Association Française pour le Nommage Internet en Coopération
chargée de la gestion des noms de domaine en *.fr* et *.re*

AFNIC comment on ICANN's draft on DNS-CERT

We have read with interest the business case for the DNS-CERT (http://www.icann.org/en/public-comment/#dns-cert). AFNIC is grateful for the opportunity to comment on such an essential initiative.

Apart from its mission to ensure security and stability of the TLD it manages, AFNIC is already involved in several initiatives to enhance the global security and stability of the Internet. AFNIC is a member of DNS-OARC, one of the initiatives mentioned in the document, works closely with the French national CERTs, and sponsors the BIND 10 project initiative.

Improving the security of the DNS infrastructure is a major goal for organisations like AFNIC and any initiative in this direction is welcome. We firmly believe that the success of such initiatives relies on their ability to grasp the decentralised nature of the management of the Internet.

For this initiative to be a success, its perimeter has to be carefully considered, in order to build a critical mass of involved stakeholders so that global progress can be made. To achieve such results an essential factor is trust and commitment. After witnessing the consultations in Nairobi and other fora, we fear that these success factors have not been given sufficient attention until now.

For instance it remains unclear to us at this stage which stakeholders have endorsed the DNS-CERT initiative.

Conficker is mentioned in section 2.6.1. It is, in our opinion, a bad example. Unlike what 2.6.1.3 says, there is no consensus among those who participated to the anti-Conficker effort about the need for a dedicated agency.

Quite the contrary, many participants expressed the opinion that the anti-Conficker effort was a good example of self-organization.

Our second concern is that the current proposal does not seem focused enough. For instance, it mentions issues which are indeed relevant to the DNS protocol, such as the Kaminsky bug but also issues about name registration which have little to do with the security and stability of the DNS (such as the Conficker case). This increases the risk of duplication of existing efforts on the one hand, and the risk of inefficiency due to dispersion on the other hand. We therefore urge ICANN to provide more details about the actual scope of the project.

AFNIC notices that no comprehensive report was published about the entire anti-Conficker effort, analyzing it and extracting lessons.

AFNIC - Immeuble International - Montigny le Bretonneux - 78181 Saint Quentin en Yvelines Cedex (France)
Tél. : +33 (0)1 39 30 83 00 - Fax : +33 (0)1 39 30 83 01 - afnic@afnic.fr - www.afnic.fr

This may be because, for the Conficker C worm, DNS was just one among many other rendez-vous techniques and there is little evidence that the takedown without due process of so many domain names did anything to throttle the worm.

However the Conficker efforts have demonstrated that efficiency on the global level requested involvement of parties far beyond the usual ICANN stakeholders, such as ISPs across the globe, hardware and software vendors... The document remains unclear about how ICANN intends to engage with these parties.

AFNIC also remarks thats, since the Internet is international, a lot of careful thought needs to be devoted to the legal issues. We need to improve the security while complying with existing legal frameworks. Exchange of data is an important concern and deserves more that the last short paragraph at the end of the proposal. Everybody regrets the lack of communication between stakeholders but few people recognize that part of this problem is the lack of data protection in some countries, which lead to the impossibility of sharing sensitive data.

Some specific detail points:

- "*Although DNS failures can be sometimes be attributed to natural phenomena, they are most often associated with intentional attacks.*"
There are no references to back up this statement, which certainly does not match our experience. Many DNS failures indeed do occur by accident or lack of technical knowledge and that is why automatic testing tools to catch configuration mistakes are so important. Any information that ICANN could share with us and the rest of the community on this issue would be highly welcome.

- The footnote in page 7 about the various names of Conficker is wrong. SQL Slammer is a completely different (and much older) beast. Same thing for "Code red".

In summary AFNIC is willing to extend its existing contribution to security and stability of the Internet, even beyond its role of TLD manager. Building a network of trusted parties both at national and international levels is key to this objective. Such network should reach to all involved stakeholders, and allows to share technical information and expertise in confidence.

Existing initiatives such as DNS-OARC or FIRST could in this respect be reinforced and would probably welcome ICANN's support in this regard.
ICANN could in particular be extremely helpful in encouraging registries and registrars to join these initiatives.

However we believe that at this stage the concept of DNS-CERT is too vague and demand has not been demonstrated. From the Nairobi consultations, we have understood that the project essentially raised concerns of duplication of efforts. Since the funding itself remains unclear as well, it is highly premature to consider allocating such a funding as detailed in the document to the concept.

That being said, we look forward to working with ICANN and other involved initiatives in order to consolidate the assessment of the risks and weaknesses described in 2.8.3.