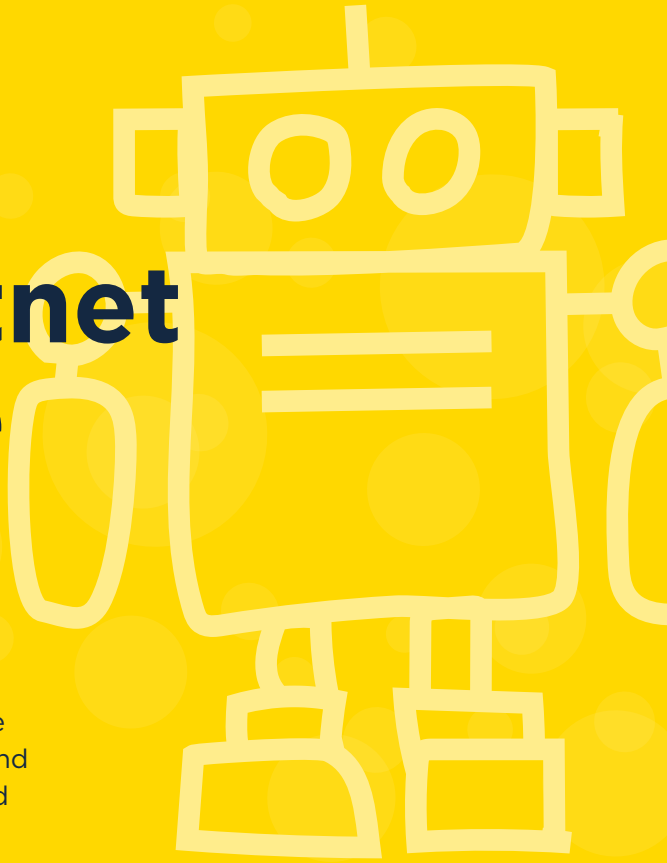
SPAMHAUS



Spamhaus Botnet Threat Update

Q3 2021

Q3 has seen a massive 82% rise in the number of new botnet command and controllers (C&Cs) identified by our research team. They have observed an explosion in the use of backdoor malware with nefarious operators hiding behind FastFlux. In turn, this has caused several new countries and service providers to be listed in our Top 20 charts.

Welcome to the Spamhaus Botnet Threat Update Q3 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

FastFlux emerging again

After analyzing this quarter's statistics, it is evident that FastFlux is once again rising in popularity. Here's a quick FastFlux refresher, including a deeper dive into how cybercriminals use it to make their infrastructure resilient against takedowns.

What is FastFlux?

FastFlux is a technique used by phishers, malware authors, and botnet operators to hide the actual location of their infrastructure behind a network of compromised hosts that are acting as a proxy, forwarding the malicious traffic to the real backend.

What makes FastFlux so attractive to cybercriminals?

All FastFlux networks that are currently in business can be rented as a service on the dark web. This makes life easy for botnet operators. All they have to do is register domains required for the botnet C&Cs and point them to the FastFlux operator's service. FastFlux takes care of the rest, ensuring that the A records rapidly change.

Here's an example of a FluBot botnet C&C domain hosted on a FastFlux botnet:

```
;; QUESTION SECTION:
;gurbngbcxheshsj.ru.       IN    A

;; ANSWER SECTION:
```

Domain	TTL	RecordType		IP Address
gurbngbcxheshsj.ru.	150	IN	A	189.165.94.67
gurbngbcxheshsj.ru.	150	IN	A	124.109.61.160
gurbngbcxheshsj.ru.	150	IN	A	187.190.48.60
gurbngbcxheshsj.ru.	150	IN	A	115.91.217.231
gurbngbcxheshsj.ru.	150	IN	A	175.126.109.15
gurbngbcxheshsj.ru.	150	IN	A	175.119.10.231
gurbngbcxheshsj.ru.	150	IN	A	218.38.155.210
gurbngbcxheshsj.ru.	150	IN	A	179.52.22.168
gurbngbcxheshsj.ru.	150	IN	A	113.11.118.155
gurbngbcxheshsj.ru.	150	IN	A	14.51.96.70

What is FluBot?

FluBot is a trojan that infects Android devices. It steals user credentials and spreads itself by turning the infected smartphone into an SMS spam zombie.

As you can see, the botnet C&C domain uses ten concurrent A records with a time to live (TTL) of only 150 seconds. Monitoring these A records reveals that the underlying FastFlux botnet consists of 100 to 150 active FastFlux nodes per day.

Generally, these nodes are compromised devices, commonly Customer Premise Equipment* (CPE), insecurely configured (e.g., running vulnerable software or using standard login credentials), and accessible directly from the internet.

These kinds of devices are a soft target for cybercriminals. They simply need to conduct internet-wide scans to discover these vulnerable devices and compromise them. This whole process can all be automated, making it quick, easy, and effective.

Operators of FastFlux botnets choose the geolocation of their target devices they use for FastFlux hosting carefully. As you will notice when reading through this report, many FastFlux C&C nodes are hosted in places that are relatively well "digitized," i.e., have good internet connections but are not as advanced along the maturity curve in terms of cybersecurity.

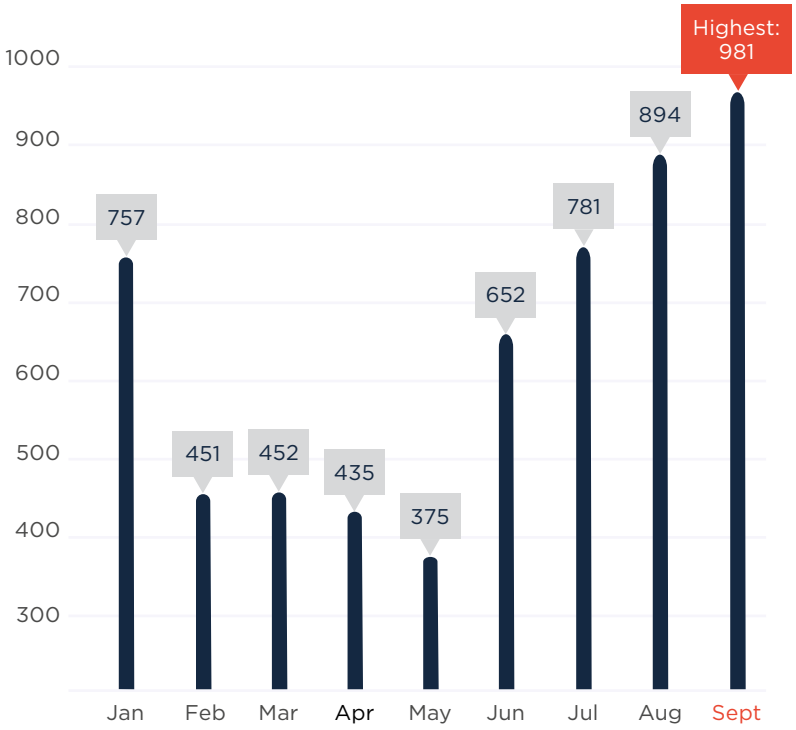
Latin America is commonly a target, e.g., Brazil, Chile, Argentina, Uruguay, and Asian countries such as Korea. The newcomers to the geolocation statistics in this update reflect this.

* https://en.wikipedia.org/wiki/Customer-premises_equipment

Number of botnet C&Cs observed, Q3 2021

In Q3 2021, Spamhaus Malware Labs identified 2,656 botnet C&Cs compared to 1,462 in Q2 2021. This was an 82% increase quarter on quarter! The monthly average increased from 487 per month in Q2 to 885 botnet C&Cs per month in Q3.

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



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

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 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.

Geolocation of botnet C&Cs, Q3 2021

Given FastFlux's influence over the past quarter, it isn't surprising that there's a clear pattern to the newcomers entering the chart for Q3 2021. Many of the countries joining the charts were responsible for hosting a large percentage of TeamBot, and FluBot botnet C&C servers - utilizing Fastflux - and fit the profile of countries with extensive internet coverage but less security-focused.

Significant increases in Russia

The number of botnet C&Cs located in Russia has dramatically risen. This is the second increase quarter on quarter that Russia has experienced:

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

Therefore, it comes as no surprise that in Q3 Russia overtook the United States for the #1 spot.

Continued increases across Europe

The trend that started in Q2 continued in Q3. Once again, there was an uptick in the number of botnet C&C servers hosted in various European countries, including the Netherlands (+63%), Germany (+45%), France (+34%), and Switzerland (+34%).

New entries

Mexico (#4), Saudi Arabia (#7), Dominican Republic (#8), Korea (#10), Uruguay (#11), Argentina (#14), Sweden (#18), Romania (#20).

Departures

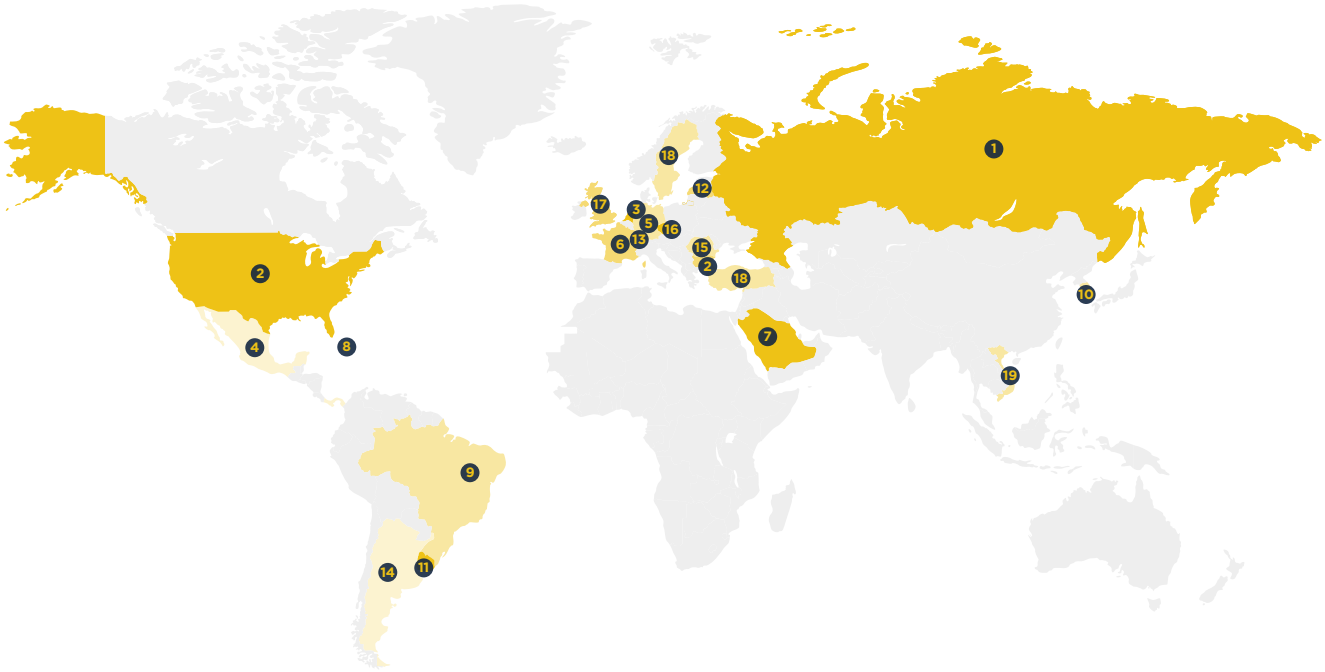
Ukraine, Seychelles, Panama, Canada, Malaysia, Poland, Finland, Turkey.

Geolocation of botnet C&Cs, Q3 2021 (continued)

Top 20 locations of botnet C&Cs

Rank	Country	Q2 2021	Q3 2021	% Change Q on Q
#1	Russia	233	381	64%
#2	United States	281	301	7%
#3	Netherlands	168	273	63%
#4	Mexico	-	182	New Entry
#5	Germany	117	170	45%
#6	France	92	123	34%
#7	Saudi Arabia	-	117	New Entry
#8	Dominican Rep	-	96	New Entry
#9	Brazil	12	86	617%
#10	Korea	-	68	New Entry

Rank	Country	Q2 2021	Q3 2021	% Change Q on Q
#11	Uruguay	-	63	New Entry
#12	Latvia	84	58	-31%
#13	Switzerland	41	55	34%
#14	Argentina	-	50	New Entry
#15	Moldova	29	49	69%
#16	Czech Republic	31	40	29%
#17	United Kingdom	57	39	-32%
#18	Sweden	-	38	New Entry
#19	Vietnam	13	34	162%
#20	Romania	-	33	New Entry



Malware associated with botnet C&Cs, Q3 2021

Here are the top malware families associated with newly observed botnet C&Cs in Q3, 2021.

TeamBot and FluBot emerging

Have you ever heard of TeamBot? Probably not. While it is neither a new nor severe threat, TeamBot sits at the top of the charts with FluBot, both backdoors.

Our threat hunters believe that TeamBot and FluBot are using the same FastFlux infrastructure, rotating the same botnet C&C IP addresses every few minutes, hence the shared listing below.

This quarter, there was an explosion in backdoor malware, making it the most prevalent type of malware associated with botnet C&Cs in Q3 2021.

RedLine wins, Raccoon loses

In 2021, we've been observing a battle for pole position between RedLine and Raccoon, both credential stealers, available for sale on the dark web. While we saw a huge increase (571%) of Raccoon botnet C&C servers in Q2 2021, RedLine malware experienced a 71% increase in Q3 2021, displacing Raccoon from its top spot.

IcedID disappears

IcedID has been relatively inactivate this year, making a brief appearance at #18 in Q2 before disappearing again this quarter. The reason behind this is unknown. However, our researchers don't believe its silence will continue indefinitely. IcedID is one of the Trojans available to ransomware groups for purchase on the dark web. These Trojans sell access to corporate networks - a very lucrative business.

What is backdoor malware?

This type of malware circumnavigates normal authentication procedures and other security measures to gain high-level access to a system,

New entries

TeamBot (#1), FluBot (#1) Smoke Loader (#9), AveMaria (#13).

Departures

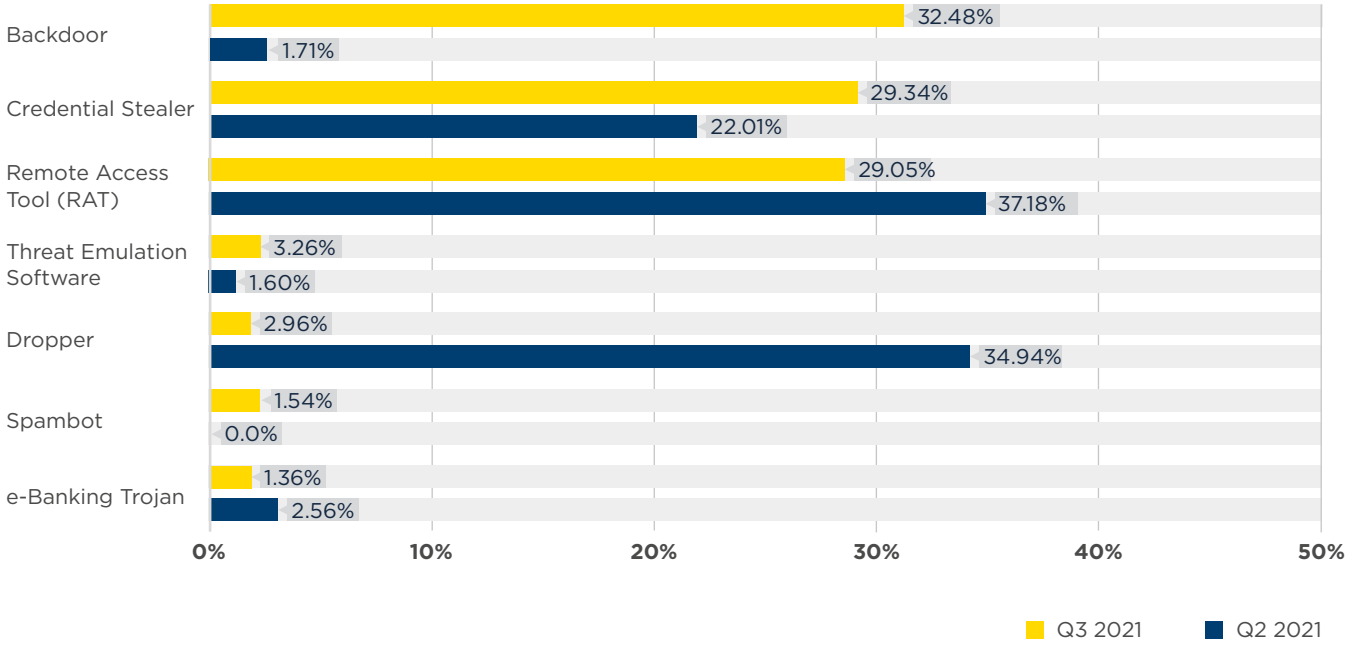
Oski, IcedID, Arkei.

Malware associated with botnet C&Cs, Q3 2021 (continued)

Malware families associated with botnet C&Cs

Rank	Q2 2021	Q3 2021	% Change	Malware Family	Description
#1	-	507	New Entry	TeamBot & FluBot	Backdoor
#2	123	210	71%	RedLine	Credential Stealer
#3	42	136	224%	BitRAT	Remote Access Tool (RAT)
#4	83	121	46%	AsyncRAT	Remote Access Tool (RAT)
#5	66	108	64%	Loki	Credential Stealer
#6	302	93	-69%	Raccoon	Credential Stealer
#7	24	71	196%	NjRAT	Remote Access Tool (RAT)
#8	15	55	267%	Cobalt Strike	Backdoor
#9	-	50	New Entry	Smoke Loader	Dropper
#10	26	43	65%	VjwOrm	Credential Stealer
#11	16	41	156%	CryptBot	Backdoor
#12	24	40	67%	RemcosRAT	Remote Access Tool (RAT)
#13	-	37	New Entry	AveMaria	Remote Access Tool (RAT)
#13	23	37	61%	NanoCore	Remote Access Tool (RAT)
#15	17	30	76%	STRRAT	Remote Access Tool (RAT)
#16	23	26	13%	Tofsee	Spambot
#17	14	24	71%	ServHelper	Credential Stealer
#18	43	23	-47%	Gozi	e-Banking Trojan
#19	11	18	64%	QuasarRAT	Remote Access Tool (RAT)
#20	23	17	-26%	AgentTesla	Credential Stealer

Malware type comparisons between Q2 and Q3 2021



Most abused top-level domains, Q3 2021

No changes at the top of the chart

In Q3, .com and .xyz continued to stay at the top of our ranking. The situation deteriorated for these two TLDs, particularly .com, which experienced a 90% increase. We hope that VeriSign, the owner of this TLD, will take all necessary steps to improve this situation and increase their TLD's reputation.

Three new TLDs

Two new gTLDs and one ccTLD joined our Top 20: .club, .co and .monster. All have seen a significant increase in the number of new botnet C&C domains registered through their service.

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.

New entries

club (#9), co (#18), monster (#19).

Departures

vip, online, live.

Most abused top-level domains, Q3 2021 (continued)

Top abused TLDs - number of domains

Rank	Q2 2021	Q3 2021	% Change	TLD	Note
#1	4113	7827	90%	com	gTLD
#2	739	833	13%	xyz	gTLD
#3	607	829	37%	top	gTLD
#4	146	665	355%	net	gTLD
#5	662	538	-19%	buzz	ccTLD
#6	151	330	119%	ru	ccTLD
#7	139	306	120%	cn	ccTLD
#8	157	265	69%	org	gTLD
#9	140	183	31%	tk	Originally ccTLD, now effectively gTLD
#9	80	183	129%	su	ccTLD
#9	-	183	New Entry	club	gTLD
#12	78	178	128%	info	gTLD
#13	208	170	-18%	br	ccTLD
#14	106	132	25%	ga	Originally ccTLD, now effectively gTLD
#15	116	126	9%	eu	ccTLD
#16	104	123	18%	ml	Originally ccTLD, now effectively gTLD
#17	73	98	34%	cf	ccTLD
#18	-	89	New Entry	co	ccTLD
#19	-	82	New Entry	monster	gTLD
#19	141	82	-42%	cloud	gTLD

Most abused domain registrars, Q3 2021

We observed significant increases across most of the domain registrars listed in our Top 20. The United States is home to the largest percentage of domain registrars; however, their share has dropped quarter on quarter, while China, the United Kingdom, and Russia have increased.

In Q2 you saw Arsys, now you don't

A nod of approval to Arsys, who was a new entry at #5 in Q2. They appear to have taken positive steps to ensure their TLD remains as clean as possible and dropped off the Top 20 in Q3, along with HiChina, 1API, Name.com, and 55hl.com. Excellent work to all these registrars.

Reseller issues

In Q3, we saw the biggest increases in newly registered botnet C&C domains at CentralNic (+488%), Tucows (+266%), RegRU (+252%), West263.com (+168%), and Network Solutions (+163%).

The vast majority of fraudulent domain name registrations originate from poor resellers who have inappropriate or non-existent customer vetting in place.

Registrars can struggle to penalize these dirty resellers for many reasons, including poorly written Terms of Services (ToS). However, other matters can also come into play, such as a vested financial interest or a fundamental lack of motivation to take responsibility for these issues.

We hope that these registrars will improve their reputation quickly by implementing stricter measures on their resellers to ensure they strive to fight against the registration of fraudulent domain names.

Registrars and botnet C&C operators

Cybercriminals need to find a sponsoring registrar to get a botnet C&C domain name registered. 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

Porkbun (#7), dnspod.cn (#11), nicenic.net (#13), Openprovider (#18), OVH (#19).

Departures

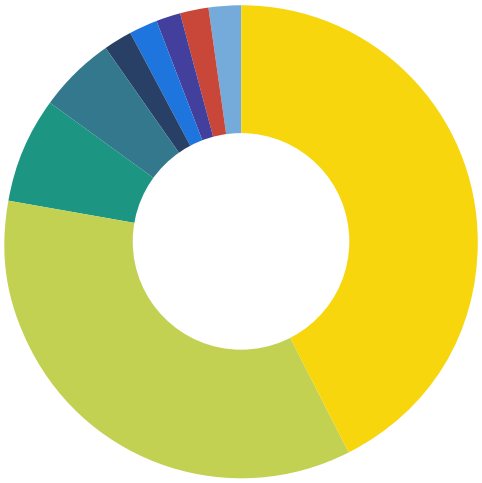
Arsys, HiChina, Name.com, 55hl.com, 1API.

Most abused domain registrars, Q3 2021 (continued)

Most abused domain registrars - number of domains

Rank	Q2 2021	Q3 2021	% Change	Registrar	Country
#1	1797	1568	-13%	NameSilo	United States
#2	955	1267	33%	Namecheap	United States
#3	504	1217	141%	Alibaba	China
#4	526	787	50%	eName Technology	China
#5	112	658	488%	CentralNic	United Kingdom
#6	135	475	252%	RegRU	Russia
#7	110	403	266%	Tucows	United States
#7	-	403	New Entry	Porkbun	United States
#9	101	266	163%	Network Solutions	United States
#10	125	255	104%	Xin Net	China
#11	80	214	168%	west263.com	China
#11	-	214	New Entry	dnspod.cn	China
#13	-	209	New Entry	nicenic.net	China
#14	215	189	-12%	Eranet International	China
#15	92	188	104%	Key Systems	Germany
#16	110	176	60%	22net	China
#17	188	169	-10%	PDR	India
#18	-	165	New Entry	Openprovider	Netherlands
#19	-	160	New Entry	OVH	France
#20	91	154	69%	WebNic.cc	Singapore

LOCATION OF MOST ABUSED DOMAIN REGISTRARS



Country	Botnets	%
United States	3907	42.8%
China	3261	35.7%
United Kingdom	658	7.2%
Russia	475	5.2%
Germany	188	2.1%
India	169	1.8%
Netherlands	165	1.8%
France	160	1.8%
Singapore	154	1.7%
Total	**9137**	

Networks hosting the most newly observed botnet C&Cs, Q3 2021

As usual, there were many changes in the networks hosting newly observed botnet C&Cs. Notably, there was an influx of networks hosting FastFlux botnet C&Cs, used by cybercriminals to host backdoor malware.

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 in a timely manner.

serverion.com

We have seen a 69% increase in the number of new botnet C&C servers installed at the Dutch hosting provider serverion.com. Our researchers believe that this increase is predominantly due to their downstream customer des.capital, which tends to attract botnet operators.

Making positive changes

In last quarter's update, we reported that a botnet hosting operation had moved from Amazon to DigitalOcean, causing the latter's listings to rocket. We want to congratulate DigitalOcean for dropping off our Top 20 list in Q3 2021, along with other networks, including Google, who were at #2, HostSailor, Microsoft, M247, and Off Shore Racks.

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 take place 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 are following 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

uninet.net.mx (#1), stc.com.sa (#3), claro.com.do (#4), antel.net.uy (#8), telefonica.com.br (#9), telefonica.com.ar (#16), uplus.co.kr (#17), hotwinds.com (#18).

Departures

google.com, itld.com, digitalocean.com, internet-it, hostsailor.com, microsoft.com, m247.ro, offshoreracks.com.

SPAMHAUS

Networks hosting the most newly observed botnet C&Cs, Q3 2021 (continued)

Newly observed botnet C&Cs per network

Rank	Q2 2021	Q3 2021	% Change	Network	Country
#1	-	177	New Entry	uninet.net.mx	Mexico
#2	68	115	69%	serverion.com	Netherlands
#3	-	105	New Entry	stc.com.sa	Saudi Arabia
#4	-	95	New Entry	claro.com.do	Dominican Rep
#5	48	89	85%	privacyfirst.sh	Germany
#6	35	69	97%	ipjetable.net	France
#7	29	68	134%	cloudflare.com	United States
#8	-	63	New Entry	antel.net.uy	Uruguay
#9	-	58	New Entry	telefonica.com.br	Brazil
#10	82	56	-32%	pq.hosting	Russia
#11	56	52	-7%	ovh.com	France
#12	46	51	11%	hetzner.de	Germany
#13	16	45	181%	mivocloud.com	Moldova
#14	40	44	10%	baxet.ru	Russia
#14	49	44	-10%	nano.lv	Latvia
#16	-	43	New Entry	telefonica.com.ar	Argentina
#17	-	41	New Entry	uplus.co.kr	Korea
#18	26	33	27%	alibaba-inc.com	China
#18	-	33	New Entry	hotwinds.com	United States
#20	47	32	-32%	mgnhost.ru	Russia

Networks hosting the most active botnet C&Cs, Q3 2021

Finally, let's take a look at the networks that hosted a large number of active botnet C&Cs in Q3 2021. Hosting providers who appear in this ranking either have an abuse problem or do not take the appropriate action when receiving abuse reports.

An increase in botnet C&C abuse

Sadly, the situation in terms of active botnet C&C servers deteriorated for many ISPs who were on our Top 20 in Q2. Ipjetable.net (FR), microsoft.com (US), vietserver.vn (VN), and openvpn (SE) all have one thing in common: instead of taking appropriate measures against the abuse on their infrastructure, the number of active botnet C&C servers increased in these networks.

uninet.net.mx & stc.com.sa

These two ISPs are new to our Top 20 this quarter and have taken #1 and #2 spots, due to the vast number of FastFlux bots hosted on their networks.

In fact, the majority of the newcomers to this chart are due to hosting FastFlux bots on their networks and not responding quickly to abuse reports. All these companies are providing a resilient botnet C&C infrastructure for botnet operators.

New entries

uninet.net.mx (#1), stc.com.sa (#2), claro.com.do (#4), antel.net.uy (#6), telefonica.com.br (#7), telefonica.com.ar (#8), tie.cl (#10), serverion.com (#10), algartelecom.com.br (#14), uplus.co.kr (#17), skbroadband.com (#19).

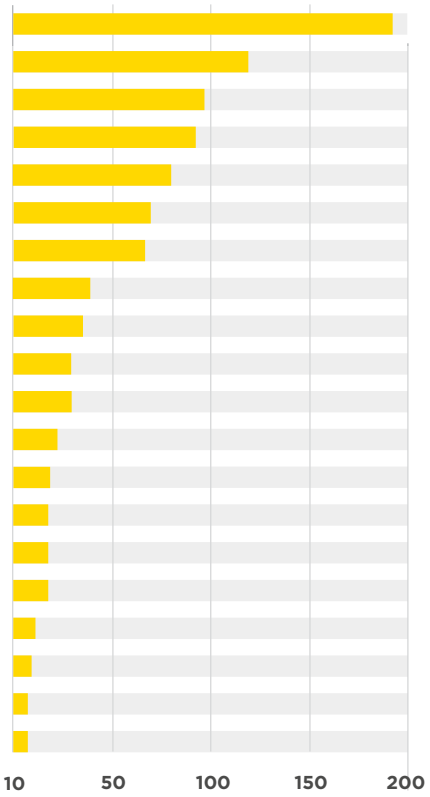
Departures

google.com, ttnet.com.tr, inmotionhosting.com, m247.ro, datawire.ch, mtnnigeria.net, eliteteam.to, unusinc.com, chinanet-js, kornet.net.

Networks hosting the most active botnet C&Cs, Q3 2021 (continued)

Total number of active botnet C&Cs per network

Rank	Q2 2021	Q3 2021	% Change	Network	Country
#1	-	185	New Entry	uninet.net.mx	Mexico
#2	-	119	New Entry	stc.com.sa	Saudi Arabia
#3	61	99	62%	ipjetable.net	France
#4	-	97	New Entry	claro.com.do	Dominican Rep
#5	58	79	36%	microsoft.com	United States
#6	-	68	New Entry	antel.net.uy	Uruguay
#7	-	63	New Entry	telefonica.com.br	Brazil
#8	-	41	New Entry	telefonica.com.ar	Argentina
#9	23	32	39%	vietserver.vn	Vietnam
#10	-	29	New Entry	tie.cl	Chile
#10	-	29	New Entry	serverion.com	Netherlands
#12	20	24	20%	ovpn.com	Sweden
#13	21	22	5%	charter.com	United States
#14	-	21	New Entry	algartelecom.com.br	Brazil
#14	18	21	17%	cloudvider.net	United Kingdom
#14	17	21	24%	une.net.co	Colombia
#17	-	19	New Entry	uplus.co.kr	Korea
#18	17	18	6%	hostry.com	Cyprus
#19	-	17	New Entry	skbroadband.com	Korea
#19	12	17	42%	claro.com.co	Colombia



That's all for now.

Stay safe and see you in January!