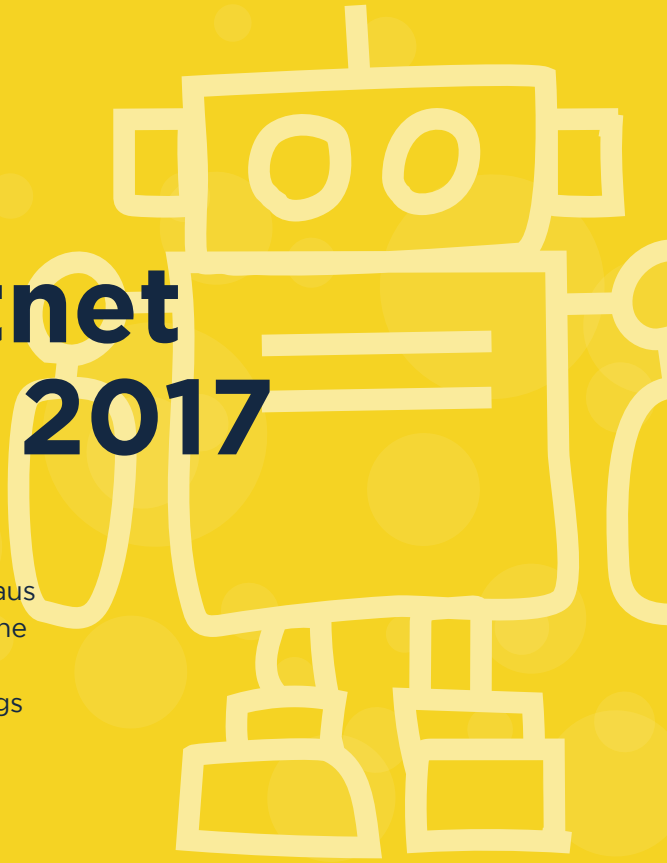
SPAMHAUS



Spamhaus Botnet Threat Report 2017

Now that 2017 is behind us, as we do each year, the Spamhaus Project would like to give some numbers and thoughts on the botnet threats we encountered. In 2017, Spamhaus Malware Labs identified and issued Spamhaus Block List (SBL) listings for more than 9,500 botnet Command & Control servers on 1,122 different networks. A botnet controller, commonly abbreviated as "C&C", is being used by fraudsters to both control malware infected machines and to extract personal and valuable data from malware infected victims. Botnet controllers therefore play a core role in operations conducted by cybercriminals who are using infected machines to send out spam, ransomware, launch DDoS attacks, commit ebanking fraud, click-fraud or to mine cryptocurrencies such as Bitcoin. An infected machine can be a desktop computer, mobile device (like a smartphone) but also an IoT device ("Internet Of Things") device such as webcam or network attached storage (NAS) that is connected to the internet.

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, the sponsoring registrars and the network hosting the botnet C&C infrastructure.

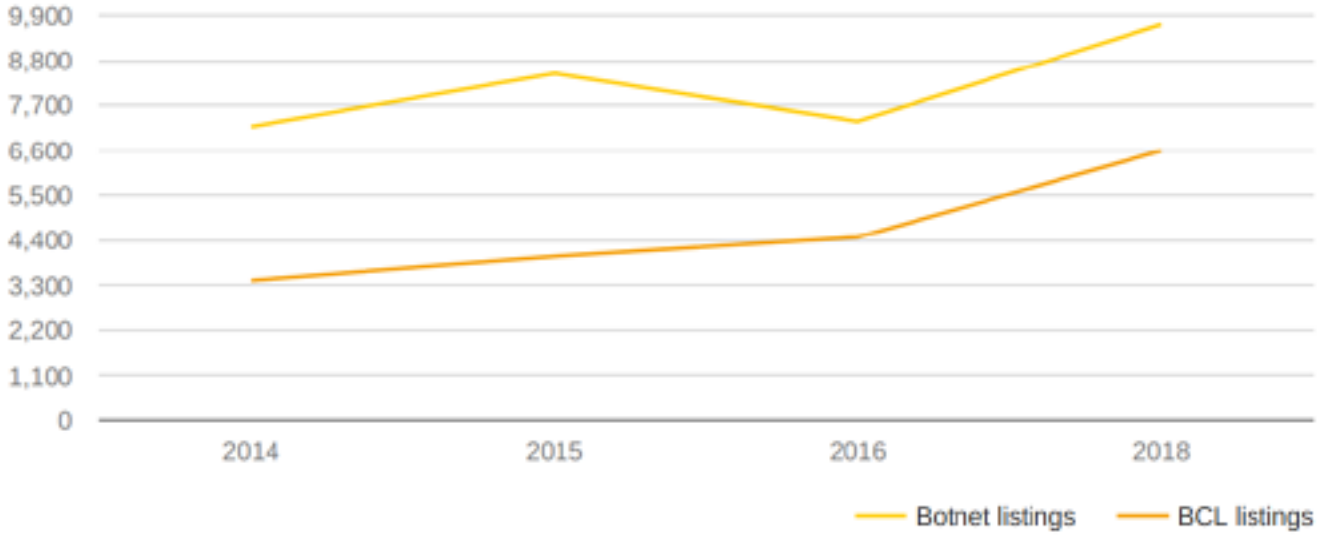
This report provides an overview of the number of botnet C&Cs associated with these elements, along with a quarterly comparison. We discuss the trends we are observing and highlight service providers struggling to control the number of botnet operators abusing their services.

Spamhaus SBL + BCL

In 2017, nearly every 7th SBL listing that Spamhaus issued was for a botnet controller. The number of such botnet "C&C" listings increased by a massive 32% in 2017. The majority (6,588 or 68%) of botnet controllers Spamhaus found in 2017 were hosted on servers that had been ordered by cybercriminals for the solely purpose of hosting a botnet controller. Of course, cybercriminals do not use their real names to order infrastructure for botnet operation: they conduct so-called fraudulent sign-ups, using a fake or stolen identity. Whenever Spamhaus' Malware Labs comes across such a botnet controller, we issue a special kind of SBL listing: A BCL listing. The BCL - which stands for Botnet Controller List - is a "drop all traffic" list intended for use by networks to null route traffic to and from botnet controllers. The Spamhaus BCL only lists IP addresses of servers set up and operated by cybercriminals for the exclusive purpose of hosting a botnet controller (fraudulent sign-ups). Because these IP addresses host no legitimate services or activities, they can be directly blocked on ISP and corporate networks without risk of affecting legitimate traffic, effectively rendering harmless infected computers that may be present on their networks. Compared to 2016, the number of such BCL listings increased by more than 40%. Comparing the number of BCL listings to 2014, it is an increase of more of 90%.

The following chart shows the number of total botnet listings (compromised websites, compromised servers, fraudulent sign-ups) Vs. pure BCL listings (fraudulent sign-ups):

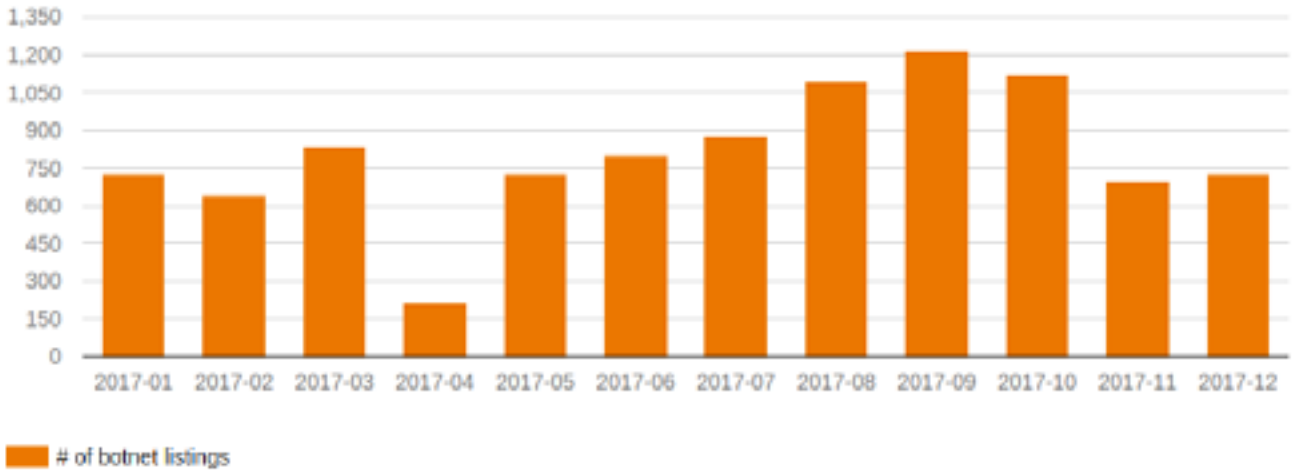
Botnet listings vs BCL listings



Spamhaus BCL Statistics (continued)

In average, we have issued between 600 and 700 BCL listings per month:

Botnet controller listings per month



The statistics exclude botnet controllers that are hosted on the dark web (like Tor). The use of such anonymization networks by botnet operators became more popular starting in 2016 because the location of the botnet controller can't be identified and hence a takedown of the server is almost impossible. For anonymization service like Tor we therefore recommend a whitelist approach: In general, block access to such service except for those users who need it (opt-in).

For botnet controllers that were not behind an anonymization network, we produced some statistics. The following table shows a list of hosting Internet Service Providers (ISP) ranked by number of C&Cs detected on that ISP's network during the past year. It also includes 2016 data to observe trends. This data includes botnet controllers that were hosted on compromised servers or websites, as well as those hosted through fraudulent sign-ups (BCL listings).

Spamhaus BCL Statistics (continued)

Overall botnet hosting (compromised websites, compromised servers, fraudulent sign-ups - BCL):

Rank	C&Cs 2017	C&Cs 2016	Network	Country
1	402	395	ovh.net	France (FR)
2	317	54	amazon.com	United States (US)
3	256	1	anmaxx.net	Seychelles (SC)
4	231	71	choopa.com	United States (US)
5	200	60	hostsailor.com	United Arab Emirates (AE)
6	197	34	alibaba-inc.com	China (CN)
7	179	83	digitalocean.com	United States (US)
8	176	14	tencent.com	China (CN)
9	162	75	worldstream.nl	Netherlands (NL)
10	144	65	timeweb.ru	Russia (RU)
11	132	72	quadranet.com	United States (US)
12	127	5	mtw.ru	Russia (RU)
13	126	24	aruba.it	Italy (IT)
14	125	79	hetzner.de	Germany (DE)
15	124	167	endurance.com	United States (US)
16	112	128	ispserver.com	Russia (RU)
17	111	71	blazingfast.io	Ukraine (UA)
18	108	19	namecheap.com	United States (US)
19	108	41	qhoster.com	Netherlands (NL)
10	107	118	colocrossing.com	United States (US)

The table shows the total number of detected botnet controllers per ISP, not distinguishing between compromised webservers/ websites or fraudulent sign-ups. This has to be considered carefully before drawing conclusions from the data. In general, large networks attract more abuse than smaller ones, simply due to the fact that they host more servers and websites that are poorly patched or not maintained at all.

It can be quite difficult for an ISP or hosting provider to prevent the compromise of a customer's server or website, since these are often fully under the control of the customer. In fact, many servers and websites are running outdated software, which makes them vulnerable to many attacks from the internet. It is an easy task for a cybercriminal to scan the internet for servers or websites that are running outdated or vulnerable software.

Spamhaus BCL Statistics (continued)

Some of the most popular open source content management systems (CMS) like WordPress, Joomla, Typo3 or Drupal are especially popular targets, due the high number of poorly maintained installations of these packages. We have seen that some of the more proactive ISPs and hosting providers are now using newer tools and methods to track down outdated software and monitor C&C traffic. Of course, blocking traffic to known C&Cs is a good start.

One of the problems we have seen in 2017 is that some hosting providers just remove the malicious file(s) on a compromised website where the botnet controllers resides, without identifying and fixing the initial infection vector. As a result of this bad practice, the botnet controller reappears shortly after the file has been removed by the hosting provider. Sometimes we have to notify a hosting provider multiple times about the botnet controller because the issue reappears again and again until the hosting provider finally identifies and fixes the culprit.

Compromised servers and websites are just one part of the problem. The other part of the ongoing botnet problem is the fraudulent sign-ups we have written about before. What stands out in 2017 is the dramatic increase of botnet controllers hosted at cloud providers: In April 2017 we blogged about this emerging abuse problem (https://www.spamhaus.org/news/article/736/botnet-controllers-in-the-cloud). While some of the cloud providers managed to deal with the increase of fraudulent sign ups, others are obviously still struggling with the problem. Thus, it is not surprising that they made it into the list of top 20 botnet controller hosting networks.

Spamhaus BCL Statistics (continued)

Botnet Controller Listings (BCL - fraudulent sign-ups) per network:

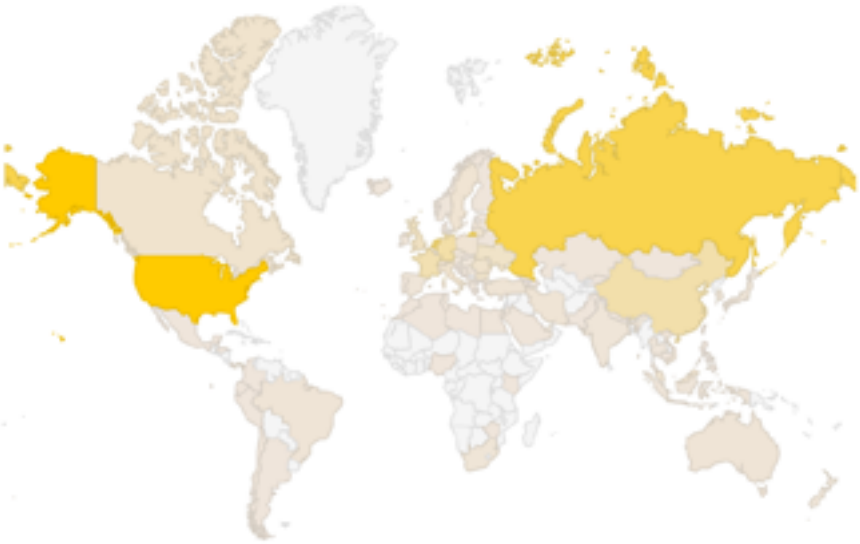
Rank	C&Cs 2017	C&Cs 2016	Network	Country
1	303	36	amazon.com	United States (US)
2	281	295	ovh.net	France (FR)
3	247	0	anmaxx.net	Seychelles (SC)
4	207	61	choopa.com	United States (US)
5	186	27	alibaba-inc.com	China (CN)
6	175	10	tencent.com	China (CN)
7	160	55	hostsailor.com	United Arab Emirates (AE)
8	147	49	worldstream.nl	Netherlands (NL)
9	128	56	digitalocean.com	United States (US)
10	112	72	quadranet.com	United States (US)
11	111	16	aruba.it	Italy (IT)
12	99	69	blazingfast.io	Ukraine (UA)
13	96	4	mtw.ru	Russia (RU)
14	88	53	leaseweb.com	Netherlands (NL)
15	87	32	iliad.fr	France (FR)
16	85	112	colocrossing.com	United States (US)
17	81	41	ghoster.com	Netherlands (NL)
18	81	23	host1plus.com	Great Britain (GB)
19	80	65	virpus.com	United States (US)
20	80	15	dataclub.biz	Belize (BZ)

Note that this table shows the raw number of botnet controllers on each network. It says nothing about how long each botnet controller was left active, or whether the provider heeded C&C reports from Spamhaus or not. In 2017, we have made the experience that hosting providers that are being misused by cybercriminals for botnet hosting for several years now in general swiftly respond to abuse complaints. Unlike most of the big cloud providers who apparently were overwhelmed by the huge amount of fraudulent sign ups hitting their service in 2017: Some of them do still need to spend much time to address and stop abuse being generated in their network.

Spamhaus BCL Statistics (continued)

Looking at the geographic location of the botnet controllers, the top botnet hosting country is the US, followed by Russia:

Botnet controller Geo location



Let us also have a look at what kind of malware was associated with the botnet controllers Spamhaus detected in 2017.
The table below shows the number of all botnet listings per malware family in 2017.

Rank	C&Cs	Malware	Note
1	1015	Downloader.Pony	Dropper / Credential Stealer
2	943	IoT malware	Generic IoT malware
3	933	Loki	Dropper / Credential Stealer
4	437	Chthonic	e-banking Trojan
5	389	Smoke Loader	Dropper / Credential Stealer
6	325	JBifrost	Remote Access Tool (RAT)
7	293	Cerber	Ransomware
8	281	Gozi	e-banking Trojan
9	264	Redosdru	Backdoor
10	258	Heodo	e-banking Trojan
11	258	Adwind	Remote Access Tool (RAT)
12	211	Glupteba	Spam bot
13	203	TrickBot	e-banking Trojan
14	175	Dridex	e-banking Trojan
15	168	Neutrino	DDoS bot / Credential Stealer
16	162	ISRStealer	Backdoor
17	148	Worm.Ramnit	e-banking Trojan
18	148	Hancitor	Dropper
19	132	AZORult	e-banking Trojan
20	131	PandaZeuS	e-banking Trojan

Spamhaus BCL Statistics (continued)

Comparing these numbers with those of 2016 leads us to some interesting findings:

- The number of IoT botnet controllers more than doubled from 393 in 2016 to 943 in 2017.
- While in 2014 a vast amount of the botnet controllers that Spamhaus identified were associated with ZeuS, 2017 was the first year were ZeuS did not made it into the top 20 malware families. It appears that the notorious ZeuS e-banking Trojan can be considered dead. Although, modern e-banking Trojans like Chthonic or PandaZeuS do still rely on the leaked source code of the original ZeuS.
- The Ransomware landscape is very dynamic: While Locky and TorrentLocker where omnipresent in 2016, those two ransomware families did not made it into the top 20 in 2017. They have been replaced by the Cerber ransomware.
- Java based malware families were flooding the web in 2017. These are usually some sort of remote access tools (RAT). One of the most popular ones in 2017 where JBifrost and Adwind.

Spamhaus DBL + Malware Domain List

To host their botnet controllers, cybercriminals usually prefer to use domain name that they register for exclusively that purpose. This is because a dedicated domain name allows the cybercriminal to fire up a new VPS, load the botnet controller kit, and immediately be back in contact with his botnet after his (former) hosting provider shuts down his botnet controller server. Not having to change the configuration of each infected computer (bot) on the botnet is a major advantage. Spamhaus therefore tracks both IP addresses and domain names that are used for C&C servers. IP addresses that host botnet controllers are listed in the Spamhaus SBL and/or BCL. Domain names that are used for botnet controller hosting are listed in the Spamhaus DBL or Malware Domain List, a sub-set of DBL that contains domain names used for botnet and malware hosting. It is not uncommon that cybercriminals use

Spamhaus DBL + Malware Domain List (continued)

a domain name generation algorithm (DGA) to make their botnet C&C infrastructure more resilient against takedown efforts and seizures conducted by law enforcement agencies or IT-security researchers.

In 2017, Spamhaus DBL listed almost 50,000 botnet controller domain names registered and set up by cybercriminals for the solely purpose of hosting a botnet controller. This excludes hijacked domain names (domains owned by non-cybercriminals that were used without permission) and domains on "free sub-domain" provider services.

There are many different top-level domains (TLDs), both generic TLDs (gTLDs) used by anybody, and country code TLDs (ccTLDs) that in many cases are restricted to use within a particular country or region (Many ccTLDs are licensed for general use and are therefore functionally equivalent to gTLDs). Let's have a look at which g/ccTLD cybercriminals chose most often for their botnet operations:

Rank	Domains	TLD	Note
1	14,218	com	gTLD
2	3,707	info	gTLD
3	3,546	top	gTLD
4	2,516	org	gTLD
5	1,607	net	gTLD
6	1,463	biz	gTLD
7	1,370	ru	ccTLD
8	1,256	click	gTLD
9	1,222	xyz	gTLD
10	848	eu	gTLD
11	729	space	gTLD
12	513	website	gTLD
13	465	us	ccTLD
14	420	work	gTLD
15	344	tw	ccTLD
16	290	online	gTLD
17	241	bid	gTLD
18	236	pro	gTLD
19	210	cc	originally ccTLD, now effectively gTLD
20	202	su	ccTLD

Spamhaus DBL + Malware Domain List (continued)

We have seen a vast amount of botnet controller domain names being registered in gTLD .com. When using domains in ccTLDs, cybercriminals choose .ru ccTLDs most often in 2017. TLDs do not have the same total numbers of registered domains. For example, the .com TLD has more than 100 million registered domains, while the .ru TLD has slightly fewer than six million. If we compare the total number of registered domain names in each TLD against the number of malicious domain names in that TLD seen by the DBL, the ccTLD .ru was the one that has been most heavily abused.

To get a (botnet) domain name registered, cybercriminals need to find a sponsoring registrar. The following table shows a list of domain registrars ranked by the total number of botnet controller domain names detected by Spamhaus DBL in 2017. Please consider that these are fraudulent domain name registrations only. More than 25% of all registered botnet domain names have been registered through **Namecheap**.

Rank	Domains	Registrar	Country
1	11,878	Namecheap	United States (US)
2	2,977	Eranet International	China (CN)
3	2,106	PDR	India (IN)
4	1,335	ENom	United States (US)
5	1,068	Shinjiru	Malaysia (MY)
6	856	Alibaba (aka HiChina/net.cn)	China (CN)
7	812	NameSilo	United States (US)
8	765	R01	Russia (RU)
9	606	Alpnames	Gibralta (GI)
10	494	RegRU	Russia (RU)
11	447	Bizcn	China (CN)
12	370	Gandi	France (FR)
13	303	Tucows	United States (US)
14	281	CentralNic	Great Britain (GB)
15	233	Xin Net	China (CN)
16	232	Ardis	Russia (RU)
17	212	NameBright (aka DropCatch)	United States (US)
18	191	Domain.com	United States (US)
19	176	Todaynic	China (CN)
20	155	WebNic.cc	Malaysia (MY)

Spamhaus DBL + Malware Domain List (continued)

As with ISPs that host botnet controllers, many of these registrars are simply large registrars. While the total numbers of botnet domains at the registrar might appear large, the registrar does not necessarily support cybercriminals. Registrars simply can't detect all fraudulent registrations or registrations of domains for criminal use before those domains go live. The "life span" of criminal domains on legitimate, well-run, registrars tends to be quite short.

However, other much smaller registrars that you might never have heard of (like Shinjiru or WebNic) appear on this same list. Several of these registrars have an extremely high proportion of cybercrime domains registered through them. Like ISPs with high numbers of botnet controllers, these registrars usually have no or limited abuse staff, poor abuse detection processes, and some either do not or cannot accept takedown requests except by a legal order from the local government or a local court. Since many cybercrime-friendly registrars are located in countries with no or slow legal recourse against cybercrime, obtaining a legal order can be difficult or impossible. Because cybercrime-registrars will not cooperate with law enforcement and other entities to shut down botnets, a botnet with C&C domains registered through such a registrar requires lengthy, coordinated, and extensive efforts to shut down. This normally works by involving the TLD or ccTLD's registry.

Meanwhile, innocent people are at risk of having online banking credentials compromised and bank accounts emptied, or other valuable information stolen for use in identity theft and fraud.

Conclusion

Looking forward to 2018, there is no sign that the number of cyber threats will decrease. The big increase of IoT threats in 2017 is very likely to continue in 2018. We are sure that securing and protecting IoT devices will be a core topic in 2018. Spamhaus products like the Botnet Controller List (BCL), Malware Domain List or Zero Reputation Domain (ZRD) can help you to protect not only your IoT devices but also spot potential intruders and infected machines in your network.

Cloud providers rotating botnet controllers around different IP addresses present a threat to Spamhaus users. We therefore hope that cloud hosting providers will speed up and increase their abuse desks to not only respond to abuse problems in time but also to take preventive measures to battle fraudulent sign ups. We also hope that hosting providers will educate abuse desk staff in order to deal with complex abuse problems in a more professional way and hence prevent that, for example, abuse problems on a compromised websites reappear by taking the appropriate measures (and not just by deleting the offensive content!).

Due to the increase of botnet controllers we recommend network owners to block traffic to anonymization services like Tor by default and provide users who want or need to access to services the possibility to “Opt-In”.

Speaking about domain names, we would like to see Registries and Registrars taking their responsibility by implementing appropriate mechanisms to prevent fraudulent domain registrations. For example, it is embarrassing that botnet operators are able to register DGA botnet controller domains under their account again and again while the sponsoring domain name registrar is not taking action against the offensive account.