Fast Flux Hosting Public Comments				
Categories	**Concerns**	**Who**	**View of the WG**	**If/How/Where to incorporate in Final Report**
1. Legitimate vs. Illegitimate use of Fast				
1.a	A clearer distinction needs to be made between legitimate reasons to have DNS records with low TTL values and those with low TTL value for no obvious reason	R Atkinson	Proposed approach by Dave: One comment focuses on beneficial uses of short TTLs. I think this is valid and would suggest we incorporate his specific comments regarding mobile applications in the appropriate section. I will work with Marika to capture the essence of Ran's comments and incorporate them into the document. I'll post to list, hopefully later this week. A second comment is that we did not carefully distinguish between beneficial uses of adaptive/volatile networking techniques (e.g. Short TTLs) and fast flux attack networks. As I said on the call, I think we need to explain how the WG formulated/refined what characterizes FF attack networks but elected to answer the questions as formulated by the GNSO counsel. I hope this can be done in 1-2 paragraphs and again, I'll post to list for review. I'll also compose a letter inviting the IETF mobility WG to comment on the report and ask that they do so by, say 21 May 2009? Avri, please send me the chair's email since you've already looked it up:-0	Proposed text to be incorporated in draft final report for review

1.b	There is no legitimate purpose that requires one site to use hundreds of hosts and have DNS changing with records	Claus von Wolfhausen	Has been addressed and captured in the report, see e.g. pages 17 and 18	
1.c	There are enough valid reasons for short TTL values	RAS	Has been addressed and captured in the report, see e.g. pages 17 and 18	
1.d	Fast flux is a threat, but at the same time a technique we all take advantage off	Richard Golodner	Has been addressed and captured in the report, see e.g. pages 17 and 18	
1.e	Only a small part of fast flux domains is legal	Davide Giuffrida	Commenter also proposes a mechanism for real time assessment of FF domains to determine whether a domain is 'good' or 'bad' - Such a system is used by some registrars as described on page 36. In addition, as part of the possible next steps, the idea of a Fast Flux Data Reporting System was included on page 54.	
1.f	Legitimate users of fast flux should not have to pay the bill because a little part of users are misusing fast flux.	Mauro	Has been addressed and captured in the report, see e.g. pages [references to be provided]	
1.g	There are many possible reasons for short TTLs, but it would be appropriate to use it as a basis for further investigation e.g. by centrally archiving short TTL domains and verify those against complaints	Gary Warner	Has been addressed and captured in the report, see e.g. pages 17 and 18	

1.h	There are so many measureable differences that it should not be difficult to separate legitimate from illegitimate behaviour, as long as safeguards are built in such as whitelisting that would address any possible false positives.	K Claffy	Contact K Claffy to obtain input on how a mechanism to separate legitimate and illegitimate use of FF could be developed	
1.i	Additional information should be provided on how to separate legitimate use of fast flux from illegitimate	Alan Murphy	Has been addressed and captured in the report, see e.g. pages 17 and 18	
2. Negative Impact of Fast Flux on				
2.a	Fast flux hosting activities results in a significant degradation of the quality of service offered by the DNS which disproportionately and unfairly burden those who already find themselves on the wrong side of the digital divide	Bill Woodcock	To be added to section 5.2. on who is harmed by fast flux activities	Draft text included in section 5.2 (page 31) for review by WG
3. Fast Flux is not the problem			(Assigned to James)	
3.a	The root cause of the problem is unpatched computers connected to the Internet and criminal behaviour	Ed		
3.b	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	Steven Chamberlain		

3.c	This is a case of blaming the network layer for inappropriate choices made for the session or application layers	Michael Holder		
3.d	The stated problem is only one in a larger space of evasion or resiliency techniques, some of which use the DNS. As a specific technique, it is an optimization of a resource utilization.	Eric Brunner-Williams		
4. Ways in which registrars and registries can restrict Fast Flux			(Assigned to Rod / Dave)	
4.a	There need to be strict laws in place to allow registrars and hosting companies to terminate fast flux hosting	Michael Brusletten		
4.b	Monitoring DNS activity and reporting suspicious behavior to law enforcement or other appropriate reporting mechanism	Ben Gelbart		
4.c	Adopting measures that make fast flux either harder to perform or unattractive	Ben Gelbart		
4.d	Registrars should undertake more due diligence when registering new domain names. Registrars have created an environment that invites abuse as they do not maintain staff and policies adequeate to prevent abuses from taking place.	RAS		

4.e	Adopting accelerated domain suspension processing in collaboration with certified investigators / responders	Mauro		
4.f	Registrars need to build detecting mechanisms of a technical nature that will detect when fast flux is evident and then generate an email alert to CERT or law enforcement agencies, contracted reporting agencies and ICANN staff	Jeffrey A. Williams		
4.g	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	IPC Constituency		
4h	Encourage registrars to adopt recognized best practices designed to curtail the harms caused by illegitimate uses of fast flux hosting	IPC Constituency		
5. Definition of fast flux			(Assigned to James)	

5.a	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 attepting to stop the website being hosted	Richard Clayton		
5.b	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 often bought with stolen cards	Suresh Ramasubramanian		
6. Role of ICANN			(Assigned to Kal)	
6.a	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 number of complaints	RAS		
6.b	Formulating a best practicepolicy for domain registries / registrars and/or ISPs to fight against the use of fast flux in illegal activities	Bonnie Chun		
6.c	Gaterhing and disseminating information regarding fast flux hosting and developing best practices for registries and registrars	IPC Constituency		

6.d	ICANN should 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	Jon Orbeton		
6.e	Promoting consistent standards and contractual arrangements	Richard Clayton		
6.f	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	Richard Clayton		
6.g	To provide leadership and guidance in developng policies and guidelines to distinguish good and bad use of the Internet.	Alan Murphy		
7. Who is benefitting from fast flux?			(Assigned to Paul)	
7.a	Lack of evidence to include 'free speech' advocacy groups as benefitting from fast flux	Jeffrey A. Williams		
7.b	There is no evidence for the existence of ree speech /advocacy groups using fast flux	Gary Warner		
7.c	Criminal entities should be added to the list of those benefitting from fast flux	Gary Warner		
8. Who would benefit from cessation?			(Assigned to Paul)	

8.a	Law enforcement and investigators as cessation would facilitate catching the criminals	Gary Warner		
9. Next steps / Possible solutions				
9.a	Report to be reviewed by relevant IETF Working Groups	R Atkinson		
9.b	Need to continue work in this area despite difficulties encountered by the WG	IPC Constituenc y		
9.c	Ban IP of infected PC's, put some responsibility of internet control back to the ISP, time delay between registrations and activation, forced security updates	Ed		
9.d	There are viable methods for disabling domains without pelanising legitimate users of fast flux techniques, and without imposing any new restrictions on domain registration such as blacklisting and filtering of domain names tht are known to host malware or illegal content, or used for phishing	Steven Chamberlain		
9.e	Secure the applications with technology that is appropriate to the level of value and risk	Michael Holder		

9.f	Listing of bad domains, which could be used to clean the network. Those domains using fast flux legitimately should be incorporated in a separate list.	Davide Giuffrida		
9.g	Further study is needed in order to establish the extend of the harm	IPC Constituency		
9.h	More study is needed to understand the rather speculative characterization of fast flux benefits and whether such benefits can be achieved in another manner	IPC Constituency		
9.i	Consider further and develop the Information Sharing and Active Engagement measures outlined in the Initial Report	IPC Constituency		
9.j	Continue to investigate the APWG's proposed best practices	IPC Constituency		
9.k	Make additional non-private information about registered domains available through DNS based queries	Jon Orbeton		
9.l	Publish summaries of unique complaint volumes by registrar, by TL and by name server	Jon Orbeton		
9.m	Cooperative, community initiatives designed to facilitate data sharing and the identification of problematic domain names	Jon Orbeton		

9.n	Stronger registrant verification procedures	Jon Orbeton		
9.o	Adopt accelerated domain suspension processing in collaboration with certified investigators / responders	Jon Orbeton		
9.p	Stronger conflict resolution measures to deal with registrars / IP space owners who are non-responsive to wide scale and numerous abuse complaints	Jon Orbeton		
9.q	Establishing a fee for modification of the name servers would not be a disincentive as in most of these cases stolen credit cards are used	Gary Warner		
9.r	Explore other means to address fast flux issues instead of initiating a PDP which is not 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	Registrar Constituency		

9.s	If a PDP is pursued, the following next steps are in order of preference: 1) further work/study to determine which solutions / recommendations are best addressed by best practices, industry solutions or policy development, 2) include fast flux hosting as part of the work now being done on registration abuse and take-down policies, 3) redefine the issue and scope.	Registrar Constituency		
9.t	There are no technical ways to proceed which are effective and avoid collateral damage, the only option is to suspend domain names.	Richard Clayton		
9.u	More attention needs to be paid to the role of ICANN, the registries and registrars in the suspension of domain names	Richard Clayton		
9.v	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	Philip Virgo		