LACRALO'S MONTHLY CAPACITY BUILDING

19/04/2012

Fake Renewals – Mike O'Connor

Member of the GNSO's ISPCP Constituency. Previously he was a member of the Commercial and Business Constituency, where he was a member of the Credentials Committee.[3] His primary focus is on GNSO (and cross-constituency) Working Groups that deal with the security and stability of the DNS, including the following: Fake Renewal Notices (FRN) (chair)

Source: ICANN Wiki

http://icannwiki.com/index.php/Mike_O%27Connor

LACRALO's MONTHLY CAPACITY BUILDING

FAKE RENEWALS – MIKE O'CONNOR

On 25 September 2008, the GNSO Council adopted a motion requesting an issues report on registration abuse provisions in Rregistry-Registrar Agreements. The issues report was submitted to the GNSO Council on 29 October 2008 and provides an overview of existing provisions in Registry-Registrar agreements relating to abuse and includes a number of recommended next steps. In December 2009, the GNSO Council agreed to charter a Working Group to investigate the open issues identified in Registration Abuse Policies report, before deciding on whether or not to initiate a Policy Development Process (PDP). A Registration Abuse Policies Working Group (RAPWG) was chartered in February 2009. This Working Group made several recommendations and one of them was related to Fake Renewals Notices.

In order to help inform its deliberations on this recommendation, the GNSO Council requested that a small group of volunteers prepare a request for information concerning Fake Renewal Notices for the Registrar Stakeholder Group. In order to see if this is a problem that worth the time to conduct a PDP, very long, time and resource consuming project for the GNSO. Before launching the PDP, the Council wanted to see if there is a problem serious enough that granted the work.

They surveyed the community of registrars to see what their evaluation was. It was not a unanimous conclusion but *Network Solutions* and *GoDaddy* among others thought that this was a problem and granted a further work. Apparently, this problem is steady and is not growing.

In the case of registrars they only see one source of these notices. All 3 of those come from the same Registrar. They take different forms, different languages. The accredited Registrar from which all is originated in these examples is the same one. In the Business Constituency, the large businesses are seeing more than one source. Specially focus on stealing domain names, stealing credentials.

Fake renewal notices are misleading correspondence sent to registrants from an individual or organization claiming to be or to represent the current registrar. These are sent for a variety of deceptive purposes. The desired action as a result of the deceptive notification is: Pay an unnecessary fee (fraud), Get a registrant to switch registrars unnecessarily "slamming" or illegitimate market-based switching, Reveal credentials or provide authorization codes to facilitate theft of the domain.

Example: A marketing company that's saying that is time to send in your registration for your domain name. This company "Domain Registration Services" is a search engine ranking and submission service provider.

The registrants are paying something they not need at all. The major concern is that the registrants switch unnecessarily from one Registrar to another.

They are not the Registrar with whom you have registered your domain name they are asking you to register for their services and fool you into moving you domain name from your current Registrar to their service. It is not a renewal notice but it is really an offer of services. The unsuspecting

consumer is fooled into changing service provider when they didn't intend to or didn't want to.

Another example: In this case the wording is more complicated. The confusing language would make unsuspecting consumer change their registration when in fact they do not necessarily want to. It is a very complicated language sort of intimidating: "*Failure to complete your domain name search engine registration by the expiration date may result in cancellation of this offer making it difficult for your customers to locate you on the web*". The intention here is to fool the customer into doing something they not necessarily and probably don't need to do.

The drafting team recommends that the GNSO Council put this report out for public comment in order to **obtain community input** on the findings and potential next steps

In the US they used to have this problem in the long distance and cell phone industry. People switched providers unnecessarily. The Business Constituency is concerned that sometimes this scam are used to reveal credentials or allow a domain name to be stolen. All of these are the harm that can come from fake renewal notices.

There's enough impact to cause concern and it needs further work, it is a real problem the need more work. The Drafting team draft conclusions. Developed and suggested some options for the GNSO to consider as potential next steps:

- Add a section to the RAA (Registrar Accreditation Agreement) that addresses Business Practices
- Add the issue to an Inter-Registrar Transfer Policy (IRTP) PDP to the upcoming PDP on the RAA
- Refer the issue to the At-Large Advisory Committee (ALAC) to encourage better education and awareness of this type of abuse amongst the end-user community
- Raise this issue with the Federal Trade Commission (FTC) in the United States to see if the registrar is in compliance with relevant law
- Initiate a PDP (Policy Development Process) on Fake Renewal Notices
- Do not proceed with any action at this time

The survey was addressed only to Registrars not to commercial users, Registry or users out of the GNSO.

Q & A:

Why raising the issue with the Federal Trade Commission?	ICANN is headquartered and is incorporated in USA, that's why the idea of raising the issue to the Federal Trade Commission.
As end-users, how can we identify the fake renewals notices? Where can we go for help?	The best defense is a good awareness, good education and training. The more people can share examples with colleagues and educate themselves the more we are going to be able to do this. It is very useful to make translations with comments explaining what they are, so that people can find information and understand. The more people know about it and differentiate legitimate requests made by legitimate registrar from illegitimate, would carry out best actions when these emails arrive.

Where in ICANN can we denounce these practices or request for information?	The place in ICANN to denounce these practices is the Compliance Department. However, the current contract's form of wording does not provide tools to seek out people who issue these false reports. The Department has no mechanism to do something about it. It's a good idea that registrars provide information explaining as clearly as possible how to differentiate a legitimate mail sent by a registrar. Encourage them to describe the notice's features that they send.

Important actions

- End-user education
- Clear information about legitimate renewal notices
- Fake renewal notices translation and diffusion.

References:

Teleconference WIKI LACRALO 19.04.2012

https://community.icann.org/display/LACRALO/LACRALO++19.04.2012+Teleconference

Report

http://www.icann.org/en/news/public-comment/fake-renewal-notices-report-21mar12-en.htm

Presentation

https://community.icann.org/download/attachments/30346437/FRN+-+Briefing+Deck.pdf?version=1&modificationDate=1334588239106

Acronym's Índex
GNSO: Generic Names Supporting Organization
ALAC: At-Large Advisory Committee
PDP: Policy Development Process