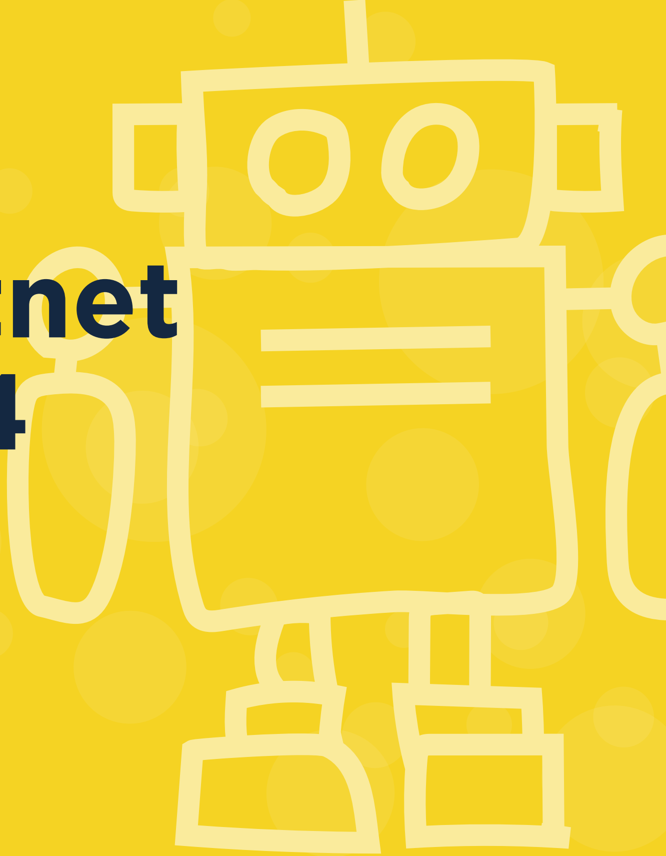
Spamhaus Botnet Summary 2014



As 2014 ends, Spamhaus reviews the botnet threats that it detected in the past year, and provides facts and useful suggestions for ISPs and web hosts on the front lines of the battle against cybercrime. To nobody's surprise, botnet activity appears to be increasing. The majority of detected botnets are targeted at obtaining and exploiting banking and financial information. Botnet controllers (C&Cs) are hosted disproportionately on ISPs with understaffed abuse departments, inadequate abuse policies, or inefficient abuse detection and shutdown processes. Botnet C&C domains are registered disproportionately with registrars in locations that have lax laws or inadequate enforcement against cybercrime.

About this report

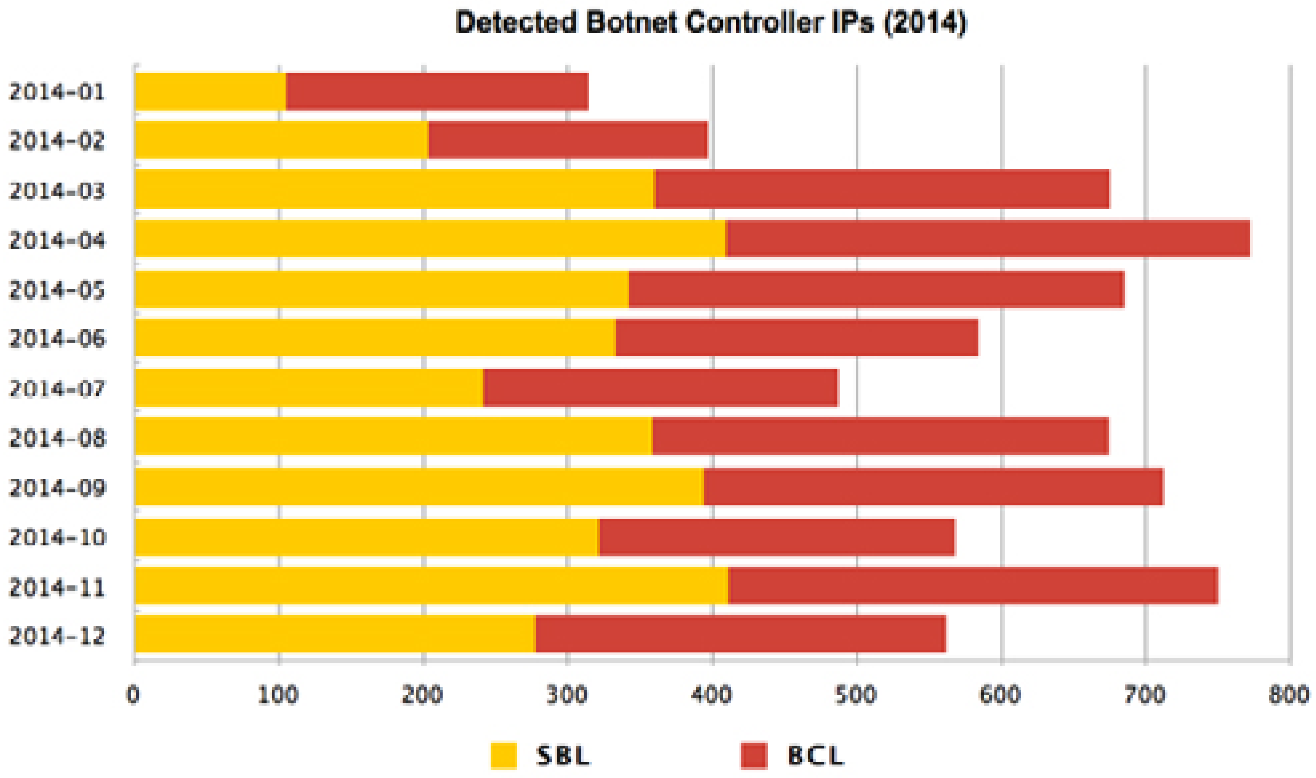
Spamhaus tracks both Internet Protocol (IP) addresses and domain names used by threat actors for hosting botnet command & control (C&C) servers. This data enables us to identify associated elements, including the geolocation of the botnet C&Cs, the malware associated with them, the top-level domains 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 BCL Statistics

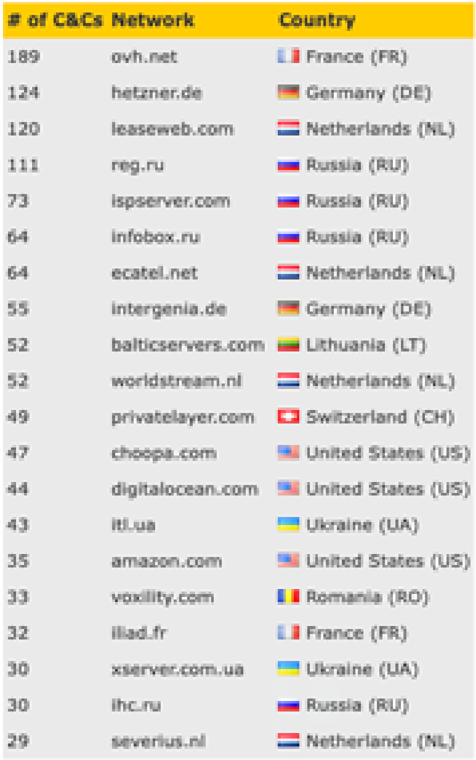
In 2014, Spamhaus detected **7,182** distinct IP addresses that hosted a botnet controller (Command & Control server - C&C). That is an increase of 525 (or **7.88%**) botnet controllers over the number we detected in 2013. Those C&Cs were hosted on **1,183** different networks.

While most of these botnet controllers were hosted on compromised webservers, **3,425** (48%) met the listing criteria for the Spamhaus Botnet Controller List (BCL) and made it onto this C&C-specific realtime data zone we provide. The BCL contains IP addresses of servers that were set up and operated by cybercriminals for the exclusive purpose of hosting a botnet controller. Because these IP addresses host no legitimate services or activities, they can be blocked (blackholed) on an ISP's or company's network without the fear of affecting legitimate traffic. IP addresses of servers that hosted other, non-botnet services (and therefore did not meet the listing criteria of BCL) were listed on the Spamhaus SBL.



Spamhaus BCL Statistics (continued)

Where were the botnet controllers hosted in 2014? The following table shows a list of ISPs ranked by number of C&Cs detected on that ISP's network during the past year.



# of C&Cs	Network	Country
189	ovh.net	France (FR)
124	hetzner.de	Germany (DE)
120	leaseweb.com	Netherlands (NL)
111	reg.ru	Russia (RU)
73	ispserver.com	Russia (RU)
64	infobox.ru	Russia (RU)
64	ecatel.net	Netherlands (NL)
55	intergenia.de	Germany (DE)
52	balticservers.com	Lithuania (LT)
52	worldstream.nl	Netherlands (NL)
49	privatelayer.com	Switzerland (CH)
47	choopa.com	United States (US)
44	digitalocean.com	United States (US)
43	itl.ua	Ukraine (UA)
35	amazon.com	United States (US)
33	voxility.com	Romania (RO)
32	iliad.fr	France (FR)
30	xserver.com.ua	Ukraine (UA)
30	ihc.ru	Russia (RU)
29	severius.nl	Netherlands (NL)

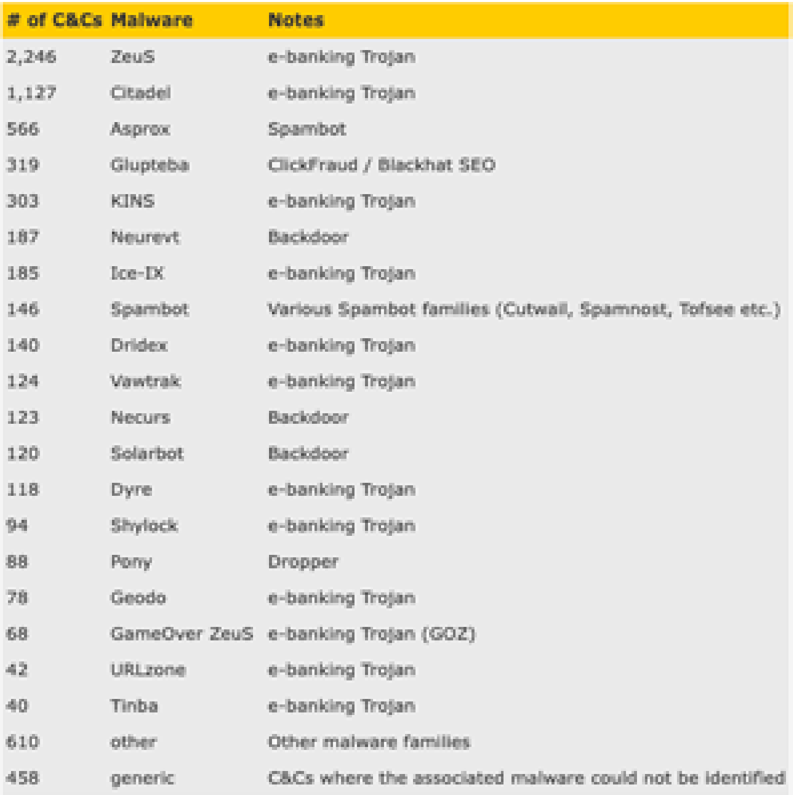
Keep in mind that this table shows the raw number of C&Cs on each ISP. The table says nothing about how long each botnet C&C was left active, or whether the ISP heeded C&C takedown requests from Spamhaus or not. In many cases, the volume of abuse originating from an ISP is proportional to the size of the ISP's network and the number of that ISP's customers.

However, the table also contains a few smaller ISPs that you might not have heard of before, but that have hosted proportionately large numbers of C&Cs. These ISPs attract more cybercriminals than other ISPs. There are several reasons that an ISP might attract disproportionate numbers of cybercriminals as customers. First, automated signup of new customers that skips or has inadequate vetting processes allows cybercriminals to set up C&Cs quickly. (See How hosting providers can battle fraudulent sign-up for information on setting up vetting.) Second, inadequately staffed abuse departments and/or lax abuse handling processes can allow cybercriminals to continue to operate for relatively long

Spamhaus BCL Statistics
(continued)

periods of time before their C&Cs are shut down. Third, the ISP’s datacenter might be located in a legal jurisdiction (province or country) that lacks sufficient resources to investigate and prosecute cybercrime, or even that actively encourages it. Geolocation is important to botnet operators, who prefer to host their C&Cs outside the jurisdiction of law enforcement agencies that actively prosecute cybercrime.

Let’s turn our attention from individual botnet controllers to malware families - types of botnet that use similar or the same malware code. The following table shows each malware family that we detect ranked by number of detected botnet C&Cs in that malware family.



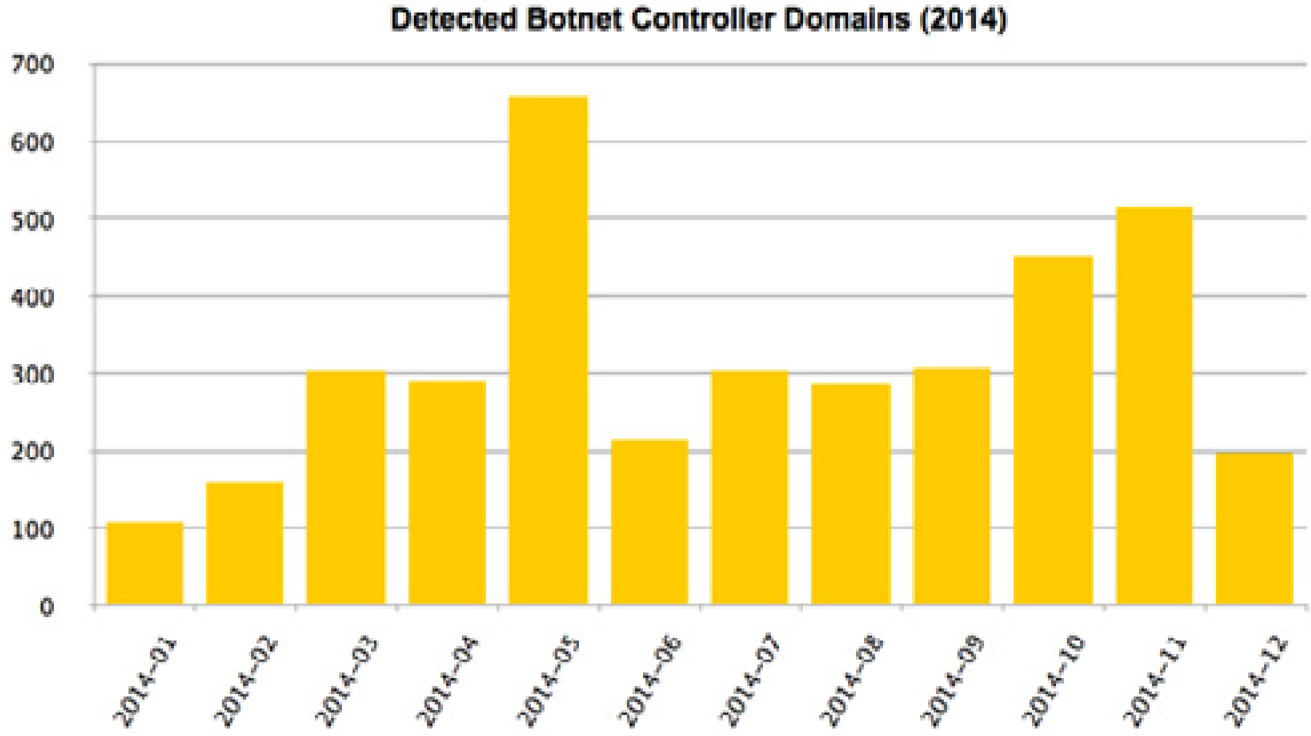
# of C&Cs	Malware	Notes
2,246	ZeuS	e-banking Trojan
1,127	Citadel	e-banking Trojan
566	Asprox	Spambot
319	Glupteba	ClickFraud / Blackhat SEO
303	KINS	e-banking Trojan
187	Neurevt	Backdoor
185	Ice-IX	e-banking Trojan
146	Spambot	Various Spambot families (Cutwail, Spamnost, Tofsee etc.)
140	Dridex	e-banking Trojan
124	Vawtrak	e-banking Trojan
123	Necurs	Backdoor
120	Solarbot	Backdoor
118	Dyre	e-banking Trojan
94	Shylock	e-banking Trojan
88	Pony	Dropper
78	Geodo	e-banking Trojan
68	GameOver ZeuS	e-banking Trojan (GOZ)
42	URLzone	e-banking Trojan
40	Tinba	e-banking Trojan
610	other	Other malware families
458	generic	C&Cs where the associated malware could not be identified

ZeuS and other malware families that are based on the leaked source code of the ZeuS kit (such as Citadel, KINS and Ice-IX) are associated with most of the detected botnet controllers. In addition, most of detected malware families are electronic banking (e-banking) trojans used to commit financial fraud.

Spamhaus DBL Statistics

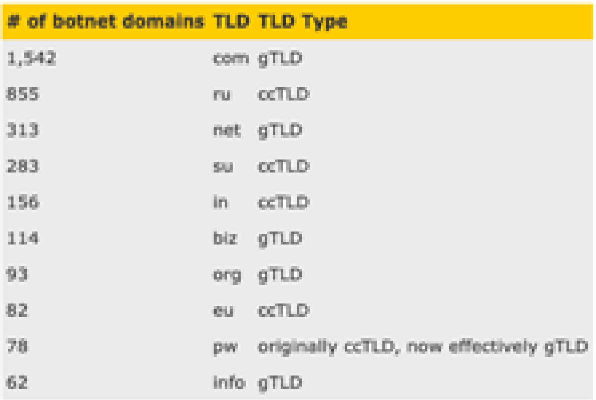
To host their botnet controllers, cybercriminals usually prefer to use their own domain names, as opposed to an ISP domain name and path or a bare IP address. Using a dedicated domain name allows the cybercriminal to fire up a new VPS, load the botnet controller kit, and immediately be back in contact 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.

In 2014, Spamhaus DBL listed **3,793** botnet C&C domains that were registered and set up by cybercriminals for the exclusive purpose of hosting a botnet controller. This list excludes hijacked domain names (domains owned by non-cybercriminals that were used without permission) and domains on “free sub-domain” provider services.



Spamhaus DBL Statistics
(continued)

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:

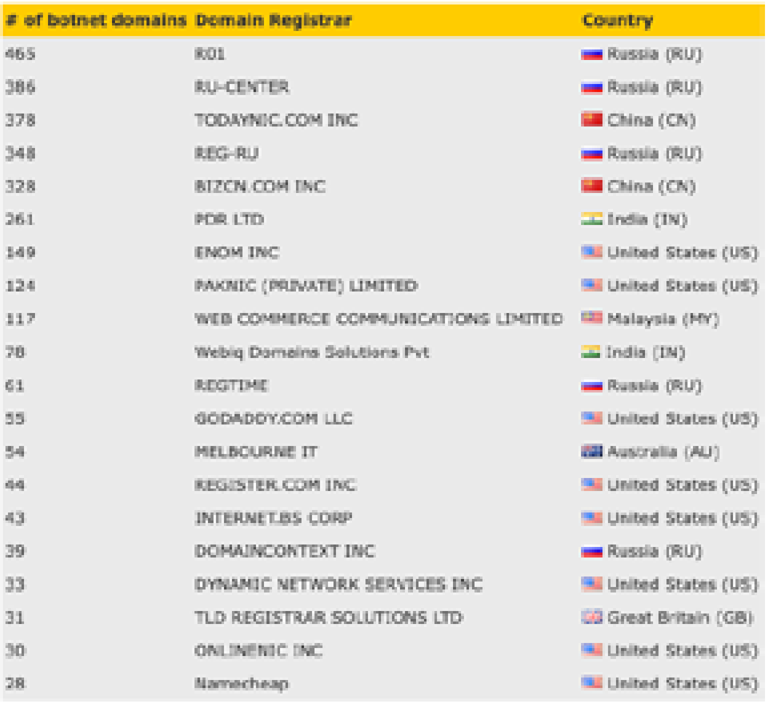


# of botnet domains	TLD	TLD Type
1,542	com	gTLD
855	ru	ccTLD
313	net	gTLD
283	su	ccTLD
156	in	ccTLD
114	biz	gTLD
93	org	gTLD
82	eu	ccTLD
78	pw	originally ccTLD, now effectively gTLD
62	info	gTLD

The table above shows that cybercriminals most often used domains in the com and net gTLDs for botnet hosting in 2014. When using domains in ccTLDs, cybercriminals chose the ru and su ccTLDs most often in 2014. TLDs do not have the same total numbers of registered domains, however. For example, the com TLD has more than 100 million registered domains, while the ru TLD has slightly fewer than five 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 DBL, the two ccTLDs ru and su were those that have been most heavily abused.

Let’s now look at the sponsoring domain registrars favoured by cybercriminals for registering botnet controller domains in 2014. The following table shows a list of domain registrars ranked by the total number of botnet controller domains detected by Spamhaus DBL in 2014.

Spamhaus DBL Statistics
(continued)



# of botnet domains	Domain Registrar	Country
465	R01	Russia (RU)
386	RU-CENTER	Russia (RU)
378	TODAYNIC.COM INC	China (CN)
348	REG-RU	Russia (RU)
328	BIZCN.COM INC	China (CN)
261	PDR LTD	India (IN)
149	ENOM INC	United States (US)
124	PAKNIC (PRIVATE) LIMITED	United States (US)
117	WEB COMMERCE COMMUNICATIONS LIMITED	Malaysia (MY)
78	Webiq Domains Solutions Pvt	India (IN)
61	REGTIME	Russia (RU)
55	GODADDY.COM LLC	United States (US)
54	MELBOURNE IT	Australia (AU)
44	REGISTER.COM INC	United States (US)
43	INTERNET.BS CORP	United States (US)
39	DOMAINCONTEXT INC	Russia (RU)
33	DYNAMIC NETWORK SERVICES INC	United States (US)
31	TLD REGISTRAR SOLUTIONS LTD	Great Britain (GB)
30	ONLINENIC INC	United States (US)
28	Namecheap	United States (US)

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 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

Spamhaus DBL Statistics (continued)

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 2015 there are no signs there will be a decrease in botnet activity. Because techniques used by criminals online are always changing, it is best to use a multi-layered defense, which should include keeping users away from dangerous resources such as the ones described above. Spamhaus will continue working to protect internet users worldwide and continue helping networks and registrars to keep their assets clean.

Have a safe 2015!