Spamhaus
Botnet Summary 2016

SPAMHAUS
THE SPAMHAUS PROJECT

2016 was a busy year for existing and emerging cyber threats. In the past year, Spamhaus researchers issued listings for over 7,000 botnet Command & Control ('C&C') servers on more than 1,100 different networks. These C&C servers enabled and controlled online crime such as credential theft, e-banking fraud, spam and DDoS attacks. They were also used for the retrieval of stolen data.

2016 will also go down in history as the first year that security issues related to the 'Internet of Things' (IoT) not only became mainstream, but turned into a serious enabler of ever larger attacks and a source of many future problems.

In 2016, one out of five SBL listings was for a botnet C&C server. Such servers are used by cyber criminals to control infected computers ('bots') and to retrieve stolen data from them. While 7,314 is a very high number of C&C servers, it is however a decrease of 1,166 (or 13.8%) in botnet controllers from the number we detected in 2015.

The majority (4,481 or 61.3%) of botnet controllers Spamhaus found in 2016 were hosted on servers that had been ordered by cyber criminals for the exclusive purpose of hosting a botnet controller (so called fraudulent sign-ups). This is an increase of 472 (or 11.8%) compared to 2015 and a new development that emerged in 2015, where the majority of newly detected botnet controllers moved from compromised websites to servers specifically ordered by cyber criminals for hosting botnet C&Cs.

All botnet C&C IP addresses detected were automatically listed on the Spamhaus Botnet Controller List (BCL), a specialized 'drop all traffic' list intended for use by networks to null traffic to and from botnet controllers. The Spamhaus BCL only lists IP addresses of servers set up and operated by cyber criminals for the exclusive purpose of hosting a botnet controller. 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.

As we show here, during 2016, the numbers of server-hosted botnet controllers decreased. One of the reasons for this is the increased use of anonymization networks ('dark web') by miscreants to cover the real location of their botnet controllers. In particular, the use of Tor by cyber criminals has vastly increased in the past year. Due to the nature of such anonymization networks, it is impossible to easily block certain content hosted in the dark web (e.g. botnet controllers), nor to identify the final target of a C&C communication (e.g. where the malware is sending the stolen data, such as credentials or credit card details). From the perspective of a network operator, the only way to prevent abuse from anonymization networks is to block them entirely (which can be a difficult choice as there are also legitimate uses for them). We believe that ISPs and hosting providers will be confronted in the near future with the question of whether to allow the use of anonymization services such as Tor or to block them completely, unless operators of anonymization services step up to stop abusers in a more effective way.

For botnet controllers that were not behind an anonymization network, we produced some statistics. The following table shows a list of ISPs ranked by number of C&Cs detected on that ISP's network during the past year, and also includes 2015 data to observe trends. These data include botnet controllers that were hosted on compromised webservers or websites, as well as those hosted through fraudulent sign-ups (BCL listings).

Botnet listings total (BCL + compromised)

Year	Listings
2016	7,314
2015	8,480
2014	7,182

Pure BCL listings

Year	Listings
2016	4,481
2015	4,009
2014	3,425

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

Rank	C&Cs 2016	C&Cs 2015	Network	Country
1	395	385	ovh.net	FR France (FR)
2	257	143	godaddy.com	US United States (US)
3	167	183	endurance.com	US United States (US)
4	144	197	hetzner.de	DE Germany (DE)
5	128	170	ispserver.com	RU Russia (RU)
6	118	106	colocrossing.com	US United States (US)
7	98	172	cloudflare.com	US United States (US)
8	89	50	quadranet.com	US United States (US)
9	83	73	digitalocean.com	US United States (US)
10	75	121	worldstream.nl	NL Netherlands (NL)
11	71	26	blazingfast.io	UA Ukraine (UA)
12	71	89	choopa.com	US United States (US)
13	69	3	chinanet-js	CN China (CN)
14	69	108	softlayer.com	US United States (US)
15	68	126	heg.com	GB Great Britain (GB)
16	68	103	itl.ua	UA Ukraine (UA)
17	68	6	virpus.com	US United States (US)
18	66	137	leaseweb.com	NL Netherlands (NL)
19	65	24	timeweb.ru	RU Russia (RU)
20	65	46	uk2group.com	FR Great Britain (GB)

Botnet hosting

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 these 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 therefore vulnerable to attacks from the internet. It is an easy task for a cyber criminal to scan the internet for servers or websites that are running outdated or vulnerable software. Some of the most popular open source CMSes like WordPress, Joomla, Typo3 or Drupal are especially popular targets, due to 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.

However, compromised servers and websites are just part of the problem. The other part of the ongoing botnet problem are the fraudulent sign-ups. 'Fraudulent sign-ups' are generally when a miscreant orders a server (e.g. VPS) at a hosting provider that is intended for the exclusive purpose of hosting a botnet controller. This means that the host running at such an IP address is not compromised; it is operated by cyber criminals. To ensure they are not traceable, cyber criminals use fake or stolen identities to place orders with service providers. Services are paid for using either stolen credit cards, compromised PayPal accounts or (anonymous) crypto-currency such as Bitcoin. Providers can battle such fraudulent sign-ups by doing proper customer verification. However, it is not unusual that a fraudulent sign-up can slip through the anti-fraud checks.

Command-and-Control servers

Note that this table shows the raw number of C&Cs on each provider. It says nothing about how long each botnet C&C was left active, or whether the provider heeded C&C reports from Spamhaus or not. In many cases, the volume of abuse originating from a provider is proportional to the size of the ISP or hosting provider's network and the number of customers.

However, the table also contains a few smaller providers that you may never have heard of, but that have hosted disproportionately large numbers of C&Cs. These providers attract more cyber criminals than other providers. Why? There are several reasons that this may happen:

Employing the automated sign-up of new customers that skips or has inadequate fraud checking in place, thus allowing cyber criminals to set up C&Cs quickly.

Inadequately staffed abuse departments and/or lax abuse handling processes can allow cyber criminals to continue to operate for relatively long periods of time before their C&Cs are shut down.

The provider's datacenter might be located in a legal jurisdiction, province, or country that lacks sufficient resources to investigate and prosecute cyber crime, or that even actively encourages it.

Rank	C&Cs 2016	C&Cs 2015	Network	Country
1	295	247	ovh.net	FR France (FR)
2	112	82	colocrossing.com	US United States (US)
3	109	153	ispserver.com	RU Russia (RU)
4	79	119	hetzner.de	DE Germany (DE)
5	72	45	quadranet.com	US United States (US)
6	69	24	blazingfast.io	UA Ukraine (UA)
7	68	3	chinanet-js	CN China (CN)
8	66	88	itl.ua	UA Ukraine (UA)
9	65	5	virpus.com	US United States (US)
10	64	106	worldstream.nl	NL Netherlands (NL)
11	61	67	choopa.com	US United States (US)
12	57	51	hostkey.ru	RU Russia (RU)
13	56	51	digitalocean.com	US United States (US)
14	55	110	hostsailor.com	AE United Arab Emirates (AE)
15	53	66	leaseweb.com	NL Netherlands (NL)
16	49	64	heg.com	FR Great Britain (GB)
17	49	45	severius.nl	NL Netherlands (NL)
18	49	11	zomro.com	UA Ukraine (UA)
19	43	38	selectel.ru	RU Russia (RU)
20	41	33	qhoster.com	NL Netherlands (NL)

Malware

Let us also have a look at what kind of malware was associated with the botnet controllers Spamhaus detected in 2016. The table above shows the number of all botnet listings per malware family in 2016.

It is fair to say that 2016 was the year of extortion. While many of the listings were related to ebanking Trojans, a new threat grew very quickly in 2016: Ransomware. The number of listings concerning Ransomware (such as TorrentLocker, Locky or Cerber) increased on an unprecedented scale in 2016.

In the autumn of 2016 Spamhaus also began listing botnet controllers associated with malware specifically targeting the 'Internet of Things'. Within just two months Spamhaus researchers identified, blocklisted and helped dismantle almost 400 IoT malware botnet controllers. We will soon publish a separate article detailing the specific challenges of IoT bots.

Botnet listings per malware family in 2016

Rank	C&Cs	Malware	Notes
1	602	Downloader.Pony	Dropper/ Credential Stealer
2	404	Locky	Ransomware
3	393	IoT	Generic IoT malware
4	305	CryptoWall	Ransomware
5	282	VMZeuS	e-banking Trojan
6	271	Gozi	e-banking Trojan
7	263	Dridex	e-banking Trojan
8	253	TeslaCrypt	Ransomware
9	229	Neurevt	Backdoor
10	213	ISRStealer	Backdoor
11	210	Nitol	DDoS bot
12	203	Citadel	e-banking Trojan
13	201	Vawtrak	e-banking Trojan
14	200	TorrentLocker	Ransomware
15	193	LuminosityLink	Remote Access Tool (RAT)
16	178	ZeuS	e-banking Trojan
17	157	Gootkit	e-banking Trojan
18	124	Smoke Loader	Dropper/Credential Stealer
19	120	Glupteba	Spam bot
20	103	Neutrino	DDoS bot/Credential Stealer
n/a	2,411	other	Other malware families
n/a	552	generic	C&Cs where the associated malware could not be identified

Contact details

Organization Admin and Industry Liaison

Organization enquiries and LEA/CERT contacts
Email: **cert-admin-ch@spamhaus.org**

www.spamhaus.org

SPAMHAUS
THE SPAMHAUS PROJECT