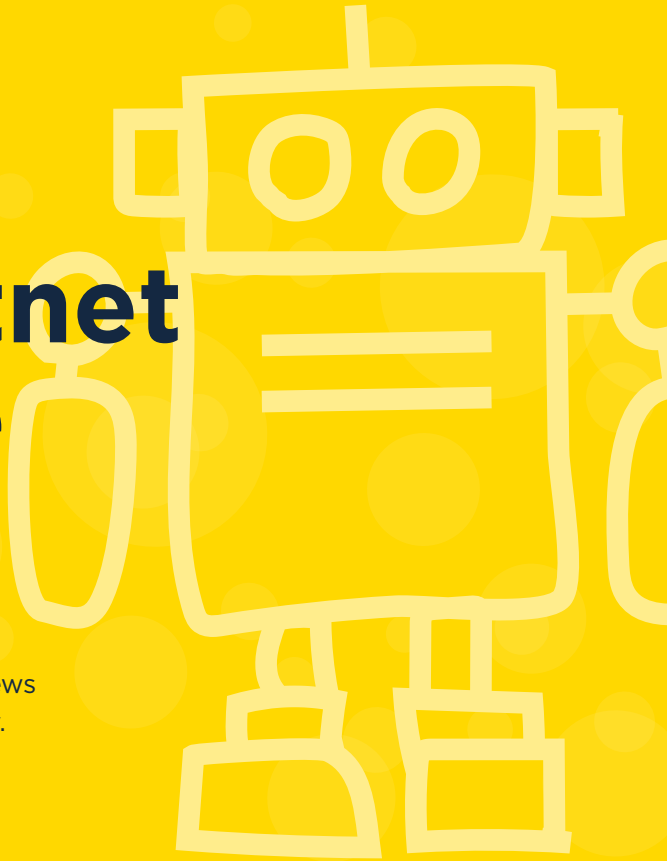
SPAMHAUS



Spamhaus Botnet Threat Update

Q1 2021

After a quiet(ish) end to 2020 in Spamhaus' botnet world, the first quarter of this year kicked off in style. The major news surrounded the takedown of the Emotet botnet in January. Nonetheless, as one malware departs, others arrive on the scene, as proved by the 24% increase in the total number of botnet C&Cs Spamhaus researchers observed.

Welcome to the Spamhaus Botnet Threat Update Q1 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

Emotet is gone, but other threats are emerging

In January 2021, an international coalition including authorities from various countries undertook a global action against the notorious Emotet botnet. Law enforcement agencies shut down infrastructure operated by the Emotet gang, sending Emotet botnet traffic to a sinkhole.

The operation appears to have been a success as the botnet has remained inactive for over two months. However, Spamhaus Malware Lab experts deem that it's highly likely that Emotet will come back into circulation.

Over the past few years, Emotet has flourished, earning itself the label of being one of the most dangerous online threats. Miscreants used it to gain an initial foothold in corporate networks, allowing them to move laterally within the victims' network, which in many cases led to encryption with ransomware.

Sadly, there's no rest in the botnet world; no sooner is one botnet extinguished than it's replaced. Rapidly, other botnet operators have rushed to fill the void that Emotet has left.

Miscreants operating botnets like IcedID, Dridex, Quakbot, and TrickBot sent out large volumes of spam emails containing malicious documents this quarter. For most of these threats, the modus operandi is similar to that of Emotet's, i.e., gain a foothold in corporate networks and encrypt them with ransomware.

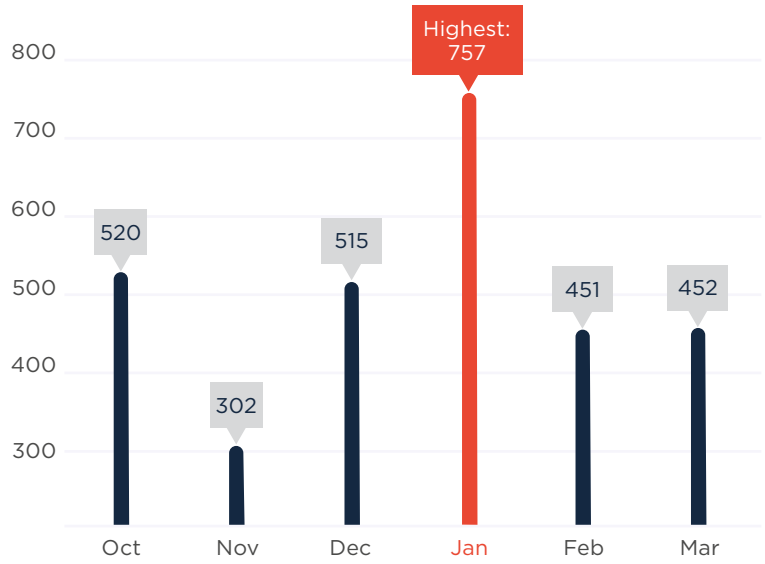
Emotet

Emotet is a former e-banking Trojan that targeted e-banking customers globally. In 2018, Emotet ceased its e-banking fraud activities and started to offer infected computers on a "Pay-Per-Install" model. From 2019 onwards, Emotet developed into one of the most dangerous botnets.

Number of botnet C&Cs observed, Q1 2021

First of all, let's look at the number of newly observed botnet Command & Control servers (C&Cs) in Q1 2021. In total, Spamhaus Malware Labs has identified 1,660 new botnet C&Cs compared to 1,337 in Q4, 2020. This is a 24% increase, with an average of 553 botnet C&Cs per month.

Number of new botnet C&Cs detected by Spamhaus since late 2020:



Q4 Monthly average: 445

Q1 Monthly average: 553

Geolocation of botnet C&Cs, Q1 2021

In some countries, we have seen an increase of newly observed botnet C&Cs while other countries have dropped out of our Top 20.

The United States holds onto #1

Despite a small 3% drop in the number of newly observed botnet C&Cs, the United States remains top of the leader board.

Increases across Europe

The Netherlands has overtaken Russia and finds itself in second position, with a total of 207 botnets, a 27% increase on Q4, 2020.

Additional European countries have experienced increases in new botnet infrastructures, including Germany (+77%), France (+82%), Switzerland (+23%), and United Kingdom (+9%).

New entries

Moldova (#11), Hong Kong (#15), Argentina (#18), Columbia (#18).

Departures

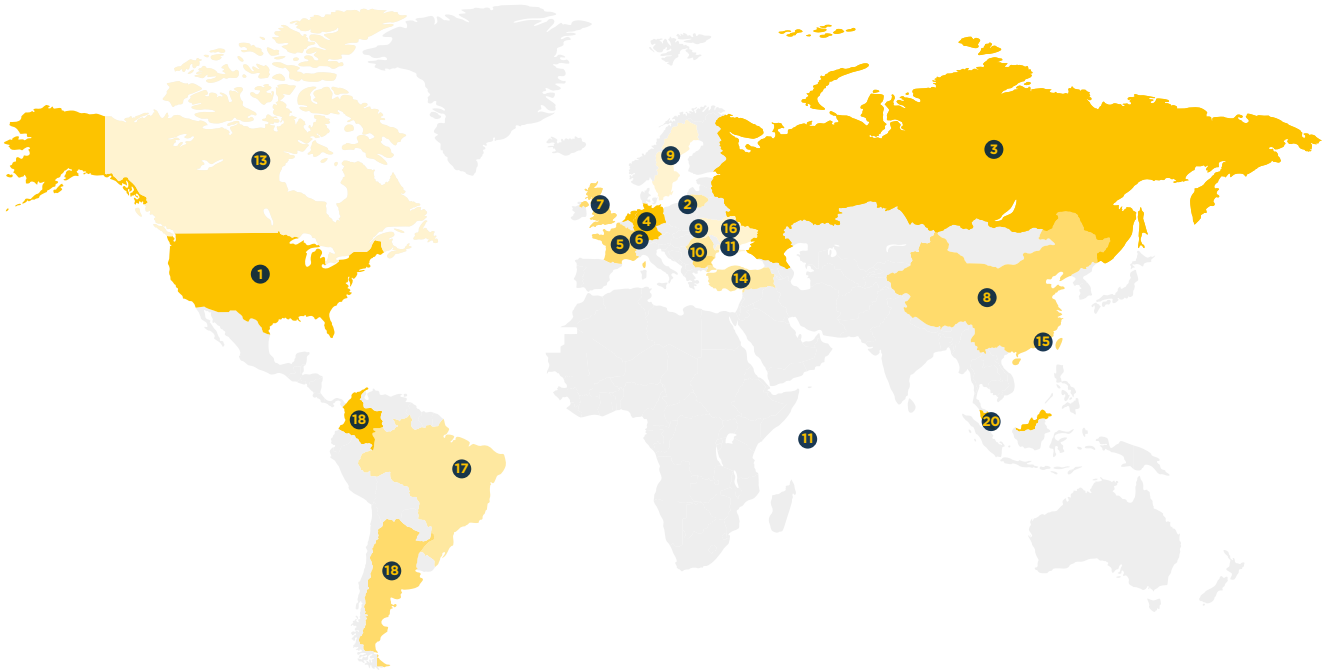
Bulgaria, Hungary, India, Vietnam

Geolocation of botnet C&Cs, Q1 2021 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Q4 2020	Q1 2021	% Change Q on Q
#1	United States	348	338	-3%
#2	Netherlands	163	207	27%
#3	Russia	247	195	-21%
#4	Germany	56	99	77%
#5	France	39	71	82%
#6	Switzerland	48	59	23%
#7	United Kingdom	45	49	9%
#8	China	32	42	31%
#9	Sweden	34	39	15%
#10	Latvia	24	31	29%

Rank	Country	Q4 2020	Q1 2021	% Change Q on Q
#11	Seychelles	10	29	190%
#11	Moldova	-	29	New entry
#13	Canada	11	25	136%
#14	Turkey	17	20	47%
#15	Hong Kong	-	24	New entry
#16	Ukraine	16	22	38%
#17	Brazil	8	20	150%
#18	Argentina	-	18	New entry
#18	Colombia	-	18	New entry
#20	Singapore	31	16	-48%



Malware associated with botnet C&Cs, Q1 2021

Emotet:

In Q1 2021, Emotet re-entered back in at #1. This comes as no surprise, given our efforts in helping Law Enforcement agencies take down Emotet botnet infrastructure in January 2021.

Raccoon:

Raccoon is a credential stealer that is new in town. In Q1 2021, we identified 45 botnet C&Cs associated with this new malware.

FickerStealer:

Another credential stealer that has been observed for the first time in Q1 2021 is FickerStealer, with 25 new associated botnet C&Cs.

QNodeService:

We first saw this malware in 2020. However, it appears that QNodeService's activity completely dropped away at the start of this year. To date, we have not observed a single C&C associated with it.

New entries

Emotet (#1), Raccoon (#8), Gozi (#10), BitRat (#12), FickerStealer (#15), Vjw0rm (#17), TriumphLoader (#17), Hancitor (#20)

Departures

Mirai, QNodeService, BazaLoader, ZLoader, CobaltStrike, Smoke Loader, Dridex, RevengeRAT

Malware associated with botnet C&Cs, Q1 2021 (continued)

Malware families associated with botnet C&Cs

Rank	Q4 2020	Q1 2021	% Change	Malware Family	Description
#1	-	272	New entry	Emotet	Dropper
#2	53	124	134%	RemcosRAT	Remote Access Tool (RAT)
#3	164	83	-49%	Loki	Credential Stealer
#4	29	69	138%	AsyncRAT	Remote Access Tool (RAT)
#5	71	68	-4%	NanoCore	Remote Access Tool (RAT)
#6	66	55	-17%	RedLine	Credential Stealer
#6	93	55	-41%	AgentTesla	Remote Access Tool (RAT)
#8	-	45	New entry	Raccoon	Credential Stealer
#9	17	39	129%	Arkei	Credential Stealer
#10	-	38	New entry	Gozi	e-banking Trojan
#11	30	36	20%	NjRAT	Remote Access Tool (RAT)
#12	21	33	57%	NetWire	Remote Access Tool (RAT)
#12	-	33	New entry	BitRAT	Remote Access Tool (RAT)
#14	38	30	-21%	AveMaria	Remote Access Tool (RAT)
#15	-	25	New entry	FickerStealer	Credential Stealer
#16	47	24	-49%	AZORult	Credential Stealer
#17	15	18	20%	QuasarRAT	Remote Access Tool (RAT)
#17	-	18	New entry	Vjw0rm	Credential Stealer
#17	-	18	New entry	TriumphLoader	Dropper
#20	-	17	New entry	Hancitor	Dropper

Most abused top-level domains, Q1 2021

For Q1 2021, the gTLD .com remains at the top of our rankings. A large majority of botnet C&C domains that Spamhaus Malware Labs identified were hosted on this TLD. However, we have seen many other listed TLDs improve their reputation with reductions across the board.

.de:

The ccTLD of Germany has once again entered the Top 20 at #19. Not good! Is this due to a weak anti-abuse policy at DENIC?

.top & .xyz:

These two gTLDs have a long history of abuse, and it's not surprising that they continue to be in the Top 5, particularly when .top had a 90% increase in the number of botnet C&Cs it hosted in Q1 2021.

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

ru (#6), org (#10), biz (#12), us (#15), info (#18), co (#19), de (#19)

Departures

casa, br, cyou, kr, ai, ac, gq

Most abused top-level domains, Q1 2021 (continued)

Most abused TLDs - number of domains

Rank	Q4 2020	Q1 2021	% Change	TLD	Note
#1	2108	1549	-27%	com	gTLD
#2	328	622	90%	top	gTLD
#3	505	345	-32%	xyz	gTLD
#4	141	124	-12%	tk	Originally ccTLD, now effectively gTLD
#5	185	121	-35%	ga	Originally ccTLD, now effectively gTLD
#6	-	114	New entry	ru	ccTLD
#7	100	108	8%	eu	ccTLD
#8	133	106	-20%	ml	Originally ccTLD, now effectively gTLD
#9	95	87	-8%	me	gTLD
#10	-	83	New entry	org	gTLD
#11	94	82	-13%	cf	Originally ccTLD, now effectively gTLD
#12	-	72	New entry	biz	gTLD
#12	81	72	-11%	net	gTLD
#14	138	66	-52%	cc	gTLD
#15	-	55	New entry	us	ccTLD
#16	77	51	-34%	su	ccTLD
#17	74	47	-36%	la	ccTLD
#18	-	46	New entry	info	gTLD
#19	-	36	New entry	co	ccTLD
#19	-	36	New entry	de	ccTLD

Most abused domain registrars, Q1 2021

Namecheap (again!)

After years of being #1 in this Top 20, Namecheap (US) continues to be the preferred domain registrar for miscreants registering botnet C&C domains.

When will this change? We don't know. But given the long history of abuse at Namecheap, we don't expect it to be any time soon!

Eranet International & RegRU

With a massive 249% increase, Eranet International (China) knocked NameSilo (United States) off its #2 spot. However, the most significant increase in the number of botnet C&C domain registrations belongs to RegRU (Russia), with a whopping 341% increase.

New entries

OnlineNIC (#13), name.com (#15), HiChina (#16), NameBright (#17)

Departures

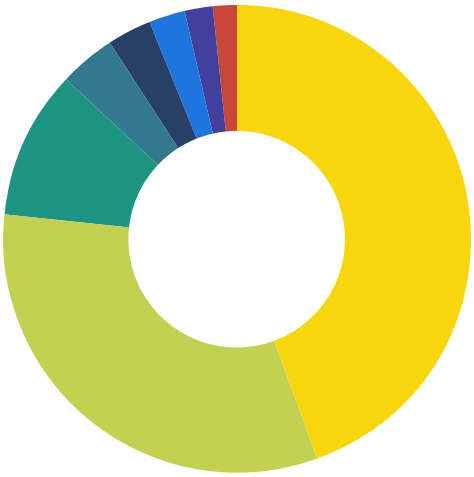
URL Solution, Hosting Concepts

Most abused domain registrars, Q1 2021 (continued)

Most abused domain registrars - number of domains

Rank	Q4 2020	Q1 2021	% Change	Registrar	Country
#1	822	628	-24%	Namecheap	United States
#2	110	384	249%	Eranet International	China
#3	444	259	-42%	NameSilo	United States
#4	54	238	341%	RegRU	Russia
#5	115	116	1%	55hl.com	China
#6	101	85	-16%	Alibaba	China
#7	343	72	-79%	PDR	India
#8	367	59	-84%	Key Systems	Germany
#9	111	56	-50%	WebNic.cc	Singapore
#10	65	50	-23%	west263.com	China
#11	25	44	76%	101Domain	Ireland
#12	48	42	-13%	Bizcn	China
#13	-	38	New entry	OnlineNIC	United States
#14	32	36	13%	OVH	France
#15	-	35	New entry	name.com	United States
#16	-	33	New entry	HiChina	China
#17	-	30	New entry	NameBright	United States
#18	53	29	-45%	Tucows	United States
#19	46	28	-39%	1API	Germany
#20	29	26	-10%	22net	China

LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Botnets	%
United States	1019	44.5%
China	736	32.2%
Russia	238	10.4%
Germany	87	3.8%
India	72	3.1%
Singapore	56	2.4%
Ireland	44	1.9%
France	36	1.6%

Networks hosting the most newly observed botnet C&Cs, Q1 2021

For this quarter, we have seen an East/West split, with a reduction in the number of botnet C&Cs hosted at providers from the East, only to be swiftly replaced by cloud service providers in the West.

Russian Virtual Private Server (VPS) providers

Various companies like invs.ru and selectel.ru dropped out of the Top 20 this quarter. This is very positive news, particularly when it comes to selectel.ru, who have been present in the Top 20 list for a long time.

Western VPS providers

Various providers located in the West have entered the Top 20 chart in Q1 2021 including, google.com, choopa.com, hetzner.de, and combahton.net.

The worst and the most improved

The most abused network is privacyfirst.sh, a VPN provider operating out of Germany. Conversely, amazon.com has reduced the number of newly observed botnet C&Cs on its network by 44% over the past quarter. A positive step forward!

New entries

Google.com (#2), intersect.host (#6), choopa.com (#12) hetzner.de (#13), combahton.net (#13), linode.com (#16), ispserver.com (#17), colocrossing.com (#17), msk.host (#17)

Departures

invs.ru, m247.ro, selectel.ru, namecheap.com, digitalocean.com, maxko.org, tencent.com, baxet.ru belcloud.net

Networks hosting the most newly observed botnet C&Cs, Q1 2021 (continued)

Newly observed botnet C&Cs per network

Rank	Q4 2020	Q1 2021	% Change	Network	Country
#1	106	131	24%	privacyfirst.sh	Germany
#2	-	53	New entry	google.com	United States
#3	33	51	55%	ovh.com	French
#4	47	45	-4%	cloudflare.com	United States
#5	15	35	133%	pq.hosting	Moldova
#6	-	32	New entry	intersect.host	Seychelles
#7	55	31	-44%	amazon.com	United States
#8	45	28	-38%	endurance.com	United States
#9	26	26	0%	alibaba-inc.com	China
#10	15	23	53%	itldc.com	Unkraine
#11	17	21	24%	serverion.com	Netherlands
#12	-	20	New entry	choopa.com	United States
#13	-	19	New entry	hetzner.de	Germany
#13	-	19	New entry	combahton.net	Germany
#13	28	19	-32%	leaseweb.com	Netherlands
#16	-	18	New entry	linode.com	United States
#17	-	17	New entry	ispserver.com	Russia
#17	-	17	New entry	colocrossing.com	United States
#17	25	17	-32%	dedipath.com	United States
#17	-	17	New entry	msk.host	Russia

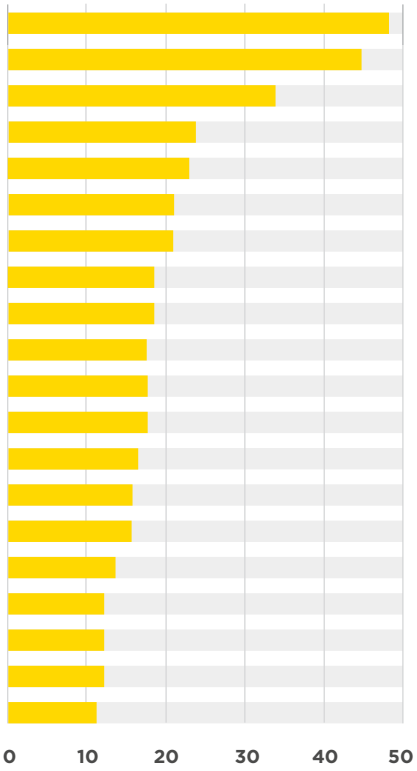
Networks hosting the most active botnet C&Cs, Q1 2021

Last but not least, let's have a look at the networks that consistently hosted a large number of active botnet C&Cs. Sadly, Microsoft heads up this Top 20, with 48 active botnet C&Cs, followed by Google with 43 active botnet C&Cs.

Networks appearing in this listing tend to have poor network hygiene and fail to act on abuse complaints – the absence of change between the past quarters indicates this fact. The botnets remain active for months!

Total number of active botnet C&Cs per network

Rank	Q4 2020	Q1 2021	% Change	Network	Country
#1	48	48	0%	microsoft.com	United States
#2	43	43	0%	google.com	United States
#3	33	33	0%	ipjetable.net	Switzerland
#4	23	23	0%	ttnet.com.tr	Turkey
#5	22	22	0%	charter.com	United States
#6	21	21	0%	inmotionhosting.com	United States
#6	21	21	0%	vietserver.vn	Vietnam
#8	18	18	0%	claro.com.co	Colombia
#8	18	18	0%	cloudvider.net	United Kingdom
#10	17	17	0%	ovpn.com	Sweden
#10	17	17	0%	une.net.co	Colombia
#10	17	17	0%	datawire.ch	Switzerland
#13	16	16	0%	mail.ru	Russia
#14	14	14	0%	chinanet-js	China
#14	14	14	0%	digitalocean.com	United States
#16	13	13	0%	mtnnigeria.net	Nigeria
#17	12	12	0%	kornet.net	Korea
#17	12	12	0%	hostry.com	Cyprus
#19	12	11	-8%	eurobyte.ru	Russia
#19	11	11	0%	telstra.com	Australia



Given the events regarding Emotet in Q1 2021, it will be very interesting to see what the next quarter will bring.

See you next quarter. In the meantime, stay safe.