
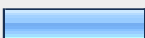
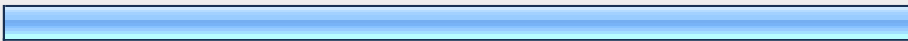


# Fast Flux - Initial Report Proposals Survey Final

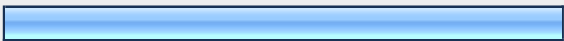



1. Respondent			
		Response Percent	Response Count
Name		100.0%	14
Company / Organisation		100.0%	14
Constituency		100.0%	14
		<i>answered question</i>	<b>14</b>
		<i>skipped question</i>	<b>0</b>

2. Proposal 3.1 - Line 208, change 'Why Fast Flux is a Problem' to Illicit Uses of Fast Flux. ----- Rationale: The current heading assumes that the current state of affairs in untenable and requires action by ICANN. Additionally, the preceding section is titled "Legitimate Uses of Fast Flux," so "Illicit Uses of Fast Flux" fits more clearly into the larger organizational structure.			
		Response Percent	Response Count
Agree		84.6%	11
Do not agree		0.0%	0
Alternative view		0.0%	0
No strong view either way		15.4%	2
		Comments	2
		<i>answered question</i>	<b>13</b>
		<i>skipped question</i>	<b>1</b>




**3. Proposal 3.2 - Insert after line 235: It should be emphasized that statements and contributions made by individual members of the Working Group in the course of this policy development process are made on an individual title and are not necessarily representative for their respective constituency. ----- Rationale: In contrast with a GNSO Task Force, Working Group members participate as individuals, not as representatives for their constituency. This should be highlighted in this section to ensure that individual contributions are not attributed wrongly to constituencies as a whole. On the contrary, constituency statements which have also been submitted in the course of this PDP are representative of the views of a particular constituency.**

		Response Percent	Response Count
Agree		100.0%	13
Do not agree		0.0%	0
Alternative view		0.0%	0
No strong view either way		0.0%	0
Comments			1
<i>answered question</i>			<b>13</b>
<i>skipped question</i>			<b>1</b>

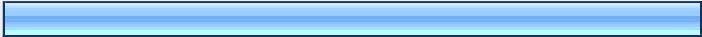


**4. Proposal 9.1 - Add additional characteristics to proposal 9 - elements of the attack network run on compromised computers - whois records are fraudently created (e.g., using stolen identities or payment methods) ----- Rationale: Joe reminds me that one of the characteristics of domains associated with fast flux attack networks is registration information that is incomplete, inaccurate, or fraudulently created. I would propose that we add this to the list of characteristics I submitted. I also think it's helpful to observe that by adding this, we have 2 characteristics that distinguish attack applications of FF from beneficial applications. Based on the discussion among at least 4 members in this thread, I would hope we could also observe that • incomplete or inaccurate whois records are problematic because such records can be found among malefactors who run FF networks for attack purposes as well as parties who use FF for beneficial purposes • malefactors benefit from registration documentation practices that are not effective in collecting and maintaining accurate and complete registration records, and thus... • efforts to maintain more accurate and complete registration records from registrants is one of several actions that could reduce domain name misuse and to some extent, also reduce the use of domain names in the fast flux attacks. This is not saying “change WHOIS” but saying “take measures to improve the quality of data collected, maintained, and published via WHOIS”. I think this is within our remit, perhaps Liz or Chuck or Avri could confirm.**

		Response Percent	Response Count
Agree		61.5%	8
Do not agree		30.8%	4
Alternative view		7.7%	1
No strong view either way		7.7%	1
Comments			3
<i>answered question</i>			<b>13</b>

5. Proposal 12 - Additional text following line 308 Lines While those sort of networks employ short TTLs, short TTLs -- in and of themselves -- are insufficient to characterize a domain name as 'fastflux.' TTLs become an issue for fastflux-related work primarily because at least one Internet Draft, <ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-bambenek-doubleflux-01.txt> (URL broken due to length) focuses primarily on establishing minimum TTLs as an approach to limiting fastflux. If constraints were to be applied to TTLs in an effort to limit fastflux, this would impact organizations which rely on short TTLs in order to be able to relocate resources as part of the process of mitigating distributed denial of service attacks, would impact organizations moving nameservers, and would impact organizations which rely on short TTLs in order to provide a variety of legitimate services, among others." ----- Rationale: The draft report does not explain why that scenario is relevant to a discussion of fastflux. There are a ton of services that use short TTLs. Proposed additional text following line 308 meant to correct that.

		Response Percent	Response Count
Agree		84.6%	11
Do not agree		0.0%	0
Alternative view		7.7%	1
No strong view either way		7.7%	1
		Comments	2
		<b>answered question</b>	<b>13</b>
		<b>skipped question</b>	<b>1</b>

6. Proposal 15 - Addition immediately following line 345: Some in the working group would point to the way in which fast flux nodes are created as prima-facie evidence of fast flux techniques constituting malicious behavior. Recall that fast flux nodes are created by compromising hosts with malicious software installed without the knowledge or consent of the system's operator/owner. With respect to malicious behaviors enabled by fast flux, one non-subjective definition of 'malicious behavior' would be, 'Activities which are illegal under the laws or regulations of a country having jurisdiction over the activity in question.' For example, in the United States, malicious activities enabled by fastflux might include, among other things: -- Cyber intrusions/unauthorized access to computers and networks -- Phishing (forgery and social engineering attacks meant to induce users to reveal sensitive financial credentials) -- Carding (trading and misuse of credit card numbers and other financial credentials) -- Distribution of viruses or other malware -- Distribution of child pornography -- Distribution of narcotics or other scheduled controlled substances without a valid prescription -- Distribution of knockoff/counterfeit versions of trademarked or copyrighted property such as watches, purses, computer software, movies or music ----- Rationale: Dissemination of malware, and unauthorized access to others' systems which have been compromised by malware, is a universally accepted example of malicious online behavior. The very motion establishing this working group (gnso.icann.org/announcements/announcement-30may08.htm ) recognized that the ICANN GNSO Council's interest in considering fast flux was because of its criminal nature. E.G., that motion stated that they were creating a Working Group in order to: "... develop potential policy options to curtail the CRIMINAL USE of fast flux hosting." [emphasis added] Our report should provide at least a brief discussion of what such behaviors might be.


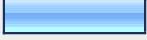
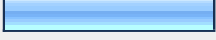
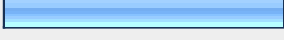
		Response Percent	Response Count
Agree		76.9%	10
Do not agree		15.4%	2
Alternative view		7.7%	1
No strong view either way		0.0%	0
Comments			1
<i>answered question</i>			<b>13</b>
<i>skipped question</i>			<b>1</b>

7. Proposal 16 - Addition of the following text after line 363: The majority of members of the working group believe that the Mannheim fast flux score formula would provide a robust and mechanically applicable definition of "fast flux" which would minimize false positives, and believe that the use of whitelisting plus manual review can eliminate any remaining potential false positives. The working group received multiple offers of fast flux-related data from <insert list of fastflux data sources here [I'm aware of at least two or three, but I'll defer to the data collection subcommittee for a definitive list]>. The working group accepted [or rejected] data from those sources, and [did what with it?], finding [what?]. Those interested in working with that data can apply to obtain access to it by contacting [who?] While it may not be possible to definitively distinguish the costs of cybercrime associated with fast flux from the costs of cybercrime conducted separate from fast flux, the working group did receive reports on aggregate estimates of cybercrime-related costs, and even if a fraction of 1% of all cybercrime can be tied to fastflux, the costs would be staggering. Moreover, at least in some cases such as the use of fast flux to distribute child pornography, there are substantial non-financial human costs which should also be recognized. -----

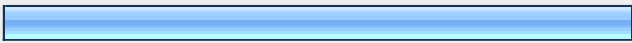
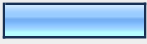
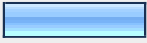
Rationale: the ability to mechanically screen potential fast flux domains is an important element of our ability to scalably and efficiently process complaints about potential fast flux domains. The availability of a simple, easily computed "flux score" eliminates the need to vett the expertise of a potential complainant since a mechanical test of this sort is objective, replicable and cost free, and doesn't rely on complainant-supplied supporting evidence. A complainant need only supply a candidate domain name, after which ICANN/registrar/registry queries to domain name and routing data (delivered via DNS) would quickly allow the submitted domain name to be screened for fast flux characteristics. Because a number of working group members expressed concern about potential false positives, I deemed it important to also include a brief discussion of how false positives could be avoided. Much of the discussion in the draft report focused on how the next step will largely be a data collection and analysis process. A number of researchers active in the fast flux area have already supplied data to this working group, so it is important to understand what has already been received, what has been done with what has been received, and the conclusions of that analysis. Peer review and replication also strongly argues for making data sets available for re-analysis and verification/validation whenever possible, recognizing that in some cases proprietary rights or other restrictions may limit the Working Group's ability to reshare data. The financial and intangible costs associated with cybercrime are huge (measured in the billions of dollars/year); see the estimates provided in <http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00264.html> and <http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00265.html> Storm, a fast flux-based spam delivery mechanism, has been estimated as spewing one fifth of all spam, as cited at: <http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00266.html> Understanding the magnitude of those costs, and the role that fastflux plays in those illegal activities, underscores the importance of attacking the fast flux problem.

		Response Percent	Response Count
Agree	<input type="text"/>	38.5%	5
Do not agree	<input type="text"/>	38.5%	5
Alternative view		0.0%	0
No strong view either way	<input type="text"/>	23.1%	3
Comments			3
<b>answered question</b>			<b>13</b>
<b>skipped question</b>			<b>1</b>

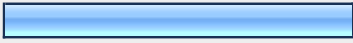
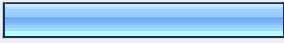

8. Proposal 16.1 - Possible minority position relating to proposal 16. Note, TBC is to be replaced by a minority / majority / or other term depending on the level of support for the proposal. TBC of Working Group members are of the opinion that applying any mechanical formula will inevitably lead to more and more false positives, and that if the formula's score is applied automatically without human oversight, many innocent bystanders will be negatively affected. In particular, just as malevolent virus authors ("the bad guys") today purchase anti-virus software to pre-test their creations against the signatures provided by anti-virus vendors, malevolent agents using fast flux techniques can certainly test their networks to see whether their score is at an "acceptable" level. In other words, they'll adapt. Thus, the formula begins to lose its power to discriminate between good and bad over time due to this adaptation. Bad guys are certainly creative and have resources to adapt. The notions of adaptation over time and pre-testing aren't confined just to anti-virus systems, but also in the email spam and web-spam worlds, to give further examples. Email providers and search engines are constantly tweaking their algorithms/formulas as spammers adapt to existing ones. A static formula is likely doomed to failure. The TBC of Working Group members wouldn't be surprised to see some of them buying registrars, or even TLD registries, to further their goal of not being shut down. The second reason that the rate of false positives will change over time is due to the adoption of beneficial fast flux techniques by a growing number of organizations, as leading edge techniques move from "early adopters" into the mainstream. I brought up this issue before in relation to Bayes' theorem, at: <http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00425.html> "The rarer the condition for which we are testing, the greater the percentage of positive tests that will be false positives." As more beneficial fast flux uses occur, the "malevolent" fast flux becomes a rarer condition, and thus the percentage of false positives will increase. If these two factors lead to forced revisions over time to the Mannheim fast flux score, TBC of Working Group members are concerned that it becomes a losing "arms race", just like signature-based anti-virus techniques. There also didn't seem to be data on malevolent fast flux networks that already might exist but that aren't caught by the Mannheim fast flux score (i.e. false negatives), which goes to the same issue of how often this Mannheim fast flux score formula might need to be revised in the future.

		Response Percent	Response Count
Agree		30.8%	4
Do not agree		15.4%	2
Alternative view		23.1%	3
No strong view either way		30.8%	4
		Comments	3
		<i>answered question</i>	13
		<i>skipped question</i>	1

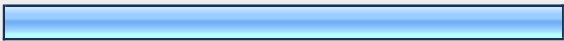
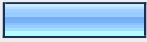

9. Proposal 18 b3 - Following #3. Individuals who receive phishing emails and are lured to a phishing site #hosted on a bot used by the miscreants/criminals who run the phishing attack #may have their identities stolen or suffer financial loss from credit card, #securities or bank fraud. add Those losses may include both direct losses which a financial institution declines to make whole, as well as indirect costs (potentially higher interest rates, reduced credit lines, declined credit applications, etc.) Identity theft can also touch on national security issues, if stolen identity information is used to illegally cross borders, to illegally remain in country or to work without permission, or to purchase items or services (such as weapons or airline travel) that might not otherwise be available if a person used their real identity.

		Response Percent	Response Count
Agree		69.2%	9
Do not agree		15.4%	2
Alternative view		0.0%	0
No strong view either way		15.4%	2
Comments			2
<b>answered question</b>			<b>13</b>
<b>skipped question</b>			<b>1</b>

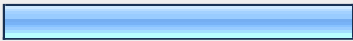

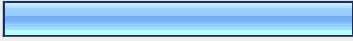
10. Proposal 18 b4 - Following #They may unwittingly disclose medical or personal #information that could be used for blackmail or coercion. add or for discriminatory treatment by employers concerned with potential costs associated with identified (but latent) genetic conditions, for example. Fear that medical record systems are porous may also deter some individuals from even seeking help ("I'd like to find out what's causing my condition, but I'm afraid that if I go in, the whole town will know I have <whatever>")

		Response Percent	Response Count
Agree		38.5%	5
Do not agree		30.8%	4
Alternative view		0.0%	0
No strong view either way		30.8%	4
Comments			3
<b>answered question</b>			<b>13</b>
<b>skipped question</b>			<b>1</b>

11. Proposal 18b5 - Delete #They may infect #their computers with malicious software that would "enlist" their computers #into a bot herd. ----- Rationale: It seems odd to have this item pop up here -- this feels more like something that belongs in an introductory paragraph explaining how fastflux works

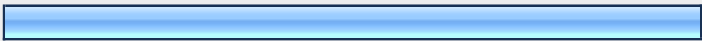


		Response Percent	Response Count
Agree		61.5%	8
Do not agree		15.4%	2
Alternative view		0.0%	0
No strong view either way		23.1%	3
		Comments	2
		<i>answered question</i>	<b>13</b>
		<i>skipped question</i>	<b>1</b>

12. Proposal 18 b6 - Below #Individuals who purchase bogus products, especially #pharmaceuticals, may be physically harmed from using such products. strike the trailing period and add ... and in a variety of ways. For example: -- teenagers might have uncontrolled access to narcotics, steroids or other dangerous controlled substances, with potentially tragic consequences, - women attempting to purchase birth control patches online might be sold adhesive bandages with no active ingredient whatsoever instead -- cancer patients, rather than receiving efficacious treatment from a licensed physician, might rely on bogus online herbal "cures" that actually do nothing to treat their disease, again, potentially resulting in deaths or serious complications Illegal generic drugs also undercut the incentive for pharmaceutical firms to invest in new drug research by cutting into their earning stream while their discovery is, or should be protected by patents. Sale of counterfeit products is another example of how fast flux networks can result in users and businesses being harmed. Counterfeit products may undermine the value of carefully nurtured brand names, leave consumers with shoddy or dysfunctional products, deny nations legitimate customs revenues associated with the importation of premium brand-name products, or result in unsafe products (for example as a result of counterfeit UL-listed electrical appliances cords).

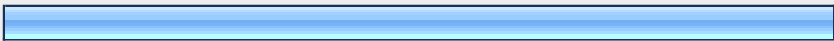

		Response Percent	Response Count
Agree		38.5%	5
Do not agree		23.1%	3
Alternative view		0.0%	0
No strong view either way		38.5%	5
		Comments	6
		<i>answered question</i>	<b>13</b>
		<i>skipped question</i>	<b>1</b>



13. Proposal 18 b7 - #4. Internet access operators Replace "Internet access operators" with "Internet service providers" -----  
 ----- Rationale: "Internet service providers" is the commonly used term for the service being referred to; "Internet access operators" would be an uncommon and potentially confusing usage

		Response Percent	Response Count
Agree		76.9%	10
Do not agree		7.7%	1
Alternative view		0.0%	0
No strong view either way		15.4%	2
Comments			1
<b>answered question</b>			<b>13</b>
<b>skipped question</b>			<b>1</b>




14. Proposal 18 b8 - Below #are harmed when their IP address blocks add and their domain names ----- Rationale: reputation damage accrues not just to IP addresses but also to domain names.

		Response Percent	Response Count
Agree		91.7%	11
Do not agree		8.3%	1
Alternative view		0.0%	0
No strong view either way		0.0%	0
Comments			1
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

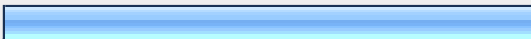
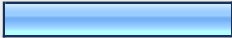
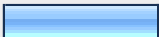
15. Proposal 18 b9 - Below: #are associated with bot nets and phishing attacks that are linked to fast flux #activities. These operators also bear the burden of switching the #unauthorized traffic that phishing attacks generate and they may also incur #the cost of diverting staff and resources to respond to abuse reports or #legal inquiries. strike the final period and add: or helping users to get cleaned up, or purchasing antivirus products to hand out to users, or deploying network-based remediation solutions. ISPs are harmed when spammers send spam spamvertising fastflux hosted sites, and the ISP get deluged with that fastflux-enabled spam. ISPs may also experience excess DNS-related traffic as a result of fastflux, resulting in the need for them to deploy additional recursive resolver capacity. ISPs may also be forced to deploy deep packet inspection equipment or other networking equipment to detect and respond to fastflux hosted sites on customer systems. (Because fast flux web sites can be easily hosted on arbitrary ports, port-based blocking solutions won't work to control fastflux hosting, unlike port 25 blocks deployed to control direct-to-MX spam).

		Response Percent	Response Count
Agree		66.7%	8
Do not agree		16.7%	2
Alternative view		0.0%	0
No strong view either way		16.7%	2
Comments			3
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

16. Proposal 18 b10 - Below #5. Registrars are harmed when their registration and DNS hosting services are used to abet "double flux" attacks. Like Internet access providers, they may also incur the cost of diverting staff and resources to monitor abuse, or to respond to abuse reports or legal inquiries. Registrars currently see wdprs.internic.net complaints in conjunction with fast flux domain simply because that's the sole complaint mechanism currently available which potentially reaches fastflux domain name abuse. Antispam activists have thus become very good at carefully scrutinizing spamvertised fastflux domain names for whois problems. Dealing with those WDPRS reports represents an additional registrar-specific cost. Providing a reporting channel that focusses on the actual issue (a domain has been detected which is engaged in criminal activity) rather than the substitute issue (there's a problem with the domain's whois data), will clarify the problem at hand.

		Response Percent	Response Count
Agree		75.0%	9
Do not agree		0.0%	0
Alternative view		8.3%	1
No strong view either way		16.7%	2
Comments			3
<i>answered question</i>			<b>12</b>
<i>skipped question</i>			<b>2</b>

17. Proposal 18 b11 - After 7. Individuals or businesses whose lives or livelihoods are affected by the illegal activities abetted through fast flux networks, as are persons who are defrauded of funds or identities, whose products are imitated or brands infringed upon, and persons who are exploited emotionally or physically by the distribution of images or enslavement. Examples of these ills can be seen in things such as child pornography, unauthorized distribution of proprietary software ("warez"), unauthorized distribution of copyrighted music and movies, unauthorized distribution of counterfeit "knock-off" trademarked merchandise, etc.

		Response Percent	Response Count
Agree		58.3%	7
Do not agree		25.0%	3
Alternative view		0.0%	0
No strong view either way		16.7%	2
Comments			2
<i>answered question</i>			<b>12</b>
<i>skipped question</i>			<b>2</b>

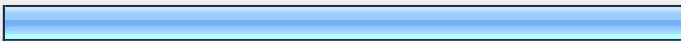

18. Proposal 18 b12 - After #8. Registries may incur the cost of diverting staff and resources to monitor #abuse or to respond to abuse reports or legal inquiries. add Uptake/legitimate use of some TLDs may also be impacted by fast flux abuse. If the public perceives that sheer use of a domain from a particular TLD may result in negative scoring by anti-spam software such as SpamAssassin, that can be a powerful disincentive hindering the adoption and use of that registry's TLD.

		Response Percent	Response Count
Agree		91.7%	11
Do not agree		0.0%	0
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			1
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

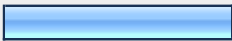
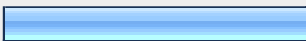
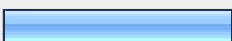

19. Proposal 18 b13 - After #Who benefits from the use of short TTLs? add "Short TTLs" per se are NOT synonymous with "fastflux." Short TTLs are only one characteristic associated with fastflux domains.

		Response Percent	Response Count
Agree		91.7%	11
Do not agree		0.0%	0
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			1
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

20. Proposal 18 b14 - After #2. Content distribution networks such as Akamai, where "add, drop, change" #of servers are common activities to complement existing servers with #additional capacity, to load balance or location-adjust servers to meet #performance metrics (latency, for example, can be reduced by making servers #available that are fewer hops from the current most active locus of users #and by avoiding lower capacity or higher cost international/intercontinental #transmission links). add Some providers may also selectively return different IP addresses in response to DNS queries from different audiences -- e.g., you might get German content if you're connecting from what appears to be a German IP address, or French content if you're connecting from what appears to be a French IP address.


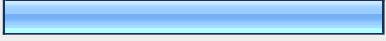
		Response Percent	Response Count
Agree		75.0%	9
Do not agree		0.0%	0
Alternative view		0.0%	0
No strong view either way		25.0%	3
Comments			0
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

21. Proposal 18 b15 - After #3. Organizations that provide channels for free speech, minority advocacies, #and activities, revolutionary thinking may use short TTLs and operate #fast-flux like networks to avoid detection. add Some members of the working group note that they haven't observed this. Free speech organizations and activist entities may offer or use encrypted, non-attributable, or covert communication channels, such as PGP/Gnu Privacy Guard, remailers, steganographic methods, Tor/"onion routing," anonymous VPN services, etc., but an example of genuine fast flux hosting (including operation on involuntarily bottled hosts) has not be identified to date. Fast flux methods, when they've been observed in use, have been used to enable hosting of spamvertised or illegal web sites. Those spamvertised and/or illegal web sites may be phishing web sites, or malware web dropping sites, or child porn sites, or warez sites, or carding sites, or whatever, but to date working group participants have not identified even a single case where political, religious or other dissident web sites have been found to be hosted on fast flux. Dissident web sites don't need fast flux. They can simply purchase legitimate extraterritorial web hosting, so that even if one country won't allow their web site to be hosted, someone abroad typically will do so. The sites which do end up on fastflux web hosting are those which are so far beyond the pale that NO ONE will host them \*anywhere\* in the world. That category is generally limited to spammers and egregious types of content such as child pornography, phishing, malware, carding, etc.

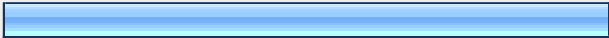

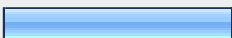
		Response Percent	Response Count
Agree		25.0%	3
Do not agree		33.3%	4
Alternative view		25.0%	3
No strong view either way		25.0%	3
Comments			4

	<i>answered question</i>	<b>12</b>
	<i>skipped question</i>	<b>2</b>


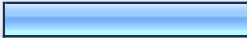
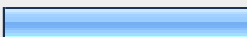
22. Proposal 19.1 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting? \_Introduction\_ While most Internet users have never heard of fastflux hosting, a growing number of them are nonetheless directly affected by it. Internet users provide both the raw material that fastflux hosting runs on (malware-compromised broadband-connected consumer PCs), while also serving as the target audience for the spamvertised web sites which fastflux enables. Internet users are thus central to the entire fastflux problem, and unless it is handled appropriately, they are also the ones who may be subject to further restrictions and loss of Internet transparency. ----- Rationale: When it comes to question 5.6, "How are Internet users affected by fast flux hosting?" I addressed the question 5.6 in my note at <http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00061.html> I would propose that that text be included as a draft response to 5.6

		Response Percent	Response Count
<b>Agree</b>		58.3%	7
Do not agree		0.0%	0
Alternative view		0.0%	0
No strong view either way		41.7%	5
Comments			1
	<i>answered question</i>		<b>12</b>
	<i>skipped question</i>		<b>2</b>

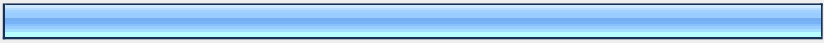
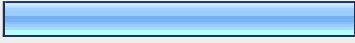
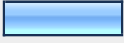
23. Proposal 19.2 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting? Malware, Spam, and Bots To understand how consumer PCs came to be converted into fastflux nodes, we need to step back for a moment and consider the related problems of malware and spam. Internet miscreants use malware -- viruses, worms, trojan horses, etc. -- to efficiently gain control over large numbers of vulnerable networked consumer PCs. Those compromised systems, subject to remote manipulation by shadowy masters, are commonly known as "bots" or "zombies." Having obtained control over those compromised PCs, the miscreants can then use those bots as a base from which to search for additional vulnerable systems, as a platform for sniffing network traffic, as a source of network attack ("DDoS") traffic, or most commonly, to deliver spam directly to remote mail servers (so-called "direct-to-MX spamming").

		Response Percent	Response Count
Agree		66.7%	8
Do not agree		8.3%	1
Alternative view		0.0%	0
No strong view either way		25.0%	3
Comments			1
<i>answered question</i>			12
<i>skipped question</i>			2



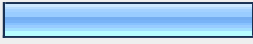
24. Proposal 19.3 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.7, "How are Internet users affected by fast flux hosting? What Are Miscreants to Do With Compromised Hosts That Can't Be Used for Spam? Abuse Working Group, a consortium of leading international ISPs, has issued recommendations for managing port 25 traffic to defend against spamming, see <http://www.maawg.org/port25> If traffic on port 25 is blocked through following those recommendations, as it now is, spam can no longer be sent directly to remote mail servers from those compromised PCs (although non-spamming normal mail use is still possible). When the ISPs control port 25, that leaves the shadowy "bot herders" with millions of compromised systems which are now unable to deliver spam directly to remote mail servers.

Agree			
Do not agree			
Alternative view			
No strong view either way			
			<i>answered question</i>
			<i>skipped question</i>

25. Proposal 19.4 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question users affected by fast flux hosting? Spammers and Other Internet Miscreants Have a Hard Time Getting Web Hosting At spammers (and other miscreants) find themselves confronting a second orthogonal problem: it has become hard if not impossible to retain mainstream web hosting for illegal content. While what's illegal will vary from jurisdiction to jurisdiction, there are some categories which are illegal virtually everywhere, including, among other things: -- narcotics, anabolic steroids and other dangerous drugs distribution -- prescription -- child pornography -- viruses, trojan horses and other malware -- stolen credit card information -- phishing web sites -- property, including pirated software ("warez"), copyrighted music and movies, and trademarked consumer goods (most notably things like watches, shoes, handbags, etc.) In fact, many hosting companies specifically exclude hosting of any product or service (whether legal or illegal) that has been "spamvertised" (advertised via spam), because they recognize that to permit spamvertised products or services on their hosts commonly result in their address space getting listed on one or more anti-spam DNS block lists, such as those operated by Spamhaus [http://www.spamhaus.org/].

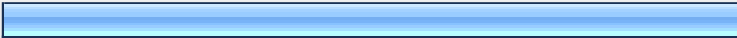
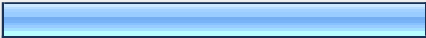
		F
Agree		
Do not agree		
Alternative view		
No strong view either way		
		C
		<i>answered</i>
		<i>skipped</i>

26. Proposal 19.5 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting?" Miscreants Discover One Thing They CAN Do With Non-pamable Compromised Hosts With that for background, it is easy to imagine what happened next: spammers repurposed some of their "surplus inventory" of compromised-but-unspammable systems to provide "web hosting" for illegal or spamvertised content which they couldn't host elsewhere.

		Response Percent	Response Count
Agree		54.5%	6
Do not agree		18.2%	2
Alternative view		0.0%	0
No strong view either way		27.3%	3
		Comments	3
		<i>answered question</i>	<b>11</b>
		<i>skipped question</i>	<b>3</b>



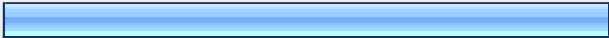
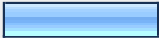
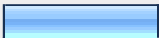
27. Proposal 19.6 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question Internet users affected by fast flux hosting? Reverse Proxies Are Used to Actually Deploy Fast Flux Hosting Networks Spammers actually replicated all the hundreds or thousands of html files, images, databases and other bits and pieces of content and software on a sophisticated web site on each of dozens or hundreds of fastflux hosts. That would be too complex, too error prone, too time consuming and too easily detected. Instead, spammers found that they could use "reverse proxy" software to accept web connections on the compromised consumer host, tunnelling that traffic back to their actual (hidden) backend master host. "nginx" is one product often used for that purpose, although it is also routinely used by regular web sites as well. The compromised consumer PC then acts as if it were delivering web content, in reality it is just acting as a pipeline to a hidden master web server (or farm of servers) located elsewhere. [insert suitable illustration showing reverse proxy setup here]

		Response Percent
Agree		63.6%
Do not agree		0.0%
Alternative view		0.0%
No strong view either way		36.4%
		Comments
		<i>answered question</i>
		<i>skipped question</i>

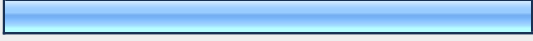
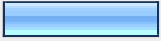


28. Proposal 19.7 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting? Use of Botted PCs Is Non-Consensual and Surreptitious The owner/user of a compromised PC doesn't know that his or her PC is being used as part of a fast flux hosting network. No one asks the owner of the compromised PC, "Do you have any objection if we use your computer to distribute stolen credit card numbers?" and no warning light goes off on the compromised PC saying "Hey, someone's serving stolen software from your system!" Typically the owner of the PC \*only\* becomes aware that they have unwittingly become a participant in illegal online activity when: -- antivirus software, or other security software, eventually detects the presence of malicious software on the system -- someone complains to their ISP, and their ISP contacts the customer with the bad news that they're infected -- the ISP disconnects the customer, blocks traffic to/from them, or plops the customer into a quarantine zone where all they have access to are clean up-related sites and tools -- the user finds their system has become slow or unstable, and takes steps to figure out why, -- the user find that they can no longer access some remote network resources because they've been blocked at those remote sites as a result of their infection, or -- the user is visited by law enforcement officials investigating the illegal activity that has been seen in conjunction with "the user's" connection.

		Response Percent	Response Count
Agree		81.8%	9
Do not agree		9.1%	1
Alternative view		0.0%	0
No strong view either way		9.1%	1
Comments			2
<b>answered question</b>			<b>11</b>
<b>skipped question</b>			<b>3</b>

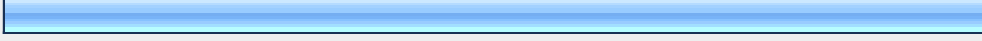
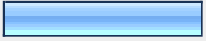
29. Proposal 19.8 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting? Post\_Fast\_Flux\_Infection\_Cleanup Once the user discovers that they've been botted and used for fastflux purposes, they are then left with the unenviable chore of trying to get their compromised system disinfected. Because of the complexity of cleaning many malware infections, and the substantial possibility that at least some lingering malware components may be missed during efforts at cleanup, most experts recommend formatting compromised systems and reinstalling them from scratch, however that can be a time consuming and laborious process, and one that may be practically impossible if the user lacks trustworthy backups or cannot find original media for some of the products they had been using. The need to deal with this mess is the first tangible user impact of fastflux hosting, but one which only some unlucky Internet users experience.

		Response Percent	Response Count
Agree		66.7%	8
Do not agree		16.7%	2
Alternative view		0.0%	0
No strong view either way		16.7%	2
Comments			3
<b><i>answered question</i></b>			<b>12</b>
<b><i>skipped question</i></b>			<b>2</b>

30. Proposal 19.9 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting? One Universal Impact of Fast Flux: Spam The next effect of fastflux hosting is one which virtually all Internet users experience, and that's spam. Remember, fastflux hosting exists to host illegal content or spamvertised products or services. All of us receive spam, whether that's an occasional message that slips through otherwise efficient filters, or a steady deluge that may have caused some of us to abandon email altogether. Without the ability to obtain reliable web hosting services, spammers are left with only a few categories of potential spam, such as stock pump-and-dump spam, where users don't need to visit a spamvertised web site to purchase a product or service. Clearly spammers are powerfully motivated to find a takedown-resistant way to host their web sites, and that's what fastflux has given them. With fastflux, if one compromised machnie is discovered and taken off line, another system will be ready to take over. It thus becomes very difficult to "completely take down" the spammer's "web hosting" unless you can: -- identify and take down the back-end hidden master web server -- take down the domain name that's being spamvertising, or -- take down the name servers that the spamvertised domain relies on.

		Response Percent	Response Count
Agree		58.3%	7
Do not agree		16.7%	2
Alternative view		8.3%	1
No strong view either way		16.7%	2
		Comments	3
		<i>answered question</i>	12
		<i>skipped question</i>	2

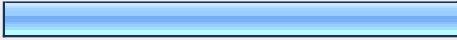

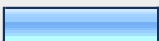
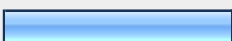
31. Proposal 19.10 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting? Fluxing \*Name Servers\* As Well As Web Sites: The Rise of "Double Flux" Spammers quickly recognized that the name servers were a weak point in their scheme, so they adapted by beginning to not just use compromised systems for web hosting, they also began to use those systems to do DNS for their domains. A domain that does both its web hosting and web DNS service via compromised systems is normally referred to as a "double fastflux" or "doubleflux" domain.

		Response Percent
Agree		83.3
Do not agree		16.7
Alternative view		0.0
No strong view either way		0.0
		Comments
		<i>answered question</i>
		<i>skipped question</i>

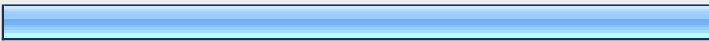


32. Proposal 19.11 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting?"

Port Blocks Won't Work to Curtail Fast Flux Web Hosting All of this malicious activity, taking place on systems that are not professionally administered, resulted in ISPs endeavoring to control these phenomena via the network. It is understandable why they were inclined to do so: blocking port 25 controlled the spewage of spam, even if it did nothing to fix the underlying condition of the infected host, so maybe something similar could be done to address fastflux and doubleflux abuse?



Unfortunately, unlike email where controlling port 25 is sufficient to control the emission of spam, when it comes to fastflux web pages, web pages can be served on *any* arbitrary port (e.g., to access a web server running on port 8088 instead of the default port 80, one might use a URL such <http://www.example.com:8088/sample.html> ).

		Response Percent	Response Count
Agree		50.0%	6
Do not agree		8.3%	1
Alternative view		16.7%	2
No strong view either way		25.0%	3
		Comments	4
		<b><i>answered question</i></b>	<b>12</b>
		<b><i>skipped question</i></b>	<b>2</b>

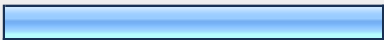
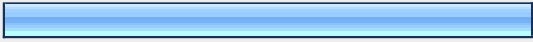
33. Proposal 19.12 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question Internet users affected by fast flux hosting? ISP Efforts to Control Fast Flux and Double Flux Result in Collateral Damage traffic from consumer web pages thus often results in ISPs deploying more draconian solutions, such as banning all web servers from customer address space, or deploying potentially expensive deep packet inspection (DPI) appliances to identify fastflux or double flux at least until the spammers begin using SSL/TLS to defeat DPI. The problem gets even more complex when double flux is involved. We are routinely hosted on consumer systems, controlling that DNS traffic requires managing port 53 traffic, blocking external DNS queries to the name server running on the compromised customer host, and typically also managing blocking or redirecting any DNS traffic coming from the local customer base, permitting it only to access the provider's own DNS recursive resolvers. This loss of Internet transparency can prevent customers from readily (and intentionally) using third party DNS servers (such as those offered to the Internet community by OpenDNS) and also complicate or preclude things such as accessing access-limited information products delivered via DNS, such as some subscription lists.

		Response Percentage
Agree		58
Do not agree		16
Alternative view		0
No strong view either way		25
		Comments
		<i>answered questions</i>
		<i>skipped questions</i>




34. Proposal 19.13 - Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting? Conclusion In conclusion, Internet users see their systems used without their permission by abusers who've set up fastflux nodes on them; they face the daunting task of cleaning up those compromised systems once they discover what's happened; they are the target of endless spam, spam that would be materially harder if fastflux hosting didn't exist; and they experience a loss of Internet transparency as ISPs struggle to control the fastflux and doubleflux problems on the network. The combination of those effects can result in Internet users having a pretty bad experience, all thanks to the choice by some Internet miscreants to use fast flux and double flux techniques.

		Response Percent	Response Count
Agree		75.0%	9
Do not agree		0.0%	0
Alternative view		0.0%	0
No strong view either way		33.3%	4
Comments			0
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

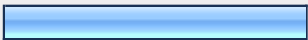
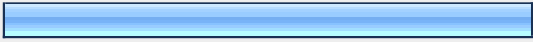

35. Proposal 20 - Line 367 -- Question 5.3 'Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?' Answering this question should be deferred until there is; a robust technical and process definition of "Fast Flux", there are reliable techniques to detect Fast Flux enhanced networks while avoiding false positives, there is reliable information as to the scope and penetration of Fast Flux networks and, there is reliable information as to the financial and non-financial impact of these networks.

		Response Percent	Response Count
Agree		41.7%	5
Do not agree		58.3%	7
Alternative view		0.0%	0
No strong view either way		0.0%	0
Comments			1
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

36. Proposal 21 - Line 367 -- Question 5.3 'Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?' In its Constituency Input Statement (attached to this report as a annex), the RyC provided detailed notes regarding the technical and policy options available to registry operators regarding fast-flux hosting. The RyC statement includes technical notes about how the DNS functions, the data available to registry operators, fast-flux detection methods, uses of short TTLs, and other pertinent items. The RyC's answers to question 3 at line 936 [THIS REFERENCE WILL HAVE TO BE UPDATED AS THE DOC GETS EDITED] and question 7 from 1008 to 1252 [THIS REFERENCE WILL HAVE TO BE UPDATED AS THE DOC GETS EDITED] are of interest. ----- Rationale: Rather than leaving question 5.3 blank, I suggest the following text, which points to some useful (and factual) technical info.


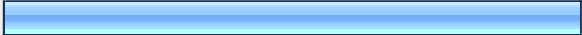

		Response Percent	Response Count
Agree		75.0%	9
Do not agree		16.7%	2
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			0
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

37. Proposals 22 - Line 370-- Question 5.4 'Are registrars involved in fast flux hosting activities? If so, how? Answering this question should be deferred until there is; a robust technical and process definition of "Fast Flux", there are reliable techniques to detect Fast Flux enhanced networks while avoiding false positives, there is reliable information as to the scope and penetration of Fast Flux networks and, there is reliable information as to the financial and non-financial impact of these networks.

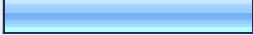


		Response Percent	Response Count
Agree		33.3%	4
Do not agree		58.3%	7
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			1
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>



38. Proposal 23 - Line 372-- Question 5.5 'How are registrants affected by fast flux hosting?' Answering this question should be deferred until there is; a robust technical and process definition of "Fast Flux", there are reliable techniques to detect Fast Flux enhanced networks while avoiding false positives, there is reliable information as to the scope and penetration of Fast Flux networks and, there is reliable information as to the financial and non-financial impact of these networks.

		Response Percent	Response Count
Agree		27.3%	3
<b>Do not agree</b>		<b>63.6%</b>	7
Alternative view		0.0%	0
No strong view either way		9.1%	1
Comments			1
<b>answered question</b>			<b>11</b>
<b>skipped question</b>			<b>3</b>

39. Proposal 24 - Line 374-- Question 5.6 'How are Internet users affected by fast flux hosting?' Answering this question should be deferred until there is; a robust technical and process definition of "Fast Flux", there are reliable techniques to detect Fast Flux enhanced networks while avoiding false positives, there is reliable information as to the scope and penetration of Fast Flux networks and, there is reliable information as to the financial and non-financial impact of these networks.

		Response Percent	Response Count
Agree		27.3%	3
<b>Do not agree</b>		<b>63.6%</b>	7
Alternative view		0.0%	0
No strong view either way		9.1%	1
Comments			2
<b>answered question</b>			<b>11</b>
<b>skipped question</b>			<b>3</b>


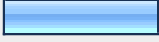

40. Proposal 25 - Lines 398 - 416 [Specific text to be provided] ----- Rationale: I'd like to see a little more in the "Information Sharing" section. Specifically something like saying that the publishing of the non-private information through DNS might be useful to assist in detecting and blocking spam that is promoting domains used in a fast flux fraud scheme. I think it's important to say why this information should be published through DNS. Additionally it should be noted that the reason for using DNS rather than WHOIS is for high real time query speed for those who would say, "Why use DNS when WHOIS is already there." Also - unless this already exists. Is there a way to determine the registrar of a domain through a DNS query? If there is I'd like to know it. If not then that is one of the fields I'd like to be able to look up through a DNS query. You might also mention that this information might also be useful for abuse reporting so that those who detect a problem can alert those who can deal with the problem.

		Response Percent	Response Count
Agree		16.7%	2
Do not agree		33.3%	4
Alternative view		0.0%	0
No strong view either way		50.0%	6
Comments			3
<i>answered question</i>			12
<i>skipped question</i>			2




41. Proposal 27 - I would also propose adding after line 411 text clarifying that: The DNS-based zone envisioned under this section need not be offered by ICANN itself, nor the registries or registrars. Rather, private entities, given bulk access to the required data, might offer that data via DNS or another mechanism in the public interest. ICANN, the registries and the registrars need only provide bulk access to the required data already available through whois (albeit currently available only at ad hoc low query volume levels). ----- Rationale: Some have expressed concern that dealing with fastflux might impose burdensome new obligations on ICANN, the registries or the registrars. It is thus important to clarify that coping with fast flux via an information-sharing-oriented approach need not impose material new burdens on those parties given the possibility of third parties massaging and arranging for re-dissemination of the data that may be required.

		Response Percent	Response Count
Agree		50.0%	6
Do not agree		25.0%	3
Alternative view		0.0%	0
No strong view either way		25.0%	3
Comments			2
<i>answered question</i>			12
<i>skipped question</i>			2


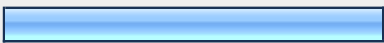

42. Proposal 30 - Line 429 replace: The ideas for active engagement that were discussed by the WG included the following, with The ideas for active engagement that were discussed by the WG included the following; the group did not reach consensus on or endorse any of them:

		Response Percent	Response Count
Agree		75.0%	9
Do not agree		16.7%	2
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			0
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

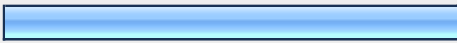
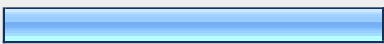

43. Proposal 31 - Line 446 – Add a bullet to the list of ideas: Allow the Internet community to mitigate fast-flux hosting in a way similar to how it addresses spam, phishing, pharming, malware, and other abuses that also take advantage of the DNS and Internet protocols."

		Response Percent	Response Count
Agree		58.3%	7
Do not agree		8.3%	1
Alternative view		0.0%	0
No strong view either way		33.3%	4
Comments			0
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

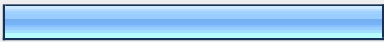
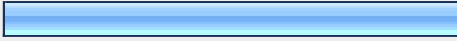

44. Proposal 32 - Line 456-- Question 5.8 'What would be the impact (positive or negative) of establishing limitations, guidelines, or restrictions on registrants, registrars and/or registries with respect to practices that enable or facilitate fast flux hosting?' Answering this question should be deferred until there is; a robust technical and process definition of "Fast Flux", there are reliable techniques to detect Fast Flux enhanced networks while avoiding false positives, there is reliable information as to the scope and penetration of Fast Flux networks, there is reliable information as to the financial and non-financial impact of these networks, there has been an assessment of need (based on the above) and, the requirements have been defined for proposed solutions.

		Response Percent	Response Count
Agree		50.0%	6
Do not agree		41.7%	5
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			1
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>


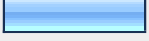
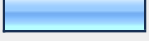
45. Proposal 33 - Line 460-- Question 5.9 'What would be the impact of these limitations guidelines, or restrictions to product and service innovation?' Answering this question should be deferred until there is; a robust technical and process definition of "Fast Flux", there are reliable techniques to detect Fast Flux enhanced networks while avoiding false positives, there is reliable information as to the scope and penetration of Fast Flux networks, there is reliable information as to the financial and non-financial impact of these networks, there has been an assessment of need (based on the above) and, the requirements have been defined for proposed solutions.

		Response Percent	Response Count
Agree		50.0%	6
Do not agree		41.7%	5
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			1
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

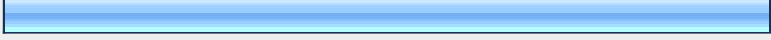


46. Proposal 34 - Line 463-- Question 5.10 'What are some of the best practices available with regard to protection from fast flux? Answering this question should be deferred until there is a robust technical and process definition of "Fast Flux".

		Response Percent	Response Count
Agree		41.7%	5
Do not agree		50.0%	6
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			1
<i>answered question</i>			12
<i>skipped question</i>			2




47. Proposal 35.1 - New version of chapter 6 incorporating proposals 36, 38, 39 and 40 (the proposed changes are underlined in the proposals document which is posted on the Wiki). 6 Constituency Statements and other View Points This section summarizes issues and aspects of fast flux reflected in the statements from the GNSO constituencies and individual Working Group members. To date, two Constituency statements (Registry Constituency and Non-Commercial Users Constituency), one input document (from individual Registrar Constituency members) and one initial reaction (Intellectual Property Interests Constituency) have been received. These entities are abbreviated in the text as follows (in the order of submission of the constituency statements): RyC - gTLD Registry Constituency IPC - Intellectual Property Interests Constituency NCUC - Non-Commercial Users Constituency Individual RC members – Individual Registrar Constituency members Annex A of this report contains the full text of those constituency statements that have been submitted. These should be read in their entirety. In addition, a number of individual statements have been submitted which can be found in Annex IV of the report. While the contributions vary considerably as to themes covered and highlighted, the following section attempts to summarize key views on fast flux. 4.1 Constituency and Other Views The Ryc, NCUC and a number of individual RC members all recognise that fast flux is being used by miscreants involved in online crime to evade detection, but at the same time question whether ICANN is the appropriate body to deal with this issue. All three emphasise that it is not in ICANN’s remit to act as an extension of law enforcement or put registries or registrars in this position. At the same time, some members of the Working Group suggest that ICANN, the registries and registrars are not being asked to act as an extension of law enforcement, but rather to facilitate compliance with existing laws and regulation in those cases where ICANN, the registries and registrars are uniquely situated to do so. In addition, the RyC, NCUC and a number of individual RC members are concerned that potential solutions for fast flux would prohibit current legitimate uses while at the same time online criminals would simply move on to another technique or method to avoid detection. The NCUC expresses specific concern in relation to the legitimate use of fast flux in facilitating anonymous speech. The RyC also points out that “the cessation of fast-flux could impede the creation of new and legitimate services on the internet”. Furthermore, the RyC points out that any GNSO policy initiative would have very limited impact as it would “only be applicable to gTLD registries and registrars, while ccTLD domain names are also used for fast flux hosting, which compromise almost half of the domain names on the Internet”. ICANN policy could then simply be circumvented by switching to ccTLD domain names. The counter argument from some members of the Working Group is that while the GNSO is not responsible for administrating ccTLD policy, by showing leadership in administration of gTLD domain policies (including policies dealing with fast flux), GNSO actions may indirectly influence the ccTLD policy development process. The RyC, NCUC and a number of individual RC members all point to the lack of data and the absence of supporting evidence outlining the scope of fast flux which is a necessity in order to balance cost – benefits of any potential solutions. The RyC and a number of individual RC members specifically point to any lack of evidence that “fast flux hosting has materially impacted the interoperability, technical reliability and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet”. At least one participant in the Working Group notes that substantial data was offered to the Working Group, both with respect to fast

		Response Percent	Response Count
Agree		69.2%	9
Do not agree		15.4%	2
Alternative views		0.0%	0
No strong view either way		15.4%	2
Comments			2
<b>answered question</b>			<b>13</b>
<b>skipped question</b>			<b>1</b>

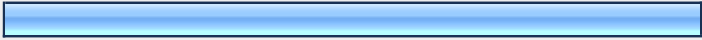
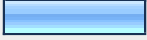
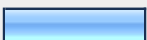
**48. Proposal 37 - Line 492 - Replace: "simply move on to another technique or method to avoid detection" with "simply move on to another technique or method, or would change their implementations, to avoid detection or mitigation efforts."**

		Response Percent	Response Count
Agree		84.6%	11
Do not agree		7.7%	1
Alternative view		0.0%	0
No strong view either way		7.7%	1
Comments			0
<b>answered question</b>			<b>13</b>
<b>skipped question</b>			<b>1</b>

49. Proposal 41 - Lines 567-572 on PDF page 24 reads: "b. Misconceptions about the scope of a PDP and remit of ICANN [Text to be provided] ----- Rationale: Following that text, I would request that we add a pointer to the Affilias Abuse Funnel Request document mentioned by Greg Aaron at <http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00285.html> as an example of how at least one TLD has successfully addressed \*precisely\* the issue our WG faced. Somehow in just two pages Affilias managed to (a) explain why abusive use of domain names is an important issue, (b) define fast flux (see pp. 2 of [www.icann.org/en/registries/rsep/afilias-abuse-funnel-request-rev-03jul08.pdf](http://www.icann.org/en/registries/rsep/afilias-abuse-funnel-request-rev-03jul08.pdf) ) and (c) forbid it unless usage has received prior permission, and (d) they even described what can/should be done (see the last two paragraphs of that page). Seems like the whole package to me. If nothing else, one possible solution would be to adopt the Affilias abuse funnel request as a foundation or model for moving forward with the gTLD fastflux discussion. Additional comment received by Greg Aaron: Speaking as one responsible for the Afilias (one "f") policy: Afilias is a private actor that is acting within a set of contractual obligations and limitations. Not all parties are similarly situated. Also, Afilias acted in this fashion in a volunteer fashion, and proposed a terms of service that it was right for it. However, there is not a one-size-fits-all solution that should be forced upon parties. One thing some parties are concerned about is being forced by ICANN to do things in a certain way. ICANN is not in a good position to dictate policies, procedures, and associated costs of this nature.

		Response Percent	Response Count
Agree		75.0%	9
Do not agree		25.0%	3
Alternative view		0.0%	0
No strong view either way		8.3%	1
Comments			3
<b>answered question</b>			<b>12</b>
<b>skipped question</b>			<b>2</b>

50. Proposal 42 - Proposed text for section 8.1 – lines 597-609 During the study of fast flux hosting, the working group quickly came to appreciate that the subject area that originally formed the basis of the study had changed rapidly in the from the time of publication of the SSAC report that stimulated GNSO interest to the issuance of the PDP. Flux hosting, flux techniques and flux facilitated attacks continued to evolve even during the WG’s study period. This section attempts to draw conclusions from a study that can in some respect be characterized as having placed the WG in the losing end of a race condition: simply put, the WG was at a disadvantage having been assigned the task of studying a moving target. 8.1 Conclusions Fast flux hosting has numerous applications. Some experts have focused on the applications of fast flux hosting that are self-beneficial but publicly detrimental and consider it to be an effective technique for keeping fraudulent sites active on the Internet for the longest period of time, and it requires domain registrations as a component for success. At the same time, a number of many of the characteristics that experts ascribe to fast flux hosting have been identified as self-beneficial without being harmful to others, or indeed, both self- and publicly beneficial. In these latter applications, the goals of fast flux hosting are to make networks survivable or highly reliable, but the motives are quite different. Gaining a common appreciation and broad understanding of the motivations behind the employment of fast flux or adaptive networking techniques proved to be a particularly thorny problem for the WG. Attempts to associate an intent other than criminal and characterizing fast flux hosting as legitimate or illegal, good or bad, stimulated considerable debate, as such labels are highly subjective in certain situations. Study by members of the WG also revealed that flux hosting is necessarily, accurately characterized as “fast flux” but more generally, that flux hosting encompasses several variations and adaptations of event-sensitive, responsive, or volatile networking techniques. The WG studied many of the methods of detecting fast flux activities and thwarting fast flux hosting required participation and intervention. The WG also studied whether certain data could be monitored, collected, and made available by various parties (e.g., registries, registrars, and ISPs) to facilitate detection and intervention in circumstances where fast flux hosting was publicly detrimental. These studies merit further attention, particularly in areas where an unacceptable level of false positives would prove detrimental to registrants affected by intervention and where measures are needed to ensure that parties reporting fast flux activity are provably trustworthy. The WG also acknowledges that fast flux and similar techniques are merely components in the larger issue of internet fraud and abuse. The techniques described in this report (and others yet to be revealed) are only part of a vast and constantly evolving toolkit for attackers: none of the techniques are necessary to the degree that mitigating any one would eliminate Internet fraud and abuse. Every attack that is enhanced by the use of one or more fast flux techniques could be pursued without them, possibly at higher cost or effort for the attacker. These various and highly interrelated issues must all be taken into account in any potential policy development process and/or next steps. Careful consideration will need to be given as to which role ICANN can and should play in this process.

		Response Percent	Response Count
Agree		76.9%	10
Do not agree		15.4%	2
Alternative view		0.0%	0
No strong view either way		15.4%	2
Comments			1
<b>answered question</b>			<b>13</b>
<b>skipped question</b>			<b>1</b>