IN FOCUS

21 Apr 2014

ACCESSING THE INACCESSIBLE

Part I: NSA's DIGITAL Tools of espionage

E. Dilipraj
Research Associate, CAPS

> *"Collect (**including through clandestine means**), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;"*[1]
>
> \- Mission Statement,
> National Security Agency

National Security Agency (NSA) has been in the news since mid-2013 for all wrong reasons especially for its infamous PRISM program. While clandestine means of collecting information is the mission statement for them, it is not a surprise that an intelligence agency like NSA of the USA, has indulged in mass surveillance programs by collecting information from both accessible and inaccessible locations all around the world in the past few years. But the surprising factor is the magnitude and the technological luxuries used for this purpose by the agency. The PRISM program is one of the projects that are operated by NSA for their data mining purpose and more similar projects on various platforms in much bigger magnitude also exist.

One such program is the NSA's sophisticated digital toolbox called the "NSA ANT Catalogue" which was revealed in *Der Spiegel*, the German weekly news magazine, in December 2013, in an article co-written by Jacob Appelbaum, Judith Horchert and Christian Stöcker. Unlike the PRISM program which was exposed by Edward Snowden to The

Washington Post and The Guardian, the exposure/whistleblower of this project is unknown. But the exposed catalogue reveals the magnitude and variety of digital weapons being used by the US intelligence agency to spy on its targets.

"The leaked NSA ANT Catalogue is a 50 page document created in 2008. Its list goes like a mail-order catalogue of digital tools, from which, the employees of NSA can order technologies from the ANT division to use it against its targets. The Advanced/ Access Network Technology (ANT) division is part of NSA's Tailored Access Operations (TAO) Department and they are specialized in covert data-mining and data-skimming operations especially on specific difficult targets. ANT tools are like elite forces which are moved in only when TAO's usual hacking and data-skimming methods are not sufficient to gather the required information from their target systems."[2]

ARTICLES BY SAME AUTHOR

INDIA STRENGTHENS TIES WITH SOUTH KOREA IN CYBER SECURITY

INDIA CHALLENGES CHINA IN LAC

BRICS' CABLE AND CYBER SECURITY

NATURAL OR TARGETED' ALLY

"The TAO department of NSA is believed to be operating from a base in Texas, which was earlier a Sony Chip Company and later converted into NSA's operative location in 2005. The operations of ANT division range from penetration of network, monitoring mobile phones, computers, to diverting, modifying and even deleting data. The network web created by the implants of these sophisticated tools is so big that it has succeeded in establishing a covert network for NSA that operates parallel to the internet. While the ANT division develops both hardware and software required for these digital tools, the catalogue of these tools not only defines the operations of the tools but also gives the cost for every tool which ranges from free to $250,000."[3]

Image: The location of NSA's TAO department.
Source: Google Earth.

Every tool that has been developed by ANT has its own special purpose and their operating devices include almost all areas of the digital world from Monitors, Cables, USBs, Routers, Servers to Radio Waves. The digital tools of NSA ANT are listed below by categorising them according to their operating device/ area:

Operating Device/Area	Tools	Operating Platform
VGA (Monitor)	• RAGEMASTER	Hardware
Firewalls	• JETPLOW	Software
	• HALLUXWATER	Software
	• FEEDTROUGH	Software
	• GOURMETTROUGH	Software
	• SOUFFLETROUGH	Software
Mobile Phones	• DROPOUTJEEP	Software

	• GOPHERSET	Software
	• MONKEYCALENDER	Software
	• TOTECHASER	Software
	• TOTEGHOSTLY 2.0	Software
	• PICASSO	Software
	• CROSSBEAM	Hardware
	• CANDYGRAM	Hardware
	• CYCLONE Hx9	Hardware
	• EBSR	Hardware
	• ENTOURAGE	Hardware
	• GENESIS	Hardware
	• NEBULA	Hardware
	• TYPHON HX	Hardware
	• WATERWITCH	Hardware
Router	• HEADWATER	Software
	• SCHOOLMONTANA	Software
	• SIERRAMONTANA	Software
	• STUCCOMONTANA	Software
Server	• DEITYBOUNCE	Software
	• GODSURGE	Hardware

	IRONCHEF	Hardware
USB	COTTONMOUTH I	Hardware
	COTTONMOUTH II	Hardware
	COTTONMOUTH III	Hardware
	FIREWALK	Hardware
LAN	NIGHTSTAND	Hardware
	SPARROW II	Hardware
For Surveillance and as Radars	CTX4000	Hardware
	LOUDAUTO	Hardware
	NIGHTWATCH	Hardware
	PHOOANGLO	Hardware
	TAWDRYYARD	Hardware
Computers	GINSU	Software
	IRATEMONK	Software
	SWAP	Software
	WISTFULTOLL	Software
	SOMBERKNAVE	Software
	HOWLERMONKEY	Hardware
	JUNIORMINT	Hardware
	MAESTRO-II	Hardware

	• TRINITY	Hardware
Keyboards	• SURLYSPAWN	Hardware

Table: List of NSA ANT Products
Source: Appelbaum, Jacob. December 30, 2013.

Most of these NSA ANT products listed above are part of a bigger product family called "ANGRYNEIGHBOR". It is with this information, some inferences can be made that there would be more such products in the family or can be worse, that there can be more families of products available with NSA for its covert operations. Alongside this and more wide range of products and its technical complexity, the most fearful factor for a common user is that, these products are implanted in the most widely used US brands around the world like Apple, Cisco, Dell, Juniper Networks, Maxtor, Seagate, and Western Digital which means no digital information is safe from NSA's eyes and ears.[4] However, these companies have denied that their devices are being used by NSA for its covert espionage purposes and a few companies have also promised its customers about its product safety.

Under such circumstances, it is wise for the countries to be aware of their digital product suppliers and to conduct frequent audits on their digital infrastructures which would help in identifying hardware implants if any. Also digital information and infrastructure security becomes more important in the defence sector as these are the networks which are most sorted by any covert espionage programs.

More information about the working and functionality of every tool of NSA ANT listed above would be available in subsequent parts in the series titled "Accessing the Inaccessible".

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies - CAPS)

End Notes

[1] http://www.nsa.gov/about/mission/, accessed on April 6, 2014.

[2] Appelbaum, Jacob and et al. , "Die Klempner aus San Antonio", *Der Spiegel,* January 2014.

[3] "Inside TAO: Documents Reveal Top NSA Hacking Unit", *Spiegel Online International*, December 29, 2013, at http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html, accessed on April 6, 2014.

[4] Appelbaum, Jacob and et al. , "Shopping for Spy Gear: Catalog Advertises NSA Toolbox", *Spiegel Online International*, December 29, 2013, at http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html, accessed on April 6, 2014.