Fast Flux Hosting Final Report

GNSO Council Meeting

13 August 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)
- June 2008: Fast Flux Hosting Working Group formed
- 26 January 2009: Initial Report published

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

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, over 1,000 emails exchanged
- Where no broad agreement could be reached, the WG would use ‘support’ and ‘alternative view’ labels to indicate level of support for certain position
- Following public comment period, close review and analysis of comments received (25) and incorporation in the report where appropriate

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?

Final Report

- Final report published on 6 August 2009
- Report provides 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
- No recommendations for new consensus policy, or changes to existing policy, but a number of ideas for next steps

Charter Questions

- Who benefits from fast flux?
  - Organizations that operate highly targetable networks
  - Content distribution networks
  - Mobility support
  - Free speech / advocacy groups
  - Criminal entities
- Who is harmed?
  - Harm can arise both from legitimate and malicious uses; the WG struggled to maintain a clear distinction between harms that arise directly from the techniques themselves and harms that arise from the malicious behavior of bad actors who may use fast flux
  - No consensus concerning the separately identifiable culpability of fast flux hosting with respect to the harm caused by malicious behavior, but the WG does recognize the way in which fast flux techniques are used to prolong an attack

Charter Questions

- Who would benefit from cessation of the practice?
  - Individuals
  - Business and organizations
  - Internet Service Provider
  - Registries and Registrars
  - Law enforcement investigators
  - Digital divide (not investigated by WG, but comment submitted)
- Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?
  - Registry Constituency (RyC) provides detailed notes regarding the technical and policy options available to registry operators regarding fast flux hosting

Charter 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

Charter 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)

Charter 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?
- Information Gathering (examples):
  - 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
- Active Engagement (examples):
  - Adopt accelerated domain suspension processing in collaboration with certified investigators
  - Stronger registrant verification procedures

Charter Questions

- 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?
  - The WG considered several possible options, including governing Time-To-Live (TTL) values, charging registrants and/or registrars for nameserver changes, and requiring multiple contacts to confirm DNS updates before having them take effect, but did not reach consensus nor endorse any of these
- What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?
  - None of the possible options noted above were deemed appropriate or viable

Charter 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
  - Mannheim formula
  - Enumerated subset of recommendations from both that FF WG believes to be applicable

Constituency Statements

- Four Constituency statements: Registry Constituency, Non-Commercial Users, Intellectual Property Constituency and Registrar Constituency
- All recognize that fast flux is being used by miscreants involved in online crime to evade detection, but disagree on whether ICANN or policy development is the appropriate way forward
- All recognize the difficulty in separating legitimate from illegitimate use, and several highlight the importance of ensuring that any potential solutions do not impact legitimate use
- Overall support for further fact-finding and data gathering

Conclusions

- The WG recognizes that fast flux is a networking technique, and as such can be employed for illicit or legitimate purposes. Many types of organizations can potentially be involved in fast flux use, including registries, registrars, ISPs, hosting firms and other online businesses. Coordination and cooperation is therefore necessary.
- The WG finds that key components to better understanding of fast flux include data collection, DNS monitoring, and data sharing among various parties (e.g., registries, registrars, ISPs, and security service providers.

Conclusions (continued)

- The WG recommends that the ICANN community consider how future coordinated operational responses involving security, DNS and law enforcement communities could confront, contain, or confound fast flux hosting.
- The WG acknowledges that fast flux and similar techniques are merely components in the larger issue of Internet fraud and abuse. The techniques described in this report are only part of a vast and constantly evolving toolkit for attackers.
- These numerous and interdependent issues should all be taken into account in any potential policy development process and/or next steps.

Recommendations

- The WG would like to put forward the following ideas, ranked in order of importance, forward for further consideration by the GNSO Council:
  - Highlight which solutions / recommendations could be addressed by policy development, best practices and/or industry solutions
  - Consider whether registration abuse policy provisions could address fast flux by empowering registries / registrars to take down a domain name involved in fast flux
  - Explore the development of a Fast Flux Data Reporting System
  - Explore the possibility of ICANN as a best practices facilitator
  - Explore the possibility to involve other stakeholders in the fast flux policy development process
  - Redefine the issue and scope

More information

- Final Report – [link to be included]
- Initial Report - http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.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

Questions?