Centr

Report
meeting on

EU - US Cooperation
against
Cyber Crime

Brussels, Belgium,
February 24 - 25, 2011

Prepared by
Wim Degezelle and Peter Van Roste

Context

The EU-US bilateral summits have recently addressed the global fight against cybercrime and identified it as one of the priorities.

DG Home was tasked to study the issue and propose mechanisms that would help LE agencies on both sides of the Atlantic to quicker respond to online fraud and criminal activities.

This is not only targeted at child protection, but includes the fight against online distribution of (prescription) drugs, pharming or phishing.

In this context, the LE community drafted the LE recommendations for changes to the Registrar Accreditation Agreement. They hope that this would avoid the many dead-ends that they encounter when trying to identify suspects of online criminal activity.

These recommendations have been endorsed by the GAC (ICANN Brussels[1]), but have still not been accepted by the registrar community.

This meeting is the second joint meeting to try to get buy-in from the registrars.

At the beginning of the meeting registrars noted that although input was given on several occasions, none of the suggestions from the registrar community had been included in the document.

Summary

Main topics discussed:
- The LE recommendations were discussed in detail:
    - Registrars should provide more info about themselves (structure, ownership, resellers owned, CEO, address, …)
    - Registrars should improve data accuracy in whois
    - Registrars should keep detailed info from registration process (email confirmations etc.) for future reference
    - Proxy registrations: LE wants to minimize the use of proxy services and only allow accredited proxy services. Significant disagreement in the room.

- Discussions on "who is law enforcement?"
    - Can we create lists of all LE's? An experiment will be launched on CECILE – the EU Commission's exchange platform
    - Can we have a center that confirms the legitimacy of a LE agent? No, INTERPOL was suggested but it has a very limited potential (e.g. prosecutors or tax authorities would not be identified by them)

- Case studies from PIR (including a clear call for the possibility for anonymity for civil rights groups), GoDaddy (online Pharmaceuticals)

- What are the mechanisms that should be used to make these changes? What is ICANN's role?
    - A change to the RAA seems the most direct way to handle these recommendations
    - This would most likely require a full PDP
    - Attendants were doubtful that a PDP is the best instrument, but nobody could come up with a realistic alternative

- RIR section
    - The American (ARIN) and European (RIPE) IP organizations gave presentations on their fraud investigation

---

[1] http://brussels38.icann.org/meetings/brussels2010/presentation-gac-raa-19jun10-en.pdf

- o Not that much interest for the RIR presentations, some even wondered why they were invited to present at the meeting
- o More interest for a presentation by the Belgian cybercrime unit warning for interim solutions during the IPv4-IPv6 transition that make it impossible for LEA's to trace eg posts, messages, … back to the author's IP address

What does this mean for ccTLDs?

Nigel Roberts (.gg), Eberhard Lisse (.na), Eleanor Bradley (.uk) and Peter Vergote (.be) presented the ccTLD's approach to these issues.
The presentations (which will be made available on the CENTR website) demonstrated clearly the difference between ccTLDs and gTLDs and highlighted the practical and constructive approach taken by ccTLDs.

While in the short term this discussion has almost no relevance for ccTLDs, it could trigger some changes in the way ccTLDs work with registrars or how registrars work with their resellers in the future. Some proposed changes to the RAA (I.e. if the concept of accredited proxy servers gets accepted) could have an indirect impact on ccTLDs as it might lead to (voluntarily) reconsider current practices.

Conclusions*:

(*These conclusions were drawn up by the FBI, it is unlikely they changed anything to the lack of support the recommendations have from the registrar community.)
Short term:
 Registrars and law enforcement look favorably on establishing the following:
 Centralized list of LE agencies and exchange of contact information
 Registrars publish physical address
 Registrars publish list of senior officers
 Registrars identify parent companies
 Registrar be legal entity in country where formed
Medium term:
 Enhanced due diligence for accreditation of registrars

No agreement on:
 Proxy services

Next steps:

A GAC representative suggested bringing some of these topics to the table at the GAC/Board meeting on Feb. 28/March 1 in Brussels:

- - How can these recommendations be included in the current RAA?
- - Should there be more money and resources be made available at ICANN for the contractual compliance team?