Centre for Air Power Studies

ACCESSING THE INACCESSIBLE

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

E. Dilipraj
Research Associate, CAPS

The US National Security Agency's (NSA) ANT department's technical expertise and sophistication in the field of espionage especially on computer equipments amuses its admirers while at the same time annoys its victims. The NSA's tools of digital espionage exposed by *Der Spiegel,* the German Weekly is a proof in itself as the catalogue exhibits the variety of tools that are being used for espionage purposes by NSA across the globe on their targets' computer devices. Having looked at the detailed list of tools, the tools of espionage on Keyboards, USB's and VGAs and also on Computers in the previous parts of this 'In Focus' series, this part will explain how NSA uses its advanced tools to exploit network devices like W-LAN and Router for their covert espionage operations.

The NSA ANT catalogue has two tools for tapping into a LAN, namely, NIGHTSTAND and SPARROW II and four tools for tapping into a router, namely, HEADWATER, SCHOOLMONTANA, SIERRAMONTANA and STUCCOMONTANA.

W-LAN

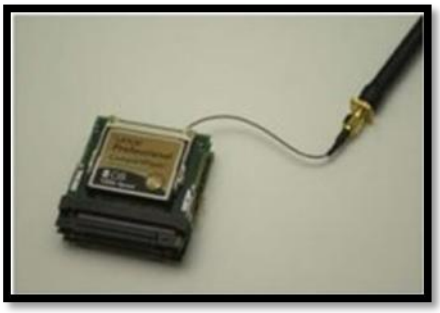
The NSA ANT tools for tapping into the W-LAN detects the wireless networks from a considerable distance and it can be used to either tap into the network or to map the various networks in a particular jurisdiction.

NIGHTSTAND

NIGHTSTAND is used in operations where wired connectivity to the target's system is impossible and hence is used to exploit the active wireless LAN of the target and inject payload like a malware. This tool is used for exploitation of Windows Operating System and has a history of successful battle field operations. NIGHTSTAND is a standalone tool running on x86 Laptop loaded with Linux Fedora Core 3 Operating System.[1]

This tool has the ability to exploit targets running on Win2k, WinXP, WinXPSP1 and WINXPSP2 operating systems and using Internet Explorer versions 5.0 to 6.0. This tool also has the capability to target multiple clients or multiple targets simultaneously. This tool has a successful operational range of 8 miles or 13 Kms while the unit cost varies from platform to platform.[2] Should the target uses the latest version of Windows Operating System or a different operating system like Linux and uses updated version of internet explorer or any other browser, then the user has the opportunity to escape from this tool.

SPARROW II



SPARROW II is one of the most sophisticated tools in the NSA ANT Catalogue. It is used in airborne operations especially on board an UAV. This tool is embedded with the software tool called BLINDDATE (another software tool which is not listed in the exposed NSA ANT catalogue). It is also integrated with Mini PCI slots for added functions like GPS and multiple Wireless Network Interface Cards. This tool collects the WLAN networks from the specified location and maps them. This tool also gives the option for connecting more PCI devices to it for the purpose of wireless command and control or to install second or third 802.11 card. The unit price of this tool is $6K.[3]

ROUTER

A Router is a computer network device that is used to forward data packets between various networks thus forming interlink of networks.[4] The NSA ANT department has managed to develop tools to exploit these router devices and according to the exposed catalogue the tools can exploit routers of two manufacturers: Huawei and Juniper. While HEADWATER tool is deployed to exploit Huawei routers, the Juniper routers are exploited by using SCHOOLMONTANA, SIERRAMONTANA and STUCCOMONTANA tools.

HEADWATER

Huawei is the second most popularly used networking device in the world after CISCO. The fact that Huawei is a Chinese brand, makes it vulnerable to attacks from the US as both China and USA are in a virtual technological race amongst themselves. Therefore, the NSA ANT department has devised the tool HEADWATER exclusively for exploiting the Huawei manufactured routers. It is a Persistent Backdoor (PBD) software implant which enables covert functions to be remotely executed within the router via an internet connection. The software tool will be installed in the router's boot ROM and will get activated after a system reboot. After activation, the PBD software captures and examines all IP packets passing through the router. This tool is also adapted in joint operations between NSA and CIA again to exploit Huawei Network equipments under the cover name TURBOPANDA.[5]

ARTICLES BY SAME AUTHOR

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

INDIA STRENGTHENS TIES WITH SOUTH KOREA IN CYBER SECURITY

INDIA CHALLENGES CHINA IN LAC

BRICS' CABLE AND CYBER SECURITY

NATURAL OR TARGETED' ALLY

SCHOOLMONTANA

Juniper is an American network manufacturing company which manufactures five families of routers: T-series, M-series, E-series, MX-series, and J-series and other networking devices. The NSA ANT tool SCHOOLMONTANA is designed to exploit the J-Series routers of the Juniper devices. This tool provides persistence for Digital Network Technologies (DNT) implants. When this tool is deployed, it modifies the target system's BIOS and adds the necessary software to it which can be executed remotely by handler.[6]

SIERRAMONTANA

Like SCHOOLMONTANA, another tool, SIERRAMONTANA, exploits the M-Series of Juniper router devices and deploys a DNT implant into the target's BIOS. After the implant, once the system is rebooted, the implant provides kernel modifications to support the execution of implant remotely by handler.[7]

STUCCOMONTANA

Similarly, the STUCCOMONTANA tool of NSA ANT provides persistence for DNT implants on the Juniper T-Series routers and its functions are similar to that of its contemporaries, SCHOOLMONTANA and SIERRAMONTANA.[8]

All three tools that exploit the Juniper router devices can survive BIOS Modifications and software upgradation.

More information about the working and functionality of many more tools of NSA ANT 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] Jacob Appelbaum , "NSA ANT W-Lan", 30C3, December 30, 2013.

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

[3] "Product Data – SPARROW II", NSA ANT Catalogue, USA.

[4] http://en.wikipedia.org/wiki/Router_(computing), accessed on August 02, 2014.

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

[6] "Product Data – SCHOOLMONTANA", NSA ANT Catalogue, USA.

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

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