Executive Summary for Fast Flux Initial Report

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?

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) 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.

  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.
- 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:

  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 behaviour 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 behaviour, but it does recognize the way in which fast flux techniques are used to prolong an attack.

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.

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

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).

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.
- While no registrar has been prosecuted for facilitating criminal activities related to fast flux domains, there is at least one recent case where some would argue there is the appearance of complicity, namely ESTDomains.

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

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.

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.

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" behaviour (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.

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.

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.

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

One source of best practices for protection 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.

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).