(S//SI) New 'Profile-Based' Target Discovery Tool Shows Promise

FROM: [redacted]
ICN STRIDE Team Leader (S2F)
Run Date: 05/19/2006

(S//SI) New large-scale metadata query capability can help identify new SIGINT targets.

(S//SI) The ICN Sigint Technology, Research, Innovations, Development and Enhancements (STRIDE) Team has been working on an exciting target discovery project for the International Narcotics Division. STRIDE is using a new large-scale metadata query capability in an attempt to discover previously unknown narcotics trafficking targets in Southwest Asia. Preliminary results are encouraging. Earlier this month, STRIDE analysts used the capability to discover a previously unknown alien smuggling network.

(S//SI) The new capability, which is part of a larger software application called WebTAS* (developed by Intelligent Software Solutions, Inc.), queries against over 2 million call event records in order to identify telephonic devices exhibiting certain types of specified behaviors during a given timeframe. A list of phone numbers fitting the general profile is then sent to Project FOSSWAY , which runs a variety of clustering algorithms and enrichment processes against the seed numbers and their first- and second-level contacts. The clustering and enrichment results, in turn, are presented to ICN STRIDE analysts for validation and further analysis. STRIDE is currently testing the new WebTAS capability against SIGINT metadata by investigating an analytic hypothesis provided by DEA SOD (the US Drug Enforcement Agency's Special Operations Division).

The Hypothesis (U)

(S//SI) Earlier this year, DEA SOD posited that the International Narcotics Division could find previously unknown drug trafficking targets by isolating groups of tightly-connected communicants in the countries of Afghanistan, Iran, and Turkey. DEA SOD, noting that the route of Afghanistan to Iran to Turkey is commonly used for drug smuggling, hypothesized that the flow of communication through these countries might -- in certain cases -- be indicative of drug trafficking or other illicit activities.

(S//SI) The International Narcotics Division tasked ICN STRIDE with testing this hypothesis against SIGINT metadata. STRIDE subsequently set out to identify groups of communicants that:

1. fit the general Afghan-Iran-Turkey communications pattern and
2. exhibit certain other suspect characteristics (e.g., contacts from/to Western Europe, as well as recurrent movement along this route).

The hypothesis was then tested against content collected from the most promising groups of communicants.

Generating Seed Information with WebTAS (U)

(S//SI) ICN STRIDE analysts tasked an ICN contractor to develop a new capability that can identify all Iran-registered phone numbers exhibiting contacts with Afghan- and Turkish-registered numbers during a given time period. The capability, which was released earlier this year, is already delivering promising results. Over 1,500 Iranian phone numbers fitting the Afghanistan-Iran-Turkey communications profile were identified in one recent 30-day WebTAS query.

(S//SI) To assist analysts in interpreting the large result set, ICN STRIDE sent the 1,500 phone numbers to members of Project FOSSWAY. FOSSWAY, in turn, has ingested these seed numbers

(along with their first- and second-level contacts) into a large-scale call graph and is now running several clustering algorithms and enrichment processes against the totality of nodes. Once the clustering is complete, STRIDE analysts will focus on the most promising clusters (i.e., those in which seed numbers and certain types of enrichment data appear) with a view to tasking the key nodes for collection, evaluating the content, and -- ultimately -- corroborating or negating the hypothesis.

(S//SI) In the meantime, STRIDE analysts have focused their preliminary analysis on several of the WebTAS-generated seed numbers exhibiting 2nd-level contacts to Western Europe. In early May, these efforts resulted in the discovery of an Iran-based alien smuggling network -- thus providing a proof of concept for the new WebTAS capability.

Proof of Concept: Southwest Asian Alien Smugglers (U)

(S//SI) The process by which the alien smuggling organization was discovered can be summarized as follows:

- (S//SI) WebTAS identified an Iranian seed number that had been in contact with Afghanistan- and Turkey-registered phone numbers at the first level, and Greece- and Italian- phone numbers at the second level.
- (S//SI) Subsequent development and voice exploitation of key nodes in this telephony network confirmed that the communicants were moving people from Pakistan to the UK by way of Afghanistan, Iran, Turkey, and Greece.
- (S//SI) While STRIDE had not expected this network to be an alien smuggling organization, its behaviors were nonetheless markedly consistent with what the team had expected to find -- namely, entities in a pre-specified group of countries moving contraband (in this case, people) into Western Europe.

(S//SI) On 15 May, STRIDE produced the first SIGINT EGRAM (2/OO/2426-06) on this organization, with a SECRET tearline releasable to Turkey. In the near future, this target will likely be handed off to ICN's Alien Smuggling Branch (S2F23) for full-time exploitation.

Conclusion (U)

(S//SI) **In sum, the recently developed WebTAS capability offers a promising and innovative means of identifying previously unknown SIGINT targets.** The capability appears to be most effective when used to test explicitly articulated analytic hypotheses (in particular, those modeled upon dialing characteristics of mobile, non-state targets) that have observable implications in SIGINT. Subsequent vetting of this data through FOSSWAY can help to further distill the results and prioritize the order in which they are evaluated by analysts.

POCs: [redacted], ICN STRIDE Team leader [redacted], ISS contractor and lead WebTAS developer Steve Cummins [redacted], FOSSWAY lead analyst

---

*(U) Notes:
WebTAS = Web-Enabled Timeline Analysis System

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid_comms)."
