NSA Playset

Transformando Espionagem em Pesquisa

Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardokleber@ricardokleber.com

GTS'24
28/11/2014

NSA ANT (Spy Catalogue)
A Inspiração...

GTER GTS .br

Um dos “vazamentos” de Snowden

- NSA ANT: Catálogo de “Ferramentas de Espionagem”
  - 48 projetos
  - Hardware e Software
  - Controle e “hacking” de sistemas computacionais
  - Disponibilizado aos agentes da NSA
  - Disponível (hoje) em vários repositórios
    - `http://www.nsaplayset.org/nsa_ant_catalog.pdf`
    - `https://www.aclu.org`
    - `http://leaksource.info`

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

NSA ANT (Spy Catalogue)
Modalidades de Ferramentas

GTER GTS .br

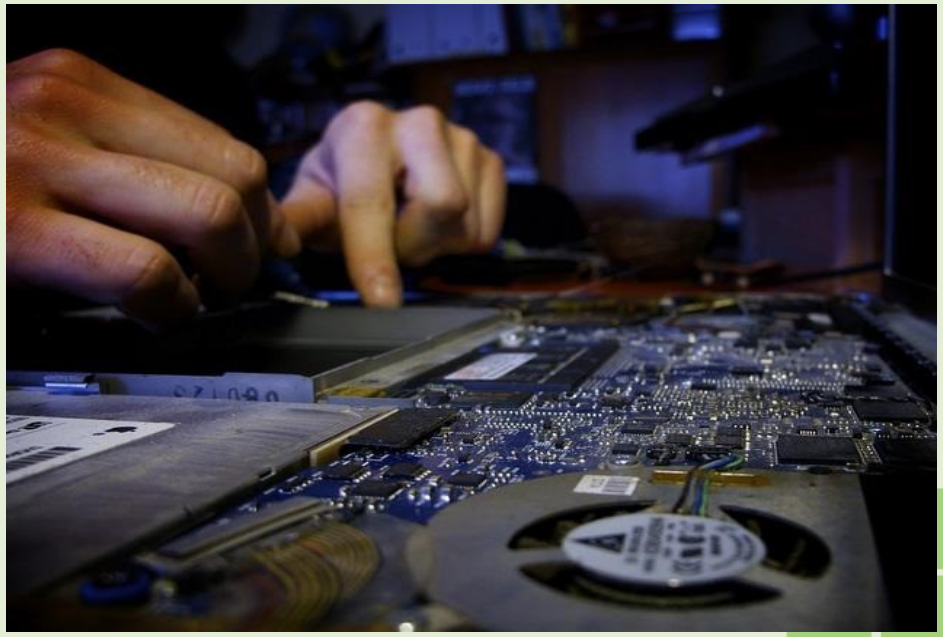
Categorias Específicas

- Implantes e Backdoors
  - “Implantes” em Hardwares
  - “Implantes” em Softwares
  - Backdoors Persistentes (em roteadores)
  - Backdoors Persistentes (em firewalls)
- Grampos e Retrorefletores
  - Grampos em Redes Wi-Fi
  - Grampos em Redes Celulares (Base Stations / Interrogation)
  - Retrorefletores RF (Radio-Frequência)

GTER
GTS
.br

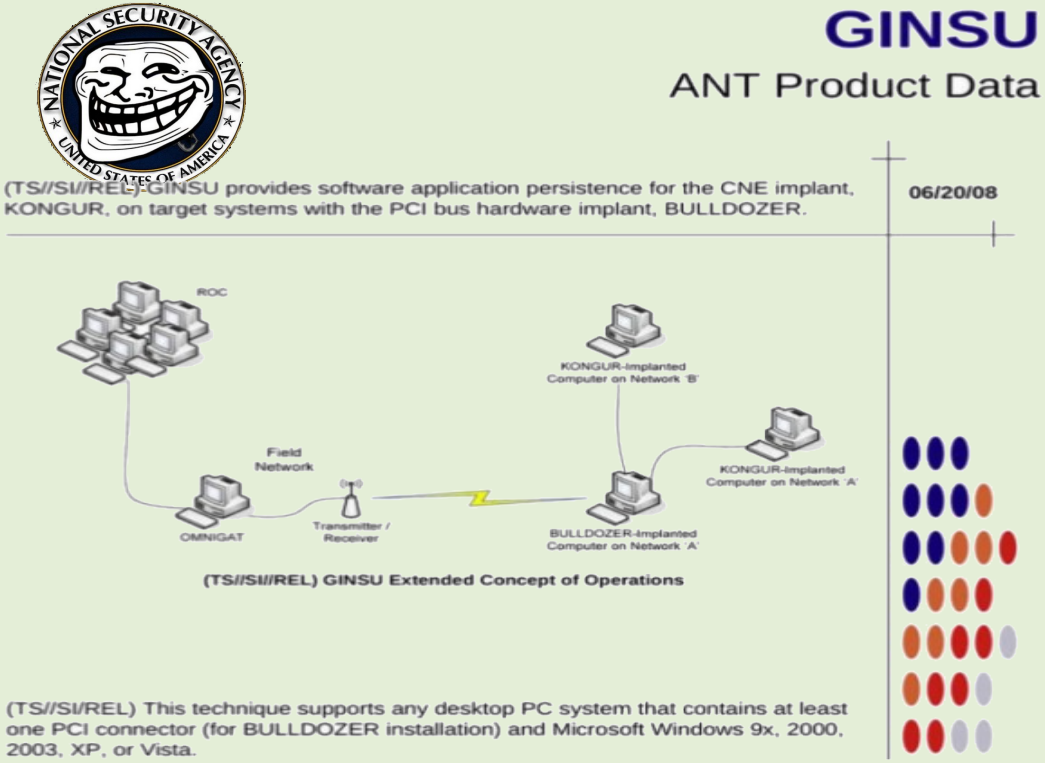
Implantes em Hardwares

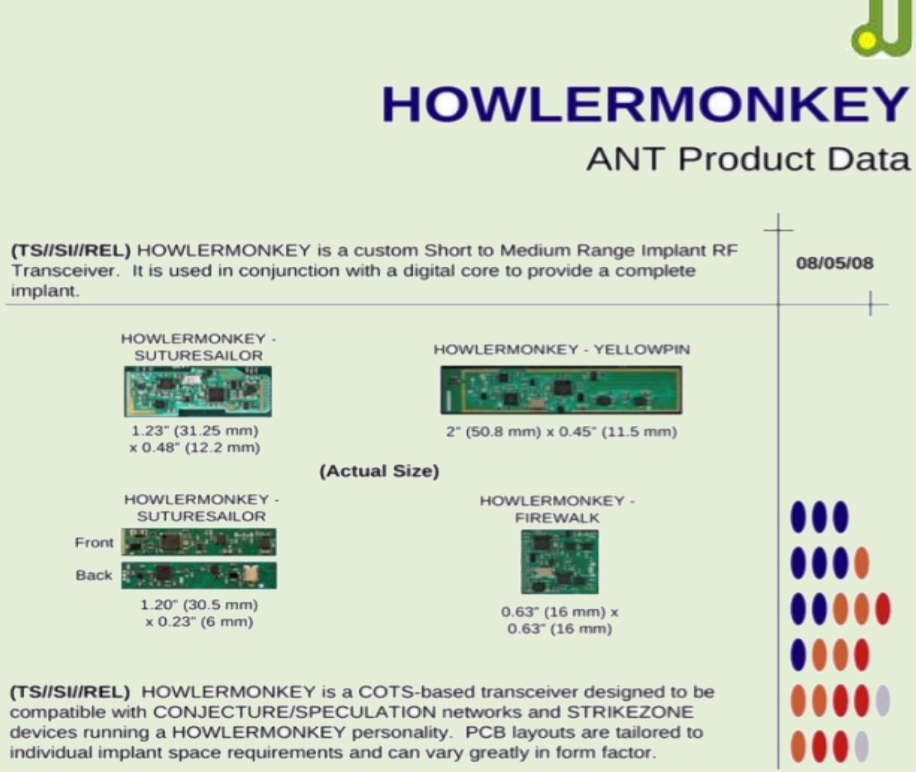
(Hardware Implants)



NSA ANT (Spy Catalogue)

Hardware Implants





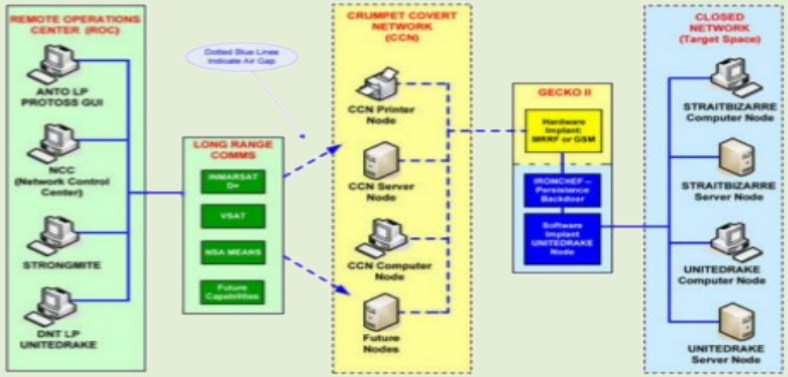
- GINSU: Technology that uses a PCI bus device in a computer, and can reinstall itself upon system boot-up.
- HOWLERMONKEY: A RF transceiver that makes it possible (in conjunction with digital processors and various implanting methods) to extract data from systems or allow them to be controlled remotely.

NSA ANT (Spy Catalogue)
Hardware Implants

IRONCHEF
ANT Product Data

(TS//SI//REL) IRONCHEF provides access persistence to target systems by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to communicate with a hardware implant that provides two-way RF communication.

07/14/08



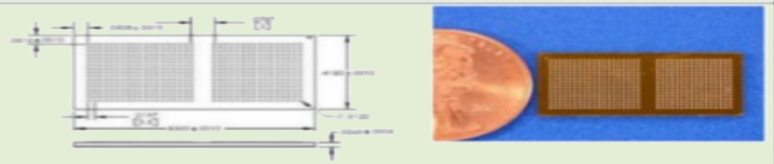
(TS//SI//REL) IRONCHEF Extended Concept of Operations

(TS//SI//REL) This technique supports the HP Proliant 380DL G5 server, onto which a hardware implant has been installed that communicates over the I²C Interface (WAGONBED).

TRINITY
ANT Product Data

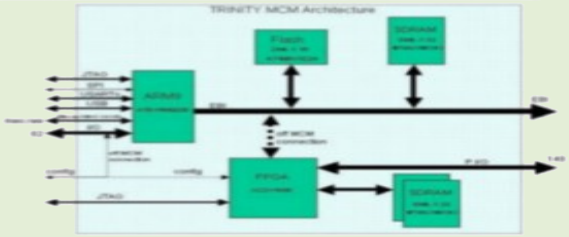
08/05/08

(TS//SI//REL) TRINITY is a miniaturized digital core packaged in a Multi-Chip Module (MCM) to be used in implants with size constraining concealments.



(TS//SI//REL) TRINITY uses the TAO standard implant architecture. The architecture provides a robust, reconfigurable, standard digital platform resulting in a dramatic performance improvement over the obsolete HC12 microcontroller based designs. A development Printed Circuit Board (PCB) using packaged parts has been developed and is available as the standard platform. The TRINITY Multi-Chip-Module (MCM) contains an ARM9 microcontroller, FPGA, Flash and SDRAM memories.

uController	Flash	SDRAM (3)	FPGA
ARM 9 180 Mhz	AT49BV322A 4 MBytes	MT48LC8M32 96 MBytes	XC2V1000 1M gates



- IRONCHEF: Technology that can "infect" networks by installing itself in a computer I/O BIOS
- TRINITY: A more recent and more powerful multi-chip module using a 180 MHz ARM9 processor, 4 MB of flash, 96 MB of SDRAM, and a FPGA with 1 million gates. Smaller than a penny. Estimated cost (2008) $625K for 100 units.c

NSA ANT (Spy Catalogue)
Hardware Implants

GTER GTS .br

COTTONMOUTH-I
ANT Product Data

08/05/08

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH-II
ANT Product Data

08/05/08

(TS//SI//REL) COTTONMOUTH-II (CM-II) is a Universal Serial Bus (USB) hardware Host Tap, which will provide a covert link over USB link into a targets network. CM-II is intended to be operate with a long haul relay subsystem, which is co-located within the target equipment. Further integration is needed to turn this capability into a deployable system.

(TS//SI//REL) CM-II will provide software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. CM-II will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-II will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-II consists of the CM-I digital hardware and the long haul relay concealed somewhere within the target chassis. A USB 2.0 HS hub with switches is concealed in a dual stacked USB connector, and the two parts are hard-wired, providing a intra-chassis link. The long haul relay provides the wireless bridge into the target's network.

- COTTONMOUTH: A family of modified USB and Ethernet connectors that can be used to install Trojan horse software and work as wireless bridges, providing covert remote access to the target machine.
- COTTONMOUTH-I is a USB plug that uses TRINITY as digital core and HOWLERMONKEY as RF transceiver. Cost in 2008 was slightly above $1M for 50 units.

NSA ANT (Spy Catalogue)
Hardware Implants

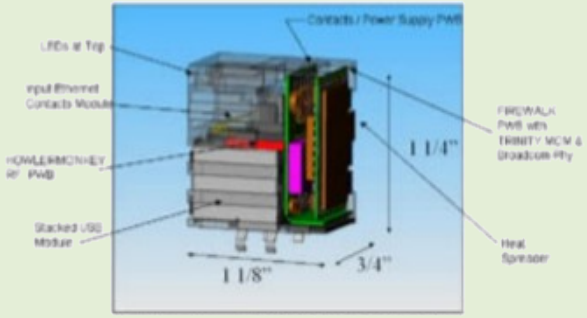
GTER GTS .br

FIREWALK

ANT Product Data

(TS//SI//REL) FIREWALK is a bidirectional network implant, capable of passively collecting Gigabit Ethernet network traffic, and actively injecting Ethernet packets onto the same target network.

08/05/08



(TS//SI//REL) FIREWALK is a bi-directional 10/100/1000bT (Gigabit) Ethernet network implant residing within a dual stacked RJ45 / USB connector. FIREWALK is capable of filtering and egressing network traffic over a custom RF link and injecting traffic as commanded; this allows a ethernet tunnel (VPN) to be created between target network and the ROC (or an intermediate redirector node such as DNT's DANDERSPRITZ tool.) FIREWALK allows active exploitation of a target network with a firewall or air gap protection. **(TS//SI//REL)** FIREWALK uses the HOWLERMONKEY transceiver for back-end communications. It can communicate with an LP or other compatible HOWLERMONKEY based ANT products to increase RF range through multiple hops.

- FIREWALK: A device that looks identical to a standard RJ45 socket that allows data to be injected, or monitored and transmitted via radio technology. using the HOWLERMONKEY RF transceiver. It can for instance create a VPN to the target computer. Cost in 2008: $537K for 50 units.

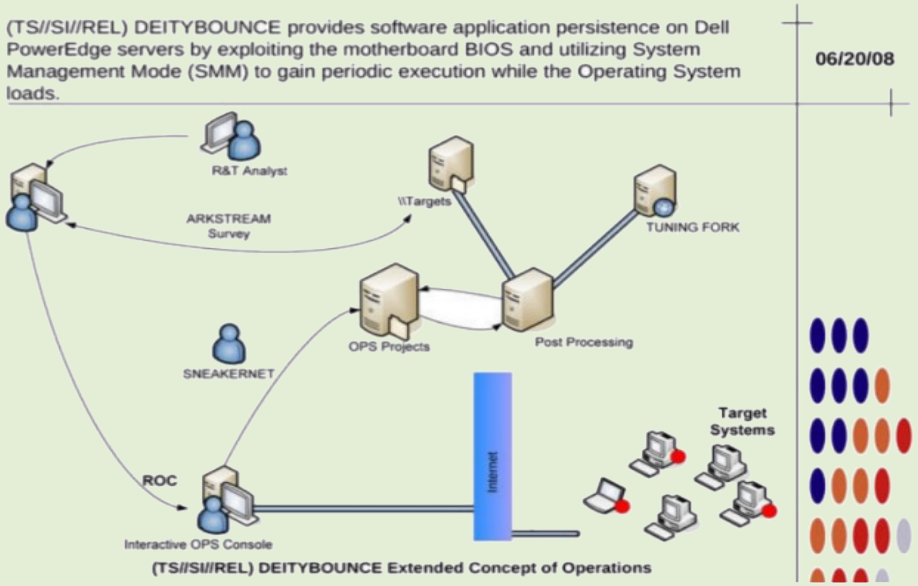
GTER
GTS
.br

Implantes em Softwares

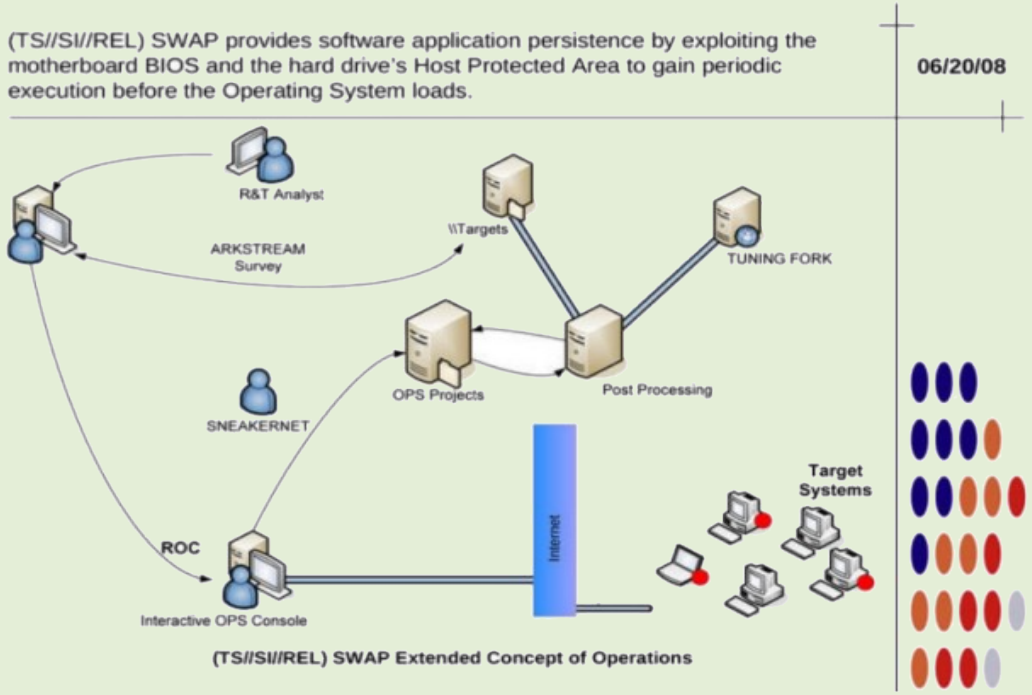
(Software Implants)

NSA ANT (Spy Catalogue)
Software Implants

DEITYBOUNCE
ANT Product Data



SWAP
ANT Product Data



- DEITYBOUNCE: Technology that installs a backdoor software implant on Dell PowerEdge servers via the motherboard BIOS and RAID controller(s).
- SWAP: Technology that can reflash the BIOS of multiprocessor systems that run FreeBSD, Linux, Solaris, or Windows.

NSA ANT (Spy Catalogue)

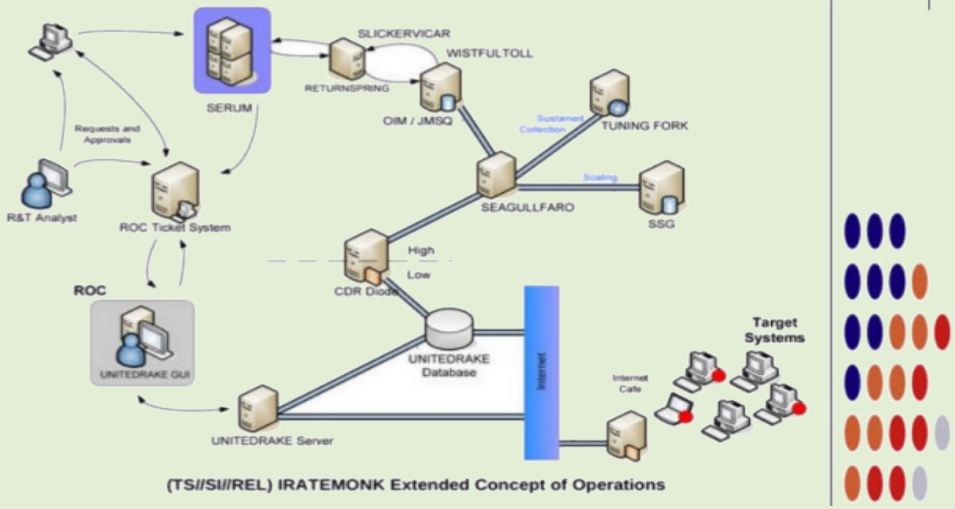
Software Implants

IRATEMONK

ANT Product Data

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

06/20/08



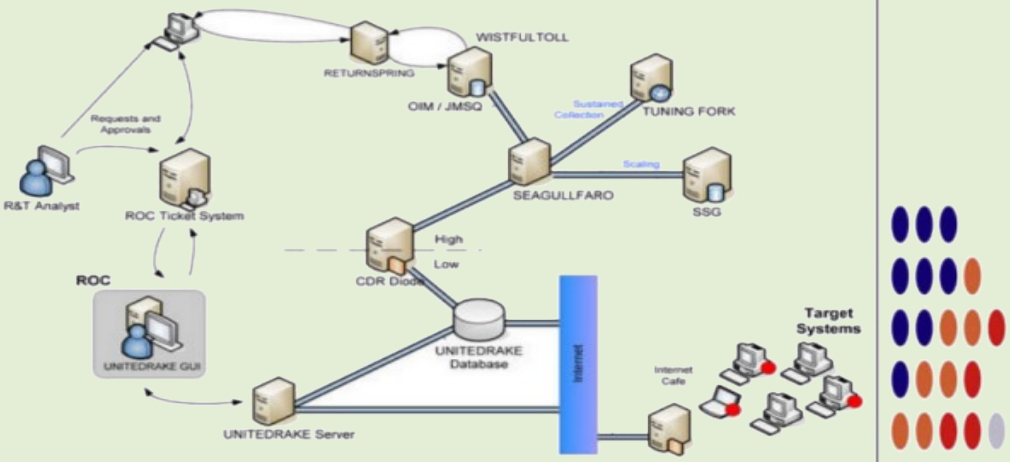
(TS//SI//REL) IRATEMONK Extended Concept of Operations

WISTFULTOLL

ANT Product Data

(TS//SI//REL) WISTFULTOLL is a UNITEDRAKE and STRAITBIZZARE plug-in used for harvesting and returning forensic information from a target using Windows Management Instrumentation (WMI) calls and Registry extractions.

06/20/08



(TS//SI//REL) WISTFULTOLL Extended Concept of Operations

- IRATEMONK: Technology that can infiltrate the firmware of hard drives manufactured by Maxtor, Samsung, Seagate, and Western Digital.
- WISTFULTOLL: Plugin Win 2000, 2003 and XP (extract forensic information using WMI)

NSA ANT (Spy Catalogue)

Software Implants

GTER GTS .br

SOMBERKNAVE

ANT Product Data

(TS//SI//REL) SOMBERKNAVE is Windows XP wireless software implant that provides covert internet connectivity for isolated targets.

08/05/08

(TS//SI//REL) SOMBERKNAVE is a software implant that surreptitiously routes TCP traffic from a designated process to a secondary network via an unused embedded 802.11 network device. If an Internet-connected wireless Access Point is present, SOMBERKNAVE can be used to allow OLYMPUS or VALIDATOR to "call home" via 802.11 from an air-gapped target computer. If the 802.11 interface is in use by the target, SOMBERKNAVE will not attempt to transmit.

(TS//SI//REL) Operationally, VALIDATOR initiates a call home. SOMBERKNAVE triggers from the named event and tries to associate with an access point. If connection is successful, data is sent over 802.11 to the ROC. VALIDATOR receives instructions, downloads OLYMPUS, then disassociates and gives up control of the 802.11 hardware. OLYMPUS will then be able to communicate with the ROC via SOMBERKNAVE, as long as there is an available access point.

- SOMBERKNAVE: Software that can be implanted on a Windows XP system allowing it to be remotely controlled from NSA headquarters.

GTER GTS .br

Backdoors Persistentes em Roteadores

(Persistent Backdoors - Routers)

NSA ANT (Spy Catalogue)
Persistent Backdoors (routers)

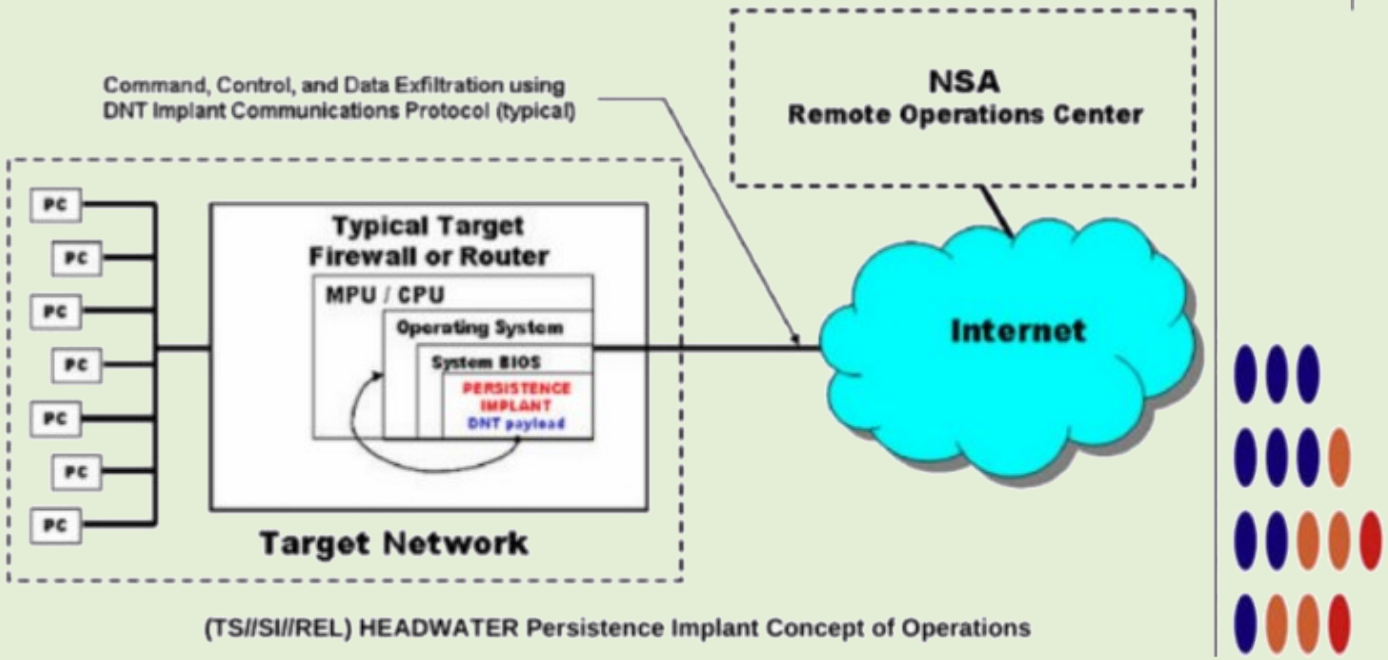
GTER GTS .br

HEADWATER

ANT Product Data

(TS//SI//REL) HEADWATER is a Persistent Backdoor (PBD) software implant for selected Huawei routers. The implant will enable covert functions to be remotely executed within the router via an Internet connection.

06/24/08



(TS//SI//REL) HEADWATER Persistence Implant Concept of Operations

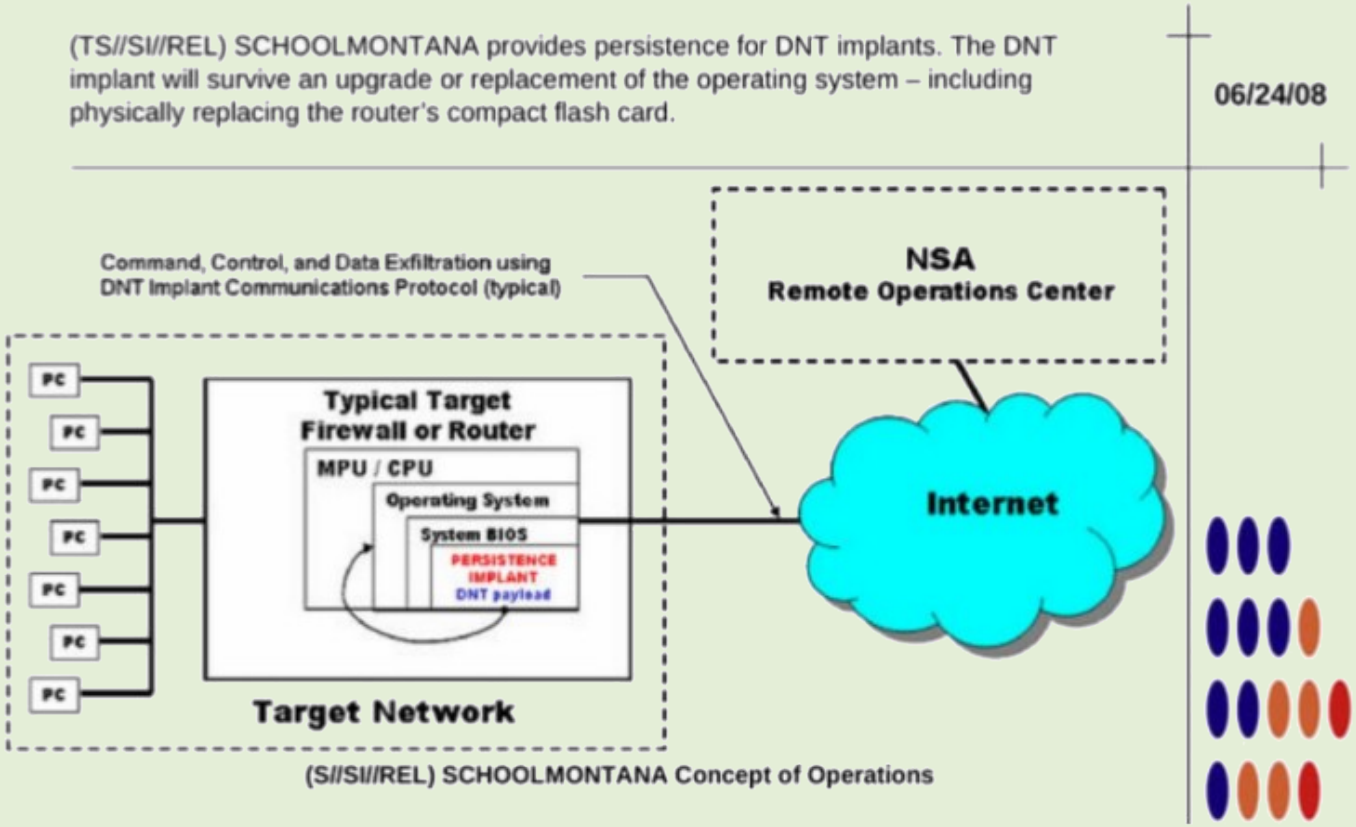
- HEADWATER: Persistent backdoor technology that can install spyware using a "quantum insert" capable of infecting spyware at a packet level on Huawei routers.

NSA ANT (Spy Catalogue)
Persistent Backdoors (routers)

GTER GTS .br

SCHOOLMONTANA

ANT Product Data



- SCHOOLMONTANA: Software that makes DNT implants persistent on JUNOS-based (Free BSD-variant) J-series routers/firewalls.

GTER GTS .br

Backdoors Persistentes em Firewalls

(Persistent Backdoors - Firewalls)

NSA ANT (Spy Catalogue)
Persistent Backdoors (firewalls)

GTER GTS .br

JETPLOW

ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)

NSA
Remote Operations Center

PC
PC
PC
PC
PC
PC

Typical Target
Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT
DNT payload

Internet

Target Network

(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

- JETPLOW: Firmware that can be implant to create a permanent backdoor in a Cisco PIX series and ASA firewalls.

NSA ANT (Spy Catalogue)
Persistent Backdoors (firewalls)

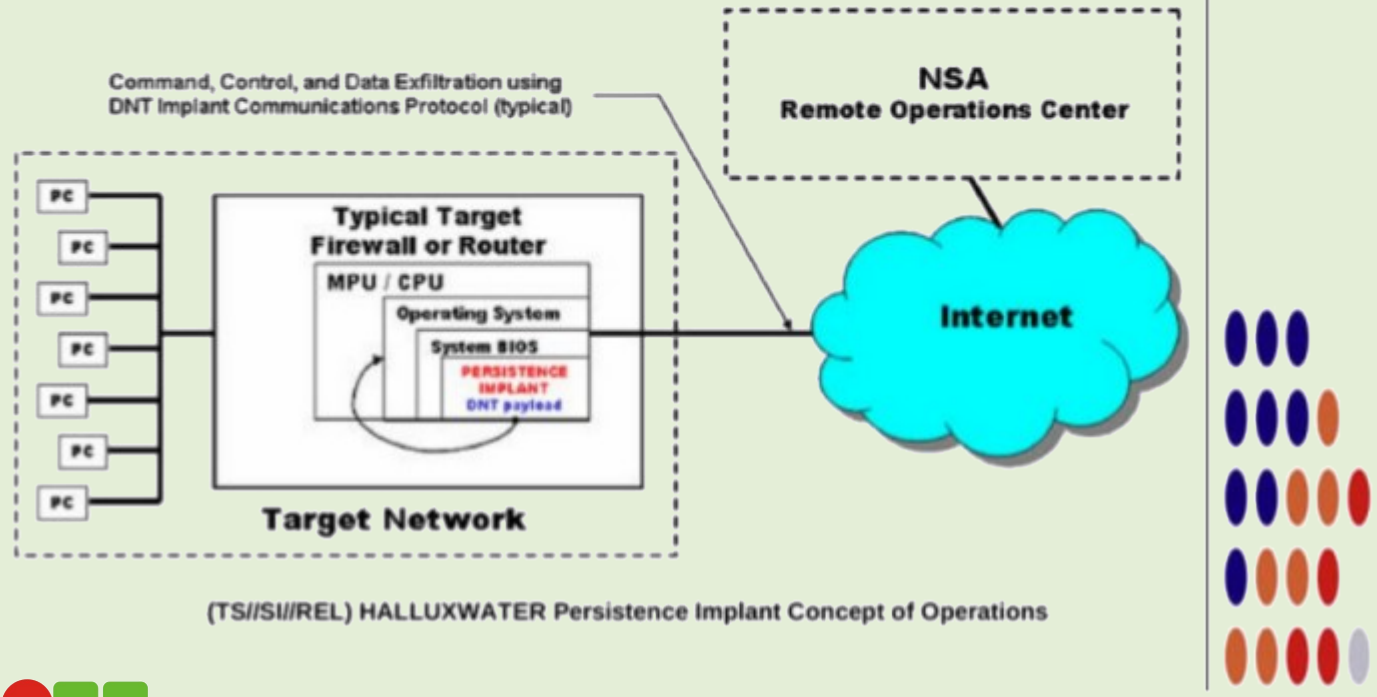
GTER GTS .br

HALLUXWATER

ANT Product Data

(TS//SI//REL) The HALLUXWATER Persistence Back Door implant is installed on a target Huawei Eudemon firewall as a boot ROM upgrade. When the target reboots, the PBD installer software will find the needed patch points and install the back door in the inbound packet processing routine.

06/24/08



(TS//SI//REL) HALLUXWATER Persistence Implant Concept of Operations

- HALLUXWATER: Back door exploit for Huawei Eudemon firewalls.

NSA ANT (Spy Catalogue)
Persistent Backdoors (firewalls)

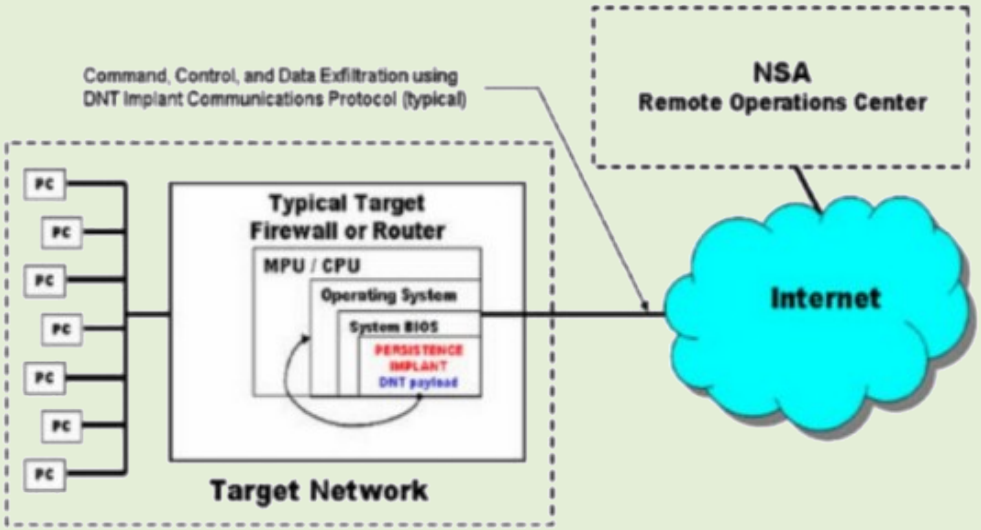
GTER GTS .br

FEEDTROUGH

ANT Product Data

(TS//SI//REL) FEEDTROUGH is a persistence technique for two software implants, DNT's BANANAGLEE and CES's ZESTYLEAK used against Juniper Netscreen firewalls.

06/24/08



(S//SI//REL) Persistence Operational Scenario

- FEEDTROUGH: Software that can penetrate Juniper Networks firewalls allowing other NSA-deployed software to be installed on mainframe computers.

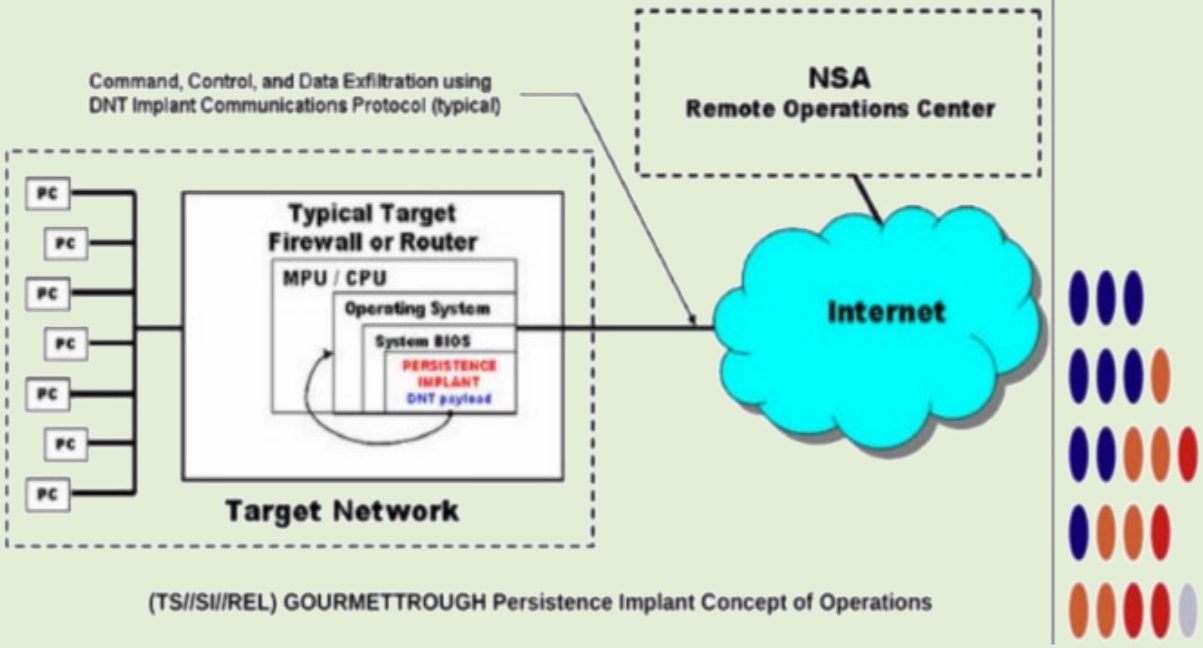
NSA ANT (Spy Catalogue)
Persistent Backdoors (firewalls)

GOURMETTROUGH

ANT Product Data

(TS//SI//REL) GOURMETTROUGH is a user configurable persistence implant for certain Juniper firewalls. It persists DNT's BANANAGLEE implant across reboots and OS upgrades. For some platforms, it supports a minimal implant with beaconing for OS's unsupported by BANANAGLEE.

06/24/08



(TS//SI//REL) GOURMETTROUGH Persistence Implant Concept of Operations

- GOURMETTROUGH: User-configurable persistence implant for certain Juniper Networks firewalls.

NSA ANT (Spy Catalogue)
Persistent Backdoors (firewalls)

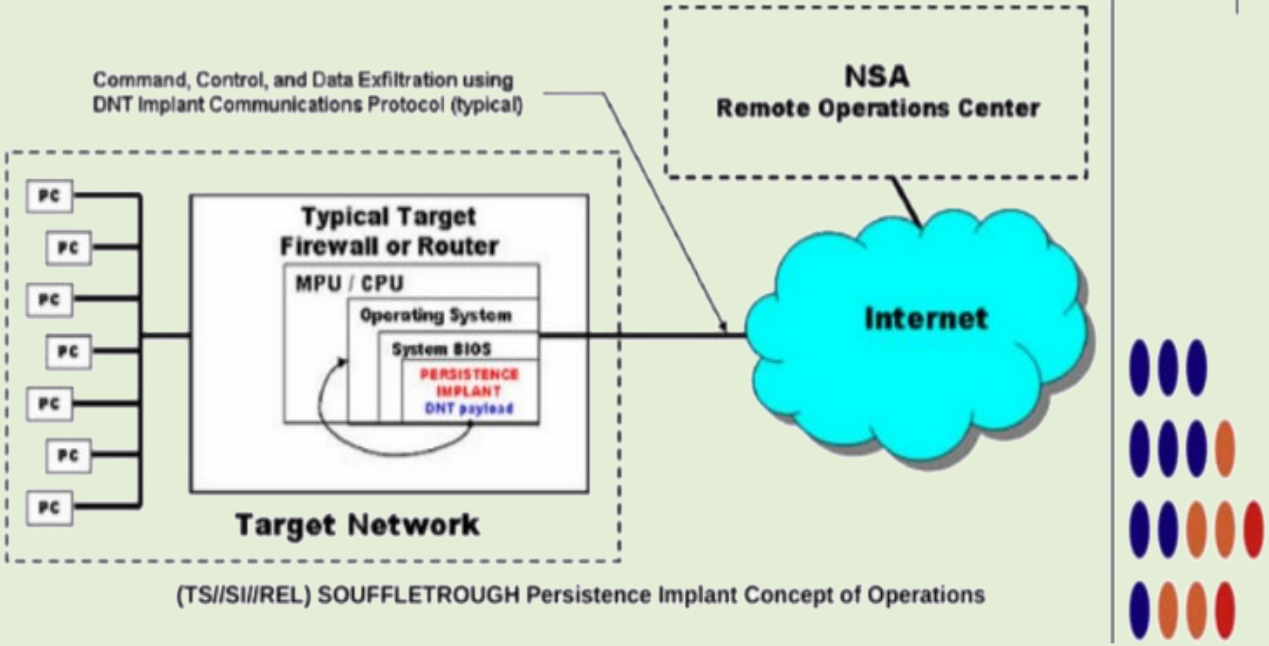
GTER GTS .br

SOUFFLETROUGH

ANT Product Data

(TS//SI//REL) SOUFFLETROUGH is a BIOS persistence implant for Juniper SSG 500 and SSG 300 series firewalls. It persists DNT's BANANAGLEE software implant. SOUFFLETROUGH also has an advanced persistent back-door capability.

06/24/08



(TS//SI//REL) SOUFFLETROUGH Persistence Implant Concept of Operations

- SOUFFLETROUGH: BIOS injection software that can compromise Juniper Networks SSG300 and SSG500 series firewalls.

Grampos e Retrorefletores de RF

- Grampos em Redes Wi-Fi
- Grampos em Redes Celulares (Base Stations / Interrogation)
- Retrorefletores RF (Radio-Frequência)

NSA ANT (Spy Catalogue)

Grampos e Retrorefletores de RF

GTER GTS .br

NIGHTSTAND

Wireless Exploitation / Injection Tool

(TS//SI//REL) An active 802.11 wireless exploitation and injection tool for payload/exploit delivery into otherwise denied target space. NIGHTSTAND is typically used in operations where wired access to the target is not possible.

07/25/08

(TS//SI//REL) **NIGHTSTAND** - Close Access Operations • Battlefield Tested • Windows Exploitation • Standalone System

System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.

- NIGHTSTAND: Portable system that wirelessly installs Microsoft Windows exploits from a distance of up to eight miles.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

NSA ANT (Spy Catalogue)

Grampos e Retrorefletores de RF

SPARROW II

Wireless Survey - Airborne Operations - UAV

(TS//SI//REL) An embedded computer system running BLINDDATE tools. Sparrow II is a fully functional WLAN collection system with integrated Mini PCI slots for added functionality such as GPS and multiple Wireless Network Interface Cards.

07/25/08

(U//FOUO) System Specs

Processor: IBM Power PC 405GPR
Memory: 64MB (SDRAM)
16MB (FLASH)

Expansion: Mini PCI (Up to 4 devices) supports USB, Compact Flash, and 802.11 B/G

OS: Linux (2.4 Kernel)

Application SW: BLINDDATE

Battery Time: At least two hours

SPARROW II Hardware

- SPARROW II: A small computer intended to be used for WLAN collection, including from UAVs. Hardware: IBM Power PC 405GPR processor, 64 MB SDRAM, 16 MB of built-inflash, 4 mini PCI slots, CompactFlash slot, and 802.11 B/G hardware. Running Linux 2.4 and the BLINDDATE software suite. Unit price (2008): $6K.

NSA ANT (Spy Catalogue)

Grampos e Retrorefletores de RF

GTER GTS .br

RAGEMASTER

ANT Product Data

24 Jul 2008

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.

- RAGEMASTER: A concealed $30 device that taps the video signal from a target's computer's VGA signal output so the NSA can see what is on a targeted desktop monitor. It is powered by a remote radar and responds by modulating the VGA red signal (which is also sent out most DVI ports) into the RF signal it re-radiates; this method of transmission is codenamed VAGRANT.

NSA PlaySet

Espionagem que virou pesquisa...

GTER GTS .br

Dá pra implementar os projetos do Catálogo (e com baixo custo)?

- Sim !!! (pelo menos a maioria)
- Alguns inclusive nem são novidade :)
- O NSA PlaySet é uma tentativa de concentrá-los

NSA Playset

www.nsaplayset.org

Principais Objetivos:

- Estudar e recriar as ferramentas (“Provas de Conceito”)
- Com criatividade e baixo custo
- Colaboração com a pesquisa em segurança
- Uso prioritário de tecnologias abertas
- Documentação detalhada do desenvolvimento
- Possibilidade de implementação fácil pelos interessados

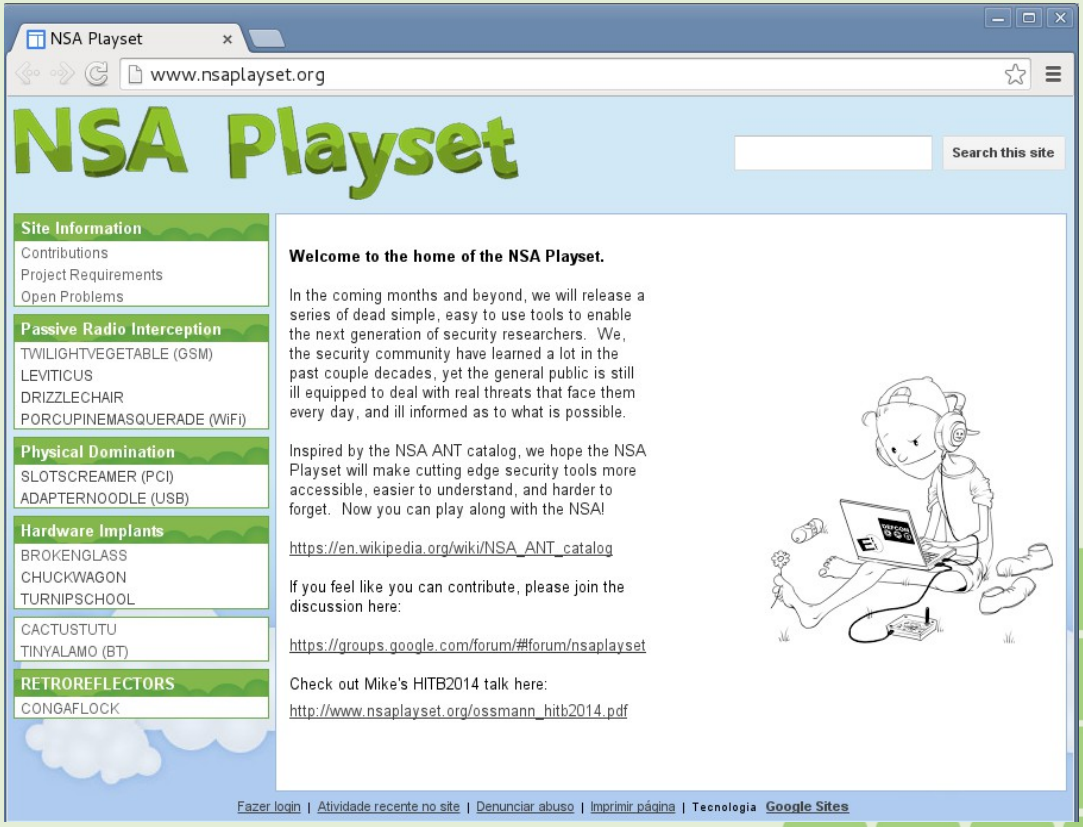
NSA Playset

"agora você pode brincar junto com a NSA!"

GTER GTS .br

www.nsaplayset.org

- "Agências de Inteligência não são mágicas"
- "Se (tecnologias anti-privacidade) são capazes de existir... é preciso conhecê-las para se proteger"



Requisitos para Participação (iniciar um projeto)

- Um Nome "bobo" (Silly Name)
  - Se o projeto é similar a um NSA ANT → usar nome parecido
  - Se não há equivalente no catálogo → crie o seu nome
  - Se faltar criatividade: www.nsanamegenerator.com
- Uma Categoria
  - Passive Radio Interception
  - Active Radio Injection
  - Physical Domination
  - Hardware Implants
  - Software Implants
  - Network Reconnaissance
- Escopo / Lista de Ingredientes / Instruções detalhadas para a reprodução de resultados

NSA PlaySet

Primeiro (grande) desafio: Um Radiorefletor RF

HACKRF

Software Defined Radio Peripheral

(U//FOUO) HACKRF is a Software Defined Radio peripheral capable of transmission or reception of arbitrary radio signals from 10 MHz to 6 GHz.

12/31/13

(U//FOUO) HackRF One with optional enclosure

(U//FOUO) HACKRF is an open source hardware platform designed to enable education, experimentation, and deployment of Software Defined Radio (SDR) technology.

(U//FOUO) HackRF One Features:

- 10 MHz to 6 GHz operating frequency
- half-duplex transceiver
- portable
- Hi-Speed USB 2.0, bus powered
- low cost
- open source
- works with GNU Radio
- 20 MHz bandwidth
- 8 bit resolution
- external clock input and output

(U//FOUO) Applications:

- spectrum analysis
- vector signal analysis
- vector signal generation
- reverse engineering
- spectrum sensing
- wireless security testing
- radio research and development

(U//FOUO) HACKRF makes cutting edge SDR technology available to everyone. Now you can build any radio you want.

Status: Available Q1 2014
http://greatscottgadgets.com/hackrf/

Unit Cost: $300 estimated

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

HackRF is open source hardware and software. Anyone may use it, build it, or modify it, not just the NSA.

HACKRF

- hardware/software para “grampo”
- conectado a computadores (ou smartphones) via USB permite o envio de dados capturados via rádio;
- transmissão ou recepção de sinais em faixas de frequência entre 10MHz e 6GHz;
- requer pouca energia (alimentado pelo próprio equipamento grampeado);
- o dispositivo espionado não precisa estar conectado à internet.

NSA PlaySet

O HACKRF: Autor (e idealizador do NSA Playset)

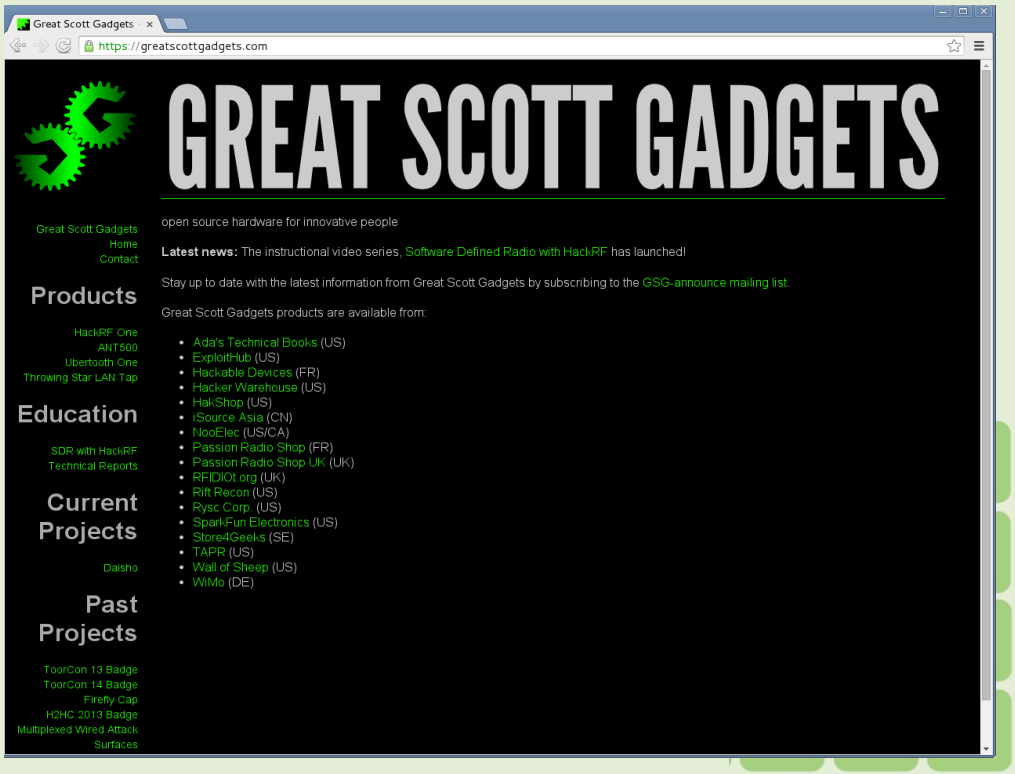
GTER GTS .br

Michael Ossman

- HachRF “caseiro”
- Site **greatscottgadgets.com**
- Um dos criadores do NSA PlaySet

NSA Playset

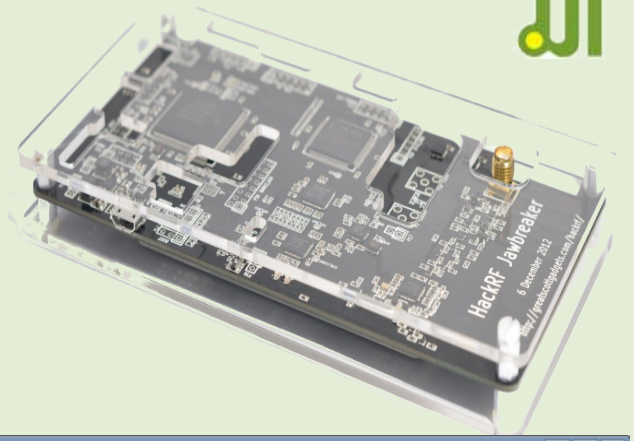
www.nsaplayset.org

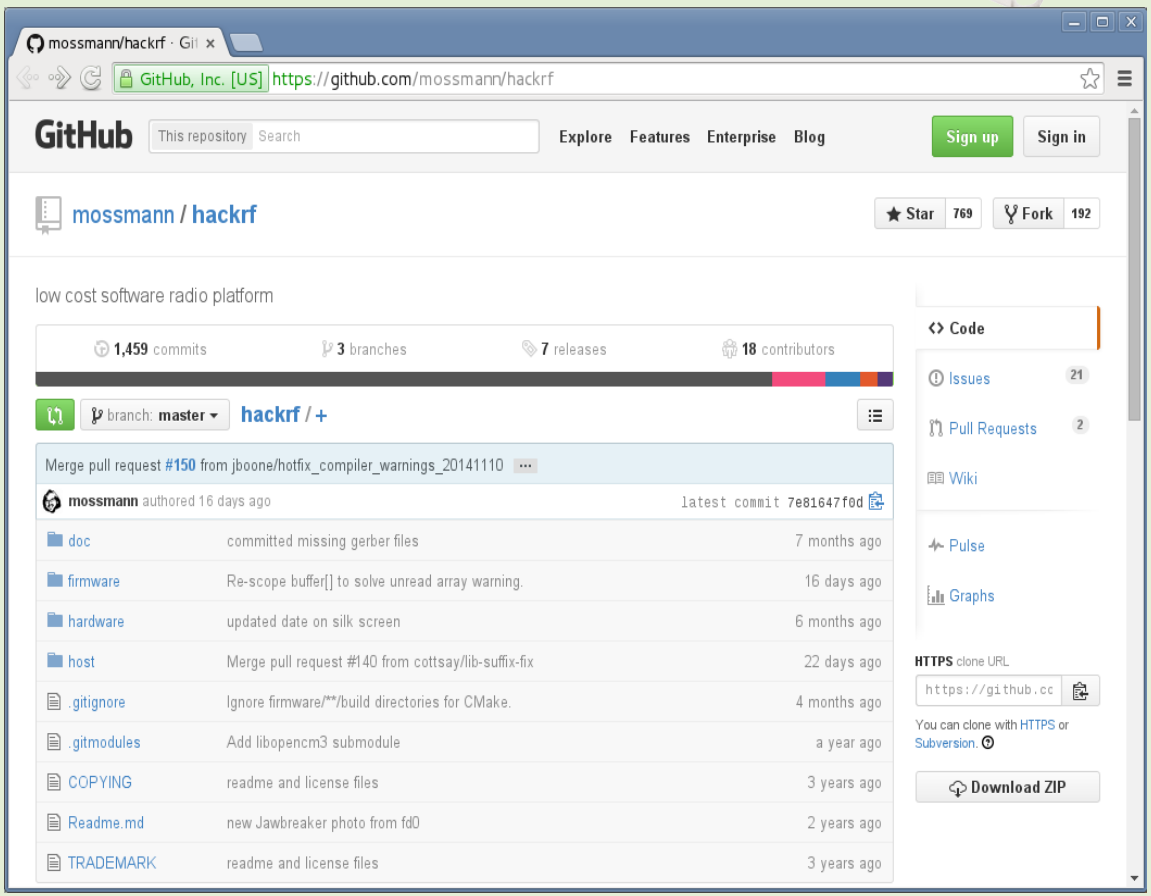


INSTITUTO FE
EDUCAÇÃO, C
RIO GRANDE DO

NSA PlaySet
O HACKRF (de Ossman)

- **`https://greatscottgadgets.com/hackrf`**
- Software (e projeto de hardware) disponível (GitHub)
- Preço médio de venda: $ 299.00
  - HakShop (US)
  - NooElec (US/CA)
  - Hacker Warehouse (US)
  - Ada's Technical Books (US)
  - Wall of Sheep (US)
  - Store4Geeks (SE)
  - Passion Radio Shop (FR)
  - Passion Radio Shop UK (UK)
  - TAPR (US)
  - iSource Asia (CN)
  - WiMo (DE)
  - Rysc Corp. (US)
  - SparkFun Electronics (US)





INSTITUTO FE
EDUCAÇÃO, C
RIO GRANDE DO

NSA PlaySet

Projetos Atuais em andamento (disponíveis no site)

GTER GTS .br

Passive Radio Interception

- TWILIGHTVEGETABLE
- LEVITICUS
- DRIZZLECHAIR
- PORCUPINEMASQUERADE

Phisical Domination

- SLOTSCREAMER
- ADAPTERNOODLE

Hardware Implants

- BROKENGLASS
- CHUCKWAGON
- TURNIPSCHOOL
- CACTUSTUTU
- TINYALAMO

Retroreflectors

- CONGAFLOCK

INSTITUTO FE
EDUCAÇÃO, C
RIO GRANDE DO

NSA PlaySet

Nem tudo é (totalmente) novidade

- Linux + Laptop + Aircrack-NG + Metasploit ≃ NIGHTSTAND
- BeagleBone Black + USBProxy ≃ COTTONMOUTH-II
- OpenWRT + AM335x Starter Kit ≃ FIREWALK
- Arduino + microcontrolador com I2C ≃ WANGOBED

Existem outras iniciativas (isoladas)

- Wifi Pineapple [www.wifipineapple.com]
- Carabola 2 [www.8devices.com/carambola-2]
- Ubertooth [ubertooth.sourceforge.net]

NSA Playset

Detalhamento

GTER GTS .br

www.nsaplayset.org

- Apresentação do Michael Ossmann na Defcon'2014:

Coming Soon!

NSA Playset: RF Retroreflectors
NSA Playset: GSM
NSA Playset: PCIe
and more!

nsaplayset.org

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

NSA Playset

Participe :)

GTER
GTS
.br

www.nsaplayset.org

Contribute your tools!

nsaplayset.org

(silly name required)