Initial Report of the

GNSO Fast Flux Hosting Working Group

STATUS OF THIS DOCUMENT

This is the Initial Report of the Working Group on fast flux hosting, for submission to the GNSO Council on 26 January 2009. A Final Report will be prepared following public comment.

SUMMARY

This report is submitted to the GNSO Council and posted for public comment as a required step in this GNSO Policy Development Process on Fast Flux Hosting.

TABLE OF CONTENTS

1 Executive summary

1.1. Background

- Following the publication of the SSAC Advisory on Fast Flux Hosting and DNS (SAC 025) in January 2008, the GNSO Council instructed ICANN staff on 6 March 2008 to prepare and Issues Report which 'shall consider the SAC Advisory [SAC 025], and shall outline potential next steps for GNSO policy development designed to mitigate the current ability for criminals to exploit the DNS via 'fast flux' IP or nameserver changes'.
- The issues report was published on 31 March 2008 and recommended "the GNSO sponsor further fact-finding and research concerning guidelines for industry best practices before considering whether or not to initiate a formal policy development process".
- At its 8 May 2008 meeting, the GNSO Council initiated a formal policy development process (PDP) and called for the creation of a working group on fast flux. The working group charter was approved on 29 May 2008 and asked the working group to consider the following questions:
  - Who benefits from fast flux, and who is harmed?
  - Who would benefit from cessation of the practice and who would be harmed?
  - Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?
  - Are registrars involved in fast flux hosting activities? If so, how?
  - How are registrants affected by fast flux hosting?
  - How are Internet users affected by fast flux hosting?
  - What technical (e.g. changes to the way in which DNS updates operate) and policy (e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior) measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?
  - 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?
  - What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?

- What are some of the best practices available with regard to protection from fast flux?

The Group was also tasked to obtain expert opinion, as appropriate, on which areas of fast flux are in scope and out of scope for GNSO policy making.

1.2. Approach taken by the Working Group

- The Fast Flux Working Group started its deliberations on 26 June 2008 and decided to start working on answering the charter questions in parallel to the preparation of constituency statements on this topic. In order to facilitate the feedback from the constituencies, a template was developed for responses (see Annex I). In addition to weekly conference calls, extensive dialogue occurred through the fast flux mailing list with over 800 messages posted.
- Except where marked differently, the positions outlined in this document should be considered in agreement by the Working Group. Where no broad agreement could be reached, the following labels have been used to indicate the level of support for a certain position:
  - Support – there is some gathering of positive opinion, but competing positions may exist and broad agreement has not been reached.
  - Alternative view – a differing opinion that has been expressed, without garnering enough following within the WG to merit the notion of either Support or Agreement. It should be noted that an alternative view could be expressed where there is broad agreement as well as support.

1.3. Discussion of Charter Questions

- A fast flux attack network, for the purposes of the working group exhibits the following characteristics:
  - Some but not necessarily all of the network nodes are operated on compromised hosts (i.e., using software that was installed on hosts without notice or consent to the system operator/owner);
  - Is ‘volatile’ in the sense that the active nodes of the network change in order to sustain the network’s lifetime, facilitate the spread of the network software components, and to conduct other attacks; and
  - Uses a variety of techniques to achieve volatility including:

    - rapid and repeated selection of systems from a pool of botted hosts, with those systems being used for the purpose of serving malicious content, for use as name servers, and for other purposes, all via DNS entries with low TTLs;
    - dispersing network nodes across a wide number of consumer grade autonomous systems;
    - monitoring member nodes to determine/conclude that a host has been identified and shut down; and
    - time, or other metric-based, topology changes to network nodes, name server, proxy targets or other components.

  Additional characteristics that in combination or collectively have been used to distinguish or "fingerprint" a fast flux hosting attack include:

    - multiple IPs per NS spanning multiple ASNs,
    - frequent NS changes,
    - in-addrs.arpa or IPs lying within consumer broadband allocation blocks,
    - domain name age,
    - poor quality WHOIS,
    - determination that the nginx proxy is running on the addressed machine: nginx is commonly used to hide/proxy illegal web servers,
    - the domain name is one of possibly many domain names under the name of a registrant whose domain administration account has been compromised, and the attacker has altered domain name information without authorization.

- The distribution and use of software installed on hosts without notice to or consent of the system operator/owner is a critically important characteristic of a fast flux attack network; in particular, it is one among several characteristics that distinguish fast flux attack networks from production uses of fast flux techniques in applications such as content distribution networking, high availability and resilient networking, etc.
- When used by criminals, the main goal of fast-flux hosting is to prolong the period of time during which the attack continues to be effective. It is not an attack itself – it is a way for an attacker to avoid detection and frustrate the response to the attack.
- The WG offers the following initial working answers to the charter questions but would like to emphasize that continued work is required in the following areas:
  - A robust technical, and process, definition of "fast flux",
  - Reliable techniques to detect fast flux networks while maintaining an acceptable rate of false positives,

- Reliable information as to the scope and penetration of fast flux networks,
- Reliable information as to the financial and non-financial impact of fast flux networks

- Charter Questions:

1. Who benefits from fast flux, and who is harmed?

Who benefits from fast flux?

- Organizations that operate highly targetable networks
- Content distribution networks
- Free speech / advocacy groups

Who is harmed by fast flux activities?

- The working group noted that harm could arise both from legitimate and malicious uses of fast flux techniques, and WG members found it difficult during their discussions to maintain a clear distinction between harms that arise directly from the techniques themselves and harms that arise from the malicious behavior of “bad actors” who may use fast flux as one of many techniques to avoid detection.
- The WG did not reach consensus concerning the separately identifiable culpability of fast flux hosting with respect to the harm caused by malicious behavior, but it does recognize the way in which fast flux techniques are used to prolong an attack.

2. Who would benefit from cessation of the practice and who would be harmed?

The parties who benefit from cessation of the practice are the same as those who are harmed when fast flux is used in support of fast flux attack networks. The WG focused its attention therefore on identifying those harmed.

- Individuals whose computers are infected by attackers and subsequently used to host facilities in a fast flux attack network.
- Businesses and organizations whose computers are infected and subsequently are to host facilities in a fast flux attack network.
- Individuals who receive phishing emails and are lured to a phishing sited hosted on a fast flux attack network may have their identities stolen or suffer financial loss from credit card, securities or bank fraud.

- Internet service providers are harmed when their IP address blocks and their domain names are associated with fast flux attack networks. An ISP may also incur the cost of diverting staff and resources to monitor and address abuse.
- The reputation of a registrar may be harmed when its registration and DNS hosting services are used to facilitate fast flux attack networks that employ “double flux” techniques. A registrar may also incur the cost of diverting staff and resources to monitor and address abuse.
- Businesses and organizations who are phished from bogus web sites hosted on fast flux attack networks.
- Individuals or business whose lives or livelihoods are affected by the illegal activities abetted through fast flux attack networks.
- Registries may incur the cost of diverting staff and resources to monitor and address abuse.

Who benefits from the use of fast flux techniques?

- Organizations that operate highly targetable networks
- Content distribution networks
- Organizations that provide channels for free speech, minority advocacies or revolutionary thinking
- Criminals, terrorists, and generally, any organization that operates a fast flux attack network

The WG recognizes that future uses of this technology may be developed and that, as a result, it is impossible to list all possible beneficial uses of this technology.

3. <u>Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?</u>

In its Constituency statement, the Registry Constituency provides detailed notes regarding the technical and policy options available to registry operators regarding fast flux hosting (see Annex III).

4. Are registrars involved in fast flux hosting activities? If so, how?

- Most registrars are not involved in fast flux or double-flux
- Of the registrars where fast flux domains are registered by miscreants, the vast majority are unwitting participants in the schemes
- Some registrars and more often resellers of registrar services have the appearance of facilitation of fast flux domain attacks.
- No registrar has been prosecuted for facilitating criminal activities related to fast flux domains, but there have been reports linking one ICANN-accredited registrar to a large number of fraudulent domains including fast flux domains.

In addition, the report describes a number of known attack vectors as well as counter measures.

5. How are registrants affected by fast flux hosting?

Registrants are targets for fast flux attackers who seek domain names they can use to facilitate double flux attacks. Attackers are attracted by to existing domains that have a positive reputation over newly registered domains as age and history have become factors investigators consider as they attempt to determine whether a domain is associated with fast flux attacks.

6. How are Internet users affected by fast flux hosting?

Internet users provide both the raw material that fast flux hosting runs on (malware-compromised broadband – connected consumer PCs), while also serving as the target audience for spamvertised web sites which fast flux enables.

7. What technical (e.g. changes to the way in which DNS updates operate) and policy (e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior) measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?

The WG wishes to emphasize that fast flux needs better definition and more research. The ideas are presented here as a draft, to record incremental progress. The solutions fall into two categories based on the type of involvement expected of ICANN and its contracted or accredited parties (gTLD registries and registrars): those that would require only the availability of additional or more accurate information, which could be used (or not used) by other parties engaged in anti-fraud and related activities as they saw fit (information gathering); and those that would require or at least benefit from some degree of active participation by ICANN and/or registries and registrars to identify and deter fraudulent or other "malicious" behavior (active engagement).

- Information Gathering – information sharing proposals discussed included the following ideas:
    - 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;
    - Encourage ISPs to instrument their own networks;
    - Cooperative, community initiatives designed to facilitate data sharing and the identification of problematic domain names.
- Active Engagement – ideas for active engagement that were discussed included:
    - Adopt accelerated domain suspension processing in collaboration with certified investigators / responders;
    - Establish guidelines for the use of specific techniques such as very low TTL values;
    - Identify name servers as static or dynamic in domain registrations by the registrant;
    - Charge a nominal fee for changes to static name server IP addresses;
    - Allow the Internet community to mitigate fast-flux hosting in a way similar to how it addresses other abuses;
    - Stronger registrant verification procedures.

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?

Any attempt by the WG to answer this question is deferred until the next constituency statements and public comments, particularly requested on these points, have been received and reviewed by the WG.

9. What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?

Any attempt by the WG to answer this question is deferred until the next constituency statements and public comments, particularly requested on these points, have been received and reviewed by the WG.

10. What are some of the best practices available with regard to protection from fast flux?

One source of best practices for protection from fast flux can be found in the phishing world. The Anti-Phishing Working Group has recently released a best practices document for domain registrars in dealing with domain names registered by phishers ("Anti-Phishing Best Practices Recommendations for Registrars" http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf). Several of the practices outlined in that document apply directly or indirectly to dealing with fast flux domain names.

In addition, SAC 035 identifies mitigations methods certain registrars practice today in case where the registrar provides DNS for the customer's domains.

11. Obtain expert opinion, as appropriate, on which areas of fast flux are in scope and out of scope for GNSO policy making

Some members of the Working Group provided reasons as to why policy development to address fast flux is outside the scope of ICANN's remit, while others disagreed. The

Working Group's fact-finding and work on definitions documented how fast-flux involves domain name use issues, rather than domain name registration issues.

1.4. Challenges

Despite the fact that the Working Group conducted its work with great enthusiasm and dedication, it encountered a number of challenges which are outlined in chapter six such as the lack of an agreed upon definition of fast flux and supporting data, and, misconception about the scope of a PDP and remit of ICANN.

1.5. Interim Conclusions

- 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.
- Study by members of the WG revealed that fast flux hosting is necessarily, accurately characterized as "fast flux" but more generally, that fast flux hosting encompasses several variations and adaptations of event-sensitive, responsive, or volatile networking techniques.
- The WG 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 are only part of a vast and constantly evolving toolkit for attackers: mitigating any one technique would not eliminate Internet fraud and abuse.
- 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.

1.6. Possible Next Steps

Note: the Working Group would like to provide the following ideas for discussion and feedback during the public comment period. Please note that at this stage the Working Group has not reached consensus on any of the ideas below. The objective of the Working Group will be to review the input received during the public comment period and determine which, if any, recommendations receive the support of the Working Group for inclusion in the final report.

- Redefine the issue and scope by developing a new charter or explore further research and fact-finding prior to the development of a new charter.
- Explore the possibility to involve other stakeholders in the fast flux policy development process.
- Explore other means to address the issue instead of a Policy Development Process.
- Highlight which solutions / recommendations could be addressed by policy development, best practices and/or industry solutions.
- Consider whether registration abuse policy provisions could address fast flux by empowering registries / registrars to take down a domain name involved in fast flux.
- Explore the possibility to develop a Fast Flux Data Reporting System (FFDRS).

2 Report Process and Next Steps

This Initial Report on fast flux is prepared as required by the Generic Names Supporting Organisation (GNSO) Policy Development Process (PDP) as stated in the ICANN Bylaws, Annex A (see http://www.icann.org/general/bylaws.htm#AnnexA). The Initial Report will be posted for public comment for 20 days. 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.

3 Background

3.1 Process background

3.1.1 Security and Stability Advisory Committee

The ICANN Security and Stability Advisory Committee (SSAC) completed a study of the way in which the Domain Name System (DNS) can be manipulated by Internet cyber-criminals to evade detection and termination of their illegal activities. The results of the study were published in January 2008 in the SSAC Advisory on Fast Flux Hosting and DNS (SAC 025)[i], which describes the techniques that are collectively referred to as "fast flux hosting," explains how these techniques enable cybercriminals to extend the maliciously useful lifetime of compromised hosts employed in illegal activities, and "encourages ICANN, registries, and registrars...to establish best practices to mitigate fast flux hosting, and to consider whether such practices should be addressed in future [accreditation] agreements."[ii]

During its teleconference meeting on 6 March 2008,3 the GNSO Council entertained the following motion, which carried:
"ICANN Staff shall prepare an Issues Report with respect to 'fast flux' DNS changes, for deliberation by the GNSO Council. Specifically the Staff shall consider the SAC Advisory [SAC 025], and shall outline potential next steps for GNSO policy development designed to mitigate the current ability for criminals to exploit the DNS via 'fast flux' IP or nameserver changes."

3.1.2 GNSO Issues Report on Fast Flux Hosting

In response to the request of the GNSO Council, ICANN Staff considered the SSAC Advisory (SAC 025), and consulted other appropriate and relevant sources of information on the topic of fast flux hosting. Its findings were published in the issues report on 31 March 2008. Based on these findings ICANN Staff recommended "the GNSO sponsor further fact-finding and research concerning guidelines for industry best practices before considering whether or not to initiate a formal policy development process". It furthermore noted that "the completion of concrete fact-finding and research will be critical in informing the community's deliberations".

3.1.3 Council Resolution & WG Charter

At its 8 May 2008 meeting, the GNSO Council initiated a formal policy development process (PDP) and called for creation of a working group on fast flux. Subsequently, at its 29 May 2008 meeting, the GNSO Council approved a working group charter to consider the following questions:

- Who benefits from fast flux, and who is harmed?
- Who would benefit from cessation of the practice and who would be harmed?
- Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?
- Are registrars involved in fast flux hosting activities? If so, how?
- How are registrants affected by fast flux hosting?
- How are Internet users affected by fast flux hosting?
- What technical (e.g. changes to the way in which DNS updates operate) and policy (e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior) measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?
- 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?
- What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?
- What are some of the best practices available with regard to protection from fast flux?

The group was also tasked to obtain expert opinion, as appropriate, on which areas of fast flux are in scope and out of scope for GNSO policy making.

3.2 Issue Background

N.B. Please note that the following content is partially taken from the GNSO Issues Report on Fast Flux Hosting – 31 March 2008 and may not reflect the opinion of the Working Group on the issue.

"Fast flux" refers to rapid and repeated changes to an Internet host (A) and/or name server (NS) resource record in a DNS zone, which have the effect of rapidly changing the location (IP address) to which the domain name of an A or NS resolves. Although some legitimate uses for this technique are known (see below), it has within the past year become a favorite tool of phishers and other cybercriminals who use it to evade detection by anticrime, antimalware and anti-phishing investigators.

How fast flux attacks work

> *N.B. Please note that the following content is based on, and in some cases taken verbatim from, the description at http://www.honeynet.org/papers/ff/fast-flux.html and may not reflect the opinion of the Working Group on the issue.*

The goal of fast flux is to assign and re-assign multiple IP addresses (sometimes hundreds or even thousands) to a single qualified domain name (such as www.example.com). These IP addresses are changed in and out of zone file A (host address) and/or NS records, sometimes using round-robin IP addresses and/or short time-to-live (TTL). Web site host names may be associated with a new set of IP addresses which can change rapidly. A browser that connects to the same web site repeatedly over a short period of time could actually be connecting to a different infected computer each time. In addition, the attackers ensure that the compromised systems they use to host their scams have the best possible bandwidth and service availability. They often use a load-distribution scheme, which takes into account node reachability-check results, so that unresponsive nodes are taken out of the pool and content availability is always maintained.

Proxy redirection adds a second layer of obfuscation to fast flux. When an attacker hosting malicious content (a phishing site, for example) uses a fast flux network, the hosts that are "fluxed" (by rapidly changing the configuration of the malicious host network) are typically proxies that redirect queries to the site that contains the attacker's actual content. That's simpler for the attacker, because instead of having to copy his malicious content to many different bots, he can put it on one host, and deploy a botnet of redirecting proxies that all point to that host. The fluxing then takes place among the redirectors. Redirection disrupts attempts to track down and mitigate fast flux service network nodes. The domain names and Uniform Resource Locators (URLs) for advertised content do not resolve to the IP address of a specific server, but instead fluctuate amongst many front-end redirectors or proxies, which then in turn forward content to another group of backend servers. While this technique has been used for some time in the world of legitimate web server operations, for the purpose of maintaining high availability and spreading load, in this case it is evidence of the technological evolution of criminal computer networks.

Fast flux “motherships” are the controlling element behind fast-flux service networks, and are similar to the command and control (C&C) systems found in conventional botnets. However, compared to typical botnet servers, fast flux motherships have many more features. The upstream fast flux mothership node, which is hidden by the front-end fast flux proxy network nodes, delivers content back to the bot client who requests it. Certain fast flux command and control systems employ peer to peer (P2P) applications and so operate successfully for extended periods of time in the wild. These nodes are often observed hosting both DNS and Hypertext Transfer Protocol (HTTP) services, with web server virtual hosting configurations able to manage the content availability for thousands of domains simultaneously on a single host.

Fast flux techniques are used to enhance the longevity and robustness of networks which support many malicious practices, including online pharmacy shops, money mule recruitment sites, phishing web sites, extreme/illegal adult content, malicious browser exploit web sites, and the distribution of malware downloads. Beyond DNS and HTTP, other services such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Message Access Protocol (IMAP) can be delivered via fast flux service networks. Because fast flux techniques utilize the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) redirects, any directional service protocol with a single target port would likely encounter few problems being served via a fast flux service network—so it's not just web sites; it could also be fraudulent email sites.

Legitimate uses of fast flux

The working group conducted research which developed evidence that legitimate high-capacity load balancing systems, and legitimate “volatile” or rapid update dependent services rely on short TTL values in the DNS records that resolve their principal domain names (e.g., www.google.com) to IP addresses in order to propagate changes quickly.

Organizations with high traffic sites or highly targetable networks might use this technique—which satisfies some narrow definitions of “fast flux”—to adapt its home page addresses to internal and external network conditions, such as server load, outages, user location, and resource reconfiguration. The ability to reconfigure a production network quickly is considered by certain service providers to be important enough to offset the additional query latency introduced by more-frequent DNS lookups.

The working group also explored the use of fast flux by service providers wishing to deal with situations in which a government or other actor is deliberately preventing access to their services from within a country or region, or is engaged in broader censorship. This was described as a possible “legitimate use”.

Certain service providers and registrars provide a name resolution service to enable web-hosting service for individuals and organizations who are assigned dynamic IP addresses. The DNS entries in these scenarios are typically assigned low TTL values. The IP addresses assigned to individuals and organizations by such providers commonly fall within a single Autonomous System Number (ASN). This is another example of legitimate use.

Illicit Uses of Fast Flux

Phishing, pharming, and other malicious (and frequently illegal) activities represent a well-known threat to the safety and security of Internet users. Those engaged in these activities can frustrate the efforts of investigators to locate and shut down their operations by using fast flux service networks to rapidly and continuously change the topology of the network on which their content is hosted, staying “one step ahead” of their law-enforcement pursuers.

Fast flux service networks are robust, resource obfuscating service delivery infrastructures. Such infrastructures make it difficult for system administrators and law enforcement agents to shut down active scams and identify the criminals operating them.

4 Approach taken by the Working Group

The Fast Flux Working Group started its deliberations on 26 June 2008 with an informal meeting during the ICANN Paris meeting where it was decided to continue the work primarily through weekly conference calls, which started on 11 July 2008. The group decided to start working on answering the charter questions in parallel to the preparation of constituency statements on this topic. In order to facilitate the feedback from the constituencies, a template was developed for responses (see Annex I). The initial idea was to have a first round of informal constituency statements, followed by a final round of constituency statements following the first draft of the initial report.

The group decided it would be useful to reference information from organizations doing fast flux domain analysis work. This material is attached to this report as an annex.

In addition to the weekly conference calls, extensive dialogue occurred through the fast flux mailing list. Over 800 emails have been posted to the mailing list as of this writing, not taking into account messages that were sent between individual Working Group members on the topic.

Except where marked differently, the positions outlined in this document should be considered in agreement by the Working Group, meaning that there was broad agreement within the Working Group (largely equivalent to “rough consensus” as used in the Internet Engineering Task Force (IETF)). Where no broad agreement could be reached, the following labels have been used to indicate the level of support for a certain position:

- Support – there is some gathering of positive opinion, but competing positions may exist and broad agreement has not been reached.
- Alternative view – a differing opinion that has been expressed, without garnering enough following within the WG to merit the notion of either Support or Agreement. It should be noted that an alternative view could be expressed where there is broad agreement as well as support.

4.1 Members of the Working Group

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 or employers.

The members of the Working Group are:

Name	Constituency/other	Affiliation
Adam Palmer	Individual	PIR
Avri Doria	Nomcom Appointee, Council Chair	Luleå Univ of Tech
Beau Brendler	ALAC	Consumer Reports WebWatch
Christian Curtis	NCUC	Brooklyn Law School
Chuck Gomes	Registry, GNSO Council Vice Chair	Verisign
Eric Brunner-Williams[iii]	Registrar	CORE
George Kirikos	CBUC	Leap of Faith Financial Services Inc
Greg Aaron	Registry	Afilias
Ihab Shraim	Registrar	Mark Monitor
James Bladel	Registrar	Godaddy
Joe St Sauver	Individual	Internet2, University of Oregon
Kalman Feher	Registrar	MelbourneIT
Liz Williams	CBUC	LSE
Marc Perkel	Individual	Internet business (Ctyme.com)
Margie Milam	Registrar	Mark Monitor
Mark McFadden	ISP	BT
Martin Hall[iv]	Individual	Karmasphere
Mat Larson	Registrar	Verisign
Jose Nazario[v]	Individual	Arbor Networks
Mike O'Connor[vi]	CBUC	The O'Connor Company of St Paul
Mike Rodenbaugh	CBUC	Rodenbaugh Law
Minaxi Gupta	Individual	Indiana University USA
Paul Diaz	Registrar	Network Solutions
Paul Stahura	Registrar	ENom
Philip Lodico	CBUC	FairWinds Partners
Randy Vaughn	Individual	Information Systems Hankamer School of Business Baylor University
Rod Rasmussen	Individual	Internet Identity

Rodney Joffe	Registry	Neustar
Steve Crocker	SSAC	Shinkuro
Steven Vine	Registrar	Register.com
Tony Holmes	ISP	BT
Wendy Seltzer	ALAC	Berkman Center for Internet & Society
Zbynek Loebl	IPC	Czech Arbitration Court

In addition, ICANN Senior Security Technologist Dave Piscitello actively participated in the Working Group's discussions.

The Working Group was supported by the following ICANN staff members: Glen de Saint Géry, Liz Gasster and Marika Konings.

To review the statements of interest of the Working Group members, please visit: http://gnso.icann.org/issues/fast-flux-hosting/soi-ff-05aug08.shtml

5 Discussion of Charter Questions

The following is a distillation from email threads and Working Group conference calls. As far as possible, answers to the charter questions have been clustered together in separate groupings.

Fast flux characteristics

A fast flux attack network, for the purposes of this working group, exhibits the following characteristics:

- Some but not necessarily all of the network nodes are operated on compromised hosts (i.e., using software that was installed on hosts without notice or consent to the system operator/owner);
- Is 'volatile' in the sense that the active nodes of the network change in order to sustain the network's lifetime, facilitate the spread of the network software components, and to conduct other attacks; and
- Uses a variety of techniques to achieve volatility including:
  - rapid and repeated selection of systems from a pool of botted hosts, with those systems being used for the purpose of serving malicious content, for use as name servers, and for other purposes, all via DNS entries with low TTLs;
  - dispersing network nodes across a wide number of consumer grade autonomous systems;
  - monitoring member nodes to determine/conclude that a host has been identified and shut down; and
  - time, or other metric-based, topology changes to network nodes, name server, proxy targets or other components.

Additional characteristics that in combination or collectively have been used to distinguish or "fingerprint" a fast flux hosting attack include:

- multiple IPs per NS spanning multiple ASNs,
- frequent NS changes,
- in-addrs.arpa or IPs lying within consumer broadband allocation blocks,

- domain name age,
- poor quality WHOIS,
  - Support:
    - Whois records are fraudulently created (e.g. using stolen identities or payment methods)
- determination that the nginx proxy is running on the addressed machine: nginx is commonly used to hide/proxy illegal web servers,
- the domain name is one of possibly many domain names under the name of a registrant whose domain administration account has been compromised, and the attacker has altered domain name information without authorization.

The distribution and use of software installed on hosts without notice to or consent of the system operator/owner is a critically important characteristic of a fast flux attack network; in particular, it is one among several characteristics that distinguish fast flux attack networks from **production** uses of fast flux techniques in applications such as content distribution networking, high availability and resilient networking, etc.

In order to constrain the working definition of “fast flux” to lie “within the scope of ICANN to address,” the WG also tentatively agreed to limit the definition to the operation of the DNS and its registration system, specifically excluding the question of what constitutes “criminal intent.”

Charter questions

5.1 Who benefits from fast flux, and who is harmed?

Who benefits from fast flux?

Production applications of volatile networks may exhibit some but not all characteristics ascribed to fast flux attack networks. For example, the Working Group assumes that unauthorized software operated on compromised hosts would not participate in or contribute to the intended and beneficial use of such volatile networks.

The WG identified the following ways in which fast flux techniques either are or plausibly could be used for legitimate purposes, without reaching consensus on whether or not any or all of these uses actually occur, or whether the beneficial uses depend on fast flux techniques or could be pursued using other means of roughly equivalent efficacy and convenience.

1. Organizations that operate highly targetable networks

Organizations that operate highly targetable networks (e.g. government and military/tactical networks) must adhere to very stringent availability metrics and use short TTLs to rapidly relocate network resources which may come under attack. While such networks employ short TTLs, short TTLs – in and of themselves – are insufficient to characterize a domain name as ‘fast flux’. TTLs become an issue for fast flux-related work primarily because at least one Internet Draft, ftp://ftp.rfc-editor.org/in-notes/interne t-drafts/draft-bambenek-doubleflux-01.txt (URL broken due to length) focuses primarily on establishing minimum TTLs as an approach to limiting fast flux. If constraints were to be applied to TTLs in an effort to limit fast flux, this action would affect 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 organizations which rely on short TTLs in order to provide a variety of legitimate services, among others.

- Alternative viewpoint:
  There are legitimate uses of short TTL values, and artificially limiting TTLs via consensus policies will simply move the problem beyond the purview of ICANN (to ccTLDs and privately operated DNS networks).

2. Content distribution networks

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).

3. Free speech / advocacy groups

Organizations that provide channels for free speech, minority advocacies, etc., may use short TTLs and operate fast flux like networks. The group was presented with a case study of a service that uses fast flux methods to purportedly allow Web users to circumvent Internet content censorship. A discussion on this issue can be found at http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00371.html.

- Alternative viewpoints:
  - Some indicated that there is a lack of evidence to actually support this category (free speech / advocacy as benefitting from fast flux).
  - Some working group members pointed out that operators of networks in this category are understandably reticent, and that information about these networks will always be very difficult to obtain.
  - Techniques other than Fast Flux (such as Tor) are used by these groups to avoid discovery.

"Who is harmed by fast flux activities?"

The WG noted that harm could arise from both legitimate and malicious uses of fast flux techniques, and WG members found it difficult during their discussions to maintain a clear distinction between harms that arise directly from the techniques themselves (*e.g.*, rapid reconfiguration of network topologies using techniques such as short TTLs and rapid changes to information in A or NS records) and harms that arise from the malicious behavior of “bad actors” who may use fast flux as one of many techniques to avoid detection and termination of their activities (spamming, phishing, etc.) by law enforcement or other anti-crime agencies. This difficulty appears to be responsible for the persistent disagreement within the WG concerning the extent to which “fast flux” is or is not a culpable element of “malicious behavior” (which itself remains a poorly-defined term).

The WG 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 fast flux 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

- Alternative view in relation to the previous paragraph:
  Due process needs to be observed. People can be falsely accused of a crime. Determination of guilt is something that should be left to the court system.

Although the WG did not reach consensus concerning the separately identifiable culpability of fast flux hosting with respect to the harm caused by malicious behavior, it recognized the way in which fast flux techniques are used to prolong an attack:

> "[A] 'flux' domain attack lasts about twice to six times longer than any other kind of phishing site. Here's a reference to an excellent paper on this by Tyler Moore and Richard Clayton of Cambridge from last year on the topic of phishing site uptimes that breaks this out based on hard data: (http://www.cl.cam.ac.uk/~rnc1/ecrime07.pdf). So these flux techniques keep a site up at least twice as long, much longer on many occasions."[vii]

The WG does not suggest that mitigating fast flux attacks would eliminate the need for other anti-abuse or law enforcement work, nor do we intend to exaggerate the benefits of this attack technique to would-be malefactors by calling detailed attention to specific harms. Rather, we call attention to these attacks in a markedly strong manner to emphasize that fast flux attacks have considerable influence in the duration and efficacy of harmful activities.

The WG offers the following initial working answers to the charter questions but would like to emphasize that continued work is required in the following areas:

- A robust technical, and process, definition of “fast flux”,
- Reliable techniques to detect fast flux networks while maintaining an acceptable rate of false positives,
- Reliable information as to the scope and penetration of fast flux networks,
- Reliable information as to the financial and non-financial impact of fast flux networks

5.2 Who would benefit from cessation of the practice and who would be harmed?

Who is harmed by fast flux techniques when used in support of attack networks?

The parties who benefit from the cessation of the practice of fast flux attacks are the same parties who are harmed when fast flux is used in support of attack networks. The WG thus focused its attention on identifying the harms, as follows.

1. Individuals whose computers are infected by attackers and subsequently used to host facilities in a fast flux attack network (e.g., nginc proxies, nameservers or web sites). The individual may have his Internet connection blocked. In extreme cases, should the computer be suspected of hosting illegal material (e.g., child pornography), the computer may be seized by law enforcement agents (LEAs) and the individual may be subject to a criminal investigation.

In addition:

– even if their connection is not blocked, users may experience degraded performance (as computer or network resources get consumed by the parasitic miscreant user(s) of their system)

– if the Internet Service Provider (ISP) does not block the infected user, remote ISPs may end up blocking all or some traffic from the user, e.g., as a result of the user's IP being listed on a DNS block list

– the user may be (repeatedly) diverted from a normal connection to a walled garden where the only resources they can access are remediation sites or tools

- a user's systems may become unstable as a result of malware which was installed to enable fast fluxing

Some specific examples of how users can be harmed by fast flux attacks, beyond what has already been mentioned, are:

- increased operational complexity and loss of Internet transparency as operators implement increasingly draconian measures in an effort to control abuse from potentially compromised users
- costs associated with the prophylactic purchase of antivirus products, home firewall "routers" and other security products meant to keep bots and other security threats at bay
- clean up costs when prophylactic measures fail (e.g., when a non-technical user needs to hire a technician to help them try to get uninfected)
- in the case of users whose subscriptions are terminated by their ISP, or users that decide to change ISP as a result of the ineffectiveness experienced by the incumbent ISP, the costs associated with moving from one ISP to another, including both direct contractual costs (such as potentially overlapping subscription costs, or disconnection and connection fees), as well as indirect costs such as changes in email addresses (with attendant lost or delayed email), time spent learning the ins-and-outs of a new ISP, time spent reconfiguring systems to use the new ISP, etc.

2. Businesses and organizations whose computers are infected and subsequently are to host facilities in a fast flux attack network. These organizations may have Internet connections blocked, which may result in loss of connectivity for all users and customers, as well as the possible loss of connectivity for any Internet services also hosted via the blocked connection (e.g., mail, web, e-merchant or ecommerce sites). Again, in the extreme, should the computer be suspected to host illegal material, the computer may be seized by LEAs and the individual may be subject to a criminal investigation. If this computer were hosting web and other services for the business/organization, the seizure could also result in an interruption of service, loss of income or "web presence". Registries may suspend name resolution of the organization’s domain if ordered by courts or LEAs.

A compromised system in a business environment also immediately raises the dreaded specter of a breach of personally identifiable information (PII). If PII was present on the compromised machine, notification may be mandated by statute, which may result in substantial direct costs to the affected organization. PII-related worries also drive the substantial costs associated with deployment of whole disk encryption. Some businesses may also be affected by specific laws e.g. the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA), which apply to financial institutions or health care institutions, respectively.

3. Individuals who receive phishing emails and are lured to a phishing site hosted on a fast flux attack network may have their identities stolen or suffer financial loss from credit card, securities or bank fraud. Those losses may include both direct losses, which a financial institution declines to reimburse, 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 a 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).

Affected individuals may unwittingly disclose medical or personal information that could be used for blackmail or coercion. Individuals who purchase bogus products, especially pharmaceuticals, may be physically harmed from using such products.

- Support:
  Individuals may be subject to 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 seeking help as they may be concerned that their medical information will not remain confidential.

- Support:
  Additional harm can occur 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 can undercut the incentive for pharmaceutical companies 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 inferior or dysfunctional products, deny countries legitimate customs revenues associated with the import of premium brand-name products, or result in unsafe products (for example as a result of counterfeit UL-listed electrical appliances cords).

4. Internet service providers are harmed when their IP address blocks and their domain names are associated with fast flux attack networks. These operators also bear the burden of switching the unauthorized traffic that fast flux attack networks generate. ISPs may also incur the cost of diverting staff and resources to respond to abuse reports or legal inquiries 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 using fast flux hosted sites, and the ISP is deluged with the fast flux-enabled spam. ISPs may also experience excess DNS-related traffic as a result of fast flux, 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 fast flux 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 fast flux hosting, unlike port 25 blocks deployed to control direct-to-MX spam).

5. The reputation of a registrar may be harmed when its registration and DNS hosting services are used to facilitate fast flux attack networks that employ "double flux" techniques. 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 group wdprs.internic.net complaints together with fast flux complaints simply because it is the sole complaint mechanism available for fast flux domain name abuse. Anti-spam experts have therefore focused at scrutinizing suspected spamvertised (advertised via spam) fast flux domain names for Whois problems. Dealing with those Whois Data Problem Report System (WDPRS) reports represents an additional registrar-specific cost. Providing a

reporting channel that would focus on the actual issue (a domain has been detected which is engaged in criminal activity) rather than the substitute issue (there is a problem with the domain's Whois data), would clarify the problem at hand.

6. Businesses and organizations who are "phished" from bogus web sites hosted on fast flux attack networks may experience financial or material loss, tarnish to brand, or loss of customer/consumer confidence. They also incur the cost associated with brand abuse monitoring, detection and mitigation.

7. Individuals or businesses whose lives or livelihoods are affected by the illegal activities abetted through fast flux attack 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 harmful images.

- Support:
  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.

8. Registries may incur the cost of diverting staff and resources to monitor abuse or to respond to abuse reports or legal inquiries relating to fast flux attack network activity. 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, it could be a powerful disincentive hindering the adoption and use of that registry's TLD.

Who benefits from the use of fast flux techniques?

The Working Group has previously explained that the use of short TTLs is insufficient to characterize a network as a fast flux network, and insufficient to characterize that fast flux network as an attack or production network. The Working Group does recognize that certain organizations and network operators benefit from the use of fast flux techniques. Examples of such networks include:

1. Organizations that operate highly targetable networks (e.g., government and military/tactical networks) strive to adhere to very stringent availability metrics and use short TTLs specifically (and other fast flux techniques as appropriate) to rapidly relocate network resources which may come under attack. Note: Targeting an IP address rather than a Fully Qualified Domain Name (FQDN) is generally preferred by intelligent attackers because this method is more difficult to detect and isolates the attack origin(s).

2. Content distribution networks such as Akamai use fast flux techniques for situations 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). 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.

3. Organizations that provide channels for free speech, minority advocacies and activities, or, revolutionary thinking may use fast flux techniques to avoid detection.

4. Criminals, terrorists, and generally, any organization that operates a fast flux attack network at public expense, harm or detriment benefit from the use of fast flux techniques.

The working group recognizes that future uses of this technology may be developed and that, as a result, it is impossible to list all possible beneficial and harmful uses of this technology. Those using fast flux for criminal purposes have had an incentive to develop uses more quickly than legitimate users in order to stay ahead of security and law enforcement efforts. Because of this and because of the private and academic research efforts focused on criminal uses of fast flux, the working group likely has a clearer picture of the illicit uses of this technology than the legitimate ones. Nevertheless, there are likely both criminal and legitimate uses of this technology that are unknown and unknowable at this time.

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 an annex), the Registry Constituency (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 and question 7 are of particular interest in this context.

5.4 Are registrars involved in fast flux hosting activities? If so, how?

1) Most registrars are not involved in fast flux or double-flux due to their business models that do not provide direct public access for the registration of domain names in volume. Of those who do offer such services, most invest significant resources (time, money, personnel) working against the practice, and against generic online fraud.

2) Of the registrars where fast flux domains are registered by miscreants, the vast majority are unwitting participants in the schemes, largely due to ignorance of problematic registrations. Once informed of a problem, most of these registrars act quickly to deal with such domains, as they usually result in abuse issues and charge-backs on the credit cards used to register them which negatively impacts a registrar. However, some registrars appear to take consistently longer to deal with them than their peers. This could be due to many factors: staffing levels, standard procedures, and communications channels. Anecdotal evidence points to weaknesses in all of these factors in such cases and no actual intent to delay shut-down of a fraudulent or criminal scheme being perpetrated by a fast flux attack.

3) Some registrars and more often resellers of registrar services have the appearance of facilitation of fast flux domain attacks. In the case of an apparent "rogue reseller" registrars are usually swift to deal with such parties once made aware of the problems they have caused. Such incidents have been communicated privately to mitigation agents and discussed in some cases publicly in defense of registrar practices (e.g. http://blog.directi.com/0-directi/actions-against-registry-services-abuse-%e2%80%93-report-oct-2008-hostexploit-and-directi/).

4) No registrar has been prosecuted for facilitating criminal activities related to fast flux domains, but there have been reports linking one ICANN-accredited registrar (ESTDomains, which has since been de-accredited) to a large number of fraudulent domains including fast flux domains (see e.g. http://voices.washingtonpost.com/securityfix/2008/09/estdomains.html). The recent de-peering of Intercage and McColo, hosting companies that both hosted a large amount of highly undesirable and criminal content and a large number of domains registered by ESTDomains, reportedly resulted in dramatic reduction of malicious activity across the entire Internet, see http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.html and http://www.norman.com/Virus/Security_Information/54482/.

Thus there is a wide range of "involvement" and reaction to fast flux domains by the diverse members of the domain registrar community. The vast majority of actual involvement by registrars is largely as an unwitting provider of services which end up victimizing the registrars as well, as these types of domain registrations are often never legitimately paid, and create support overhead to deal with abuse issues. However, there is at least the possibility that at least one registrar could have become involved in directly facilitating such activities.

In general, registrars become targets for registration abuse (and abuse of registered domain names) when attackers discover they can exploit weaknesses in the registrar's registration services and internal processes. The attackers' objectives are in most cases to gain control of a customer's domain account so that he can use the domain names and name servers as resources for a subsequent attack, i.e., by modifying or adding name servers that host zone files of domain names used in phishing and other forms of attack that employ domain names.

Some of the known attack vectors are mentioned below:

- Attackers scan registrar web sites to identify web application vulnerabilities. They exploit vulnerabilities in registration web pages to gain unauthorized access to existing customer accounts.

- Attackers impersonate registrars using phishing techniques. A registrar-impersonating phisher tries to lure a registrar's customer to a bogus copy of the registrar's customer login page, where the customer may unwittingly disclose account credentials to the attacker who can then modify or assume ownership of the customer's domain names (See SAC 028 at http://www.icann.org/committees/security/sac028.pdf).
- Attackers will brute force customer account credentials when they detect that no countermeasures are implemented to block account access after repeated attempts to login have failed.
- Attackers may attempt to coerce or socially engineer help desk and support staff into making changes to customer accounts, or to grant access without proper identification and credentials.
- Attackers may create customer accounts using false credentials and stolen credit cards. They register domain names under this account and submit incomplete, inaccurate and intentionally fraudulent registration contact information. Attackers target registrars whom they have determined have insufficient measures when he completes a registration information form. In certain cases, attackers will initially submit superficially valid whois (e.g., the information may correspond to the credit card holder). Once the domains are created, the attacker returns to falsify contact information so that the contact information is not obviously linked to the credit card holder in displayed WHOIS information.\

This list is representative but not exhaustive. The above-mentioned attacks are also used to gain administrative control over domain names for purposes other than fast flux attacks. For example, any attack that allows an attacker to control a domain name can be used to facilitate a web defacement attack or other forms of denial of service attack involving domain names and DNS.

Some registrars are aware of the range of attacks that can be perpetrated against registrars and customers, and take proactive measures to protect themselves and their customers from attacks of the nature described above. Some of these are done as part of a general abuse prevention service while others are premium services that pay particular attention to customers that have high profile or high value domain name portfolios. Examples of such measures are mentioned below:

- Certain registrars provide a brand equity protection service. They proactively study domain name registrations to identify and block attempts to mimic or abuse IP, brands, copyrights and trademarks.
- Certain registrars monitor and limit DNS configuration changes for name servers that are to be included in TLD zone files. They may limit frequency of change, minimum TTL parameter values, number of DNS changes in a given time period, and total number of name servers that can be created for a given domain name.
- Abuse and brand protection staff of certain registrars work in cooperation with contracted parties and self-help groups to identify domain names and IP addresses of systems that appear to be participants in fast flux attacks. They correlate the IP addresses with routing information (ASNs), domains and hyperlinks found in blacklisted phish email messages and work cooperatively with registries to suspend or delete domains used in harmful attacks. Some registrars work with ISPs, hosting service providers, system administrators whose systems have been compromised and used to host fraudulent web sites to mitigate the effects of the attacks.
- Certain registrars offer customized domain name administration services to protect registrants from unauthorized access and misuse of that registrant's domains. Such services prevent fast flux attackers from using domains that are perceived as legitimate by black listing services and consumers for harmful purposes.

The above mentioned protection services do not focus specifically on mitigating fast flux attacks, but more broadly on protection from domain hijacking, malicious configuration of DNS, and brand protection.

5.5 How are registrants affected by fast flux hosting?

Registrants are targets for fast flux attackers who seek domain names they can use to facilitate double flux attacks. Attackers often gain administrative control over a registrant's portfolio of domain names using some of the methods described in Section 5.4. The attacker uses domains he controls via compromised accounts in fast flux attacks by modifying or adding to DNS configuration information via the registrant's domain administration account.

Attackers are attracted to existing domains that have a positive reputation (i.e., are not blacklisted) over newly registered domains. This attraction has increased because domain name (registration) age and history have become factors investigators consider as they attempt to determine whether a domain is associated with phishing, spam, and fast flux attacks. Attackers are also aware that registrars and registries often require stronger evidence of abuse and typically proceed more cautiously take down requests are submitted against "established" domains.

The impact to a registrant in such circumstances can be severe, ranging from service disruption to domain blacklisting or suspension. Service disruption can cause loss of revenue, service, advertising or business opportunities. Blacklisting or suspension can cause considerable reputational harm to a registrant's brands and trademarks.

5.6 How are Internet users affected by fast flux hosting?

Introduction

While most Internet users have never heard of fast flux hosting, a growing number of them are nonetheless directly affected by it. Internet users provide both the raw material that fast flux hosting runs on (malware-compromised broadband-connected consumer PCs), while also serving as the target audience for the spamvertised web sites which fast flux enables. Internet users are thus central to the entire fast flux problem, and unless it is handled appropriately, they are also the ones who may be subject to further restrictions and loss of Internet transparency.

Malware, Spam, and Bots

To understand how consumer PCs came to be converted into fast flux nodes, it is important to take a step back and consider the related problems of malware and spam. Internet miscreants use malware - viruses, worms, trojan horses, etc. - to gain control over large numbers of vulnerable networked consumer PCs. Those compromised systems, subject to remote manipulation by the “bot herder”, are commonly known as "bots" or "zombies." Having obtained control over those compromised PCs, the miscreants can than 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").

- There was support for the following:

  What are miscreants to do with compromised hosts that cannot be used for spam?

  The Messaging Anti-Abuse Working Group, a consortium of leading international ISPs, has issued recommendations for managing port 25 traffic to defeat direct-to-MX spamming (see http://www.maawg.org/port25). If traffic on port 25 is blocked following those recommendations, as many ISPs worldwide do, spam can no longer be sent directly to remote mail servers from those compromised PCs (although non-spamming normal mail users can still send regular mail). When ISPs control port 25, "bot herders" are left with millions of compromised systems that are incapable of directly spamming remote mail servers.

- There was support for the following:

  The difficulty for spammers and other Internet miscreants to find web hosting

  At the same time, spammers (and other miscreants) find themselves confronted with a second unrelated problem: it has become hard if not impossible for them to obtain and retain mainstream web hosting for illegal content. While what is illegal will vary from jurisdiction to jurisdiction, there are some categories of content which are illegal virtually everywhere, including, among other things:

  - narcotics, anabolic steroids and other dangerous drugs distributed without a valid prescription
  - child pornography
  - viruses, trojan horses and other malware
  - stolen credit card information
  - phishing web sites
  - pirated intellectual property, including pirated software ("warez"), copyrighted music and movies, and trademarked consumer goods (most notably things such as premium watches, shoes, handbags, etc.)

  In fact, many hosting companies specifically exclude hosting of any product or service (whether legal or not) which has been spamvertised, because they recognize that to permit spamvertised products or services on their hosting service will commonly result in their address space being listed on one or more anti-spam DNS block lists, such as those operated by Spamhaus [http://www.spamhaus.org/].

- There was support for the following:

  Miscreants discover one thing they can do with non-spamable compromised hosts

  Taking into account the previous section, it is easy to imagine what happens next: spammers repurposed some of their "surplus inventory" of compromised-but-unspamable systems to provide "web hosting" for illegal or spamvertised content which they cannot host elsewhere.

Reverse proxies are used to deploy fast flux hosting networks

Spammers do not replicated all the hundreds or thousands of html files, images, databases and other pieces of content and software that make up a sophisticated web site on each of the fast flux hosts. This would be too complex, too error prone, too time consuming, and too easily detected. Instead, spammers discovered that they can use reverse proxy software to accept web connections on the compromised consumer host and tunnel that traffic back to their actual (hidden) back-end master host. Nginx is one product often used for that purpose, although it is also routinely used by regular web sites. With reverse proxy, the compromised consumer PC acts as if it were delivering web pages, but in reality it is just acting as a pipeline to a hidden master web server (or farm of servers) located elsewhere. For further background information on fast flux service networks, please see http://honeyblog.org/junkyard/paper/08_ff_it-underground.pdf

Use of botted PCs is non-consensual and surreptitious

The owner/user of a compromised PC does not know that his or her PC is used as part of a fast flux hosting network. No one asks the owner of the compromised PC for permission to use their computer to distribute stolen credit cards, no warning lights goes off alerting the user that the computer has been compromised and is used to distribute stolen software. Typically the owner of the PC 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 are infected
- the ISP disconnects the customer, blocks traffic to/from the customer, or puts 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 finds that he can no longer access some remote network resources because they have been blocked at those remote sites as a result of the infection
- the user is visited by law enforcement officials investigating the illegal activity that has been seen in conjunction with "the user's" connection.

Post fast flux infection cleanup

Once the user discovers that he has been ‘botted’ and used for fast flux purposes, he is left with the unenviable chore of attempting to disinfect their compromised system. Because of the complexity of cleaning malware infections, and the 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 this 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 he had been using. The need to deal with this mess is the first tangible user impact of fast flux hosting, but one which only some unlucky Internet users do experience.

- Support:

  One universal impact of fast flux: spam

  Another effect of fast flux hosting is one which virtually all Internet users experience, and that is spam. As noted before, fast flux hosting is used to host illegal content or spamvertised products or services. Everyone with an e-mail account receives spam, whether it is an occasional message that slips through otherwise efficient filters, or a steady deluge that may have caused some users 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 do not need to visit a spamvertised web site to purchase a product or service. Clearly spammers are extremely motivated to find a takedown-resistant way to host their web sites, and that is what fast flux has given them. With fast flux, if one compromised machine 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.

o Support:

Fluxing name servers and 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 not only using compromised systems for web hosting, but also use those systems to manage DNS for their domains. A domain that does both the web hosting and gets its DNS service via compromised systems is normally referred to as a "double fast flux" or "double flux" domain.

o Support:

Port Blocks that might not work to curtail Fast Flux Web Hosting

All of this malicious activity, normally taking place on systems that are not professionally administered, results in ISPs endeavouring to control these phenomena via the network. It is understandable why they are inclined to do so: blocking port 25 controlled the overflow of spam, even if it did nothing to fix the underlying condition of the infected host. Maybe something similar could be done to address fast flux and double flux abuse? Unfortunately, unlike email where controlling port 25 is sufficient to control the emission of spam, when it comes to fast flux 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).

o Alternative view:

Although there are many valid arguments to avoid port blocking, the phenomena of double fast-flux would never have happened had ISPs routinely blocked inbound port

53. Those networks which routinely block ports by default are not prone to have hosts participate in fast flux networks. In addition, serving on an alternate port can be a signal that something is not in order. If ISPs would block port 80, and then end users would configure their systems to only read content from port 80, this would allow them to avoid sites served by residential ISPs that might be compromised, instead of professional webhosting companies.

- Support:

ISP efforts to control fast flux and double flux result in collateral damage

Blocking http traffic from consumer web pages often results in ISPs deploying more draconian solutions, such as banning all web servers from dynamic customer address space, or deploying potentially expensive deep packet inspection (DPI) appliances to identify fast flux or double flux traffic (at least until the spammers begin using SSL/TLS to defeat DPI). The problem gets even more complex when double flux is involved. When name servers are routinely hosted on consumer systems, controlling that DNS traffic requires managing port 53 traffic, blocking external DNS queries coming in 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 keep customers from readily (and intentionally) using third party DNS servers (such as those offered to the Internet community by OpenDNS), and may also complicate or preclude things such as accessing access-limited information products delivered via DNS, such as some subscription DNS block lists.

In conclusion, Internet users see their systems used without permission by miscreants that have set up fast flux nodes on the compromised systems; users face the daunting task of cleaning up those compromised systems once they discover what has happened; users are the target of endless spam, spam that would be more difficult to send if fast flux hosting did not exist; and users experience a loss of Internet transparency as ISPs struggle to control the fast flux and double flux problems on the network. The combination of those effects can result in Internet users having a bad on-line experience, partially thanks to the choice by some Internet miscreants to use fast flux and double flux techniques to avoid detection.

5.7 What technical (e.g. changes to the way in which DNS updates operate) and policy (e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior) measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?

This section summarizes the ideas ("solutions") that were discussed by the WG. The WG wishes to emphasize that "fast flux" needs better definition and more research. These ideas are presented here as a draft, to record incremental progress.

The solutions fall into two categories based on the type of involvement expected of ICANN and its contracted or accredited parties (gTLD registries and registrars): those that would require only the availability of additional or more accurate information, which could be used (or not used) by other parties engaged in anti-fraud and related activities as they saw fit; and those that would require or at least benefit from some degree of active participation by ICANN and/or registries and registrars to identify and deter fraudulent or other "malicious" behavior.

Information sharing

Solutions in this category focus on enhancing the ability of non-ICANN-affiliated parties to deal with fraud and other abusive or malicious behavior without recruiting ICANN or its affiliated registries and registrars as active agents of fraud detection or prevention. WG members advocating or supporting this approach noted that it would not require ICANN or its affiliates to decide what types of behavior are "abusive" or "malicious," and therefore would obviate the debate within the WG (and in the community at large) about how ICANN should define that dimension of "the fast flux problem."

The information sharing proposals discussed by the WG included the following ideas[viii]:

- Make additional non-private information about registered domains available through DNS-based (not WHOIS[ix]) queries (e.g., by defining new uses for TXT resource records), perhaps including the age of the domain, the number of name server changes made during a recent defined time interval, and the like.
    - There was support for the following statement:

  - o The DNS-based zone envisioned under this section need not to 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).

- Publish summaries of unique complaint volumes by registrar, by TLD, and by name server. Also provide a report by privacy protection service associated with complained-of domains.
- Encourage ISPs to instrument their own networks, so they have visibility into what is being done with their resources, and to their customers.
- Cooperative, community initiatives designed to facilitate data sharing and the identification of problematic domain names. Examples include the Anti-Phishing Working Group (APWG) and PhishTank for phishing, the Messaging Anti-Abuse Working Group (MAAWG) and various blacklists for spam, ShadowServer Foundation for botnets, and StopBadware.org for malware. Such community efforts may provide possible models for sharing information about fast-flux hosting.

Active engagement

Some of the “solution” ideas discussed by the WG focused on how ICANN and its affiliated registries and registrars might actively participate in efforts to discourage and deter or detect and stop “bad behavior” of various kinds, either by recommending voluntary changes to the way in which the DNS, registries, and registrars operate or by compelling changes through policies that would modify the contractual obligations of gTLD registries and/or the accreditation criteria for registrars. For the most part, these discussions were concerned more with the potential efficacy of actions and behaviors that ICANN might encourage or require rather than with the effective scope of ICANN’s involvement in distinguishing “good” from “bad” behavior or participating in efforts to fight “bad” behavior.

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:

- Adopt accelerated domain suspension processing in collaboration with certified investigators/responders
- Establish guidelines for the use of specific techniques, such as very low TTL values for resource records and limiting the number of modifications to the same A or NS record that can be made within a defined time period, to deter the core fast-flux activities.
- Identify name servers as static or dynamic in domain registrations by the registrant. If static name servers, the IP addresses used for those name servers should be provided. If dynamic, that is fine, but sites electing to use dynamic name servers should expect that their choice will be taken into account when other sites assess their reputation and decide what (if anything) they want to do with their traffic. Additionally, it could be considered to charge a premium for dynamic name server domains.
- Charge a nominal fee for changes to static name server IP addresses, split between ICANN and the Registry. The funds received from that fee could be dedicated to abuse handling/security-related purposes at ICANN and each Registry.
- 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.
- Stronger registrant verification procedures

The Working Group would like to point out that a number of registries -- including generic, sponsored, and country code TLDs – currently have policies that might serve as examples of how TLDs can take individual action in the area of domain abuse. Various TLDs are differently situated, and have different needs and approaches in this area[x].

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?

Any attempt by the WG to answer this question is deferred until the next Constituency Statements and public comments, particularly requested on these points, have been received and reviewed by the WG.

- There was support for:
  Proposed solutions may include limitations, guidelines or restrictions on registrants, registrars and/or registries, designed to mitigate the occurrence and longevity of fast

flux attacks. At that point, the WG might make an assessment of need for proposed solutions, balanced against the potential impacts.

5.9 What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?

Any attempt by the WG to answer this question is deferred until the next Constituency Statements and public comments, particularly requested on these points, have been received and reviewed by the WG.

- There was support for:
  Proposed solutions may include limitations, guidelines or restrictions on registrants, registrars and/or registries, designed to mitigate the occurrence and longevity of fast flux attacks. At that point, the WG might make an assessment of need for proposed solutions, balanced against the potential impacts.

5.10 What are some of the best practices available with regard to protection from fast flux?

One source of best practices for protection from fast flux can be found in the phishing world. The Anti-Phishing Working Group has recently released a best practices document for domain registrars in dealing with domain names registered by phishers ("Anti-Phishing Best Practices Recommendations for Registrars" http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf). Several of the practices outlined in that document apply directly or indirectly to dealing with fast flux domain names. While the audience for this particular document is the domain registrar community so some particular recommendations may not translate to other entities within the domain registration space, the same general principles can apply to domain registries, domain resellers, and other providers of domain registration or support services.

The following is a paraphrased sampling of some of the applicable practices mentioned in this document:

- Track the IP address, date, time, frequency and action of all account changes such as updating DNS or WHOIS information

- Limit the ability of registrants to repeatedly change their name servers via a programmatic interface to reduce or eliminate automated name server hopping.
- Proactively use available data to identify and/or shut-down malicious domains: There are numerous data sources that can provide information that may help in identifying malicious activity. Lists such as the SORBS Dynamic User and Host List can provide networks associated to dial-up, DSL, and cable networks that are more likely to be abused. The Composite Block List (CBL) may indicate fraud or that a machine has been compromised. Optimally a registrar would check against this information at DNS set-up or modification time, however periodic scanning should see good results.
- Use a "Registrar Lock" on registrations that are deemed to be suspicious enough to warrant further investigation.
- Another source for suggested practices to mitigate the use of domain names in the "double flux" variant of fast flux attacks is SAC 025, Fast Flux Hosting and DNS (http://www.icann.org/committees/security/sac025.pdf).

SAC 035 identifies mitigations methods certain registrars practice today in cases where the registrar provides DNS for the customer's domains:

- Authenticate contacts before permitting changes to name server configurations.
- Implement measures to prevent automated (scripted) changes to name server configurations.
- Set a minimum allowed TTL (e.g., 30 minutes) that is long enough to thwart the double flux element of fast flux hosting. [The WG notes that this method could interfere with customers (registrants) who use low TTLs for legitimate uses, without harm to others. In such cases, the DNS provider might provide exception case processing or white listing.]
- Implement or expand abuse monitoring systems to report excessive DNS configuration changes.
- Publish and enforce a Universal Terms of Service agreement that prohibits the use of a registered domain and hosting services (DNS, web, mail) to abet illegal or objectionable activities (as enumerated in the agreement).

6 Challenges

Despite the fact that the Working Group conducted its work with great enthusiasm and dedication, it encountered a number of challenges. An overview of the main challenges encountered by the fast flux Working Group is presented below.

a. Lack of an agreed upon definition of fast flux and supporting data

The issues report and the Working Group charter defined “fast flux” as “rapid and repeated changes to A and/or NS resource records in a DNS zone, which have the effect of rapidly changing the location (IP address) to which the domain name of an Internet host (A) or name server (NS) resolves”. However, some members of the Working Group expressed that this definition lacked the detail and specificity needed to answer the charter questions. A substantial amount of time was spent on reworking the definition, which in itself proved to be a challenge mainly due to difficulties over separating the technical and process elements of fast flux from the intent and activities for which it is being used. In addition, as outlined above, the group struggled to come up with a definition that would separate good use of fast flux from bad use. As a result, the discussion on possible solutions proved to be problematic. In the absence of an agreed-upon definition of fast flux (and a good assessment of the extent or impact of the problem) it was not clear what proposed solutions were supposed to fix.

In a number of instances, the Working Group encountered difficulties in separating between fast flux as a facilitating technique and the activities it facilitates. This resulted in discussions that went far beyond the scope and the mandate of the Working Group, as well as ICANN’s. It is worth remembering that in general the WG does not consider fast flux as a distinct fraud or attack vector comparable to spam, phishing, or malware. The WG feels that the primary effect of FF when it is used by "bad guys" is to delay the response. That is, FF serves to prolong the period of time during which the attack continues to be effective, before the domain is taken down by a "good guy." It is not an attack itself - it is a way for an attacker to frustrate the response to the attack.

The lack of data and lack of understanding of the full scope of fast flux also made discussions difficult. Working Group members for the most part agree that further fact finding and data gathering is imperative in order to have an informed discussion on this subject. Lack of a clear definition and disagreement on the exact scope of the problem made it extremely difficult to continue discussions as participants were speaking on the basis of different assumptions and different expectations as to what a potential recommendation on fast flux should look like.

b. Issues with the Charter

Neither the GNSO Council nor the charter identified what the objective of a potential recommendation on fast flux should be. Also the Council sought a structured fact-finding effort to examine the issues of fast flux (beyond the staff-authored Issues Report), but because no such mechanism currently exists, this effort was conducted in the context of a PDP. As a result, some felt that the charter did not provide sufficient information on what was expected to be delivered by the Working Group nor were important questions included. The group struggled with finding the right balance between respecting the charter, the lack of information and the need to find a solution and consensus. In its upcoming revision of the PDP, the GNSO should include an orientation of Working Group members as an early step for every group, to familiarize participants with the PDP process.

Some members of the Working Group offered reasons why policy development to address fast flux is outside the scope of ICANN's remit. Others disagreed. As some participants pointed out, some of the discussions and proposed actions might be more appropriate for other professional or community bodies that deal with security and Internet abuse issues.

7 Interim Conclusions

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 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.

7.1 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 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.

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. 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. Measures are needed to ensure that parties reporting fast flux activity are to be trusted.

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 are only part of a vast and constantly evolving toolkit for attackers: mitigating any one technique would not 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.

8 Possible Next Steps

Note: The Working Group would like to provide the following ideas for discussion and feedback during the public comment period. Please note that at this stage the Working Group has not reached consensus on any of the ideas below. The objective of the Working Group will be to review the input received during the public comment period and determine which, if any, recommendations receive the support of the Working Group for inclusion in the final report.

- **Redefine the issue and scope**
  In order to address some of the problems encountered by the Working Group to define the issue and answering the charter question, the possibility could be explored to redefine the issue and scope by developing a new charter. Another possible outcome of this process could be that further research and fact-finding is desirable before a new charter can be developed.

- **Explore the possibility to involve other stakeholders in the fast flux policy development process**
  As the use of fast flux is not limited to gTLDs and touches upon a number of other issues, the possibility could be explored to involve other ICANN entities such as the ccNSO, GAC, ASO and ALAC as well as including stakeholders external to ICANN (examples include: APWG, MAAWG, CCERT, IETF, FIRST, Artists Against 419.org, StopBadware.org, Regulatory enforcement agencies such as the FTC, Law enforcement).

- **Explore other means to address the issue instead of a Policy Development Process**
  In its current form, the Policy Development Process might not be best suited to address the issue of fast flux. It could be explored whether there are other possibilities to deal with the issue, either within an ICANN context or outside.

- **Highlight which solutions / recommendations could be addressed by policy development, best practices and/or industry solutions**
  Additional work could be undertaken by the Working Group to review the solutions discussed in this report in further detail and indicate how these could be implemented; by policy development, best practices or industry solutions.

- **Consider whether registration abuse policy provisions could address fast flux by empowering registries / registrars to take down a domain name involved in fast flux**
  In light of other possible GNSO policy initiatives relating to registration abuse policy provisions, it could be explored whether a Policy Development Process in that area would in effect also address the use of fast flux and result in the rapid take-down or suspension of domain names involved in a fast flux attack by registrars and registries.

- **FFDRS (Fast Flux Data Reporting System)**
  Collection of data about fast flux is an integral part of the work of this group, and the foundation for future analysis of the fast flux issue. Currently there is no publicly available formal mechanism for members of the community to submit potential fast flux domains for consideration by the working group. The Whois Data Problem Reporting Service (WDPRS), see http://wdprs.internic.net/, is an excellent example of a existing public domain name-related data submission mechanism similar to what the Working Group might consider, albeit one that is focused on Whois data problems rather than the fast flux problem. Another example of a public cyber-security-related domain name problem submission portal is Phishtank, http://www.phishtank.com/.

Annex I – First-round Constituency Input Template

Constituency Input Template

The GNSO Council has formed a Working Group of interested stakeholders and Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, in order to develop potential policy options to curtail the criminal use of fast flux hosting.

An early part of the working group's effort will incorporate ideas and suggestions gathered from Constituencies. View this as a brainstorming effort, rather than a formal policy-comment process (a formal Constituency Statement process is scheduled to start about a month from now). Our goal at this stage is to allow very broad participation in our drafting effort. So there is no requirement that your Constituency provide any suggestions at this time -- but any ideas are welcome.

Inserting your Constituency's response in this form will make it much easier for the Working Group to summarize the Constituency responses. This information is helpful to the community in understanding the points of view of various stakeholders.

Process:

- Please identify the members of your constituency who participated in developing the perspective(s) set forth below.
- Please describe the process by which your constituency arrived at the perspective(s) set forth below.

Questions:

1. Who benefits from fast flux, and who is harmed?
2. Who would benefit from cessation of the practice and who would be harmed?
3. Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?
4. Are registrars involved in fast flux hosting activities? If so, how?

5. How are registrants affected by fast flux hosting?
6. How are Internet users affected by fast flux hosting?
7. What technical, e.g. changes to the way in which DNS updates operate, and policy, e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?
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? What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?
9. What are some of the best practices available with regard to protection from fast flux?
10. Which areas of fast flux are in scope and out of scope for GNSO policy making.

Note:

Consensus is not required at this stage of the process. If ideas differ within the Constituency, please provide all of them. The Working Group will work to resolve the differences and the Constituency will have an opportunity to comment in the formal Constituency Statement process.

Annex II - Constituency Statements (Summary)

This section summarizes issues and aspects of fast flux reflected in the statements from the GNSO constituencies.

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 III of this report contains the full text of those constituency statements that have been submitted. These should be read in their entirety.

While the contributions vary considerably as to themes covered and highlighted, the following section attempts to summarize key views on fast flux.

Constituency Views

The RyC, NCUC and a number of individual RC members all recognize 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 emphasize that it is not in ICANN's remit to act as an extension of law enforcement or put registries or registrars in this position.

In addition, the RyC, NCUC and a number 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, or would change their implementations to avoid detection or mitigation efforts. The NCUC expresses specific concern in relation to the legitimate use of fast flux in facilitating anonymous speech. The RyC is 'concerned 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 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 inter-operability, technical reliability and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet".

The RyC points out that some of the solutions discussed by the Working Group "are currently impossible, or would require significant revisions to DNS protocols, or would require significant upgrades in deployed resolver code".

Further Work Suggested by Constituencies

The RyC and RC members emphasize the need for further data gathering and analysis before any further work is undertaken in this area. Both groups question though whether ICANN is the appropriate vehicle to take this discussion further.

Annex III – Constituency Statements (Full versions)

Version August 7, 2008

Registry Constituency Input Template:

Fast-Flux Working Group

The GNSO Council has formed a Working Group of interested stakeholders and Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, in order to develop potential policy options to curtail the criminal use of fast flux hosting.

An early part of the working group's effort will incorporate ideas and suggestions gathered from Constituencies. View this as a brainstorming effort, rather than a formal policy-comment process (a formal Constituency Statement process is scheduled to start about a month from now). Our goal at this stage is to allow very broad participation in our drafting effort. So there is no requirement that your Constituency provide any suggestions at this time -- but any ideas are welcome.

Inserting your Constituency's response in this form will make it much easier for the Working Group to summarize the Constituency responses. This information is helpful to the community in understanding the points of view of various stakeholders.
Please identify the members of your constituency who participated in developing the perspective(s) set forth below:

Voting in favor of this document, in full (listed alphabetically by TLD): NeuStar (.BIZ), puntCAT (.CAT), VeriSign (.COM, .NET), DotCooperation LLC (.COOP), Afilias (.INFO), Employ Media (.JOBS), mTLD (.MOBI), Global Name Registry (.NAME), Public Interest Registry (.ORG), RegistryPro (.PRO). Voting against: none. Abstaining: none. Absent/no response: SITA (.AERO), dotAsia Organisation (.ASIA), MuseDoma (.MUSEUM), TelNIC (.TEL), Tralliance Corp. (.TRAVEL).

Please describe the process by which your constituency arrived at the perspective(s) set forth below:

Based upon discussion of the issues, Registry Constituency members created a draft document, which was then circulated amongst all Constituency members for rounds of discussion and editing. Further discussion took place in two constituency teleconferences. After several iterations, a final draft was voted upon.

NOTE: Consensus is not required at this stage of the process. If ideas differ within the Constituency, please provide all of them. The working group will work to resolve the differences and the Constituency will have an opportunity to comment in the formal Constituency Statement process.

Executive Summary:

The Registry Constituency recognizes that fast-flux hosting is used by criminals to perpetrate a variety of illegal activities, which harm a variety of parties including registry operators. Constituency supports further discussion of voluntary best practices that would facilitate data sharing and are designed to identify problematic domain names.

The Registry Constituency feels that key issues are outside of ICANN's purview, and beyond the scope of GNSO policy-making:

1. ICANN's purview with regard to making policy to mitigate criminal use of the DNS is very limited, and technical. At the core, combating fast-flux hosting is a matter of identifying and disabling domains that are being used for illegal purposes.

2. It is not within ICANN's purview to place gTLD registries in a position to become extensions of law enforcement regimes around the world, by requiring registries to take action against a domain name that may be in violation of one or more nation's laws. In addition, it is not within ICANN's purview to determine (or license another evaluative body to determine) which domain names are being used for illegal purposes.

3. To require registries to act against certain domain names may also expose registries to unknown liabilities, and it is not clear whether ICANN has an effective ability to protect contracting parties from these liabilities.

4. Contracted parties should have the ability to set relevant terms of service for their respective TLDs or registrar service, as applicable. Various parties already have the ability

to act against problematic domain names, according to their various contracts and terms of service. Models for this activity already exist in directly relevant areas, and fast-flux domains are already being taken down. Every day, members of the Internet community – including hosting providers, network operators, registrars, registries, businesses and intellectual property owners, and law enforcement bodies—deal with domain names used for phishing, spam, malware, and other problems. Such problems have been resolved without involving ICANN, and we believe that most proposed solutions to deal with fast-flux hosting should not involve ICANN intervention.

5. There are venues for dealing with criminal activity, but ICANN is not such a venue. Criminals adapt their tactics quickly, and the parties taking action against them should be free to craft their own solutions as conditions suggest.

6. We do not believe that the Working Group has yet demonstrated, from a technical standpoint, 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. These continue to function well.

7. We believe that as of the date of this statement, the Working Group has not adequately quantified the scope of the problem based upon data. It is therefore difficult to evaluate the costs/benefits of solutions.

The Registry Constituency also explains below why it feels that some proposed solutions:

1. Are technically and legally outside the power of registries to implement,

2. Present significant engineering issues that could require revisions to protocols and the DNS itself,

3. Are not relevant to some registries, and

4. Could negatively impact various parties, some of which may be using fast-flux techniques for legitimate purposes.

Questions:

1. Who benefits from fast flux, and who is harmed?

Phishing, pharming, spam, and other illegal activities that may be perpetrated through the use of fast-flux networks represent a well-known threat to the security of Internet users. These types of domain name abuses can also harm the reputations and brands of specific TLDs. TLDs can be saddled with negative reputations for higher-than-average abuse rates. Some registries have adopted voluntary means to help address these issues. Most registries have no direct relationship with the registrants responsible for the abusive behavior.

2. Who would benefit from cessation of the practice and who would be harmed?

We will use the definitions found in the GNSO Issues Report on Fast Flux Hosting, which are:

Fast Flux: In this context, the term “fast flux” refers to rapid and repeated changes to A and/or NS resource records in a DNS zone, which have the effect of rapidly changing the location (IP address) to which the domain name of an Internet host (A) or name server (NS) resolves.

Fast Flux Hosting: The practice of using fast flux techniques to disguise the location of web sites or other Internet services that host illegal activities.

Using these definitions, “fast flux” is a technique or technical implementation, while “fast flux hosting” is the use of the technique for criminal purposes.

We are concerned that solutions aimed at certain types of nefarious activities criminal activity could prohibit or constrain legitimate activities that uses similar techniques, or might not accurately interpret the intent of the activity. It may be difficult to distinguish some criminal uses from non-criminal uses, especially using technical means only.

We are also concerned that cessation of fast-flux could impede the creation of new and legitimate services on the Internet, and we would like to know whether the cessation of fast-flux would impact any existing services, for example commercial services or services that facilitate speech on the Internet. As noted in its bylaws, one of ICANN’s core values is “Respecting the creativity, innovation, and flow of information made possible by the Internet.”

3. Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?

Some TLDs probably have never had domains that operate on fast-flux networks, and are less vulnerable. Fast-flux domains used for nefarious purposes are registered by criminals, who may not have easy access to domains in certain sTLDs. Some solutions might therefore not be good fits for all registries, and voluntary participation to best practices and/or specific programs might therefore be more viable.

Fast-flux hosting can be addressed if the domain names involved are not allowed to resolve. Domain names are stopped from resolving by removing them from the zone (by placing an EPP HOLD status, or removing the associated nameservers from the domain record, or by deleting the name from the registry.) Two parties have the technical ability to remove a domain name from the TLD zone – the sponsoring registrar, or the registry operator. (Registrants and resellers act through a registrar's system.) The relevant hosting provider(s) also have the ability to stop a domain name from functioning, by making changes at the nameservers.

ICANN's agreements with gTLD registry operators give registry operators varying rights to suspend domain names. Registrars, on the other hand, have direct contractual relationships with their registrants, and are often in a better position to communicate directly with their customers. (See Question #4 below for more.) Therefore, registries have often adopted practices to present abuse reports to the registrar of record.

As per its bylaws, the mission of ICANN is to "coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems," and ICANN "coordinates policy development reasonably and appropriately related to these technical functions." We do not think that making policy to mitigate criminal use of fast-flux hosting is reasonably and appropriately related to ICANN's technical functions. At the core, combating fast-flux hosting is a matter of identifying and disabling domains that are being used for illegal purposes.

It is not within ICANN's purview to require registries to become an arm of a law enforcement regime, nor to act on every allegation that may be made about purported illegal uses of domain names. It is not within ICANN's purview to determine (or license another evaluative body to determine), which domain names are being used for illegal purposes. To require registries to act against certain domain names may also expose registries to unknown liabilities, and it is not clear whether ICANN has an effective ability to protect contracting parties from these liabilities.

The GNSO Issues Report on Fast Flux Hosting stated: “The community of researchers, system administrators, law enforcement officials, and consumer advocates who are fighting Internet scams that are enabled or accelerated by fast flux hosting have concluded that trying to thwart fast flux hosting by detecting and dismantling the botnets (fast flux service networks) is not effective.” We agree. However, the Issues Report then went on to say: “Other measures that require the cooperation of DNS registries and registrars to identify or defeat fast flux techniques are expected to be much more effective.” And that “ICANN Staff research has confirmed that fast flux hosting…. could be significantly curtailed by changes in the way in which DNS registries and registrars currently operate.” (page 10)

We believe that those statements, especially relating to registries, are overbroad and need careful examination. Some of the proposed solutions involving registries are impossible for registries to implement, or will be ineffective for technical reasons. For example, registries have no role in how many fast-flux networks operate, registries are not necessarily privileged in their ability to detect fast-flux domains, and registries have differing abilities to act directly against abusive uses of domain names.

Please see response to Question 7 below for more commentary on technical and policy solutions that may involve registries. The Registry Constituency is interested in addressing, with the wider community, the problems caused by fast-flux hosting.

4. Are registrars involved in fast flux hosting activities? If so, how?

Fast-flux hosting can be addressed if the domain names involved are not allowed to resolve. As far as we are aware, all ICANN-accredited registrars have registrar-registrant contracts and terms of service that prohibit registrants from using their domain names for illegal or abusive purposes. These contracts allow registrars to variously suspend such domain names (i.e., stop them from resolving), delete them, and/or cancel the registrant’s rights and/or control over the domain. The agreements usually require the registrants to indemnify the registrars as well. Registrars are free to enforce their terms of service, and exercise these rights regularly by suspending many gTLD domain names each day for spam, phishing, malware distribution, the distribution of child pornography, and other abuses.

5. How are registrants affected by fast flux hosting?

6. How are Internet users affected by fast flux hosting?

7. What technical, e.g. changes to the way in which DNS updates operate, and policy, e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?

It is important to understand the technical means available to TLD registries, including the relevant Internet specifications and protocols. Unfortunately, some proposed solutions to fast-flux hosting that involve registries are currently impossible, or would require significant revisions to DNS protocols, or would require significant upgrades in deployed resolver code. Other proposed solutions may have limited impact, or are not exclusive to registries only.

Beyond the technical issues, some proposed solutions would require wide-ranging changes to registration paradigms, registrant behavior, and registry business practices. These should be examined carefully. In all cases the benefits should be proven to outweigh the costs, and registries should be given the means to recover the costs associated with any solutions imposed upon them.

Network operators, businesses, hosting providers, government organizations, intellectual property owners, registries, and registrars all have roles to play when addressing various Internet abuses, and collaborative solutions and data sharing may be useful.
Below are some assumptions and proposals about how registries may be involved in fast-flux hosting:

The GNSO Issues Report on Fast Flux Hosting [http://gnso.icann.org/issues/fast-flux-hosting/gnso-issues-report-fast-flux-25mar08.pdf] stated:
Registries and registrars can curb the practice in two ways: (1) by monitoring DNS activity (fast flux is easy to detect) and reporting suspicious behavior to law enforcement or other appropriate reporting mechanism; and (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 server query responses; Fast-Flux Working Group: Registry Constituency Input Template - August 7, 2008 6
• limiting the number of name servers that can be defined for a given domain; and
• limiting the number of address record (A) changes that can be made within a specified time interval to the name servers associated with a registered domain.
(page 11)

The SSAC Advisory on Fast Flux Hosting and DNS [http://www.icann.org/en/committees/security/sac025.pdf] identified the following potential solutions that could possibly involve registries:

- Adopting procedures that accelerate the suspension of a domain name,
- Remove domains used in fast flux hosting from service
- Authenticate contacts before permitting changes to name server configurations.
- Implement measures to prevent automated (scripted) changes to name server configurations.
- Set a minimum allowed TTL (e.g., 30 minutes) that is long enough to thwart the double flux element of fast flux hosting.
- Separate "short TTL updates" from normal registration change processing.
- Implement or expand abuse monitoring systems to report excessive DNS configuration changes.
- Publish and enforce a Universal Terms of Service agreement that prohibits the use of a registered domain and hosting services (DNS, web, mail) to abet illegal or objectionable activities (as enumerated in the agreement).
- Rate-limit or (limit by number per hour/day/week) changes to name servers associated with a registered domain name.

Below we will examine these ideas and others; we find many of them problematic.

Do registries have any control over fast-flux networks?

Single-flux fast-flux networks do not involve changes to records in a TLD registry. Single-flux service networks change A records for their front-end node IP address. This happens at a level below the registry.

Therefore, registries and registrars have no control over single-flux networks. No registry records are changed, and registries cannot monitor or detect that change activity via registry data. A great deal of fast-flux hosting takes place on single-flux networks.

Double-flux fast-flux networks do involve changes to records in a TLD registry. Double-flux is where both the NS records (authoritative name server for the domain) and A records (Web serving host or hosts for the target) are regularly changed, making the fast-flux service network more dynamic. For double-flux techniques to work, the registrant must frequently change the NS information at the registry.

Registries could analyze registry records to find nameserver changes, but would have to couple them with a single-flux detection method in order to be meaningful.

We see the following additional issues:

1. Problematic changes (i.e., those done for criminal intent) must be distinguished from non-problematic updates. This is a non-trivial matter in a registry of any size. Domain name registries are not in a position to interpret what does or does not constitute criminal activity in every legal jurisdiction in the world.

2. There is some evidence that some operators of double-flux networks change their nameserver records only on an infrequent basis. In some observed cases the interval between changes is days or even weeks. Such change rates do not qualify as rapid, and some so-called double-flux networks might not be worthy of the name.

3. There are many legitimate reasons why a registrant would want to change nameserver records more than twice or three times in the course of a month. Restrictions on change rates at such levels would unnecessarily restrict normal operations and user freedom.

4. Changes at the TLD level are detectable to anyone analyzing the TLD zone files, which are available daily free of charge.

5. Since changes to TLD records are relatively easy for the registry operator and other observers to detect, they might not be attractive methods for criminals.

6. By themselves, registry records give an incomplete picture in other ways. Registry operators cannot see some hosting-related changes because they involve changes to registry records in other TLDs. A registry's records can reveal when the IP of a nameserver object is changed – but only if the nameserver exists on a domain in that TLD. For example, the nameserver ns1.example.com exists as a record in the .COM registry, and that nameserver record must have an IP address associated with it, because the .COM registry is authoritative for .COM objects. The nameserver ns1.example.com may also exist as an object in the .ORG registry as well. However, that nameserver record in the .ORG registry cannot have an IP address associated with it, because the .COM registry is authoritative for .COM objects. This means that the .ORG registry operator cannot use its registry records to see if the IP of ns1.example.com is changing.

There is a need for more data to understand how many fast-flux networks operate on single flux versus double flux, at what rates double flux networks change their nameserver records in registries, and how frequent such changes need to be in order for a network to be considered a double-flux network. At this time there is not enough data to establish the scope of the problem.

Are registries in a special position to detect fast-flux hosting?

No. Fast-flux hosting is most commonly detected by querying nameservers for A records and recording the changes to those records over time. This method requires basic tools, and is currently practiced by many entities, including security companies, network operators, and academic researchers. Most subscribe to the gTLD zone files, which ICANN requires the registries to make available free of charge.

Some registry operators may be able to analyze DNS query data that comes to the TLD servers. This data is voluminous in larger TLDs, and is harder to interpret.

Is fast-flux hosting easy to detect, or easy to positively identify? Is it easy to identify criminal behavior?

The answers to all these questions is “no.” While it is easy to compile query data in the way described above, that data must then be interpreted. The key concept is that the observer must be able to separate out criminal uses of the fast flux technique from non-criminal uses, and in some cases this can be very difficult.

Some believe that fast flux hosting can easily be identified on an automated basis. But automated checking is not accurate when determining the criminal intent of any particular implementation. Rather, it may be possible for a certain percentage of criminal fast-flux hosting to be identified to a high degree of accuracy. This means that some criminal fast-flux hosting may be overlooked or discarded because it does not pass enough “tests” of bad intent, that manual checking is advisable, and that false positives will probably never be eliminated.

These problems are important, because the ultimate goal may be to suspend the resolution of fast-flux domain names. Parties who suspend domain names must perform due diligence, and are exposed to liability.

The Working Group has also examined case studies that demonstrate that:

1. fast-flux detection systems create false-positives.

2. It is not always possible to determine the intent that some fast-flux domains are being used for.

3. It is not always possible to determine whether the hosts involved are compromised.

Improved information availability may be useful for combating fast flux, but will result in incremental improvements only, just as blacklists and antivirus products have produced incremental progress against spam, phishing, and malware.

Can TLD registries control TTL values?

No, not in a way that is meaningful to this problem. Practically, domain name users and their hosting providers are in control of the TTLs related to their domain names, and are free to set whatever TTL they like.

Registrars have no mechanism by which they can set the TTL on records in the parent zone for domains they register, and registrars do not set or populate the time-to-live (TTL) for the resource records found in TLD zone files.

TLD registries may set a default TTL value. However, this TTL value is a default value only and does not control the actual TTLs associated with names in the zone. Instead, a TTL is set by the authoritative nameserver for a particular resource record. The authoritative data for a zone is below the zone cut, and any registry operator has a limited to no influence on the TTL on a delegation.

For example, any long TTL specified in the .COM zone in the NS set for a domain would be overwritten in resolvers' caches by the TTL specified in the daughter zone, which the registry does not host. So if the .COM registry operator sets a TTL of 600 minutes, and whoever hosts the individual domain name sets a TTL of 3 seconds, what gets cached is 3 seconds.

So, this default TTL has no practical impact on fast-flux hosting, because domain name registrants and their hosting providers are ultimately in control of the authoritative TTLs, and are free to set whatever TTL they like. This user-set value is the TTL value that prevails on the Internet, and this is a current, designed feature of the DNS. We do not know of any mechanism by which ICANN could limit the TTLs that zone administrators decide to install on their own RRsets.

Note that the EPP registry-registrar protocol offers no mechanism for registrars to specify TTL values to the registry.

What are the effects of either short or long TTLs on NS sets above the zone cut for queries which follow those delegations? This is not well understood. It is not known, for example, if increasing the TTL on NS sets in TLD zones could have an effect on some caches across the Internet. Before ICANN makes any related policy, we would expect ICANN to commission a credible technical study, and there should be significant input from the IETF. Any proposed changes to the DNS protocols, or to their standard implementations, should have the support of the engineering community, and such discussions should involve a formal consultative process with the IETF.

Are there legitimate uses for short TTLs?

Yes. Any entity that operates a Web site or other Internet service has legitimate reasons for using short TTLs, at least for finite periods of time. Such uses are written into relevant RFCs, including the domain name RFCs 1034 and 1035. Internet services that are subject to a high change frequency legitimately use low TTLs, and even TTLs of zero. Uses of zero-length TTLs are mentioned in relevant RFCs, including RFC 1035.

Imposing minimum lengths for TTLs is therefore contrary to standard engineering practices, will interfere with the operation of existing sites and services, may stifle the development of innovative services, and will impose costs on site operators and their service providers. Even if such limits were desired, there is presently no practical way that any entity could impose minimum TTLs on those parties responsible for setting them authoritatively. We do not know of any technical mechanism by which ICANN could limit the TTLs that zone administrators decide to install on their own RRsets. Any policy mechanism to limit the TTLs that zone administrators decide to install on their own RRsets would require volunteer compliance from all hosting parties world-wide -- which will not be practical or effective.

Is it practical or desirable to implement measures that limit the number of nameserver changes allowed in a given time period, or prevent automated (scripted) changes to name server configurations? Would authenticating contacts before permitting changes to NS records be practical or desirable?

Such a solution would force registrants to change their behaviors and expectations, and would impose delays and inconveniences upon Web site managers. The current paradigm allows gTLD registrants to change their records as they see fit, and it would be difficult to roll this back.

Such a system would also impose additional costs on registrars, which could be passed on to registrants in the form of higher registration fees.

As noted above, these counter-measures are effective against double-flux networks only, and the use of double-flux networks should be quantified so as to understand the impact of the proposed solution and weigh the benefits against the costs.

Is limiting the number of name servers that can be defined for a given domain practical or desirable?

No. Fast-fluxing domain names usually only have a few nameservers associated with them, often only four or five. There are legitimate reasons for registrants to use that number of nameservers, including robustness and redundancy. An example is icann.org, which has five nameservers listed.

Is reporting to law enforcement useful and effective?

We applaud the dedicated work of law enforcement, and encourage reporting, but it does not provide a comprehensive or speedy solution. Counter to some popular perception, the vast majority of Internet crime is not addressed through the efforts of law enforcement, and is not reported to law enforcement. Domain take-downs are usually accomplished by the entities affected, working with ISPs, hosting companies, server operators, registrars, registries, and individual computer owners. Law enforcement bodies are often under-funded, and often do not have resources to devote to cyber-crime. Jurisdictional issues also hamper the investigation and prosecution of Internet crimes. Some registries and registrars have established relationships with law enforcement bodies to provide information related to nefarious uses of domain names.

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? What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?

Also see number 7 above for discussions of the applicability and impact of establishing limitations, guidelines, or restrictions on those parties.

Some solutions aimed at criminal activity could prohibit or constrain non-criminal activity that use similar techniques, or might not differentiate adequately based on the intent of the activity. Other solutions may require parties to separate the criminal uses from the non-criminal, which is sometimes difficult. Whether solutions to criminal fast-flux may constrain non-criminal services and/or the creation of new and legitimate services on the Internet are pertinent issues for consideration. See also #7 above. One case study examined by the Working Group indicates the possible existence of such a service (UltraReach, which claims to be an anti-censorship service founded under human rights repression). The Working Group does not know how many relevant sites or services may already be operating on the Internet, or what they do, and therefore does not know the impact of some potential solutions. Absent such knowledge, we think it wise to “do no harm” and avoid limitations, guidelines, or restrictions that could impact legitimate services.

We also note that fast flux hosting is a phenomenon that utilizes the DNS, and therefore is technically relevant to all TLDs. Fast flux hosting currently occurs on many domain names and hosts across a wide range of TLDs. Regulation in the gTLD space only would leave fast flux activity unaddressed in the ccTLD space. We ask whether there is lasting value to developing gTLD policy regarding any issue that occurs in both gTLDs and ccTLDs. Attempts to technically (rather than administratively) cope with fast flux may result in increasingly complicated solutions that may inadvertently impact innocent parties, and/or may or break the network in hard-to-diagnose ways.

9. What are some of the best practices available with regard to protection from fast flux?

It may be useful to look at fast flux as an example of a generalized problem: domain name abuse. In many ways, fast-flux hosting is not conceptually any different from other domain name abuses. Spam, phishing, pharming, and malware also all take advantage of the DNS and Internet protocols. Efforts to mitigate these problems involve detection of potential problem domains, determinations of whether the activities on specific domain names may be illegal or violate terms of service, and then mitigation work. These are many of the exact same issues faced in the current fight against fast-flux hosting, and best practices for domain name takedowns could be adapted. In fact, fast-flux domains are already being mitigated using these existing practices.

Those problems are mitigated on a daily basis by private parties, including ISPs and network operators, hosting companies, registrars, registries, security companies, law enforcement, and individuals. This community is free to adapt its tactics and invent new alliances as needed. We recall that one of ICANN's core values, enshrined in its bylaws, is: "To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties."

There are cooperative initiatives designed to facilitate data sharing and the identification of problematic domain names. Examples include the Anti-Phishing Working Group (APWG) for phishing and identity theft, the Messaging Anti-Abuse Working Group (MAAWG) for spam, ShadowServer Foundation for botnets, StopBadware.org for malware, and so on. Such efforts are a possible model for addressing fast-flux hosting.

See also #10 below.

10. Which areas of fast flux are in scope and out of scope for GNSO policy making?

The GNSO Issues Report on Fast Flux Hosting noted that a consensus policy resulting from the GNSO policy-development process would only be applicable if fast flux hosting is an issue "for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, technical reliability, and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet." While fast-flux hosting is a recognized problem that impacts various parties, fast-flux hosting has not materially impacted the interoperability, technical reliability, and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet. Those services continue to function in a stable and reliable manner.

As we have stated before, we believe that ICANN's purview with regard to making policy to mitigate criminal use of the DNS is very limited. At the core, combating fast-flux hosting is a matter of identifying and disabling domains that are being used for illegal purposes. It is not within ICANN's purview to impose requirements that registries act as judge and jury, or to act on every allegation that may be made about purported illegal uses of domain names. To do so would turn registries into enforcement agencies. It is not within ICANN's purview to determine (or license another evaluative body to determine), which domain names are being used for illegal purposes. To require registries to act against certain domain names may also expose registries to unknown liabilities, and it is not clear whether ICANN has an effective ability to protect contracting parties from these liabilities. As per the GNSO Issues Report on Fast Flux Hosting, “General Counsel further notes that the overall question of how to mitigate the use of fast flux hosting for cybercrime is broader than the GNSO policy development process.” We agree. How to mitigate or prevent the use of fast-flux hosting for crime is indeed the central issue.

Efforts within ICANN and the GNSO will yield only incremental results. ICANN policies related to fast-flux hosting would only be applicable to gTLD registries and registrars. ccTLD domain names are also used for fast-flux hosting, which comprise almost half of the domain names on the Internet. Criminals who use fast-flux hosting could simply avoid the effects of ICANN policy by using ccTLD domain names. Therefore, we are unsure of the "lasting value" to developing gTLD policy regarding this issue. ICANN policies that target fast-flux hosting would only be applicable to gTLD registries and could impact their costs, and therefore affect their competitiveness with ccTLDs.

The GNSO Issues Report on Fast Flux Hosting stated that “The question of whether policy options would have ‘lasting value or applicability’ is a particularly important consideration in the context of fast flux hosting, where new static rules imposed through a policy development process might be quickly undermined by intrepid cybercriminals.” There are venues for dealing with criminal activity, and ICANN is not such a venue. ICANN is not suited to creating or overseeing detailed policies and procedures in such a rapidly evolving environment as cybercrime, where the criminals and responders are continually employing new measures and counter-measures. Instead, it may be more helpful to let private actors have the freedom and power to act within relevant legal and contractual contexts.
Spam, phishing, pharming, and malware are threats at least as prominent as fast-flux hosting, and arguably cause more damage and problems. Those abuses also leverage the DNS, have not entailed policy-making at the ICANN level, and have not demanded uniform or coordinated resolution. We therefore question why fast-flux hosting is a suitable topic for an ICANN process.

In many ways, fast-flux hosting is not conceptually any different from other domain name abuses. Spam, phishing, pharming, and malware also all take advantage of the DNS and Internet protocols. Those problems are mitigated on a daily basis by private parties, including ISPs and network operators, hosting companies, registrars, registries, security companies, and individuals. (Counter to some popular perception, the vast majority of abusive domain names are not taken down by the efforts of law enforcement.) These mitigation efforts often involve detection of potential problem sites, determinations of whether the activities on specific domain names are illegal or not, and then mitigation efforts. These are many of the exact same issues faced in the fight against fast-flux hosting. One of ICANN's core values, enshrined in its bylaws, is: "To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties."

IPC Initial Reaction

"The IPC appreciates very much the activity of the Fast Flux WG. We recognize that Fast Flux is a serious topic which so far has not been widely discussed and analysed. The work of the Fast Flux WG enables members of the IPC to learn more about the issues involved. At the moment IPC does not have any specific comments or recommendations regarding Fast Flux and the most appropriate resolution of negative impacts connected with Fast Flux, nevertheless we hope to be able to comment in detail at a later stage of the work of the WG."

Non-Commercial Users Constituency Statement on Fast Flux Hosting

The NCUC formally collects constituent input via its email discussion list as well as through a variety of informal communications.

Definitions

The working group has struggled considerably to define the term “fast flux,” largely because the term already has a preexisting meaning within the computer security community. Discussions have, however, made clear that the group needs terms in order to have productive discussion on this issue. Specifically, the group must be able to distinguish between those technical measures which it may be possible to effectively identify and regulate and the more difficult to measure elements such as intent and legality.

Additionally, the working group ought to have some terms to distinguish between those malevolent uses that are universally reviled and other uses, which might be effected by remedial measures. Legality has proven to be an inadequate benchmark, since the Internet is by nature global, and ICANN should not take it upon itself to resolve international conflicts of laws. Moreover, determinations of legality often turn on elements such as intent, which the DNS community is ill-disposed to assess.

Because of the inherent need for these distinctions, and because of the baggage associated with the terms “fast flux” and “fast flux hosting” it would be best to craft new terms to describe these concepts. As far as semantics are concerned, the working group's task is not to find the meaning of the terms we have been using but rather to find terms that will facilitate a meaningful discussion.

Benefits and Harms

The techniques of using domains with a short time to live or using a large network of computers to host content at a single domain are not inherently moral, immoral, beneficial or harmful. These qualities come not from the technologies themselves, but from the ways in which they are used. ICANN should be particularly wary of any attempt to ban a technology because of one use associated with it.

Insofar as fast flux can be used by criminals to evade authorities or to make a website appear more trustworthy than it is, it contributes to these harms. It would, however, be a mistake to equate the nefarious activities with the technology. Even if fast flux were completely eliminated these activities would still persist on-line.

Moreover, this technology (FFH) has demonstrated significant legitimate uses. Fast flux has been shown to be helpful in combating a denial of service attack and also with facilitating anonymous speech. Both current and future uses may be significantly impaired by attempts to ban the use of this technology. Unfortunately, it is difficult to assess how these uses may be impacted by ICANN measures, both because of the inherent difficulty in anticipating new technology and because of the difficulties of trying to communicate with speakers who may be currently using similar techniques to speak anonymously.

ICANN should take particular care to protect anonymous speech. Anonymous speech allows free expression by parties who might otherwise be subject to scorn or retribution for expressing unpopular opinions. This right to express one's true opinions without fear of reprisal is fundamental to the shared ideals of free speech, privacy, and basic human dignity. These rights are recognized and protected by the First Amendment to the U.S. Constitution and Article 12 of the Universal Declaration of Human Rights. Even where the strongest legal protections for free speech exist, the right to speak anonymously is still needed to protect against attacks by individuals, ensure open and honest discourse, and to allow speakers to contribute ideas without sacrificing privacy. For this reason, the U.S. Supreme court has explicitly ruled that the U.S. Constitution protects an individual's right to speak anonymously. ICANN should not take it upon itself to usurp this governmental function and second guess which human rights should be guaranteed to individuals and which should be terminated.

Potential Remedies

Any attempt to remedy the harms that accompany fast flux hosting should be evaluated with due consideration to the limits of what ICANN can and should do. ICANN must be vigilant to recognize the limited scope of its authority and mandate. ICANN is not a police force, government regulator or court of law. It is ill suited to determine which countries' laws should control on-line activity, determine when those laws have been breached, or create new rules intended to combat social ills.

There are significant dangers inherent in making any private entity, including ICANN, responsible for determining when anonymous speech is or is not permissible. Democratic societies have constitutions, elections, and courts to carefully balance the rights of the speaker against the rights of others. Private entities do not have the same incentives and legal compulsions to protect the rights of individuals. Because of this, private censorship is the single greatest threat to free speech on the Internet.

Many plaintiffs have already considered registrars and ISPs as potential private censors. They have filed suit against these entities because they objected to certain speech on-line. AOL, Network Solutions, and Dynadot are among those targeted by such suits. Sometimes these plaintiffs seek to have the content removed or rendered harder to access. Sometimes they are merely seeking a defendant with deep pockets. In all cases, however, the plaintiffs assert that Internet companies should censor the content of their customers.

Because of these problems, ICANN should be extremely wary of proposed solutions that discourage anonymous communications on the presumption that such communications are inherently malevolent. Informational approaches are preferable to those which prevent anonymous speech, and precautions should be included in any solution to ensure that we are not creating a precedent of censorship within the DNS community.

Fast-Flux PDP Working Group

Input from Registrar Constituency Members

Summary

We acknowledge that some perpetrators of online criminal acts employ the fast-flux technique, and that these illicit activities can cause harm to a variety of parties including registrars and their customers. Nevertheless, the use of fast-flux is not indicative that a domain or registrant is engaged in some illicit behavior. Even when objectionable activity does occur, it may be beyond ICANN's limited technical mandate to address it. We do not believe that the Fast-Flux PDP Working Group has an adequately formed sense of the issue to proceed with the policy development process at this time. We do believe that further quantification and analysis of the issue is warranted and would aid in its definition. Only then should any ICANN-chartered working group begin discussions of voluntary best practices that would facilitate data sharing and are designed to identify problematic domain names. This input is being provided by the undersigned members of the Registrar Constituency who are serving on the Fast-Flux Working Group. There is no official input statement from the Registrar Constituency at this time.

Overview and Response to Questions

It is evident from its voluminous email archive that the Fast-Flux PDP Working Group has struggled to adequately define the issue. The lack of a clear understanding of the scope and ramifications of fast-flux hosting also has undermined discussion of potential courses of action to address illicit activities. Significantly, there is disagreement about whether this issue even falls within the scope of the GNSO Policy Development Process and ICANN's limited technical mandate. For all of these reasons, we believe that this issue needs to be reconsidered from the start. We will highlight our specific concerns as we address the key questions that were put to the Working Group in its charter.

1. Who benefits from, fast flux, and who is harmed?

The Working Group determined that individuals and groups that are attempting to avoid or evade detection, identification, and takedown may use fast-flux hosting. These users could include spammers, fraud agents, distributors of illegal products or materials, and other "bad actors." Alternatively, they may comprise political dissidents and other free speech advocates use fast-flux hosting to avoid suppression or censorship. Furthermore, some website administrators use fast-flux as a tool to optimize network performance and reliability. It also can be used to perform maintenance or route diagnosis on domains under management.

> At this time the only thing that we can reasonably conclude is that fast-flux hosting "benefactors" and "victims" defy a simple definition. Much of this is the result of the Working Group not having adequate data to inform its discussion. Most of the provided examples were anecdotal, and lacked the necessary specificity to formulate a comprehensive description. It is not clear when (or even if) a more substantial base of data will be available. We believe that collection and analysis of fast flux-related data is essential. We also believe that this GNSO-constituted Working Group is not necessarily the most appropriate body to conduct the research. Perhaps the SSAC should be charged with developing the necessary data in consultation with industry experts, academic researchers, and other industry groups such as the APWG. Since this issue extends beyond the GNSO's constituency groups, future policy development should include the ccNSO and law enforcement representatives.

2. Who would benefit from cessation of the practice and who would be harmed?

The Working Group hypothesized that the entire community might benefit – but only under the assumption that illicit activities alone will be impeded by eliminating fast flux. It was generally agreed that criminal elements would quickly adapt their tactics, and any policy-induced gains would be temporary. Security companies also might benefit, but this assumes that Registrars and Registries become de facto data collection and enforcement agencies. This raises liability concerns and significant questions about scope, however. If we assume that ICANN can prohibit any use of the fast flux technique, then free speech advocates and network administrators who use it for their own ends clearly would be harmed.

> We are discouraged that the Working Group's charter includes such a loaded

> question. It implies that all fast flux activity is negative and does not consider legitimate uses of the technique. More importantly, we have not seen any data demonstrating that fast-flux hosting has materially impacted the inter-operability, technical reliability and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet. If cannot demonstrate or effectively quantify harm within the scope of ICANN's mandate, how can we reliably identify benefactors or victims?

3. Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?

4. Are registrars involved in fast flux hosting activities? If so, how?

5. How are registrants affected by fast flux hosting?

6. How are Internet users affected by fast flux hosting?

No gTLD Registry Operator was cited in the Working Group's deliberations. There were suggestions that sophisticated criminal networks may create or control an ICANN-accredited registrar to facilitate illicit activities using fast-flux hosting, but no data has been provided to support this claim. Besides being victimized by the illicit scams facilitated by fast-flux hosting (spam, identity theft, phishing, fake pharmaceuticals, etc.), registrants could be affected if registrars' transaction streams are swamped by fast-flux traffic. Unless they are directly victimized by a fluxing online scam, fast-flux hosted domains probably won't be visible to Internet users.

Again, we are discouraged that the Working Group's charter questions include loaded terms. Also, no data has been offered to corroborate claims that some Registrars are "involved" in fast-flux hosting activities. Care should be taken to distinguish between fast-flux as a facilitating technique and the illicit activities themselves. In many cases it is beyond ICANN's narrow technical mandate to try to address issues that are considered criminal in certain local jurisdictions.

7. What technical, e.g. changes to the way in which DNS updates operate, and policy, e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior

measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?

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? What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?

Different measures have been suggested to reduce or eliminate fast-flux activities, including:

- limiting the frequency of nameserver and/or A record add/edit/delete transactions; and/or
- limiting the time-to-live (TTL) minimum value that would be accepted by registry operators; and/or
- whitelisting legitimate fast-flux activities; and/or
- Restricting or limiting foreign nameservers, i.e. those that are controlled by a different TLD (especially ccTLDs) than the domain to which they are associated.

The Working Group also discussed the need to provide some liability protection for Registrars in addressing false positive cases generated by programmatic fast-flux identification systems.

> Many registrars (as well as other Working Group participants) feel that these questions are outside the scope of this working group. In fact, both the ICANN staff and General Counsel recommended gathering more information before initiating the PDP since a number of the questions appeared to be out of scope. We concur with the Registry Constituency's statement that "[w]e do not think that making policy to mitigate criminal use of fast-flux hosting is reasonably and appropriately related to ICANN's technical functions. At the core, combating fast-flux hosting is a matter of identifying and disabling domains that are being used for illegal purposes."

We also agree with the Registry Constituency's position that it is not within ICANN's purview to place registrars or registries in a position to become extensions of law enforcement regimes around the world, nor to act on every allegation about illegal uses of domain names. ICANN is not in a position to distinguish between legitimate domain names and those used for illegal purposes solely on the basis of fast-flux detection.

9. What are some of the best practices available with regard to protection from fast flux?

Until such time that we have the necessary data and analysis to establish the scope of the problem, we feel that it is premature to ask any ICANN-chartered working group to begin discussions of voluntary best practices that would facilitate data sharing and are designed to identify problematic domain names.

10. Which areas of fast flux are in scope and out of scope for GNSO policy making.

This question is best addressed by ICANN's General Counsel. We have also noted our concerns about questions of scope above.

Respectfully submitted,

Paul Stahura, eNom, Inc.
James Bladel, GoDaddy.com, Inc.
Kal Feher, Melbourne IT Ltd.
Paul Diaz, Network Solutions, LLC.
Steven Vine, Register.com, Inc.

Annex IV Fast Flux Case Study

The curious case of [Subject_Domain].hk.

By RL Vaughn

Executive Summary: Researchers have identified metrics useful for classifying domains as fast flux. However, Registrars and Registries may be reticent to rely solely on such research-based classifiers. This reticence is understandable given the risks which registrars and registries assume when they cancel a domain. Further, experiential misclassification (false-positive and false-negative) rates may differ significantly from those obtained using research data. For example, fast flux operators may adapt their practices in order to avoid detection or may attempt to exploit registrants to unwitting allow the fast flux operators control of their domains. It is the opinion of this author that investigative-protocols need to be in place in order to both strengthen the confidence of domain classification metrics and to gain understanding of the true purpose of domains identified as fast flux domains. This case demonstrates highlights those opinions by a detailed study of a domain which upon initial inspection provided only weak evidence of being a fast flux domain. Additional studies added support to the fast flux classification of this domain and had the unexpected side-effect of uncovering a sizable multi-purposed fast flux network.

Link to complete study: https://st.icann.org/pdp-wg-ff/index.cgi?randy_vaughn_s_case

Annex V – Fast Flux Metrics

A number of organizations have been collecting data about fast fluxing domains. The methods and data used to detect and monitor fluxing domains vary, but each data set provides unique graphical perspectives on the scope of the issue.

The data sets presented here are based on separate research activities by Arbor and Karmasphere and include:

- New Fluxing Domains Detected by Date
- Total Number of Fluxing Domains by Date
- Total Number of Fluxing Domains by TLD
- Number of Fluxing Domains per 10,000 registered domains by TLD

Key observations:

- Fast Flux is an ongoing problem.
- Take downs have a temporary impact but miscreants move to other hosting environments.
- The problem is not limited to one TLD, or to gTLD or CCTLD.
- By domain volume, 95-99% of all fluxing domains discovered have been detected in .CN, .COM and .NET.

Note that discrepancies in results between Arbor and Karmasphere are due to differences in detection techniques used by each organization.

New Fluxing Domains Detected by Date

Graphs 1 and 2 illustrate the number of new domain names used in fluxing attacks each day over a period of three months. "New" means that the domains had not been previously identified as actively used in a fluxing attack. The Y-axis represents the total number of domains, ranging from 1 (various dates) to a peak in 6465 on 1 November 2008 (Karmasphere) and 3695 on 8 October (Arbor).

The spike on November 1 2008 in Karmasphere’s detections came from an injection of a large number of .CN domains into the largest fast flux botnet being tracked by Karmasphere.

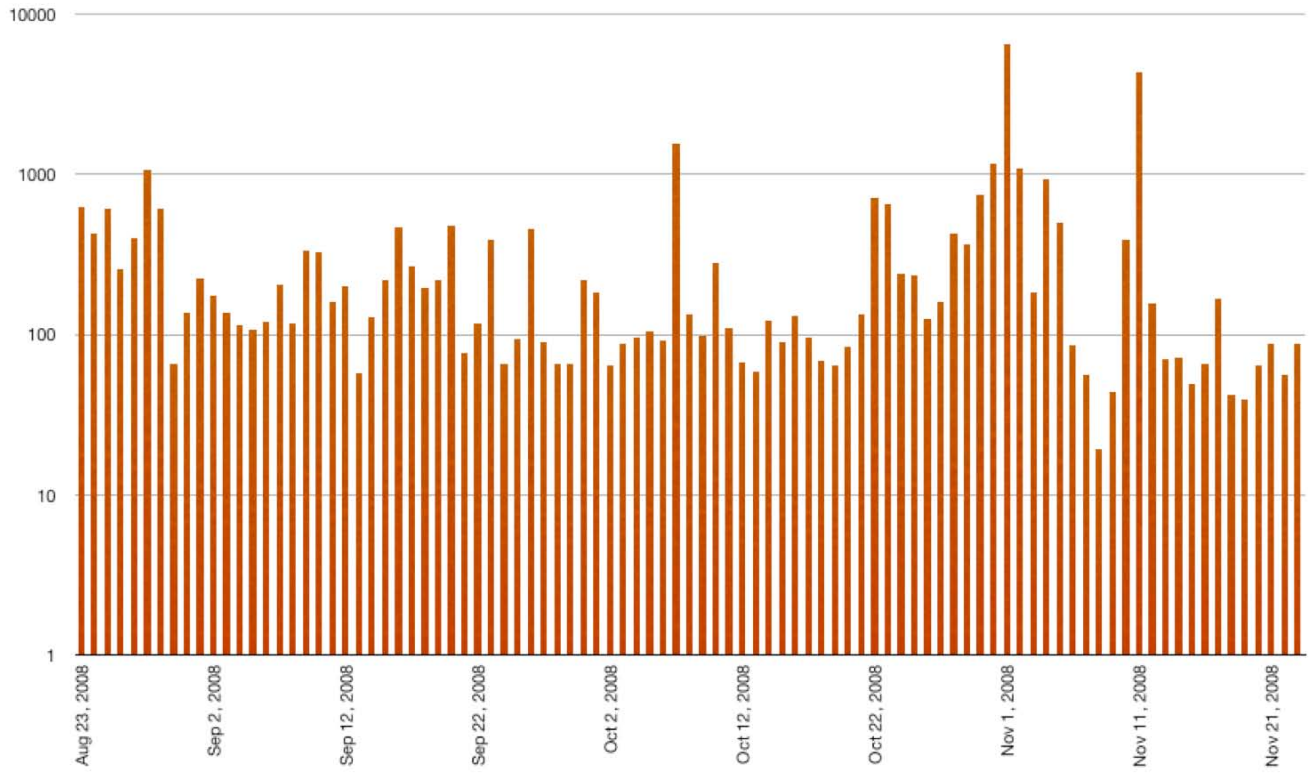
The average number of new fluxing domains detected daily by Karmasphere was 361 domains/day. The median was 133 domains/day.

The average number of new fluxing domains detected daily by Arbor was 104 domains/day. The median was 38 domains/day.

Differences in detection results between Karmasphere and Arbor are based, at least in part, on different data sources and heuristics.

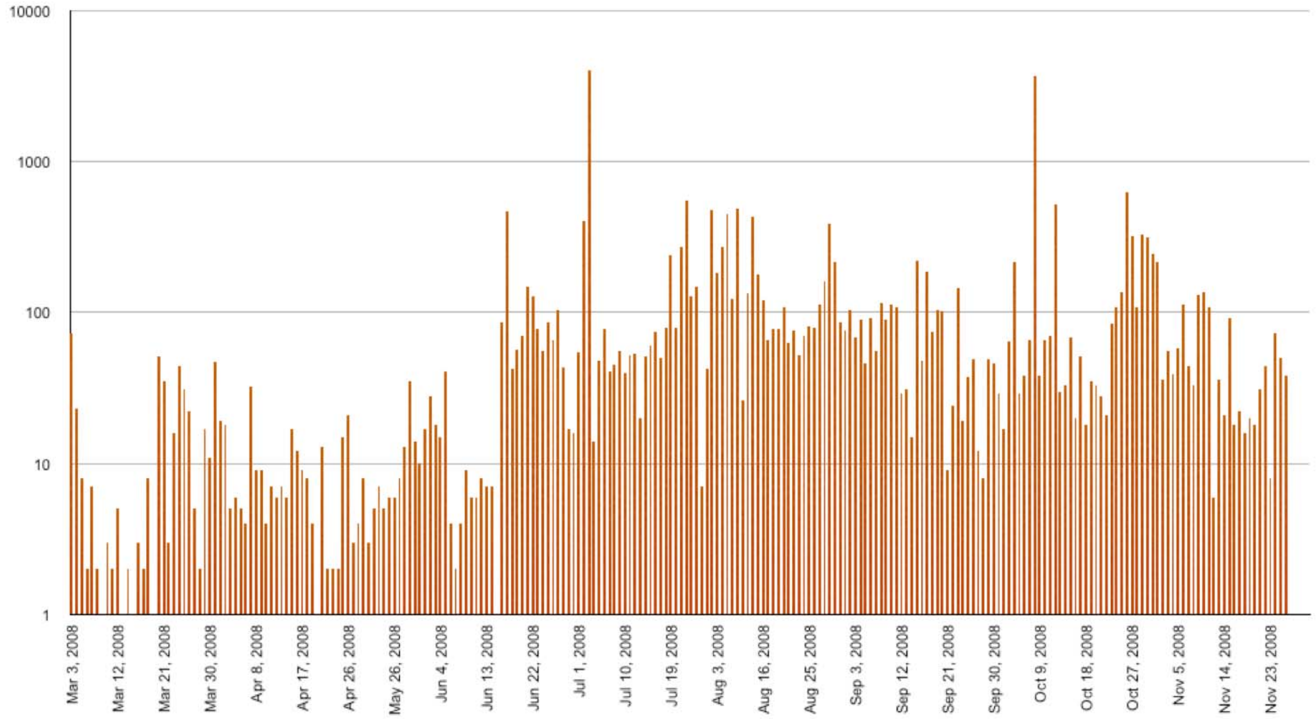
Graph 1 (Logarithmic Y-axis)

Fluxing Domains Detected: 8/23/08 – 11/23/08 (Karmasphere)



Graph 2 (Logarithmic Y-axis)

Fluxing Domains Detected: 3/3/08 – 11/26/08 (Arbor)

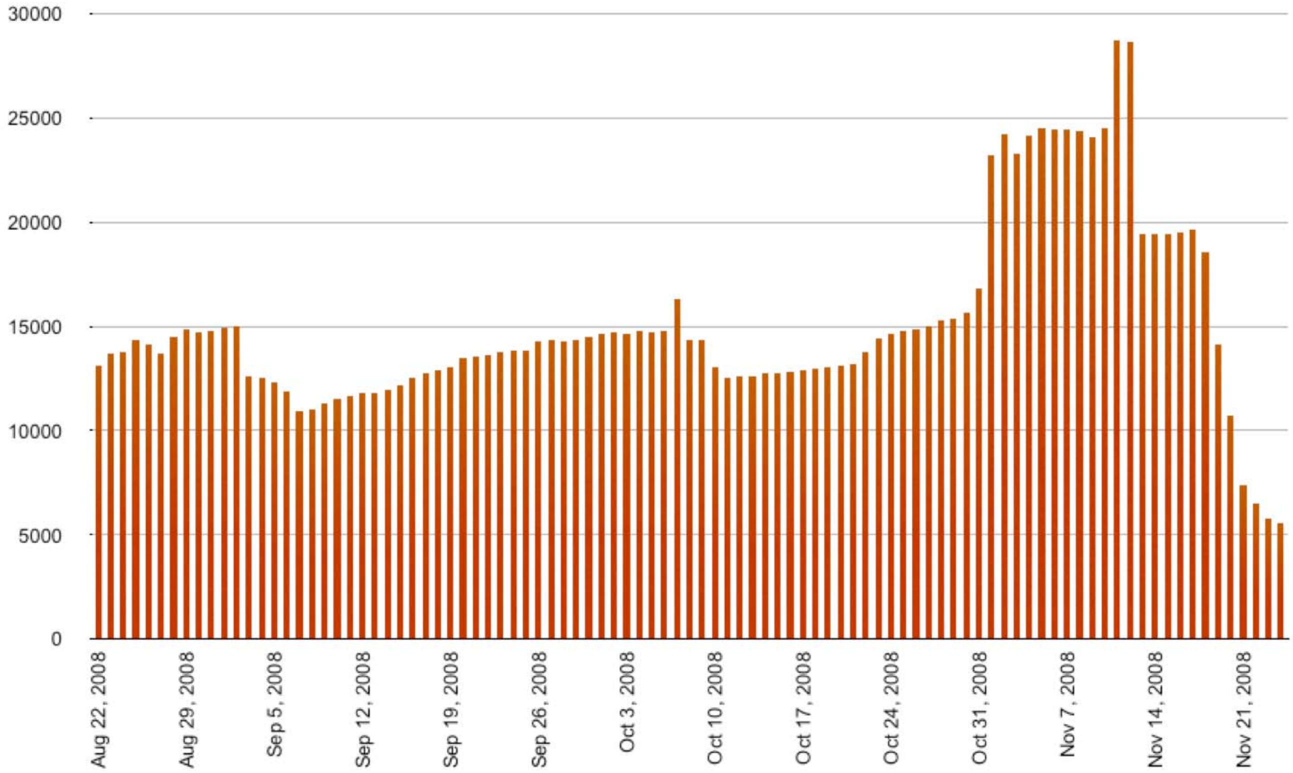


Total Number of Fluxing Domains by Date

Graph 3 illustrates the total number of fluxing domains used in fluxing attacks each day over a period of three months. For each day of the measurement period, this graph illustrates the sum of the domain names detected to date that continue to resolve using DNS and continue to exhibit malicious fluxing characteristics. The graph illustrates the persistent nature of fluxing attack networks.

Graph 3

Total Number of Fluxing Domains: 8/23/08 – 11/23/08 (Karmasphere)



Fluxing Domains Detected by TLD

The pie charts illustrate the distribution of fluxing domains by TLD and include both generic and country-code TLDs.

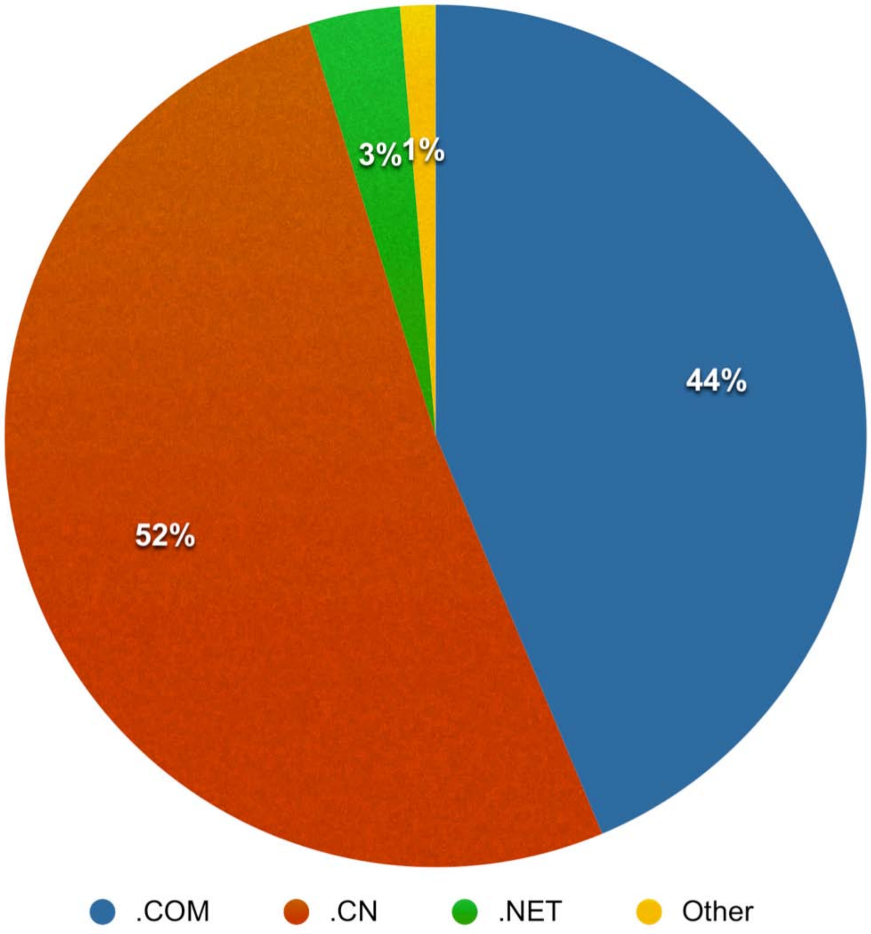
Karmasphere and Arbor independently found fluxing domains in 37-39 TLDs and 95% or more of all fluxing domains in just 3 TLDs - .CN, .COM and .NET.

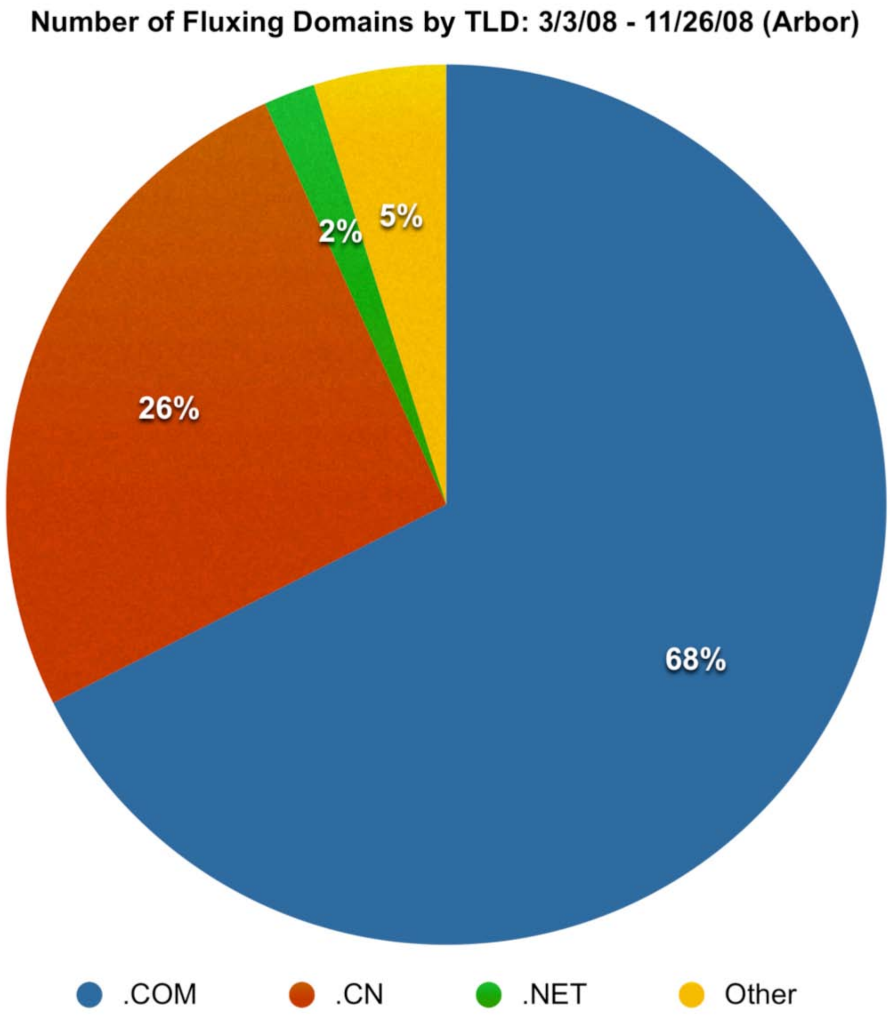
During Karmasphere's three month measurement period, the largest concentration of fluxing domains discovered by Karmasphere was in the China (CN) TLD, representing 52% of overall fluxing domains. The second largest concentration was found in .COM (44 %). Fluxing domains were found in a total of 37 different TLDs . 99% of all fluxing domains were discovered in .CN, .COM and .NET.

During Arbor's eight month measurement period, the largest concentration of fluxing domains discovered by Arbor was in the generic .COM TLD, representing 68% of overall fluxing domains. The second largest concentration was found in .CN (26%). Fluxing domains were found in a total of 39 different TLDs . 95% of all fluxing domains were discovered in .CN, .COM and .NET.

The pie charts illustrate absolute counts. This does not take into consideration the total number of registered domains per TLD, and thus may not be the most accurate way to determine the incidence of fluxing domains of any TLD relative to others.

Number of Fluxing Domains by TLD: 8/23/08 - 11/23/08 (Karmasphere)





Fluxing Domains Detected Proportionately by TLD

Using a useful metric used by the Anti Phishing Working Group in their "Global Phishing Survey: Domain Name Use and Trends in 1H2008" (See: www.antiphishing.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf), the number of fluxing domains were analyzed to see how many fell into which TLDs. The absolute counts by TLD are interesting, but the sizes of the various TLDs vary widely. To place the numbers in context and measure the prevalence of fluxing in a TLD, we use the Metric "Fluxing Domains per 10,000".

"Fluxing Domains per 10,000" is a ratio of the number of fluxing domain names in a TLD to the number of registered domain names in that TLD. This metric is a way of revealing whether a TLD has a higher or lower incidence of fluxing relative to others.

The following tables show only those TLDs that have at least 10 fluxing domains, at least 10,000 registered domains and one or more fluxing domains per 10,000 domains registered in that TLD.

Top 7 Fluxing TLDs by Score (Karmasphere)

Rank	TLD	TLD Location	Number of Fluxing Domains (8/23/08-11/23/08)	Domains in Registry (July 08)	Score: Fluxing per 10,000 registered domains
1	.CN	China	24171	12,364,615	19.55
2	.SU	Soviet Union	42	68,891	6.10
3	.BZ	Belize	19	43,500	4.37
4	.COM	Generic TLD	20488	78,191,881	2.62
5	.NET	Generic TLD	1617	11,903,723	1.36
6	.ME	Montenegro	10	95,007	1.05
7	.ASIA	Pan Asia/Asia Pacific	21	209,722	1.00

Top 5 Fluxing TLDs by Score (Arbor)

Rank	TLD	TLD Location	Number of Fluxing Domains (3/3/08-11/26/08)	Domains in Registry (July 08)	Score: Fluxing per 10,000 registered domains
1	.SU	Soviet Union	52	68,891	7.55
2	.CN	China	6,393	12,364,615	5.17
3	.BZ	Belize	14	43,500	3.22
4	.COM	Generic TLD	16,818	78,191,881	2.15
5	.RU	Russian Federation	155	1,535,153	1.01

Fluxing Domains by TLD (Karmasphere and Arbor)

TLD	Fast-flux domains observed by Karmasphere (8/23/08 - 11/23/08)	Fast-flux domains observed by Arbor (3/3/08 - 11/26/08)
com	20488	16818
cn	24171	6393
net	1617	470
org	33	399
uk	48	177
ru	81	155
tk	75	86
su	42	52
biz	39	38
mobi	27	34
in	14	25
eu	14	25
name	24	22
cc	22	22
tv	21	16
ws	14	15
info	28	14
bz	19	14
kg	7	13
jp	3	13
us	14	12
gs	16	12
be	12	10
me	10	7
es	5	7
md	1	6
ca	6	6
asia	21	6
st	2	5
ec	2	5
ph		4
tw	5	3
cz	10	3
at	3	2
ua		1
li	2	1
it		1
fr		1
ch	3	1
vu	1	
hk	1	

Annex VI – Individual Statements

Please note that the following individual statements were submitted in response to earlier drafts of this initial report and therefore do not necessarily relate to the current content of the report.

Fast Flux Lessons Learned, a Personal Reflection

Mike O'Connor

I. Introduction

There are some observations that I would like to share that fall outside the scope of the deliverables of the Fast Flux working group. The points I will make in this paper relate to several chartering issues which made it very hard for the good people who volunteered for that effort to complete the task they were given. I view this commentary as a way to record some "lessons learned" in hopes that we can avoid some of these issues in the future.

I'm writing this in the first person to highlight that these opinions are strictly my own, and arise from the experience of Chairing the working group. I am deeply honored to be offered the opportunity to serve in this role and quite enjoyed the experience – although there were times when I felt like I had my hair on fire and was putting it out with a hammer. I eventually resigned, mostly because of the issues that I'll describe below.

I view ICANN and the GNSO as very young organizations that are going through a process of maturing – and transitioning (as many organizations have before) from being a start-up into a more mature and stable organization. This is often the time in the life of the organization that professional management techniques are introduced – and we can see that on the "functional management" side of ICANN with the introduction of strategic-planning and budgeting processes.

I would submit that we need to pay attention to strengthening ICANN and GNSO "project management" capabilities as well. To clarify – "functional management" techniques apply to running organizations that continue forever (a payroll function, a corporation, etc.) while "project management" techniques apply to projects (which have a beginning, middle and end) that produce deliverables of some sort.

I would further submit that the process by which we deliver the primary "product" of ICANN (policies) is through a series of ephemeral projects which develop recommendations for ongoing functional organizations (the Board, the Councils, etc.) to act on. Strong project-management capability **and** functional-management capability will be helpful in ensuring our ongoing success.

Once in my career, I was a project manager who could fairly reliably deliver (or rescue) small to mid-sized ($1 million to $5 million) technology projects. My skills are out of date – I haven't managed a project of that size since I retired almost a decade ago. Nonetheless, there are some fundamental principles that still apply – and perhaps the most fundamental of all is the value of developing good project charters. That old adage "it doesn't matter which way you turn the wheel if you don't know which way is West" applies to projects just as well as functions. Strategic plans are what guide functions, charters are what guide a projects.

The Fast Flux working group suffered from having a poorly defined charter, and I feel very strongly that we need to do better at this if we are to nurture an ever-larger cadre of skillful and energetic volunteers to participate in working groups. Conversely, if we continue to launch projects (PDPs, whatever) without good charters, we will burn out those same volunteers and find it ever more difficult to recruit new ones.

II. **Chartering** – the basics

Here is a set of questions which, when answered, can provide a pretty good charter for a small project like the ones we run during the PDP process. There are a number of recognized standards in this area, I am using this list only because I developed it and thus can share it without getting in trouble with intellectual property attorneys (a group that is well represented within the GNSO, I say with a smile). I would submit that launching a project without answers to questions like these is a Bad Idea.

Mike's Pretty-Good Project-Chartering Questions

Problem Statement

What is the problem (or puzzle) to be solved? How does not solving this problem get in the way of achieving the organization's objectives? What is the chronology of the situation - how did you get here? Are there trends at work - social, industry, financial, economic? Is this a 'solution' that has turned into a problem - if so, what is the original problem that this solution-turned-problem was supposed to solve? What alternatives have been explored?

Stake Holders

Who will be affected by the problem? Which employees? Stakeholders? Customers? Others? Have they been involved sufficiently up to this point? Should they be brought in to the project? When? To what degree do they share the belief that this is a problem that needs to be solved? Who ought to 'champion' this project? To whom should the project team report? Has a project leader been selected yet?

Scope, Size and Perspective

What written definition clearly distinguishes between what is inside this project, and what is outside? What is the level of detail and precision involved in this effort - is this a sweeping global effort (like a vision or strategy) or is this a project to produce specific outcomes (like install a system, or build a house)? What is the point of view that should be taken during the project - there can be more than one, better to identify them rather than discover them at final review. What is the degree of generalization being sought?

Goals & Objectives

What tangible, deliverable things do we want to see when this project is completed? How do we know when the project is done?

Critical Success Factors

What things do we need to do well in order for this project to succeed? What are the attributes of projects like this that have succeeded in the past? Describe some projects of this type that have failed. What can we do to avoid those problems this time?

Preferred Problem-Solving Approach

Who will do what, with whom, by when? What are the intermediate milestone events or deliverables that we can use as checkpoints to monitor the progress of the project? Are they more than 1 or 2 weeks apart? Do we need more (or fewer) objectives to keep the project under a reasonable level of control?

Readiness

How dissatisfied are people with the current state of affairs? How clear is the vision? Do people think this project needs to happen? Do people have the tools and training they require in order to perform their role in the project team? What do other people in the organization need to do in order to get ready? Is the project team in need of some time to establish how they are going to work together, or have they succeeded as a group before?

Resource Requirements

What people, time, money, access-to-decision-makers, technology, space, etc. do we estimate this project to take? How well do people understand the resources required to solve the problem? Are those resources available, or do we need to redirect from somewhere else? Is there wide support, and willingness to commit the resource, across the whole organization? Do people think the change is worth the investment? What are the organizational impacts (how broad, how deep)?

I'd like to make a series of points, based on this list of chartering questions.

III. Problem statement – ours was too broad

We struggled on several dimensions because the problem statement we were provided needed to be narrowed before our initiative was launched. Were we to be a research group trying to understand the definition and impact of fast flux? Or were we a design group, trying to craft good responses for the community? Were we chartered as a policy group, trying to hammer out changes to rules that would be applied to various Constituencies? The questions we were posed touch on all of these and more. Which, to use an engineering example, is like trying to buy the steel for a bridge at the same time that we're determining whether a bridge needs to be built while simultaneously developing tools to test how deep the water is.

IV. **Stakeholders** – we had uneven representation

A number of working group members observed that we needed to have more people at the table. This was a very healthy observation. Countless projects have failed because the project team didn't include participation from all the people who had a stake in the outcome. To again hold up an example from another industry, a Human Resources project will fail if they install an employee system without involving the security and regulatory staff, a Manufacturing project will fail if they don't have the cost-accounting people at the table, etc.

At the same time, we had a cadre of people who represented one stakeholder group, who had a tendency to drown out the voices of the others. This project "leaked" members pretty much right from the start as moderate and opposing voices drifted on to other things. I've got some ideas about how to address this – take a look at the "Resource Requirements" section below.

V. **Scope** – ballooned dramatically, almost immediately

We had a very difficult time managing the scope of this project, partly due to the issues in the Problem Statement, but also because we didn't have a written definition of what was in scope (and what was not) before we started the effort. That blew up when we realized that some definitions of Fast Flux are much broader than others. That, combined with the overly broad Problem Statement, resulted in a project with a gigantic scope on a fixed timeline. Much like trying to make a baby in a month by putting 9 women on the project, this resulted in some weird tensions.

"Scope creep" is a phenomenon that kills a lot of projects if it's not managed. Fast Flux was a project afflicted with "scope gallop." With perfect hindsight I realize that I should have taken this issue back to my Steering Committee and gotten a ruling on this the first time I recognized what was going on. Part of the trouble there was that I didn't have a Steering Committee, nor was I required to make periodic status reports to anybody. Thus, there really wasn't an avenue for this discussion, except through my Council Liaison, who happened to be the primary advocate for the flawed charter we were given. Take a look at "Resource Requirements" for a discussion of that issue as well.

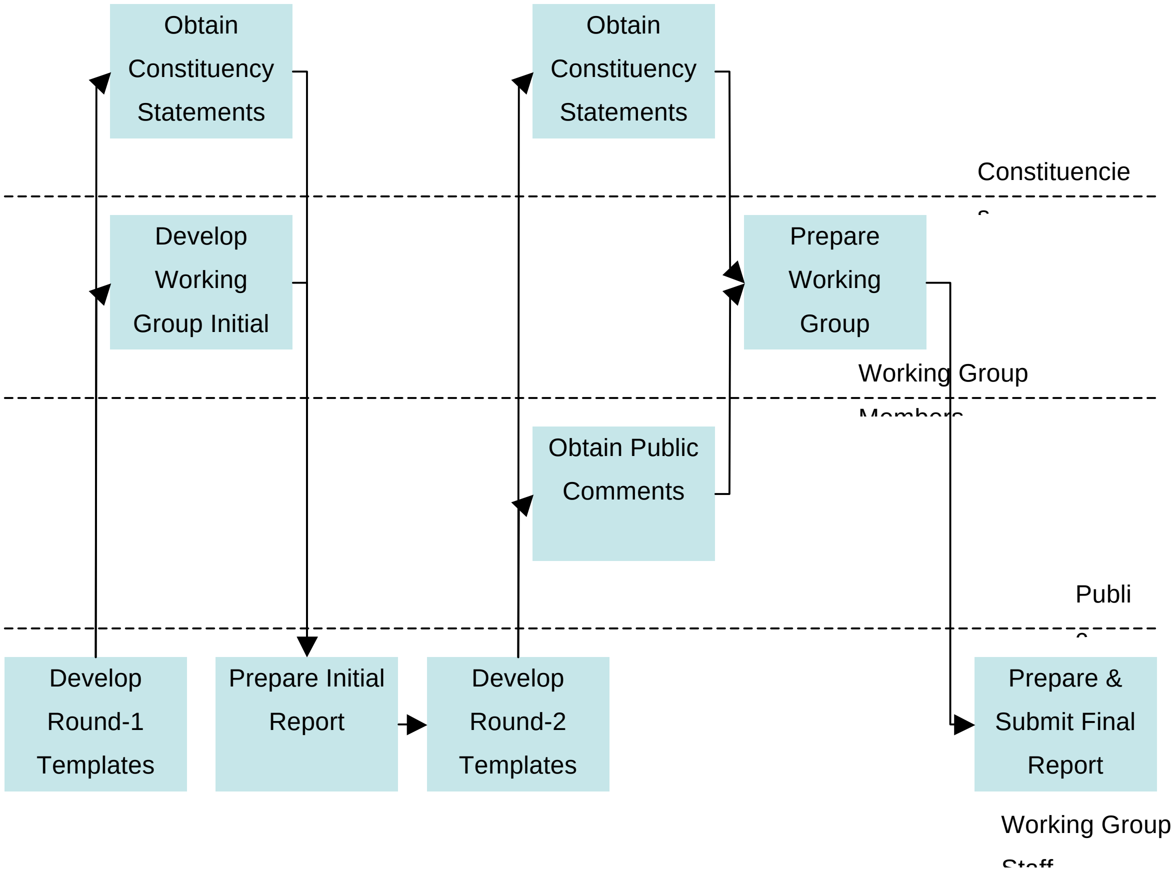
VI. **Approach** – we had several kinds of project, all in the same wrapper

"Approach" in project-manager-speak is the description how the work is broken down – what tasks need to be done, what sequence they should be done in, what deliverables should be produced, etc.

We used a PDP "approach" to structure the work of the Fast Flux working group. That approach is best suited to making very narrowly-cast, incremental changes to an existing body of policy. Unfortunately, that approach was **not** well suited to the work that we were engaged in, nor did it address all the deliverables we were asked to produce.

Sometimes pictures are helpful, so here are several illustrations of this point.

Current approach – a working-group PDP


Obtain Constituency Statements
Obtain Constituency Statements
Constituencie
s
Develop Working Group Initial
Prepare Working Group
Working Group
Members
Obtain Public Comments
Publi
c
Develop Round-1 Templates
Prepare Initial Report
Develop Round-2 Templates
Prepare & Submit Final Report
Working Group
Staff

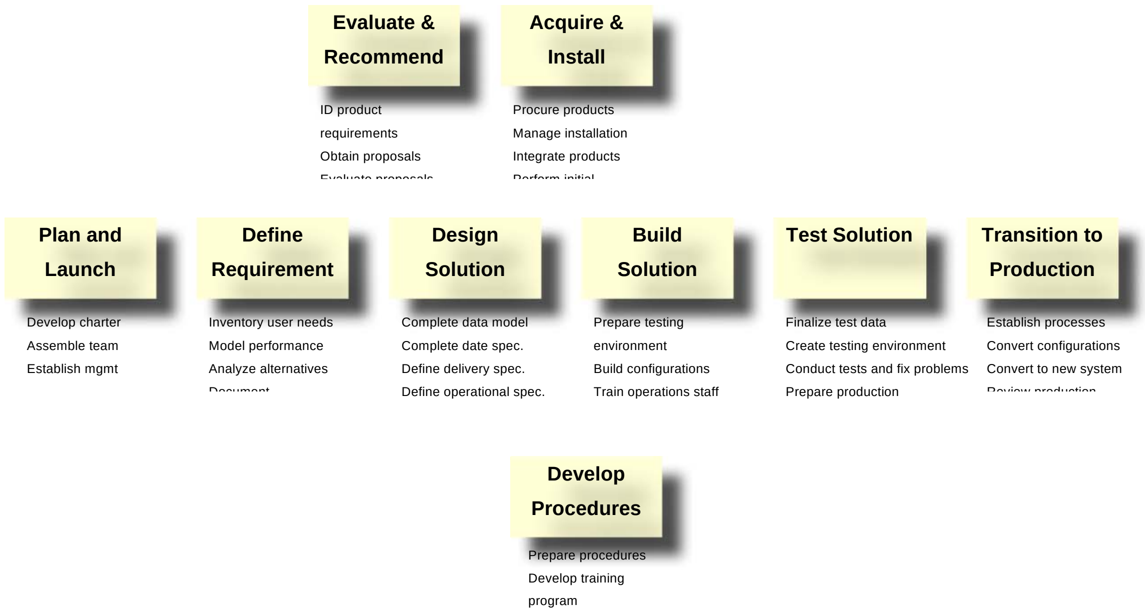
This is the series of tasks and deliverables that we operated under in this project. It caused a little stress because of the need to adhere to fixed timing defined in GNSO bylaws, rather than timing that's defined by the amount of work to be done. But the biggest problem is that this is an approach designed to deliver policy – which isn't all of what we were asked to do in our charter.

Alternate Approach #1 – Traditional System-Selection and Implementation

One component of what the working-group was asked to do was to answer the question "what technical and policy measures could be implemented by registries and registrars to mitigate the negative effects of Fast Flux?"

This is a huge question – not unlike the question "what new systems could we put in place to fix our payroll processes, or improve manufacturing efficiency?"

This is not just a policy question – it's a solution-selection question. Here's a diagram of an "approach" that's often used to answer that kind of question in the systems world. We weren't asked to do all of this, but we were asked to do the things on the left side of the diagram.



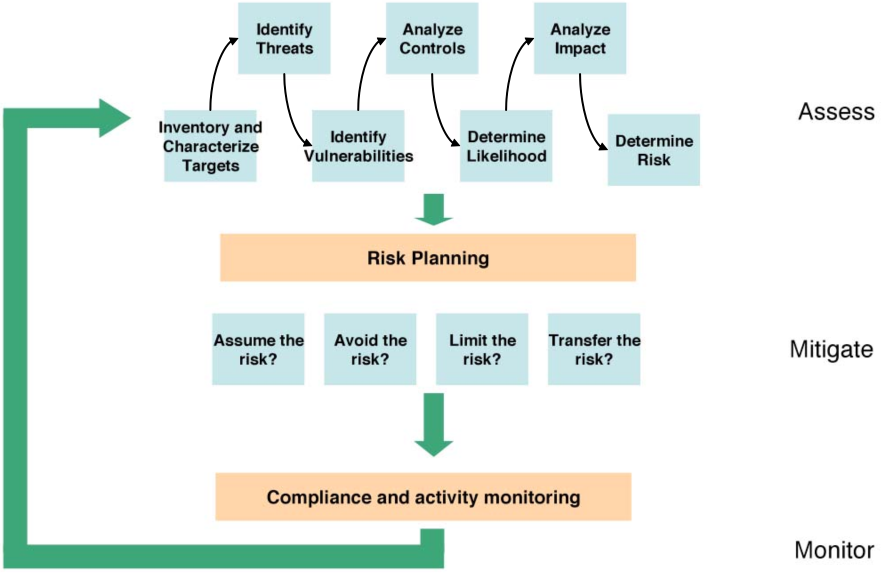
Several observations are in order. First, this is work that's usually done in phases, not all at once. Each phase takes longer, uses more (but less senior) people, and will fail if managed badly. This kind of project typically takes between 6 and 36 months, depending on the scope of the problem being addressed. Trying to accomplish this kind of work within the constraints of a PDP "approach" is doomed from the start.

Another important point – this kind of project is almost always preceded by a project to assess the need and develop a (financial and operational) **justification**. Questions of "who pays for what?" are almost always answered before a project like this are kicked off. Please note that nowhere has there been any justification work done when it comes to the issue of Fast Flux. Indeed the staff report alludes to this in their Staff Recommendations section when they say that they "recommend that the GNSO sponsor further fact-finding and research concerning guidelines for industry best practices before considering whether or not to initiate a formal policy development process."

But wait! There's more!

Alternate Approach # 2 – Risk Management

Another question the working group was asked to answer was "how are Internet users affected by Fast Flux hosting?" This is quite different from the "policy" and "solutions" questions discussed above. Indeed, I would argue that this is a risk-management question – and for that, there's yet another industry-standard approach that could be applied;



Actuaries the world over will recognize this approach. It's what they do for a living, as do corporate risk-managers. Projects like this are also undertaken by information-security teams that are trying to inventory and manage the risks associated with the systems they are charged with protecting. Indeed, new law in the United States requires this kind of work be done (and documented) on a regular basis. The scope of this question is breathtaking, and this kind of project also typically takes anywhere from 6 to 36 months to complete.

I would submit that the quite-spectacular lack of factual evidence backing up the claims of the Fast Flux team would have been avoided had we included some of this here Risk Management stuff in our project charter.

All of this discussion (and all of these pictures) is simply a series of examples to show that:

- the "Approach" section of a project charter is not trivial,
- one size (PDP in this case) does not fit all, and
- the charter we were given did not acknowledge the scope and scale of work that would be required.

VII. **Readiness** – we weren't ready

Another component of a good project charter is an operational and organizational readiness assessment. The important thing here is not to focus on the negative (I would propose that the Fast Flux working group suffered from several readiness issues) but rather to discover what the organization and the team need in order to get ready for the work to follow.

For example – I'm not ready to run a marathon today. That's not a good thing or a bad thing, it's just a statement of my readiness. It's also clear what I would need to do if I wanted to get ready to run such a race (change diet, graduated training program, etc.).

We faced several readiness issues during this project. Probably the most fundamental was the **lack of agreement that this effort should be undertaken at all**. That disagreement (both on the GNSO Council, and among the working-group members) resurfaced time and again during our deliberations – and should have been resolved by the people developing the charter, before the project was launched. Another approach to this would have been for the working group to recast its charter in such a way that everybody could agree to it, but that was impossible because there was no mechanism available to make charter revisions.

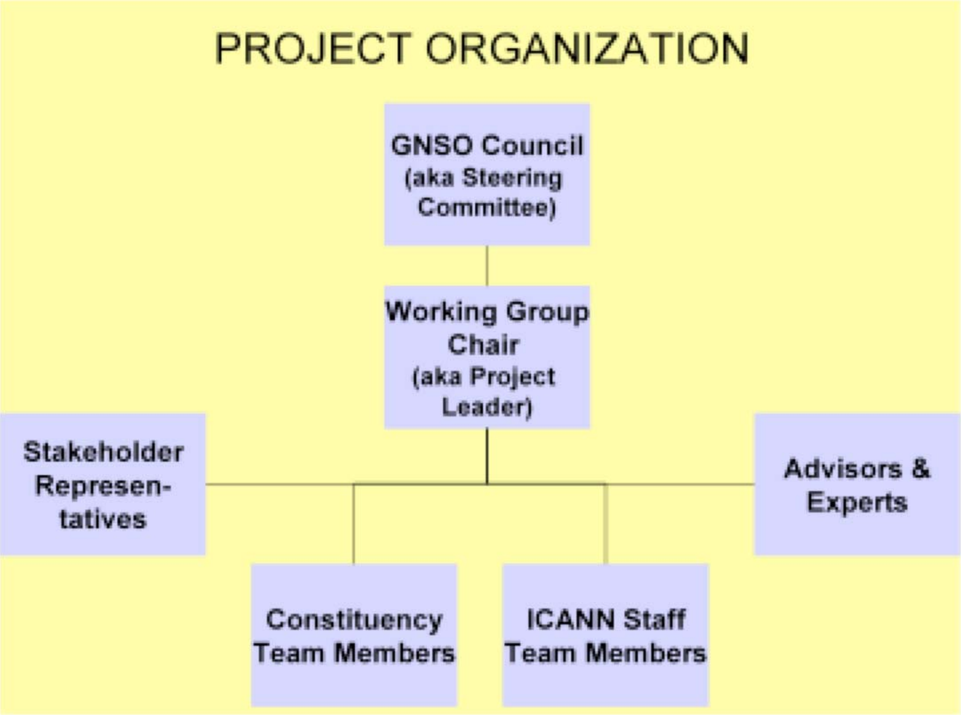
Another readiness issue has to do with the makeup of the team. Unlike most PDP teams which are limited to members of GNSO constituencies and who are familiar with the constraints of the policy-making process, the Fast Flux working group included a much broader range of people. With crystal clear hindsight, I should have recognized this problem and spent some time bringing people to a shared understanding of the limits of what can be accomplished in a policy-making project defined by the PDP process.

VIII. Resource Requirements – we didn't know our respective roles and responsibilities

I'm starting to see a pattern in PDP projects. They suffer not being well chartered when it comes to resources. I'm used to a process where resources, organization, roles, responsibilities, and project timing are laid out before the project starts (once the problem-statement, scope, approach, etc. have been defined). That hasn't happened in the PDPs I've been involved with and certainly didn't in this one. The upshot is that roles weren't clear, dates were missed, people get frustrated and so forth.

Several issues in the Fast Flux PDP were caused by classic mistakes in the way the effort was organized. Again, my analysis benefits from 20/20 hindsight. The good news here is that we are presented with a substantial opportunity to improve the odds of success **and** provide the means to develop volunteers and leaders.

Here is an example of a classic project organization chart (lightly edited to reflect a GNSO context)


PROJECT ORGANIZATION
GNSO Council (aka Steering Committee)
Working Group Chair (aka Project Leader)
Stakeholder Represen-tatives
Advisors & Experts
Constituency Team Members
ICANN Staff Team Members

And here are the roles and responsibilities that are typically associated with each of these;

- **GNSO Council (aka Steering Committee)** – Provides sponsorship, sets policy and direction, resolves key issues, provides resources, accepts and acts on findings

  Note what an active statement of participation that is. Steering committees are generally considered part of a project team, and are assigned a very important role to play. I think it would have been very helpful to have an active Steering Committee for the Fast Flux working group. We got into a fair amount of trouble because we didn't have a clear path to resolving these chartering issues. Having a clear understanding of who the Chair reports to would go a long way to solving this problem. If the Council finds it too cumbersome to act as that committee, one option might be to designate a subset of the committee to act in this role.

- **Working Group Chair (aka Project Leader)** – Has overall day to day project responsibility; planning, outreach, coordination and control

  Here's a puzzler. If we have projects that need to be done (like PDPs) and we want them led by constituents rather than staff, how are we going to ensure that those leaders have the skills and tools that they need to be successful? Most of us aren't trained as project leaders and yet that's the role that's being asked of the Chair. A Chair also needs to be credible within the GNSO's cultural and political landscape. Since it's impossible to create instant history within GNSO, I think that we will need to focus on providing project-management training and support for our constituent-Chairs. I have a bit more to say about this in the "Progression" section below.

  It's important to make the distinction between project leadership and project administration (or project management). Project administration is a staff function that can quite appropriately be handled by a staff person who has the right training and skills. Work planning, scheduling, status reporting and so forth fall into this bailiwick. T'would have been lovely to have had this kind of role called out right from the start.

- **Constituency and ICANN-Staff Team Members** – Are responsible for work products, analyses and deliverables

  One of the interesting moments I had was when one of the working group members announced that, since I'd signed up to be Chair I'd also signed up to summarize all the email we'd exchanged (something on the order of 1500 messages at that point) and produce a first-draft report. I think we'd all have benefitted from clearer definitions of our roles before we got under way. What do we expect of team members? Is it the same each time? Who decides? A good charter could have helped with this.

  Another puzzler – right now constituent team members are self-selected volunteers. How do we protect a PDP project from being captured by an enthusiastic bloc of volunteers who share the same views? Should we really rely on self-selection to populate the core working-team of a PDP, or should we find a way to recruit an effective core team and find another place to engage volunteers? See below.

- **Stakeholder representatives** – Raise issues overlooked by the team, improve preliminary conclusions and endorse findings

  One phenomenon I've observed is that there are people who sign up for working groups simply to keep tabs on what's happening, and only participate if things don't seem to be going their way. This makes it hard to build cohesion within the core working-team because it's hard to know who's in that core group and who's there as a representative of a point of view. I think it would have been good for the working group if the "representing" folks had been separated into their own group and engaged differently than the core day-to-day working-team members. See above.

- **Advisors and Experts** – Provide skills and knowledge not available from GNSO volunteer and staff team members

  Same goes for this group. I had a pretty wild time on the Fast Flux working group coping with the dynamics between the people who were in the working group as subject-matter experts and those who were there as GNSO constituents. Again, if I were granted unlimited powers, I'd put the experts in a separate group and treat them differently than core work-team members.

- **Council Liaison**

  Note that I left the Council Liaison role out of this picture. I'm not convinced that it's a good idea to put a filter between project leaders and their steering groups. In our case, the liaison was also the sponsor of the project on the GNSO Council and that made the communication between the team and the Council even more complicated. If the liaison idea stays, I think it would be a good idea to clarify what that person's duties are and make sure that they're an impartial player in the conversation between Chair (project leader) and Council (steering committee).

Progression

One useful byproduct of all this organization-chart and role-definition stuff is that we might be able to kill two birds with one stone. For sure we'll improve the way our PDP projects work, but we could also use this to provide an orderly way to deepen our pool of volunteer participants and avoid putting people into roles before they are ready.

We (ICANN and the GNSO) are like any organization that needs to deliver a lot of projects – we need to be aware of how we develop our (paid and volunteer) human resources. One model we might want to look at is the large consulting firms. In those organizations, your role in projects changes as you progress. At first, you are a junior member of a working-team and you get lots of support and supervision. As your skills mature, you are given progressively more responsibility within working-group teams. If you turn out to be a person with the potential to be a leader, you are then given the opportunity to assist in the project-management duties. If you prove to have the skills and inclination, you get to lead larger and larger projects. I call this the "let no good deed go unpunished" school of HR development.

The Fast Flux working group would have benefited a lot from having this structure in place. As it was, we had a Chair (that would be me) that was in there before he was ready, and it hurt us.

If we crafted this "progression" idea well, we could create an orderly framework to broaden participation (and build a shared culture) within the GNSO. As a relatively new member of the GNSO gang, I can testify that it's pretty hard to figure out who's who and what's going on. It would have been great to be introduced to the organization by somebody saying "if you want to get to know us, you might consider signing up a small role in a Working Group as a place to start."

IX. Conclusions

Enough. This has already grown too long. Here's a little series of bullets for those of you who've made it this far:

- The group thought it was outside the scope of the working group to either fix its own charter, or recommend changes for the future (I disagree, hence this narrative)

- The working group's charter was flawed – it was too broad, contained several fundamentally different kinds of work, was shoehorned into an inappropriate (PDP) "approach," had weak/narrow sponsorship and ill-defined organization structure.

- GNSO should consider using a more rigorous chartering process before launching PDPs – in the case of larger efforts (like Fast Flux) the chartering effort may have to be a project in and of itself

- GNSO should consider developing alternative approaches when the required work falls outside the narrow bounds of the PDP process (e.g. research projects, solution-evaluations, risk management, etc.)

  - Develop in-house (staff or volunteers) capability, or
  - "Outsource" the work to better-qualified organizations, or
  - Contract to have the work done

- The benefits of good chartering and human-resource development are;

  - Greater odds of success (on-time, on-budget, meet need)
  - Improved buy-in for recommendations and work products
  - Easier projects to run, and deliver
  - Less stress on project participants
  - Broader involvement
  - Deeper pools of policy-making volunteers and leaders

Again, thanks for the opportunity to Chair this effort. Sorry I didn't quite get it across the finish line.

Mike O'Connor

Things Learned, Knobs Not Turned

Eric Brunner-Williams

September 8, 2008

Abstract

This is important. Kaminsky took a known concept and did the hard engineering work to make it feasible. To slightly misuse a quote that's more often applied to crypto, amateurs worry about algorithms; pros worry about economics. The economics of the attack have now changed. (And we need to get DNSSEC deployed before they change even further.)
Steve Bellovin, in a note to NANOG, in the context of discussion of the cache poisoning exploit. This note attempts to identify some of the economics of the issues present.

1 Preface

The process for the GNSO-FF-PDP-May08 Working Group is slightly confusing. Either the WG is tasked to conduct some novel task, nominally some "research" activity or activities, or the WG is tasked to develop Constituency Statements, which may or may not contain some "research" component. This is the abridged personal notes from a GNSO-FF-PDP-May08 Working Group Contributor.

2 Things learned thus far

We know that discussion of this subject is complicated by the assumption by some that "fast flux" is a technical term, or a term for a criminal activity, or both.

In this note I adopt the convention that what is called "fast flux" has a "bad use" and a "good use" This should not be understood to mean that I think either use is "bad" or "good" only that I observe a social convention that amounts to an abuse of notation.

2.1 Mechanism(s)

We know that "fast flux" is just one technique used, and that it is used together with other techniques, from overt email to covert instant messaging, for good and bad purposes. We also know that "the bad use" of the technique uses a domain name in the message payload (via email or htttp or ... instant messaging or ...), in the past one (or more of a set of) fixed ip address was used, and if domain names and a fixed payload weren't more economic than a set of ip addresses in a set of payloads, that "the bad use" would still be using address sets rather than "fluxed" domains, and will return to using address sets and sets of payloads if domains become less economic for their business model(s).

We can get the "bad use" out of the DNS, in theory (ignoring cost, the risk to "good use" and who pays it all), but that won't get the "bad use" out of the net.

What is more, as ipv6 transition continues, and router vendors, and network service providers adapt to the physical fundamentals, which affects the business fundamentals of network service providers, whatever the "bad use" can exploit it will to retain and expand its business model(s).

2.2 Non Harm, Non Locus, Non Interest

There is no data that "fast flux" is affecting the operations of the IANA root, or any gTLD, or ccTLD registry.

There is data that "bad use" exploits some of the gTLDs, COM, NET, ORG and some others, but not all, and also exploits some ccTLDs, CN, and some others. The "bad use" is proportional to volume, no other relationship is yet supported by data. The same applies for "good use" (load balancing, censorship evasion, etc.).

Government is not involved in the Working Group.

2.3 Security, Stability, TTLs and ICANN Contractual Parties

While decreased TTL values for nameservers could increase load on the root and registry servers by a factor of 5, the number of NS records being "fluxed" is sufficiently small that actual load induced is not detectable. We're also unable to find any damage to registries, registrars, or registrants, directly and uniquely produced by "bad use" to those roles and their standing in the ICANN gTLD system, and suspect the same is true for the IANA ccTLD system as well.

2.4 Definitional Works

We've got an improvement over the original definition, and in the course of doing so have developed an understanding that discerning "bad use" from "good use" requires human intervention, and even so may fail.

There is no consensus about the scope of the Working Group, some think it is a debating exercise, some think it is an exercise whiteboarding solutions, etc.

2.5 Who plays? Who pays?

We don’t know if this is a real problem, or even a solvable problem. If it is a real problem, it appears that the cost is intended to be paid by registrars. Arguing against this being a real problem is the fact that the network operations community (with or without the ICANN ASO and/or GNSO ISPC, as presently constituted) is uninvolved. Similarly, Government is uninvolved.

3 Knobs are for Turning

This isn’t our problem. It isn’t our problem because we can’t fix it. It isn’t our problem because it doesn’t affect us.

3.1 It isn’t our problem because we can’t fix it.

We could fix it if the second “N” in “ICANN” weren’t a fiction. However, both the institutional engagement of the NRO ARIN, RIPE, APNIC, LACNIC, AfriNIC in ICANN, at the BoD level, and at the GNSO level is negligible, and the operational role of the IANA is limited to allocation of ASnums and IP address blocks. BCP 38 is not sufficiently operationalized to make IP spoofing an unreliable service.

We could fix it if the first “N” in “ICANN” were operational. However, despite adequate institutional engagement by generic DNS registries and their registrars, their operational role in DNS is also limited to allocation of some 2LD (and for some, 3LD) DNS resources. And of course the whole “fix” fails outside of the g-space. DNS QID non-randomness was demonstrated during the lifetime of the WG.

The requirement for what is called an RPKI (routing public key infrastructure) arises from real “security and stability” issues. AS36561, AS7007, AS27506 and AS9121 are all events which altered routing. Today’s “accidents” are tomorrow’s exercises in operational art. AS path prepending was demonstrated during the lifetime of the WG.

3.2 Anchors

The authority/delegation models between the name spaces and the address spaces are analogous. However, both lack operational means of validation. In theory, were validation of each possible, the two could share a common trust anchor, and in theory, ICANN could manage the common trust anchor. Of course, multiple trust anchors are also possible. Indifference to the trust model is equivalent to indifference to RFC 2826.

3.3 The Shared Fate Problem

Any mechanism which is indifferent to the stability and security of the operating systems executing on network attached nodes, that is, which accepts socializing the cost of Microsoft's memory protection model to third parties, and relies upon some property of the attached network, and which attempts to validate some information originating elsewhere, to enable some admission control or related mechanism(s), requires a mechanism to provide trust, and some anchor for that trust.

3.4 A Proof of Concepts

A Resource Certificate Trial was conducted by APNIC using X.509 v3 Public Key Certificates (RFC3280) with IP address and ASN extensions (RFC3779), using OpenSSL as the foundational platform (adding resource extension (RFC3779) support) with the design of a Certification framework anchored on the IP resource distribution function.

3.5 What we're not doing, and why we're not doing it

We could be fixing, or sharing the trust anchor(s) that enable fixing, the authority/delegation predicates for policies which degrade the value of the compromised assets which make ancillary use of the DNS. Unfortunately, we're not, and we're not likely to be given (a) the 2nd "N" problem (at both levels), and (b) the 1st "N" problem and the institutional benefits of identifying a "security problem" which can only be cured by advancing a profoundly absurd agenda within the GNSO-C.

3.6 No Cause, No Effect

It isn't our problem because it doesn't affect us. Not the IANA root. Not the gTLD registries. Not the ICANN accredited Registrars. Not the Registrants. Registrants loose domains, but not because of this. Registrars go out of business or their ICANN chit is yanked, but not because of this. Registries, well, no failure data yet, some failure to thrive data, but none of it remotely attributable to this.

4 Retail Economics

Registrars need not process credit cards, and registrars may offer prices above the sum of the ICANN and registry fees. There is no requirement arising from the RAA to offer prices below-cost, nor to race to the bottom and subordinate registrar business interests to the interests of the credit card industry. We don't necessarily have credit card fraud, and because registrars which do not have credit card fraud also do not have a lot of similar abuse issues, abuse appears to be more sensitive to price and highly automated resource provisioning than any other control. A similar observation may made for registries which are "more expensive" or "more policied" than the legacy registries and their business model imitators.

Not only should we be unwilling to accept the consequences of non-registrars-non-registries attempting to socialize their costs to registrars and registries, we should be unwilling to accept the consequences of sub-cost registrars attempting to socialize costs to actual-cost registrars.

The RAA does not require us to share the fate of the credit card industry, or to adopt their fraud risk, or place ourselves in the position of being likely to be the target of a take-down attempt or domain hijacking to benefit businesses which elected to share the fate of the credit card industry and adopt their fraud risk. We're not unaware of the problem, or indifferent to it, but socializing the cost of theft from some victims, who accepted the risk, to more victims who did not, and have no share in the benefits from that involuntarily shared risk, doesn't solve the problem, it merely repeats the theft.

Unintended Consequences

There have been unintended consequences.

We need to reconsider the institutional role of "security" We can accept that ICANN's "security" agent may be compromised, and is in the present. Do we leave it unminded, pretend it didn't happen, and won't happen again, or do we take it as a given and institutionalize corruption, parcel out the "security" budget to the constituencies and get on with "security" being both subjective and created by compromise? The capture of the "security and stability" blob in the org chart by the "identity theft" mob is a non-trivial event. The upcoming SSAC Review is the appropriate venue to pursue the question of the SSAC's performance, structure, and institutional responsibilities.

Issues with the Charter
By Christian Curtis

The working group struggled to produce answers to the questions in its charter. The working group believes that this is due largely to the way in which the charter was formulated, and is concerned that the issues before it may be too expansive and/or improperly framed. For this reason, the working group wishes to document its concern and provide recommendations to the GNSO council in case it wishes to further evaluate this issue.

Definition

The working group had difficulty with the definition of fast-flux it was provided with. The charter adopted the definition of "fast-flux" used in the GNSO issues report. That definition reads,

> *[T]he term "fast flux" refers to rapid and repeated changes to A and/or NS resource records in a DNS zone, which have the effect of rapidly changing the location (IP address) to which the domain name of an Internet host (A) or name server (NS) resolves.*

The working group felt that applying this definition would excessively limit the scope of the PDP beyond the council's intent. Despite its best efforts, however, the working group has been unable to reach consensus on any alternative definition.

The primary problem presented by the definition in the charter is that it focuses excessively on a single technological measure. There was widespread agreement within the working group that the networks that the council intended to address had many characteristics beyond that included in the definition. Furthermore, the group largely agreed that the "rapid and repeated changes to A and/or NS resources records" was not an essential characteristic of such networks—this was largely because a network could make these changes slowly and still present the same issues. The working group was not, however, able to reach agreement on which characteristics were essential to define a network as a "fast flux" network. In fact, this issue was a significant point of contention.

The primary reason reaching a definition was so difficult is that it is inherently tied to questions of which action the group will recommend and the appropriate role of ICANN. For example, one suggestion was that the working group limit the definition of “fast flux” to include only those networks operating on compromised hosts. While this definition would provide an inherent justification for combating all such networks, it operates on an assumption that we can identify compromised hosts, it requires that a new term be coined to refer to those networks that could potentially be misidentified, and it may not address the harms from otherwise identical networks that operate on an “opt in” basis. Similarly, another early suggestion was that “fast flux” be defined only to include those networks with a criminal purpose. This definition, however, assumes that it is appropriate for ICANN or the registrars to performed an adjudicative function by determining which laws apply and whether those laws were breached.

The consequence of this intertwining of definition and policy resulted in the working group's inability to agree upon a definition. Each potential definition implied an appropriate course of action, so each member found their opinion about a proposed definition shaped by their beliefs about what the GNSO wanted to address, what the GNSO should address, and what action the GNSO should take.

Despite this disagreement as to how to define a “fast flux network”, the working group was able to identify several of characteristics of the networks we believe to council intended it to address. Such networks frequently:

- Operate on one or more compromised hosts (i.e., using software that was installed on hosts without notice or consent to the system operator/owner);
- Are 'volatile’ in the sense that the active nodes of the network change in order to sustain the network’s lifetime, facilitate the spread of the network software components, and to conduct other attacks; and
- Use a variety of techniques to achieve volatility including:
  - (rapid) modification of IP addresses for malicious content hosts, name servers, and other network components via DNS entries with low TTLs;
  - dispersing network nodes across a wide number of consumer grade autonomous systems;
  - monitoring member nodes to determine/conclude that a host has been identified and shut down; and

- time, or other metric-based, topology changes to network nodes, name server,
- proxy targets or other components."

Scope and Process

The working group additionally encountered difficulties from the scope and nature of the PDP. The wide variety of issues, coupled with a lack of clear and orderly means of addressing these issues led to difficulty addressing any one issue without becoming mired in the others. The working group feels that the council should be aware of these problems so that it may strive to avoid them in initiating other PDPs on this or any other issues.

Part of the working groups difficulty stems from path dependency. For example, insofar as the first two questions, "who benefits from Fast Flux and who is harmed?" and "who would benefit from cessation of the practice and who would be harmed?" are intended to identify stakeholders to bring into the process, these questions should be answered and addressed before moving on to the more substantive questions. Similarly, it would be counterproductive to suggest action and then determine the scope of the issue to be addressed.

While it may be possible in many cases for a working group to determine the best path for a PDP, that proved exceedingly difficult in this case. One reason for this is that certain path choices must be made by the council in drafting the charter, rather than in the PDP. For example, the working group did not feel that it had authority to suspend the PDP while reaching out to other stakeholders. Another reason is that creating an effective process requires at the outset a clear understanding of the nature of the work that will be required at each step. Such an understanding was not possible in this case because the issue to be addressed was not well defined and because some of the basic research was ongoing throughout the PDP process.

The working group also encountered difficulty stemming from the broad scope of the PDP. As the chair at one point observed, the working group contained both members primarily interested in the policy implications of any proposed action and members primarily interested in crafting a proposal that would be technologically effective. These categories are hardly discreet, since every member had views on both issues, but it does serve to highlight a division of priorities, expertise, and concerns within the working group.

The borrow the language of the chair, the result was “like trying to buy the steel for a bridge at the same time that we're determining whether a bridge needs to be built while simultaneously developing tools to test how deep the water is.” While the obvious solution would be to ask members of the group to temporarily suspend certain questions when asking others (for example by assuming that ICANN is the appropriate entity to address the issues while considering what actions would be possible), this proved to be neither simple nor feasible in practice. The technical and policy questions were more intertwined than, “should we have a bridge here” and “how should we design a bridge here.” Proposed technological measures often rested on policy assumptions such as 'it is appropriate to encourage registrars to take down domains based on content hosted there,' while answers to policy questions may well depend on what technological measures are available.

Misleading Answers

Several of the questions asked by the GNSO council are particularly likely to solicit misleading answers. Questions such as “who benefits from fast flux and who is harmed?” as well as “Who would benefit from cessation of the practice and who would be harmed?” seem aimed not merely at identifying stakeholders but also at providing the council with information to understand the consequences of any action considered by the GNSO. Yet, as these questions are formulated, the answers to them will provide little guidance to the council and may give false impressions. Consequently, the council should carefully reformulate these questions before rechartering this or any other group on the subject.

One problem with these questions is that they assume only one possible action by the GNSO—a complete ban of fast flux. If the working group were convened purely to evaluate the consequences of such a ban, then this formulation may be helpful. The working group, however, has also be asked to consider all possible means of addressing fast flux and to determine the extent to which the issue is appropriate for GNSO action at all. The various potential measures discussed by the working group would have differing impacts on different parties. Because the working group was unable to address the impact of specific measures requested elsewhere in the charter, it wants to be quite clear that any answers to the first two questions suggested during this PDP are in no way an assessment of impact of any GBSO action.

Another problem with these questions is that they fail to quantify the benefits and harms that they address. The questions merely ask who benefits and who is harmed, not how and to what degree. This can lead to some misleading answers. Nearly any criminal activity that can benefit from an online presence can benefit from evasion techniques. Thus, some efforts to answer these questions have resulted in expansive lists. Yet, these lists do little to illuminate the extent to which fast flux impacts these activities. No action ICANN takes will eliminate crime on the Internet, so merely listing ways in which fast flux is used does little to assess its impact. While the working group attempted to address this issue, it feels that more research is necessary to do so, and advises the council not use any answers suggested to the first two questions as an assessment of the effect of the availability of fast flux.

The working group's struggles with the definition of fast flux further creates potential for misleading answers. For example, one early proposed definition of fast flux would have included only the malicious uses of the technology and hence categorically excluded all legitimate uses from any answer to the charter's first two questions. Since the working group has failed to agree upon a definition of fast flux, the council should be cautious about any inferences it draws from answers to these questions. More importantly, potential means of addressing fast flux will vary significantly depending upon how fast flux is defined.

Conclusion

Though the working group has not taken upon itself to recommend or evaluate alternative processes, it does feel that the council should be aware of these observations both to better understand the groups output and to possible avoid or alleviate these problems in future PDPS.

[i] http://www.icann.org/committees/security/sac025.pdf

[ii] Although the report (SAC 025) refers only to “agreements,” the SSAC presentation on Fast Flux Hosting at the February 2008 ICANN meeting in Delhi (http://delhi.icann.org/files/presentation-rasmussen-fast-flux-13feb08.pdf) made it clear that the intended reference is to “accreditation agreements.”

[iii] Resigned from the Working Group on 9 October 2008

[iv] Joined the Working Group in October 2008

[v] Joined the Working Group in October 2008

[vi] Resigned from the Working Group on 27 September 2008

[vii] From a message by Rod Rasmussen to the WG email list.

[viii] This list simply captures the ideas that were discussed by the members of the WG, noting arguments either in favor or against an idea only where the WG as a whole achieved rough consensus.

[ix] A DNS-based system could provide similar or additional data than WHOIS systems do, and at rates higher than many port 43 WHOIS servers currently allow.

[x] Related to policies, a purpose of the recent "GNSO Issues Report on Registration Abuse Policies" was to "identify and describe various provisions in a representative sampling of gTLD registration agreements which relate to contracting parties' and/or registrants rights and obligations with respect to abuse". The report found that among the gTLDs, "research found that eleven out of sixteen gTLDs have provisions in place that address (seven of eleven) or potentially could address (four of eleven) abuse." Many ccTLDs also have policies against criminal and/or abusive uses of domain names, with .DE and .UK being but two examples. Related to needs, various studies have demonstrated that the amount and types of abuses vary greatly from TLD to TLD, and that some TLDs do not suffer certain types of abusive domain name uses at all. For example, see the Data Annex to this FFWG report by Arbor Networks and Karmasphere, The Anti-Phishing Working Group's "Global Phishing Survey: Domain Name Use and Trends in 1H2008" report, and URIBL.COM TLD statistics.