Need for Contact repository

Executive Summary

The Contact Repository Implementation (CRI) WG was set up in 2011 to advise the community on how to implement a service that would enable ccTLD operators to send each other early warnings of large-scale DNS(-related) incidents. The service is known as the "ccTLD Contact Repository" and originates from the work of the Incident Response (IR) WG, which the ccNSO established in the aftermath of the Conficker incident in 2009.

The CRI WG has been working on the requirements and governance model of the Contact Repository, but without articulated realistic use cases (illustrating how the service would be used for what types of incidents) the added value of the service is problematic, especially considering the potential costs. .

The WG has been working under the assumption of the following use cases:
The use of the repository is limited to respond to incidents, defined as:
A. Large scale, unintended malfunction of the DNS or
B. Systematic, rigorous preparation of or actual attack on:

1. The availability of the DNS or registration systems
2. The data integrity or privacy of the DNS or registration systems
3. The stability or security of the Internet at large

Where a coordinated international response by operators and supporting organizations is advised.

Before moving forward, we would like to collect feedback from the community: ,

- Are the use cases listed above still appropriate and do they warrant a contact repository?
- If not appropriate, should the documented use cases be expanded? If you think so, are you willing to help out with drafting a few realistic use cases, preferably based on (anonymized) real-world incidents?

The WG also thinks that a contact repository as envisioned, only adds value, if the vast majority of at least the ccTLD community will subscribe to the service. Assuming the use cases are adequate, the WG would be interested to know if you will subscribe to the service, even when a subscription fee has to be paid.

The WG will be conducting a survey to seek your feed-back.

Background and Introduction

The ccNSO Contact Repository Implementation Working Group (CRI WG) was established in May 2011. Purpose of the CRI WG is to explore as a first step:

1. Explore in detail costs, and other relevant factors to implement, maintain and operate an incident repository as proposed by the Incident Response Planning Working Group and inform the ccTLD community and Council accordingly;
2. Explore different funding, management and governance models to implement, operate and maintain an Incident response repository as proposed, and report to the ccTLD community and Council a recommended and preferred option

According to its charter the WG should take into account and be guided by:

- The non-binding relationship of the ccTLD registries to any one particular entity except possibly with their own governments;
- Diversity of language, time zones, resources, expertise;
- Particular policies and practices by which ccTLDs may be guided.

The activities of the CRI WG are limited to and shall take into consideration the outcome and results of the work of the Incident Response Planning Working Group as proposed in their Final Report (http://cartagena39.icann.org/meetings/cartagena2010/presentation-ccnso-members-irwg-07dec10-en.pdf), in particular regarding:

- The definition of incident for the purpose of incident response
- The description of use cases of contact repository i.e. for what purposes can the repository be used:
    - Information exchange
    - Counter action
- The definition of contact repository data attributes
- The general criteria for implementation and maintenance of repository:
    - Support the envisioned use cases
    - High availability (24/7)
    - Alternative communication channels (not using the internet)
    - Actively maintain and keep data up-to-date

To date the WG has made progress, but to move forward the WG needs to understand whether the basic assumptions are still valid.
The basic assumptions are around:

- The use cases as defined
- Potential use of the Service
- The service concept, also in the context of potential costs

Use cases

The work of the CRI WG is based on and is guided by the results of the Incident Response WG[1], in particular the definition of the use cases and the definition of incidents. Accordingly the use of the repository is limited to respond to incidents, defined as:

A. Large scale, unintended malfunction of the DNS or

B. Systematic, rigorous preparation of or actual attack on:

4. The availability of the DNS or registration systems
5. The data integrity or privacy of the DNS or registration systems
6. The stability or security of the Internet at large

Where a coordinated international response by operators and supporting organizations is advised.

In case of incidents as defined above, the use of the repository is limited to:

1. Information exchange:
    a. Provide a security contact point under any circumstances.
    b. Generate best practice advisories on the prevention if DNS security incidents (technical, process related)

2. Counter action
    a. Inform the "participating community" about "an incident".
    b. Coordinate responses
    c. Facilitate/enable community support for a "community member".

Potential use of the service

In the view of the CRI WG the value of the repository system and therefore its successful implementation, depends on the value of the system for individual ccTLD operators. The value of the system depends on the following factors:

- Number of subscribed ccTLDs (there's a critical lower limit)
- Capacity of ccTLDs to appoint dedicated point of contact(s) (24X7)
- Capacity of individual ccTLD operators to take mitigating actions
- Cost of subscription

To date the WG has worked on the basic presumption that a vast majority of the ccTLD community, both in terms of absolute number of ccTLDs and weighed according to the total number of domain names under management, will subscribe to the service and maintain their contact details up-to-date. In other words: if the service is only provided to a limited number of ccTLDs or a limited number of ccTLDs with a large number of domain names under management, the value of the system as a whole for individual ccTLD operators who have subscribed is limited.

[1] The Incident Response WG was established in the aftermath of the Conficker incident in 2009. The Incident Response WG was established end 2009 at the time as the community felt a need to be able to coordinate actions and the need for a contact repository.

The WG is aware that the costs of implementation and maintenance of the system is a key factor for subscription. In the view of the WG the critical factor here is maintenance of the system. This is not limited to maintenance of the database as such. The main costs will be associated with maintaining the organization that operates the incident response and the need to keep the data attributes in the database accurate, confidential and available.

Based on some very preliminary research done by the previous WG, the potential costs categories are:

- Set-up fee (once off), either to build a new repository or to adjust existing system to the requirements defined. This depends on the preferred method of implementation (buy, make or use and adjust existing system)
- Maintenance fee (Annual Subscription). Depending on the adopted requirements (maintenance of contact details and organization, governance structures etc.)

The CRI WG considers the issues around the capacity of individual ccTLDs to appoint dedicated points of contact and to take mitigating actions out of its scope. However, it is the view of the WG that capacity issues need to be considered by the community.

Before taking any further steps, the CRI WG would like to understand if:

1. The use cases for the contact repository is still adequate, and creating a contact repository still has added value for the community at large;

2. A critical mass of the ccTLD operators is interested in subscribing to the Incident repository service, in particular in light of the potential expenditures associated with subscribing and maintaining the system.

We believe answering these questions is necessary because the WG was established two years ago and a lot has changed since, for instance because ccTLD registries have increasingly become high-value targets for cybercriminals[2]. In addition, the environment in which ccTLDs operate will soon change dramatically with the launch of the new gTLDs.

The CRI WG will conduct a survey to understand the interest in the service.

At the same time, the CRI WG will investigate alternatives, for example close collaboration with already well-established initiatives like DNS-OARC.

---

[2] Maarten Van Horenbeeck, "Update on DNS hijackings", ccNSO Tech Day, Durban, July 2013, http://durban47.icann.org/meetings/durban2013/presentation-dns-hijacking-horenbeeck-15jul13-en.pdf