Draft Proposals and Work plan Incident Response Planning Working Group.

This is a draft paper and is published by the Chair of the WG to inform the ccTLD community prior to the ICANN Seoul meeting of the progress made so far. Please note this document has not been signed-off by the Incident Response Planning Working Group. The members of the WG will continue to discuss the document into the Seoul meeting.

A. Introduction and Background

According to its charter the purpose of the Incident response planning working group (IRP WG) is to develop sustainable mechanisms for the engagement of and interaction with ccTLD registries during incidents that may impact the DNS.

In considering feasible methods the IR WG should take into account and be guided by:

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

The activities of the working group are limited to:

1. Defining the relevant elements of the following mechanisms:
   a. the timely development of a repository of ccTLD contacts responsible for incident handling and emergency response;
   b. the necessary primary and alternate channels of communication;
   c. the qualification of incidents and associated escalation procedures;
   d. the qualification and procedures for action paths
2. Identify the relevant parties to create sustainable mechanisms as identified
3. Identify the elements for sustainability.

B. Proposals and Work plan.

[1.a.] ccTLD Incident Handling Contact

(1) Mission

- Provide an effective emergency incident response to their ccTLD registry system and customers for computer security incidents that may impact the DNS or utilize the DNS to perform a malicious intent

(2) Objective

- Provide a reporting point for receipt of incident/threats reports and remediation information pertaining to DNS registration system.
- Provide technical support in response or conduct actual response to computer security incident and threats impacting the DNS.
- Ensure the security of the DNS registration infrastructure.
- Provide mechanisms for the synchronization and/or coordination of counter measures
- Provide mechanisms to conduct pro-active security and penetration testing on the ccTLDs?
- Provide an effective communication channel for the ccTLDs to inform and coordinate with other ccTLDs, gTLDS, and the DNS root manager on security incidents

- Provide a Common Incident Response Repository where handlers who had dealt with problems can add their experience and procedures used, so it may be useful in some other time when the same incident takes place. Because when critical incident's occurs time is of the essence and rapid response is required. This repository will reduce the response time and the system restoration time.

(3) ccTLD incident handling contact function definitions

- Receiving requests and reports
  - Provide 24/7 available contact point which can receive security incidents relating reports and requests in secure manner
- Triaging requests and reports
  - Sorting, categorizing and correlating threats to assess and prioritize the risk associated with threats
- Responding requests and reports
  - Taking action to protect systems affected or threatened by intruder activities
  - Providing solutions and mitigation strategies from relevant advisories or alerts
- Analyzing incidents/events

(4) Availability

- Handling contacts are registered to the repository of ccTLD contacts which is maintained by XXX (this could be regional ccTLD managers, ICANN GP, security team)
- Handling contact repository is accessible/available to Regional TLD association managers, ccTLDs, ICANN Global Liaisons /security team
- Registered Incident Handling Contacts (email address and emergent contact telephone number) are available 24x7 (??)

(5) Interactions and information Disclosure

- Information will be categorized as following

(6) Interfaces with other services

- ICANN Global collaborative Response
    - ICANN as facilitator of communication and information sharing with general DNS operational community when events that threaten systemic security stability and resiliency of the DNS occurs
- National CERTs?

(7) Priority

- Request comes from ccNSO incident contact point arrangement is recommended to put higher priority to response

[1.b] The necessary channels of communication

(1) Points of Contact

1. ccTLD name:
2. Name of person representing the team:
3. Host organization of ccTLD response contact point
4. Country the contact is located
5. Internet domain
6. Regular telephone number (country code, telephone number, time-zone relative to UTC):
7. Emergency telephone number (country code, telephone number, time-zone relative to UTC):
8. Email address:
9. Messenger services (service, id):
10. Facsimile number (country code, fax number):
11. Other telecommunication facilities:
12. Language:

(2) Availability of the defined of contact

[1.c] the qualification of incidents and associated escalation procedures

(1) Guidelines on the kind of events to report

Events that threaten systemic security, stability, and resiliency of the DNS

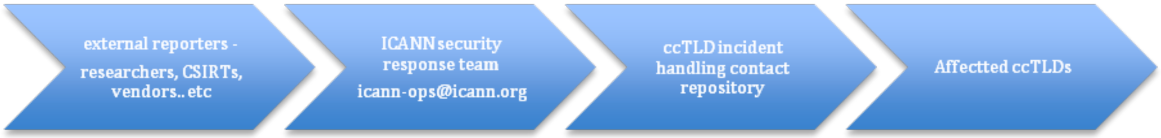
- Events and incidents where the DNS or registration services are exploited and/or misdirected on a large scale attacks where the name service or domain registration is used to facilitates attacks, or where the DNS infrastructure or registration services are the targets of malicious activity

Basic scenario examples;

- ○ Name service for very large population of Internet users are threatened (e.g., botnet activity) or adversely affected (e.g., Denial of service attacks)
- ○ The means of minimizing, reducing or mitigating the threat will require cooperation across multiple TLDs
- ○ A common form of attack is used to exploit domain registration services

[1.d] the qualification and procedures for action paths

(1) Procedures to follow for externally triggered events


external reporters -
researchers, CSIRTs, vendors.. etc
ICANN security response team
icann-ops@icann.org
ccTLD incident handling contact repository
Affectted ccTLDs

Incident Response Process v1.0

1. Incident occurs
2. Incident is reported to IR Team (E-mail, Fax, Phone call, SMS etc)
3. General questionnaire is filled upon receiving the incident
4. An entry is opened in the Incident tracker.
5. An incident handler is assigned
6. Repository is checked for previous incidents of similar nature. If a similar incident has occurred, adopt the procedures used in the previous incident.
7. IR team resource personnel are identified and an IR task force is compiled
8. A preliminary analysis is conducted
9. Obtain vital data of evidential value from the incident site.
10. Comprehensive analysis of the incident by the Task force
11. Relevant contacts are identified and they are updated regarding the incident.
12. Update the Incident tracker
13. Generate a report of the incident
14. Dispatch it to the IR Team
15. Close the case