SPAMHAUS
THE SPAMHAUS PROJECT

Botnet Threat Update
Q3–2019

You would be right to assume that malware authors and botnet operators in the Northern Hemisphere took a break over the summer months. Unfortunately, that assumption would be incorrect; the amount of newly detected botnet command & control servers (C&Cs) reached an all-time high in July this year with more than 1,500 botnet C&Cs detected by Spamhaus Malware Labs. This is far in excess of the monthly average, set in the first half of this year, of 1,000 botnet C&Cs.

One of the most notorious botnets called ‘Emotet’, however, did appear to go on vacation. This botnet went silent for several months, but returned in September with a large scale spam campaign.

Spotlight

Emotet returns from Summer Break

In June this year, the notorious Emotet botnet went quiet, as noted in the Q2 2019 Botnet Threat Update[1]. The threat actors behind Emotet abruptly stopped sending out their daily spam campaigns which were responsible for distributing the Trojan around the globe. However, the botnet itself remained active.

The reason for the sudden disappearance of Emotet remains unclear. While some security researchers thought that Emotet had gone for good, the majority believed that it was just a matter of time until Emotet reappeared on the threat landscape. The latter turned out to be correct.

In September 2019, almost three months after Emotet had stopped emitting spam, the threat actor 'reactivated' the botnet. Emotet became live again[2]. It didn't take long until the first Emotet spam campaigns started to flood millions of email boxes again. It appears that Emotet simply had an extended summer vacation.

During the three months that Emotet was inactive nothing changed in its modus operandi; once infected, Emotet tries to steal the following information from a victim's machine:

- Email address book
- Email credentials (Username/Password/SMTP server)
- Email conversations

Emotet exfiltrates the stolen information from the victim's machine to a botnet C&C server. Subsequently, the threat actor uses the stolen information to send out malspam campaigns in the name of the victim by 'hijacking' legit email conversations and abusing the stolen email credentials.

Dependent on the IT environment and geographical location of the victim's machine, Emotet may drop additional malware, for example, Gozi, Quakbot, or TrickBot. Some of these Trojans are used for lateral movement; e.g. once inside a corporate network, they then drop ransomware like Ryuk or MegaCortex.

Emotet – a modular (banking) trojan

Emotet, also known as 'Heodo', was a former ebanking Trojan that targeted e-banking customers around the world. In 2018, Emotet ceased its ebanking fraud activities and started to offer infected computers on a 'Pay-Per-Install' model to other cybercriminals. As of 2019, Emotet is one of the most dangerous botnets and indirectly responsible for a large amount of ransomware campaigns like Ryuk.

What is lateral movement?

This refers to the sideways, i.e. lateral movement an attacker makes once he has breached a network. The initial attack is from the outside to the inside (vertical). Usually, threat actors look for a 'soft' target to easily gain access to a network. However, once inside this network, they move across it to reach their final, intended target. This is lateral movement.

[1] https://www.spamhaus.org/news/article/785/spamhaus-botnet-threat-update-q2-2019

[2] https://www.zdnet.com/article/emotet-todays-most-dangerous-botnet-comes-back-to-life/

Number of botnet C&Cs observed, Q3 2019

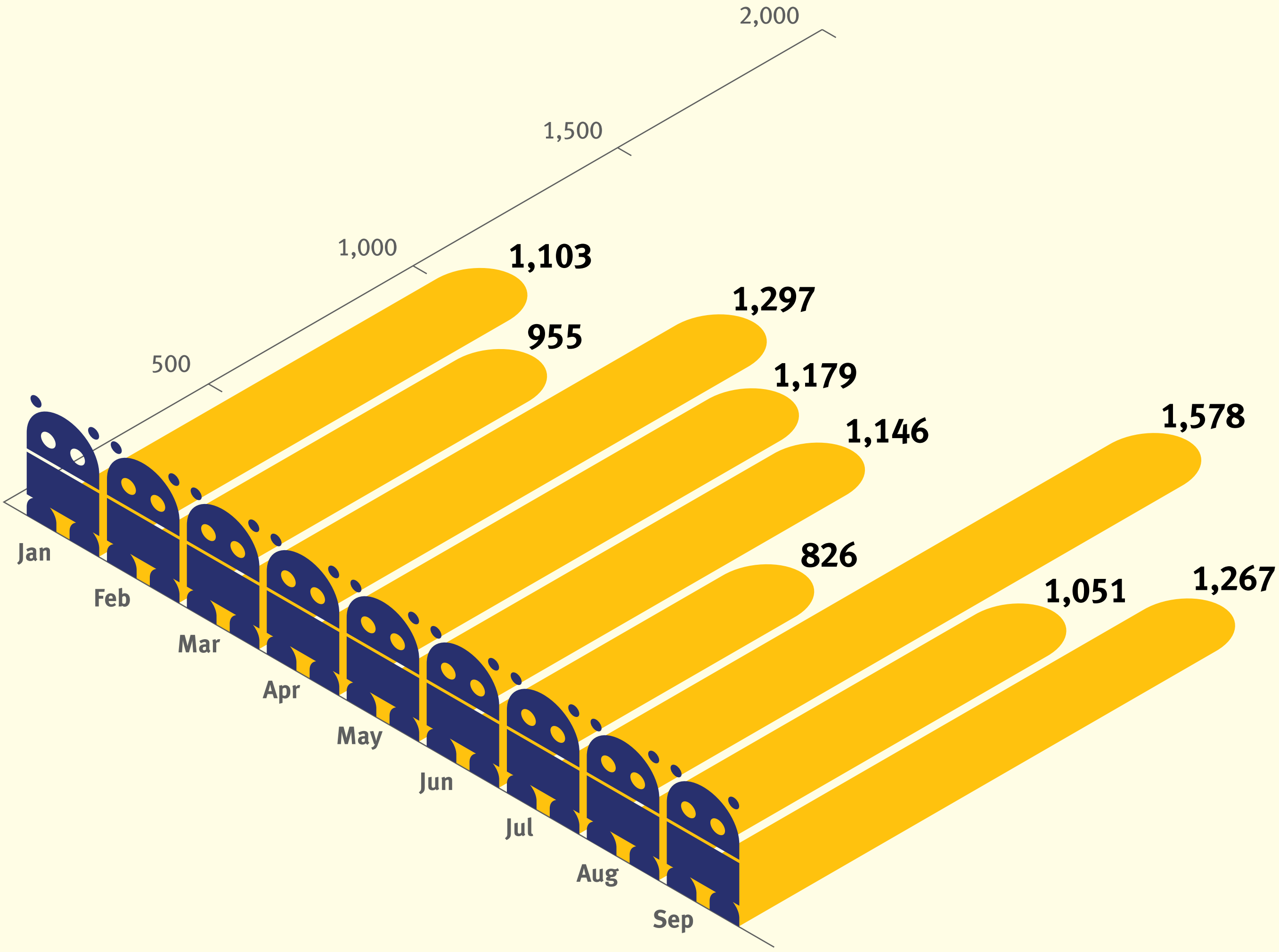
As we mentioned at the beginning of this report, the number of newly detected botnet C&Cs, resulting from fraudulent sign-ups, continued to increase in Q3 2019. Spamhaus Malware Labs detected approximately 1,300 new botnet C&Cs per month. This was a 30% increase on the monthly averages seen in the first two quarters of 2019. Even more worrying: we have observed and blocked more botnet C&Cs to date in 2019 than we did in the whole of 2018:

- Q1–Q4, 2018 – 10,263 botnet C&Cs
- Q1–Q3, 2019 – 10,402 botnet C&Cs

Given this statistic, it will come as no surprise that in July 2019 we detected 1,587 new botnet C&C servers – which is a new monthly record!

What is a 'fraudulent sign-up'?

This is where a miscreant is using a fake, or stolen identity to sign-up for a service, usually a Virtual Private Server (VPS) or a dedicated server, for the sole purpose of using it for hosting a botnet C&C.



Botnet controller listings per month

Malware associated with botnet C&Cs, Q3 2019

The most notable change between Q2 and Q3 has to be that of TrickBot. We detected a 550% increase in the number of botnet C&Cs associated with this malware family. There were additional smaller changes in the malware landscape, with some families dropping out of the charts and others appearing.

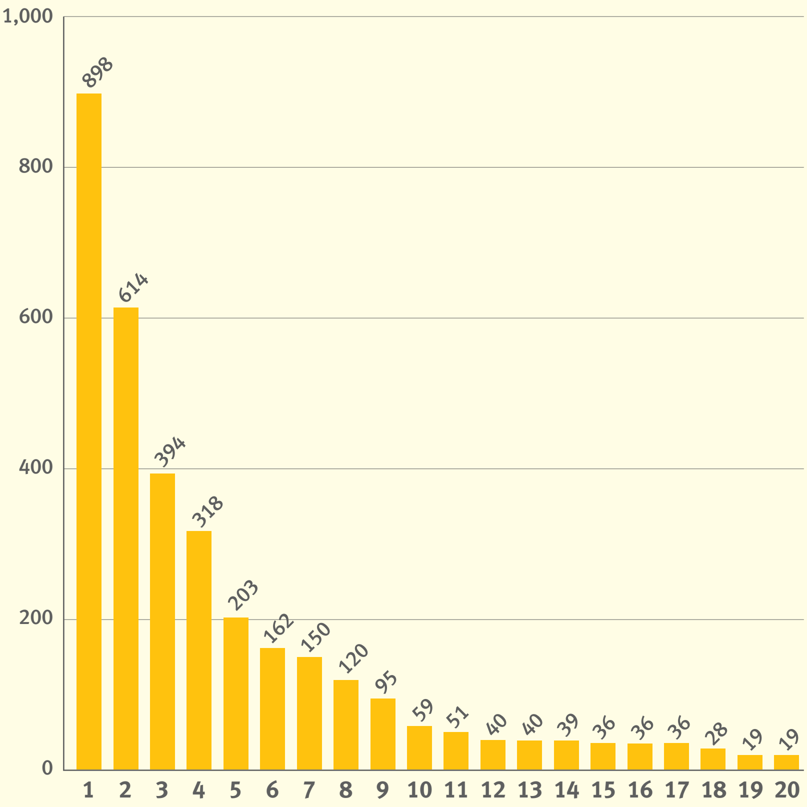
Lokibot: While the number of botnet C&C servers associated with Lokibot dramatically decreased by almost 400, Lokibot remained at the top of the chart with the highest number of newly detected botnet C&Cs.

AZORult and TrickBot: AZORult was knocked off its #2 spot by TrickBot. As detailed above, TrikBot's activity increased significantly over the past three months, from 64 botnet C&Cs associated with this malware family in Q2 to 614 in Q3. The good news is that the number of newly detected botnet C&Cs associated with AZORult decreased from 771 in Q2 to only 394 in Q3.

RevengeRAT and AveMariaRAT: We said goodbye to RevengeRAT, which dropped out of the Top 20 chart and got replaced by a newcomer called AveMariaRAT. The high fluctuation of remote access tools (RATs) and Credential Stealers shows the bitter fight to gain market share between malware authors.

Baldr & IcedID: First observed in April 2019, Baldr quickly ascended to the heady heights of #14 in Q2. However, the malware's infamy was short-lived and faded away, dropping off the chart in Q3 2019, along with IcedID, an e-banking Trojan.

Malware families associated with botnet C&C



Rank	Malware	Note
1	Lokibot	Credential Stealer
2	TrickBot	Dropper/Backdoor
3	AZORult	Credential Stealer
4	NanoCore	Remote Access Tool (RAT)
5	Gozi	e-banking Trojan
6	Emotet	Dropper/Backdoor
7	Pony	Credential Stealer
8	PredatorStealer	Credential Stealer
9	RemcosRAT	Remote Access Tool (RAT)
10	njrat	Remote Access Tool (RAT)
11	Adwind	Remote Access Tool (RAT)
12	AgentTesla	Credential Stealer
13	KPOTStealer	Credential Stealer
14	NetWire	Remote Access Tool (RAT)
15	QuasarRAT	Remote Access Tool (RAT)
16	CoinMiner	generic crypto miners
17	ArkeiStealer	Credential Stealer
18	Amadey	Credential Stealer
19	AveMariaRAT	Remote Access Tool (RAT)
20	LimeRAT	Remote Access Tool (RAT)

Most abused top-level domains, Q3 2019

This quarter saw the number of country code top-level domains (ccTLDS) increase in the Top 20 list. Almost half of the TLDs were within the ccTDL name space: '.ru', '.pw', '.eu', '.ga', '.tk', '.su', '.ml', '.cf' and '.me.'

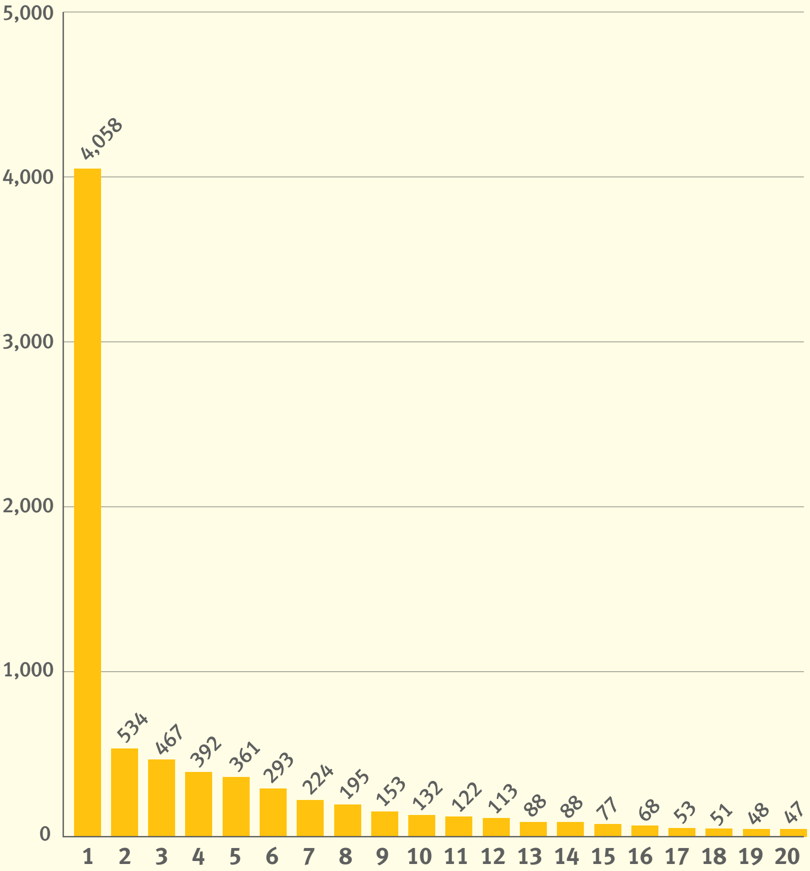
The leader of the chart remained the same, as in Q2; the generic top-level domain (gTLD) '.com.' Meanwhile the number of fraudulent domain names registered within ccTLD '.ru' almost halved from 731 domains in Q2 to 392 domains in Q3.

An interesting change to note is that in Q3 two more gTLDs joined '.com' in Q3 in the top 3: '.net' and '.info'.

What domains do these statistics include?

Remember that we only count domain names that have been registered fraudulently for the sole purpose of hosting a botnet C&C. These statistics do not include botnet C&Cs hosted on compromised websites or domain names.

Top abused TLDs – number of domains



Rank	TLD	Note
1	com	gTLD
2	net	gTLD
3	info	gTLD
4	ru	ccTLD of Russia
5	top	gTLD
6	pw	ccTDL of Palau
7	org	gTLD
8	xyz	gTLD
9	eu	ccTLD of the European Union
10	icu	gTLD
11	ga	originally ccTLD, now effectively gTLD
12	tk	originally ccTLD, now effectively gTLD
13	name	gTLD
14	live	gTLD
15	su	ccTLD of soviet union
16	ml	originally ccTLD, now effectively gTLD
17	cf	originally ccTLD, now effectively gTLD
18	site	gTLD
19	club	gTLD
20	me	ccTLD of Montenegro

Most abused domain registrars, Q3 2019

Namecheap: The US-based domain registrar ‘Namecheap’ continued to be the favorite place for malware authors to register their botnet C&C domains.

OpenProvider: The number of fraudulently registered domain names registered through the Dutch domain registrar ‘OpenProvider’ (aka ‘Hosting Concepts’) almost doubled from 188 in Q2 to 344 in Q3, placing them at #3 in the chart.

Register.com: Great work by ‘register.com’, who looks to have improved processes, as they no longer appeared on our Top 20 most abused domain registrars in Q3. This is in stark comparison to Q1, where they accounted for 22% of the total number of registered domains used for botnet C&Cs.

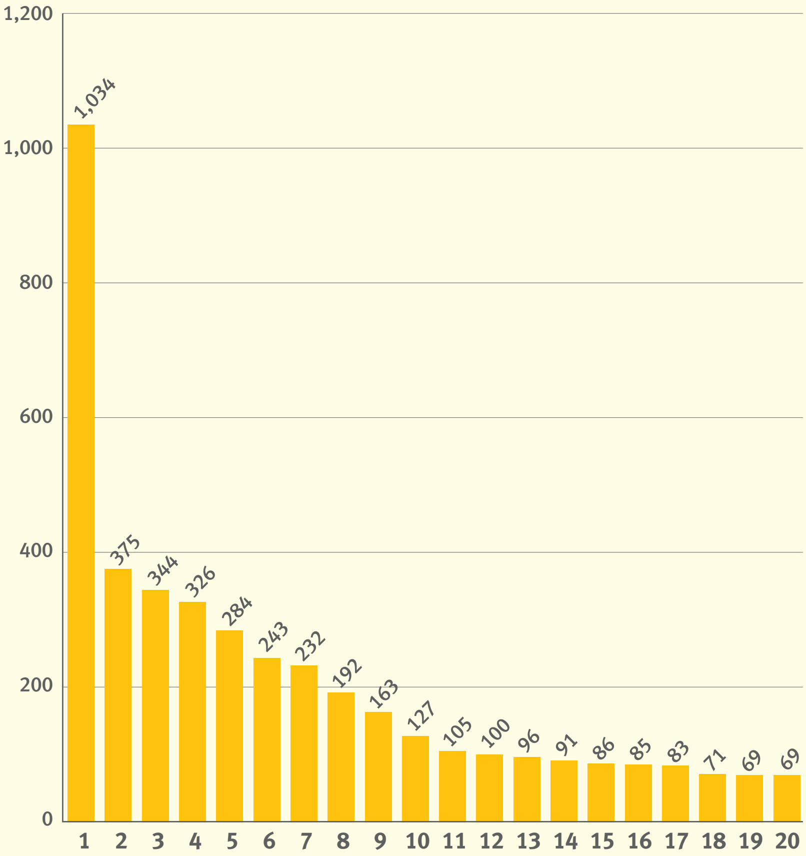
Newcomers: Newcomers to our chart of most abused domain registrars were the German based domain registrar ‘Key Systems’ and the French registrar ‘OVH’.

Poor processes leave operators open to abuse

To register a domain name, a botnet operator must choose a domain registrar. Domain registrars play a crucial role in fighting abuse in the domain landscape: they not only vet the domain registrant (customer) but also have the ability to suspend or delete domain names.

Unfortunately, many domain registrars do not have a robust customer vetting process, leaving their service open to abuse.

Most abused domain registrars – number of domains



Rank	Registrar	Country
1	Namecheap	United States
2	West263.com	China
3	OpenProvider	Netherlands
4	Reg.ru	Russia
5	55hl.com	China
6	Namesilo	United States
7	WebNic.cc	Singapore
8	CentralNic	United Kingdom
9	PDR	India
10	Arsys	Spain
11	NameBright/DropCatch	United States
12	1API	Germany
13	OVH	France
14	RU-CENTER	Russia
15	Eranet international	China
16	GMO	Japan
17	Hostinger	Lithuania
18	Xin Net	China
19	Key Systems	Germany
20	OnlineNIC	China

Internet Service Providers (ISPs) hosting botnet C&Cs, Q3 2019

Cloudflare Vs. Alibaba: We continued to see ‘cloudflare.com’, a US-based content delivery network (CDN) provider, being one of the preferred options by cybercriminals to host botnet C&C servers. This trend has been evident since 2018. Disappointingly, we have still seen no apparent attempts from Cloudflare to battle the ongoing abuse of their network for botnet hosting and other hostile infrastructure. However, as of Q3, Cloudflare got beaten by the Chinese cloud provider Alibaba, by a narrow margin of 4.

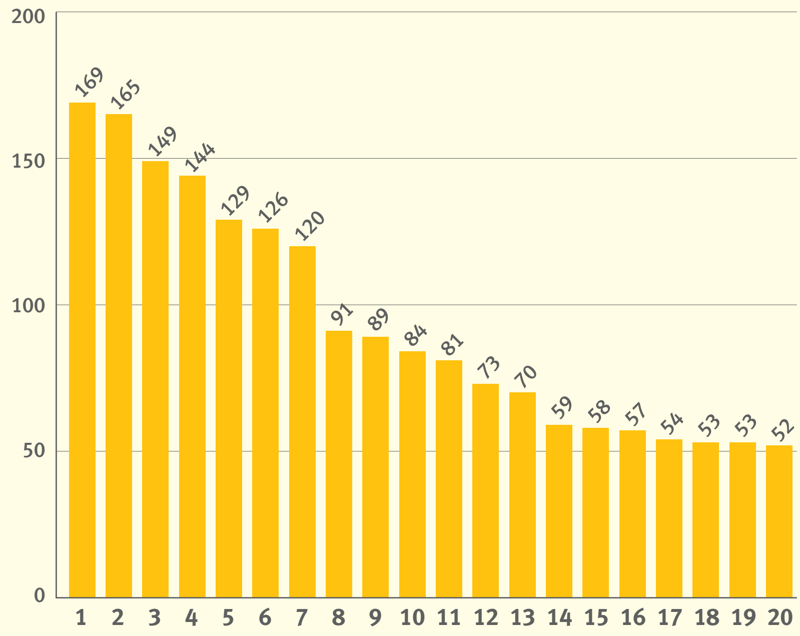
A surge in the number of Botnet C&Cs hosted in Russia: We saw a proliferation of botnet C&Cs hosted across various hosting providers in Russia, notably ‘ispserver.com’, ‘reg.ru’, ‘simplecloud.ru’, ‘marosnet.ru’ and ‘spacenet.ru’. After a short period of respite, we are once again seeing a trend in cybercriminals moving their infrastructure to Russian Internet service providers.

Google back in the game: In Q1 and Q2 2019, there were a minimal number of botnet C&C servers hosted on Google’s network. Unfortunately, in Q3, we have seen an increase in newly detected botnet C&C servers being installed on Google’s Cloud Infrastructure. This has resulted in the return of Google to our Top 20 chart.

Cloudflare

While Cloudflare does not directly host any content, it provides services to botnet operators, masking the actual location of the botnet controller and protecting it from DDoS attacks.

Botnet C&Cs per ISP



Rank	Network	Country	
1	alibaba-inc.com	China	🇨🇳
2	cloudflare.com	United States	🇺🇸
3	ispserver.com	Russia	🇷🇺
4	ovh.net	France	🇫🇷
5	colocrossing.com	United States	🇺🇸
6	reg.ru	Russia	🇷🇺
7	simplecloud.ru	Russia	🇷🇺
8	marosnet.ru	Russia	🇷🇺
9	spacenet.ru	Russia	🇷🇺
10	your-vpn.network	Jamaica	🇯🇲
11	m247.ro	Romania	🇷🇴
12	netangels.ru	Russia	🇷🇺
13	server-panel.net	Netherlands	🇳🇱
14	adminvps.ru	Russia	🇷🇺
15	selectel.ru	Russia	🇷🇺
16	comfortel.pro	Russia	🇷🇺
17	fink.org	Switzerland	🇨🇭
18	itldc.com	Ukraine	🇺🇦
19	mtw.ru	Russia	🇷🇺
20	google.com	United States	🇺🇸

Thanks for reading. We’ll see you in 2020! Stay malware free in the meantime.