June 2010

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) [redacted], Chief, Access and Target Development (S3261)

(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away… In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network. Upon initiating the survey, SIGINT analysts from TAO/Requirements & Targeting determined that the implanted device was providing even greater accesses than we had hoped: We knew the devices were bound for the Syrian Telecommunications Establishment (STE) to be used as part of their internet backbone, but what we did not know was that STE's GSM (cellular)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20350501

network was also using this backbone. Since the STE GSM network had never before been exploited, this new access represented a real coup.

(TS//SI//NF) TAO is now able to automatically exfiltrate call detail records (CDRs) containing billing information from STE, showing subscribers' interlocutors and their geographic locations. This access has, in turn, enabled access to CDRs from other GSM networks in the region, including GPRS data as well as the exploitation of a GSM switch that provides target voice content exfiltration. A very successful operation!

(U//FOUO) Want to know more about AO? Type "go AO" in your browser.

(U//FOUO) POC: [redacted]