DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL

(TS//SI//REL) New Technique Geolocates Targets Active at Yemeni Cafes

FROM: [redacted]
INDEX Team, Arabian Peninsula/Levant/Iraq Branch, Menwith Hill Station (F77)
Run Date:

(TS//SI//REL) Analysts: The technique described below is currently being used only in Yemen, but it could potentially be applied to internet cafes in other geographic regions, under certain conditions. If you have questions about whether this might work on your target, please contact the author.

(TS//SI//REL) In late 2009, analysts at Menwith Hill Station envisioned a new way to geolocate targets who are active at internet cafés in Yemen: combine HUMINT information with networking protocols and passive SIGINT collection to obtain target geolocations. MHS has collaborated with offices across the enterprise[1] to turn this concept into a new mission capability. Currently, the technique enables the identification of tasked and hot-listed targets active at almost 40 different geolocated internet cafés in Sana'a and Shabwah, Yemen.

(TS//SI//REL) In the short time that results from this technique have been available, many targets have been located to these cafés, including targets tasked by several target offices at NSA[2] and GCHQ. Perhaps most significantly, the technique provides some insight into the movements and activities of terrorist targets in Yemen (Al Qaeda in the Arabian Peninsula and Al Qaeda in East Africa -- both high priorities for the Intelligence Community).

(TS//SI//REL) Most internet users in Yemen access the internet via YemenNet, a telecommunications company and ISP (internet service provider) owned and operated by a subdivision of Yemen's Ministry of Telecommunications and Information technology. YemenNet provides services to subscribers primarily via ADSL, DSL, and dial-up connections by dynamically allocating IPs from a pool of 10000-20000 IP addresses. The use of dynamic IPs and landlines for internet connections means that many traditional geolocation techniques (like GHOSTHUNTER[3]) cannot be applied. Instead, MHS analysts determined they could combine HUMINT information from physical surveys of cafés (MORK data) with Tailored Access Operation (TAO - S32) collection of RADIUS[4] logs (WINDCHASER) and passive collection of target activity (MARINA, XKEYSCORE) to provide target geolocations. The basic steps of the process are:

1. Extract a café IP address from a detailed café record in MORK. This is the IP that the café was using at the time of the physical survey. This IP is dynamic and only associated with the café for the length of this particular session. It cannot be used as a long-term café identifier or be associated with target activity after the session is over.

2. Query the IP in WINDCHASER using the timestamps from the MORK survey records. This query will pull TAO-collected RADIUS logs for the dynamic IP and can be used to discover session information for the café, including session start and stop times, ATM port, and customer userID.

3. Find the userID that is active at the time of the MORK survey. The userID belongs to the customer who logged in to initialize the internet session. UserIDs have a more consistent relationship with end users and are critical to following a target effectively in a dynamic IP environment. For café sessions, the userID generally represents the café administrator.

4. Repeat. Because of variations and uncertainties in RADIUS and MORK data, this process should be repeated with additional MORK records to ensure results are consistent. Consistent results show that the WINDCHASER userID belongs to the administrator of the café surveyed in the MORK record.

5. Associate MORK geo with correlated userID. Once a correlation has been found, the geo information from the MORK record can be associated with RADIUS sessions initiated by the customer's userID.

   Query SPARKLEPONY[5] to find targets active at the located café. SPARKLEPONY will use passive collection in MARINA and information from RADIUS sessions initiated by a given userID to find all email addresses active during the customer's sessions. This list can be filtered to focus on tasked and hot-listed targets.

(TS//SI//REL) MORK data

(TS//SI//REL) Above, MORK physical survey data is combined with RADIUS logs to provide target geolocation

(TS//SI//REL) MHS coordinated with developers to change analyst tools in order to make this concept a reality and to simplify and automate the overall process. For example, MORK has added WINDCHASER userIDs to records when strong correlations have been made. MARINA and WINDCHASER will be adding links to MORK records from correlated RADIUS customer records and enriching query results to notify analysts of likely connections between the two datasets. MARINA is also developing a custom SPARKLEPONY report (based on samples provided by MHS analysts) to identify all targets active at all correlated cafés and a tipping capability for faster notifications of target activity. Target locations can then be passed to TOPIs for further analysis and reporting.

(TS//SI//REL) More information on this and other RADIUS analytic techniques can be found at the RADIUS Data Analysis wiki.

(U//FOUO) POC: [redacted], INDEX Team, Arabian Peninsula/Levant/Iraq Branch, MHS Analytic Discovery Division [redacted])

(U) Notes:

1. (TS//SI//REL) This includes NSAW's Tailored Access Operations, Network Analysis Center, GHOSTWolf, CT Trends office, MARINA developers, and others. Project GHOSTWolf supports efforts to capture or eliminate key nodes in terrorist networks. GHOSTWolf focuses primarily on providing actionable geolocation intelligence derived from SIGINT to customers and their operational components.

2. (C//REL) CT, MENA, International Crime and Narcotics, International Security issues, NSA/CSS Threat Operations Center

3. (S//SI//REL) GHOSTHUNTER - Technique that performs geolocation of IP over satellite return channels.

4. (U//FOUO) RADIUS - Remote Authentication Dial-in User Service is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service.

5. (U//FOUO) More MHS work using SPARKLEPONY can be found in 3/AL/TELIR/13-09.

(U//FOUO) SIDtoday editor's note: This article is reprinted from MHS's Horizon newsletter, February 2010 edition.