DAVID PISCITELLO

SSR: securing the Internet's identifier systems

Dave Piscitello is a Senior Security Technologist for ICANN. A 30-year Internet veteran, Dave currently serves on ICANN's Security and Stability Advisory Committee and the Internet Policy Committee of the Anti-Phishing Working Group (APWG).

dave@corecom.com

NO SINGLE ENTITY IS RESPONSIBLE for the administration and oversight of all aspects of the Internet. One entity, Internet Corporation for Assigned Names and Numbers (ICANN) *is* tasked with the responsibility of coordinating the Internet's unique identifier systems and with participating in the global operation of the Domain Name System (DNS). Part of this responsibility involves ensuring the security and stability of these identifier systems. This responsibility is not only a key element of ICANN's mission statement but an obligation under the September 30, 2009 Affirmation of Commitments by the United States Department of Commerce and ICANN [1]. How ICANN intends to meet this obligation is described in its Security, Stability and Resiliency Plan (SSR).

In this article, I highlight the critical elements of that plan, scoping ICANN's remit and describing the activities ICANN will perform directly, as well as activities where ICANN will be one of potentially many collaborative players.

Who Runs—and Secures—the Internet?

The simple answer is "no one and everyone." Originally, the term Internet derived from the concept of an "an *inter*connection of *net*works." Today, the term Internet more broadly applies to the combination of technology infrastructure and the ecosystem of communities that create, make use of, and sustain this critical infrastructure. Internet communities—governments, public and private organizations, and individuals, also called *stakeholders*—cooperate to develop policies and business practices necessary to sustain a productive ecosystem, and they must do so at the same pace as Internet technology evolution.

These stakeholders must also respond to the persistent and growing sets of threats posed by criminal, combatant (terroristic), and miscreant actors. This set of "bad actors" exploits the transportation routes the Internet provides to perpetrate criminal and malicious activities. They also exploit the Internet's unique and critical sets of identifiers, using *domain names* and *Internet addresses* to facilitate unwanted activities ranging from identity theft, fraud,

and disruptions or denials of service, to illegal sales of controlled substances and pharmaceuticals and human trafficking.

ICANN's Remit

ICANN facilitates multi-stakeholder, consensus-based policy and program development to ensure that identifiers such as domain names and IP addresses are allocated fairly and equitably. These policies and processes influence how the DNS operates, how domain names may be composed and registered, and how addresses are allocated. These policies are typically reflected in contracts and agreements established between ICANN and operators around the world (governmental and private). Contrary to numerous popular perceptions, ICANN is not a regulatory, legislative, or law enforcement entity. ICANN is not involved in activities related to dealing with cyber-espionage, terrorism, or warfare and does not take a role in what constitutes illegal content on the Internet. Historically, and now formally as stated in a Security, Stability and Resiliency plan [2], ICANN has taken steps to ensure that the identifiers it coordinates are used in ways that do not threaten the Internet ecosystem.

ICANN's Direct Roles

ICANN has several direct roles in ensuring the Internet's security, stability, and resiliency. As the performer of the Internet Assigned Numbers Authority (IANA) function, ICANN administers and ensures the integrity of the very large set of assigned numbers that are critical to the correct operation of the Internet infrastructure. This set not only includes the familiar domain names and IP addresses, but dozens of other databases (registries) of system and protocol numbers as well. The IANA operation is also responsible for the coordination and publication of the authoritative root zone for the DNS. This activity involves the coordination and verification of zone information for 280 delegated top-level domains (TLDs) and 13 root name servers. IANA's performance objective for this activity is effectively "zero tolerance for misconfiguration error." ICANN will also shortly work in cooperation with its root zone management partners (US NTIA and VeriSign) to cryptographically sign the root zone, an action that is expected to accelerate the adoption of DNS Security (DNSSEC). DNSSEC will add origin authentication, zone data integrity, and authenticated denial of existence services that are designed to defeat DNS cache poisoning and hijacking attacks.

ICANN also operates one of 13 root name servers for the DNS. In this role, ICANN maintains a fully redundant, highly secured, anycast-enabled root name server system ("L") at geographically diverse locations. Each operation is kept resilient from attacks and operationally available following industry best practices in design, capacity, and security planning.

Another of ICANN's direct roles evolves naturally from the experience and expertise gained from operating large-scale DNS facilities. ICANN staff assist in the development and delivery of training and security awareness programs to TLD operators, when invited. These activities help improve the overall security of domain name resolution and registration services offered by TLD operators.

ICANN's Collaborative Roles

The ICANN acronym is often associated with the community of stakeholders and participants with which it collaborates. This blurred distinction does

cause confusion, but it also reflects the practical realities all stakeholders, including ICANN, face: (a) strengthening the security, stability, and resiliency of the Internet can only be accomplished through collaboration on a global level; and (b) cooperation of law enforcement, private sector, DNS, and security communities is needed to successfully intervene or respond to security incidents where the DNS is attacked or exploited on a global scale. ICANN's commitment to playing this role, as well as the commitments of TLD operators worldwide, are best exemplified by the ongoing effort to contain the Conficker worm [3]. ICANN staff worked with over one hundred TLD operators to preemptively block thousands of domain registrations identified daily by security companies who had cracked the Conficker executable and in doing so had discovered the algorithm the worm writers had used to generate domain names for would-be botnet rendezvous points. ICANN is working with the community to apply the lessons learned from this collaborative effort to improve and define response systems that will prove to be agile and adaptive to attacks and criminal activities. A recent example of this is the Expedited Registry Security Request, a collaborative effort between ICANN and gTLD registries to develop a process for quick action in cases where gTLD registries inform ICANN of "a present or imminent security incident to their TLD and/or the DNS" [4].

ICANN's SSR plan calls for participation in and engagement with organizations that work to contain or eliminate criminal activities such as phishing, fraud, identity theft, and abuse of intellectual property. These elements of the plan are reflected in several critically important areas of development, most notably programs relating to the addition of new TLDs and internationalized domain names. As part of its development of guidelines for new TLD applicants, ICANN solicited input from the Anti-Phishing Working Group (APWG), Registry Internet Safety Group (RISG), BITS Fraud Reduction Program, American Banking Association, Financial Services Information Sharing and Analysis Center (FS-ISAC) and Financial Services Technology Consortium (FSTC) to help define what the community believes constitutes *malicious conduct* [5]. ICANN also tasked a group of experts to study the risks associated with adding DNSSEC, new TLDs, and IPv6 to the root zone of the DNS [6]. Lastly, ICANN gathered input from experts from the security and financial communities, as well as with its own Security and Stability Advisory Committee (SSAC), to develop a high security voluntary verification program for new TLD registries [7]. Combined, the results of these joint activities will allow ICANN's contractual compliance program to better ensure that contractual obligations are taken into account by ICANN's contracted parties.

Way Forward for ICANN

This article calls attention to a fraction of the commitments ICANN has made in its SSR plan. The plan is ambitious even if one only assumes ICANN will take the lead on all the initiatives in the plan. The way forward for ICANN is to lead where its remit demands it lead, and collaborate when the opportunity to meet objectives in the SSR through collaboration appears. The SSR plan formalizes ICANN's commitment to contribute in the realms of security, stability, and resiliency as a central part of ICANN's role in coordinating global identifiers in a multi-stakeholder environment.

REFERENCES

[1] ICANN, "The Affirmation of Commitments: What It Means": http://www.icann.org/en/announcements/announcement-30sep09-en.htm#affirmation.

[2] ICANN, "Plan for Enhanced Internet Security, Stability and Resiliency": http://www.icann.org/en/announcements/announcement-2-21may09-en.htm.

[3] Conficker Working Group: http://www.confickerworkinggroup.org/wiki/.

[4] ICANN, "Expedited Registry Security Request Process": http://www.icann.org/en/announcements/announcement-01oct09-en.htm.

[5] ICANN, "New gTLD Program Explanatory Memorandum: Mitigating Malicious Conduct": http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf.

[6] ICANN, "Root Scaling Study": http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf.

[7] ICANN, "New gTLD Program Explanatory Memorandum: Model for a High-Security Zone Verification Program," draft version 1.0: http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf.