

Fast Flux Hosting PDP Update to the GNSO Council

Mike Rodenbaugh, Council Liaison to the Fast Flux Hosting Working Group

Sunday, 1 March 2009



Background

- January 2008: SAC 025 Fast Flux Hosting and DNS
 - Characterizes Fast Flux (FF) as an evasion technique that enables cybercriminals to extend lifetime of compromised hosts employed in illegal activities
 - 'Encourages ICANN, registries, and registrars [...] to establish best practices to mitigate fast flux' and 'consider whether such practices should be addressed in future agreements'.
- March 2008: GNSO Council Request for an Issues Report
 - Issues report recommends further fact-finding and research
- May 2008: GNSO initiates Policy Development Process (PDP) on Fast Flux Hosting
- June 2008: Fast Flux Hosting Working Group formed

Charter Questions

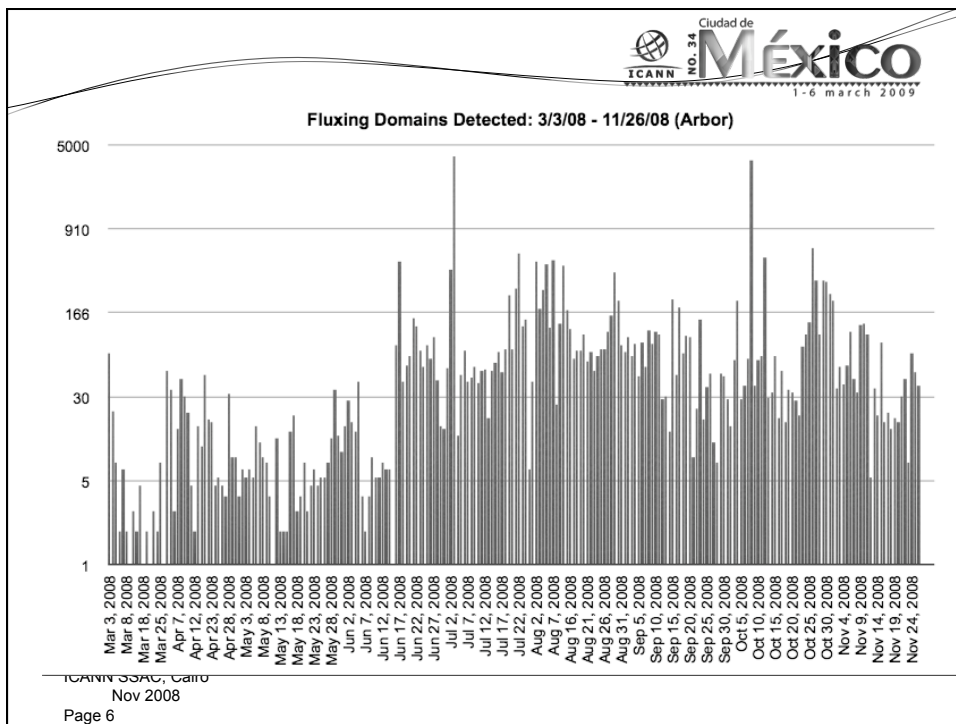
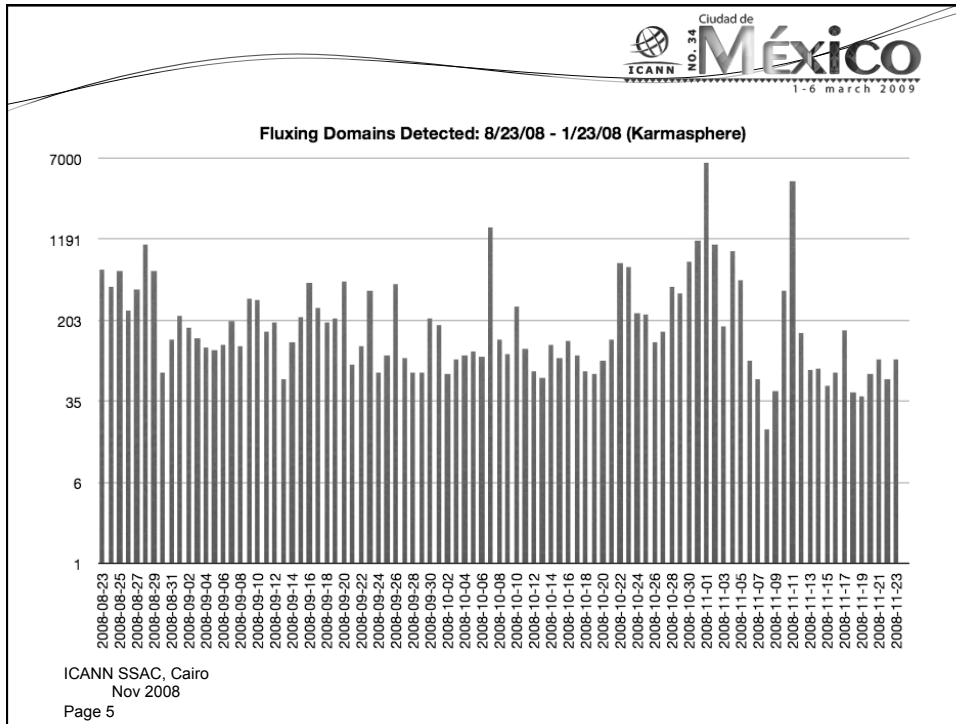
- Who benefits from FF, who is harmed?
- Who would benefit from cessation of the practice, who would be harmed?
- Are registry operators involved in FF hosting activities? If so, how?
- Are registrars involved in FF hosting activities? If so, how?
- How are registrants affected by FF hosting?
- How are Internet users affected by FF hosting?
- What technical and policy measures could be implemented by registries & registrars to mitigate the negative effects of FF hosting?
- What would be the impact of establishing limitations, guidelines, or restrictions on registrants, registrars or registries with respect to practices that enable or facilitate FF 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?
- Obtain expert opinion on which areas of fast flux are in scope and out of scope of GNSO policy making


3

Approach by the WG

- WG started working on answering charter questions in parallel to preparation of Constituency Statements
- In addition, several members of the WG worked on collecting supporting data on Fast Flux to be incorporated in the report
- Weekly conference calls, close to 900 emails exchanged to date
- Where no broad agreement could be reached, the WG would use 'support' and 'alternative view' labels to indicate level of support for certain position

4






ICANN NO. 34 Ciudad de México 1-6 march 2009

Challenges encountered

- Purview
 - Does this matter fall within ICANN's remit or should other avenues be pursued?
 - How should Fast Flux be defined?
 - Legitimate vs. Illegitimate use
- Activities
 - What kinds of monitoring are needed?
 - How should monitored data be reported, published, shared?
 - What actions (responses) are appropriate?
- Roles of players
 - Who monitors FF activities today? Are they trustworthy?
 - Are registrars and registries expected to monitor FF activity?
 - Are data currently collected accurate and sufficient to justify a domain suspension action?
 - What is an acceptable "false positive" rate?

7



ICANN NO. 34 Ciudad de México 1-6 march 2009

Initial Report

- Initial Report published on 26 January 2009
- Report provides initial answers by the WG to the Charter Questions, incl. a list of characteristics that a fast flux attack network might exhibit and fast flux metrics
- Interim Conclusions:
 - Challenges encountered by the WG in relation to intent and definition / characterization of fast flux
 - Fast flux is one component of larger issue of Internet fraud and abuse
 - Perhaps these broader, interrelated issues ought to be taken into account in any potential PDP and/or next steps.
 - Careful consideration to be given to the role ICANN should play in this process

8

GNSO Questions

- Who benefits from fast flux?
 - Organizations that require high availability, have highly targetable assets, or operate highly adaptive networks (CDNs)
 - Free speech and and advocacy groups
 - Criminals, anyone who uses the technique for harmful purposes
- Who is harmed?
 - Users/consumers/victims of criminal activities abetted by flux attack networks
 - Parties who are exploited (FIs, emERCHANTS, Govts, ...)
 - Some debate as to the extent to which FF attacks contribute to the overall impact of e-crime
 - “fast flux attacks have considerable influence in the duration and efficacy of harmful activities”

GNSO Questions

- Are registrars involved in fast flux hosting activities? If so, how?
 - Varying opinions on what the WG should say here, as “involvement” has many interpretations:
 - Reputable registrars are “uninvolved”
 - Certain registrars are unwitting participants (ignorant of problematic registrations)
 - Certain registrars appear to lack competence in managing abuse
 - The actions of certain registrars (or lack thereof) create the appearance of facilitation or complicity

GNSO Questions

- How are registrants affected by fast flux hosting?
 - Registrants who employ self-beneficial flux techniques improve network availability and resiliency to failure/attack
 - Registrants are also targets for phishing and other forms of attacks that result in unauthorized access to domain accounts and DNS exploitation
- How are Internet users affected by fast flux hosting?
 - They are the victims of fraud, malicious, and criminal activities that are abetted by flux hosting which is used to extend the duration of the attack
 - Internet user assets are used to facilitate flux attacks (e.g., bots on PCs, compromised servers, domain accounts and name services)
 - Bear the burden of detection and recovery costs (individual users as well as businesses and organizations that make use of online presence)

GNSO Questions

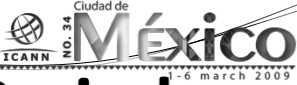
- What technical (e.g. changes to the way in which DNS updates operate) and policy (e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior) measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?
 - Examples of solutions involving registries and registrars
 - Sharing of additional non-private DNS information via TXT response messages (domain age, # of NS changes over a measurement interval)
 - Publish summaries of unique complaint volumes by registrar, by TLD, and by name server
 - Cooperative, cross-community information sharing
 - Adopt accelerated domain suspension processing in collaboration with certified investigators
 - Stronger registrant verification procedures

GNSO Questions

- What are some of the best practices available with regard to protection from fast flux?
 - Cited Anti-Phishing Best Practices Recommendations for Registrars from APWG
http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf
 - Cited SAC 025
 - Enumerated subset of recommendations from both that FF WG believes to be applicable

Initial Report

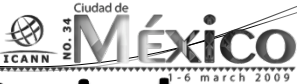
- Possible next steps (ideas for discussion and feedback during the public comment period):
 - Redefine issue and scope by developing new charter or explore further research and fact-finding prior to new charter
 - Explore the possibility to involve other stakeholders in the fast flux policy development
 - Explore other means to address the issue instead of a PDP
 - Highlight which solutions / recommendations could be addressed by policy development, best practices and/or industry solutions
 - Consider whether registration abuse policy provisions could address fast flux by empowering registries / registrars
 - Explore the possibility to develop a Fast Flux Data Reporting System



Public Comment Period

- Public Comment Period ran from 26 January to 15 February 2009
- 25 Comments received, including two from GNSO Constituencies (IPC, RC)
- Comments focused on:
 - Legitimate vs. Illegitimate use of fast flux
 - Negative impact of fast flux on digital divide
 - Unpatched computers and unsecure applications are the real reason why fast flux can be used by criminals
 - Ways in which registrars and registries can restrict fast flux
 - Restricting fast flux will not stop criminal behaviour


15



Public Comment Period

- Comments focused on (cont'd):
 - Role of ICANN in tracking and publishing reports on registrars' response rate to abusive domain names
 - Role of ICANN in formulating a best practice and/or consensus policy for registries, registrars and ISP
 - Fast flux as a technique is not a problem, only the way in which it is used by criminals to avoid detection
 - Need for accelerated domain suspension process
 - Lack of evidence to include 'free speech' advocacy groups as benefitting from fast flux
 - Need to continue work in this area despite difficulties encountered by the WG
 - Support for rapid implementation of policy measures discussed in report

16




ICANN NO. 34 Ciudad de México 1-6 march 2009

Public Comment Period

- Comments focused on (cont'd):
 - Need for stronger conflict resolution measures to deal with non-responsive registrars / IP owners
 - Problems with 'proving' the crime and take down of hosted domain does not necessarily address underlying infrastructure
 - Creation of a blacklist / whitelist of FF domains
 - Support for other means than a PDP to address fast flux
 - Need for further study and research
 - Need for more accurate description of the problem, its scope and role of ICANN, registries and registrars in suspension of domain names
 - No technical solution possible, suspension of domain names is only possibility
 - ICANN to provide leadership and guidance in developing policies and guidelines to distinguish good and bad use

17



ICANN NO. 34 Ciudad de México 1-6 march 2009

Next Steps

- Working Group to review, discuss and analyze comments received
- Continue discussions with aim to develop a final report with recommendations for the GNSO Council to consider

18

More information

- Initial Report -
<http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jano9.pdf>
- Summary of Public Comments -
<http://forum.icann.org/lists/fast-flux-initial-report/msg00025.html>
- Public Comment Forum -
<http://forum.icann.org/lists/fast-flux-initial-report/>
- Working Group Wiki -
https://st.icann.org/pdp-wg-ff/index.cgi?fast_flux_pdp_wg

19

Questions?

20