GNSO Issues Report on Fast Flux Hosting

STATUS OF THIS DOCUMENT

This is the Issues Report on Fast Flux Hosting requested by the GNSO Council.

SUMMARY

This report is submitted to the GNSO Council in response to a request received from the Council pursuant to a Motion proposed and carried during the Council teleconference meeting on 6 March 2008.

TABLE OF CONTENTS

1 Executive Summary

Background

The ICANN Security and Stability Advisory Committee (SSAC) recently completed a study of the way in which the DNS can be manipulated by Internet cyber-criminals to evade detection and termination of their illegal activities. The results of the study were published in January 2008 in the *SSAC Advisory on Fast Flux Hosting and DNS* (SAC 025)[1], which describes the techniques that are collectively referred to as "fast flux hosting," explains how these techniques enable cybercriminals to extend the maliciously useful lifetime of compromised hosts employed in illegal activities, and "encourages ICANN, registries, and registrars...to establish best practices to mitigate fast flux hosting, and to consider whether such practices should be addressed in future [accreditation] agreements."[2]

During its teleconference meeting on 6 March 2008,[3] the GNSO Council entertained the following motion, which carried:

> "ICANN Staff shall prepare an Issues Report with respect to 'fast flux' DNS changes, for deliberation by the GNSO Council. Specifically the Staff shall consider the SAC Advisory [SAC 025], and shall outline potential next steps for GNSO policy development designed to mitigate the current ability for criminals to exploit the DNS via 'fast flux' IP or nameserver changes."

In responding to this request, ICANN Staff have considered the SAC Advisory (SAC 025), and have consulted other appropriate and relevant sources of information on the topic of fast flux hosting.

Definitions

Fast Flux

In this context, the term "fast flux" refers to rapid and repeated changes to A and/or NS resource records in a DNS zone, which have the effect of rapidly changing the location (IP address) to which the domain name of an Internet host (A) or name server (NS) resolves.

Single Flux

[1] http://www.icann.org/committees/security/sac025.pdf
[2] Although the report (SAC 025) refers only to "agreements," the SSAC presentation on Fast Flux Hosting at the February 2008 ICANN meeting in Delhi (http://delhi.icann.org/files/presentation-rasmussen-fast-flux-13feb08.pdf) made it clear that the intended reference is to "accreditation agreements."
[3] http://gnso.icann.org/meetings/agenda-06mar08.shtml

A variant of fast flux in which rapid updates to A records in the zone file of a subdomain (usually second- or third-level) cause the location (IP address) of Internet hosts (*e.g.*, web sites or other content servers) to change rapidly.

Name Server Flux
A variant of fast flux in which rapid updates to NS records in the zone file of a top-level domain cause the location (IP address) of the name server(s) for one or more subdomains to change rapidly.

Double Flux
A variant of fast flux in which both single flux and name server flux are employed to cause the location of both hosts and name servers to change rapidly.

Fast Flux Hosting
The practice of using fast flux techniques to disguise the location of web sites or other Internet services that host illegal activities.

Fast Flux Service Network
A network of compromised computer systems (a "botnet") with public DNS records that are constantly changing.

Staff recommendation

The issues surrounding fast flux hosting have generated significant discussion among several constituencies and stakeholders and would benefit from further research and review. Staff therefore recommends that the GNSO sponsor further fact-finding and research concerning guidelines for industry best practices before considering whether or not to initiate a formal policy development process. Staff resources would be made available to support these research activities and objectives. To assist the community with its decision-making process, ICANN staff would welcome guidance on specific directions for further research.

However the GNSO may choose to proceed, staff notes that the completion of concrete fact-finding and research will be critical in informing the community's deliberations.

In determining whether the issue is within the scope of the ICANN policy process and the scope of the GNSO, staff and the General Counsel's office have considered the following factors:

- whether the issue is within the scope of ICANN's mission statement;
- whether the issue is broadly applicable to multiple situations or organisations;
- whether the issue is likely to have lasting value or applicability, albeit with the need for occasional updates;
- whether the issue will establish a guide or framework for future decision-making; and
- whether the issue implicates or affects an existing ICANN policy.

Based on the above, the General Counsel's opinion is that some aspects relating to the subject of fast flux hosting are within the scope of the ICANN policy process and within the scope of the GNSO. However, the General Counsel further notes that the overall question of how to mitigate the use of fast flux hosting for cybercrime is broader than the GNSO policy development process. Some steps that may be employed to discourage or curb fast flux hosting, such as steps that might be taken by ccTLDs, ISPs, or by Internet users themselves, would not be within the scope of GNSO policy making. Domains in ccTLDs are targeted as well. In addition, the question of whether policy options would have "lasting value or applicability" is a particularly important consideration in the context of fast flux hosting, where new static rules imposed through a policy development process might be quickly undermined by intrepid cybercriminals.

Based on information available to-date, staff suggests that potential policy development options be studied more closely. Further fact-finding will provide needed insights to best inform the Council as to the policy options that would be most effective. Preferred options could then provide the foundation for launching a specific policy development process.

2 Objective

This report is submitted in response to the request from the GNSO Council for an "Issues Report on Fast Flux Hosting."

In this context, and in compliance with ICANN Bylaw requirements:

a. The proposed subject raised for consideration is fast flux hosting.
b. The identity of the party submitting the issue is the GNSO Council.

c. How that party is affected by the issue: The GNSO is responsible for policy development concerning generic top-level domains. Fast flux hosting frequently targets gTLDs (although it is also observed in ccTLDs), and the GNSO is concerned about the phishing, pharming, and other cybercrime activities that may reduce the operational stability and security of the Internet and that are facilitated by techniques that may fall within the scope of the GNSO's policy making responsibilities.
d. Support for the issue to initiate the PDP: Adequate support for the preparation of this Issues Report was demonstrated during the GNSO Council teleconference meeting on 6 March 2008. There were 10 votes in favor of developing an Issues Report, and 14 votes in opposition. Under the ICANN bylaws an issue may be raised for consideration as part of a PDP "by a vote of at least 25% of the members of the Council present…".

3 Background

"Fast flux" refers to rapid and repeated changes to A and/or NS resource records in a DNS zone, which have the effect of rapidly changing the location (IP address) to which the domain name of an Internet host (A) or name server (NS) resolves. Although some legitimate uses for this technique are known (see below), it has within the past year become a favorite tool of phishers and other cybercriminals who use it to evade detection by anti-crime investigators.

How fast flux works[4]

The goal of fast-flux is for a fully qualified domain name (such as *www.example.com*) to have multiple IP addresses (hundreds or even thousands) assigned to it. These IP addresses are changed in and out of zone file A (host address) and/or NS (name server) records with extreme frequency, using a combination of round-robin IP addresses and a very short time-to-live (TTL). Web site host names may be associated with a new set of IP addresses which can change rapidly. A browser connecting to the same web site repeatedly over a short period of time could actually be connecting to a different infected computer each time. In addition, the attackers ensure that the compromised systems they are using to host their scams have the best possible bandwidth and service availability. They often use a load-distribution scheme which takes into account node health-check results, so that unresponsive nodes are taken out of flux and content availability is always maintained.

[4] The material in this section is based on, and in some cases taken verbatim from, the description at http://www.honeynet.org/papers/ff/fast-flux.html.

Proxy redirection adds a second layer of obfuscation to fast flux. When someone hosting malicious content (a phishing site, for example) uses a fast-flux network, the hosts that are “fluxed” (by rapidly changing the IP address to which the domain name resolves) are typically proxies that redirect queries to the site that contains the attacker’s actual content. That’s simpler for the attacker, because instead of having to copy his malicious content to many different bots, he can put it on one host, and deploy a botnet of redirecting proxies that all point to that host. The fluxing then takes place among the redirectors. Redirection disrupts attempts to track down and mitigate fast-flux service network nodes. The domain names and URLs for advertised content no longer resolve to the IP address of a specific server, but instead fluctuate amongst many front-end redirectors or proxies, which then in turn forward content to another group of backend servers. While this technique has been used for some time in the world of legitimate webserver operations, for the purpose of maintaining high availability and spreading load, in this case it is evidence of the technological evolution of criminal computer networks.

Fast-flux “motherships” are the controlling element behind fast-flux service networks, and are similar to the command and control (C&C) systems found in conventional botnets. However, compared to typical botnet servers, fast-flux motherships have many more features. It is the upstream fast-flux mothership node, which is hidden by the front end fast-flux proxy network nodes, that actually delivers content back to the victim client who requests it. Certain fast flux command and control systems employ peer to peer (P2P) applications and so operate successfully for extended periods of time in the wild. These nodes are often observed hosting both DNS and HTTP services, with web server virtual hosting configurations able to manage the content availability for thousands of domains simultaneously on a single host.

Fast-flux networks are responsible for many malicious practices, including online pharmacy shops, money mule recruitment sites, phishing web sites, extreme/illegal adult content, malicious browser exploit web sites, and the distribution of malware downloads. Beyond DNS and HTTP, other services such as SMTP, POP, and IMAP can be delivered via fast-flux service networks. Because fast-flux techniques utilize TCP and UDP redirects, any directional service protocol with a single target port would likely encounter few problems being served via a fast-flux service network—so it's not just web sites; it could also be fraudulent email sites.

Legitimate uses of fast flux

From preliminary research, staff understands 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.[5] A high-traffic site might use this technique—which satisfies the definition of "fast flux"—to adapt its home page addresses to internal and external network conditions, such as server load, outages, user location, and resource reconfiguration. Because almost all web browsers cache domain name lookups for at least 15-20 minutes, regardless of the advertised TTL, the net effect of a short TTL is to set the actual timeout to the "attention horizon" of the browser. The ability to reconfigure quickly is considered by these service providers to be important enough to offset the additional query latency introduced by more-frequent DNS lookups. More research is needed to better understand legitimate uses and their prevalence.

Staff also understands that service providers might be able to fast-flux their IP addresses to deal with situations in which a government or other actor is deliberately blocking ("black-holing") their addresses in an effort to prevent access to their services from within a country or region. This was described anecdotally as a possible "legitimate use". This is another area where both technical issues may need to be better understood to inform further discussion.

Why fast flux is a problem

Phishing, pharming, and other malicious (and frequently illegal) activities represent a well-known threat to the safety and security of Internet users. Those engaged in these activities can frustrate the efforts of investigators to locate and shut down their operations by using fast flux service networks to rapidly and continuously change the IP address at which their content is hosted, staying "one step ahead" of their law-enforcement pursuers.

Single-flux service networks change the DNS records for their front end node IP address as often as every 3-10 minutes, so even if one flux-agent redirector node is shut down, many other infected redirector hosts are standing by and available to quickly take its place. Fast-flux networks tend to be composed primarily of compromised home computers, because unlike the computing infrastructure of a company or other organization with an IT department, home computers are difficult to protect with anti-malware measures.

Fast-flux service networks create robust, obfuscating service delivery infrastructures that make it difficult for system administrators and law enforcement agents to shut down active scams and identify the criminals operating them.

[5] Information received by Staff suggests that TTLs of 300 seconds may be typical in these configurations. Again, more research is needed to verify.

Why ICANN should be concerned about fast flux

The community of researchers, system administrators, law enforcement officials, and consumer advocates who are fighting Internet scams that are enabled or accelerated by fast flux hosting have concluded that trying to thwart fast flux hosting by detecting and dismantling the botnets (fast flux service networks) is not effective. Other measures that require the cooperation of DNS registries and registrars to identify or defeat fast flux techniques are expected to be much more effective. ICANN should consider whether and how it might encourage registry operators and registrars to take steps that would help to reduce the damage done by cybercriminals by curtailing the effectiveness of these DNS-based exploits.

4 Discussion of possible directions

ICANN Staff research has confirmed that fast flux hosting:

- is a real phenomenon—it has been observed, documented, and reported by a variety of reputable sources, including members of the Anti-Phishing Working Group;
- makes it more difficult for investigators to identify and shut down malicious activity; and
- could be significantly curtailed by changes in the way in which DNS registries and registrars currently operate.

Because fast flux hosting involves many different players—the cybercriminals and their victims, ISPs, companies that provide web hosting services, and DNS registries and registrars—it is possible to imagine a variety of different approaches to mitigation. The SSAC advisory identifies three approaches to mitigation, each of which requires the cooperation of a different set of actors:

- eliminate botnets (users and ISPs);
- identify and shut down the fast flux hosts (ISPs); and
- change the way in which registries and registrars handle zone updates, which may reduce fast flux or make it unattractive (registries and registrars). As explored further below, more research and discussion is needed to explore the effectiveness of various options over time.

Anti-cybercrime experts have told Staff that trying to stop phishing and other Internet fraud by eliminating botnets is futile. Most botnets are assembled from compromised computers connected to residential

broadband networks (for example, DSL or cable), and it is just too easy to spread malware among that population; and although it might be possible to get ISPs in some countries to cooperate in the identification and elimination of botnets, some ISPs may be out of reach and provide "safe havens" for malicious botnet operators.

Anti-cybercrime investigators and law enforcement officials are often able to obtain court orders to shut down phishing and pharming sites when they are identified, but fast flux is designed specifically to evade these "takedown" efforts by making it difficult to track illegal activity and identify its actual location.

Registries and registrars can curb the practice in two ways: (1) by monitoring DNS activity (fast flux is easy to detect) and reporting suspicious behavior to law enforcement or other appropriate reporting mechanism; and (2) by adopting measures that make fast flux either harder to perform or unattractive. Some possible measures that have been suggested (and in some cases implemented[6]) include:

- authenticating contacts before permitting changes to NS records;
- preventing automated NS record changes;
- enforcing a minimum "time to live" (TTL) for name server query responses[7];
- limiting the number of name servers that can be defined for a given domain; and
- limiting the number of address record (A) changes that can be made within a specified time interval to the name servers associated with a registered domain.[8]

While these measures have been suggested, each may have further implications that staff recommends be explored. It should be noted that the GNSO policy development process is one of several ways that fast flux hosting might be addressed within the ICANN community. This section describes the various mechanisms for addressing this issue in order to inform the ICANN community of possible directions that may be taken.

[6] Staff is aware of steps that were taken recently by the Public Interest Registry to make it unattractive for cybercriminals to use fast flux in the .org TLD.
[7] 30 minutes has been suggested as a reasonable TTL lower bound, and staff understands that some registrars have implemented a 30 minute TTL. Registries and registrars might be able to define exception conditions for legitimate uses of shorter TTLs but it may be difficult in practice to differentiate legitimate uses from malicious applications.
[8] Some are suggesting to staff that legitimate activities would not be hurt by limiting the number of name servers for a given domain to 5, and limiting the number of changes to 5 per month. In PIR's experience, charging a very small fee for changes in excess of 5 per month, rather than prohibiting them, is sufficient to eliminate fast fluxing entirely.

Development of industry best practices guidelines

Additional research and discussion within the community could lead to the development of a set of guidelines for industry best practices. Within ICANN's purview, these might form the basis of either voluntary actions by registries and registrars or, pursuant to a subsequent policy development process, requirements incorporated into registry contracts or registrar accreditation agreements. Outside of ICANN's immediate purview, these might be promoted to ISPs and other Internet infrastructure operators and service providers as desirable actions and measures that they might voluntarily undertake.

As stated in the staff recommendations (see Section 5 and Executive Summary in Section 1), ICANN staff support the sponsorship of additional fact-finding and research to develop best practices guidelines as the first step that should be undertaken by the GNSO.

GNSO Policy Development Process

A policy recommendation on this issue could impose new requirements, or institute new prohibitions applicable to contracted parties, which ICANN staff would then implement and enforce through its contracts with registries and/or registrars. However, ICANN could only impose new obligations on registries and registrars if fast flux hosting is an issue "for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, technical reliability, and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet." (RAA Section 4.2.1)

5 Staff recommendation

As discussed in more detail below, staff recommends that the GNSO sponsor additional fact-finding and research to develop best practices guidelines concerning fast flux hosting. It may be appropriate for the ccNSO also to participate in such an activity.

Scope

In determining whether the issue is within the scope of the ICANN policy process and the scope of the GNSO, staff and the General Counsel's office have considered the following factors:

Whether the issue is within the scope of ICANN's mission statement

The ICANN Bylaws state that:
“The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In particular, ICANN:
1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are
    a. domain names (forming a system referred to as "DNS");
    b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and,
    c. protocol port and parameter numbers.
2. Coordinates the operation and evolution of the DNS root name server system.
3. Coordinates policy development reasonably and appropriately related to these technical functions.”

Fast flux hosting involves the association of domain names with IP addresses through the operation of name servers, including the information about a delegated second-level domain that is maintained by registrars and by the registry for the TLD in which that SLD is registered. ICANN has only limited responsibility for policy development related to these technical functions. While items 1a and 3 above are general subjects that fall within the scope of ICANN’s mission statement, some policy options would not be within the scope of GNSO policy making.

Whether the issue is broadly applicable to multiple situations or organisations

A consideration of the issues surrounding fast flux hosting would be broadly applicable to multiple situations or organisations, including each existing gTLD under contract with ICANN, each of 800+ accredited registrars, and a diversity of existing and potential registrants. Note however that a consensus policy resulting from the GNSO policy-development process would only be applicable to gTLD registries and registrars operating under contract with ICANN (and only if if fast flux hosting is an issue “for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, technical reliability, and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet.” See, e.g. RAA Section 4.2.1).

Whether the issue is likely to have lasting value or applicability, albeit with the need for occasional updates

Completion of policy development work on issues related to the subject of fast flux hosting may affect future gTLDs, future registrars, and potential business or non-commercial entities which have not as yet

entered the market. Consideration will need to be given to how to develop policy options that have more enduring benefit and that will not be quickly circumvented by malicious actors.

Whether the issue will establish a guide or framework for future decision-making

The outcome of a policy development process may have lasting value as precedent, although the particular circumstances of the market will continue to evolve, and will thus establish a framework for future decision-making on related issues.

Whether the issue implicates or affects an existing ICANN policy

The issue does not implicate or affect an existing ICANN policy. A list of consensus policies is available at http://www.icann.org/general/consensus-policies.htm.

Based on the above, the General Counsel's opinion is that some aspects relating to the subject of fast flux hosting are within scope of the ICANN policy process and within the scope of the GNSO. As fast flux hosting activities concern gTLDs, the issue is within the scope of the GNSO to address. However, the overall question of how to mitigate the use of fast flux hosting for cybercrime is broader than the GNSO policy development process. Some steps that may be employed to discourage or curb fast flux hosting, such as steps that might be taken by ISPs or by Internet users themselves would not be within the scope of GNSO policy making. Furthermore, although fast flux hosting frequently targets gTLDs, it is also observed in ccTLDs. In addition, the question of whether policy options would have "lasting value or applicability" is a particularly important consideration in the context of fast flux hosting, where static policies might be quickly undermined by intrepid cybercriminals. Based on information available to-date, staff suggests that potential policy development options be studied more closely. Further fact-finding will provide needed insights to best inform the Council as to the available policy options that would be most effective. Preferred options could then provide the foundation for launching a specific policy development process.

Recommended action

Staff recommends that the GNSO sponsor additional fact-finding and research to develop best practices guidelines concerning fast flux `hosting, and to provide data to assist policy development and illuminate potential policy options. The development of best practices should be done by collaborating broadly with knowledgeable individuals and organizations and shared broadly to encourage broad input and wide adoption. Some registrars may already implement some of the measures identified in SAC 025 and staff

recommends consultation with these registrars to determine the efficacy of these measures how they can best be implemented. Staff resources can be made available to support these research activities and objectives.

The SSAC's study of fast flux hosting, as well as several trade articles have focused on the following important questions, including:

- Who benefits from fast flux, and who is harmed?
- Who would benefit from cessation of the practice and who would be harmed?
- How are registry operators involved in fast flux hosting activities?
- How are registrars involved in fast flux hosting activities?
- How are registrants affected by fast flux hosting?

Some additional questions that might productively be addressed as part of fact-finding include:

- How are Internet users affected by fast flux hosting?
- What enforceable rules could be applied to reduce or eliminate the negative effects of fast flux hosting?
- What would be the impact (positive or negative) of establishing limitations, guidelines, or restrictions on registrars and/or registries with respect to practices that enable or facilitate fast flux hosting?
- What measures should be implemented by registries and registrars to mitigate the negative effects of fast flux? Should these measures be documented and promoted as "industry best practices," incorporated into registry contracts and registrar accreditation agreements, or promulgated in some other way?

Annex 1 – GNSO Request for Issues Report on Fast Flux Hosting

This annex reproduces in full the request for an issues report sent by the GNSO Council:

Whereas, "fast flux" DNS changes are increasingly being used to commit crime and frustrate law enforcement efforts to combat crime, with criminals rapidly modifying IP addresses and/or nameservers in effort to evade detection and shutdown of their criminal website;

Whereas, the Security and Stability Advisory Committee has reported on this trend in its Advisory SAC 025, dated January 2008: http://www.icann.org/committees/security/sac025.pdf/

Whereas, the SSAC Advisory describes the technical aspects of fast flux hosting, explains how DNS is being exploited to abet criminal activities, discusses current and possible methods of mitigating this activity, and recommends that appropriate bodies consider policies that would make practical mitigation methods universally available to all registrants, ISPs, registrars and registries,

Whereas, the GNSO is likely an appropriate party to consider such policies

The GNSO Council RESOLVES:

ICANN Staff shall prepare an Issues Report with respect to "fast flux" DNS changes, for deliberation by the GNSO Council. Specifically the Staff shall consider the SAC Advisory, and shall outline potential next steps for GNSO policy development designed to mitigate the current ability for criminals to exploit the DNS via "fast flux" IP or nameserver changes.