

Draft Fast Flux Initial Report – Updated following FF Conference Call on 10 September 2008

| Original text | Proposed text | Proposed by | Agreed |
|--|---|-------------|--------|
| Chapter 3 – Background – Lines 56 - 219 | | | |
| 1. | | | |
| <p>Lines 191-194: The working group conducted preliminary research which developed anecdotal evidence that some high-capacity load-balancing systems may 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.</p> | <p>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.</p> <p>-----</p> <p>Rationale: The evidence that various legit systems rely on short TTLs was documented in the threads, and is not "anecdotal".</p> | Greg Aaron | Y |
| 2. | | | |
| <p>Lines 199-200: More research is needed to better understand legitimate uses [of short TTLs] and their prevalence, once a more robust definition of "fast flux" has been developed."</p> | <p>Delete sentence</p> <p>-----</p> <p>Rationale: I think there was well-supported info about the legit uses of short TTLs, and consensus that limiting TTL lengths is not a viable solution to fast-flux. The DNS RFCs themselves allow short TTLs and describe such uses. See also lines 1213-1228 for background and references.</p> | Greg Aaron | Y |
| 3. | | | |
| <p>Line 206: This was described anecdotally as a possible "legitimate use".</p> | <p>Delete "anecdotally"</p> <p>-----</p> <p>Rationale: It was discussed as a possible legitimate use.</p> | Greg Aaron | Y |

| Chapter 4 – Approach taken by the Working Group – Lines 220 - 238 | | | |
|--|--|--------------------|-----|
| 4. | | | |
| After line 237, update affiliation of WG members | George Kirikos CBUC Leap of Faith Financial Services Inc Philip Lodico FairWinds Partners Rodney Joffe RYC Neustar ----- Rationale: Currently data seems to be missing or wrongly allocated to WG members | George Kirikos | Y |
| 5. | | | |
| After line 238, add link to statement of interest for all FF WG member | http://gnso.icann.org/issues/fast-flux-hosting/soi-ff-05aug08.shtml ----- Rationale: To provide all relevant information about WG members | Glen de Saint Géry | Y |
| 6. | | | |
| After line 238, add | In addition, ICANN Senior Security Technologist Dave Piscitello actively participated in the working group's discussions. ----- Rationale: Provide complete information about who participated in WG discussions | Marika Konings | Y |
| Chapter 5 – Discussion of Charter Questions – Lines 239 - 465 | | | |
| 7. | | | |
| Replace line 258 ““A Fast Flux network, for the purposes of this working group: | A fast flux attack network, for the purposes of this working group, exhibits the following characteristics: | Dave Piscitello | Y/N |
| 8. | | | |
| Lines 260-261 · Is operated on one or more compromised hosts (i.e., using software that was installed on hosts without notice or consent to the system operator/owner); | 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); ----- Rationale: This considers the scenarios the WG discussed where attackers use bulletproof web hosting or hosts they "lease" for the phishing or illegal web sites and use obfuscation/redirection thru proxies operated on compromised sites. | David Piscitello | Y/N |

| | | | |
|---|--|-----------------|-----|
| 9. | | | |
| Suggested addition: Insert after line 274 | <p>Additional characteristics that in combination or collectively have been used to distinguish or "fingerprint" a fast flux hosting attack include:</p> <ul style="list-style-type: none"> - Multiple IPs per NS spanning multiple ASNs, - frequent NS changes, - in-addr of 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 <p>The distribution and use of software that is 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.</p> <p>-----</p> <p>Rationale: These characteristics that have been extracted from various "fast flux detection methods" reviewed by WG members and discussed in email threads. Some of these were mentioned in various analyses; others I believe are derived from the Manheim formula.</p> <p>Read item list for the definition of fast flux carefully; in particular, note that lines 260-26 describe what is generally regarded as maliicious, unlawful, unauthorized activity. Now scroll down to the list of "who benefits from fast flux?" and we list reputable businesses organizations and legitimate network operators. Thus, we are saying "these legitimate businesses, et. Al. rely on malicious software running on compromised machines." The second paragraph would correct this.</p> | Dave Piscitello | Y/N |
| 10. | | | |

| | | | |
|--|---|-------------------------------------|-------------------|
| <p>Section 5.1, (Note) Lines 286-287 currently read:</p> <p>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.</p> | <p>-----</p> <p>Rationale: The definition above this section begins by stating that a fast flux network is operated on one or more compromised host. I find it difficult to think of no parties who benefits from fast flux other than attackers if we continue to include this characteristic in the definition.</p> <p>However, I believe that the presence of software that was installed on hosts without notice or consent to the system operator/owner is a critically important characteristic, one among several that distinguishes volatile attack networks from volatile production networks. (my preceding comment enumerates others)</p> | <p>Dave Piscitello</p> | <p>Y/N</p> |
| <p>11.</p> | | | |
| <p>Insert before Line 298 which currently reads "The WG identified the following ways in which fast flux techniques"</p> | <p>Production applications of volatile networks may exhibit some but not all characteristics ascribed to fast flux attack networks. For example, the WG assumes that unauthorized software operated on compromised hosts would not participate in or contribute to the intended and beneficial use of such volatile networks.</p> <p>-----</p> <p>Rationale: This is a clarification that is needed to maintain consistency with the earlier comments and additions from lines 258-274. The same rationale applies.</p> | <p>Dave Piscitello</p> | <p>Y/N</p> |
| <p>12.</p> | | | |
| <p>Additional text following line 308 Lines</p> | <p>While those sort of networks employ short TTLs, short TTLs -- in and of themselves -- are insufficient to characterize a domain name as 'fastflux.'</p> <p>TTLs become an issue for fastflux-related work primarily because at least one Internet Draft, ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-bambenek-doubleflux-01.txt (URL broken due to length) focuses primarily on establishing minimum TTLs as an approach to limiting fastflux. If constraints were to be applied to TTLs in an effort to limit fastflux, this would impact organizations which rely on short TTLs in order to be able to relocate resources as part of the process of</p> | <p>Joe St Sauver Greg Aaron</p> | <p>Y/N</p> |

| | | | |
|---|--|---------------|-----|
| | <p>mitigating distributed denial of service attacks, would impact organizations moving namerservers, and would impact organizations which rely on short TTLs in order to provide a variety of legitimate services, among others."</p> <p>-----</p> <p>Rationale: The draft report does not explain why that scenario is relevant to a discussion of fastflux. There are a ton of services that use short TTLs. Proposed additional text following line 308 meant to correct that.</p> | | |
| 13. | | | |
| Line 323: Organizations that provide channels for free speech, minority advocacies, and activities, revolutionary thinking may use short TTLs and operate fast-flux like networks to avoid detection. | <p>Organizations that provide channels for free speech, minority advocates, and so on may use short TTLs and operate fast-flux 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).</p> <p>-----</p> <p>Rationale:</p> | Greg Aaron | Y |
| 14. | | | |
| Line 329: Other techniques are used by these groups to avoid discovery, not fast flux, or at least no evidence has been provided to support this. | <p>Some indicated that there is a lack 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 discovery.</p> <p>-----</p> <p>Rationale: "not sure what "not fast flux" means or refers to; might need some grammatical editing?"</p> | Greg Aaron | Y |
| 15. | | | |
| Addition immediately following line 345 | <p>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 behavior. Recall that fast flux nodes are created by compromising hosts with malicious software installed without the knowledge or consent of the system's operator/owner.</p> <p>With respect to malicious behaviors enabled by fast flux, one non-subjective</p> | Joe St Sauver | Y/N |

| | | | |
|--|--|--|--|
| | <p>definition of 'malicious behavior' would be, 'Activities which are illegal under the laws or regulations of a country having jurisdiction over the activity in question.' For example, in the United States, malicious activities enabled by fastflux might include, among other things:</p> <ul style="list-style-type: none"> -- 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 <p>-----</p> <p>Rationale: Dissemination of malware, and unauthorized access to others' systems which have been compromised by malware, is a universally accepted example of malicious online behavior.</p> <p>The very motion establishing this working group (gnso.icann.org/announcements/announcement-30may08.htm) recognized that the ICANN GNSO Council's interest in considering fast flux was because of its criminal nature. E.G., that motion stated that they were creating a Working Group in order to: "... develop potential policy options to curtail the CRIMINAL USE of fast flux hosting." [emphasis added]</p> <p>Our report should provide at least a brief discussion of what such behaviors might be.</p> | | |
|--|--|--|--|

| | | | |
|--|---|-----------------|------------|
| 15.1 | | | |
| Line 360 reads: Reliable techniques to detect fast flux networks while avoiding false positives | Reliable techniques to detect fast flux networks while maintaining an acceptable rate of false positives ----- Rationale: I do not believe that setting an accuracy requirement of 100% is appropriate here. | Dave Piscitello | Y/N |
| 16. | | | |
| Addition of the following text after line 363 | Some members of the working group believe that the Mannheim fast flux score formula would provide a robust and mechanically applicable definition of "fast flux" which would minimize false positives, and believe that the use of whitelisting plus manual review can eliminate any remaining potential false positives. The working group received multiple offers of fast flux-related data from <insert list of fastflux data sources here [I'm aware of at least two or three, but I'll defer to the data collection subcommittee for a definitive list]>. The working group accepted [or rejected] data from those sources, and [did what with it?], finding [what?]. Those interested in working with that data can apply to obtain access to it by contacting [who?] While it may not be possible to definitively distinguish the costs of cybercrime associated with fast flux from the costs of cybercrime conducted separate from fast flux, the working group did receive reports on aggregate estimates of cybercrime-related costs, and even if a fraction of 1% of all cybercrime can be tied to fastflux, the costs would be staggering. Moreover, at least in some cases such as the use of fast flux to distribute child pornography, there are substantial non-financial human costs which should also be recognized. ----- Rationale: the ability to mechanically screen potential fast flux domains is an important element of our ability to scalably and efficiently process complaints | Joe St Sauver | Y/N |

| | | | |
|--|--|--|--|
| | <p>about potential fast flux domains.</p> <p>The availability of a simple, easily computed "flux score" eliminates the need to vett the expertise of a potential complainant since a mechanical test of this sort is objective, replicable and cost free, and doesn't rely on complainant-supplied supporting evidence. A complainant need only supply a candidate domain name, after which ICANN/registrar/registry queries to domain name and routing data (delivered via DNS) would quickly allow the submitted domain name to be screened for fast flux characteristics.</p> <p>Because a number of working group members expressed concern about potential false positives, I deemed it important to also include a brief discussion of how false positives could be avoided.</p> <p>Much of the discussion in the draft report focused on how the next step will largely be a data collection and analysis process.</p> <p>A number of researchers active in the fast flux area have already supplied data to this working group, so it is important to understand what has already been received, what has been done with what has been received, and the conclusions of that analysis. Peer review and replication also strongly argues for making data sets available for re-analysis and verification/validation whenever possible, recognizing that in some cases proprietary rights or other restrictions may limit the Working Group's ability to reshare data.</p> <p>The financial and intangible costs associated with cybercrime are huge (measured in the billions of dollars/year); see the estimates provided in http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00264.html and http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00265.html</p> | | |
|--|--|--|--|

| | | | |
|--|---|-----------------|------------|
| | <p>Storm, a fast flux-based spam delivery mechanism, has been estimated as spewing one fifth of all spam, as cited at: http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00266.html</p> <p>Understanding the magnitude of those costs, and the role that fastflux plays in those illegal activities, underscores the importance of attacking the fast flux problem.</p> | | |
| 17. | | | |
| Lines 365. Question 5.2. | <p>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 and, there is reliable information as to the financial and non-financial impact of these networks.</p> | Mike O'Connor | Y/N |
| 18. | | | |
| a. | | | |
| <p>Lines 365-379 list six of the questions that the working group was charged with addressing, including 5.2:</p> <p>"Who would benefit from cessation of the practice and who would be harmed?"</p> | <p>Who is harmed by fast flux techniques when used in support of attack networks?</p> <ol style="list-style-type: none"> 1. Individuals whose computers are infected by attackers and subsequently used to host facilities in a fast flux attack network (e.g., nginc proxies, nameservers or web sites). The individual may have his Internet connection blocked. In 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. 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) | Dave Piscitello | Y/N |

| | | | |
|--|--|--|--|
| | <p>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.</p> <p>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. They may unwittingly disclose medical or personal information that could be used for blackmail or coercion. They may infect their computers with malicious software that would "enlist" their computers into a bot herd. Individuals who purchase bogus products, especially pharmaceuticals, may be physically harmed from using such products.</p> <p>4. Internet access operators are harmed when their IP address blocks 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.</p> <p>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.</p> <p>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</p> | | |
|--|--|--|--|

| | | | |
|--|--|--|--|
| | <p>associated with brand abuse monitoring, detection and mitigation.</p> <p>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.</p> <p>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.</p> <p>Who benefits from the use of fast flux techniques</p> <p>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).</p> <p>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).</p> <p>3. Organizations that provide channels for free speech, minority advocacies, and</p> | | |
|--|--|--|--|

| | | | |
|--|--|---------------|-----|
| | <p>activities, revolutionary thinking may use fast flux techniques to avoid detection.</p> <p>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.</p> <p>Friendly addition by Christian Curtis:</p> <p>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.</p> <p>-----</p> <p>Rationale: The rationale for including this change is that provides a reasonably complete set of harms and benefits given the working definition of fast flux we include in the report. The harms are an enumeration of harms identified in prior work on fast flux (Honeynext FF paper, SSAC report). The benefits capture the suggested beneficial uses of fast flux techniques that appear to have been acceptable to several members of the FFWG. The proposed text in this section has been revised to match the working definition of fast flux including changes I proposed earlier.</p> | | |
| b. | | | |
| Lines 365-379 list six of the questions that the working group | <p># "Who is harmed by fast flux activities?"</p> <p>#</p> <p>#1. Individuals whose computers are infected by attackers and subsequently</p> | Joe St Sauver | Y/N |

| | | | |
|---|---|--|--|
| <p>was charged with addressing, including 5.2:</p> <p>"Who would benefit from cessation of the practice and who would be harmed?"</p> <p>Addition to proposed revision in part a.</p> | <p>#used to host name servers or web sites for a fast flux phishing attack. The #individual may have his Internet connection blocked. In the extreme, should #the computer be suspected of hosting illegal material, the computer may be #seized by law enforcement agents (LEAs) and the individual may be subjected #to a criminal investigation.</p> <p>Add:</p> <ul style="list-style-type: none"> -- 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) <p>Some specific examples of how users can be harmed by this, beyond what's already been mentioned, can be seen in things like:</p> <ul style="list-style-type: none"> -- 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 | | |
|---|---|--|--|

| | | | |
|--|---|--|--|
| | <p>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 attendant lost or delayed email), time spent learning the ins-and-outs of a new ISP, time spent reconfiguring systems to use the new ISP, etc.</p> <p>#2. Businesses and organizations whose computers are infected may have #Internet connections blocked, which may result in loss of connectivity for #all users 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".</p> <p>A compromised system in a business environment also immediately raises the dreaded spectre of a breach of personally identifiable information (PII).</p> <p>If PII was present on the compromised machine, notification may be mandated by statute, which may result in substantial direct costs to affected organization (my understanding is that a dollar a notification is a very conservative floor for notification costs, and obviously some PII incidents involve millions of affected individuals). PII-related worries also drive the substantial costs associated with deployment of whole disk encryption.</p> | | |
|--|---|--|--|

| | | | |
|--|--|--|--|
| | <p>Some businesses may also be affected by additional legislation specific to their discipline, e.g., here in the States, things like GLBA or HIPAA apply to financial institutions or health care institutions, respectively.</p> <p>Employees may also be subject to non-criminal consequences, including sanctions up to and including dismissal if they are found to be, or are simply *believed to be*, at least partially responsible for their company-supplied system being compromised.</p> <p>#3. Individuals who receive phishing emails and are lured to a phishing site #hosted on a bot used by the miscreants/criminals who run the phishing attack #may have their identities stolen or suffer financial loss from credit card, #securities or bank fraud.</p> <p>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.)</p> <p>Identity theft can also touch on national security issues, if stolen identity information is used to illegally cross borders, to illegally remain in 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.</p> <p>#They may unwittingly disclose medical or personal #information that could be used for blackmail or coercion.</p> <p>Or for discriminatory treatment by employers concerned with potential costs associated with identified (but latent) genetic conditions, for example.</p> | | |
|--|--|--|--|

| | | | |
|--|---|--|--|
| | <p>Fear that medical record systems are porous 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>")</p> <p>#They may infect #their computers with malicious software that would "enlist" their computers #into a bot herd.</p> <p>[It seems odd to have this item pop up here -- this feels more like something that belongs in an introductory paragraph explaining how fastflux works]</p> <p>#Individuals who purchase bogus products, especially #pharmaceuticals, may be physically harmed from using such products.</p> <p>... and 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 (true example, BTW) -- 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</p> <p>and the list goes on... [Illegal generics also undercut the incentive for pharmaceutical firms to invest in new drug research by cutting into their earning stream while their discovery is protected by patents.]</p> <p>Besides pillz, I'd also note that sale of counterfeit products is another example of how fast flux networks can result in users and businesses being harmed.</p> | | |
|--|---|--|--|

| | | | |
|--|--|--|--|
| | <p>Counterfeit products may undermine the value of carefully nurtured brand names, leave consumers with shoddy or dysfunctional products, deny nation's legitimate customs revenues associated with the importation of premium brand-name products, result in unsafe products (I was surprised to learn that counterfeit UL-listed electrical appliances cords are a routinely available item, for example).</p> <p>#4. Internet access operators</p> <p>I'd probably call them Internet access providers or Internet service providers instead of Internet access operators</p> <p>#are harmed when their IP address blocks and their domain names</p> <p>#are associated with bot nets and phishing attacks that are linked to fast flux #activities. These operators also bear the burden of switching the #unauthorized traffic that phishing attacks generate and they may also incur #the cost of diverting staff and resources to respond to abuse reports or #legal inquiries.</p> <p>... or helping users to get cleaned up, or purchasing antivirus products to hand out to users, or deploying network-based remediation solutions.</p> <p>They also get slammed on the other end of the pipe, when fastflux enables spamvertised sites, and they get deluged with piles of inbound spam advertising those fastflux hosted spamvertised domains.</p> <p>ISPs may also experience excess DNS-related traffic as a result of fastflux, resulting in the need for more recursive resolver capacity than they'd otherwise need to deploy.</p> | | |
|--|--|--|--|

| | | | |
|--|---|--|--|
| | <p>ISPs may also be forced to deploy deep packet inspection equipment or other gear to detect and respond to fastflux hosted sites on customer systems. (Because web sites can be easily hosted on arbitrary ports, port-based blocking solutions won't work to control fastflux hosting, unlike port 25 blocks depoloyed to control direct-to-MX spam).</p> <p>#5. Registrars are harmed when their registration and DNS hosting services #are used to abet "double flux" attacks. 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.</p> <p>I'd also explicitly recognize that registrars will likely see things like wdprs.internic.net complaints in conjunction with fast flux domains, simply because that's one of the only complaint mechanisms which are available, so antispam activists have become very good at carefully scrutinizing domain whois data for whois problems. Dealing with those WDPRS reports represents an additional specific cost, and one possibility might be to provide a reporting channel that focusses on the actual issue (a domain has been detected which engaged in criminal activity) rather than the substitute issue (there's a problem with the domain's whois data).</p> <p>#6. Businesses and organizations who are "phished" from bogus web sites #hosted on fast fluxing 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. #</p> <p>#7. Individuals or businesses whose lives or livelihoods are affected by the #illegal activities abetted through fast flux 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</p> | | |
|--|---|--|--|

| | | | |
|--|---|--|--|
| | <p>#the distribution of images or enslavement.</p> <p>The intent of that paragraph might be clarified by explicitly talking about child pornography, unauthorized distribution of proprietary software (warez), unauthorized distribution of copyrighted music and movies, unauthorized distribution of counterfeit merchandise, etc.</p> <p>#8. Registries may incur the cost of diverting staff and resources to monitor #abuse or to respond to abuse reports or legal inquiries.</p> <p>Uptake/legitimate use of some TLDs may also be impacted by fast flux abuse. If the public perceives that simple use of a domain from a particular TLD may result in negative scoring by things like SpamAssassin, that can be a powerful disincentive hindering use of that registry's TLD.</p> <p>#Who benefits from the use of short TTLs?</p> <p>I'd emphasize that "short TTLs" are NOT synonymous with "fastflux" and that short TTLs are only one characteristic associated with fastflux domains. It is important to discuss legitimate use of short TTLs, however, because they have legitimate uses as well as a strong association with some fastflux domains.</p> <p>##2. 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).</p> | | |
|--|---|--|--|

| | | | |
|--|---|--|--|
| | <p>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.</p> <p>#3. Organizations that provide channels for free speech, minority advocacies, #and activities, revolutionary thinking may use short TTLs and operate #fast-flux like networks to avoid detection.</p> <p>I haven't seen this. I've certainly seen organizations offer encrypted, non-attributable, or covert communication channels, such as use of PGP/Gnu Privacy Guard, remailers, steganographic methods, Tor/"onion routing," anonymous VPN services, etc., but I've NOT seen those organizations use fastflux web hosting.</p> <p>Fastflux, when I've seen it used, has been to host spamvertised web sites.</p> <p>Those spamvertised web sites may be phishing web sites, or malware web dropping sites, or child porn sites, or warez sites, or carding sites, or whatever, but I can't think of even a single case where political, religious or other dissident web sites have ended up hosted on fastflux.</p> <p>Why? Because in every case I'm aware of, dissident web sites can simply purchase legitimate extraterritorial web hosting, so that even if Kerblechistan won't allow their web site to be hosted domestically, someone abroad will typically happily step up to the table.</p> <p>The only folks who end up on fastflux are those who are so beyond the pale that NO ONE will host them *anywhere* in the world. Dissidents simply aren't "bad</p> | | |
|--|---|--|--|

| | | | |
|--|--|---------------|------------|
| | <p>enough" to have trouble getting hosting, and fastflux does not encompass attempts to covertly access Internet resources without detection by authoritative regimes.</p> <p>So... I'd love to see a concrete example of a free speech or other web site that *is* using fastflux hosting (and by this I mean "a web site that's hosted on, or which appears to be hosted on, compromised consumer PCs, without that PC owner's informed consent"). [I say "appears to be hosted on" because most fastflux sites don't actually host content locally, they just reverse proxy traffic back to the backend "mother ship" elsewhere, where the content is really hosted]</p> <p>-----</p> <p>Rationale: Dave Piscitello's provided a fine answer to that question at http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00048.html , one which I commented on at http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00055.html I propose that that text be included as a response to 5.2</p> | | |
| 19. | | | |
| <p>Lines 365-379 list six of the questions that the working group was charged with addressing, including question 5.6, "How are Internet users affected by fast flux hosting?"</p> | <p>While most Internet users have never heard of fastflux hosting, a growing number of them are nonetheless directly affected by it.</p> <p>Internet users provide both the raw material that fastflux hosting runs on (malware-compromised broadband-connected consumer PCs), while also serving as the target audience for the spamvertised web sites which fastflux enables.</p> <p>Internet users are thus central to the entire fastflux problem, and unless it is handled appropriately, they are also the ones who will be subject to yet more breakage and loss of Internet transparency.</p> <p>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.</p> | Joe St Sauver | Y/N |

| | | | |
|--|--|--|--|
| | <p>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."</p> <p>Having obtained control over those compromised PCs, the miscreants can then 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").</p> <p>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).</p> <p>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.</p> <p>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.</p> <p>While what's illegal will vary from jurisdiction to jurisdiction, there are some categories of content which are illegal virtually everywhere, including, among other</p> | | |
|--|--|--|--|

| | | | |
|--|--|--|--|
| | <p>things:</p> <ul style="list-style-type: none"> -- 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.) <p>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/].</p> <p>Listings on Spamhaus or similar lists result in significant complaints regular customers who may be incidentally impacted by such a listing.</p> <p>With that for background, you can now guess 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.</p> <p>By this do we mean that 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</p> | | |
|--|--|--|--|

| | | | |
|--|---|--|--|
| | <p>fastflux hosts? No, that would be too complex, too time consuming, and too easily detected.</p> <p>Instead, spammers found that they could simply 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.</p> <p>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.</p> <p>[insert suitable illustration here]</p> <p>Naturally, you might wonder, "Does the owner of the compromised PC know that all this is going on via his or her computer and network connection?"</p> <p>"No."</p> <p>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?"</p> <p>No warning light goes off on the compromised PC saying hey, "Someone's serving stolen software from your system!"</p> <p>Typically the owner of the PC *only* becomes aware that they have unwittingly become a participant in illegal online activity when:</p> <ul style="list-style-type: none"> -- 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 | | |
|--|---|--|--|

| | | | |
|--|---|--|--|
| | <p>bad news that they're infected</p> <ul style="list-style-type: none"> -- 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. <p>The user is then left with the unenviable chore of trying to get their compromised system cleaned up. Because of the complexity of cleaning many infections, and the substantial possibility that at least some lingering badness may be missed during efforts at cleanup, most experts recommend formatting compromised systems and reinstalling it 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.</p> <p>What a mess. That mess is the first impact of fastflux hosting, but one which only some unlucky users experience.</p> <p>The next effect of fastflux hosting is one which virtually all Internet users experience, and that's spam. Remember, fastflux hosting exists to host illegal content or spamvertised products or services. All of us receive spam, whether that's an occaisional message that slips through otherwise efficient filters, or a steady deluge that may have caused some of us to abandon email altogether.</p> <p>Without the ability to obtain reliable web hosting services, spammers are left with</p> | | |
|--|---|--|--|

| | | | |
|--|--|--|--|
| | <p>only a few categories of potential spam, such as stock pump-and-dump spam, where users don't need to visit the spammer's web site to purchase a product or service. Clearly spammers are powerfully motivated to find an alternative, and that's what fastflux has given them. With fast flux, they've got it.</p> <p>With fastflux, 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:</p> <ul style="list-style-type: none"> -- 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. <p>Spammers quickly recognized that the name servers were a weak point in their scheme, so they adapted. How did they adapt?</p> <p>Well, they began not just using compromised systems for web hosting, but 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.</p> <p>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, so maybe something similar could be done to address fastflux and doubleflux abuse.</p> <p>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</p> | | |
|--|--|--|--|

| | | | |
|--|--|--|--|
| | <p>on *any* arbitrary port (e.g., to access a web page on port 8088 instead of the default port 80, one might use a URL such http://www.example.com:8088/sample.html).</p> <p>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.</p> <p>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.</p> <p>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 struggle 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 to use fastflux and double flux</p> | | |
|--|--|--|--|

| | | | |
|--------------------------|--|---------------|------------|
| | <p>techniques.</p> <p>-----</p> <p>Rationale: When it comes to question 5.6, "How are Internet users affected by fast flux hosting?" I addressed the question 5.6 in my note at http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00061.html</p> <p>I would propose that that text be included as a draft response to 5.6</p> | | |
| 20. | | | |
| Line 367 -- Question 5.3 | <p>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 and, there is reliable information as to the financial and non-financial impact of these networks.</p> | Mike O'Connor | Y/N |
| 21. | | | |
| Line 367 -- Question 5.3 | <p>In its Constituency Input Statement (attached to this report as a 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 at line 936 [THIS REFERENCE WILL HAVE TO BE UPDATED AS THE DOC GETS EDITED] and question 7 from 1008 to 1252 [THIS REFERENCE WILL HAVE TO BE UPDATED AS THE DOC GETS EDITED] are of interest.</p> <p>-----</p> <p>Rationale: Rather than leaving question 5.3 blank, I suggest the following text, which points to some useful (and factual) technical info.</p> | Greg Aaron | Y/N |
| 22. | | | |
| Line 370-- Question 5.4 | <p>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 and, there is reliable</p> | Mike O'Connor | Y/N |

| | | | |
|-------------------------|---|---------------|------------|
| | information as to the financial and non-financial impact of these networks. | | |
| 23. | | | |
| Line 372-- Question 5.5 | 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 and, there is reliable information as to the financial and non-financial impact of these networks. | Mike O'Connor | Y/N |
| 24. | | | |
| Line 374-- Question 5.6 | 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 and, there is reliable information as to the financial and non-financial impact of these networks. | Mike O'Connor | Y/N |
| 25. | | | |
| Lines 398 - 416 | <p>-----</p> <p>Rationale: I'd like to see a little more in the "Information Sharing" section. Specifically something like saying that the publishing of the non-private information through DNS might be useful to assist in detecting and blocking spam that is promoting domains used in a fast flux fraud scheme. I think it's important to say why this information should be published through DNS.</p> <p>Additionally it should be noted that the reason for using DNS rather than WHOIS is for high real time query speed for those who would say, "Why use DNS when WHOIS is already there."</p> <p>Also - unless this already exists. Is there a way to determine the registrar of a domain through a DNS query? If there is I'd like to know it. If not then that is one of the fields I'd like to be able to look up through a DNS query.</p> | Mark Perkel | Y/N |

| | | | |
|--|--|----------------|------------|
| | You might also mention that this information might also be useful for abuse reporting so that those who detect a problem can alert those who can deal with the problem. | | |
| 26. | | | |
| Lines 402-408 | Change "affiliated" to "contracted" and "affiliates" to "contracted parties" ----- Rationale: : a number of ccTLDs have MOUs with ICANN, and most ccTLDs are affiliated with ICANN via their participation in GAC and ICANN | Greg Aaron | Y |
| 27. | | | |
| I would also propose adding after line 411 text clarifying that | The DNS-based zone envisioned under this section need not 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). ----- Rationale: Some have expressed concern that dealing with fastflux might impose burdensome new obligations on ICANN, the registries or the registrars. It is thus important to clarify that coping with fast flux via an information-sharing-oriented approach need not impose material new burdens on those parties given the possibility of third parties massaging and arranging for re-dissemination of the data that may be required. | Joe St Sauver | Y/N |
| 28. | | | |
| Footnote 5 states: 5. A DNS-based system could be queried through automation rather than manually. Whois is a manual protocol and is not suitable for | Whois is a protocol which, as routinely deployed, generally forbids automated queries, and hence is only suitable for ad hoc manual query volumes. DNS has demonstrated the ability to scale to extremely large automated query volumes in support of things like DNS block lists, and should not be require the same sort of a priori query traffic volume limits, although limits to control demonstrable abuse may still be needed from time to time. ----- | Joe St Stauver | N |

| | | | |
|---|---|------------|-----|
| real time queries. | <p>Rationale: The footnote as originally written was factually incorrect and needed to be corrected. The additional text also explains why DNS may be a worthy alternative to whois (e.g., DNS has proven its ability to scalably act as a distributed database infrastructure for arbitrary data)</p> <p>Additional comment received by Greg Aaron: As currently stated, the footnote at 409 is factually incorrect. WHOIS is NOT a manual protocol. Port 43 WHOIS protocol is fully automated. Registrars and other parties make millions upon millions of automated queries to port 43 WHOIS servers every day. Some port 43 servers are rate-limited (via IP, etc.) to prevent WHOIS mining by spammers, etc.</p> <p>Joe's interested in a system that would make certain data available in a higher-volume fashion than is available via rate-limited WHOIS.</p> | | |
| 29. | | | |
| Footnote 5 states: 5. A DNS-based system could be queried through automation rather than manually. Whois is a manual protocol and is not suitable for real time queries. | <p>A DNS-based system could provide similar or additional data than WHOIS systems do, and at rates higher than many port 43 WHOIS servers currently allow.</p> <p>-----</p> <p>Rationale: WHOIS is not a manual protocol, and was in fact designed for real-time queries.</p> | Greg Aaron | Y |
| 30. | | | |
| Line 429: The ideas for active engagement that were discussed by the WG included the following: | <p>The ideas for active engagement that were discussed by the WG included the following; the group did not reach consensus on or endorse any of them:</p> <p>-----</p> <p>Rationale:</p> | Greg Aaron | Y/N |
| 31. | | | |
| Line 446 – Add a bullet to the list of ideas | 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 | Greg Aaron | Y/N |

| | | | |
|--|---|---------------|------------|
| | advantage of the DNS and Internet protocols." ----- Rationale: | | |
| 32. | | | |
| Line 456-- Question 5.8 | 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. | Mike O'Connor | Y/N |
| 33. | | | |
| Line 460-- Question 5.9 | 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. | Mike O'Connor | Y/N |
| 34. | | | |
| Line 463-- Question 5.10 | Answering this question should be deferred until there is a robust technical and process definition of "Fast Flux". | Mike O'Connor | Y/N |
| Chapter 6 – Constituency Statements – Lines 466 - 518 | | | |
| 35. | | | |
| Line 484 - 4.1 Constituency Views Line 512 - 4.3 Further Work Suggested by Constituencies | Line 484 - 6.1 Constituency Views Line 512 - 6.2 Further Work Suggested by Constituencies ----- Rationale: Correct incorrect numbering | Mike O'Connor | Y |
| 36. | | | |
| Addition following lines 486- | Some members of the working group suggest that ICANN/the registries/the | Joe St Sauver | Y/N |

| | | | |
|---|---|----------------------|-------------------|
| <p>489:</p> <p>"The Ryc, NCUC and RC members all recognise that fast flux is being used by miscreantsinvolved in online crime to evade detection, but at the same time question whether ICANN is the appropriate body to deal with this issue. All three emphasize that it is not in ICANN's remit to act as an extension of law enforcement or put registries or registrars in this position."</p> | <p>registrars are not being asked to act as an extension of law enforcement, but rather are merely being asked to facilitate compliance with existing laws and regulation when ICANN/the registries/the registrars are uniquely situated to do so.</p> <p>-----</p> <p>Rationale: Alternatively, if folks believe that the constituency statements should not be subject to comment, I'd be okay with the omission of the section 6 recap/summary, allowing the constituency statements to just stand on their own, unaltered/uncommented, as appendicies.</p> | | |
| <p>37.</p> | | | |
| <p>Line 492 - Replace: "simply move on to another technique or method to avoid detection"</p> | <p>simply move on to another technique or method, or would change their implementations, to avoid detection or mitigation efforts.</p> <p>-----</p> <p>Rationale:</p> | <p>Greg Aaron</p> | <p>Y/N</p> |
| <p>38.</p> | | | |
| <p>Addition following Lines 495-499:</p> <p>"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</p> | <p>The rejoinder from some members of the working group is that while GNSO is not responsible for administering ccTLD policy, by showing leadership in administration of gTLD domains policies (including policies dealing with fastflux), GNSO actions may indirectly influence the ccTLD policy development process.</p> <p>-----</p> <p>Rationale: Alternatively, if folks believe that the constituency statements should not be subject to comment, I'd be okay with the omission of the section 6 recap/summary, allowing the constituency statements to just stand on their own, unaltered/uncommented, as appendicies.</p> | <p>Joe St Sauver</p> | <p>Y/N</p> |

| | | | |
|--|--|---------------|------------|
| <p>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."</p> | | | |
| 39. | | | |
| <p>Addition following lines 501-503: "The RyC, NCUC and 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 -- benefit of any potential solutions."</p> | <p>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. ----- Rationale: Alternatively, if folks believe that the constituency statements should not be subject to comment, I'd be okay with the omission of the section 6 recap/summary, allowing the constituency statements to just stand on their own, unaltered/uncommented, as appendices.</p> | Joe St Sauver | Y/N |
| 40. | | | |
| <p>Addition following lines 508-510: "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."</p> | <p>"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 " ----- Rationale: Alternatively, if folks believe that the constituency statements should not be subject to comment, I'd be okay with the omission of the section 6 recap/summary, allowing the constituency statements to just stand on their own, unaltered/uncommented, as appendices.</p> | Joe St Sauver | Y/N |


| | | | |
|--|---|---------------|------------|
| | <p>Additional comment received by Greg Aaron:</p> <p>Note that the RyC said "some" solutions.</p> <p>Some of the problematic solutions that were suggested included:</p> <ul style="list-style-type: none"> * limiting TTL lengths (short TTLs are explicitly allowed by the DNS RFCs...) * making registries monitor flux (they can't see single-flux in the registry, for example...) * There was implication in the Issues Paper that registry operators might increase the TTL on the delegation RRset in order to "thwart fast flux hosting". <p>Experimentation would be required to confirm this, but as far as the DNS protocol standards are concerned that is not, in fact, a viable approach. Any long TTL specified (for example) in a TLD zone in the NS set for a domain would be overwritten in resolvers' caches -- unless resolver code is changed.</p> <p>So Joe, I guess the sticky parts are:</p> <p>A. "Contrary to that perspective" is not needed, since it's not contrary, and</p> <p>B. I don't think there's consensus that using TXT records is a "required solution."</p> | | |
| Chapter 7 – Challenges – Lines 519 – 594 | | | |
| 41. | | | |
| <p>Lines 567-572 on PDF page 24 reads:</p> <p>"b. Misconceptions about the scope of a PDP and remit of ICANN</p> | <p>-----</p> <p>Rationale: Following that text, I would request that we add a pointer to the Affilias Abuse Funnel Request document mentioned by Greg Aaron at http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00285.html as an example of how at least one TLD has successfully addressed *precisely* the issue our WG faced.</p> <p>Somehow in just two pages Affilias managed to (a) explain why abusive use of domain names is an important issue, (b) define fast flux (see pp. 2 of www.icann.org/en/registries/rsep/afilias-abuse-funnel-request-rev-03jul08.pdf) and (c) forbid it unless usage has received prior permission, and (d) they even described what can/should be done (see the last two paragraphs of</p> | Joe St Sauver | Y/N |

| | | | |
|--|---|-----------------|------------|
| | <p>that page). Seems like the whole package to me.</p> <p>If nothing else, one possible solution would be to adopt the Affilias abuse funnel request as a foundation or model for moving forward with the gTLD fastflux discussion.</p> <p>Additional comment received by Greg Aaron:</p> <p>Speaking as one responsible for the Afilias (one "f") policy:</p> <p>Afilias is a private actor that is acting within a set of contractual obligations and limitations. Not all parties are similarly situated. Also, Afilias acted in this fashion in a volunteer fashion, and proposed a terms of service that it was right for it. However, there is not a one-size-fits-all solution that should be forced upon parties. One thing some parties are concerned about is being forced by ICANN to do things in a certain way. ICANN is not in a good position to dictate policies, procedures, and associated costs of this nature.</p> | | |
| Chapter 8 – Conclusions and Possible Next Steps – Lines 595 - 742 | | | |
| 42. | | | |
| Addition following line 597 | <p><i>Placeholder</i></p> <p>-----</p> <p>Rationale: This section needs to be revised to reflect changes in preceding text, particularly the definition of FF. I also think that there are other conclusions worthy of inclusion:</p> <ul style="list-style-type: none"> - conclusions relating how fast flux is only one form of flux attack - conclusions relating the challenges posed when attempting to associate an intent to networks that employ fast flux techniques (I think that the text that characterize fast flux in attacks versus fast flux in production/operational networks pushes us in | Dave Piscitello | Y/N |

| | | | |
|-----------------------------|--|-----------------|------------|
| | a promising direction, mine is an attempt to reconcile the definitions work of Randy, George, Greg and my own. | | |
| 43. | | | |
| Addition following line 611 | <p><i>Placeholder</i> -----</p> <p>Rationale: 8.2 Possible next steps (and subsections)</p> <p>- delete all references to consensus, rough consensus, minority, etc. We do not need consensus to include possible next steps - IMO the fact that we offer several is sufficient to meet our remit.</p> <p>Lines 622-624 - delete this note. I believe it's accurate that the group agreed to publish a report. I don't think we can accurately gauge support for P1 or P2 until we all have an opportunity to review - and I would encourage a roll call of opinion if not a formal vote to show support for each (P1, P2, and any others that may be added).</p> <p>- who is the WG recommending consider these options? A continuance of this WG, a new WG? The GNSO council?</p> | Dave Piscitello | Y/N |
| 44. | | | |
| Lines 628-630 | <p><i>Placeholder</i> -----</p> <p>Rationale: - once we sort out S1, S2 through S4 must be presented in the same level of detail or we prejudice the choice by providing too little information for comparing the options.</p> | Dave Piscitello | Y/N |
| 45. | | | |
| Lines 632-649 | <p><i>Placeholder</i> -----</p> <p>Rationale: - S1 does not discuss "roles and players" - for example, there are several discussions in various threads relating to collecting data, making it available, but no</p> | Dave Piscitello | Y/N |

| | | | |
|---|---|-----------------|------------|
| | <p>clear understanding who is collecting and who gets to access the data. There are also "historical data and analysis" discussions. These are not adequately distinguished in S1.</p> <ul style="list-style-type: none"> - S1 discusses developing algorithms but does not talk about testing, nor does it define a target metric value for "false positives" - Similarly, S1 does not identify the target entities for financial and operational justifications - registrants, ISPs, users, registrars, registries, ICANN, all? | | |
| 46. | | | |
| Line 636: Develop algorithms that can be used to detect the "problem" with safeguards to minimize false positives | <p>-----</p> <p>Rationale: I have a question about "develop algorithms." I question whether ICANN is the right place to develop such algorithms or specific technical implementations. ICANN WGs are not designed to do engineering work, and ICANN doesn't usually commission or fund such engineering work -- it sets policy or requirements. (ICANN has done engineering studies and tests when it had a direct relation to ICANN's narrow technical mandate -- an example being the IDN TLDs test-bed.)</p> | Greg Aaron | Y/N |
| 47. | | | |
| Line 665 and 667 (Options S3 and S4) | <p>Delete options S3 and S4</p> <p>-----</p> <p>Rationale: Any solutions mandated by ICANN would have to be the product of a future PDP; and any solutions will not be built, tested, or deployed by ICANN anyhow -- they'll be done by some party or parties other than ICANN.</p> | Greg Aaron | Y/N |
| 48. | | | |
| Line 673+ | <p><i>Placeholder</i></p> <p>-----</p> <p>Rationale: - Why is SSAC excluded from the list of stakeholders?</p> | Dave Piscitello | Y/N |
| 49. | | | |
| Line 666+ | <p><i>Placeholder</i></p> <p>-----</p> | Dave Piscitello | Y/N |

| | | | |
|---|---|-----------------|------------|
| | Rationale: - I think there is a third option that is "broader than fast flux and smaller than (all) fraud and abuse". We have talked about slow flux, double flux, and characteristics that have less to do with TTL values and more to do with other network attributes that make the network "volatile" We should include this option and it should fall within GNSO's remit. | | |
| 50. | | | |
| Line 695+ | <i>Placeholder</i> ----- Rationale: - - I don't think we have discussed approaches enough to make the claims included in this section. I think "weak rough consensus" is an impossible term to parse and object to notes making such claims without some roll call or recorded vote. | Dave Piscitello | Y/N |
| 51. | | | |
| Line 710 | <i>Placeholder</i> ----- Rationale: - - Please provide the roll call or vote that corroborates the claim that the group is evenly divided or remove this. | Dave Piscitello | Y/N |
| 52. | | | |
| Line 719 | <i>Placeholder</i> ----- Rationale: - - This can be rephrased as a question to the GNSO and ICANN board | Dave Piscitello | Y/N |
| Annex III – Fast Flux Case Studies – Lines 1650 - 1657 | | | |
| 53. | | | |
| Insert for placeholder on line 1655 | 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 | Randy Vaughn | |

| | | | |
|---|--|-----------------------|------------|
| | <p>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 unwittingly 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 fastflux network.</p> <p>Link to complete study: https://st.icann.org/pdp-wg-ff/index.cgi?randy_vaughn_s_case</p> | | |
| 54. | | | |
| Addition to Annex III | <p>http://fluxor.laser.dico.unimi.it/~fluxor/summary.html</p> <p>My understanding is that their detection/qualification is mostly based on spam traps and reporting from individuals. This averages to a little over 160 FFLUX domains per day through the 25th of August detected in their system.</p> | Rod Rasmussen | Y/N |
| Annex IV – Individual Statements | | | |
| 55. | | | |
| New annex to be created | <p>Document provided on 8 September 2008</p>  <p>gns0-ff - Eric Brunner-Williams staterne</p> | Erik Brunner-Williams | |
| 56. | | | |
| New annex to be created | Charter observations by the Chair (document to be provided) | Mike O'Connor | |