**Summary of Public Comments on the Fast Flux Hosting Initial Report**

*This summary is not a full and complete recitation of the comments received. It is an attempt to capture in broad terms the nature and scope of the comments. This summary has been prepared in an effort to highlight key elements of these submissions in an abbreviated format, not to replace them. Every effort has been made to avoid mischaracterizations and to present fairly the views provided. Any failure to do so is unintentional. The comments may be viewed in their entirety at http://forum.icann.org/lists/fast-flux-initial-report/.*

Summary and analysis of public comments for:

Fast Flux Hosting (Initial Report)

Comment period ended: 15 February 2009

Summary published: 18 February 2009

Prepared by: Marika Konings, Policy Director

*Background*

In May 2008, the GNSO Council initiated a Policy Development Process (PDP) and called for the creation of a working group on fast flux. The working group was asked to consider a number of questions relating to fast flux. The Fast Flux Working Group started its deliberations in June 2008 and published an Initial Report. In this report, the Working Group provided initial answers to the charter questions, drew interim conclusions and provided a number of ideas for possible next steps. The public comment period was created to solicit feedback from the Internet community on the Fast Flux Hosting Initial Report.

*Summary and Analysis*

The comment period ran from 26 January to 15 February 2009. Twenty-five comments were received, including two from GNSO Constituencies. The public comments on this forum are archived at http://forum.icann.org/lists/fast-flux-initial-report/.

The relevant comments below are listed in the order they were received.

Michael Brusletten (Spacesquad AntiSpam Services): Brusletten notes that 'fast flux hosting needs to have strict laws put in place to allow registrars and hosting companies to terminate the offenders that that try to use these schemes'. He adds that fast flux hosting is not only used by criminals to distribute spam, but also for the distribution of malware and computer viruses. He understands 'the problems and complexities of shutting [criminals] down', but notes that 'registrars and hosting companies are in the unique position to get this done'. He fears that if no measures are put in place to address fast flux hosting, 'it will just continue to get worse'.

Bill Woodcock (Packet Clearing House): Woodcock comments on behalf of Packet Clearing House which 'is a not-for-profit global authoritative DNS infrastructure provider to nearly sixty top-level domains, operating servers on six continents'. In his comments he raises a point that he feels the report has not taken into account: the increased use of fast flux hosting 'has led to a radical change of paradigm in the distribution of DNS record changes from registries to their authoritative nameservers.

Whereas the majority of registries used to publish zone updates on, at most, a daily basis, many now flood the network with a constant stream of updates, and consider propagation delays of more than a few seconds problematic'. He notes that this development has 'worsened the digital divide' on two fronts:

- 'First, accepting this flood of illegitimate changes poses a cost in Internet bandwith, and ultimately money, to anyone who would spread authoritative nameserves among development countries'. In addition, 'because it floods constricted circuits, it can cause incremental zone transfer processes to fail, taking servers offline for hours or days at a time'.
- Secondly, Registry Service Level Agreements (SLAs) 'catering to the fast-flux market now promise that DNS servers will be purposely removed from service if they're unable to keep up with, or lose connectivity from, the flood of fast-flux changes. […] Countries that suffer incidents of national disconnection are usually those already laboring under the heaviest burdens: Pakistan, Sri Lanka, and Zimbabwe, for example'.

Woodcock concludes that 'these are significant degradations of the quality of service offered by the domain name system, and they disproportionately and unfairly burden those who already find themselves on the wrong side of the digital divide'.

R Atkinson (individual): Atkinson notes that the Fast Flux Initial report fails to recognize a number of 'legitimate uses for DNS records with very low TTL values' such as mobility support (short TTL values for the DNS A/PTR) or renumbering of a network (short TTL values for A/PTR, MX/KK/other DNS records). He recommends that a clearer distinction is made in the report between 'legitimate reasons to have DNS records with low TTL values [and] cases where a particular DNS record type has a low TTL value for no obvious reason'. In his comment he provides a number of links to papers on the use of DNS for Internet mobility and notes that active research in this area is undertaken by a number of groups (examples of current research projects are referenced). He recommends that the report be reviewed by the relevant IETF WGs as 'it is important to ensure that not only current DNS-related specifications and deployments, but also emerging and anticipated DNS-related specifications and deployments, are fully taken into account in the report'.

Ed (individual): Ed comments that he does not think 'fast flux technology should be banned, or any other technology for that matter'. He notes that a fair balance needs to exist between privacy / freedom on the one hand and public safety / regulation on the other, which might not always be easy. In his view, the root cause of the problem is 'un-patched computers connected to the internet' and 'criminal behaviour'. Ed proposes the following solutions for consideration to address the former: 'banning the ip of infected pc's […]; put some responsibility of internet control back to the ISP level; time delay between registrations and activation [which could be avoided by] registering in person and providing photo ID and biometric data; and, forced updates […] where a security patch is applied'.

Ben Gelbart (Spacequad AntiSpam Services): Gelbart notes that fast flux hosting is a 'very serious problem'. He comments that there are two ways in which registries and registrars can restrict fast flux:

1) 'By monitoring DNS activity […] and reporting suspicious behavior to law enforcement or other appropriate reporting mechanism.'
2) 'By adopting measures that make fast flux either harder to perform or unattractive. Some possible measures that have been suggested include:
    - authenticating contacts before permitting changes to NS records;
    - preventing automated NS record changes;
    - enforcing a minimum time to live (TTL) for name query responses;

- limiting the number of name servers that can be defined for a given domain.'

Claus von Wolfhausen (UCEPROTECT-Network): Von Wolfhausen comments that 'there is no legitimate purpose that requires one site to use hundreds of hosts and have DNS changing with records'.

Steven Chamberlain (individual): Chamberlain comments that in his view 'it is wrong and ultimately futile to restrict the use of fast flux as a way to counter' malware, phishing and hosting of illegal content. In addition, he notes that there are numerous legitimate fast flux domains that benefit from this technique to increase speed, facilitate load balancing and enhance reliability. He notes that there are 'viable methods for disabling domains without penalising legitimate users of fast flux techniques, and without imposing any new restrictions on domain registration' such as blacklisting of domain names that are known to host malware or illegal content, or are used for phishing. He suggests that the date for such a blacklist(s) 'can be compiled and published by government or law-enforcement agencies, security researchers or private individuals'. A way to disable those domains included in these blacklists would be to 'remove their records from all authoritative root servers worldwide' or 'ISPs could make use of the blacklist data'. Chamberlain describes a number of techniques that can be used by ISPs to filter such domains and notes that these techniques could also be applied in corporate environments, educational establishments, other providers of Internet access and individuals.

RAS (individual): RAS states that he works for an ISP and deals with fast flux domains and other internet abuse issues on a daily basis. In his view there are 'enough valid reasons for short TTL values' which should be a reason to avoid any policies that would hamper these legitimate uses. RAS notes that 'the best way to address this may be to start with registrars who are not able to quickly identify and take down these domains because they will typically not improve unless they are forced to'. He adds that registrars 'have created an environment that invites abuse' as they 'do not maintain staff and policies adequate to prevent [...] abuses from taking place'. He recommends that registrars undertake more due diligence when registering new domain names, even if this would bring along additional costs. In addition, he promotes that 'ICANN should take a more active role by encouraging, tracking, and publishing reports of registrars who are slow to act on abusive domains and should be more aggressive on dealing with registrars who generate large numbers of complaints'.

Richard Golodner (individual): Golodner recognizes that fast flux is a threat, but at the same time notes that it is a technique 'we all take advantage of'. He raises the question of 'what can be done at the domain registry level to make it more difficult […] for the bad guys to use Fast Flux as a means of continuing their criminal enterprises?'

Michael Holder (TRD Associates) – Holder notes that 'this is a case of blaming the network layer for inappropriate choices made for the session or application layers'. In his view the solution is 'to secure the applications with technology that is appropriate to the level of value and risk'.

Bonnie Chun (Hong Kong Internet Registration Corporation Limited) – Chun shares the experience of the .hk registry in dealing with fast flux domains and notes that the introduction of 'additional measures to stop criminals from registering .hk domain names for illegal use' and 'help of the local law enforcement agencies and the local CERT, brought the situation back under control. Based on this experience, the .hk

registry supports 'ICANN in formulating a best practice policy for domain registries / registrars and/or ISPs to fight against the use of fast flux in illegal activities'.

Davide Giuffrida (individual): Giuffrida welcomes the initiative to counter the abuse of fast flux technology by criminals. He notes that 'only a small part of fast-flux domains is legal' and promotes the listing of bad domains, those that abuse fast flux, which could be used to clean the network. Those domains using fast flux legitimately should be incorporated in a separate list.

Eric Brunner-Williams (Core): In his comments, Brunner-Williams refers to note he wrote while he was participating in the Fast Flux Working Group in which he made the following observations:

- 'The stated problem is only one in a larger space of evasion or resiliency techniques, some of which use the DNS'
- 'The stated problem exists in a larger context of technical infrastructure, only some of which are even remotely within the largest scope of technical coordination of ICANN's SOs'
- 'As a specific technique, it is an optimization of a resource utilization'
- 'The stated problem exists in an unstated relation to technical fundamentals'

He notes that the response to these observations at the time was that 'there is no relation between the techniques exploited for evasion or resiliency and the consequences of v4 address exhaustion, and the non-adoption of v6 addressing'. In addition his shares his views on the comments made by Woodcock, Atkinson, Chun and Holder. He concludes by pointing to his concerns over the process, SSAC, the Fast Flux WG and lack of technical participation which he notes have also been communicated to various bodies and individuals within ICANN.

Mauro (individual): Mauro shares his experience as a 'private citizen running [his] own web/mail servers on a dynamic IP range' as a result of which he has already experienced a number of problems such as the refusal of emails. He expresses his disagreement with the idea discussed in the report to charge a premium for dynamic name server domains as he believes that individual internet users should not 'have to pay the bill because a little part of user[s] are misusing the Internet'. From his experience as a cybercrime analyst, he notes the difficulty in take downs of fast flux domains explaining that in the case of .ch, domains cannot be taken down unless there is an order coming from a judge. In his view 'adopting accelerated domain suspension processing in collaboration with certified investigators / responders should be a must in the fight against fast flux domains'.

Jeffrey A. Williams (INEGroup): Williams expresses concerns that the views of his group are not reflected in the report. He disagrees with the inclusion of advocacy groups and free speech as benefitting from fast flux. He notes that the 'Initial report seems to be pushing down the actual responsibility from ICANN's accredited Registrars and Registries, down to Registrants which is partly justified, and ISP's, which is not justified [as they are not] the originator. He disagrees with the idea raised in the report to strengthen registrant verification and identification processes as way to mitigate fast flux as this would result in 'a reduction of privacy protection for Registrants'. He suggests that 'registrars […] need to build detecting mechanisms of a technical nature that will detect when Fast Flux of DNS is evident, and than generate a Email alert to CERT, other law enforcement agencies, contracted reporting agencies, and ICANN staff that this activity has been recognized'.

Philip Virgo (individual): Virgo uses the, in his view, slow progress made in addressing fast flux hosting as an example of the 'institutional failure at the heart of Internet Governance'.

Claudio DiGangi (IPC Constituency): DiGangi submits his comments on behalf of the Intellectual Property Constituency (IPC). The IPC is of the opinion that 'any steps that can be taken to identify and prevent the illegitimate use of Fast Flux hosting should be pursued'. The IPC recognizes the difficulties identified by the WG in separating legitimate use of fast flux from illegitimate, but wants to encourage the WG 'to continue its work and to work with others to identify, manage and overcome these challenges'. On the role of ICANN, the IPC notes that 'even if the involvement of third parties will be required to fully address the problems associated with the illegitimate use of Fast Flux, ICANN is in a position to protect the stability and integrity of the Internet by taking positive incremental steps towards resolving these issues (including by, at a minimum, gathering and disseminating information regarding Fast Flux hosting and developing best practices for registries and registrars)'. The IPC expresses its agreement with the conclusion of the WG that further work is required in a number of areas, and recommends that such work should be conducted before the issuance of a final report. In addition, the IPC provides comments on each of the charter questions addressed by the WG in the Initial Report. In relation to question 1, who benefits from fast flux, and who is harmed, the IPC notes that 'in order to establish the extend of the harm […] further study is needed (especially regarding piracy activities resulting from Fast Flux activities)'. On question 2, who would benefit from cessation of the practice, and who would be harmed, the IPC states that 'the report fails […] to provide any empirical data to support the speculative list of benefits of fast flux hosting. To balance any arguable benefits of Fast Flux hosting against its adverse impacts to IP owners and the public, more study is needed to understand the rather speculative characterization of Fast Flux benefits and whether such benefits can be achieved in another manner'. On question 3, are registry operators involved or could they be in Fast Flux hosting activities, the IPC is of the opinion that 'the registry community is in a position to assist in mitigating problems arising as a result of the illegitimate use of Fast Flux hosting'. While acknowledging that other stakeholders might need to be involved, 'the IPC is of the view that taking even small steps may be effective in mitigating the harms caused by illegitimate uses of Fast Flux hosting'. In relation to question 4, are registrars involved in Fast Flux hosting activities, the IPC notes that although it agrees with the report's assessment that most registrars are not involved, it is concerned as 'registrar's responses and defensive mechanisms to Fast Flux activities appear to vary widely in substance and timeliness' which may result in 'certain registrars being increasingly targeted for Fast Flux activities'. On question 5, how are registrants affected by fast flux hosting, the IPC points to the risks for trademark owner registrants whose domain names might become a target for attackers looking for reputable domains, the possible consequences of blacklisting and suspension of a domain associated with a fast flux attack, and harm to a registrants trademark. On question 7, what technical measures should be implemented by Registries and Registrars to mitigate the negative effects of Fast Flux, the IPC 'strongly encourages the Working Group to further consider and develop the Information Sharing and Active Engagement measures outlined in the Initial Report'. In relation to question 8, what would be the impact of establishing limitations, guidelines, or restrictions on Registrants, Registrars, and/or Registries with respect to practices that enable or facilitate Fast Flux hosting, the IPC recognizes that it is difficult to assess the impact without knowing the exact measures, but is of the opinion that the benefits for affected registrants and internet users is likely to 'outweigh the identified harms to the Registrars and Registries in the Initial Report. On question 10, what are some of the best practices available with regard to protection from Fast Flux, the IPC 'encourages the Working Group to continue to investigate the APWG's proposed best practices' and 'encourages members of the registrar community to adopt recognized best practices designed to curtail the harms caused by illegitimate uses of Fast Flux hosting'.

Suresh Ramasubramanian (individual): Ramasubramanian notes that the legitimate uses of fast flux identified in the report do not have the same characteristics as the abusive use of fast flux. Legitimate uses of fast flux do not use hijacked bots, have full control over IP ownership data and do not use 'throwaway domains with fake whois contacts […] that are quite often bought with stolen cards'. He adds that 'the vast majority of fastflux is used for criminal purposes and is hosted on illegally acquired […] hosts'. He furthermore notes that registrars and registries 'are the single point of failure for dns based fastflux or double fast flux.

Jon Orbeton (PayPal): Orbeton's comments specifically relate to charter question 7, what technical changes and policy measures could be implemented by registries and registrars to mitigate the negative effects of fast flux. Orbeton notes that the following could, if implemented properly, 'significantly reduce the risk created by fast-flux networks':

- 'Make additional non-private information about registered domains available through DNS based queries;
- Publish summaries of unique complaint volumes by registrar, by TLD and by name server;
- Cooperative, community initiatives designed to facilitate data sharing and the identification of problematic domain names;
- Stronger registrant verification procedures;
- Adopt accelerated domain suspension processing in collaboration with certified investigators / responders'.

In addition, Orbeton encourages stronger conflict resolution measures to deal with 'registrars/IP space owners who are non-responsive to wide scale and numerous abuse complaints to ensure resolution of conflict' comparable to e.g. the UDRP. He implores 'ICANN to consider as a first step, rapid implementation of the suggestions already called out within [the] report along with the establishment of an Advisory Board on how to continually improve these suggestions'.

Gary Warner (University of Alabama): Warner is Director of Research in Computer Forensics at the University of Alabama. In relation to the question 'who benefits from fast flux', he questions whether free speech / advocacy groups belong on this list, as he has not seen any evidence of such groups. In addition, he notes that the only example provided in the report is a site that encourages violation of local law, which in his opinion should not belong in a free speech category condoned by ICANN. He does urge the group to add 'criminal entities' to the list of those who benefit from fast flux. To the question 'who would benefit from cessation', he proposes to add 'law enforcement and investigators' as cessation would facilitate catching the criminals. In response to the question 'are registrars involved', Warner states that 'there is strong evidence that registrars which operate "reseller practices" – particularly those registrars who are based in China and have resellers in St. Petersburg Russia – have resellers of their services which are entirely corrupt and who practice fast flux registration as a matter of course'. He also notes that sometimes criminals use a variety of registrars in different countries to establish their fast flux network which makes it difficult to investigate. On the question 'what measures could be implemented', Warner notes that 'one problem is convincing the registrars that they should do something about fast flux domains'. He recognizes the problem of proving the crime and notes that 'the problem of breaking up a particular hosted domain does not necessarily address the issue of the underlying infrastructure'. In relation to the impact of establishing limitations, he notes that establishing a fee for modification of name servers would not be a disincentive as in most of these cases stolen credit cards are used. With regard to targeting short TTLs, he disagrees with this approach as there are 'many possible reasons for short TTLs', but adds that it would be appropriate to use it as a basis for further investigation e.g. by centrally archiving

short TTL domains that could be used to verify against complaints received about domains on this list which should then be terminated. In relation to reporting to law enforcement, Warner notes that law enforcement will be more interested to learn about the fast flux hosting infrastructures than individual domain names, while at the same time highlighting the importance of information sharing. Warner welcomes the fast flux data metrics and remarks that 'tying those domains to spam […] may provide a more useful picture'. In addition, Warner offers to share supporting data from a paper that is currently being authored with the Working Group on 'which netblocks are most commonly associated with high volume spam attacks'.

Clarke D. Walton (Registrar Constituency): Walton submits his comments on behalf of the Registrar Constituency (RC). The RC notes that the comments 'capture the overall sentiment expressed by the RC Members', but 'due to time constraints […] no formal vote […] was taken'. After reviewing the different ideas for next steps in the report, the RC 'strongly encourages the Council to explore other means to address the fast flux issues instead of initiating a Policy Development Process' which it does not consider suitable 'because of the rapidly evolving nature of fast flux, combined with the minimal effect new policy would likely have on Internet fraud and abuse'. In addition, the RC is of the opinion that other organizations are more suited to lead mitigation efforts in this area. However, should the Council decide to pursue a PDP in this area, the RC 'recommends that these next steps, as suggested by the WG, occur in the following order:

1) Further work/study to determine which solutions/recommendations are best addressed by best practices, industry solutions, or policy development. The RC prefers development of best practices and industry solutions with policy development reserved as a last resort.
2) Include flux hosting, flux techniques and flux facilitated attacks as part of the work now being done on registration abuse and take-down policies.
3) If the Council pursues policy development specifically for fast flux, the Council should redefine the issue and scope to address some of the problems encountered by the WG and to develop a narrower and more sharply focused charter. This can only be done by first following the WG advice on additional research and fact-finding to address the questions and issues raised in the Initial Report.'

Richard Clayton (University of Cambridge): Clayton is a security researcher in the Computer Laboratory of the University of Cambridge and has, amongst others, published a number of papers that examine the lifetime of phishing web sites and the factors that influence this lifetime. He states that he is 'deeply unimpressed' with the report. In his view the report does not describe the problem accurately; does not explain the roles of ICANN, registries and registrars; 'does not consider the issues abstractly enough, but narrowly concentrates on some aspects of current criminal behaviour'; and, does not provide any hard data that details the scope of the problem nor how it has changed over time. In short, he notes that 'the report fails to provide any basis for policy development and short be completely reworked before any other actions are considered'. He notes that the report does not provide a general definition of fast flux, but instead resorts to provide a number of characteristics some of which are also relevant for legitimate uses of fast flux. He states that 'the specific distinguisher of a fast-flux attack is that the dynamic nature of the DNS is exploited so that if a website is to be suppressed then it is essential to prevent the hostname resolving, rather than attempting to stop the website being hosted'. Taking this into account, he notes that 'there are no technical ways to proceed which are effective and avoid collateral damage', the only option is to suspend the domain names. In view of this conclusion, Clayton argues that more attention needs to be paid to the role of ICANN, the registries and registrars in the suspension of domain names, 'with

ICANN having a role in promoting consistent standards and contractual arrangements'. He agrees that 'the difficulty that needs to be addressed is to establish when it is appropriate to suspend a domain name' and recommends that 'establishing guidelines and principles […] and arranging compensation for any innocent domains caught in the cross-fire, would be a useful role for an ICANN report'. In relation to some of the technical suggestions made in the report, Clayton puts forward insights as to why 'they all tackle the symptoms rather than the disease'. Clayton shares some recent data comparing the removal time for ordinary phishing websites and fast-flux sites from which he concludes that 'fast-flux hosting is prolonging website lifetimes, but the situation is not getting worse, and there are signs of it getting a little better'. In his overall conclusions, Clayton notes that 'the bottom line on fast-flux today is that it is almost entirely associated with a handful of particular botnets, and a small number of criminal gangs. Law enforcement action to tackle these would avoid a further need for ICANN consideration. […] If ICANN are determined to deal with this issue […] attention should be paid instead [of to the technical issues] to the process issues involved, and the minimal standards of behaviour to be expected of registries, registrars, and those investigators who are seeking to have domain names suspended'.

K Claffy (individual): Claffy argues that the claim that it is not possible to separate legitimate use of fast flux from illegitimate use 'only holds on paper'. In her view, 'there are so many measurable differences' that it should not be difficult to separate one from the other, as long as safeguards are built in such as whitelisting that would address any possible false positives. She concludes that this report and the way it outlines potential concerns in dealing with this issue are 'excellent steps forward'.

Alan Murphy (Spamhaus Project Team): Murphy commends the efforts made by the WG in this report. One of the suggestions he makes is that additional information is provided on how to separate legitimate use of fast flux from illegitimate. He expresses his hope that 'ICANN considers [the report] to be a starting point for implementing policies designed to inhibit the illicit use of fast flux hosting'. He adds that 'both for ICANN-dependent entities, but also for ccTLDs and others which are not beholden to ICANN, ICANN is in an excellent position to provide leadership and guidance in developing policies and guidelines to distinguish good and bad use of the Internet'.
Philip Virgo (individual): In a follow up comment, Virgo observes that there is 'confusion, including over the way that the "supply chain" for domain names actually works in practice, as opposed to theory" and suggest therefore that "a group be set up to facilitate the exchange of information on the conditions of service of registries and registrars and how these work in practice'.

*Next Steps*

The comments received will be analyzed and used for redrafting of the Initial Report into a Final Report to be considered by the GNSO Council for further action.

*Contributors*

Contributors are in order of first appearance and number of postings if more than one:

Michael Brusletten, Spacequad AntiSpam Services
Bill Woodcock, Packet Clearing House
R Atkinson
Ed

Ben Gelbart, Spacequad AntiSpam Services
Claus von Wolfhausen, UCEPROTECT-Network
Steven Chamberlain
RAS
Richard Golodner
Michael Holder, TRD Associates
Bonnie Chun, Hong Kong Internet Registration Corporation Limited
Davide Giuffrida
Eric Brunner-Williams, CORE
Mauro
Jeffrey A. Williams, INEGroup
Philip Virgo (two postings)
Claudio DiGangi, Intellectual Property Constituency
Suresh Ramasubramanian
Jon Orbeton, PayPal
Gary Warner, University of Alabama
Clarke D. Walton, Registrar Constituency
Richard Clayton, Computer Laboratory, University of Cambridge
K Claffy
Alan Murphy, Spamhaus Project Team