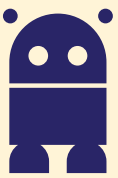
SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus
Botnet Threat Report 2019

Contents



Welcome to the Spamhaus Botnet Threat Report 2019. Last year the researchers at Spamhaus Malware Labs detected the highest number of botnet command & controllers (C&C) on record, observing more than 10,000 botnet C&Cs.

Spamhaus tracks both Internet Protocol (IP) addresses and domain names that are used for botnet C&C servers. This data enables us to identify the malware, location, hosting provider, domain name and registrar associated with the botnet C&C.

In this report, we highlight key trends from 2018 and provide insights as to what can be done to reduce global botnet C&C traffic, alongside giving recommendations as to what you and your teams can do to protect your business and users from these threats.

Number of botnet C&Cs observed in 2018

The research team at Spamhaus Malware Labs identified and blocked 10,263 malware botnet controllers (C&C) hosted on 1,121 different networks in 2018. That is an 8% increase from the number of botnet C&Cs seen in 2017.

To understand how 'popular' botnet C&Cs were as a cybercriminal's vector of choice throughout 2018 we reviewed the Spamhaus Block List (SBL), and examined how many listings were issued for botnet C&C traffic:

2018: 25% of all SBL listings

2017: 15% of all SBL listings

The 67% increase in botnet C&C listings on the SBL clearly illustrates that there was a shift from other threats. This indicates that cybercriminals had an increased focus on stealing credentials directly from the user, rather than purely phishing for them.

Botnet controllers – a brief explanation

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, ransomware, launch DDoS attacks, commit e-banking fraud, click-fraud or to mine cryptocurrencies such as Bitcoin.

Desktop computers and mobile devices, like smartphones, aren't the only machines which can become infected. There is an increasing number of devices which are connected to the internet, for example, the Internet of Things (IoT) devices, such as webcams, or network attached storage (NAS). These are also at risk of becoming infected.

Geolocation of botnet C&Cs in 2018

Despite the increase in the numbers of botnet C&Cs, their locations remained unchanged from 2017. The top botnet C&C hosting country was the US, followed by Russia and the Netherlands:

Rank	Botnet controllers	Country
1	2272	United States
2	1939	Russia
3	1080	Netherlands
4	457	Germany
5	350	France
6	305	Great Britain
7	265	Ukraine
8	233	Canada
9	21	Switzerland
10	177	Lithuania

Rank	Botnet controllers	Country
11	175	Bulgaria
12	173	Turkey
13	157	China
14	150	Chile
15	149	Romania
16	122	Singapore
17	101	Italy
18	99	Malaysia
19	95	South Africa
20	93	Poland

It is evident where the threats were coming from geographically, now let's take a look at what those threats were, i.e., what malware was connected with these botnet C&Cs.

Malware associated with botnet C&Cs in 2018

The threat landscape is always highly dynamic, and 2018 didn't disappoint. While some trends such as remote access tools (RATs) continued to gather momentum, additional ones started to rear their heads, such as CoinMiners.

Credential Stealers: As in 2017, credential stealers were still accounting for the most significant amount of botnet C&C traffic; however there were changes as to which were top of the leader board.

'Pony' held the #1 spot for 2 years, however in 2018 'Loki' took pole position, having more than doubled the number of unique botnet C&Cs associated with it.

Remote Access Tools (RATs): This type of malware saw a significant increase in 2018, in particular, a Java-based RAT, called JBifrost (aka Adwind).

Back in 2017, we reported that JBifrost was starting to flood the botnet landscape, however, in 2018 we witnessed an explosion in the number of unique botnet C&C listings associated with it. The sheer volume of these listings has placed JBifrost at #2 on our leader board.

CoinMiners: Making their first appearance in the Top 20 list last year were CoinMiners. These are malicious pieces of software that silently mine cryptocurrencies, such as Bitcoin and Monero, without the consent or approval of the user. In 2018, we identified 83 botnet C&Cs associated with CoinMiners. Please note the advice detailed later in this report in relation to 'mining pools,' which are used by cryptominers.

Ransomware & e-banking Trojans: Botnet C&Cs associated with both types of malware dropped significantly in 2018.

Malware families associated with 2018 botnet C&C listings

Rank	C&Cs	Malware	Note	% change
1	2,347	Lokibot	Credential Stealer	+151 ▲
2	1,300	JBifrost	Java based Remote Access Tool (RAT)	+300 ▲
3	955	Pony	Dropper/Credential Stealer	–6 ▼
4	915	AZORult	Credential Stealer	+593 ▲
5	686	Heodo/Emotet	Dropper/Backdoor	+166 ▲
6	413	Gozi ISFB	e-banking Trojan	+47 ▲
7	322	NanoCore	Remote Access Tool (RAT)	–
8	269	Smoke Loader	Dropper/Backdoor	–31 ▼
9	241	TrickBot	e-banking Trojan	+19 ▲
10	203	RemcosRAT	Remote Access Tool (RAT)	–
11	157	RedAlert	Android Trojan	–
12	122	NetWire	Remote Access Tool (RAT)	–
13	117	AgentTesla	KeyLogger/Remote Access Tool (RAT)	–
14	107	Chthonic	e-banking Trojan	–75 ▼
15	106	PandaZeuS	e-banking Trojan	–19 ▼
16	98	ImminentRat	Remote Access Tool (RAT)	–
17	96	Neurevt	e-banking Trojan	–
18	82	ISRStealer	Credential Stealer	–49 ▼
19	70	ArkeiStealer	Credential Stealer	–
20	51	NjRAT	Remote Access Tool (RAT)	–
–	89	CoinMiners malware	Various crypto currency miners	–
–	46	IoT malware	Various IoT malware	–95 ▼
–	456	Generic	*	–
–	1,015	Others	Other malware families	–

* C&Cs where the associated malware could not be identified

An understanding of the type of malware we need to protect ourselves from is helpful, but to get to the root of the problem, and stop the proliferation of botnet C&Cs, it's vital to understand which providers are supporting the infrastructure that is being used for botnet C&Cs.

We'll start by looking at the domains these botnet C&Cs were registered to, before moving onto the ISPs and hosting providers who were providing hosting capabilities to the cyber-criminals.

Number of botnet C&C domain names registered in 2018

Last year, compared to 2017, we saw a 100% increase in the number of the domain names registered and set up by cybercriminals for the sole purpose of hosting a botnet C&C:

2017: 50,000 domains

2018: 103,503 domains

N.B. These numbers exclude hijacked domain names; domains owned by non-cybercriminals that were used without permission, and domains on 'free sub-domain' provider services.

Most abused top-level domains in 2018

There were some interesting (and concerning) developments in this area, perhaps most notably was the rise of domain names being registered to '.bit,' a decentralized top-level domain (dTLD). Domain names with this type of top-level domain (TLD) create additional issues when it comes to blocking malicious traffic and taking down these bad operators.

Palau '.pw' was the most abused TLD: The listings associated with '.pw' rose by 56% in 2018, which was an additional 4,835 botnet C&Cs connected with this domain from the previous year.

Russia '.ru' had a reduced number of domain registrations for botnet C&Cs: We noted a small decrease from 1,370 domain listings in 2017 to 1,183 in 2018. This saw '.ru' ccTLD move out of the top ten rankings, down to #17.

Historically cybercriminals heavily abused '.ru' & '.su' ccTLDs, however, over recent years their operator has implemented measures which are having positive effects in reducing the amount of abuse across these 2 TLDs.

'.tk,' '.ml,' '.ga,' '.gg' and '.cf' make their first appearances in the Top 20: Originally ccTLDS these are now operated by Freenom and are considered to be gTLDs. As the name implies 'Freenom' provide domain names for free. Given this business model, it's not surprising that there has been a huge increase in abusive activity associated with them: Cybercriminals realize that their nefarious actions are likely to lead to their domain name being shut down, therefore prefer to obtain them for free rather than pay for them.

The importance of domain names

Cybercriminals prefer to use a domain name registered exclusively to host the botnet C&C.

A dedicated domain name allows them to fire up a new virtual private server (VPS), load the botnet C&C kit, and immediately be back in contact with their botnet after their (former) hosting provider shuts down their botnet C&C server. Not having to change the configuration of each infected computer (bot) on the botnet is a major advantage.

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

dTLD '.bit' had an upsurge in listings: This dTLD didn't make it into the 'Top 20' however we observed 108 domain names hosting botnet C&Cs with the dTLD '.bit.' dTLDs provide criminals with advantages over other TLDs and consequently pose additional threats to users; therefore we feel it is necessary to highlight them:

- These domain names cannot be taken down or suspended when being used for malicious purposes, because there is no governing body associated with a dTLD.
- dTLDs bypass DNS Firewalls/Response Policy Zones (RPZ) that numerous ISPs and businesses use to protect their customers/users from cyber threats. They by-pass DNS Firewalls because dTLD domains are not resolvable through common DNS and must be resolved through nameservers that support '.bit', such as OpenNIC. To protect against this kind of threat look to Border Gateway Protocol data feeds as an added layer of security.
- Researching malicious activity becomes more challenging as domain name registrations within dTLDs are usually completely anonymous, with registrant information not being required.

Domain name generation algorithm (DGA)

It is not uncommon that cybercriminals use a DGA to make their botnet C&C infrastructure more resilient against takedown efforts and seizures conducted by law enforcement agencies or IT-security researchers.

Top abused TLDs

Rank	Domains	TLD	Note
1	13,422	pw	ccTLD of Palau
2	11,815	com	gTLD
3	10,909	review	gTLD
4	9,399	top	gTLD
5	7,464	stream	gTLD
6	6,894	download	gTLD
7	5,983	tk	originally ccTLD, now effectively gTLD
8	5,704	xyz	gTLD
9	5,427	ml	originally ccTLD, now effectively gTLD
10	3,735	bid	gTLD
11	2,461	ga	originally ccTLD, now effectively gTLD
12	2,183	gq	originally ccTLD, now effectively gTLD
13	2,137	cf	originally ccTLD, now effectively gTLD
14	1,684	info	gTLD
15	1,504	sx	ccTLD of Sint Maarten
16	1,350	trade	gTLD
17	1,182	ru	ccTLD of Russia
18	1,081	science	gTLD
19	1,026	win	gTLD
20	650	club	gTLD

Having looked at the preferred TLDs cybercriminals use we investigated the registrars who were enabling them to get their botnet C&C domain names registered.

Most abused domain registrars in 2018

To get a botnet C&C domain name registered cybercriminals need to find a sponsoring registrar. In 2018, the top 3 registrars on our list were accountable for over 60% of the total number of botnet C&C domain names registered throughout the year.

Registrars can't easily detect all fraudulent registrations, or registrations of domains for criminal use before these domains go live. However, the 'life span' of criminal domains on legitimate, well-run, registrars tend to be quite short.

Namecheap was the most abused registrar: 21% of all botnet C&C domain names were registered through this US-based registrar, keeping it at the #1 spot it held in 2017. It is worth noting that 2018 saw a massive 220% increase in the number of botnet C&C domain names registered with Namecheap.

PDR took the #2 spot from Eranet International: The Indian based registrar PDR also had a huge rise in the number of domain registrations for botnet C&Cs in 2018; a whopping 530%!

New entries: Four out of the seven registrars who made a new appearance in 2018 were based in the United States: Network Solutions (aka web.com) US, Register.com US, Arsys ES, west263.com US, Gransy (aka suberg.cz) CZ, OnlineNIC US, RU-Center RU.

2017 entries no longer listed: It's good to see Shinjiru MY, Gandi FR, Domain.com US, Todaynic CN, and WebNic.CC MY drop off the list. We also note that Bizcn CN & Ardis RU are no longer listed, but from research, we believe this may be as a result of having stopped trading (for the time being at least).

Fraudulent domain name registrations

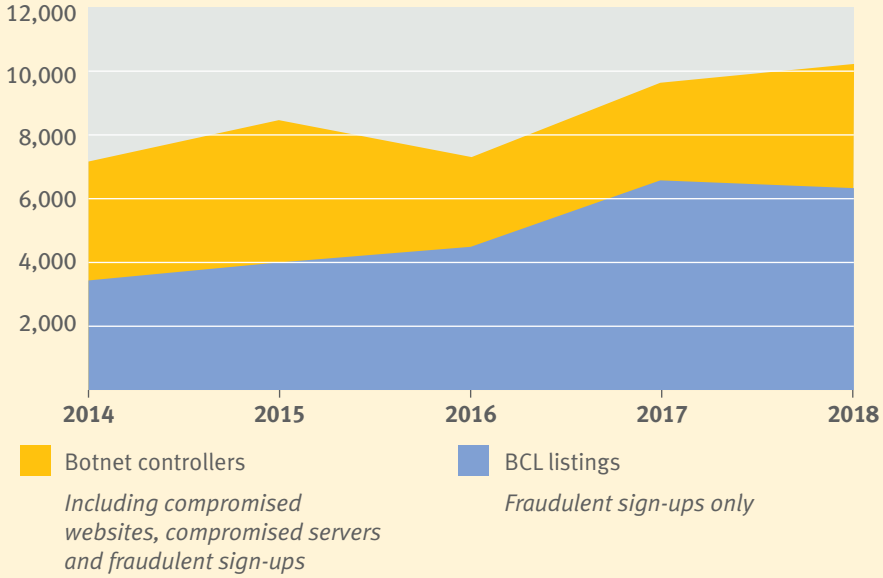
Rank	Domains	Registrar	Country
1	38,072	Namecheap	United States
2	13,261	PDR	India
3	3,322	Eranet International	China
4	1,448	RegRu	Russia
5	908	Alibaba (aka HiChina/net.cn)	China
6	764	NameSilo	United States
7	438	Network Solutions (aka web.com)	United States
8	378	ENom	United States
9	366	Xi Net	China
10	339	Register.com	United States
11	311	Arsys	Spain
12	309	CentralNic	Great Britain
13	291	west263.com	China
14	274	Tucows	United States
15	239	Gransy (aka subreg.cz)	Czech Republic
16	190	R01	Russia
17	175	NameBright (aka DropCatch)	United States
18	167	OnlineNIC	United States
19	159	RU-Center	Russia
20	158	Alpnames	Gibraltar

Fraudulent sign-ups with ISPs and hosting providers drives botnet traffic in 2018

Out of the botnet C&Cs Spamhaus observed 61% were as a result of fraudulent sign-ups, compared to 68% in 2017. While this points to a small increase in the number of botnet C&Cs that were hosted on compromised servers, or websites, it was evident that botnet operators were still predominantly relying on servers they own and operate.

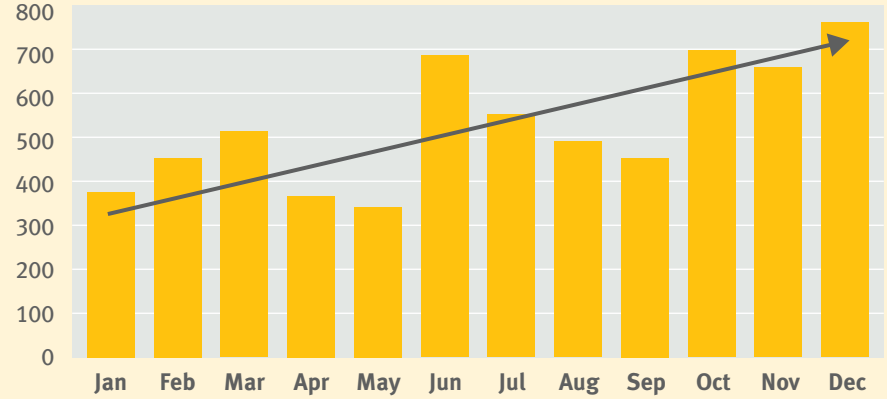
When a botnet C&C is noted to be the result of a fraudulent sign-up, it is subject to a listing on the Spamhaus Botnet C&C List (BCL). The graph below shows the overall number of botnet C&C listings versus the number of botnet C&C listings on the BCL between 2014–2018.

Total of newly detected botnet C&C listings vs newly detected BCL listings 2014–2018



In 2018, we averaged approximately 530 BCL listings per month, however, as the graph below illustrates there has been a notable increase from 376 listings at the beginning of the year in January to 762 at the end of the year in December.

Botnet controller listings per month



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 VPS or a dedicated server, for the sole purpose of using it for hosting a botnet C&C.

How to utilize the BCL

This is a 'drop all traffic' list intended for use by networks to null route traffic to and from botnet C&Cs. These IP addresses host no legitimate services or activities, so they can be directly blocked on both ISP and corporate networks without the risk of affecting legitimate traffic. Infected computers, that may be present on their networks, are effectively rendered harmless.

The dark side of the Internet

These statistics exclude botnet C&Cs hosted on the dark web (like Tor). The use of such anonymization networks by botnet operators started becoming more popular in 2016. This popularity is more than likely driven by the fact that the location of the botnet C&C is unidentifiable; making the takedown of a server almost impossible. This trend has continued into 2018. However, a vast amount of the botnet C&Cs detected by Spamhaus Malware Labs in 2018 were still hosted on the clear web.

For anonymization services like Tor, we recommend a whitelist approach: In general, block access to anonymization services except for those users who need it (opt-in).

Will this upward trend of fraudulent sign-ups driving botnet C&C traffic continue into 2019? We believe that by identifying the problem areas, i.e. the ISPs and hosting companies who have a large amount of botnet activity on their networks, it is possible to stem the increase.

ISPs that were hosting botnet C&Cs in 2018

Before we reveal which hosting ISPs had the largest number of botnet C&Cs on their networks in 2018 it is essential to understand some key points:

Preventing Botnet C&Cs on compromised servers or websites: It can be difficult for an ISP or hosting provider to do this since these are often under the control of the customer. Many servers and websites are running outdated software, which makes them vulnerable to attacks from the internet.

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 botnet C&C traffic. Of course, blocking traffic to known botnet C&Cs is a good start.

Preventing Botnet C&Cs on servers used solely for hosting a botnet C&C: ISPs have far more control in this situation since when a new customer tries to sign-up a customer verification/vetting process should take place before commissioning the service.

Where ISPs have a high number of BCL listings (botnet C&Cs hosted on servers solely for that purpose, i.e., a fraudulent sign-up) it highlights one of the following issues:

1. ISPs are not following the best practices for customer verification processes.
2. ISPs are not ensuring that ALL their resellers are following robust customer verification practices.
3. Employees or owners of ISPs are directly benefiting from fraudulent sign-ups, i.e. knowingly taking money from miscreants in return for hosting their botnet C&Cs.

The larger the ISP, the larger the volumes of abuse: while it may seem obvious it's important to remember that due to their increased hosting capabilities the bigger ISPs and hosting providers have a higher volume of poorly patched servers and websites on their network, that's if they are maintained at all.

Outdated software makes for an easy target

It is a simple task for a cybercriminal to scan the internet for servers or websites that are running outdated or vulnerable software. Some of the most popular open source content management systems (CMS) like WordPress, Joomla, Typo3 or Drupal are especially popular targets, due to the high number of poorly maintained installations of these packages.

Proxy nodes

Botnet operators not only use hosting providers and anonymization services to host their botnet infrastructure. Spamhaus Malware Labs has also seen an increase of malware-infected machines (bots) that cybercriminals turn into a proxy node.

In doing so, these bots become a part of the botnet infrastructure and are used to relay botnet C&C communications from other infected machines to the real botnet controller. While this is not a new technique that has appeared in 2018, malware families like Qadars, Quakbot, and others have been using this approach for several years; we have observed a substantial increase of Heodo / Emotet infected machines that have become a part of the Heodo / Emotet botnet infrastructure.

It is worth noting that if you think that your internet connection is suddenly running slower than expected, then your computer could potentially be infected and be acting as a proxy for a botnet operation.

Total botnet C&C hosting numbers by ISP

Including compromised websites, compromised servers and fraudulent sign-ups (BCL)

Rank	C&Cs 2017	C&Cs 2018	% change	Network	Country
1	100	704	+604 ▲	cloudflare.com	United States
2	14	603	+4,207 ▲	gerber-edv.net	Switzerland
3	256	431	+68 ▲	anmaxx.net	Russia
4	402	358	–11 ▼	ovh.net	France
5	95	274	+188 ▲	selectel.ru	Russia
6	197	185	–6 ▼	alibaba-inc.com	China
7	101	147	+46 ▲	iliad.fr	France
8	127	143	+13 ▲	mtw.ru	Russia
9	94	135	+44 ▲	godaddy.com	Unites States
=10	200	116	–42 ▼	hostsailor.com	United Arab Emirates
=10	37	116	+214 ▲	morene.host	Russia
11	105	115	+10 ▲	leaseweb.com	Netherlands
=12	112	111	–1 ▼	ispserver.com	Russia
=12	144	111	–23 ▼	timeweb.ru	Russia
13	179	110	–39 ▼	digitalocean.com	United States
14	1	107	+10,600 ▲	neohost.com.ua	Ukraine
15	39	97	+149 ▲	mchost.ru	Russia
16	0	91	—	melbicom.net	Russia
17	81	90	+11 ▲	dataclub.biz	Belize
18	231	86	–63 ▼	choopa.com	US
19	0	77	—	eksenbilisim.com.tr	Turkey
20	47	75	+60 ▲	swiftway.net	United Kingdom

Botnet C&C hosting numbers, by ISP, as a result of fraudulent sign-ups

Listings on the BCL

Rank	C&Cs 2017	C&Cs 2018	% change	Network	Country
1	100	704	+604 ▲	cloudflare.com	United States
2	14	603	+4,207 ▲	gerber-edv.net	Switzerland
3	273	431	+58 ▲	anmaxx.net	Russia
4	70	238	+240 ▲	selectel.ru	Russia
5	186	163	–12 ▼	alibaba-inc.com	China
6	87	138	+59 ▲	iliad.fr	France
7	36	113	+214 ▲	morene.host	Russia
8	1	92	+9,100 ▲	neohost.com.ua	Ukraine
9	88	86	–2 ▼	leaseweb.com	Netherlands
10	37	81	+119 ▲	mchost.ru	Russia
11	80	80	0	dataclub.biz	Belize
12	160	78	–51 ▼	hostsailor.com	United Arab Emirates
=13	0	77	– ▲	eksenbilisim.com.tr	Turkey
=13	96	77	–20 ▼	mtw.ru	Russia
14	128	75	–41 ▼	digitalocean.com	United States
15	207	87	–58 ▼	choopa.com	United States
16	0	69	– ▲	melbicom.net	Russia
17	66	67	+1 ▲	ispserver.com	Russia
18	4	66	+1,550 ▲	timeweb.ru	Russia
19	85	62	–27 ▼	colocrossing.com	United States
20	19	58	+205 ▲	zare.com	United Kingdom
=21	27	57	+111 ▲	swiftway.net	United Kingdom
=21	175	57	–67 ▼	tencent.com	China

Cloudflare was the top botnet C&C hosting network: Cloudflare is a Content Delivery Network (CDN) provider from the US. While they do not directly host any content, they provide services to botnet operators, masking the actual location of the botnet controller and protecting it from DDoS attacks.

Many cybercriminals sign-up for Cloudflare's free plan with the sole purpose of using it exclusively for hosting a botnet C&C. Usually such a listing would be placed on our BCL, however, because the hosting of the botnet C&C is on a Cloudflare shared IP address it is placed on the SBL. In this extraordinary circumstance, we have chosen to list the same figures in both charts.

Gerber-edv.net was the second worst botnet hosting provider: This Swiss ISPs listings were all on the BCL indicating that every listing was as a result of a fraudulent sign-up.

Some further research, which can be viewed here[1], reveals that gerber-edv.net is connected with anmaxx.net, which was the third most abused network for botnet hosting in 2018.

Additional ISPs with only BCL listings: anmaxx.net (RU) and eksenbilisim.com.tr (TR). We could not find a single compromised server or website on these networks that were abused for botnet C&C hosting.

New entries for 2018: The Turkish ISP eksenbilisim.com.tr and the Russian ISP melbicom.net made it onto the list in 2018. Having both had zero listings against their name in 2017 the amount of botnet activity on their networks last year saw a sizable increase to 77 and 69 botnet C&C listings respectively.

[1] https://abuse.ch/blog/anmaxx-gerber-edv-and-the-qrypter-connection/

Entries who dropped off the list for 2018: Congratulations to worldstream.nl, quadranet.com, aruba.it, blazingfast.io, qhoster.com, host1plus.com, virpus.com, hetzner.de, edurance.com, namecheap.com, who were all on the Top 20 list in 2017 but dropped off in 2018.

A particular mention needs to be made to Amazon, who were top of the BCL list in 2017, and have implemented appropriate processes and procedures to prevent cybercriminals from signing up for their services for botnet C&C hosting.

The East/West divide in cloud hosting: Hosting botnet C&Cs in the Cloud was a big trend in 2017, as you can read about here[2]. After the rise of botnet C&Cs in the Cloud in 2017, we saw a significant decrease in 2018, as Amazon's departure from the listings proves. However, there was a big difference between Cloud providers in the western world and those from the far east, especially China. Chinese Cloud providers like Tencent and Alibaba continued to have issues with finding a way to battle fraudulent sign-ups. Both, Tencent and Alibaba, were hosting a significant amount of botnet C&Cs in 2018, as our charts above demonstrate.

Conclusion

In such a fluid environment, with new threats quickly appearing while others are fading away, it is challenging to forecast developments for 2019. However, based on our findings we believe these are critical areas for concern:

Rise in threats from CoinMiners & CoinStealers: Despite the exchange rate of cryptocurrencies like Bitcoin having dropped significantly in 2018, we believe that we will continue to see a rise in CoinMiners and CoinStealers in 2019.

One of the reasons behind this is due to the anonymity and decentralization that certain cryptocurrencies like Monero offer. Although the value of Bitcoins haven't hugely increased since 2017, they continue to provide an easy, anonymous and reliable way to generate a monthly income for cybercriminals.

Decentralized TLDs: In 2019, we anticipate an increase in the number of registered botnet C&C domain names within decentralized TLDs (dTLDs) such as .bit (Namecoin), making it more difficult for ISPs, security researchers and the industry to protect their users from cyber threats.

Increased use of anonymization services for botnet C&C infrastructure: The trend that we started to see in 2017, as detailed here[3], whereby botnet C&C infrastructure is moving from the clear web to anonymization services like Tor continued. Once again in 2018, we identified an increase, which in turn, makes the job of detecting and blocking botnet C&C traffic on networks more difficult for ISPs and network owners.

Below are issues that cause concern in relation to providers that host botnet C&Cs:

Inadequate verification processes of hosting providers & resellers: To battle botnets, hosting providers must have adequate customer verification/vetting processes. This is not something new. We have been attempting to convince hosting providers towards such standards since 2012 as outlined here[4].

Issues with mining pools

In 2018, we not only witnessed a considerable increase of CoinMiner botnet C&Cs, but we also issued 156 SBL listings for 111 cryptocurrency mining pools that were used by the CoinMiners. Some of these cryptocurrency mining pools appeared to be rogue; however, the majority were legitimate pools that were being abused by CoinMiners.

We tried to approach the responsible hosting providers, asking them to have the offending user(s) of the mining pool suspended, to stop the fraudulent activity. Unfortunately, this was not always possible because some cryptocurrencies, such as Monero, are entirely anonymous, unlike Bitcoin.

Due to emerging threats originating from CoinMiners, we recommend a whitelist approach when dealing with this area: In general, block access to cryptocurrency mining pools except for those users who need it (opt-in).

[2] https://www.spamhaus.org/news/article/736/botnet-controllers-in-the-cloud
[3] https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017
[4] https://www.spamhaus.org/news/article/687/how-hosting-providers-can-battle-fraudulent-sign-ups

While many hosting providers implement appropriate processes and procedures, they don't always enforce these mechanisms with all of their resellers. This provides cybercriminals with a loophole, i.e. they sign-up for a VPS with a hosting provider's reseller, where there's a much greater chance of getting access to the service due to the reseller's lax verification/vetting procedures.

We would like to see customer verification and vetting processes enforced across all resellers. In addition, resellers who are lacking in such procedures, and consequently become the culprit for an increase in botnet C&C abuse, should be sanctioned accordingly.

Inadequate verification processes for Cloud hosting providers: Customer verification is not only a topic related to traditional hosting providers. We have observed Cloud providers in China, and CDN providers like Cloudflare, having problems with filtering out fraudulent sign-ups from the real ones. These issues lead to an increase in the number of botnet C&Cs hosted on such services. Providers should implement and follow a thorough customer verification/vetting process and become increasingly proactive in fighting abuse on their network.

Slow reaction time frames of hosting providers: Unlike others[5], Spamhaus does not publish any statistics on the reaction time of ISP abuse desks. However, we can divulge that at the date of writing this report, it is still possible for cybercriminals to host their botnet C&Cs at Cloud providers like Google, Tencent and Alibaba for weeks, if not even months, before their abuse desks 'pull the plug'.

Over the past 20 years, Spamhaus has attempted to convince network operators to deal with abuse reports promptly. We hope that there will soon come a time, particularly with the big players in the hosting business, that we no longer have to do this.

Recommended precautionary actions

In such a rapidly changing environment a flexible and swift (if not automated) approach is required by those who protect networks and users. In addition to current security measures you currently have implemented, based on the botnet C&C threats observed in 2018, we recommend the additional following precautionary actions:

- Block access to cryptocurrency mining pools by default, and provide users who require access with the ability to 'opt-in.'
- Block traffic to anonymization services like Tor by default, and provide users who require access with the ability to 'opt-in.'
- To combat threats from botnet C&Cs utilizing dTLDs look to Border Gateway Protocol data feeds, automatically blocking connections to IP addresses associated with botnet C&Cs.
- To avoid your website being hacked by cybercriminals to host a botnet C&C, always ensure the installed CMS, such as WordPress or Typo3, including any installed 3rd party plugins, are up-to-date.
- If you operate a server, ensure that your operating system (OS) is up to date and any installed software such as Apache2 or PHP are running with the latest security patches.
- Avoid your server being one of the many that are comprised on a daily basis as a result of brute force or stolen SSH passwords. Use SSH key authentication whenever possible or deploy two-factor authentication (2FA).

GDPR and WHOIS data

No report covering 2018 would be complete without mentioning the General Data Protection Regulation (GDPR). As outlined in this article here, the new legislation has led to limitations on the information that domain registrars are disclosing. There are a number of disadvantages this has brought about for security and anti-abuse researchers across the globe:

1. Data that listed historically on WHOIS, prior to GDPR, could be used as an indicator that someone with less than honorable intentions owned a domain. Losing access to this data means that we have lost a way to determine 'badness,' along with the ability to easily attribute a domain to a malware operation.
2. It has become more challenging to distinguish which domains are owned by the 'good' guys, e.g., security researchers, who are creating sink-holes for this botnet traffic. This has the potential to skew some registrar/registry figures.
3. Due to the anonymity of domain owner information, when security researchers and anti-abuse researchers discover phishing sites, they are no longer able to contact the relevant domain owner to advise them of the fact.

We hope that this data will be made available to those who are focused on keeping the internet a safer place.

[5] https://urlhaus.abuse.ch/statistics/reactiontime/

About Spamhaus

The Spamhaus Project is an international nonprofit organization whose mission is to track the Internet's spam operations, to provide dependable real-time anti-abuse protection & threat-intelligence for Internet networks and to work with Law Enforcement Agencies to identify and pursue cybercriminals worldwide. The number of internet users mailboxes that are currently protected by Spamhaus DNSBLs now exceeds 3 billion. Founded in 1998, Spamhaus is based in Geneva, Switzerland and London, UK and is run by a dedicated team of investigators and forensics specialists located across the globe.

www.spamhaus.org

@spamhaus

SPAMHAUS

THE SPAMHAUS PROJECT