Update on 2016 Activities

ICANN Office of the CTO
Security, Stability and Resiliency Team | 3 February 2017

Introduction

The ICANN Office of the CTO (OCTO) Security, Stability and Resiliency (SSR) team concluded a successful 2016 with growth in many of our functional areas. Capability building and global stakeholder engagements grew dramatically in 2016, reaching deeper into several regions. We expanded our training capacity and improved our training courses. We continued our development of proofs of concept for identifying malicious domain name registrations and furthered our development of a platform for studying or reporting security threats. We continued security and technology awareness-raising programs and made these available to the ICANN organization, the ICANN community and the Internet community at large.

Sustaining and Expanding Opportunities for Collaboration

Our team continued to lend competencies in information security, cybersecurity, Internet and domain name system (DNS) operations. These activities earned or improved trust for the ICANN organization among organizations that are typically not part of the ICANN community, and encouraged those organizations to participate in ICANN's multistakeholder consensus-based policy development. Security threats in the emerging Internet of Things (IoT) became a hot topic wherever the OCTO SSR team presented or trained. Our team was also called upon to discuss, comment or collaborate on IoT technology evolution, security and adoption, and how to address challenges. We participated in a number of forums, e.g., the Eastern European DNS Forum/UADOM and the Computer Association of Nepal's Information and Communications Technologies Conference (CAN ICT Conference). Discussion topics included the IoT cyberopportunities, the IoT threat landscape, the role of "things" in global cyberattacks and misuse of the Internet's identifier systems. These engagements contributed to a greater understanding of the potential roles of the ICANN organization and the ICANN community in the future of IoT. The OCTO SSR team and others in the ICANN organization are studying the roles we could play.

Capacity Building

The capacity building our team delivered included training programs with live demonstrations of techniques and hands-on learning opportunities. In 2016, the team provided on-site or remote training programs in all regions (North America, Latin America and the Caribbean, Europe, Africa and Asia Pacific).

Training and "Training the Trainers"

Champika Wijayatunga, Regional SSR Engagement Manager for Asia Pacific, and Carlos Alvarez, SSR Technical Engagement Senior Manager, led training and engagements in the Asia Pacific and Latin American and Caribbean regions, respectively. Richard Lamb, Senior Program Manager of DNS Security Extensions (DNSSEC), began delivering training in Africa. Dave Piscitello, VP of Security and ICT Coordinator, led training sessions in North America, Europe and Eastern Europe. John Crain's role as Chief SSR Officer took him to all regions.

We continued to seek partners for our training. In March, the United Kingdom Computer Emergency Response Team (CERT-UK) trainer candidates accompanied ICANN organization staff to "shadow train" at an event in the U.K. A member of ICANN's Security and Stability Advisory Committee (SSAC) attended this training and volunteered to give the training on our behalf at Europol in August 2017. The breadth and degree of expertise needed to teach such courses is considerable, and interest for this training remains high in all regions. We continued to seek opportunities for ICANN to seed regions with subject matter expertise and eventually have these partners deliver training in local languages. We are optimistic that the program will grow over time.

In 2016, we began a survey-based performance assessment of our training activities. The survey was intended to help the OCTO SSR team to quantify training success in three areas:

- **Does our training clarify ICANN's role in investigations involving domain name system (DNS) or registration services?**
- **Does our training clarify the roles of generic top-level domain (gTLD) registry and registrar stakeholders in investigations involving DNS or registration services?**
- **Does our training give investigators a better understanding of how the Internet's system of unique identifiers and associated registration systems work?**

The initial responses were very encouraging. Ninety-four (94) percent of trainees responded positively when asked if their understanding of ICANN's role in investigating the DNS or assisting law enforcement officers had improved as a result of the training. Over 90 percent of trainees indicated that their working knowledge of registry or registrar roles had expanded or had been reinforced through the training,

and between 80 and 85 percent of trainees indicated that their working knowledge of the DNS and Internet numbering systems had expanded or had been reinforced. We will continue the survey throughout 2017.

Expanding Our Reach

Highlights for 2016 included:

- **Two- and three-day training sessions for Peruvian law enforcement, investigators and heads of information security from the Peruvian government, in coordination with the Peruvian Ministry of Foreign Affairs**
- **Presentations, both in person and online, and training for law enforcement in Costa Rica, Cuba, Argentina, Colombia, Honduras, the Dominican Republic, Mexico and Ecuador**
- **Capacity-building workshops on DNS and DNSSEC and identifier systems abuse handling in Phnom Penh, Cambodia, during an event hosted by the Ministry of Post and Telecommunications (PTA)**
- **Workshop for Thai police at the Thai Police Headquarters in Bangkok, in collaboration with the Thailand National Network Information Center (THNIC)**
- **Tutorials on DNS operations, country code top-level domain (ccTLD) management and a five-day hands-on workshop on deploying DNSSEC at the South Asia Network Operators Group Conference (SANOG28) in Mumbai, India**
- **Training for law enforcement in Doha, Dubai and Beirut**
- **Week-long DNSSEC hands-on training in Ankara, Turkey, to government, banks, Internet service providers, registries, registrars and startups**

- **DNSSEC technical implementation keynote, cybersecurity panel and IoT closing plenary at the conference of the Eurasian Network Operator's Group (ENOG) in Armenia**
- **Training on investigating DNS abuse and criminal use of the DNS in Vienna (hosted by the Austrian Cybersecurity Competency Center); Tbilisi, Georgia (hosted by the Internet Development Initiative); Glynco, Georgia, U.S. (U.S. Federal Law Enforcement Center); and London, U.K. (International Communications Data and Digital Forensics Seminars)**
- **Keynotes and cybersecurity presentations at conferences in Warsaw (Cybersecurity Foundation), Krakow (European Cybersecurity Forum), and Kiev (EE DNS/UADOM)**
- **Workshop on cybersecurity and cybercrime for Commonwealth Parliamentarians, organized by the Commonwealth Parliamentarians Association in the U.K. and hosted by Queensland Parliament, Australia**
- **Four days of hands-on training on DNS, DNSSEC and network management at the Middle East Network Operations Group (MENOG) meeting in Istanbul, Turkey**
- **Keynote on cybersecurity, cooperation, and IoT opportunity with the Minister of Communications at the Computer Association of Nepal's annual ICT Conference (CAN ICT Conference)**

Strengthening Relationships with Security Communities

We continued to strengthen our relationship with the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). Carlos Alvarez is now co-chair of the M3AAWG's Anti-Phishing Special Interest Group (SIG), which gives our team greater access to communities that address phishing. Dave Piscitello was elected to the Board of Directors of the Anti-Phishing Working Group (APWG) and continues as an associate fellow at the Geneva Centre for Security Policy. The team also provided subject matter expertise and in-person and virtual training to the Organization of American States (OAS) Cyber Program and to the Organization for the Security and Cooperation in Europe (OSCE). The team worked in cooperation with the ITU and OAS to raise awareness of Identifier systems security at conferences in Quito, Ecuador, Washington, D.C., and Bogota, Colombia. John Crain led a team effort to provide subject matter expertise and to collaborate with domain registries, Europol, Interpol, Eurojust, the Registrar of Last Resort, and national law enforcement agencies to dismantle the criminal infrastructure known as the malware- and ransomware-supporting Avalanche network.

Working with Global Stakeholder Engagements

The SSR team continued to promote multistakeholder approaches to governance when we presented or trained through engagements arranged by ICANN's Global Stakeholder Engagement (GSE) team and through engagements resulting from our own relationships. In 2016, through the GSE team, the SSR team conducted engagements in Eastern Europe for the first time. Champika Wijayatunga, the shared member of the GSE and SSR teams, delivered first-time engagements on behalf of SSR in Papua New Guinea, Vietnam, Bhutan and Cambodia. Carlos Alvarez expanded the SSR team's reach in the Latin American and Caribbean region, reaching new audiences in Peru, Argentina, Costa Rica and Colombia.

Increased Threat Intelligence Reporting and Response

We continued to assist with cyberincident requests and supported anti-abuse, operations and security efforts to dismantle large-scale infrastructures that exploit DNS and domain registration systems. In these cases, our team considered requests and where appropriate, discussed them with ICANN organization staff. We assisted by verifying information or by validating the reporter's credentials. Some of these requests for assistance were mundane, e.g., inquiries seeking a clarification on policy, technical assistance or an introduction to a point of contact. Others were quite complex and involved cooperation from both the gTLD and ccTLD registry operators as well as private and public sector actors. The coordinating role our team plays required us to assist regularly for several months.

We worked with ICANN's Contractual Compliance team to explore issues related to the Centralized Zone Data Service (CZDS) and cases involving high volumes of WHOIS inaccuracy complaints. The SSAC invited us to support an ICANN SSAC study into CZDS and WHOIS rate limiting. This activity will extend into 2017.

Security and Technology Activities to Raise Awareness

The SSR team continued its popular series of blog posts, Raising Security Awareness: One Definition at a Time. In 2016 we attempted to demystify topics such as metadata collection, privilege escalation and DNS covert channels. Our past blog posts (with abstracts) are available and the team's document archive has been restored. The SSR team also contributed to periodic training for the ICANN organization, hosting "brown bag lunches" on a range of topics that included ransomware, business email compromise and IoT.

The SSR team participated in expanding a framework for registry operators to use to analyze and report on domains in the TLD that are being used to perpetrate security threats and how to mitigate those threats. As part of this effort, we published a blog to clarify the nature of security threats and the availability and kinds of data sources that could be used in such technical analyses. We also published articles in the *European Cybersecurity Journal* on investigating identifier systems abuse, in the *G20 China Foundation* on mitigating cybercrime, and in *El Tiempo* on the consequences of domain name expiration and domain name portfolio management. Carlos Alvarez continued publishing posts in Spanish on identifier systems issues at *El Lado Oscuro de Internet*, and popular posts on Dave Piscitello's blog "The Security Skeptic" are now translated into Spanish.

SSR Framework

Since 2009, ICANN has periodically published its SSR Framework. The framework describes ICANN's role and boundaries in supporting a single, global interoperable Internet and the challenges for the Internet's systems of unique identifiers. In early 2016, the SSR team prepared a combined FY15 and FY16 OCTO SSR Framework. It describes:

- **Implementation of the SSR Review Team's October 2012 recommendations**[1]
- **Incorporation of goals regarding the unique identifier ecosystem that were defined in ICANN's Strategic Plan 2016–2020**[2]
- **Role of the ICANN Security team under the Office of the Chief Technology Officer**
- **Projected activities for FY16 and FY17**

[1] 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.
[2] Strategic Plan 2016–2020, 10 October 2014, https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf.

One World, One Internet

ICANN.ORG