Draft 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 [TBC]. 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

TBD…

2 Report Process and Next Steps

This Initial Report on fast flux is prepared as required by the GNSO Policy Development Process 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 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)[1], 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."[2]

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 that "the GNSO sponsor further

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

[2] 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."

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 taken from the GNSO Issues Report on Fast Flux Hosting – 31 March 2008 and does not reflect the opinion of the Working Group on the issue. Indeed, one of the major conclusions of this working group is the need to further study and refine the definition of "fast flux" before undertaking further steps. Please look to the body of this report for further discussion.

"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. 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 anti-crime investigators.

How fast flux works

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 does not reflect the opinion of the Working Group on the issue. Again the working group wishes to emphasize the need to further study and refine the operational definition of "fast flux" before undertaking further steps. Please look to the body of this report for further discussion.

The goal of fast-flux is for a fully qualified domain name (such as www.example.com) to have multiple IP addresses (sometimes hundreds or even thousands) assigned to it. These IP addresses are changed in and out of zone file A (host address) and/or NS (name server) 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 connecting 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 are using to host their scams have the best possible bandwidth and service availability. They often use a load-distribution scheme which takes into account node health-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 someone 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 URLs for advertised content no longer 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. It is the upstream fast-flux mothership node, which is hidden by the front end fast-flux proxy network nodes, that actually delivers content back to the victim 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 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 is a technique that is 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 SMTP, POP, and IMAP can be delivered via fast-flux service networks. Because fast-flux techniques utilize TCP and 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 time-to-live 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. A high-traffic site 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 quickly is considered by these service providers to be important enough to offset the additional query latency introduced by more-frequent DNS lookups.

Marika Konings 9/23/08 12:17 PM
Deleted: preliminary

Marika Konings 9/23/08 12:17 PM
Deleted: anecdotal

Marika Konings 9/23/08 12:17 PM
Deleted: some

Marika Konings 9/23/08 12:17 PM
Deleted: may

Marika Konings 9/23/08 12:20 PM
Deleted: More research is needed to better understand legitimate uses and their prevalence, once a more robust definition of “fast flux” has been developed.

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”.

Marika Konings 9/23/08 12:21 PM
Deleted: anecdotally

[Tentative] Illicit Uses of Fast Flux

Marika Konings 10/13/08 10:09 AM
Deleted: **Why fast flux is a problem**

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 create robust, obfuscating service delivery infrastructures that 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.

In addition to the weekly conference calls, extensive dialogue occurred through the fast flux mailing list. Over 490 e-mails 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.

In order to reflect that many positions in this report are not consensus views, it was agreed by the Working Group to use the following labels to indicate the level of support for a certain position:

- Agreement – there is broad agreement within the Working Group (largely equivalent to "rough consensus" as used in the IETF)
- 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.

4.1 Members of the Working Group

[Tentative] 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.

Name	Constituency/other	Affiliation

Beau Brendler	ALAC	
George Kirikos	CBUC	Leap of Faith Financial Services Inc
Minaxi Gupta	Individual	Indiana University USA
Adam Palmer	Individual	PIR
Avri Doria	Nomcom Appointee, Council Chair	Lule Univ of Tech
Chuck Gomes	RyC, GNSO Council Vice Chair	Verisign
Christian Curtis	NCUC	
Eric Brunner-Williams[3]	RC	CORE
Greg Aaron	RyC	Afilias
Ihab Shraim	RC	Mark Monitor
James Bladel	RC	Godaddy
Joe St. Sauver	Individual	Security Programs Manager, Internet2, University of Oregon
Kalman Feher	RC	MelbourneIT
Liz Williams	CBUC	LSE
Marc Perkel	Individual	Internet business (Ctyme.com)
Margie Milam	RC	Mark Monitor
Mark McFadden	ISP	BT
Mat Larson	RC	Verisign
Mike O'Connor[4]	CBUC	
Mike Rodenbaugh	CBUC	Rodenbaugh Law
Paul Diaz	RC	Networksolutions
Paul Stahura	RC	ENom
Philip Lodico	CBUC	FairWinds Partners
Randy Vaughn	Individual	Information Systems Hankamer School of Business Baylor University
Rodney Joffe	RyC	Neustar
Rod Rasmussenn	Individual	Internet Identity
Steve Crocker	SSAC	Shinkuro
Steven Vine	RC	Register.com
Tony Holmes	ISP	BT
Wendy Seltzer	ALAC	Brooklyn Law School
Zbynek Loebl	IPC	

The members of the Working Group are:

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

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

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

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 e-mail threads and Working Group conference calls. As far as possible, answers to the charter questions have been clustered together in different groupings. Due to the challenges outlined in Chapter 6, the Working Group abandoned the effort to provide answers to charter questions or reach consensus, but focused instead on issues such as the definition of fast flux, reviewing different fast flux data sources and describing options for next steps.

Fast flux characteristics

Marika Konings 9/18/08 2:00 PM
Deleted: definition

> *Note: Although it is not one of the explicitly stated "charter questions," the question "what is fast flux?" was determined to by the working group to be a crucial underpinning of any further discussion. The working group feels that this conversation needs to be continued and completed as the first order of business in any subsequent effort. The working group developed the following preliminary characteristics, but did not reach consensus and offers this draft as a way to capture progress to date.*

Marika Konings 9/18/08 2:01 PM
Deleted: *working definition*

"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)[i];
- 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;

Marika Konings 9/23/08 12:27 PM
Deleted: Is

Marika Konings 9/23/08 12:27 PM
Deleted: one or more

- 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 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 server

[Tentative] There was support in the Working Group to add the following characteristics:

- Elements of the attack network run on compromised computers
- Whois records are fraudulently created (e.g. using stolen identities or payment methods)

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 resiliency 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 (a) the accuracy of WHOIS information (an issue which is being considered in a broader ICANN conversation, and is not unique to fast flux) and (b) the question of what constitutes "criminal intent."

Charter questions

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

Note: While there is not consensus on this point, a majority of working group members feel that it is important to note that "fast flux," as defined above, is a technique which is beneficial or harmful only to the extent that it is used to conduct beneficial or harmful activities. The WG found it impossible to come to consensus around the answers to questions of "who uses fast flux 'legitimately', who uses it 'maliciously,' and who is harmed by either use?" because of the difficulty associated with determining or assigning intent and legality. It also should be noted that the way in which fast flux has been characterised above, as an attack technique related to compromised hosts, would make it inconsistent to speak about 'benefits'. Nevertheless, the WG did identify a number of benefits that are outlined below.

Marika Konings 9/18/08 2:02 PM
Deleted: *defined*

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) that must adhere to very stringent availability metrics and use short TTLs to rapidly relocate network resources which may come under attack.

[Tentative] In addition, there was agreement to include: while those sorts of 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 would impact organizations which rely on short TTLs in order to be able to relocate resources as part of the process of mitigating distributed denial of service attacks, would impact organizations moving nameservers, and would impact organizations which rely on short TTLs in order to provide a variety of legitimate services, among others.

[Tentative] As an alternative viewpoint, the following was offered: 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 (ccTLDs and private 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, and so on, 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 (http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00371.html).

Marika Konings 9/23/08 2:05 PM
Deleted: and activities

Marika Konings 9/23/08 2:05 PM
Deleted: , revolutionary thinking

Marika Konings 9/23/08 2:06 PM
Deleted: to avoid detection

Possible minority view

Some indicated that there is a lack of evidence to actually support this category (free speech / advocacy) as benefitting from fast flux. Some indicated that there is a lack

Marika Konings 9/23/08 2:08 PM
Deleted: Other techniques are used by these groups to avoid discovery, not fast flux, or at least no evidence has been provided to support this.

of evidence to actually support this category (free speech / advocacy) as benefitting from fast flux. Techniques other than Fast Flux (such as TOR) are used by these groups to avoid discover. Other working group members point out that operators of networks in this category are understandably reticent, and that information about these networks will always be very difficult to obtain.

"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).

[Tentative] In addition, there was agreement for the following addition: Some in the working group would point to the way in which fast flux nodes are created as prima-facie evidence of fast flux techniques constituting malicious behaviour. 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 behaviours enabled by fast flux, one non-subjective definition of 'malicious behaviour' 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

[Tentative] One alternative view was expressed in relation to the previous addition noting that 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."[5]

Note: The WG did not answer the following charter-questions due to the lack of:

- *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*

Marika Konings 9/23/08 2:16 PM
Deleted: *avoiding*

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?

1. Individuals whose computers are infected by attackers and subsequently used to host

[5] From a message by Rodney Joffe to the WG email list.

facilities in a fast flux attack network (e.g., nginc proxies, nameservers or web sites). The individual may have his Internet connection blocked. In the extreme, 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 subjected to a criminal investigation.

In addition:

- even if their connection doesn't end up completely blocked, users may experience degraded performance (as computer or network resources get consumed by the parasitic miscreant user(s) of their system)
- also, even if the ISP doesn't 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 (even some *vendors* have trouble building patches that are safe for *all* version/patch permutations, so it shouldn't be surprising if some malware also causes stability issues)

Some specific examples of how users can be harmed by this, beyond what's already been mentioned, can be seen in things like:

- 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 who get dropped by their ISP, or who become so disgusted with their ISP that they leave, 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 attendent 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 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 subjected 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 spectre 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 organisation. 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. GLBA or 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. ***[Tentative]*** Those losses may include both direct losses which a financial institution declines to make whole, as well as indirect costs (potentially higher interest rates, reduced credit lines, declined credit applications, etc.) Identity theft can also touch on national security issues, if stolen identity information is used to illegally cross borders, to illegally remain in 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).

They may unwittingly disclose medical or personal information that could be used for blackmail or coercion. ***[Tentative]*** There was support to add: or for discriminatory treatment by employers concerned with potential costs associated with identified (but latent) genetic conditions, for example. Fear that medical record systems are porus may also deter some individuals from even seeking help (“I’d like to find out what’s causing my condition, but I’m afraid that if I go in, the whole town will know I have <whatever>”). Individuals who purchase bogus products, especially pharmaceuticals, may be physically harmed from using such products. ***[Tentative]*** There was support to add: this 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 also undercut the incentive for pharmaceutical firms to invest in new drug research by cutting into their earning stream while their discovery is, or should be protected by patents. Sale of counterfeit products is another example of how fast flux networks can result in users and businesses being harmed. Counterfeit products may undermine the value of carefully nurtured brand names, leave consumers with shoddy or disfunctional products, deny nations legitimate customs revenues associated with the importation of premium brand-name products, or result in unsafe products (for example as a result of counterfeit UL-listed electrical appliances cords).

Marika Konings 10/13/08 10:51 AM
Deleted: They may infect their computers with malicious software that would "enlist" their computers into a bot herd.

4. ***[Tentative]*** 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 and they may also incur the cost of diverting staff and resources to respond to abuse reports or legal inquiries. ***[Tentative]*** Agreement was expressed to also add: or helping users to get cleaned up, or purchasing antivirus products to hand out to users, or deploying network-based remediation solutions. ISPs are harmed when spammers send spam spamvertising fast flux hosted sites, and the ISP get deluged with that 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

Marika Konings 10/13/08 10:56 AM
Deleted: access operators

port 25 blocks deployed to control direct-to-MX spam).

5. Registrars may be reputationally harmed when their 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. ***[Tentative]*** Registrars currently see wdprs.internic.net complaints in conjunction with fast flux domain simply because that's the sole complaint mechanism currently available which potentially reaches fastflux domain name abuse. Antispam activists have thus become very good at carefully scrutinizing spamvertised fast flux domain names for whois problems. Dealing with those WDPRS reports represents an additional registrar-specific cost. Providing a reporting channel that focusses on the actual issue (a domain has been detected which is engaged in criminal activity) rather than the substitute issue (there's a problem with the domain's whois data), will clarify the problem at hand.

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 images or enslavement. ***[Tentative]*** There was support to add: 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. ***[Tentative]*** Uptake/legitimate use of some TLDs may also be impacted by fast flux abuse. If the public perceives that sheer use of a domain from a particular TLD may result in negative scoring by anti-spam software such as SpamAssassin, that can be a powerful disincentive

hindering the adoption and use of that registry's TLD.

Who benefits from the use of fast flux techniques? *[Tentative]* Short TTLs" per se are NOT synonymous with "fastflux." Short TTLs are only one characteristic associated with fastflux domains.

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 a dotted quad rather than a FQDN is generally preferred by intelligent attackers because this method is more difficult to detect and isolate 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). *[Tentative]* 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, 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[ii].

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?

[Tentative] There was agreement to add that in its Constituency Input Statement (attached to this report as an annex), the RyC provided detailed notes regarding the technical and policy options available to registry operators regarding fast-flux hosting. The RyC statement includes technical notes about how the DNS functions, the data available to registry operators, fast-flux detection methods, uses of short TTLs, and other pertinent items. The RyC's answers to question 3 question 7 are of interest in this context.

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

5.5 How are registrants affected by fast flux hosting?

5.6 How are Internet users affected by fast flux hosting?

[Tentative] 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 fastflux nodes, we need to step back for a moment and consider the related problems of malware and spam. Internet miscreants use malware -- viruses, worms, trojan horses, etc. -- to efficiently gain control over large numbers of vulnerable networked consumer PCs. Those compromised systems, subject to remote manipulation by shadowy masters, are commonly known as "bots" or "zombies." Having obtained control over those compromised PCs, the miscreants can 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").

[Tentative] There was support to add:

What_Are_Miscreants_to_Do_With_Compromised_Hosts_That_Can't_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 through following those recommendations, as it now is at many ISPs worldwide, 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 the ISPs control port 25, that leaves the shadowy "bot herders" with millions of compromised systems which are now incapable of directly spamming remote mail servers.

Spammers_and_Other_Internet_Miscreants Have_a_Hard_Time_Getting_Web_Hosting_

At the same time, spammers (and other miscreants) find themselves confronting a second orthogonal problem: it has become hard if not impossible for them to obtain and retain mainstream web hosting for illegal content. While what's 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" (advertised via spam), because they recognize that to permit spamvertised products or services on their hosting service will commonly result in their address space getting listed on one or more anti-spam DNS block lists, such as those operated by Spamhaus [http://www.spamhaus.org/].

Miscreants Discover One Thing They CAN Do With Non-spamable Compromised Hosts

With that for background, it is easy to imagine what happened next: spammers repurposed some of their "surplus inventory" of compromised-but-unspamable systems to provide "web hosting" for illegal or spamvertised content which they couldn't host elsewhere.

[Tentative] There was agreement to add:

Reverse Proxies Are Used to Actually Deploy Fast Flux Hosting Networks

Spammers actually replicated all the hundreds or thousands of html files, images, databases and other bits and pieces of content and software making up a sophisticated web site on each of dozens or hundreds of fastflux hosts. That would be too complex, too error prone, too time consuming, and too easily detected. Instead, spammers found that they could use "reverse proxy" software to accept web connections on the compromised consumer host, tunnelling that traffic back to their actual (hidden) backend master host. "nginx" is one product often used for that purpose, although it is also routinely used by regular web sites as well. The compromised consumer PC then acts as if it were delivering web pages, but in reality it is just acting as a pipeline to a hidden master web server (or farm of servers) located elsewhere. [insert suitable illustration here showing reverse proxy setup here]

Use of Botted PCs Is Non-Consensual and Surreptitious

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

[Tentative] There was agreement to add:

Post Fast Flux Infection Cleanup

Once the user discovers that they've been botted and used for fast flux purposes, they are then left with the unenviable chore of trying to get their compromised system disinfected. Because of the complexity of cleaning many malware infections, and the substantial possibility that at least some lingering malware components may be missed during efforts at cleanup, most experts recommend formatting compromised systems and reinstalling them from scratch, however that can be a time consuming and laborious process, and one that may be practically impossible if the user lacks trustworthy backups or cannot find original media for some of the products they had been using. The need to deal with this mess is the first tangible user impact of fast flux hosting, but one which only some unlucky Internet users experience.

[Tentative] There was support to add:

One Universal Impact of Fast Flux: Spam

The next effect of fast flux hosting is one which virtually all Internet users experience, and that's spam. Remember, fast flux hosting exists to host illegal content or spamvertised products or services. All of us receive spam, whether that's an occasional message that slips through otherwise efficient filters, or a steady deluge that may have caused some of us to abandon email altogether. Without the ability to obtain reliable web hosting services, spammers are left with only a few categories of potential spam, such as stock pump-and-dump spam, where users don't need to visit a spamvertised web site to purchase a product or service. Clearly spammers are powerfully motivated to find a takedown-resistant way to host their web sites, and that's what 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.

[Tentative] There was agreement to add:

Fluxing *Name Servers* As Well As Web Sites: The Rise of "Double Flux"

Spammers quickly recognized that the name servers were a weak point in their scheme, so they adapted by beginning to not just use compromised systems for web hosting, they also began to use those systems to do DNS for their domains. A domain that does both its web hosting and which gets its DNS service via compromised systems is normally referred to as a "double fastflux" or "doubleflux" domain.

[Tentative] There was support to add:

Port Blocks Won't Work to Curtail Fast Flux Web Hosting

All of this malicious activity, taking place on systems that are not professionally administered, resulted in ISPs endeavoring to control these phenomena via the network. It is understandable why they were inclined to do so: blocking port 25 controlled the spewage of spam, even if it did nothing to fix the underlying condition of the infected host, so maybe something similar could be done to address fastflux and doubleflux abuse? Unfortunately, unlike email where controlling port 25 is sufficient to control the emission of spam, when it comes to fastflux web pages, web pages can be served on *any* arbitrary port (e.g., to access a web server running on port 8088 instead of the default port 80, one might use a URL such http://www.example.com:8088/sample.html).

[Tentative] Two alternative views were expressed stating that although there are many valid arguments to avoiding port blocking, the phenomena of double fast-flux would never had happened had ISPs routinely blocked inbound port 53. Those networks which routinely block ports by default are not prone to have hosts participate in fastflux networks. In addition, serving on an alternate port can be a signal that something is not kosher. If ISPs blocked port 80, and then end users configured 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.

[Tentative] Support was offered for the following:

ISP Efforts to Control Fast Flux and Double Flux Result in Collateral Damage

Blocking http traffic from consumer web pages thus 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 fastflux 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.

[Tentative] There was agreement that in conclusion, Internet users see their systems used without their permission by abusers who've set up fastflux nodes on them; they face the daunting task of cleaning up those compromised systems once they discover what's happened; they are the target of endless spam, spam that would be materially harder if fastflux hosting didn't exist; and they experience a loss of Internet transparency as ISPs strugle to control the fastflux and doubleflux problems on the network. The combination of those effects can result in Internet users having a pretty bad experience, all thanks to the choice by some Internet miscreants to use fast flux and double flux techniques.

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?

Note: Although the members of the WG did not reach consensus on the existence or character of "the negative effects of fast flux," and therefore did not agree on the nature of "the problem," they presented and discussed a number of potential technical and policy approaches to dealing with it. This section summarizes the ideas ("solutions") that were discussed by the WG. The WG wishes to emphasize that until "fast flux" is better defined and researched, there are insufficient underpinnings to recommend any of these – they 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[6]:

- Make additional non-private information about registered domains available through DNS-based (not WHOIS[7]) 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. ***[Tentative]*** There was support to add the following clarification: 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's being done with their resources, and to their customers.

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; ***[Tentative]*** the group did not reach consensus on or endorse any of them:

[6] 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.

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

Marika Konings 9/25/08 11:07 AM
Deleted: A DNS-based system could be queried through automation rather than manually. Whois is a manual protocol and not suitable for real time queries

- Adopt accelerated domain suspension processing in collaboration with certified investigators/responders
- Establish guidelines for the use of specific techniques, such as very low time-to-live (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's 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. 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.
- ***[Tentative]*** 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.

Note: The WG did not answer the following charter-questions due to the lack of:

- *A robust technical, and process, definition of "fast flux",*
- *Reliable techniques to detect fast flux networks while avoiding 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*
- *An assessment of need, based on the above*
- *A definition of requirements, or designs, for proposed solutions*

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?

[Tentative] There was support for the following response: Answering this question should be deferred until there is; a robust technical and process definition of "Fast Flux", there are reliable techniques to detect Fast Flux enhanced networks while avoiding false positives, there is reliable information as to the scope and penetration of Fast Flux networks, there is reliable information as to the financial and non-financial impact of these networks, there has been an assessment of need (based on the above) and, the requirements have been defined for proposed solutions.

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

[Tentative] There was support for the following response: Answering this question should be deferred until there is; a robust technical and process definition of "Fast Flux", there are reliable techniques to detect Fast Flux enhanced networks while avoiding false positives, there is reliable information as to the scope and penetration of Fast Flux networks, there is reliable information as to the financial and non-financial impact of these networks, there has been an assessment of need (based on the above) and, the requirements have been defined for proposed solutions.

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

6 [Tentative] Constituency Statements and Other View Points

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

To date, two Constituency statements (Registry Constituency and Non-Commercial Users Constituency), one input document (from individual Registrar Constituency members) and one initial reaction (Intellectual Property Interests Constituency) have been received. These entities are abbreviated in the text as follows (in the order of submission of the constituency statements):

RyC - gTLD Registry Constituency
IPC - Intellectual Property Interests Constituency
NCUC - Non-Commercial Users Constituency
Individual RC members – Individual Registrar Constituency members

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

In addition, a number of individual statements have been submitted which can be found in Annex IV of the report.

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

4.1 Constituency and Other Views

The Ryc, NCUC and a number of individual RC members all recognise that fast flux is being used by miscreants involved in online crime to evade detection, but at the same time question whether ICANN is the appropriate body to deal with this issue. All three emphasise that it is not in ICANN's remit to act as an extension of law enforcement or put registries or registrars in this position. At the same time, some members of the Working Group suggest that ICANN, the registries and registrars are not being asked to act as an extension of law enforcement, but rather to facilitate compliance with existing laws and regulation in those cases where ICANN, the registries and registrars are uniquely situated to do so.

In addition, the RyC, NCUC and a number 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 counter argument from some members of the Working Group is that while the GNSO is not responsible for administrating ccTLD policy, by showing leadership in administration of gTLD domain policies (including policies dealing with fast flux), GNSO actions may indirectly influence the ccTLD policy development process.

The RyC, NCUC and a number of individual RC members all point to the lack of data and the absence of supporting evidence outlining the scope of fast flux which is a necessity in order to balance cost – benefits of any potential solutions. The RyC and a number of individual RC members specifically point to any lack of evidence that "fast flux hosting has materially impacted the inter-operability, technical reliability and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet". At least one participant in the Working Group notes that substantial data was offered to the Working Group, both with respect to fast flux usage, and the costs associated with malicious activity facilitated by fast flux techniques.

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". Contrary to that perspective, Working Group members have described how required solutions can be implemented using existing record types and the existing/deployed resolver code base, so that protocol changes and changes to installed software is not required. See for example: http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00085.html.

4.3 Further Work Suggested by Constituencies

The RyC and RC members emphasise 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.

7 Challenges

Note: Despite the fact that the Working Group conducted its work with great enthusiasm and dedication, it encountered a number of stumbling blocks which prevented progress on answering the charter questions and finding a consensus within the group. 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, the Working Group quickly concluded 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 servers 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. However, the members do not agree as to whether ICANN is the best organization to conduct this activity. This point is expanded on in the next section of the report.

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.

The question was asked whether a PDP was started prematurely. The March 2008 Issues Report had already recommended that further fact-finding and research would be helpful in order to inform the community's deliberations.

b. Misconception about the scope of a PDP and remit of ICANN

[Tentative] [Placeholder: Include information on Affilias Abuse Funnel Request document which received agreement from the WG (proposal 41)]

As mentioned under point a, one could consider that a PDP on fast flux was premature as there was not sufficient information available to inform the debate or agreement on the exact scope and nature of fast flux. In addition, neither the GNSO Council nor the charter identified what the objective of a potential recommendation on fast flux should be.

The format of a Working Group that was chosen for this PDP also caused some issues. Various participants that had not previously participated in ICANN policy development were part of the group, which is to be welcomed as it brought new expertise and important views to the table. However, with perfect hindsight it is clear that the process should have included a period of briefings and familiarization where all participants could have been made aware of the constraints and limitations of the PDP process.

In addition, many 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.

Although the issues report clearly stated that “the overall question of how to mitigate the use of fast flux hosting for cybercrime is broader than the GNSO policy development process”, some members of the Working Group had difficulty in accepting this limitation. As a result, discussions started focussing on how to fight cybercrime, including spam and phishing, instead of looking at the narrower question of fast flux as it pertains to ICANN constituencies. As some participants pointed out, some of the discussions and proposed actions would be more appropriate for bodies like the Anti-Phishing Working Group (APWG) than ICANN taking into account its current remit.

8 Conclusions and Possible Next Steps

[Tentative] *During the study of fast flux hosting, the working group quickly came to appreciate that the subject area that originally formed the basis of the study had changed rapidly in the from the time of publication of the SSAC report that stimulated GNSO interest to the issuance of the PDP. Flux hosting, flux techniques and flux facilitated attacks continued to evolve even during the WG's study period. This section attempts to draw conclusions from a study that can in some respect be characterized as having placed the WG in the losing end of a race condition: simply put, the WG was at a disadvantage having been assigned the task of studying a moving target*

8.1 Conclusions

Fast flux hosting has numerous applications. Some experts have focused on the applications of fast flux hosting that are self-beneficial but publicly detrimental and consider it to be an effective technique for keeping fraudulent sites active on the Internet for the longest period of time, and it requires domain registrations as a component for success. At the same time, a number of many of the characteristics that experts ascribe to fast flux hosting have been identified as self-beneficial without being harmful to others, or indeed, both self- and publicly beneficial. In these latter applications, the goals of fast flux hosting are to make networks survivable or highly reliable, but the motives are quite different.

Gaining a common appreciation and broad understanding of the motivations behind the employment of fast flux or adaptive networking techniques proved to be a particularly thorny problem for the WG. Attempts to associate an intent other than criminal and characterizing fast flux hosting as legitimate or illegal, good or bad, stimulated considerable debate, as such labels are highly subjective in certain situations.

Study by members of the WG also revealed that flux hosting is necessarily, accurately characterized as "fast flux" but more generally, that flux hosting encompasses several variations and adaptations of event-sensitive, responsive, or volatile networking techniques. The WG studied many of the methods of detecting fast flux activities and thwarting fast flux hosting required participation and intervention. The WG also studied whether certain data could be monitored, collected, and made available by various parties (e.g., registries, registrars, and ISPs) to facilitate detection and intervention in circumstances where fast flux hosting was publicly detrimental. These studies merit further attention, particularly in areas where an unacceptable level of false positives would prove detrimental to registrants affected by intervention and where measures are needed to ensure that parties reporting fast flux activity are provably trustworthy.

The WG also acknowledges that fast flux and similar techniques are merely components in the larger issue of internet fraud and abuse. The techniques described in this report (and others yet to be revealed) are only part of a vast and constantly evolving toolkit for attackers; none of the techniques are necessary to the degree that mitigating any one would eliminate Internet fraud and abuse. Every attack that is enhanced by the use of one or more fast flux techniques could be pursued without them, possibly at higher cost or effort for the attacker.

These various and highly interrelated issues must all be taken into account in any potential policy development process and/or next steps. Careful consideration will need to be given as to which role ICANN can and should play in this process.

Marika Konings 10/13/08 12:19 PM

Deleted: Fast flux is considered by some experts 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 legitimate uses of similar techniques have been identified that need to 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, as fast flux (the technique) is only one component in the larger issue of internet fraud and abuse. In addition, it should not be forgotten that fast flux techniques (including short TTLs and rapidly changing A and NS records) are convenient tools for attackers, but they are not necessary - every attack that is enhanced by the use of one or more fast flux techniques could be pursued without them, albeit at higher cost or effort for the attacker.

8.2 Possible next steps

Note: The Working Group proposes the following options for next steps to address the issues and challenges outlined in this report. Please note that the WG was not able to reach consensus around all of these choices.

8.2.1 Problem statement

- Option P1 – Continue to focus on Fast Flux, a rapidly-emerging technique (that relies on Internet names and numbers) which is used to harden malicious networks

NOTE: The group has formed a rough consensus around recommending this narrower focus. However there are strong arguments to be made that Fast Flux is merely an example of a technique that leverages Internet names and numbers to harden networks used for fraud and abuse and that the broader view would lead to a more effective response.

- Option P2 – Explore a broader issue; how Internet names and numbers are used to enable Internet fraud and abuse, and the role of the ICANN community in addressing this problem

8.2.2 Scope

- Option S1 – Assess need
    - Develop process and technical definitions of the "problem" selected from above
    - Develop algorithms that can be used to detect the "problem" with safeguards to minimize false positives
    - Identify and recruit partners who can provide data for analysis and tools to analyze that data
    - Develop data that quantifies;
        - The quantity and trends of the "problem"
        - In the case of Fast Flux, determine the proportion of fraud/abuse attacks that utilize the technique
        - In the case of Fast Flux, determine the quantifiable financial and non-financial impacts of Fast Flux extrapolated from the proportions above
    - Develop a financial and operational justification for any further steps
    - Develop a charter for the next phase of the effort
    - Conduct a formal PDP to accept the results and make a go/no-go decision on the next phase

    NOTE: There is rough consensus among the Working Group that this is the appropriate next step, and that the scope of the effort should be limited to this "Assess Need" task.

- Option S2 – Also include a phase to define solutions and requirements based on the needs identified in Phase I

    NOTE: Examples of "Solutions" described in this phase could include: policy changes, pricing changes, process changes, protocol changes, software tools, information-sharing collaborations, collaborations with certified investigators/responders or something else. The working group has formed a rough *consensus that any "solution" proposal must be underpinned by a robust justification, based on facts developed during the Assess Need phase of the work.*

- Option S3 – Also include a phase to design, build and test solutions

- Option S4 – Also include a phase to deploy solutions

NOTE: Much of the difficulty encountered by the Working Group was due to the desire by some members to jump directly to this phase, while other members were still trying to develop the underpinnings to justify that move.

8.2.3 Stakeholders

- Option ST1 – GNSO, ccNSO and ALAC to participate in the effort

NOTE: There is rough consensus that these Supporting Organizations need to be included in subsequent work

- Option ST2 – Also include the ASO, IETF and GAC

- Option ST3 – Also include stakeholders external to ICANN (examples include: APWG, MAAWG, CCERT, FIRST, Artists Against 419.org, StopBadware.org, Regulatory enforcement agencies such as the FTC, Law enforcement).

8.2.4 Champion

- Option C1 – If the problem-statement remains focused on Fast Flux, GNSO should champion the effort
- Option C2 – If the problem-statement is the broader "fraud and abuse" question, the ICANN Board should champion the effort.

NOTE: There is rough consensus around these choices of "champion"

8.2.5 Approach

- Option A1 – Use a “project” approach that is less focused on pure policy-making than the PDP Working Group process.

  NOTE: There is a weak rough consensus around this choice of “approach”

- Option A2 – Include a “ratify the results” PDP at the end of the phase to provide a connection back to the policy-making process.

  NOTE: There is a weak rough consensus around this refinement of the approach

- Option A3 – Continue to use the GNSO PDP process.

8.2.6 Readiness

- Question – “Does this project need to happen?”

  NOTE: There is not consensus that a followup effort should happen – the group is about evenly divided on this.

- Question – “Should ICANN take the lead?”

  NOTE: There is not consensus that ICANN is the appropriate organization to be taking the lead on either of these issues. Again, the group is about evenly divided. The following suggestions came from those who felt that ICANN is not the appropriate lead – Law enforcement, security vendors, governments and APWG.

8.2.6 Resources

- Question – “What type of people would need to be involved?”

  NOTE: This is an undifferentiated list, polled from the working group. The group that charters the next effort should view this merely as a suggestion of possibilities and *refine the list as needed. Suggestions include; law enforcement, governments, researchers, anti-crime/anti-fraud organizations, policy developers, project managers, consumer stakeholders, data & risk analysts, Internet experts, rights-protection experts.*

- Question – "What's your best guess as to the elapsed time this project would take, in weeks?"

  NOTE: Responses ranged from 12 to 104 weeks with predominance around 16-26 weeks. The Chair takes the liberty of strongly suggesting that elapsed-time estimates be deferred until the chartering choices have been made, and detailed work-plans developed.

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 Input

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 III 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 fastflux. 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, fastflux operators may adapt their practices in order to avoid detection or may attempt to exploit registrants to unwitting allow the fastflux 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 fastflux 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 fastflux domain. Additional studies added support to the fastflux classification of this domain and had the unexpected side-effect of uncovering a sizable multi-purposed fasflux network.

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