Identifier System SSR Update – 30 June 2014

Dave Piscitello, VP Security and ICT Coordination

Expanding opportunities in trust-based collaboration, capability building, increased use of ICANN's threat awareness channels by trust communities, analytics projects planning, and a program for GSE-ISSSR engagement tracking and measurement highlight the 30 June 2014 Identifier Systems SSR Update.

New Collaboration and Stakeholder Opportunities for ICANN

One of the purposes of lending competencies to the community and engaging in trust-based collaboration is to grow 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.

During the 4-month period ending 30 June 2014, the team received approval for membership in M^{3}AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group. This membership formalizes a relationship not only with M^{3}AAWG, but creates opportunities for the ISSSR team to work closely with global email and Internet service providers. We also strengthened our relationship with the AntiPhishing Working Group (APWG) by sponsoring the CeCOS VIII Conference in Hong Kong and by becoming a Sponsoring Member.

ICANN staff accepted invitations to speak or provide capability building from ICANN Global Stakeholder Engagements, ICANN Speaker Bureau or directly from these hosting organizations:

- INHOPE
- SLAM/SPAM
- APWG CeCOS VIII
- The Financial Services Roundtable/BITS
- Global Cybersecurity Capacity Centre
- Caribbean Stakeholder's Meeting
- CITEL
- Organization of American States (OAS) / Inter-American Telecommunications Commission (CITEL)
- NTN24 Latin news channel
- Internet2
- Newspaper features for The Guardian, BBC/Horizon, Süddeutsche Zeitung

Note that these are in addition to speaking and capability building programs that we coordinate with GSE and deliver through training partners. As a result of these participations, we were able to meet with and encourage participation in future

ICANN meetings; for example:

- ENISA staff, Scotland Yard, Operation Sterling, and European Commission Policy officers attended ICANN London
- NCFTA staff and public safety community members attended ICANN London
- MAAWG has been invited to participate in a DNS Abuse session at ICANN Los Angeles
- California OAG and *CNN en Español* have been invited to attend ICANN Los Angeles
- OAS/APWG/NCSA have expressed interest in coordinating security awareness training in the Caribbean
- BITS and FS-ISAC have expressed interest in assisting the ISSSR Team with studies of domain registration protection practices in the financial community
- SG.NIC, MENOG, LACNIC, CR.NIC, TR.NIC, and regional infrastructure operators have requested DNSSEC training
- LACNIC, APWG, OAS, UK National Crime Agency, Spamhaus, Kaspersky, iSight Partners, Colombian Ministry of ICT, the Colombian Chamber of Informatics and Telecommunications (CCIT), colCERT, and .co Internet have expressed interest in supporting a training event in Colombia (a regional key country in cyber security matters for law enforcement, ISPs and regional CERTs.)

Reinforcing ICANN Relationships

Security team staff were able to use the keen interest in cybersecurity as a segue to promote ICANN and multi-stakeholder approaches to governance when they present or train at engagements arranged by GSE and through our own relationships (CCI, network operations group, ccTLDs, RIRs); specifically:

- Informal meetings with ministries of Caribbean countries at the Caribbean Stakeholders' Meeting resulted in inquiries for further in-country assistance from the Commonwealth Cybercrime Initiative by 4 countries (Trinidad & Tobago, Grenada, St. Lucia, St. Vincent & Grenadines) and further interest in GAC participation. These have been reported to GSE and our team will coordinate.
- GSE and the Cyber Security Program of the Organization of American States will cooperate to provide capability building in LATAM regional events.
- Team members met with regional Interpol headquarters (SA, EU, SG) to discuss how best to transfer DNS and DNS abuse knowledge from ICANN staff to Interpol trainers.
- Team members led DNS/DNSSEC hands-on training for SG, MENOG, CR, and TR. These were combined with awareness workshops covering government and business interests and direct engineering assistance for implementation. Participants included regional telecom and finance ministries, executives from businesses, academics, and engineers.

Trust Communities Increase and Expand Threat Awareness Reporting

We have been asked to assist with or facilitate introduction to appropriate parties (internal or external) on a wide set of awareness reporting and response activities in Trimester III including:

- Inquiries related to alleged 2013 RAA violations, where the public safety community needs assistance with the submission process.
- Advice in preparing court orders and ERSR waivers for a global botnet disruption action. 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.
- 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 voluntarily take action against demonstrably criminal domain names.
- Assistance in understanding the CZDS or to inquire whether TLD registry operators are satisfying their agreements in circumstances where requests for access are denied.
- Identification of new TLD applicant implementation problems (WHOIS, DNS zone publication, CZDS).
- Reports of DNS vulnerabilities (via the Coordinated Vulnerability Disclosure).

In these cases, the Identifier System SSR Team considers the report or request, communicates this to ICANN staff or an ICANN contracted party with additional technical information, context, or with a validation of the reporter's credential. 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

The Security Team has developed plans for and begun the following analytics projects:

- 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 (e.g., SAC 040, 044) for protecting registrations against hijacking or other registration service threats.
- 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.

Program for GSE-ISSSR engagement tracking

To increase communication and coordination, the GSE and Security teams now schedule weekly conference calls to discuss upcoming training and engagements. In addition to these regular calls, the Security team has implemented a training tracking system, which enables the team to better plan resources in which to our training programs.

By implementing this training tracking system, ISSR is better able to engage with the GSE Regional VPs in long term planning. As an example, we now have exposure to the Middle East strategic plan and have potential training opportunities reaching out as far as April 2015. This will allow us to be more strategic in our planning of training and engagement opportunities surrounding a workshop.