Centre for Air Power Studies

ACCESSING THE INACCESSIBLE

PART VII – NSA'S ESPIONAGE TOOLS FOR MOBILE PHONES

E. Dilipraj
Research Associate, CAPS

The NSA's ANT department's digital tools of espionage which has been discussed in the series titled "Accessing the Inaccessible", has so far covered various tools meant to conduct surveillance and espionage on USBs, VGAs, Keyboards, CPUs, W-Lan, Router, Firewalls & Servers, and also for conducting audio and visual surveillance. As the final part of the series, the paper aims to discuss in detail the NSA's ANT department's various tools of espionage on mobile phones and mobile networks. These tools were exposed in the German weekly *Der Spiegel* in December 2013.

In the 21st century, mobile phones have become an indispensible part of human life thereby creating an invisible network of communication across the globe. According to reports from International Telecommunication Union (ITU), till 2012, the number of mobile phone connections has crossed 6 billion and is expected to cross more than 7 billion by the end of 2014. Out of these 6 billion connections, nearly 1.1 billion are mobile internet facilities.[1] The data clearly signifies that mobile phones and mobile networks are the technology for modern day communication through which bulk of information flows across the world every single second. Therefore, in the age of information, use of mobile technology is risky especially during sensitive information communication because both devices as well as networks are vulnerable targets for the wealth of information readily available in it.

In order to harness this information for intelligence purposes; the NSA has developed number of tools which are used as implants on the devices, and the mobile networks. Although,

gathering intelligence is a widely accepted phenomenon, the fact that privacy of individuals would be compromised for such a purpose is an unacceptable condition. Moreover, it is not only the privacy of common man which is under question, but at times, even the heads of states have to face the wrath of digital espionage which leads to questioning the legitimacy of intelligence gathering through clandestine operations.

However, this part of the series, as mentioned above, focuses into the various tools of espionage on mobile phones and networks which were developed by NSA's ANT department, revealed in late 2013. The documents divulged 15 different tools which were developed for this purpose by the ANT department way back before 2007. These tools can be divided into two broad categories – (a) tools meant for mobile phone devices and (b) tools meant to operate on mobile networks.

Tools for Mobile Devices

DROPOUTJEEP

DROPOUTJEEP, is a software implant for Apple iphone operation system which uses an undisclosed framework called CHIMNEYPOOL to provide specific signal intelligence. This implant can be used to remotely push or pull files from the mobile device including SMS, contacts, voicemails, geographic location, room audio through hot mic, camera visuals, mobile tower location, etc. Through SMS or GPRS connectivity, the command, control and exfilteration of data from the implanted device can be achieved covertly and in encrypted format.[2] Although this implant was in the development phase during 2007, it is believed that the ANT department would have succeeded in developing this technology later.

TOTEGHOSTLY 2.0

TOTEGHOSTLY 2.0, is again a software based implant but meant for the windows operating system based mobile devices, to provide specific signal intelligence. Its functions remain similar to DROPOUTJEEP, except the fact that this implant operates on windows based mobile devices and also was under development in 2007.[3]

GOPHERSET

GOPHERSET, is a software implant for GSM (Global System for Mobile Communications) based SIM (Subscriber identification Module) cards. This implant is used to extract phonebook, SMS and the call log information from the target device and sends to a user-defined phone number via SMS. Exploiting the SIM Toolkit interface, the interface which issues commands and makes requests to the device – GOPHERSET retrieves the information from the target. This implant is loaded to the target's SIM card either using a USB smartcard reader or via over-the-air provisioning.[4]

MONKEYCALENDER

MONKEYCALENDER, is again a software implant for GSM (Global System for Mobile Communications) SIM (Subscriber identification Module) cards. This implant retrieves the geographic location information from the target's handset and sends it to the user defined phone number via SMS. The functioning and installation process of this implant resembles that of GOPHERSET.[5]

TOTECHASER

TOTECHASER, is a specially built software implant for Thuraya 2520 handset. This implant exploits the Windows CE operating system of the device. Thuraya 2520, is an advanced smart phone that functions as a 3-in-1 integrated handset with satellite, GSM (Tri-band), and GPS connectivity.[6] This implant is used to extract information like GPS and GSM geo-location, call log, contact list and other user information from the phone. The implant uses SMS messaging for command, control and data exfiltration path both in satellite mode and GSM mode without alerting the target. The TOTECHASER system consists of the modified handsets and a collection system.[7]

PICASSO

PICASSO, is the technology for modifying handsets which are used to collect data, location information and even room

audio. Command and Data exfiltration is done from a laptop and via regular phone via SMS without alerting the target. The data exfilterated through these modified handsets includes call log, recently registered networks, Geo-location codes, room audio using hot mic, recent successful PINs entered into the phone during the power-on cycle, phone number when the phone is turned on – in case new SIM has been used. Apart from these the controller can also block calls to deny service to the device. The device models which are used for this purpose are Eastcom 760c+, Samsung E600, X450 and Samsung C140 and the cost for making one unit with this technology is approximately $2500.[8]

CROSSBEAM

CROSSBEAM, according to the revealed documents is a GSM module that mates a modified commercial cellular product with a WAGONBED controller board. This tool is capable of collecting and compressing voice data. It can also receive GSM voice, record voice data and transmit the received information via connected modules or 4 different GSM data modes (GPRS, Circuit Switched Data, Data Over Voice and DTMF) back to a secure facility. The cost of one unit of this tool is $4K.[9]

GENESIS

GENESIS, is a technology that is used as a covert signal intelligence transceiver through a modified commercial GSM handset. A commercial GSM handset is modified to include Software Defined Radio (SDR) and additional system memory. This SDR allows a witting user to covertly perform network surveys, record Radio Frequency spectrum or perform handset

PREVIOUS PARTS

"ACCESSING THE INACCESSIBLE" PART I: NSA's DIGITAL TOOLS OF ESPIONAGE

PART II: KEYBOARDs, USBs & VGAs

PART III: NSA'S TOOLS OF ESPIONAGE ON COMPUTERS

PART IV: NSA'S TOOLS OF ESPIONAGE IN W-LAN AND ROUTER

PART V: NSA'S TOOLS OF ESPIONAGE IN FIREWALLS AND SERVERS

PART VI: NSA'S DIGITAL RADARS FOR AUDIO AND VISUAL SURVEILLENCE

More Articles

location in hostile environments. This modified handset has a concealed SDR, external antenna port, 16GB internal memory, multiple internal antennas, spectrum analyser capability and integrated Ethernet facilities. The cost of one unit of such modified handset is $15K.[10]

Tools for Mobile Networks

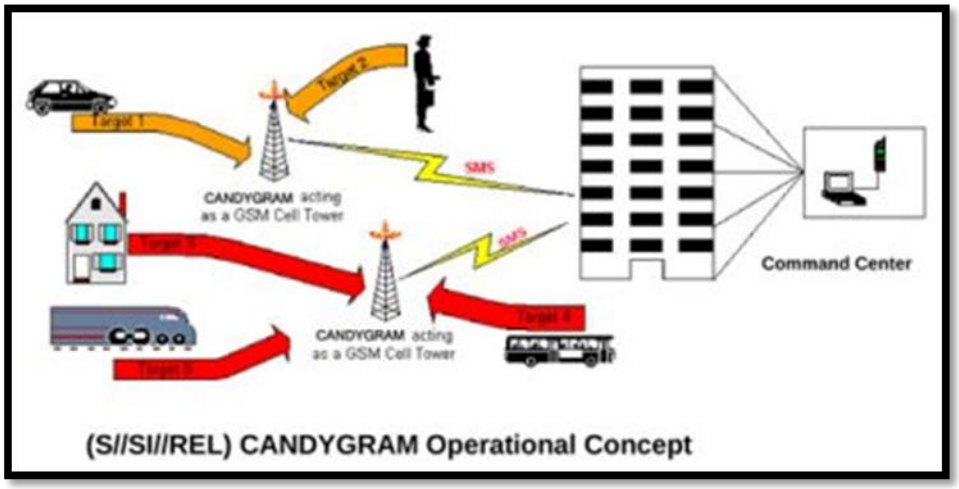
WATERWITCH

WATERWITCH, is a hand held detection tool used for geo-location targeted handsets in the field. This is a tactical tool used by operators on the field to locate the targeted handsets. This tool has an external antenna for target detection and an internal antenna for communication with active interrogator, and also the device uses E-ink technology in its display for low light emissions. The tool possesses multiple technology capability based on SDR platform.[11]

CANDYGRAM

CANDYGRAM, is not one single tool but a setup of devices that mimics the GSM cell phone tower of a target network. When the target handset enters the area of influence of CANDYGRAM base station, the system sends out an SMS to the registered watch phones through an external network. This system operates on the frequency of 900, 1800 and 1900 MHz. Following are the scenarios in which CANDYGRAM can be employed:

- for asset validation,
- for target tracking and identification and
- for identifying hostile surveillance units with GSM handsets.



Source: "Product Data – CANDYGRAM", NSA ANT Catalogue, USA.

The technology has unique features like automatic network configuration, capable of configuring 200 phone numbers in its target deck, remote restart and data erasure.[12]

CYCLONE Hx9

CYCLONE Hx9, is a Network-In-a-Box (NIB) system which uses the existing Typhon Graphical User Interface and supports the full Typhon feature base and applications. This tool is a base station router, when employed provides network for field operations. This tool has a range of more than 32 Km and it can handle voice and high-speed data transfer.[13]

EBSR

EBSR, is a low power tri-band active GSM base station interrogator with internal 802.11/GPS/handset capability. This device is used in the operations on the networks. This has two models namely LxT and LxU with voice and high-speed Data capability and also SMS capability.[14]

ENTOURAGE

ENTOURAGE, is a direction finding software application operating on the device called HOLLOWPOINT. This whole system is capable of providing line bearing for GSM/UMTS/CDMA200/FRS signals. This software application works in conjunction with another base station router called NEBULA to achieve Find/Fix/Finish capabilities of the GALAXY program.[15]

NEBULA

NEBULA, is a base station router and a Network-In-a-Box system. The cost of one unit of this device is $250K. This device supports GSM, UMTS, CDMA2000 applications at the ranges of 900, 2100 and 1900 MHz respectively.[16]

TYPHON HX

TYPHON HX, is a base station router and Network-In-a-Box (NIB) system supporting GSM bands 850/900/1800/1900 and associated full GSM signaling and call control. This equipment is used in tactical operations to find, fix and finish targeted handset users. Using this equipment it is possible for the operators to geo-locate the handset and the user.[17]

Inferences gathered from the study on NSA ANT Catalogue

A study on understanding the functions and operational capabilities of the 50 NSA ANT tools in this series helped to arrive at the following inferences:

- These tools are meant for special operations which are highly covert in nature for the purpose of information gathering, sabotage, espionage and surveillance.
- The functionality of the tools can be mainly associated with military operations, but not necessarily be confined to military only, as few tools like COTTONMOUTH can also be used for non-military operations.

- Few tools belong to a family of tools called ANGYNEIGHBOR, which denotes that there are more families of tools either under operation or development.
- All the disclosed documents related to NSA ANT catalogue are dated in the year 2007. Therefore, there are high chances for these tools to have become obsolete and new versions and models of tools would have replaced them by now.
- There are passing references to many new technologies whose functionalities do not appear in any of the exposed documents. This means that there are many more undisclosed tools developed by ANT department whose capabilities are unknown.
- The fact that these tools being revealed to the world would have created a compulsion for the agency to either abandon these tools on the whole or switch to more covert methods of espionage and surveillance.
- In case of abandoning, the agency would have abandoned many units of these tools which were operational in the field somewhere across the globe. Identifying and investigating these tools, if any other country's agencies could lay hands on them might uncover more precise capabilities about the tools.
- Many implant both hardware and software are implanted on devices manufactured by most widely used brands like Samsung, Cisco, Juniper, etc. Therefore, this results in distrust on US brands which in turn create more hassles for any country's procurement body in terms of rigorous audit during procurement of any such devices from US especially for national security purposes.
- It is also revealed from the documents that the NSA implants few of their tools by a method called interdiction, in which the agency would intervene during the supply chain process and place their implant on the devices before it gets delivered to its intended recipient. This emphasizes the need for enhancing safety for any supply-chain process especially for defence equipments irrespective of their size or function.
- The fact that many implants can be installed, controlled, operated and executed remotely, emphasizes the need for enhanced network security and also acts as a point of realization for disintegrating and isolating few sensitive networks from other national grids.

(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] "World to have more mobile connections than people by 2014", NDTV Gadgets, 11 December 2012, in http://gadgets.ndtv.com/mobiles/news/world-to-have-more-mobile-connections-than-people-by-2014-304001, accessed on 20 November 2014.

[2] "Product Data – DROPOUTJEEP" NSA ANT Catalogue, USA.

[3] "Product Data – TOTEGHOSTLY 2.0", NSA ANT Catalogue, USA.

[4] "Product Data – GOPHERSET", NSA ANT Catalogue, USA.

[5] "Product Data – MONKEYCALENDAR", NSA ANT Catalogue, USA.

[6] "Thuraya SG-2520 Brochure", Thuraya Products.

[7] "Product Data – TOTECHASER", NSA ANT Catalogue, USA.

[8] "Product Data – PICASSO", NSA ANT Catalogue, USA.

[9] "Product Data – CROSSBEAM", NSA ANT Catalogue, USA.

[10] "Product Data – GENESIS", NSA ANT Catalogue, USA.

[11] "Product Data – WATERWITCH", NSA ANT Catalogue, USA.

[12] "Product Data – CANDYGRAM", NSA ANT Catalogue, USA.

[13] "Product Data – CYCLONE Hx9", NSA ANT Catalogue, USA.

[14] "Product Data – EBSR", NSA ANT Catalogue, USA.

[15] "Product Data – ENTOURAGE", NSA ANT Catalogue, USA.

[16] "Product Data – NEBULA", NSA ANT Catalogue, USA.

[17] "Product Data – TYPHON HX", NSA ANT Catalogue, USA.
