Internet New Zealand (Inc)

Submission to ICANN

on

Global DNS-CERT Business Case

13 April 2010
Public Version (there is no confidential version)

For further information, please contact:

Jay Daley	.nz Registry Services	jay@nzrs.net.nz
Keith Davidson	InternetNZ	keith@internetnz.net.nz
Debbie Monahan	Domain Name Commission Ltd	dnc@dnc.org.nz

Table of Contents

1 Introduction

1.1 This submission is from InternetNZ (Internet New Zealand Inc)

1.2 InternetNZ is a membership-based, non-partisan, not-for-profit charitable organisation responsible for the administration of the .nz top level domain.

1.3 Our mission is to protect and promote the Internet for New Zealand; we advocate the ongoing development of an open and uncaptureable Internet, available to all New Zealanders.

1.4 InternetNZ has two wholly-owned charitable subsidiaries to whom management, operation and regulation of the .nz top level domain are delegated. These are:

1.4.1 .nz Registry Services, the Registry
1.4.2 Domain Name Commission Limited, the Regulator

1.5 The concept of a DNS-CERT is well established, as it was one of the long-term objectives of DNS-OARC when it was formed in 2004. It was recognised then, as it is now by ICANN, that the first step in securing the long-term security of the DNS is instrumentation and analysis of DNS data, currently provided by DNS-OARC, CAIDA and SSAC; the second is a shared medium for incident referral between peers, as provided by many groups, and; the third is a single coordination point for information sharing and coordinated incident response, which has so far developed on a per-threat basis. The fourth step, which is absent from this proposal, is a forum for the long-term strategic planning of securing the DNS such as the work of SSAC, RISG and some private groups.

1.6 We congratulate ICANN on getting up to speed on the strategic need to secure the DNS and their desire to contribute to the extensive work already being undertaken in this area.

1.7 In summary, we regard this proposal as under-developed in some key areas and over-developed in some less relevant areas and recommend the concerns we express here are incorporated into a new proposal that is balanced and comprehensive.

2 Scope

2.1 It is unclear from the proposal whether ICANN is making a distinction between DNS and domain names. This is particularly important when looking at the influence that those tasked with protecting claims of intellectual property have had on other aspects of ICANN policy making and operations. This influence is most notable in the erroneous conflation of preventing criminal activity and trademark protection, which is generally a civil matter, into a single concept of domain name security. This is evidenced by the placeholder in the proposal on High Security TLDs in DAG v3 for later inclusion of protecting claims of intellectual property.

2.2 As a result of this general conflation it is unclear whether ICANN intends the DNS-CERT to tackle only criminal activity or whether they intend it to be used as a means for fast takedown of domains alleged to be infringing trademarks. If there were any suggestion that this proposal would be for anything other than tackling obvious criminal activity then we could not support it at all.

2.3 A third possible area of scope for a DNS-CERT might be the detection and 'policing' of DNS synthesis below the TLD level but it is difficult to see how that might be possible without the appropriate regulatory framework to fall back on.

3 Justification

3.1 On balance we agree that a DNS-CERT would add to the provision for DNS incident response but we question the assertions in the business case that the lack of DNS-CERT provides gaps for vulnerabilities to slip through and consider that other solutions are possible.

3.2 The Kaminsky variant on cache poisoning is cited an example of where a DNS-CERT would be needed to help protect us from the impacts of a similar vulnerability being discovered. Disappointingly no mention is made of the response to the Kaminsky discovery, presumably because it is contra-indicative of the urgent need for a DNS-CERT.

3.3 The response to the Kaminsky discovery saw the rapid-formation of an ad-hoc group of DNS experts, managers of large DNS infrastructures and developers of DNS software. This group coordinated the development and release of patches for those DNS products that were most vulnerable (it is important to note that many products were far less vulnerable than others) which were generally applied on global scale on the basis trust alone because the nature of the vulnerability was not disclosed. As well as accomplishing this extraordinary feat it took place without any significant leakage of the details of the vulnerability before a solution was ready.

3.4 This clearly demonstrates that the community acted in an agile, available and successful way to handle a major threat of this nature without the involvement of a DNS-CERT.

3.5 Another example given in the business case is that of the response to the Conficker worm. This saw the TLD community cooperating on an unprecedented scale with such effectiveness that the authors of the malware quickly moved away from using DNS in this way to other mechanisms that were easier to exploit. This conclusion from this reaction is quite clear, that the self-coordinated efforts of TLDs defended DNS to such an extent that it is now seen a hard target not a soft target by malware writers and they will almost certainly go elsewhere to follow the path of least resistance.

3.6 It is difficult to see how the response to Conficker could have been any better. Yes some TLDs needed prodding to participate, but they all did so willingly and effectively. So much so that there are some questioning whether the threat from Conficker was exaggerated.

3.7 So the claim in the business case that a "dedicated and sustained incident response coordination activity would have enhanced the global response to this issues." does not stand up. It is difficult to see what benefit a DNS-CERT could have provided other than taking over some of the activities that others undertook voluntarily.

4 Other groups

4.1 As ICANN have acknowledged there are many other groups already working in the area of incident response for DNS. The business case lists some of them and there are other private and secret groups that also contribute substantially to the cause. The most notable omission from the business case is ICANN's own Security and Stability Advisory Committee (SSAC) which is one of the few groups taking the longer term strategic view on DNS security.

4.2 What these groups all have in common is:

- 4.2.1 a trust model for authenticating participants, communications channels and controlling access to information. Each has a different model, depending on the way they operate but each model is well defined and the culture of cooperation is well established.
- 4.2.2 established situational awareness. These groups and the people in them already have a very good situational awareness arising from the roles of the participants. These participants are all professionals in the DNS industry, security industry or law enforcement and so do not have to go out to develop the necessary interactions to build situational awareness, it comes to them.
- 4.2.3 committed participants. This is not a big industry and the same people appear in different places.

4.3 It is important to understand what these groups do without being too specific on what group does what to understand what a DNS-CERT might contribute. Various groups are responsible for:

- 4.3.1 instrumentation of DNS services and exchange of baseline operational data
- 4.3.2 detection of vulnerabilities and bad actors
- 4.3.3 detection and rapid takedown of domain names registered for obvious criminal purposes
- 4.3.4 research into DNS behaviour and behaviour of malware targeting DNS
- 4.3.5 development of policies for automated data sharing
- 4.3.6 development of policies for legal liabilities and indemnification
- 4.3.7 coordination of exchange of research findings and collaborative research
- 4.3.8 coordination of data exchange on domains of interest
- 4.3.9 strategic planning for long term success against criminals

4.4 If we look carefully at how a DNS-CERT might compare to these groups then we see some positives and negatives. The positives are:

4.4.1 A DNS-CERT could likely involve more TLDs due to the support of ICANN and its claim to be the single coordination point.

4.4.2 If it has the funding indicated in the business plan then it will be better funded than any of the other organisations, though how it will be funded is not specified. It is also not explored whether the money identified could be better spent by supporting other existing organisations.

4.4.3 Planned to be 24x7x365, which is again better than the other groups who are not staffed for 24x7 or rely on voluntary efforts.

4.5 The negatives are:

4.5.1 Planned to only cover one narrow aspect of this work and even that is not as clearly defined as the other groups, which precipitates unintended scope creep.

4.5.2 Does not have an established trust model so will need to build one quickly to be effective whilst ensuring there is no infiltration.

4.5.3 The individuals will not have the day job that maintains their situational awareness and so will need to continuously work to maintain it.

4.5.4 Not clear how it would work with other groups already established.

4.6 We should also acknowledge that a few committed individuals have been involved in many of the groups, both formal and ad-hoc described above. They have been instrumental in creating the whole scope of DNS security and their continuing engagement in any major development such as a DNS-CERT is vital if it is to succeed.

5 Trust and reputation

5.1 As described above, trust and reputation are vital in the efforts to protect the DNS by existing groups. The malware industry is large, heavily integrated with organised crime and there is genuine risk to those individuals involved in combating it. The mitigation for this is closed communities with strict entry controls and protected sources of information.

5.2 The DNS-CERT proposal will have some difficulty in establishing a globally supported group, receiving information from multiple sources and spreading that to multiple different sources whilst maintaining a trust model between all the participants. In fact it may be too difficult to achieve with any practical success, in which case we should be clear of the consequences.

5.3 Much reporting of criminal domains or hosts comes from security researchers either in law enforcement or security companies. They cannot let criminals become aware of the work they do in gathering and sharing that information because of the risks that come from that. Therefore without that assurance they will not provide the information that a DNS-CERT needs to work with.

5.4 It might be claimed that this can be overcome by the DNS-CERT acting as the intermediary for the data, anonymising the source. However this leads to

serious issues of liability and accountability, which reduces the trust that recipients of the data can place on it, again potentially reducing their involvement in the system. If the DNS-CERT were to assume the liability itself then it would need to be trusted for people to act on its data, which takes time to build up and only happens if nobody abuses the system.

5.5 If the DNS-CERT were established within an existing incident response organisation with an existing trust model then this issue could be tackled quickly. Without wishing to offend we should be clear that ICANN does not have the level of trust required to achieve this. Many individuals working for ICANN do but organisationally it does not.

5.6 We should point out that one of the groups listed in the business case does not seek such publicity and asks members not to reveal the existence of the group. For ICANN to have 'blown its cover' in a document about increasing security is a sad irony and indictment of ICANN's current situational awareness.

6 Urgency

6.1 Recent comments from the ICANN CEO are that DNS is in crisis and a DNS-CERT is urgently needed to address this issue. The indication was that this comes from the dual threats of criminal activity and DNS synthesis. DNS synthesis is indeed a blight on DNS but it is not possible to see what role a DNS-CERT could have in combating that, as mentioned above. This leaves just obvious criminal activity as the urgent threat.

6.2 While nobody can be sure of the big picture of DNS threats it is clear that the urgency has been significantly exaggerated. Yes DNS threats are real and yes they need tackling, but the single biggest gain will come from the full implementation of DNSSEC and if there is any area where greater urgency is required then it will be in the end user adoption of DNSSEC once the root is signed.

6.3 We therefore explicitly reject any suggestion that the security threats are so bad that the response should be a hurried establishment of a DNS-CERT. Doing it right is more important than doing it quickly.

7 Suitability of ICANN

7.1 While the proposal is quite clear that there is no presupposition to ICANN running the DNS-CERT we feel sufficiently strongly that ICANN should not run a DNS-CERT that we make this case here. The reasons for this view are:

7.1.1 ICANN has a limited operational role under contract to NTIA, the rest and majority of the work is policy. The separation of policy from operations provides for a clear demarcation of responsibilities, which will be undermined by incorporating activities such as operating a DNS-CERT in ICANN. It isn't as if ICANN isn't involved in the security area as they already have SSAC doing an

important job in monitoring security and stability and proposing appropriate policies to ensure the ongoing operation of the DNS.

7.1.2 A DNS-CERT does not fit within ICANN's multi-stakeholder model. There is some overlap in stakeholders but the overall picture is very different. For example only a few security companies are involved in ICANN (though with a disproportionate influence) whereas the majority will need to engage with the DNS-CERT. Managing an organisation with such a different set of stakeholders would not be beneficial to either ICANN or the DNS-CERT, but without a different set of stakeholders it would be difficult to create the trust needed.

7.1.3 The combination of a DNS-CERTs responsibilities with the role of ICANN puts too many parts of due process into the hands of one organisation and sees ICANN increase the risk it has to manage considerably. ICANN would be in the position of setting the policy in the gTLD space, investigating and alerting on criminal activity by the DNS-CERT and then taking enforcement action on those reports as ICANN., with all the risks such action incurs.

7.2 We note that the business plan is far more detailed than we would expect if there was genuine neutrality on where the function should be performed. If a third party organisation were to consider the role then we would expect them to propose staffing levels, operational practices and funding mechanisms.

8 Recommendations

8.1 We recommend that ICANN:

8.1.1 Amend this proposal to cover the issues identified above and remove the excess detail from the business plan that unduly constrains a potential third party.

8.1.2 Includes as part of the amended version, an option for funding a DNS-CERT as an external venture.

8.2 With the amended version in place ICANN could then ask for expressions of interest from third party organisation interested and capable of running a DNS-CERT with a special emphasis on current involvement in this space and their track record in establishing such services.

With many thanks for your consideration,

Yours sincerely,

InternetNZ