(U) SIGINT Development Support II Program Management Review

- 24 April 2013

The overall classification of this brief is

TOP SECRET//COMINT//NOFORN

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20291123

PMR Agenda

- **Strategic & Technical Overview –** [redacted]
- **Placemats & Highlights** – Client Service Leads (CSLs) &

  Senior Mission Technical Leads (SMTLs)
- **PMR Spotlight**
  - MONSTERMIND – [redacted]
  - SDS Support to CHELSEABLUE – [redacted]
- **Technical Health –** [redacted]

(TS//SI//REL TO USA, FVEY)

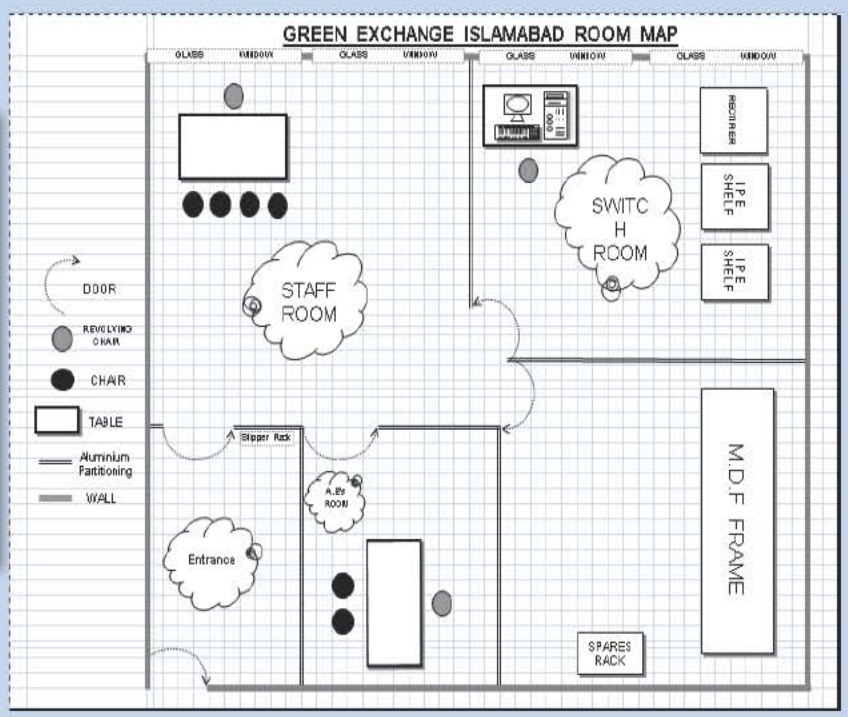
SID Priority: Traditionally Inaccessible Network

SIGINT Development Challenge: Establish a proven foundation of targets in Pakistan's National Telecommunications Corporation's (NTC) VIP Division.

Mission Example and Result: Successfully enabled positive identification of users in NTC's VIP division who focus on maintaining the Green Exchange. The Green Exchange branch houses ZXJ-10 switches, which are the backbone of Pakistan's Green Line communications network. This network is used by senior Pakistani civilian and military leadership. Four machines in the VIP division who have Green Exchange related documents on their machines were successfully implanted.

Our Approach

- Evaluated currently tasked selectors related to NTC's VIP division.
- Conducted SIGDEV against known selectors to identify other related targets.
- Collaborated with R&T to use SECONDDATE and QUANTUM to successfully implant four new CNE accesses within the Green Exchange.



SIGINT Development Outcome: Four new CNE accesses were gained for the VIP Division and a baseline of collection related to the Green Exchange was established.

(TS//SI//REL TO USA, FVEY)

(TS//SI//NF)

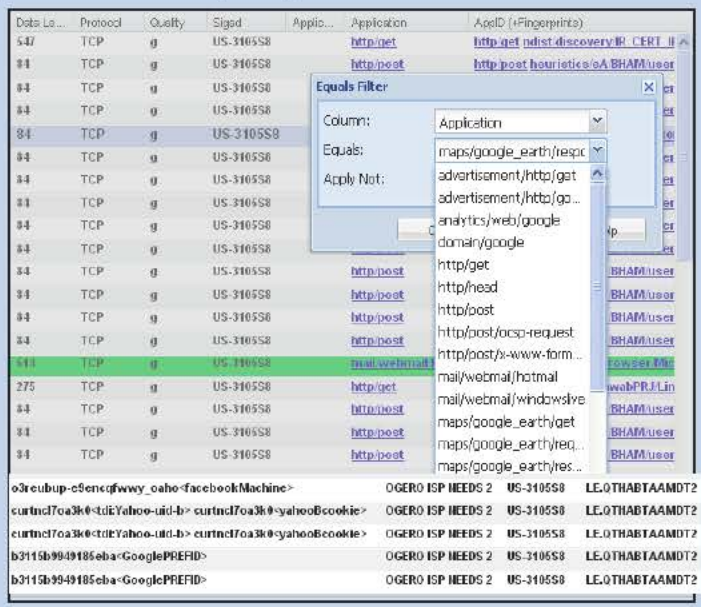
SID Priority: Traditionally Inaccessible Target Networks

SIGINT Development Challenge: Passive access in Lebanon is limited, thereby hindering SIGDEV, Discovery, and Mobility Exploitation. TAO project REXKWONDO successfully enabled Country-Wide Shaping and Man-in-the-Middle (MiTM) capabilities against Lebanon's Internet traffic for the first time ever.

Mission Example and Result: Combined CT SIGDEV and CNE analysis effort within REXKWONDO, the Lebanese owned OGERO ISP, resulted in multiple successful CNE operations that yielded initial access and collection from Lebanon's International Gateway routers. Currently shaping Hizballah-related traffic to SSO-STORMBREW, providing SIGDEV discovery opportunities for S2I, S2E, and SSG\NAC via XKEYSCORE and MARINA.

Our Approach

- S2I53 CT SIGDEV SDS analysts provided technical support on various high-interest targets and assisted in exploitation and implant of the head of the OGERO NOC and the core routers.
- Collaboration between multiple divisions within TAO and S2I5 led to the development of a custom-built router exploit and new HAMMERCORE implant builds.
- The OGERO ISP gateway router (RB) was exploited via HAMREX to enable SECONDDATE MiTM.
- The OGERO upstream Liban Telecom routers were exploited with CGDB, then implanted with HAMMERCORE and HAMMERSTEIN to enable successful Shaping of Hizballah Unit 1800 related traffic for multiple CT projects.
- Traffic was exfiltrated to STORMBREW from core routers and was accessible to S2I, S2E, and SSG\NAC analysts via XKEYSCORE in less than 24 hours following the successful shaping tasking.



SIGINT Development Outcome: SDS collaboration across the TAO and S2I5 previously denied access to the International Gateway routers in Lebanon and Sole-Source Discovery against Hizballah. 100 +MB of Hizballah Unit 1800 data has been collected and ingested into XKEYSCORE. S2I22 confirms CADENCE dictionary and XKEYSCORE fingerprint hits. NSA SIGINT Enterprise analysts can now conduct SIGDEV on any target IP range of interest in Lebanon using a single passive database [US-3105S8] in XKEYSCORE.

(TS//SI//NF)