IN FOCUS

25 June 2014

ACCESSING THE INACCESSIBLE

Part III – NSA's tools of espionage on Computers

E. Dilipraj
Research Associate, CAPS

The digital catalogue of NSA's tools of digital espionage, which was exposed in *Der Spiegel*, the German weekly reveal the amount of sophisticated digital tools used by the US to conduct its espionage operations around the world.[1] The 49 tools which got exposed belong to the same family called 'ANGRYNEIGHBOUR' and can be sorted into many categories according to their operating devices/ platforms (see Part I for the categorisation). In these, both hardware and software tools serve their purpose in collecting data from inaccessible devices around the world through unconventional technological means. These tools are designed specifically to function on particular devices ranging from keyboards, USBs, VGAs (see Part 2), to a whole computer/CPU to firewalls, LANs, Servers, Routers, and Mobile Phones and to even act as radars to transfer data to their local data collection centres.

Among the various NSA ANT tools, the specific tools for computers/CPU comprise both hardware and software implants which make it more vulnerable to espionage. Therefore, the tools of espionage on a computer or in other terms a CPU (Central Processing Unit) will be the topic of discussion for this part. The exposed catalogue reveals 9 tools dedicated to computers out of which 5 are software based implants and the remaining 4 are hardware implants. The software based implants are GINSU, IRATEMONK, SWAP, WISTFULTOLL, and SOMBERKNAVE and the hardware based implants are HOWLERMONKEY, JUNIORMINT, MAESTRO – II and TRINITY. "The software implants hide themselves in the master boot

record or even in the BIOS of the computer while the hardware implants are implanted by intercepting the computer during the delivery in a process called by the agency as NSA '**Interdiction**'." [2] In order to understand the functions of these tools in dept, it is essential to study them individually.

GINSU

GINSU is a software application that enables persistence for the CNE software implant KONGUR, which in turn works on the PCI bus hardware implant BULLDOZER, implanted on the target system. During operations, there may be occasions when the software implant KONGUR, which supports the functions of BULLDOZER hardware implant on the PCI bus, is removed from the system due to any upgrade in the operating system or due to reinstallation; in such case, the software implant would be triggered by GINSU on the next reboot of the system.

This technique can operate on any desktop PC system that functions on Microsoft Windows 9x, 2000, 2003, XP or Vista based operating system and has at least one PCI connecter for enabling BULLDOZER implant. This implant comes free of cost.

ARTICLES BY SAME AUTHOR

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

PART II: KEYBOARDs, USBs & VGAs

INDIA STRENGTHENS TIES WITH SOUTH KOREA IN CYBER SECURITY

INDIA CHALLENGES CHINA IN LAC

BRICS' CABLE AND CYBER SECURITY

NATURAL OR TARGETED' ALLY

IRATEMONK

IRATEMONK is another software application that provides persistence by implanting the hard drive firmware on the targeted desktop or laptop which gains execution through Master Boot Record (MBR) substitution. This technique works on many brands of hard drives like Western Digital, Seagate, Maxtor and Samsung, but can boot only from systems which does not have RAID hardware.

The agency uses its technique of Interdiction through the implants like UNITEDRAKE or STRAITBIAZZARE in conjunction with SLICKERVICAR to upload the hard drive firmware onto the machine in order to implant IRATEMONK to the system. Once implanted, IRATEMONK's frequency is configurable and will occur whenever the target system powers on. This implant technology is again free of cost.

SWAP

"SWAP is also a software application that gains periodic execution even before the Operating System loads by exploiting the motherboard BIOS and the hard drive's Host Protected Area. Windows, Linux, FreeBSD or Solaris based single or multi-processor systems support this technique. SWAP and its payload are implanted on the targeted machine through remote access or interdiction. ARKSTREAM is used to reflash the BIOS and TWISTEDKILT is used to write the Host Protected Area on the hard drive of the targeted system to implant SWAP. This is a no cost tool."[3]

WISTFULTOLL

WISTFULTOLL is plug-in software for UNITEDRAKE and STRAITBIZZARE implants and is used for harvesting and returning forensic information from the target system using Windows Management Instrumentation (WMI) calls and Registry extractions. Systems based on Microsoft Windows 2000, 2003, and XP operating systems support this plug-in.

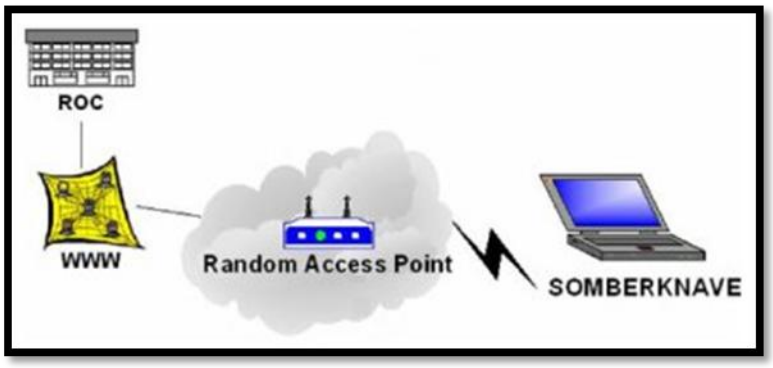
The plug-in is executed through remote access or interdiction, either as a UNITEDRAKE or STRAITBIZZARE plug-in or as a stand alone executable, and the extracted information is sent back to NSA through the hardware implants. If the plug-in is executed via a USB thumb drive then the extracted information is stored in the same thumb drive. This is a no cost tool.

SOMBERKNAVE

"SOMBERKNAVE is a Windows XP software implant that provides covert internet connectivity for isolated systems. This software implant routes TCP traffic from a designated process to a secondary network via an unused embedded 802.11 network device. An air-gapped target computer is connected via 802.11 interface through OLYMPUS or VALIDATOR with the

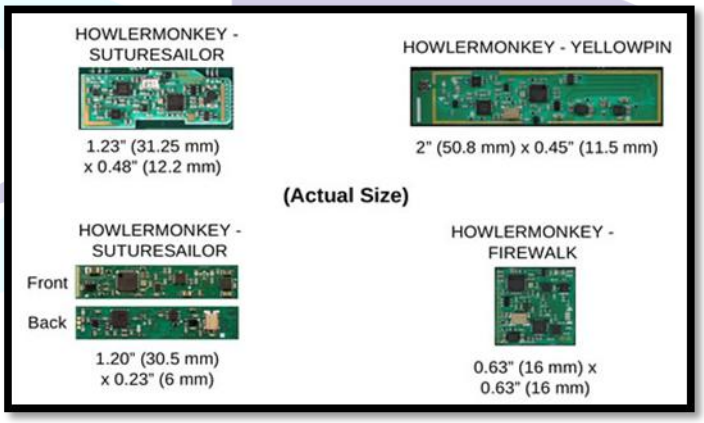
help of SOMBERKNAVE. However, if the 802.11 interface is already in use by the target computer, SOMBERKNAVE will not attempt to transmit."[4]

During operation, VALIDATOR initiates a call and SOMBERKNAVE triggers from the named event and tries to associate with an access point. Once the connection is successful, data is transmitted over the 802.11 interface to the ROC. Receiving the instructions, VALIDATOR downloads OLYMPUS and disassociates itself and gives up the control of 802.11. Now Olympus will be able to communicate with the ROC via SOMBERKNAVE, as long as the access point is available. The cost of one unit of this software implant is $50k.



HOWLERMONKEY

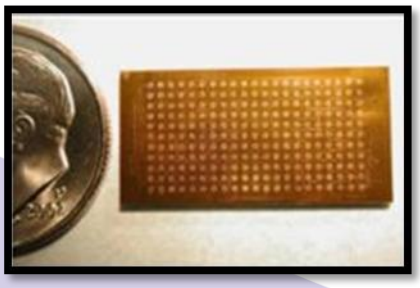
"HOWLERMONKEY is a custom built Short to Medium Range Radio Frequency Transceiver hardware implant that is used in conjunction with a digital core to make a complete implant. The Printed Circuit Board (PCB) layouts of the HOWLERMONKEY implants are tailored according to individual implant space requirements and differ in form factor. These PCBs are designed to be compatible with CONJECTURE/SPECULATION networks and STRIKEZONE devices that run on HOWLERMONKEY personality. The cost of HOWLERMONKEY for 40 units is $750 each and the cost of 25 units is $1000 each."[5]



JUNIORMINT

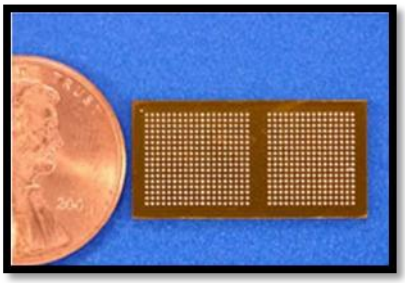
JUNIORMINT is a hardware implant which comes in two forms; a digital core packaged in a mini PCB which can be used in a conventional concealment and also a miniaturized Flip Chip Module which can be used in implants with size constraining concealments. TAO's standard implant architecture model is used to make this JUNIORMINT and this architecture is claimed to provide robust, reconfigurable, standard digital platform which can result in dramatic performance. The cost of this implant is unavailable and will be stated on placing the order based on the sophistication of the required implant.

MAESTRO - II



MAESTRO – II is a hardware implant of miniaturized digital core packaged in a Multi-Chip Module (MCM) which can be used in size constraining concealments. This implant contains an ARM7 microcontroller, FPGA, Flash and SDRAM memories. MAESTRO – II is also made using the TAO standard architecture for a robust, reconfigurable, standard digital platform that can result in a dramatic performance. The unit cost of this implant is $3-4k.

TRINITY



TRINITY is also a hardware implant of miniaturized digital core packaged in a Multi-Chip Module (MCM) which can be used in size constraining concealments. The function of TRINITY is similar to that of MAESTRO – II and the unit cost of this implant is $625k for 100 units.

All the software and hardware implants described above work on the CPU of the targeted computer to extract information and transfer it to the NSA. As these implants hide themselves and operate in stealth mode, it becomes impossible to trace their existence and eradicate the threat of espionage.

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] Appelbaum, Jacob, ET NL, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox", *Der Spiegel*, December 29, 2013.

[2] Appelbaum, Jacob. "NSA ANT Rechner", *Der Spiegel*, 30C3, 30 December 2013.

[3] SWAP: NSA Exploit of the Day, February 06, 2014, in https://www.schneier.com/blog/archives/2014/02/swap_nsa_exploi.html, accessed on June 03, 2014.

[4] "SOMBERKNAVE: NSA Exploit of the Day", February 05, 2014, in http://www.the-ethical-hacker.com/2014/02/somberknave-nsa-exploit-of-the-day/, accessed on June 03, 2014

[5] http://www.telefoniert-nach-hause.de/index.php/NSA/HOWLERMONKEY, accessed on June 04, 2014.