DNS Security Survey for National Computer Security Incident Response Teams – December 2010

Summary

As referenced during the ICANN meeting in Brussels, Belgium in June 2010, ICANN developed a survey on DNS security response operations for national computer security incident response teams (CSIRTs). The survey was sent in August 2010 via the Computer Emergency Response Team Coordination Center at Carnegie Mellon University (CERT/CC) (distributed worldwide), the European Network and Information Security Agency (ENISA, covering the European region), APCERT (covering the Asia-Pacific region) and the Organization of Islamic Conference-CERT secretariat (OIC-CERT, covering Islamic countries) to 55 CSIRTs with national responsibility. Responses were received from 26 national CSIRTs.

The survey results are not comprehensive enough data to draw any broad conclusions. While there are over 246 ccTLDs and 22 gTLDs (not including newly delegated IDN ccTLDs), according to CERT/CC, there are a total of only 56 National CSIRTs from all regions (see http://www.cert.org/csirts/national/contact.html). Note – while this list of CSIRTs is complete to the best of CERT/CC's knowledge, it is not an authoritative number and does not cover all the National CSIRTs. Less than half of the CSIRTs in each region responded. Additionally, analysis has not been conducted on potential bias of those who did and did not respond to the survey.

Main Themes

1. There are clearly areas that specific CSIRTs identify gaps related to DNS operations and security operations.

2. Most of the survey respondents believe National CSIRTs work sufficiently as a means to reach DNS operators in another country when there is presence. However the sufficiency of this mechanism depends on the country and obviously the presence of a national CSIRT.

3. 17 of 26 respondents identify contact points database for response and information sharing/mechanism is needed to improve incident coordination on issues involving DNS at CSIRT community. 6 of 26 respondents identify coordination center is needed to improve incident coordination on issues involving DNS at CSIRT community.

4. Almost all the respondents who answered named WHOIS as the mechanism to identify outreach points of contact despite weaknesses in the accuracy of WHOIS data.

5. Two questions drew very consistent answers: Q2-1, where almost all National CSIRTs would like to receive information on trends in the use of DNS by attackers including new attack methodologies and how CSIRTs can best respond to them or advise their constituencies on the defense from them.

Additionally Q-4 shows only 15% of teams subscribed to any security/response mailing lists for DNS registries /

registrars' operators.

6. Those who do not subscribe to the DNS security relating mailing list look for following kinds of information -

DNS attack method trends,
Incident response techniques,
DNS spoofing issues,
New attack trend and methodologies of DNS related incidents and effective response methods,
Knowledge about new vulnerabilities,
Case studies,
Best practices

Detailed Data

What do you think the CSIRT community needs to improve incident coordination on issues involving DNS?

[Original Comments:]

Respondents from AP region

- Coordination centre, Contact point database, Information Sharing, and Incident Cases Sharing.
- Attacks, incidents and contact point database
- Information sharing related to concrete and actual way of response to contemporaneous incidents.
- Coordination work through issuance of advisories or alerts
- Knowledge about new attack techniques, new vulnerabilities, case studies, best practices
- A single and reliable interface for escalating incidents, discussions and information sharing. Initiatives like this already exist but probably not formalized and/or completed.

Respondents from Latin America and Caribbean region

- The real problem with taking down domains being used for criminal activities are the gTLDs' registrars and resellers that don't have policies and don't act on the problems. It is also hard to find contact information for abuse reports and most don't understand the problem – e.g. several times they don't have knowledge of local issues, like brands or other names used for fraud.
  If a central entity would be created it would be useful for helping CSIRTs to find the right contacts and help the registrars and resellers to prioritize which requests are more urgent and also identify if the organization complaining is really a CSIRT or a victim of a crime/abuse using a given domain name.
- Coordination centre, contact point database, technical knowledgment,
  etc.)
- Coordination Center

#

Respondents from Middle East and Africa region

- Share information and best practices
- To have a trusted central database for PoC
- Define a coordination framework to facilitate incident response.
- Sharing lessons learnt about incidents, publicize work below between different TLDs, joint projects and specialized trainings.

Respondents from Europe region

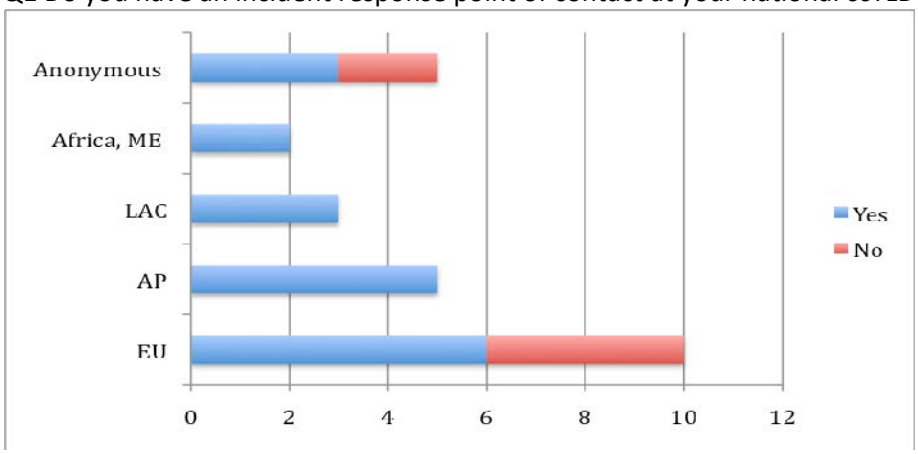
- DNS security is a serious issue, where several parties are involved (which is true for every internet related issue). There is no single DNS authority but merely a chain of services and capabilities offered to operate and safeguard name resolution services. In that respect it is early to propose a single DNS-CERT, since incident response is already handled by the different owners of systems. We support the increased attention for DNS Security and we are interested further advise in how this can be achieved best, knowing the existing expertise, ownership, relationships and capabilities.
- Establish good working contacts to key stake holders: Registries, Policy makers, --In many (European) countries the Domain business is regulated by the government. For .ch we talked for more than a year with the respective authorities to changes the laws, so we could actually react to misuse and still respect the Swiss legal system. At the end few changes hat a big impact in misuse patterns, the time speaking to the authorities are was well spent. I can elaborate on this if needed.
- A contact point DB would be lovely. Moreover, we need someone to raise the awareness level of ccTLDs about security and abuse issues.
- Information sharing between response teams, Incident coordination center to improve the handling effort on a given incident, Push for implementing security measures and standard baseline for all registrars.
- CSIRT teams efficiently cooperate with each other and provide response to all kinds of incidents. Some countries might need to strengthen cooperation with their ccTLD on the national level,
- Probably an international coordination centre and single contact point in each country
- Detailed (technical) publicly available information
- I think that would be useful a coordination center, mainly based in provide correct contacts points and also providing guides, manuals, etc. related to DNS security and incident handling.
- Another goal should be interchange information between different ccTLD and CSIRTs with their experience. Also if possible share information how-to mitigate real attacks and how they handled incidents involving.
- I think there is no crucial need for a separate coordination infrastructure for DNS incident response from CSIRT's point of view. I expect there are operational means of communication between registries and the question should be rather addressed to them.
- ICANN should seek to facilitate needs of existing CSIRTs and possibly implement safeguards that would minimize emergence of fast-flux and similar problems.

#

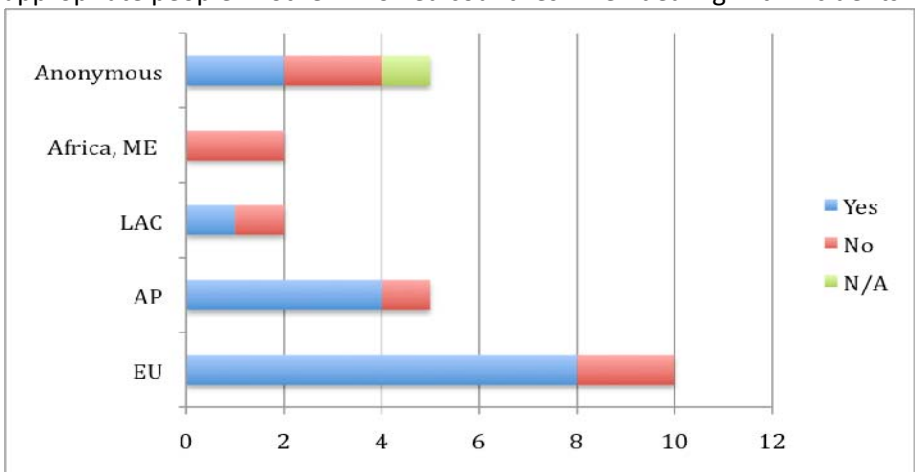
Anonymous

- Contact list, information sharing, new vulnerabilities reports
- A reliable and current contact database regarding all ccTLD and major DNS product and related infrastructures. A center-of-excellence for accumulated knowledge may also be useful.
- Contact point database
- Point of Contact, Referral Centre for DNS

Q1 Do you have an incident response point of contact at your national ccTLD?

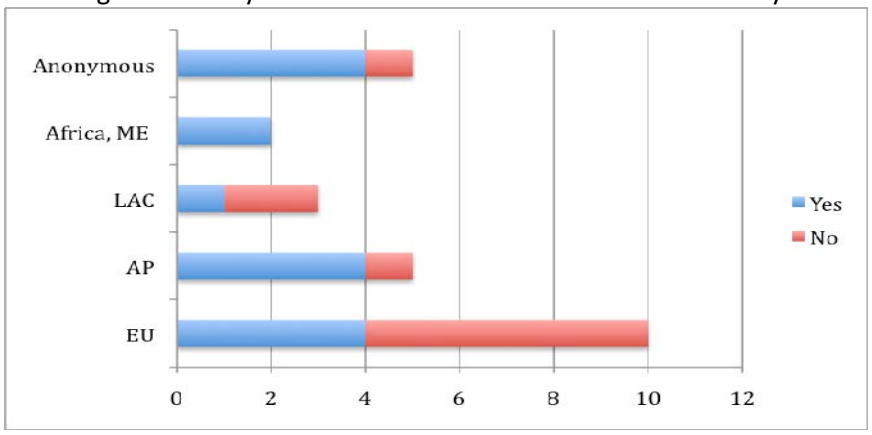


Q1-1 Do you think that you have sufficient contacts in the National CSIRT or ccTLD registries to reach the appropriate people in other involved countries when dealing with incidents involving DNS?

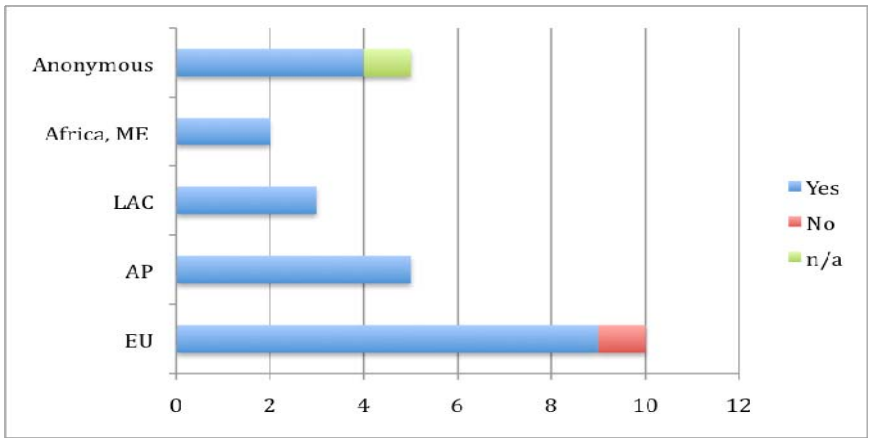


#

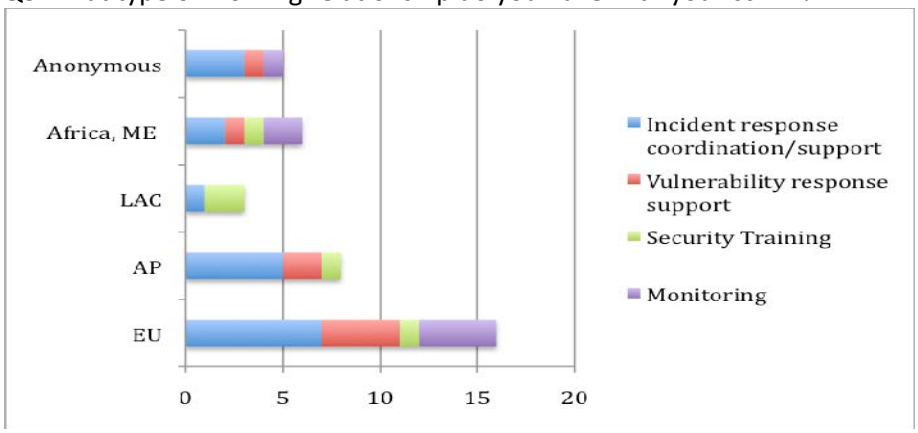
Q2 Do you need more DNS technical expertise to provide support for DNS related incident handling including work with your ccTLD and others in the DNS community?



Q2-1 Would it be helpful to receive information on trends in the use of DNS by attackers including new attack methodologies and how CSIRTs can best respond to them or advise their constituencies on the defense from them?

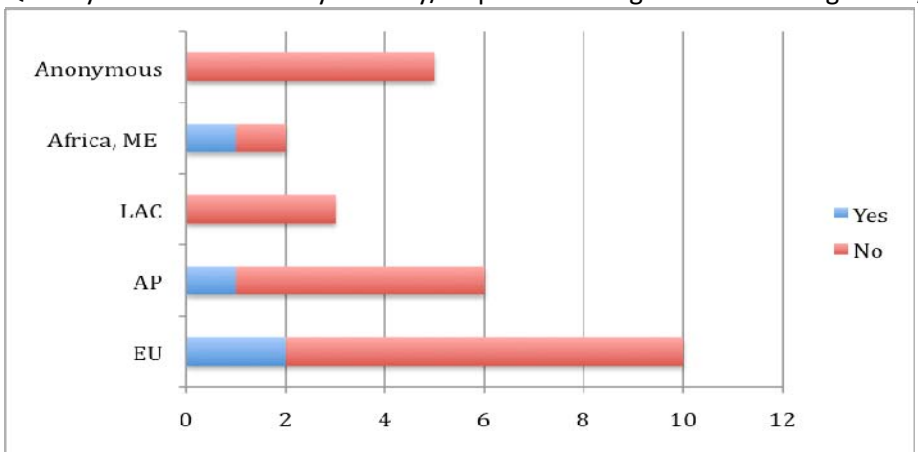


Q3 What type of working relationship do you have with your ccTLD?

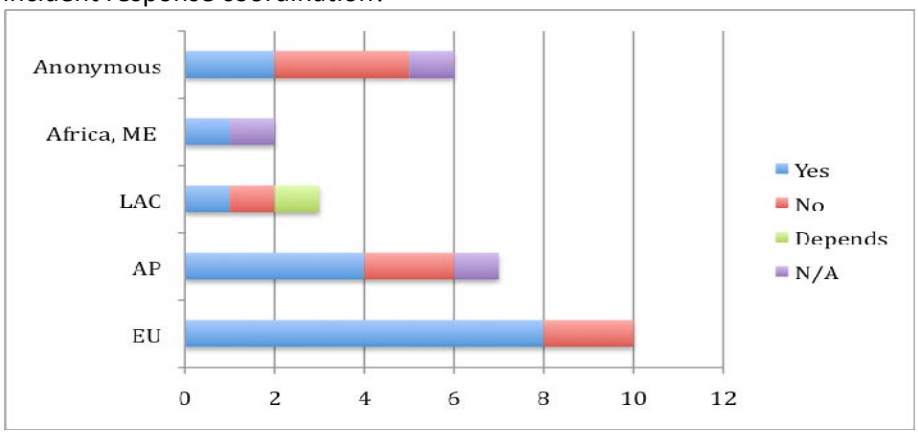


#

Q4 Do you subscribe to any security/response mailing lists for DNS registries / registrars operators?



Q5 Do you have a mechanism to identify contact point at registry/registrar for malicious domain incident response coordination?



Appendix A

#

	National CSIRT Survey on DNS Security	
Your Name		
Affiliation		
1.	Do you have an incident response point of contact at your national ccTLD?	Yes No
1-1.	Do you think that you have sufficient contacts in the National CSIRT or ccTLD registries to reach the appropriate people in other involved countries when dealing with incidents involving DNS?	Yes No (Comments)
2.	Do you need more DNS technical expertise to provide support for DNS related incident handling including work with your ccTLD and others in the DNS community?	Yes No
	If yes, please check which of following expertise sets you think are useful. (Check all that apply)	( ) DNS protocol expertise ( ) DNS root or TLD operations ( ) DNS server software expertise ( ) DNS resolver software expertise ( ) Other questions involving DNS when handling incidents
2-1.	Would it be helpful to receive information on trends in the use of DNS by attackers including new attack methodologies and how CSIRTs can best respond to them or advise their constituencies on the defense from them?	Yes No
3.	What type of working relationship do you have with your ccTLD?	( ) Incident response coordination/support ( ) Vulnerability response support ( ) Security Training ( ) Monitoring ( ) Others (free form) [ ]

#

4.	Do you subscribe to any security/response mailing lists for DNS registries / registrars operators?	Yes - Please specify [ ] No
	If yes, do these lists meet your needs from an incident response perspective?	Yes No
	If not, what kind of information do you need?	- Information you need [ ]
5.	Do you have a mechanism to identify contact point at registry/registrar for malicious domain incident response coordination?	Yes - Please specify [ ] No
6.	What do you think the CSIRT community needs to improve incident coordination on issues involving DNS?	Free form: (e.g. coordination centre, contact point database, etc.) [ ]