ICANN Identifier System SSR Update – 2H 2014

A dramatic uptick in capability building, ongoing support of trust communities via ICANN's threat intelligence channels, and increased global stakeholder engagement highlight the Identifier Systems Security, Stability and Resiliency (IS SSR) Update for the second half of 2014 (2H 2014).

Sustaining and Expanding Collaboration Opportunities for ICANN

Our team lends its competencies in information security, cybersecurity, Internet, and DNS operations to a global community of diverse stakeholders. Recognition of these competencies and our consistent demonstration of trustworthiness form the bases for *trust-based collaboration* – multi-party, multi-stakeholder efforts mitigate abuse or misuse of the Internet in general and the Internet Identifier systems, specifically. By lending time and talent, we earn trust for ICANN among organizations that are not part of the ICANN community and from this trust, encourage them to participate in ICANN's multi-stakeholder consensus policy development.

Capability building reaches five regions

The capability building our team delivers is typically a half-, full, or multi-day training program with live demonstrations of techniques and hands-on learning opportunities. In 2H 2014, the team provided thirty-seven (37) on-site or remotely delivered training programs in five regions (NA, LAC, EU, AF, AP). Of these, six were delivered in Spanish, and 29 in English.

The most popular training delivered in 2H 2014 was our DNS abuse/misuse program (23 deliveries). We were able to satisfy numerous requests in 2H 2014 from South America and Asia Pacific regions following "train the trainer" efforts in April in the US and in Asia Pacific in July. The current queue of requests for 2015 suggests that interest in these programs will sustain at this rate.

Requests for DNSSEC training remain strong (12). In 2014, ad, au, aw, es, gd, hr, id, ie, ke, no, pe, sj, tn, and vu signed their zones.

Strengthening Relationships

Our team took advantage of its membership in M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group and began to work more closely with global email and Internet service providers. ICANN greatly benefitted from these relationships when the company fell victim to a series of phishing attacks: the many offers for assistance to mitigate and investigate these attacks illustrates that trust-based collaboration benefits organizations in many ways.

We continued to grow our relationship with the Anti-Phishing Working Group (APWG) in 2h 2014 by sponsoring the eCrime Symposium Conference in Birmingham, AL. We are taking advantage of the eCrime eXchange cybercrime event data we can now access via our APWG membership. We have included the feed in our analytics activities and we collaborate regularly with APWG on ways to make this event data useful and relevant to the DNS community.

Reinforcing ICANN Relationships

Security team staff continue to use the persistent interest in cybersecurity as segue to promote ICANN and multi-stakeholder approaches to governance when we present or train through engagements arranged by GSE and through engagements resulting from our own relationships (CCI, network operations groups, ccTLDs, RIRs). The team satisfied 62 engagement requests in 2H 2014 including sessions at ICANN or regional workshops. Of these, thirty-two were collaborations with governance, ministerial, policy, or cybersecurity communities and 17 of these collaborations were coordinated or jointly attended with GSE staff and three were arranged by ICANN's speaker bureau. Noteworthy among these activities are:

- Invited participation at the Munich Security Conference (Germany)
- Invited presentations at the NASK Internet Policy Conference (Poland)
- Invited presentations at the American University of Science and Technology in Beirut and the Lebanese Internet Center (Lebanon)
- iLAC Roadshow (Bolivia)
- DNS Forum (Turkey)
- National Conference on Cybersecurity (Sri Lanka)
- Cybersecurity Event, meetings with Bulgarian Deputy Ministers of

Communications, Interior (Bulgaria)
- Invited presentations at the International Security and Diplomacy in Cyberspace Workshop, meetings with Bolivian Vice Minister of ICT and Telecommunications regulatory authority (Colombia and Bolivia)
- PACNOG Conference (New Zealand)
- APriIGF, APRIGF (India)
- Indonesia Stakeholder Engagements (Indonesia)
- NCFTA (USA)
- LACTLD Technical Training (Brazil)
- Diplo Summer School Program (Serbia)
- Monterey Cyber Security Initiative
- Investigating DNS Workshop (Romania)

APJII
Asosiasi Penyelenggara Jasa Internet Indonesia
INDONESIA NETWORK INFORMATION CENTRE
OPEN POLICY MEETING
(IDNIC - OPM)
The Ritz Carlton Hotel Mega Kuningan - Jakarta, 18 Desember 2014
APJII Services:
IIX
NETID

Trust Communities Increase and Expand Threat Intelligence Reporting

We continued to assist with or facilitate introduction to appropriate parties (internal or external) on a wide set of awareness reporting and response activities in 2H 2014. We resolved 18 of 18 inquiries or requests for assistance, including:

- Inquiries related to alleged 2013 RAA violations or other policy matters, where the public safety community needs assistance with submission processing, explanations of policy, etc.
- Requests for technical assistance, coordination with ICANN contracted parties or assistance with obtaining ERSR waivers needed for global botnet disruption actions. We identify points of contacts, the terminology that most accurately describes the action to a registry or registrar operator, and explain how to prepare lists of Internet identifiers so that orders may be executed expediently.
- Assistance with mitigation of malicious registrations, where the public safety community seeks assistance in communicating the gravity of a criminal enterprise to a registrar so that the registrar may take voluntarily action.
- Response to threats to the DNS, where we assisted with coordinating mitigation or containment of distributed denials of service attacks (DDoS), or provided DDoS protection or mitigation subject matter expertise.

In these cases, the Identifier System SSR Team considers the request and discusses the report with ICANN staff (e.g., Compliance). We assist by verifying information, or by validating the reporter’s credentials. The outcomes are typically positive. The public safety community values opportunities to better understand why an initial response resulted in a different outcome than they sought, and are typically satisfied whether they are given a clearer explanation of policy, or a better understanding of what they need to do or provide to obtain what they consider a positive outcome.

Analytics Projects

In our previous activities report, we identified two studies:

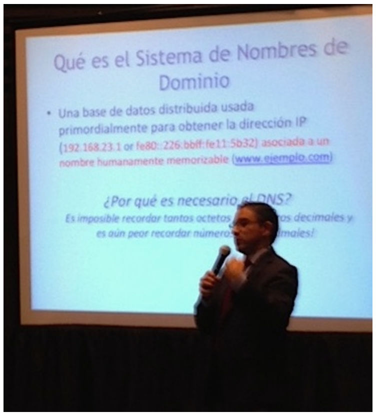
- *A study into the domain registration protection practices of selected vertical industries, to understand how registrants manage domain portfolios and whether they apply best practices for protecting registrations against hijacking or other registration service threats*. This study is complete and the report is under review. As the report reveals behaviors that could be exploited by malicious actors, we will deliver the work product to a representative agency of the industry we studied in confidence.
- *A monitoring and reporting program to detect and pursue potential violations of the 2013 or 2009 Registrar Accreditation Agreement, registrar involvement in malicious activity, or attacks against ICANN*. We continue to work on this program in cooperation with ICANN Compliance.

With one project near completion, we have begun experimenting with ways to apply the APWG eCrime eXchange cybercrime event data in a meaningful way for the ICANN community; in particular, we are studying how we may illustrate the misuse of new TLD domains for phishing URL domains.

Program for GSE-ISSSR engagement tracking

With the deployment of our engagement tracking software, the IS SSR team has been able to work with GSE (Global Stakeholder Engagements) to facilitate relevant training and engagement with sufficient lead-time to provide proper planning and cost-efficient travel.

Early planning and collaboration with GSE also increased our ability to engage in “events of opportunity”, where we work with the ICANN Regional VPs to engage with other individuals, events or governments while we’re on the ground and in country or region.



Qué es el Sistema de Nombres de Dominio

- Una base de datos distribuida usada primordialmente para obtener la dirección IP (192.168.23.1 or fe80::226:bbff:fe11:5b32) asociada a un nombre humanamente memorizable (www.ejemplo.com)

¿Por qué es necesario el DNS?

Es imposible recordar tantos octetos [illegible]os decimales y es aún peor recordar números [illegible]males!

Careful planning has allowed us to maximize the bandwidth of our small team: we increase our engagements with ICANN communities or stakeholders with a modest increase in travel time or expense.

Because of our active use of the tracking system, IT Operations has asked that we be one of the first groups to utilize the new ticketing system that is being rolled out in 2015. This inter-departmental collaboration will allow IS SSR to learn and push the new system while providing relevant feedback to IT Operations for a smoother organizational deployment.

Remote Delivery

We delivered nine webinars as part of our experimentation with remote delivery and experimented with one remote broadcast of a live training session. The webinars covered *DNS basics* and were well attended. The broadcast of live training exposed some challenges; for example, we were reminded that bandwidth constraints can impact not only recipients of a live streaming event but affect local presentation as well, and that hands-on training as we deliver is difficult without the ability to remotely connect to a student's computer (which itself is problematic for certain organizations that request training).

We will continue to investigate the viability of offering training in a remote environment. Through valuable communications with the ICANN Online Learning Team, IS SSR has a stronger understanding of the strengths and weaknesses of online learning (in general) and the platform that ICANN uses. Having collected this data, the IS SSR team has decided to develop and deploy a "trial" course for 2015. This course, entitled *Understanding DNS*, will act as a foundational element in our engagements and trainings, as well as a stand-alone remote learning mechanism that GSE and others can offer to their community.

Online Learning is just one piece of the overall remote engagement puzzle though. IS SSR has also delivered a number of remote trainings through the tools that IT has offered. These remote trainings have been valuable, as we are able to offer a sub-set of our training curriculum remotely. We are exploring ways in which to enhance this.