(TS//SI//REL) The Wizards of OZ II: Looking Over the Shoulder of a Chinese C2C Operation

FROM: [redacted]
MUSKETEER, NSA's Special Deployments Division (S3161)
Run Date: 08/28/2006

(TS//SI//REL) A US SIGINT collection team carried out a survey in Beijing and discovered that the Chinese were covertly extracting files from a foreign embassy. The US team not only succeeded in collecting the files themselves, but also learned about Chinese methods for conducting C2C operations.

(TS//SI//REL) **Once upon a time in China...** a joint MUSKETEER/Special Collection Service (SCS) team deployed to Beijing to survey 802.11 wireless LAN targets for sustained collection. The MUSKETEER OZ II survey revealed several high-interest targets accessible from US-968U (Beijing), including the embassies of India, Singapore, Pakistan, Colombia, and Mongolia.

(TS//SI//REL) While analyzing the Indian Embassy's diplomatic communications, the team discovered that possibly Chinese Government-sponsored entities have compromised several of the computers inside the Indian Embassy. The analysis of outgoing communications showed that someone was exfiltrating approximately ten sensitive diplomatic documents per day through covert channels to drop box hosts located on the public Internet. Exfiltrated files were often Microsoft Office-compatible files or Adobe PDF documents.

(TS//SI//REL) The team identified the procedure by which the files are being exfiltrated and tasked them for sustained collection. This action provided access to sensitive Indian diplomatic files that otherwise would not have been collected because of the high level of encryption employed on the Indians' outgoing communications.

(TS//SI//REL) Additionally, the findings gave insight into how the Chinese conduct computer-to-computer (C2C) operations against foreign targets. Experts from the NTOC (NSA/CSS Threat Operations Center) have confirmed that this activity fits the standard operating procedure for PRC network attacks. MUSKETEER OZ II findings have allowed NTOC analysts to locate this type of Computer Network Exploitation by the PRC in several other locations.

(U) The team came, conquered, and went home. After all, there's no place like home!