Centre for Air Power Studies

ACCESSING THE INACCESSIBLE

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

E. Dilipraj
Research Associate, CAPS

With the aim of taking a look into the complicated espionage tools of the Advanced/ Access Network Technology (ANT) Department of the National Security Agency's (NSA) of the US, this series has so far covered the detailed list of tools, the tools of espionage on Keyboards, USB's and VGAs, the tools of espionage on personal Computers, and also the tools of espionage on W-LANs and Routers. Having been exposed by *Der Spiegel,* the German Weekly this NSA ANT tools catalogue has not gained much global audience due to the complexity in understanding the technologies behind ever tool and also because of the fact that only a small list of tools has been exposed which makes the understanding incomplete.

Nevertheless, this part of the series would try to look into the NSA ANT tools specially designed to conduct espionage by breaching the Firewalls and reaching the Servers. In the world of computing, Firewalls are software or hardware based network security systems which act as a barrier between a secured domestic network or a personal computer and the external network which is generally considered not so well secured. Similarly, Servers are computer systems which run applications i.e. softwares that are capable of accepting and processing requests from clients and responding to them accordingly. Due to the constant interaction with the client systems, servers are always well secured to avert any interuption in the connection and also to avoid loss of sensitive data.

But, the fact that NSA ANT tools are able to breach the firewalls and the security of servers make it an interesting subject to study from the aspect of cyber security. According to the exposed catalogue, there are three tools for exploiting Servers namely DEITYBOUNCE, GODSURGE & IRONCHEF and five tools for exploiting the Firewalls namely JETPLOW, HALLUXWATER, FEEDTROUGH, GOURMETTROUGH & SOUFFLETROUGH.

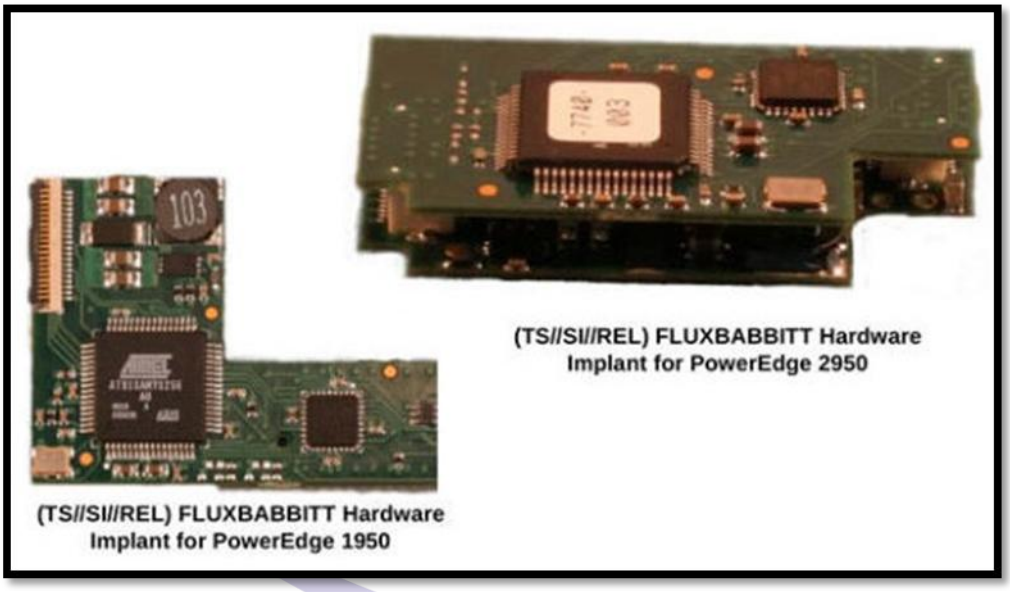
Server

DEITYBOUNCE

DEITYBOUNCE is a software application which exploits the motherboard BIOS and utilises the System Management Mode (SMM) in order to periodically execute itself while the operating system loads. The limitation of this tool is that it can exploit only Dell PowerEdge Servers which are using particular BIOS versions namely A02, A05, A06, 1.1.0, 1.2.0 and 1.3.7. DEITYBOUNCE can be installed into the target system either by interdiction or by using a technique called ARKSTREAM. While ARKSTREAM is a virtual technology to reflash the software into the target system, interdiction is a physical method in which an USB contaning the software installer is inserted into the target system to install the application. Once installed, DEITYBOUNCE's execution is configurable and it comes to life when the target system powers on.[1]

GODSURGE

GODSURGE is a software application persistence tool, again directed against the Dell PowerEdge servers to exploit the JTAG debugging interface of the server's processors. This software application runs on the hardware implant called FLUXBABBIT, which is again a espionage tool of ANT whose technologies has not been exposed so far.[2]



For GODSURGE to conduct its task, the target system has to be rightly fitted with JTAG scan chain and the hardware implant FLUXBABBIT through interdiction. FLUXBABBIT has to be pre-programmed with GODSURGE application code, the payload and the implant installer. Once the target system powers on GODSURE will occur and its frequency of execution is configurable. The cost of FLUXBABBIT hardware implant and to install GODSURGE in it is together estimated to be $500.[3]

IRONCHEF

IRONCHEF enables access persistence to communicate with the hardware implant like UNITEDRAKE and STRAITBIZARRE which provides two way Radio Frequency (RF) communications. This technique is supported by HP Proliant 380DL G5 model server. Interdiction is the technique which is used to install IRONCHEF, the software implant and the hardware implant into the target system. Even if the software implant is removed from the machine, IRONCHEF can be used to access the machine, determine why the software was removed and also to reinstall the software from a nearby listening post to the target system.[4]

Firewalls

JETPLOW

JETPLOW is a software persistent application for the BANANAGLEE software implant that is used to exploit Cisco PIX Series and ASA Firewalls. It also has the capability to act as a back door persistent. JETPLOW gives persistence to BANANAGLEE software implant to modify the Cisco firewall's operating system (OS) during the booting stage. Even if BANANAGLEE software is found unsuppotable during booting the operating system, JETPLOW provides a back door capability through which the OS can be modified and even BANANAGLEE can be installed later through the back door. JETPLOW can also be remotely installed provided BANANAGLEE already exists at the target.[5]

HALLUXWATER

HALLUXWATER is a persistent back door implant designed specially for Huawei Eudemon firewall to function as a boot ROM upgrade. HALLUXWATER gives covert access to the NSA operator to read and write memory, execute an address or a packet using a TURBOPANDA insertion tool. This implant has the capability to survive boot ROM upgrades and even OS upgrades.[6]

FEEDTROUGH

FEEDTROUGH is a persistence providing technique for two software implants, namely DNT's BANANAGLEE and CSE's ZESTYLEAK. FEEDTROUGH works only against Juniper Netscreen Firewalls. When the firewall is booted the first step taken is to direct the code to check if the OS is in the list of FEEDTROUGH database. If it exists, then a chain of events ensures the installation of either BANANAGLEE or ZESTYLEAK softwares or in some cases both the implants. The limitation of FEEDTROUGH is that it can work only when the OS is listed in its database. According to the exposed document FEEDTROUGH has been deployed in many platforms.[7]

GOURMETTROUGH

GOURMETTROUGH is again a software persistent implant for certain Juniper firewalls. It gives persistence to BANANAGLEE software during reboot and OS upgrades. According to the exposed document GOURMETTROUGH has also been deployed in many target platforms.[8]

SOUFFLETROUGH

SOUFFLETROUGH is a BIOS persistence implant for Juniper firewalls specified to SSG 500 and SSG 300 series. It also has the capability to provide back door persistence. This implant modies the Juniper firewall's OS during booting by persisting the BANANAGLEE software implant. SOUFFLETROUGH is remotely upgradable and it can takes advantage of Intel's System Management Mode (SMM) for enhanced reliability and covertness. The exposed document also reveals that the deployment of this implant is ongoing and there is huge stock available which helps in its deployment.[9]

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

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

More Articles

A carefull look into the exposed documents on firewalls and servers reveals more information in terms of names of few more tools like STRAITBIZARRE, UNITEDRAKE and names of few more departments in NSA like PBD, DNT and CSE. It is little frightning as well as interesting to imagine that when only the ANT department of NSA can create more than 50 tools how many tools and techniques the other departments would have got under their purview ready to use it against their targets.

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] "Product Data – DEITYBOUNCE", NSA ANT Catalogue, USA.

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

[3] Ibid

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

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

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

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

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

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

***