NSA/CSS Threat Operations Center

Cyber Profiling and Operations Support (V43)

(U) MORECOWBELL

(S//REL) A Covert HTTP/ DNS Monitoring System for Operations Support

(U) Topics

- (U) What is MORECOWBELL?
- (U) What are the benefits?
- (U) How does it work?
- (U) Architecture
- (U) Future Work

(U) What is MORECOWBELL?

- (S//REL) MORECOWBELL (MCB) is a V43 developed system used to support V3 and JFCC-Network Warfare Operations
- (S//REL) Built on the PACKAGEDGOODS infrastructure and cover mechanisms.
- (S//REL) Deployed on a covered infrastructure on the public Internet
- (S//REL) Performs DNS lookups and HTTP requests against targets on regular intervals
- (S//REL) Used to track changes to DNS resolution as well as up/down status of websites

(U) Benefits

- (S//REL) MCB enables the NTOC to monitor thousands of Internet websites in near real-time
  - (S//REL) Foreign government websites
  - (S//REL) Terrorist/Extremist web forums
  - (S//REL) Malware Domains (callback or beacon addresses)
  - (S//REL) U.S. Government websites via Request for Technical Assistance from Homeland Security
- (S//REL) Currently used to support Battle Damage Indication after CNA and for Situation Awareness
- (S//REL) OPSEC: unattributable to the USG

(U) How Does it Work?

- (U) Consists of:
  - (U//FOUO) Central tasking system housed in V43 office Spaces
  - (S//REL) Several covertly rented web servers (referred to as bots) in: Malaysia, Germany, and Denmark
- (S//REL) The MCB bots utilize open DNS resolvers to perform thousands of DNS lookups every hour.
- (S//REL) MCB bots have the ability to perform HTTP GET requests (mimicking a user's web browser)
- (S//REL) The data is pulled back to the NSA every 15-30 minutes
- (S//REL) Data Currently available on NSANet via web services