ICANN Identifier System SSR Update – 1H 2015

Satisfying steady demands for capability building and global stakeholder engagement, supporting trust communities via ICANN's threat intelligence channels, developing proofs of concept for novel analytics and information collection, and making progress on train the trainer programs highlight the Identifier Systems Security, Stability and Resiliency (IS SSR) Update for the first half of 2015 (1H 2015).

Sustaining and Expanding Collaboration Opportunities for ICANN

In 1H 2015, our team succeeded in lending its competencies in information security, cybersecurity, Internet, and DNS operations to several communities where we had previously been unable to reach. 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. These engagements not only provide much-needed cybersecurity and operations capacities for these communities, but extended ICANN's trust-based collaborative reach as well.

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 1H 2015, the team provided twenty-nine (29) on-site or remotely delivered training programs in five regions (NA, LAC, EU, AF, AP). This is numerically fewer than 2H2014, however, many of the DNS Abuse trainings are now more advanced, span multiple days, and for the first time, we were able to partner with RIPE NCC to deliver multi-day *Identifier System Abuse* training. This engagement afforded us with the opportunity to share and exchange training insights and material: in future DNS Abuse training, we'll be incorporating more Internet address and autonomous system investigation methods.

Training Trainers

Our team, cooperating with our training partners at Network Startup Resource Center, NSRC, conducted a pilot *Train the Trainer* course on DNS Operations in Dubai, UAE in May. Ten individuals from the Middle East and African region were made familiar with our course material and delivery techniques, and were further instructed on how to utilize tools such as virtual server platforms. We will continue to explore Train the Trainer courses as these enable regions to offer ICANN-related training for their constituents and expand our reach. The intent here is for ICANN to seed regions with subject matter expertise and eventually have these partners deliver training in local languages. This is a formidable undertaking: the breadth and degree of expertise that candidates to train such courses require is considerable. We are, however, optimistic that the interest in all regions is high and that the program will grow over time.

Strengthening Relationships with Security Communities

In 2H2014, 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.

This year, we solidified our relationship with the Anti-Phishing Working Group (APWG). We increased our participation level and ICANN has been invited to assume steering committee responsibilities for both the APWG and APWG EU.

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 44 engagement requests in 1H2015.

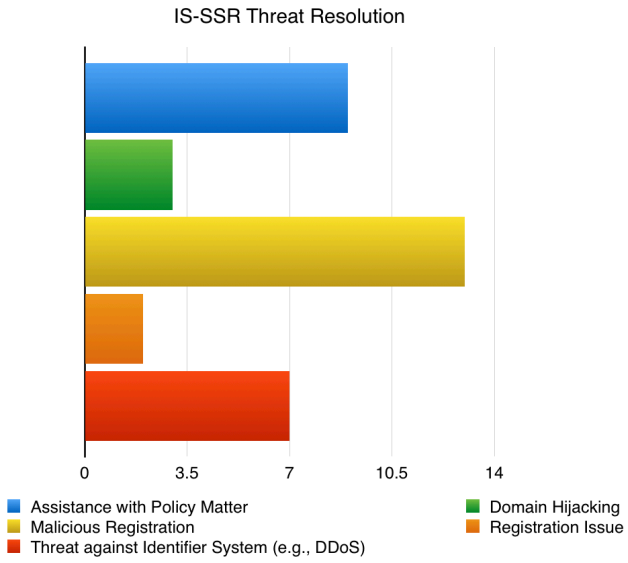
Noteworthy among these activities in 1H 2015 included:

- An identifier systems and cybercrime workshop for European Commission Directorates General in Brussels (February)
- Collaboration with M3AAWG to revise its best practices to address online and mobile threats to include a chapter, *Threats involving Internet Identifiers*, (February)
- Multi-day training open to all branches of UK law enforcement at ICDDF (March).
- Cyber Secure Pakistan (ME, April) included workshops for cybercrime investigators, technical and academic communities, and the Pakistan Telecommunication Authority, visits to Pakistan's NR3C/FIA and activities with government regulatory, technical, operations and CERT staff.
- Presentations and workshops at DEFTcon, La Sapienza University, and for Italian law enforcement (Rome, April).
- Participation in the South School on Internet Governance, Costa Rica (April)
- DNS Abuse training to Peruvian National Police, Lima.
- A joint SSR and GSE collaboration and training exercise with law enforcement in Tonga, Kiribati, and Fiji (May) received very good feedback and requests for further assistance in SSR capacity building.

- Engagements in India (APAC, April, May) included a DNS/DNSSEC Workshop and Workshop to Government of India Security Advisors, Investigators and Law Enforcement.
- Workshops for CERT, ISP, and law enforcement in Cairo (May)

Increased and Expanded Threat Intelligence Reporting and Response

Perhaps no better indicator of how dramatically cyber incidents have spiked in 2015 is that our team resolved 34 inquiries or requests for assistance in 1H2015, nearly double over the previous reporting period, as illustrated in the following chart:



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.

Raising Security Awareness

Members of the Security team regularly publish articles on identifier system and general security topics at the ICANN blog, industry publications or blogs (El Tiempo, Tech Target, Security Skeptic), in English or Spanish. We also published a Security Awareness Resource Locator page. The resources on this page can help consumers, business or IT professionals avoid online threats or harm and make informed choices regarding (personal) data disclosure or protection. We have also launched a monthly blog series, Security Awareness: One Security Term at a Time. Team

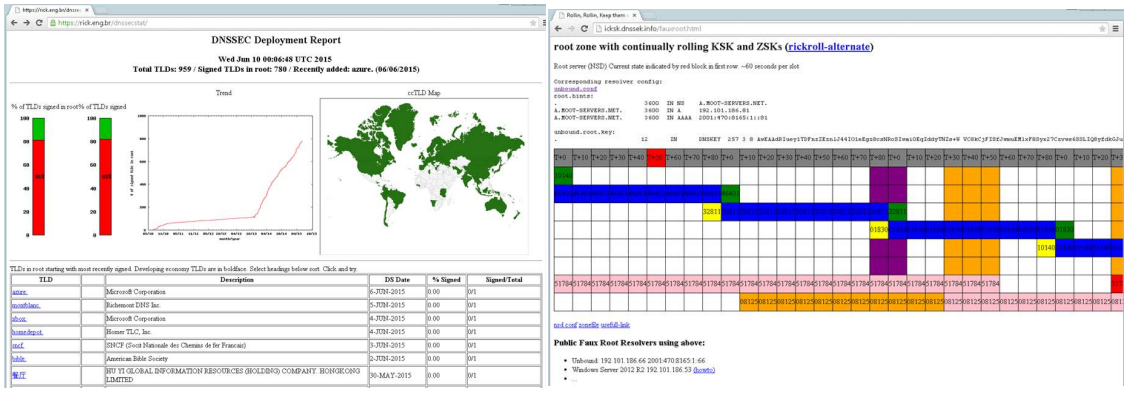
members published seven articles on DNS-related topics and an additional ten articles on general security matters in 1H 2015.

Analytics Projects

We continue to take advantage of the eCrime eXchange cybercrime event data we can now access via our APWG membership. During 1H2015, we developed a proof of concept software to obtain phishing URLs associated with Top Level Domains delegated as part of the new TLD program. The next phase of this project is to migrate the software to a supported platform for wider internal consumption and to improve automation.

We also developed a proof of concept utility for gathering information about a suspicious domain name or URL from multiple sources – DNS, Domain and IP Whois, passive DNS replication databases, and reputation systems – and generate a single report. The next phase for this project is still under discussion.

For some time, Richard Lamb has been supporting a DNSSEC Status Page and a resource page that supports public root key rollover testing. We are investigating ways to host these and possibly other tools Rick has created on production systems.



Tracking IS-SSR Activity

Starting in 2014, our team began to track our activities. This included our engagements, threats, trainings, workshops, and other activities. Utilizing our internal RT tracking system, we created a queue that would allow us to track our training activities well in advance of the event, allowing us to better plan individual and team activities. This has helped us better coordinate our trainings with the Global Stakeholder Engagements team, who help us arrange additional engagements while we're in a given region as well as give us visibility on the number of asks we get to train or participate, even if they don't become realized events.

In an effort to consolidate some of the other activities we capture and track, we have moved all of our relevant data into ICANN's RT system. This will give our team a

single location to deposit data and will soon be able to provide KPI data to the business intelligence team in an automated fashion, ensuring timely input from our team to the corporate dashboard.