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

(U//FOUO) NSA's Offensive and Defensive Missions: The Twain Have Met

FROM: [redacted]
NSA/CSS Threat Operations Center (NTOC) Hawaii
Run Date: 04/26/2011

(U//FOUO) A push to allow closer interaction between NSA's offensive and defensive missions has been underway for years now -- since at least 2003. Has it been successful, and if so, what have we gained*

from it? Here's a success story demonstrating that we are indeed seeing concrete benefits right now from "mission blending":

(TS//SI//REL) Years ago it would have been hard to imagine that NSA's defensive side of the house (Information Assurance) and its offensive (SIGINT) mission could work together and allow NSA to collect ***other people's*** SIGINT, but that is exactly what is happening as we speak.

(S//REL) Our story begins in July 2009 at the NSA/CSS Threat Operations Center (NTOC) -- an organization with a blended foreign intelligence (SIGINT) and information assurance mission. While analyzing malicious files targeting DoD users, NTOC personnel at Fort Meade discovered an IP address of a command-and-control node being used by Asia-based hackers associated with an organized series of intrusions known as BYZANTINE RAPTOR. (Note this success story started with a tip from the computer-network defense side of the house.)

(TS//SI//REL) With this IP address in hand, SIGINTers (specifically SID's Tailored Access Operations (TAO/S32)) were able to get sustained collection on this C2 node. Consequently, NTOC-Hawaii has enjoyed visibility into data that BYZANTINE RAPTOR is routing through the node. This data includes tasking and collection from a Chinese computer-network exploitation (CNE) operation against the United Nations.

(TS//SI//REL) This collection occasionally includes documents China has stolen from the United Nations network. Since NSA has sustained collection on this C2 node, we can intercept these same documents. In effect, NSA is able to tap into Chinese SIGINT collection -- a phenomenon called "Fourth Party collection."**

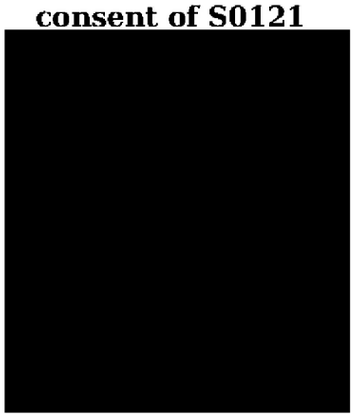
(TS//SI//REL) The collection is sent to the PINWALE raw-traffic database for corporate storage and retrieval. Whenever new documents are sent to PINWALE, NTOC-Hawaii tips off target analysts in S2. As a result, S2's UN target office has issued three SIGINT reports based on this "Fourth Party collection," all dealing with high-interest, high-profile current events.

(U//FOUO) This is a tremendous example of the entire NSA -- the offensive and defensive missions, headquarters and field -- truly operating as a single enterprise, with analysts and collectors connecting data in non-traditional ways to get intelligence to our customers.

(U) Notes:

* (U/FOUO) Ref: DIRgram-290 ("Transformation 2.0 - The Next Step"), the first "strategic thrust." Also, for background on what drove mission blending, see this SID*today* interview with former IAD Chief [redacted], question 4.

** (S//SI//REL) See a related article for background on 4th Party collection.



DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL
DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007
DECLASSIFY ON: 20320108