IN FOCUS

29 May 2014

ACCESSING THE INACCESSIBLE

Part II: Keyboards, USBs & VGAs

E. Dilipraj
Research Associate, CAPS

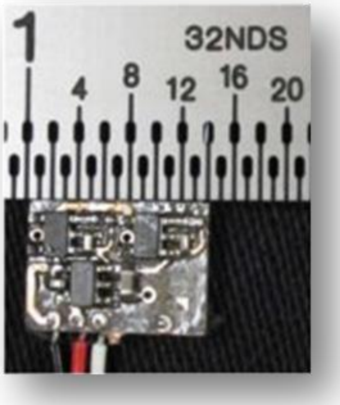
The NSA's digital tools of espionage exposed by the German Weekly *Der Spiegel* reveal the sophistication of every tool that is being used by the agency to spy upon its digital targets around the world. These tools are customized to work on different devices and platforms. The exposed catalogue reveals a list of 49 sophisticated digital tools, which are either hardware implants or software applications camouflaged within a device to enable espionage operations (See PART I for the list).

While, bugging electronic devices are a common practice around the world, NSA's ANT project differs from the conventional methods because of the following factors:

- Devices selected for the implants,
- Technological sophistication of the tools and
- The way these tools are implanted in the devices without creating suspicion.

While a few devices are targeted either by hardware or software implant, the devices like Mobile Phones and client computers are being targeted using both hardware and software implants. The list of devices that are being implanted includes the most commonly used devices around the world like the VGA Cables, USBs and keyboards. These three devices are mainly implanted with hardware tools, with the exception of one software application that is being used in USBs. A deeper look into the NSA ANT digital tools implanted on these three devices is given in subsequent paragraphs:

Keyboards



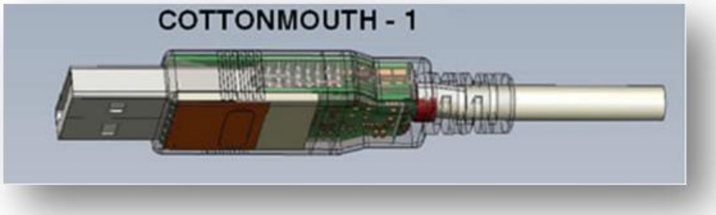
"SURLYSPAWN" is a $30 hardware implant designed to gather keystrokes of the targeted user's keyboard without requiring any supporting software running on the targeted system. The retro-reflector is compatible with both USB and PS/2 keyboards while the laptop keyboard variant was still under development during 2009.

This hardware board taps into the data line from the keyboard to the processor and generates a square wave oscillating at a preset frequency. The square wave frequency is shifted from higher or lower depending on the level of the data-line signal or in other terms, the square wave becomes frequency shift keyed (FSK). When the unit is illuminated by a CW signal from a nearby radar, the illuminating signal is amplitude-modulated (AM) with this square wave. The radar receives the signal re-radiated and demodulates the signal, which is then processed to recover the keystrokes.[1]

USBs

Since USBs are the most widely used connecting mechanism available, NSA has created implants to exploit this facility and to spy upon the targets. According to the exposed secret documents, NSA ANT catalogue provides four implants namely "COTTONMOUTH-I", "COTTONMOUTH-II", "COTTONMOUTH-III" and "FIREWALK" to enable their espionage operations. This form of disguised USB bug can be any kind of USB extension plug that is silently inserted into the different ports of the computer. They work by sending and receiving signals over short distances or by creating channels for other implants to work or by sending signals over long distances. These implants allow both the computer and the network it is connected to be monitored as well as send and receive signals both to the computer and to the hijacked network.

COTTONMOUTH-I



COTTONMOUTH-I (CM-I) is a USB hardware implant that provides a wireless bridge into the target's network as well as the ability to load exploiting software onto the target's PCs. This implant provides air-gap bridging, software persistence capability, "in-field" re-programmability and covert communications with a host software implant over the USB. The radio frequency link through this implant enables command and data infiltration and extraction. It also communicates with Data Network Technologies (DNT) software, STRAITBIZARRE through a covert channel implemented on the USB and passes the commands and data to the hardware and software implants using this channel.[2]

This implant is also capable of concealing other components like TRINITY, switches and HOWLERMONKEY within the USB Series-A cable connector. This implant also has the ability to contact other COTTONMOUTH devices using an over-the-air protocol called SPECULATION. There is not much description on the working of this protocol. Also, the term STRAITBIZARRE denotes an unknown software technology which has not been exposed and therefore can be understood to be a high end technology belonging to another family of digital espionage tools.

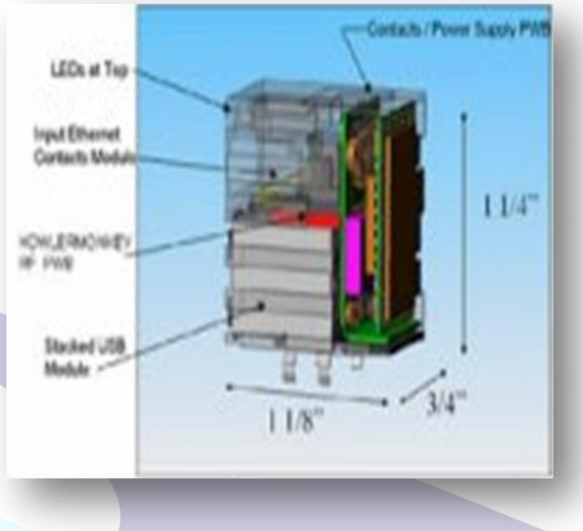
COTTONMOUTH-II

COTTONMOUTH-II (CM-II) is again a USB hardware Host tap implant which provides a covert link over USB link into the target's network. It is intended to operate within a long haul relay subsystem, which would be co-located within the target equipment.

CM-II provides software persistence capability, "in-field" re-programmability and covert communications with host software implant over the USB. Like CM-I, CM-II also communicate with DNT software, STRAITBIZARRE through a covert channel implemented on the USB and passes commands and data between the hardware and software using this channel. It is the ability of long haul relay of CM-II that provides wireless bridge into the target's network. According to the exposed documents, CM-II costs around $200K for 50 units.

COTTONMOUTH-III

Most of the operations of COTTONMOUTH-III (CM-III) is similar to COTTONMOUTH-I but differs only in the way it conceals the digital components. CM-III conceals digital components TRINITY, switches, and HOWLERMONKEY radio frequency transceiver within a RJ45 Dual Stacked USB connector unlike CM-I which conceals in a USB Series-A Cable Connector. Also, CM-III provides a short range inter-chassis link to other CM devices and it can also provide inter-chassis radio frequency link to a long haul relay subsystem. CM-III costs $1,248K for 50 units.[3]

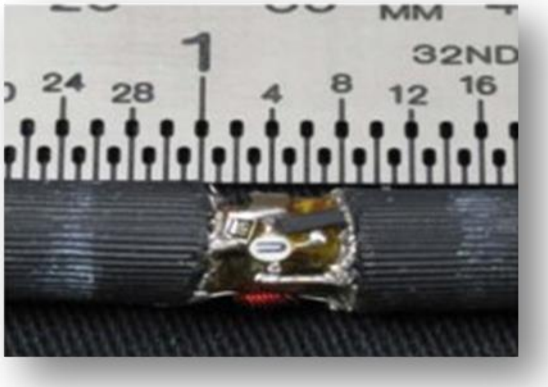


FIREWALK

FIREWALK is a bidirectional network implant which resides within adual stacked RJ4/ USB connector. It is capable of passive collection of Gigabit Ethernet network traffic, and injection of Ethernet packets onto the same target network. FIREWALK can surpass any firewall or air-gap protection in order to exploit the targeted network. It works in sync with HOWLERMONKEY, another digital tool for communications. FIREWALK costs $537 for 50 units.

VGA Cables:

The hardware implant designed for use in VGA cable is called RAGEMASTER. It is a $30 device which provides a target for Radio Frequency (RF) flooding and allows for easier collection of the VAGRANT video signal. This implant is neatly concealed in a standard computer Video Graphics Array (VGA) cable between the video card and video monitor. It is usually installed in the ferrite on the video cable tapping the red video line between the video card within the desktop unit and the computer monitor.[4]



A radar unit is used to illuminate the RAGEMASTER, which in turn modulates the red video line information. The re-radiated information from the red line is picked up at the radar, demodulated and passed on to the processing units. The processer recreates the horizontal and vertical cross sections of the targeted monitor, thus allowing the NSA personal to see the visuals displayed on the targeted monitor.

The technologies used for processing the re-radiated information are named in the exposed document of the NSA as LFS-2, NIGHTWATCH, GOTHAM and VIEWPLATE (as a future technology). There is no information available about these technologies in any of the exposed documents and hence, it can be assumed that these technologies are part of another family of digital tools of espionage.

Crafted with the state-of-art technologies, the above described implants and more are being used in various digital espionage operations around the world since 2008 by NSA.

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] https://www.schneier.com/blog/archives/2014/02/surlyspawn_nsa.html, accessed on may 06, 2014.

[2] Jacob Appelbaum, NSA ANT USB, 30C3, 30 December 2013

[3] Ibid

[4] Jacob Appelbaum, NSA ANT Bildschirm, 30C3, 30 December 2013.

ARTICLES BY SAME AUTHOR

ACCESSING THE INACCESSIBLE: PART I: NSA'S Digital Tools of Espionage

INDIA STRENGTHENS TIES WITH SOUTH KOREA IN CYBER SECURITY

INDIA CHALLENGES CHINA IN LAC

BRICS' CABLE AND CYBER SECURITY

NATURAL OR TARGETED' ALLY