

Threat Report 2018



Deteque is a division of Spamhaus and integrated with a global network of service providers and a community of researchers who have been dedicated to combating DNS abuse since 2008. Each year the research team at Spamhaus’ Malware Labs publishes its findings and this Report builds on the threat landscape of 2017 with latest figures from 2018 to date.

A key malicious actor tracked is the botnet controller, commonly abbreviated as ‘C&C’, used by fraudsters to both control malware infected machines and to extract personal and valuable data from malware infected victims. Spamhaus’ Malware Labs identified 9,500 botnet Command & Control servers on 1,122 different networks in 2017.

Botnet controllers therefore play a core role in operations conducted by cyber criminals 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 Internet of Things (IoT) device such as a webcam or network attached storage (NAS) that is connected to the internet.

Botnet Controllers

The number of 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 cyber criminals for the sole purpose of hosting a botnet controller. Of course, cyber criminals 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, an entry is created into our BotnetCC threat intelligence feed.

The BotnetCC – which stands for Botnet Command and Controller – is a ‘drop all traffic’

list intended for use by networks to block queries to botnet controllers.

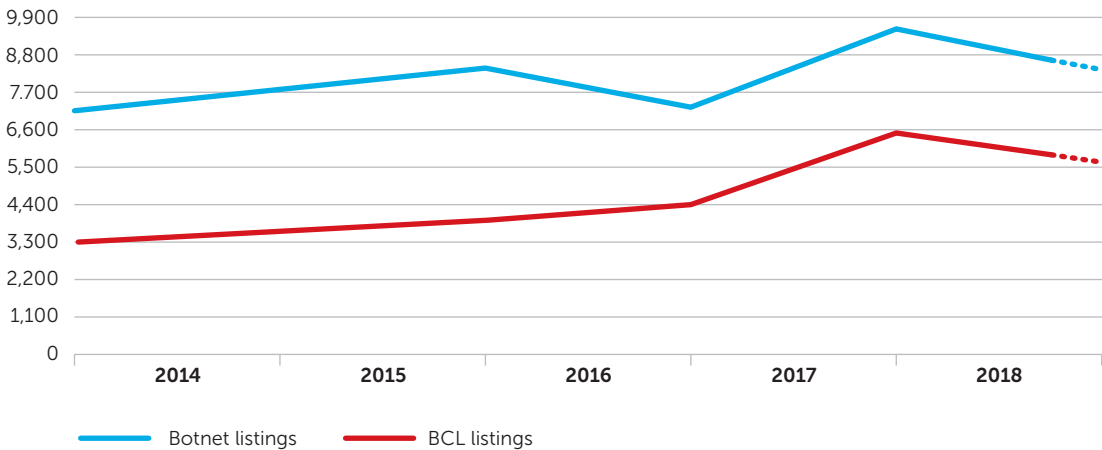
The Deteque BotnetCC feed only lists IP addresses of servers set up and operated by cyber criminals for the exclusive purpose of hosting a botnet controller (fraudulent sign-ups). Because these IP addresses host no legitimate services or activities, access to these IPs can be blocked on ISP and corporate networks without risk of affecting legitimate traffic. This renders infected computers on these networks harmless, while still allowing them to be identified. Compared to 2016, the number of such BotnetCC listings increased by more than 40%. Comparing the number of BotnetCC 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 BotnetCC listings (fraudulent sign-ups).

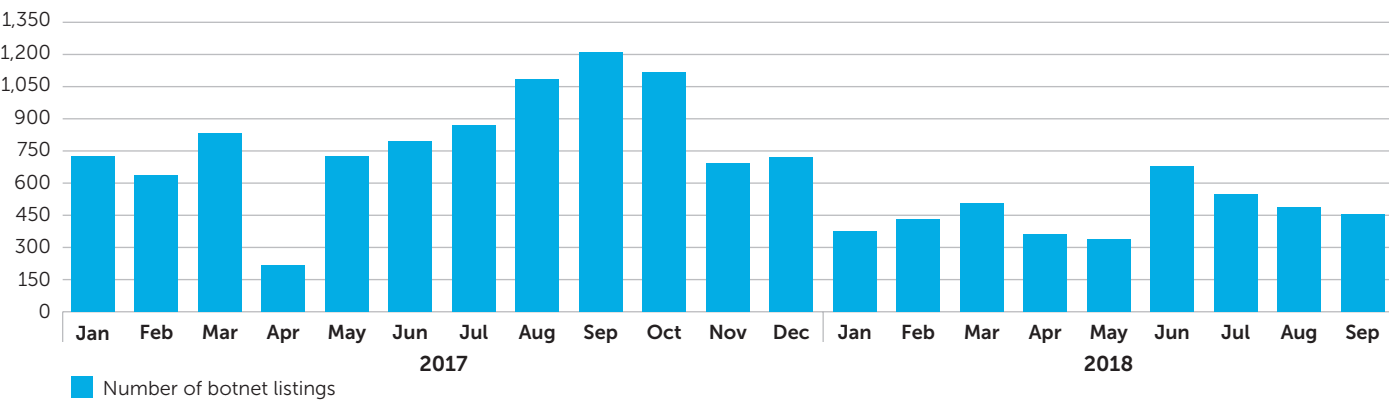
On average, we have issued between 600 and 700 BotnetCC listings per month.

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

Botnet vs BCL listings



Botnet controller listings per month



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. 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 (BotnetCC listings).

The table shows the total number of detected botnet controllers per ISP, not distinguishing between compromised webserver/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 cyber criminal 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.

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

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 reside, 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 previously. What stands out in 2017 is the dramatic increase of botnet controllers hosted at cloud providers. 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.

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 noted that hosting providers that have been misused for several years by cyber criminals for botnet hosting, now in general respond swiftly 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 these providers do still need to spend more time to address and stop abuse being generated on their network.









Deteque Threat feeds:
Domain and Malware

To host their botnet controllers, cyber criminals usually prefer to use a domain name that they registered exclusively for that purpose. This is because a dedicated domain name allows the cyber criminal 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.

Deteque 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 BotnetCC feed. Domain names that are used for botnet controller hosting are listed in the Deteque dbl.zone data set or malware.zone of Deteque’s DNS Firewall Threat Feeds. It is not uncommon that cyber criminals use 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, Deteque’s DBL and Malware feeds listed almost 50,000 botnet controller domain names registered and set up by cyber criminals for the solely purpose of hosting a botnet controller. This excludes hijacked domain names (domains owned by non-cyber criminals that were used without permission) and domains on ‘free sub-domain’ provider services.

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

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

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.

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 when ZeuS did not make 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.

Malware Types

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	ISRSStealer	Backdoor
17	148	Worm.Ramnit	e-banking Trojan
18	148	Hancitor	Dropper
19	132	AZORult	e-banking Trojan
20	131	PandaZeuS	e-banking Trojan

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 cyber criminals chose most often for their botnet operations.

We have seen a vast amount of botnet controller domain names being registered in gTLD .com and within ccTLD .pw (which is acting as a de-facto gTLD). When using domains in ccTLDs, cyber criminals chose .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.

Rank	Domains	TLD	Note
1	14,218	com	gTLD
2	8,587	pw	gTLD
3	3,707	info	gTLD
4	3,546	top	gTLD
5	2,516	org	gTLD
6	1,607	net	gTLD
7	1,463	biz	gTLD
8	1,370	ru	ccTLD
10	1,256	click	gTLD
11	1,222	xyz	gTLD
12	848	eu	gTLD
13	729	space	gTLD
14	513	website	gTLD
15	465	us	ccTLD
16	420	work	gTLD
17	344	tw	ccTLD
18	290	online	gTLD
19	241	bid	gTLD
20	236	pro	gTLD

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

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

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 cyber criminals. 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 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 cyber crime 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 cyber crime-friendly registrars are located in countries with no or slow legal recourse against cyber crime, obtaining a legal order can be difficult or impossible. Because cyber crime-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.



Case study

Global managed cloud provider Rackspace is protecting customers and improving connectivity by using Deteque's DNS Firewall to block malicious domain traffic and botnet activity.

The challenge

As the leading provider of managed cloud services, Rackspace is always looking for ways to augment its multi-layered approach to security and stay ahead of the threats from Distributed Denial of Service (DDoS) attackers looking to exploit its global infrastructure and highly connected customer base.

High volumes of domain queries across the company's infrastructure are an integral part of usual operations but Rackspace was looking for ways to reduce traffic related to malicious domains and help ensure the infrastructure isn't used by botnets to mount DDoS attacks.

In addition to security concerns, DDoS attacks are also parasites on an infrastructure, stealing bandwidth to carry out their malicious attacks.

The solution

After a market analysis of different options, Rackspace worked with Deteque's value-added delivery partner, SecurityZones, to fully deploy DNS Firewall. This included developing a pilot to ensure technical compatibility and delivery requirements with the monitoring of results prior to full implementation. Rackspace chose to have DNS Firewall threat feeds delivered as a zone transfer feed to ensure domain queries are filtered on their own DNS servers to reduce latency and because they had the skills available to implement directly.

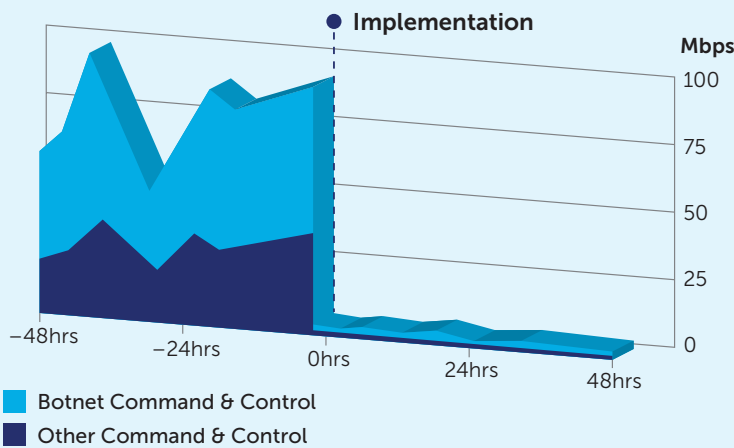
Rackspace uses industry standard BIND servers for DNS resolution and the zone transfer feed was test integrated and was soon delivering results, blocking malicious domains, without the installation of any extra hardware.

The results

Rackspace's customers rely on their users to have a seamless online experience. For eCommerce customers that means a seamless experience from advertising through to online store and final purchase. Underpinning this is multiple DNS resolution across different sites so any interruption would have an immediate business impact.

The implementation drastically cut down on botnet and other malicious Command & Control beaconing traffic. Each beaconing message is very small but an active botnet can consume massive amounts of bandwidth when it is switched on to mount a DDoS attack. Rackspace was able to virtually eliminate this traffic with no impact on customers' business flows.

Outbound botnet and other Command & Control traffic



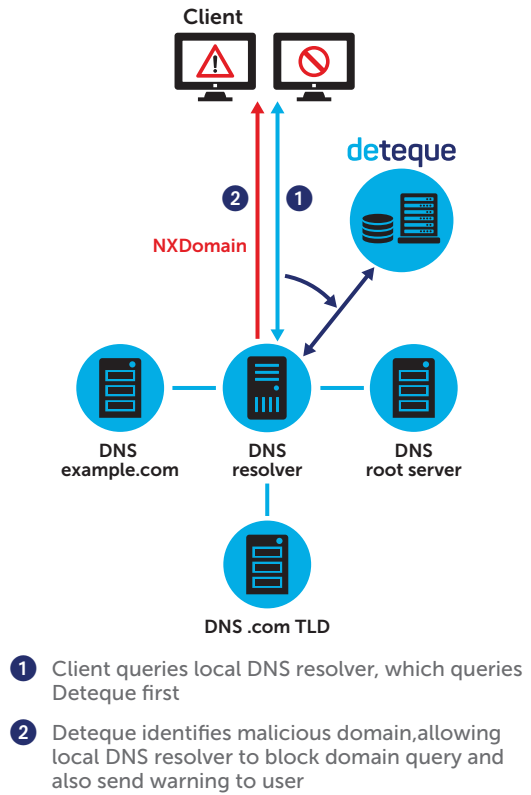
How it works

Without a DNS Firewall, a client queries a local DNS resolver and if the IP address for that domain is not included in its cache, it will query in turn an external root server, the Top Level Domain server and the domain server itself to get access to the site. The process will return both legitimate and malicious sites as there is no check in the process to exclude malicious domains.

When a client initiates a query on a Deteque enabled nameserver, each step of the recursive DNS lookup process is analyzed to identify known bad domains, addresses and nameservers. If Deteque identifies a security risk the DNS server returns a 'does not exist' type answer which prevents access to the threat.

Each organization can customize the user warning page to include security awareness and best practice training messages. It's an essential step to make sure everyone across an organization contributes to online security.

Deteque's threat feeds can be delivered as a data query service, so it is a DNS Firewall acting on your behalf. For organizations operating larger commercial operations serving more than 5,000 users, Deteque domain-based reputation data is available via IXFR.



Conclusion

The big increase of IoT threats in 2017 is very likely to continue and we are sure that securing and protecting IoT devices will continue to be a core topic.

DNS Firewall Threat Feeds, such as Deteque's BotnetCC, Malware Domain List and Zero Reputation (ZRD) feed can help you protect IoT devices on your network. Additionally, these feeds can assist you in identifying potential intruders and infected machines which are trying to connect to these malicious sources.

Cloud providers rotating botnet controllers around different IP addresses present a threat to Spamhaus users. We therefore hope that cloud hosting providers will increase their abuse desks' capacity to not only respond to abuse problems promptly but also to take preventative 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'.

In relation to 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.

It is up to all parties to pull together and take responsibility for making the Internet safer which includes individual IT, security and network teams ensuring they take a multi-layered approach to their security strategy; protecting their users, customers and networks.