ICANN Identifier System SSR (IS-SSR) Update – 2H 2015

The second half of 2015 (2H 2015) was a period of exploration, growth and change. The IS-SSR Team's capability building and global stakeholder engagement grew in several dimensions. We continued to investigate DNS abuse or misuse. We developed proofs-of-concept for identifying abuse registrations in the new TLD program. We introduced security and technology awareness raising programs and delivered these to ICANN staff, ICANN community and the Internet at large. The IS-SSR Team began reporting to the Office of the Chief Technology Officer (OCTO) and team members began close collaboration with a newly formed research team focused on the Internet's Identifier Systems and related technologies.

Sustaining and Expanding Collaboration Opportunities for ICANN

In 2H 2015, our team continued to lend competencies in information security, cybersecurity, Internet, and DNS operations. By lending time and talent, we earn trust for ICANN among organizations that are not part of the ICANN community. We encourage them to participate in ICANN's multi-stakeholder consensus policy development. IS-SSR team-led training and in country engagements provide much-needed cybersecurity and operations capacities for these communities and provide welcomed, additional technically competent participation for the ICANN community.

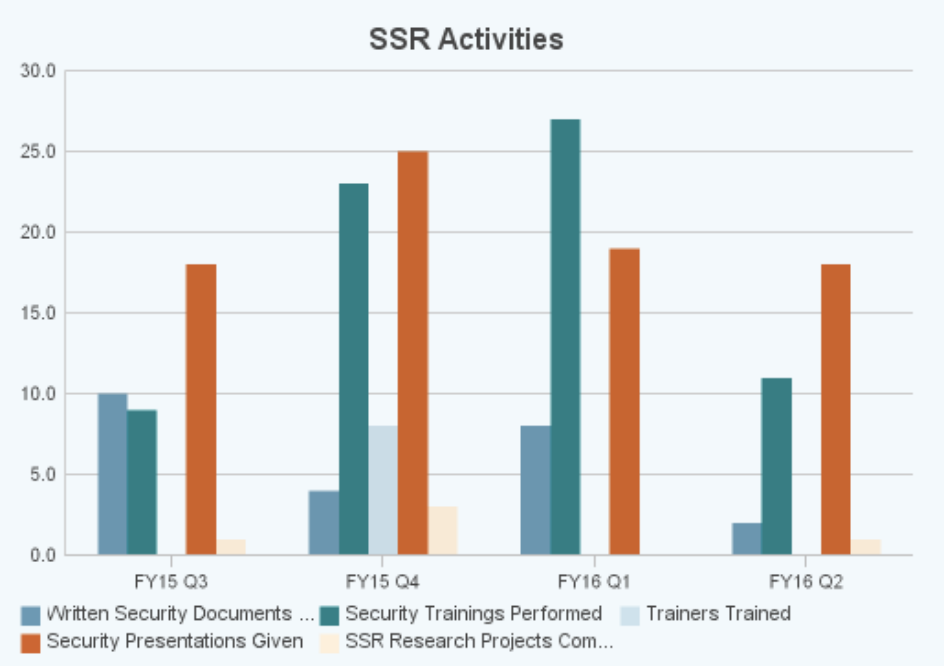


Figure 1. Composite of SSR Team Activities, FY15Q3-FY16Q2
(Source: ICANN BETA KPI Dashboard, December 2015)

The SSR Team's 2H 2015 activities correspond to those identified in Figure 1 from FY16Q1-FY16Q2. Table 1 shows all 2015 activities by Quarter:

SSR	Q1	Q2	Q3	Q4	
Written Security Documents Published (Published articles, ICANN blogs, technical reports)	10	4	8	2	24
Security Trainings Delivered by SSR Team (See capability building, below)	9	23	27	11	70
Security Engagements Delivered	18	25	19	18	79
SSR Research Projects Completed	1	3	0	1	5
SSR Research Projects In Progress					2

Capability Building Reaches Five Regions – Again!

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 2015, the team provided thirty-eight (38) on-site or remotely delivered training programs in five regions (NA, LAC, EU, ME, AP).

Training Trainers

Based on the success of the Train-the-Trainer course conducted in Dubai last year, we will be conducting another course in the second half of 2016. This course will be held for the Asia/Pacific region and will be comprised of 10-15 professionals with a special focus on getting more involved from the pacific islands. Due to flights and location diversity, training in the Pacific Islands has always been one of our most expensive target areas. As before, the training will focus on instructor techniques as well as providing course material that is relevant to the ICANN mission. By having trained professionals in the region, SSR hopes to reduce our own resource allocation and expenses over time by maximizing the expertise in region.

We conducted a Train-the-Trainer workshop for the Centre for Development of Advanced Computing (C-DAC) in India. Twenty (20) representatives from various key institutions participated, including the Department of Electronics and Information Technology (DeitY), the National Internet eXchange of India (NIXI), Education and Research Network (ERNET), the Indian Space Research Organization (ISRO), ISRO Satellite Centre (ISAC), and the Indian Institute of Science (IISc) .

Late in 2H 2015, we met to discuss opportunities for CERT-UK to deliver DNS investigations training to law enforcement in the UK. We will begin training at CERT-UK in January 2016 and CERT-UK trainer candidates will accompany ICANN staff to train at a UK event in March.

Strengthening Relationships with Security Communities

In 2H 2014, our team strengthened its relationship with M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group and began to work more closely with global email and Internet service providers. Our expanded involvement in M3AAWG provides an important ICANN policy resource to that community. We solidified our relationship with the Anti-Phishing Working Group (APWG) and now have steering committee responsibilities for both the APWG and APWG EU. As part of our steering committee remit, we have become more involved with the STOP.THINK.CONNECT. program and in collaboration with ICANN's Communications team, we launched an educational series, Raising Security Awareness, One Definition at a time. We also worked with APWG to improve and expand participation in the APWG Accelerated Malicious Domain Suspension Program (AMDoS). We established new working relationships with the Geneva Centre for Security Policy (GCSP) and sustained relationships with the Oxford Martin Global Cyber Security Capacity Centre (GCSCC), DNS-OARC, OAS, Interpol, Europol, Asia Pacific Telecommunity Cyber Security Forum (APT-CSF), Asia Pacific Computer Emergency Response Team (APCERT) Asia Pacific Financial Coalition Against Child Pornography (APAC-FCACP), and the Organization for the Security and Co-operation in Europe (OSCE) and the South School on Internet Governance.

Working with Global Stakeholder Engagements

The Security team continues to promote multi-stakeholder approaches to governance when we present or train through engagements arranged by GSE and through engagements resulting from our own relationships. The team satisfied thirty-seven (37) engagement requests in 2H 2015.

Noteworthy among these activities were:

- OAS Cyber Conference, Washington DC US
- NCFTA Slam Spam V, Pittsburgh, PA US
- Cyber Security Capacity Centre, Oxford, UK
- Cyber Security Workshops, NTRA and CERT EG, Egypt
- National ICT Conference, Zabljak Montenegro
- DNS/DNSSEC Hands-on training, Johannesburg South Africa
- Direct engineering assistance to .TR, .CR and .AR, Buenos Aires AR
  International Conference on Information Security (ICIS-2015), KR
- Centre for Development of Advanced Computing (CDAC), IN
- Network Security Workshop in collaboration with WorldBank & APNIC, MM
- Asia Pacific Computer Emergency Response Team (APCERT) Conference, MY
- South School on Internet Governance, San José, Costa Rica
- Security Analysts Summit Latin America, Santiago, Chile
- DNS Abuse training to cyber crime police units in Chile, Colombia, Costa Rica, Argentina and Spain

We continue to engage with ICANN's Global Stakeholder Engagement (GSE) team on a regular basis, including regular calls between SSR and GSE. These calls ensure that both teams have a better understanding of what's upcoming in a region, as well as work out any communication or logistic issues that may arise. SSR also regularly attends the GSE retreats which are typically held before each ICANN meeting. This, too, is to build on and strengthen our existing relationship between SSR and GSE. In 2016, SSR will also be moving away from our current ticketing system and migrate to the same management system that GSE uses. By doing this, we expect that this will increase our transparency and collaboration, not only with GSE, but with other teams within ICANN as well.

Increased and Expanded Threat Intelligence Reporting and Response

We continue to assist with cyber incident requests. Following a multi-party investigation of attacks against ccTLD authoritative name servers (ICANN, NSRC, and MarkMonitor), the SSR Team gathered input from investigating parties and published a Top Level Domain Incident Response "Recovery Checklist" and presented this during the ICANN Dublin CCNSO Tech Day. The SSR Team is also using the lessons learned and documented in the Recovery Checklist as a basis for a secure registry operations hands-on training course we will trial in 1Q 2016.

In these cases, our team considers the request and where appropriate, discusses the report with ICANN staff. We assist by verifying information, or by validating the reporter's credentials. Some of these requests for assistance are fairly mundane, i.e., inquiries seeking a clarification on policy, technical assistance, or an introduction to a point of contact. Others can be quite complex and involve cooperation from both the gTLD and ccTLD registry operators as well as private and public sector actors. The coordination role our team performs obliges us to assist regularly for several months.

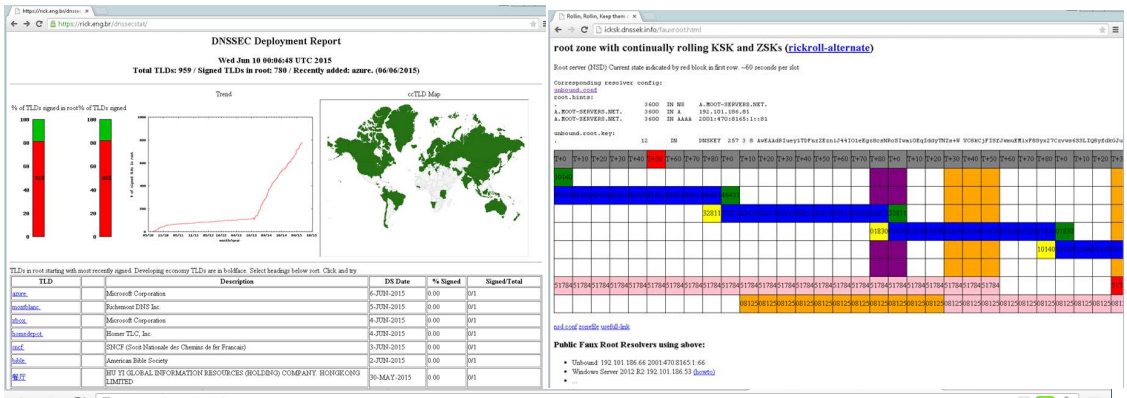
The outcomes remain encouragingly positive. The public safety community values opportunities to better understand why an initial response resulted in a different outcome than they sought, and are typically satisfied whether they are given a clearer explanation of policy, or a better understanding of what they need to do or provide to obtain what they consider a positive outcome.

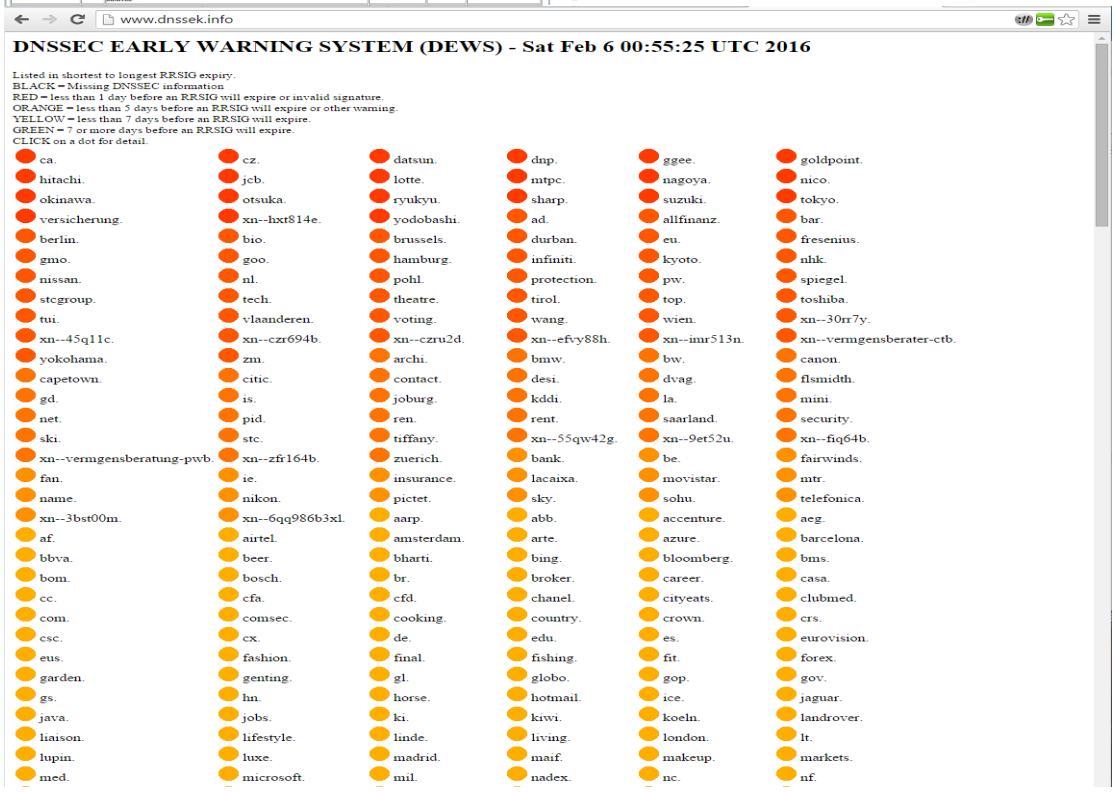
Analytics Projects

We expanded our proof-of-concept software activities in 2H 2015 to take advantage of publicly available cybercrime event data as well as event data feeds that security community members provided to our team for research purposes (This is yet another benefit ICANN derives from trust-based collaboration). We developed a proof-of-concept monitoring software to obtain lists and counts of spam domains delegated from the new top-level domains and companion software to identify the sponsoring registrars of those domains. We continue to investigate ways to migrate

the software to a supported platform for wider internal consumption and to improve automation.

ICANN's Richard (Rick) Lamb continues to support a DNSSEC Status Page and a resource page that supports public root key rollover testing. We are investigating ways for the research team to utilize or host these and possibly other tools Rick has created on production systems. The status page has helped to provide early notifications of signing issues since 2010. (see the snapshots below). In parallel, Rick runs daily checks on all TLDs and this ad hoc system sends email alerts to key ICANN staff and the technical contact of the affected TLD as listed in the IANA database when DNSSEC signatures are about to expire.





Security and Technology Awareness Raising Activities

In 2H 2015, the SSR Team began a series of blog posts, Raising Security Awareness: One Definition at a Time. The monthly are intended to de-mystify Internet and cybersecurity terminology. A list of past blog posts, with abstracts, is available, and the team's document archive has been restored. We will continue the series in 2016 and hope to complement our team's areas of expertise with guest contributions.

As a part of our work and collaboration within OCTO, SSR is involved with a new initiative that was launched in 2015. As part of OCTO's mission to increase technical expertise and awareness in the ICANN community, we have rolled out a series of tutorials during the ICANN meetings called "How it Works." The intention of these tutorials is to increase the technical foundation of knowledge to those who attend ICANN meetings. To date, these sessions have included information regarding the Internet Engineering Task Force (IETF), Internet routing basics, protocols used when operating a registry, and a history and overview of the Root Server Operating System.

The SSR team also continued periodic training for ICANN staff and delivered phishing awareness and Identifier Systems basics training to staff in LA, DC, and Brussels. Visits to Istanbul and Singapore offices have been scheduled for early 2016.

SSR Framework

Since 2009, ICANN has published an annual Security, Stability and Resiliency Framework. The framework describes ICANN's role and boundaries in supporting a single, global interoperable Internet and the challenges for the Internet's unique identifier systems. The framework is recognized in the Affirmation of Commitments[1], and has been analyzed favorably by the Security, Stability and Resiliency Review Team[2] as part of the Affirmation of Commitments review process. We began work on a combined FY15, FY16 IS SSR Framework late in 2H 2015. We expect this to be available early in 1H2016. It will include implementation of the SSR Review Team's October 2012 recommendations[3], incorporation of Unique Identifier ecosystem goals defined in ICANN's Strategic Plan 2016-2020[4], the role the ICANN

[1] Affirmation of Commitments by the United States Department of Commerce and ICANN, http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm.

[2] Final Report of the Security, Stability and Resiliency Review Team, 20 Jun 2012, http://www.icann.org/en/about/aoc-review/ssr/final-report-20jun12-en.pdf.

[3] Adoption of the SSR Review Team recommendations by the ICANN Board of Directors, 18 October 2012, http://www.icann.org/en/about/aoc-review/ssr/board-action.

[4] Strategic Plan 2016-2020, 10 October 2014, https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf

Security team will fall under the Office of the Chief Technology Officer, and projected activities in FY15 and FY16.