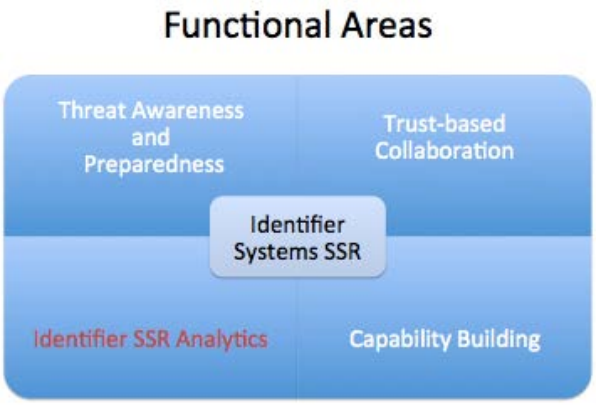
Identifier Systems Security, Stability, and Resiliency Programs

Dave Piscitello, VP Security and ICT Coordination

This program note describes one of four IS SSR programs, **Identifier System Analytics.**



Identifier System analytics has until 2015 been limited by staffing constraints; in particular, the IS SSR Team has not been in a position to hire data analytics expertise to execute on several of the originally intended project.

In the absence of in-house data analytics expertise, the IS SSR Team chose to contract experts to conduct some investigative data analyses. The reports use advanced threat intelligence analytics, multiple threat and intelligence feeds techniques to collect domain data registration (Whois) of two ICANN accredited registrars who are reputed to sponsor a disproportionate number of malicious domain registrations (domains use for spam, phishing, botnet C2C, or malware hosting). Using human OSINT to inspect point of contact data in Latin and Japanese script, they were able to corroborate allegations that the registrars failed to meet RAA 2013 contractual obligations on an excessive scale.

Team members also developed proofs of concept software and scripting that take advantage of threat intelligence or abuse data feeds that the IS SSR team can access through its trust relationships, including APWG, Shadowserver Foundation, Farsight, Spamhaus and SURBL. Initial scripts scanned entire zone files of select new TLD delegations, including several that the OPSEC community alleges to be excessively populated with malicious domain registrations. Subsequent scripts associated the malicious registrations with sponsoring ICANN accredited registrars. These reveal that three registrars account for an extraordinary percentage of spam registrations. These reports were shared with GDD and Compliance, and these proofs of concept efforts may be formally incorporated into the Identifier Health Indicators project.

Projects in this program focus on gaining an understanding of characterizing how miscreants or criminal actors exploit Identifier Systems, especially domain names. Some projects attempt to quantify the extent of abuse. Others attempt to identify factors – policies, practices, or technology – that create opportunities for these

abuses. Yet others attempt to identify whether miscreant or criminal actors flock to certain registries or accredited registrars and why.

Examples of completed or ongoing analytics projects include:

- **Prevalence of Phishing URLs in new TLDs**. A proof of concept activity to investigate how to effectively use the APWG eCrimeX phishing feed to assess whether phishers are exploiting domain names in new TLDs.
- **Prevalence of Spam domains in new TLDs**. A proof of concept activity to (i) assess the extent to which spammers are exploiting domain names in new TLDs and (ii) determine whether spammers are exploiting or flocking to certain registrars when they register new TLDs domain names.
- **Registrar compliance with RAA 2013**. A deep investigation to assess the extent to which ICANN accredited registrars were satisfying RAA 2013 compliance.