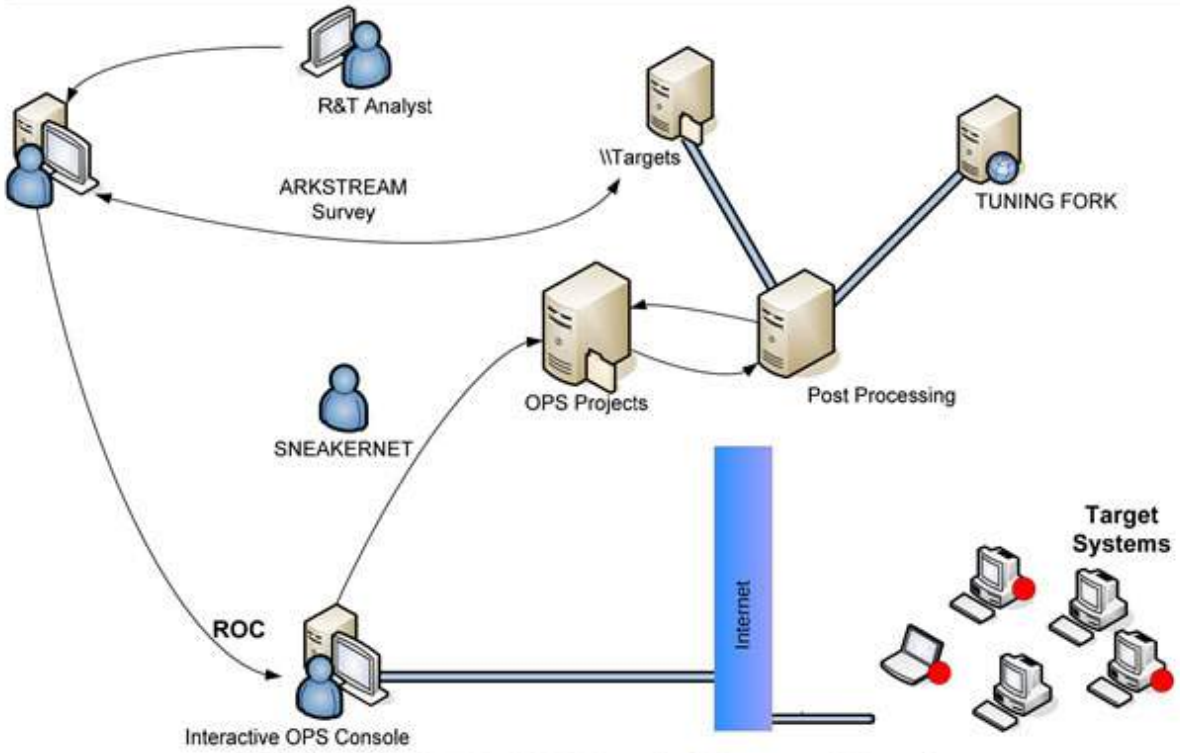
DEITYBOUNCE

ANT Product Data

(TS//SI//REL) DEITYBOUNCE provides software application persistence on Dell PowerEdge servers by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to gain periodic execution while the Operating System loads.

06/20/08



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

(TS//SI//REL) This technique supports multi-processor systems with RAID hardware and Microsoft Windows 2000, 2003, and XP. It currently targets Dell PowerEdge 1850/2850/1950/2950 RAID servers, using BIOS versions A02, A05, A06, 1.1.0, 1.2.0, or 1.3.7.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS on a target machine to implant DEITYBOUNCE and its payload (the implant installer). Implantation via interdiction may be accomplished by non-technical operator though use of a USB thumb drive. Once implanted, DEITYBOUNCE's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

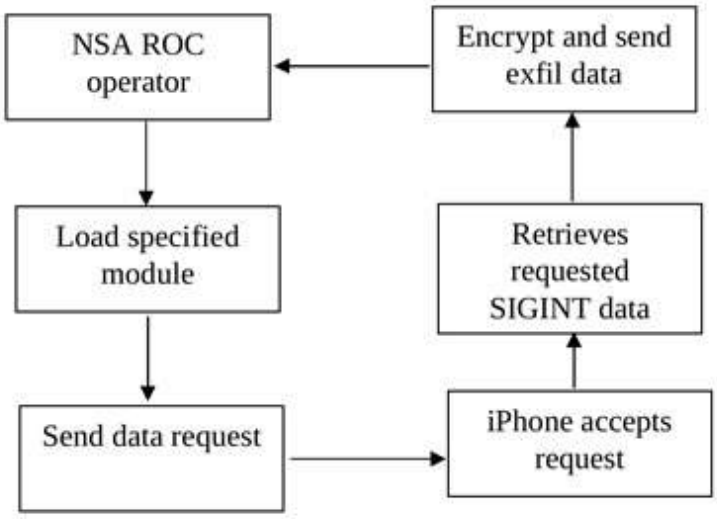
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

DROPOUTJEEP

ANT Product Data

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08



(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

Unit Cost: $ 0

Status: (U) In development

POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

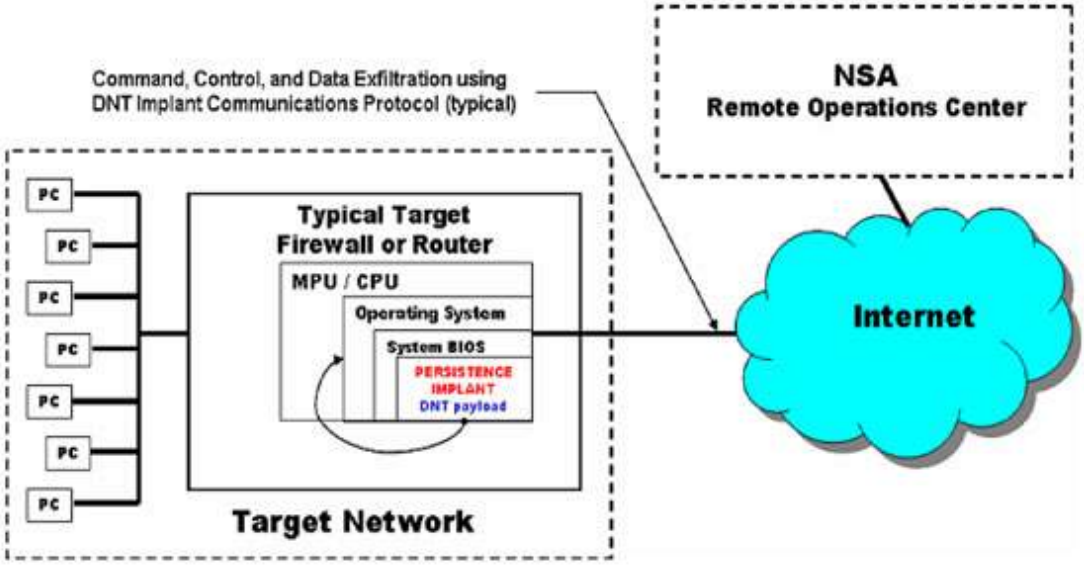
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

(TS//SI//REL) FEEDTROUGH can be used to persist two implants, ZESTYLEAK and/or BANANAGLEE across reboots and software upgrades on known and covered OS's for the following Netscreen firewalls, ns5xt, ns25, ns50, ns200, ns500 and ISG 1000. There is no direct communication to or from FEEDTROUGH, but if present, the BANANAGLEE implant can receive and transmit covert channel comms, and for certain platforms, BANANAGLEE can also update FEEDTROUGH. FEEDTROUGH however can only persist OS's included in it's databases. Therefore this is best employed with known OS's and if a new OS comes out, then the customer would need to add this OS to the FEEDTROUGH database for that particular firewall.

(TS//SI//REL) FEEDTROUGH operates every time the particular Juniper firewall boots. The first hook takes it to the code which checks to see if the OS is in the database, if it is, then a chain of events ensures the installation of either one or both implants. Otherwise the firewall boots normally. If the OS is one modified by DNT, it is not recognized, which gives the customer freedom to field new software.

Status: (S//SI//REL) FEEDTROUGH has on the shelf solutions for all of the listed platforms. It has been deployed on many target platforms

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

GODSURGE

ANT Product Data

(TS//SI//REL) GODSURGE runs on the FLUXBABBITT hardware implant and provides software application persistence on Dell PowerEdge servers by exploiting the JTAG debugging interface of the server's processors.

06/20/08

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 2950

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 1950

(TS//SI//REL) This technique supports Dell PowerEdge 1950 and 2950 servers that use the Xeon 5100 and 5300 processor families.

(TS//SI//REL) Through interdiction, the JTAG scan chain must be reconnected on the target system by removing the motherboard from the chassis and attaching the depopulated parts back onto the circuit board. After this step is complete, the hardware implant itself must be attached to the motherboard. The implants should already be programmed with the GODSURGE application code and its payload, the implant installer. Once implanted, GODSURGE's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $500 for Hardware and Installation

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

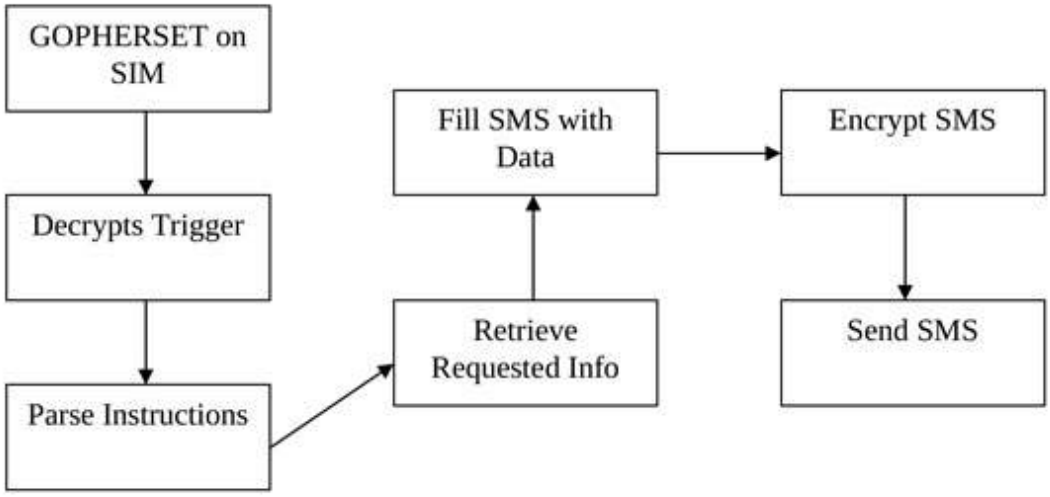
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

GOPHERSET

ANT Product Data

(TS//SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08



(U//FOUO) GOPHERSET – Operational Schematic

(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. GOPHERSET uses STK commands to retrieve the requested information and to exfiltrate data via SMS. After the GOPHERSET file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration.

Unit Cost: $0

Status: (U//FOUO) Released. Has not been deployed.

POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

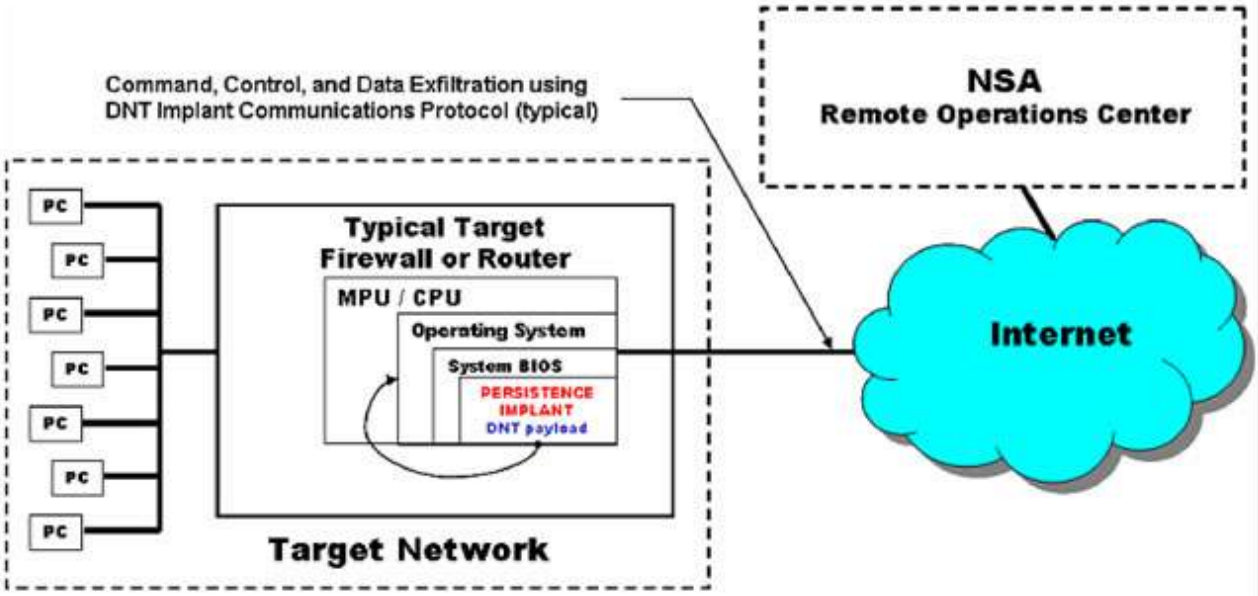
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

(TS//SI//REL)For supported platforms, DNT may configure BANANAGLEE without ANT involvement. Except for limited platforms, they may also configure PBD for minimal implant in the case where an OS unsupported by BANANAGLEE is booted.

Status: GOURMETTROUGH is on the shelf and has been deployed on many target platforms. It supports nsg5t, ns50, ns25, isg1000(limited). Soon- ssg140, ssg5, ssg20

Unit Cost: $0

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

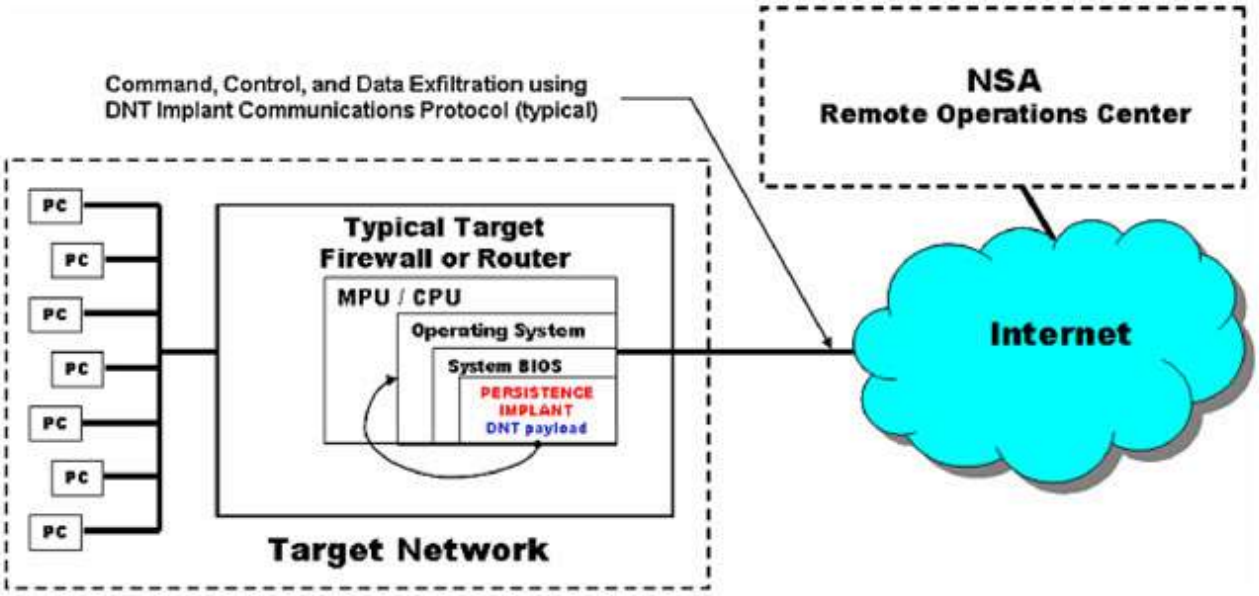
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

(TS//SI//REL) Once installed, HALLUXWATER communicates with an NSA operator via the TURBOPANDA Insertion Tool (PIT), giving the operator covert access to read and write memory, execute an address, or execute a packet.

(TS//SI//REL) HALLUXWATER provides a persistence capability on the Eudemon 200, 500, and 1000 series firewalls. The HALLUXWATER back door survives OS upgrades and automatic bootROM upgrades.

Status: (U//FOUO) On the shelf, and has been deployed.

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

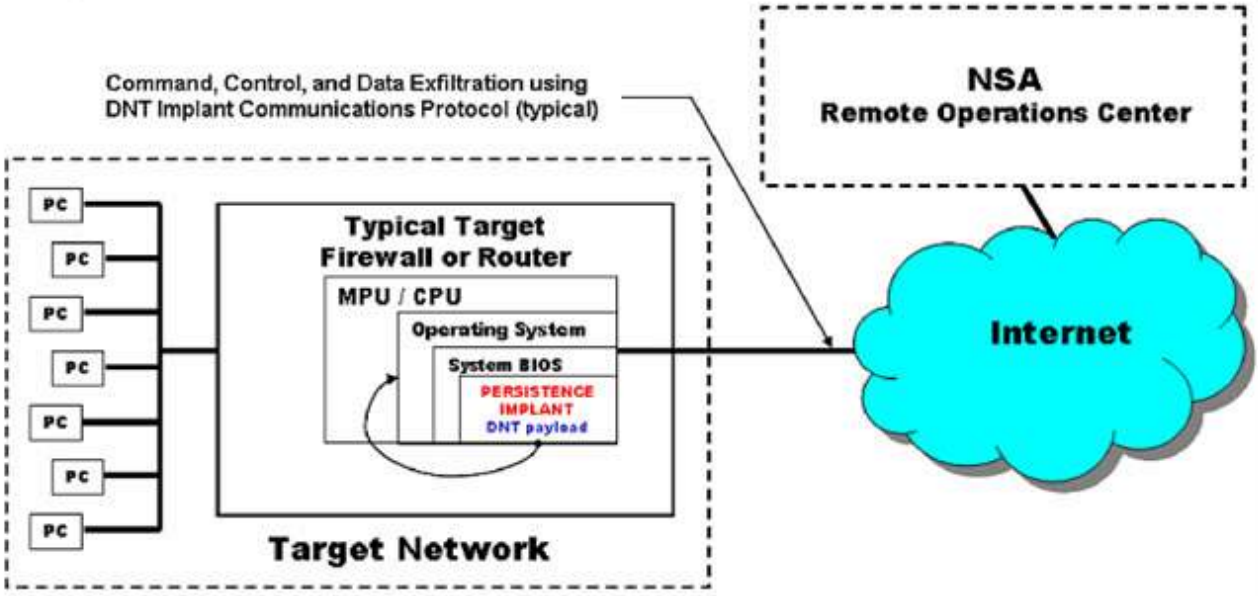
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

(TS//SI//REL) HEADWATER PBD implant will be transferred remotely over the Internet to the selected target router by Remote Operations Center (ROC) personnel. After the transfer process is complete, the PBD will be installed in the router's boot ROM via an upgrade command. The PBD will then be activated after a system reboot. Once activated, the ROC operators will be able to use DNT's HAMMERMILL Insertion Tool (HIT) to control the PBD as it captures and examines all IP packets passing through the host router.

(TS//SI//REL) HEADWATER is the cover term for the PBD for Huawei Technologies routers. PBD has been adopted for use in the joint NSA/CIA effort to exploit Huawei network equipment. (The cover name for this joint project is TURBOPANDA.)

Status: (U//FOUO) On the shelf ready for deployment.

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

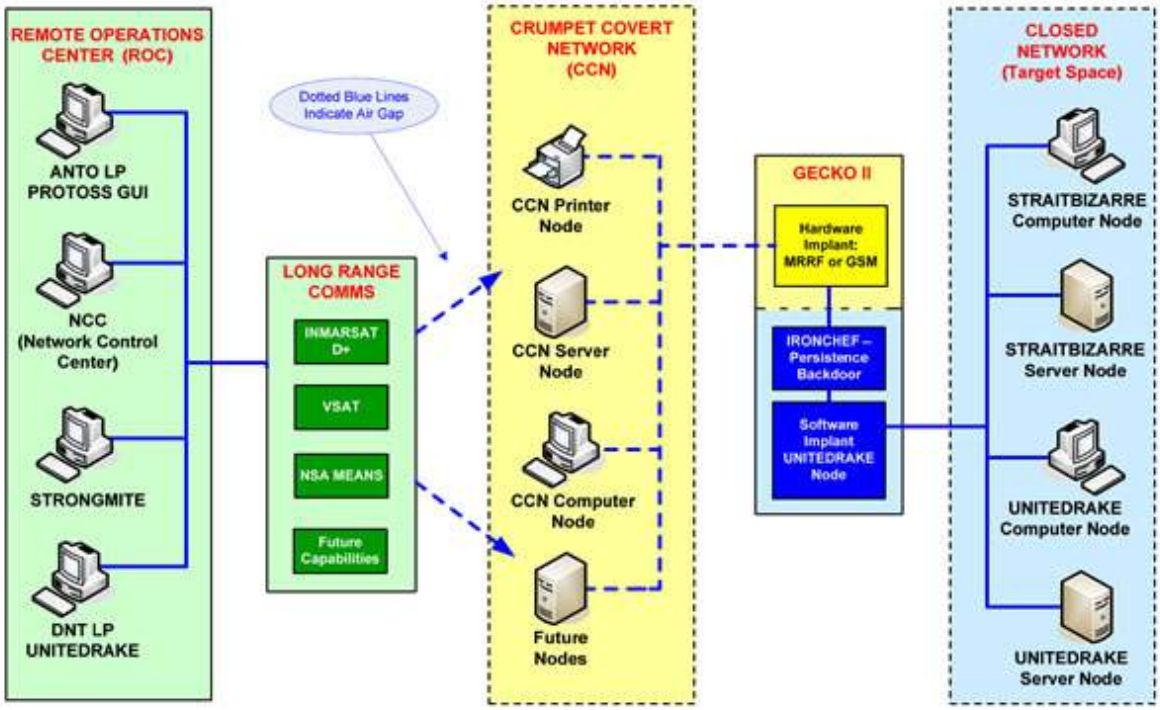
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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 I^2C Interface (WAGONBED).

(TS//SI//REL) Through interdiction, IRONCHEF, a software CNE implant and the hardware implant are installed onto the system. If the software CNE implant is removed from the target machine, IRONCHEF is used to access the machine, determine the reason for removal of the software, and then reinstall the software from a listening post to the target system.

Status: Ready for Immediate Delivery **Unit Cost:** $0

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

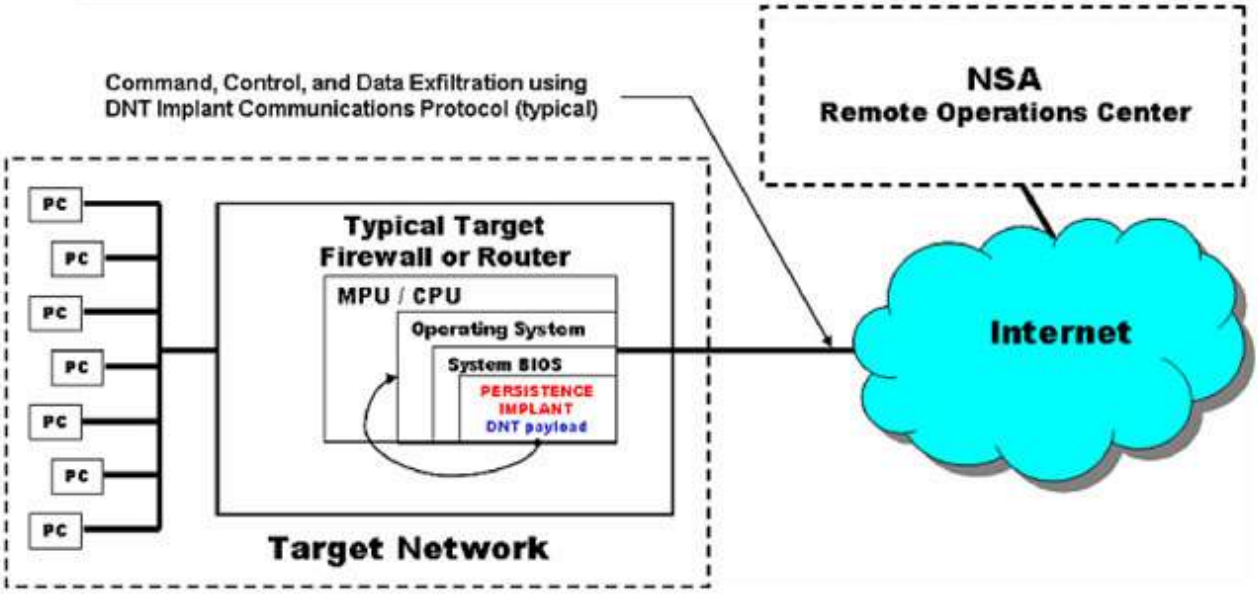
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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



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

(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 and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details).

Unit Cost: $0

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

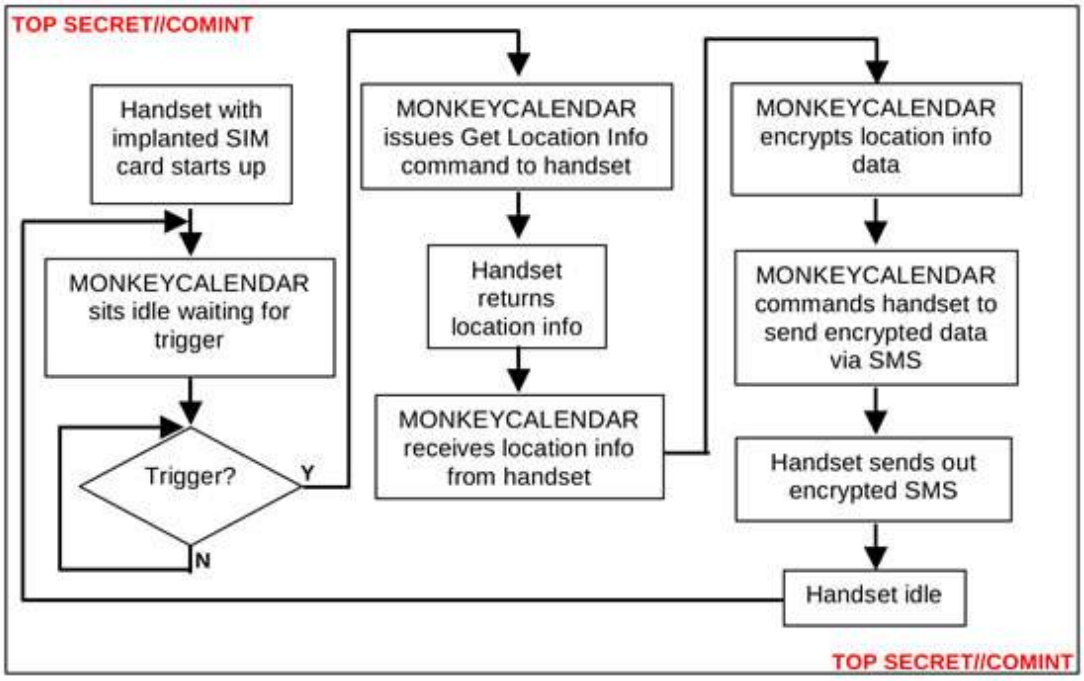
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

MONKEYCALENDAR

ANT Product Data

(TS//SI//REL) MONKEYCALENDAR is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls geolocation information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08



(U//FOUO) MONKEYCALENDAR – Operational Schematic

(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. MONKEYCALENDAR uses STK commands to retrieve location information and to exfiltrate data via SMS. After the MONKEYCALENDAR file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration

Unit Cost: $0

Status: Released, not deployed.

POC: U//FOUO [redacted], S32222, [redacted] [redacted]@nsa.gov

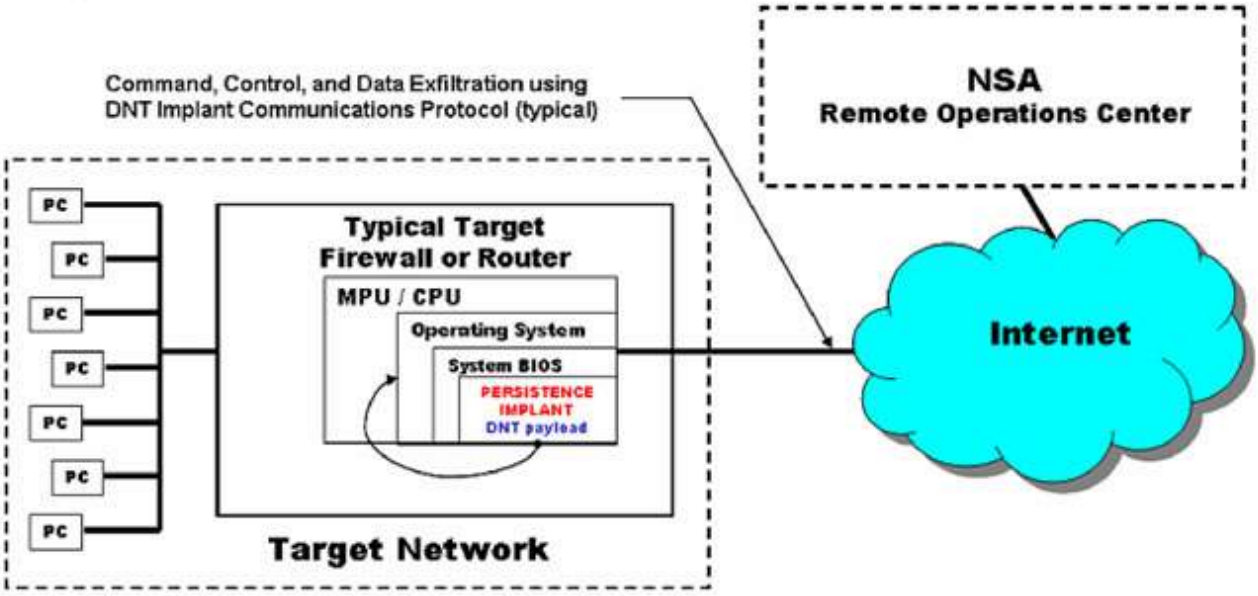
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SCHOOLMONTANA

ANT Product Data

(TS//SI//REL) SCHOOLMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

06/24/08



(S//SI//REL) SCHOOLMONTANA Concept of Operations

(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the SCHOOLMONTANA implant at the end of its native System Management Mode (SMM) handler.

(TS//SI//REL) SCHOOLMONTANA must support all modern versions of JUNOS, which is a version of FreeBSD customized by Juniper. Upon system boot, the JUNOS operating system is modified in memory to run the implant, and provide persistent kernel modifications to support implant execution.

(TS//SI//REL) SCHOOLMONTANA is the cover term for the persistence technique to deploy a DNT implant to Juniper J-Series routers.

Status: (U//FOUO) SCHOOLMONTANA completed and released by ANT May 30, 2008. It is ready for deployment.

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

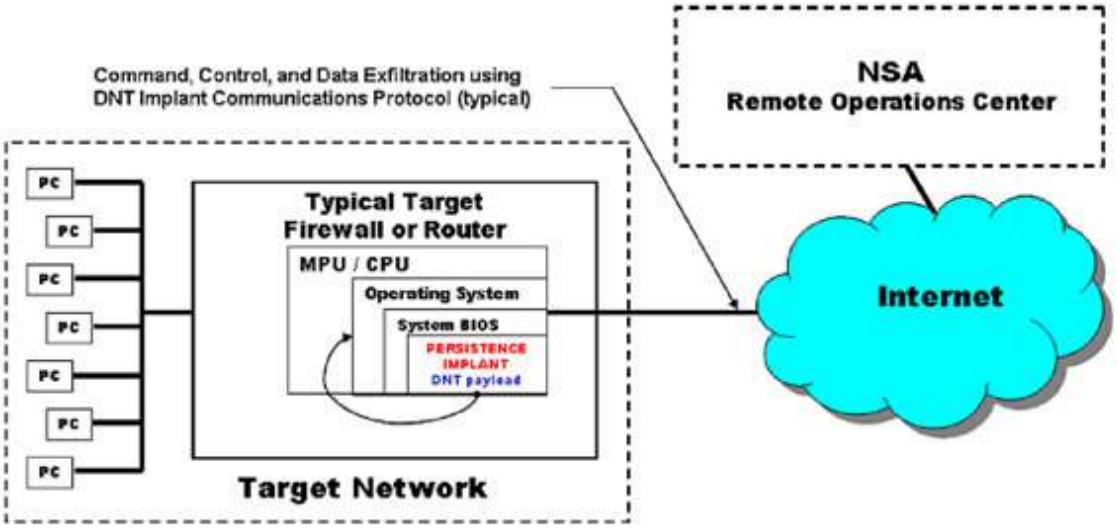
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SIERRAMONTANA

ANT Product Data

(TS//SI//REL) SIERRAMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

06/24/08



(S//SI//REL) SIERRAMONTANA Concept of Operations

(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the SIERRAMONTANA implant at the end of its native System Management Mode (SMM) handler.

(TS//SI//REL) SIERRAMONTANA must support all modern versions of JUNOS, which is a version of FreeBSD customized by Juniper. Upon system boot, the JUNOS operating system is modified in memory to run the implant, and provide persistent kernel modifications to support implant execution.

(TS//SI//REL) SIERRAMONTANA is the cover term for the persistence technique to deploy a DNT implant to Juniper M-Series routers.

Unit Cost: $

Status: (U//FOUO) SIERRAMONTANA under development and is expected to be released by 30 November 2008.

POC: U//FOUO [redacted], S32222, [redacted] [redacted]@nsa.gov

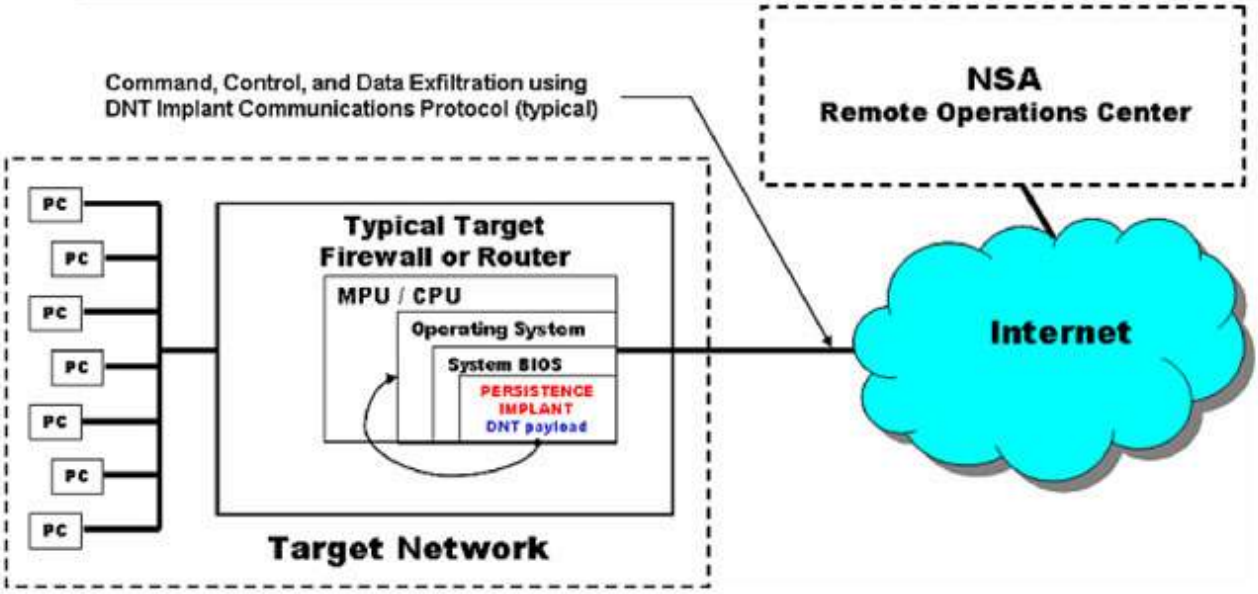
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

(TS//SI//REL) SOUFFLETROUGH is a BIOS persistence implant for Juniper SSG 500 and SSG 300 series firewalls {320M, 350M, 520, 550, 520M, 550M}. It persists DNT's BANANAGLEE software implant and modifies the Juniper firewall's operating system (ScreenOS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. It takes advantage of Intel's System Management Mode for enhanced reliability and covertness. The PBD is also able to beacon home, and is fully configurable.

(TS//SI//REL) A typical SOUFFLETROUGH deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. SOUFFLETROUGH is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been deployed. There are no availability restrictions preventing ongoing deployments.

Unit Cost: $0

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

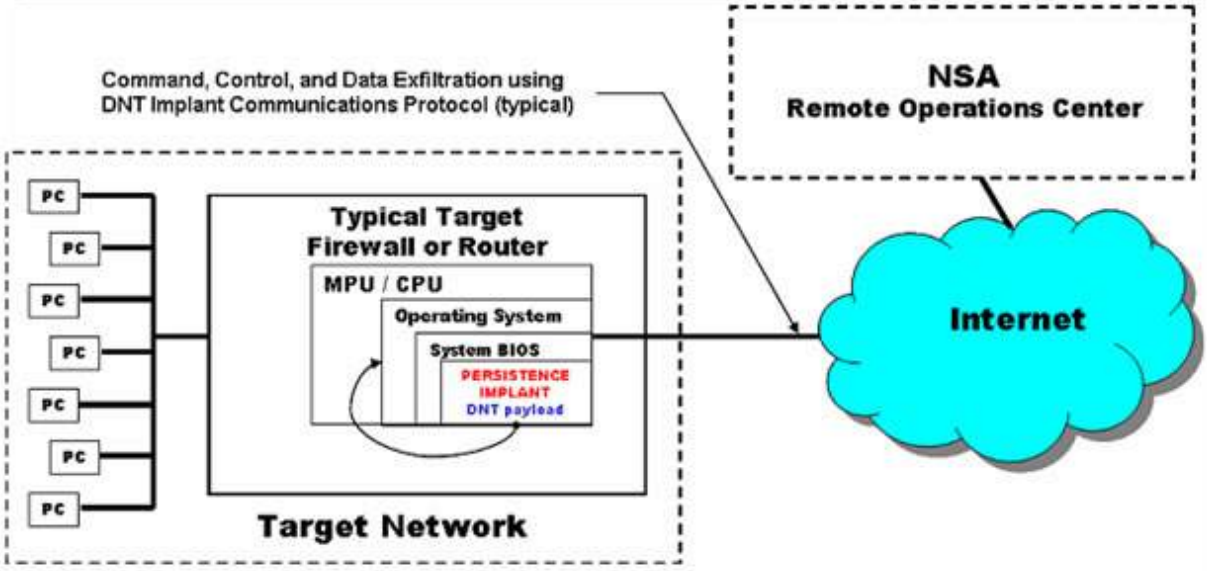
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

STUCCOMONTANA

ANT Product Data

(TS//SI//REL) STUCCOMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

06/24/08



(S//SI//REL) STUCCOMONTANA Concept of Operations

(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the STUCCOMONTANA implant at the end of its native System Management Mode (SMM) handler.

(TS//SI//REL) STUCCOMONTANA must support all modern versions of JUNOS, which is a version of FreeBSD customized by Juniper. Upon system boot, the JUNOS operating system is modified in memory to run the implant, and provide persistent kernel modifications to support implant execution.

(TS//SI//REL) STUCCOMONTANA is the cover term for the persistence technique to deploy a DNT implant to Juniper T-Series routers.

Unit Cost: $

Status: (U//FOUO) STUCCOMONTANA under development and is expected to be released by 30 November 2008.

POC: U//FOUO [redacted], S32222, [redacted] [redacted]@nsa.gov

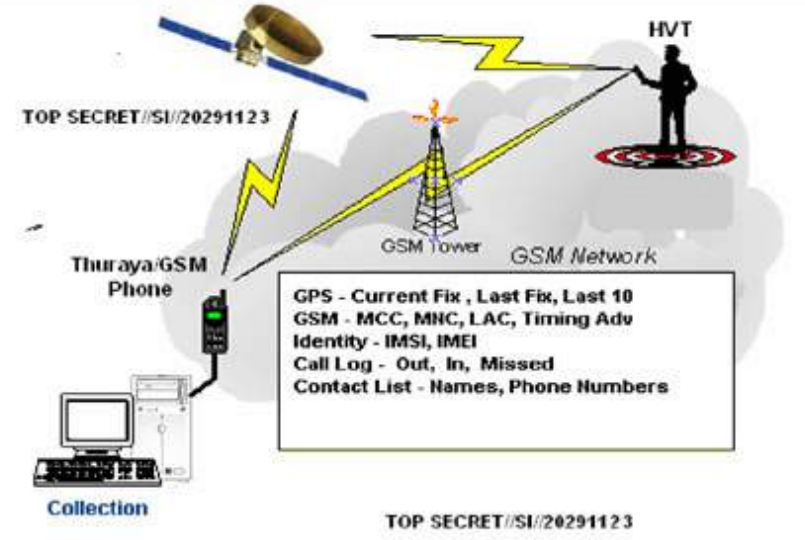
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOTECHASER

ANT Product Data

10/01/08

(TS//SI//REL) TOTECHASER is a Windows CE implant targeting the Thuraya 2520 handset. The Thuraya 2520 is a dual mode phone that can operate either in SAT or GSM modes. The phone also supports a GPRS data connection for Web browsing, e-mail, and MMS messages. The initial software implant capabilities include providing GPS and GSM geo-location information. Call log, contact list, and other user information can also be retrieved from the phone. Additional capabilities are being investigated.



(U//FOUO) TOTECHASER – Operational Schematic

(TS//SI//REL) TOTECHASER will use SMS messaging for the command, control, and data exfiltration path. The initial capability will use covert SMS messages to communicate with the handset. These covert messages can be transmitted in either Thuraya Satellite mode or GSM mode and will not alert the user of this activity. An alternate command and control channel using the GPRS data connection based on the TOTEGHOSTLY implant is intended for a future version.

(TS//SI//REL) Prior to deployment, the TOTECHASER handsets must be modified. Details of how the phone is modified are being developed. A remotely deployable TOTECHASER implant is being investigated. The TOTECHASER system consists of the modified target handsets and a collection system.

(TS//SI//REL) TOTECHASER will accept configuration parameters to determine how the implant operates. Configuration parameters will determine what information is recorded, when to collect that information, and when the information is exfiltrated. The configuration parameters can be set upon initial deployment and updated remotely.

Unit Cost: $

Status:

POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

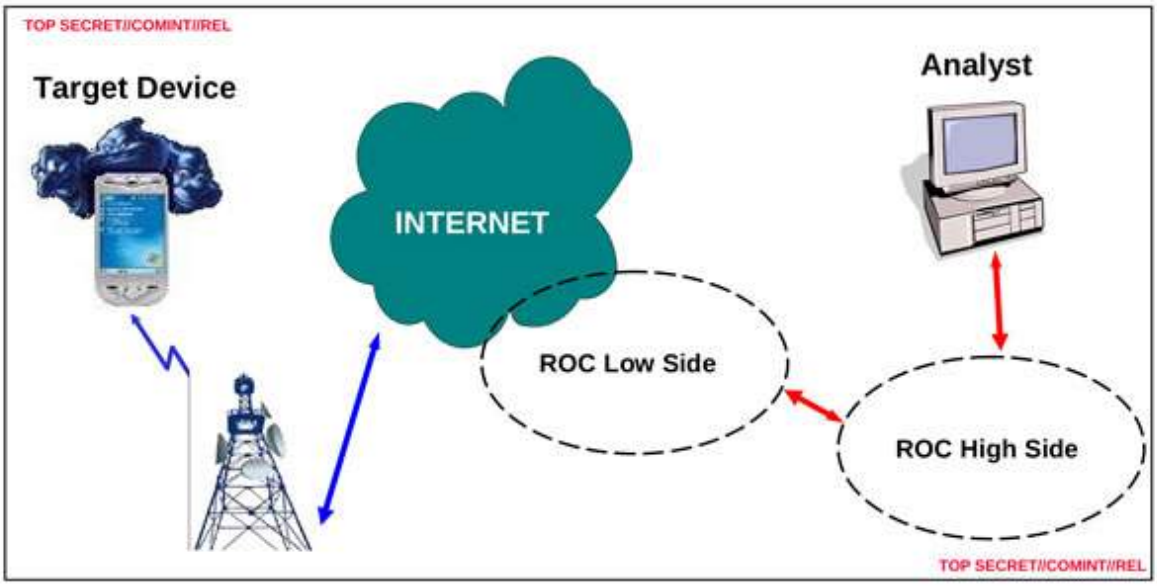
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOTEGHOSTLY 2.0

ANT Product Data

(TS//SI//REL) TOTEGHOSTLY 2.0 is a STRAITBIZARRE based implant for the Windows Mobile embedded operating system and uses the CHIMNEYPOOL framework. TOTEGHOSTLY 2.0 is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08



(U//FOUO) TOTEGHOSTLY – Data Flow Schematic

(TS//SI//REL) TOTEGHOSTLY 2.0 is a software implant for the Windows Mobile operating system that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. A FRIEZERAMP interface using HTTPSlink2 transport module handles encrypted communications.

(TS//SI//REL) The initial release of TOTEGHOSTLY 2.0 will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

(TS//SI//REL) TOTEGHOSTLY 2.0 will be controlled using an interface tasked through the NCC (Network Control Center) utilizing the XML based tasking and data forward scheme under the TURBULENCE architecture following the TAO GENIE Initiative.

Unit Cost: $0

Status: (U) In development

POC: U//FOUO [redacted], S32222, [redacted] [redacted]@nsa.gov

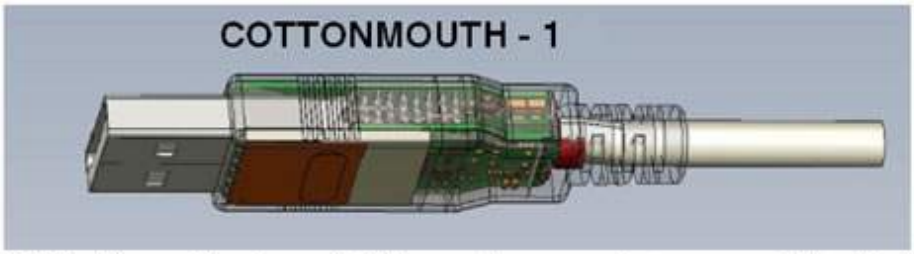
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

COTTONMOUTH-I

ANT Product Data

08/05/08

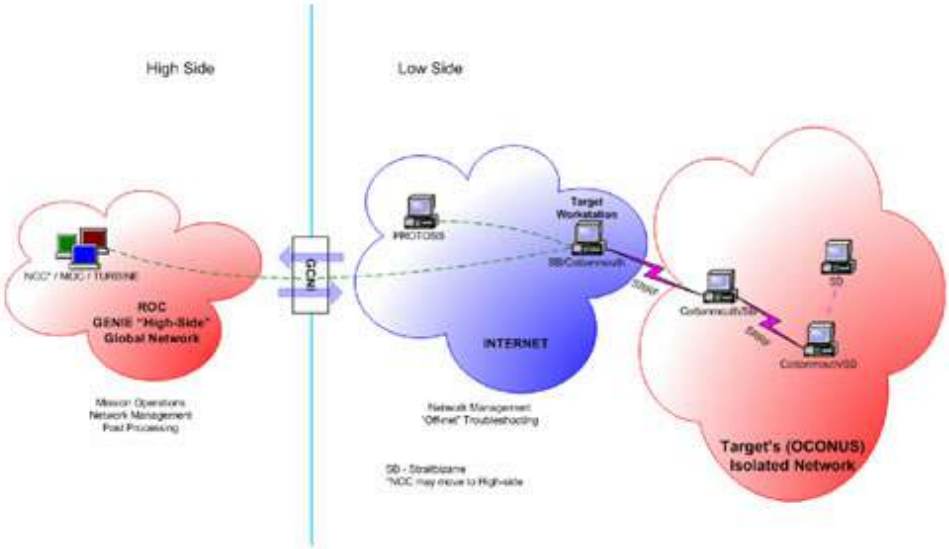
(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.



(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 CONOP
INTERNET Scenario



Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

COTTONMOUTH-II

ANT Product Data

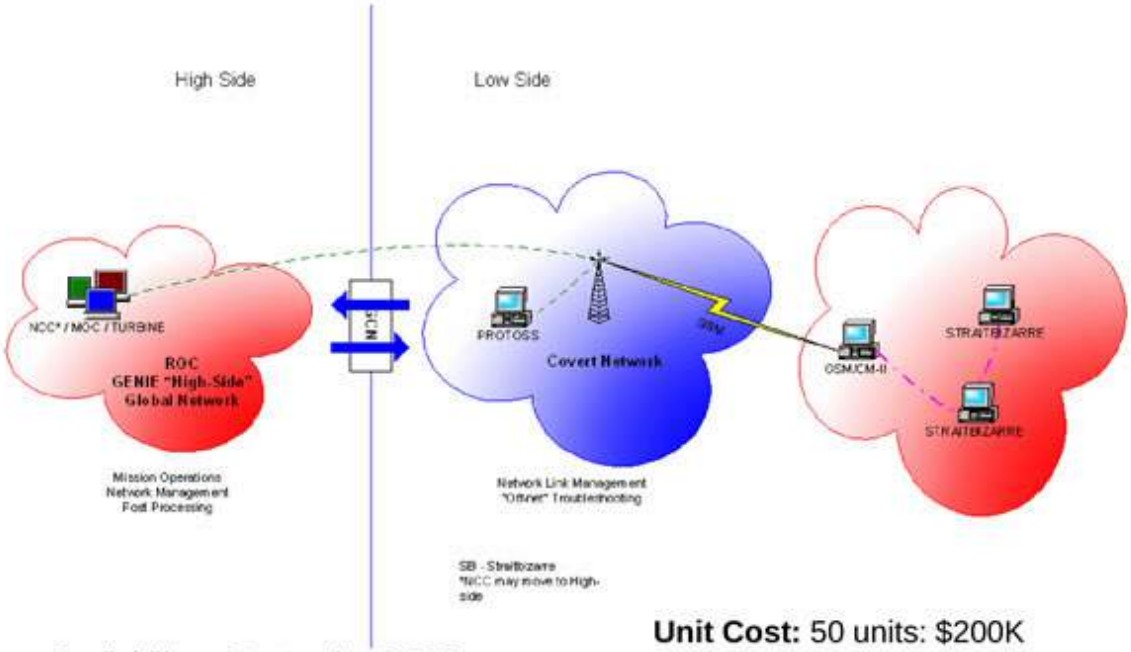
(TS//SI//REL) COTTONMOUTH-II (CM-II) is a Universal Serial Bus (USB) hardware Host Tap, which will provide a covert link over USB link into a targets network. CM-II is intended to be operate with a long haul relay subsystem, which is co-located within the target equipment. Further integration is needed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

08/05/08

(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 - II (CM-II) CONOP
ANT Covert Network Scenario



Unit Cost: 50 units: $200K

Status: Availability – September 2008

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

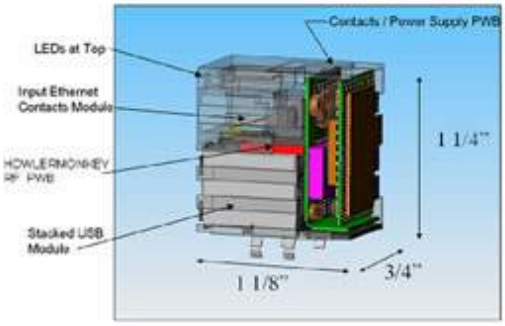
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

COTTONMOUTH-III

ANT Product Data

08/05/08

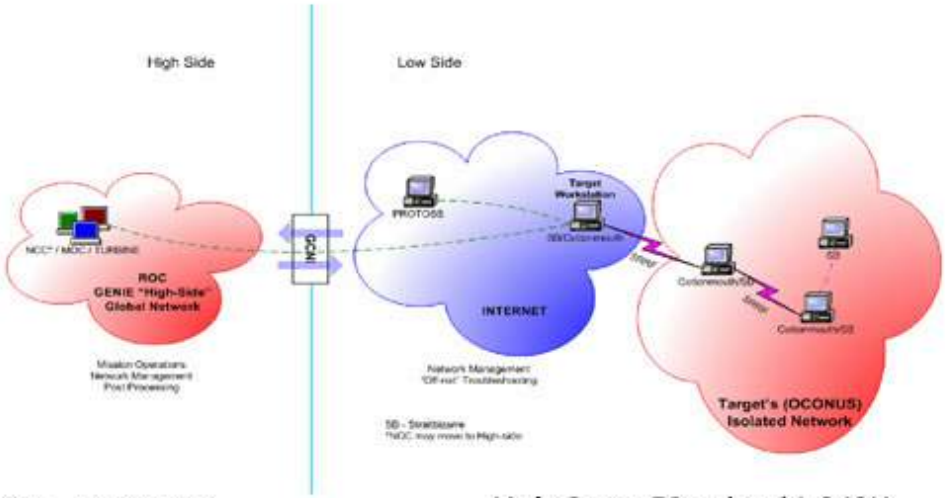
(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant, which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.



(TS//SI//REL) CM-III 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-III 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-III will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-III conceals digital components (TRINITY), a USB 2.0 HS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within a RJ45 Dual Stacked USB connector. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION. CM-III can provide a short range inter-chassis link to other CM devices or an intra-chassis RF link to a long haul relay subsystem.

COTTONMOUTH CONOP
INTERNET Scenario



Status: Availability – May 2009

Unit Cost: 50 units: $1,248K

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

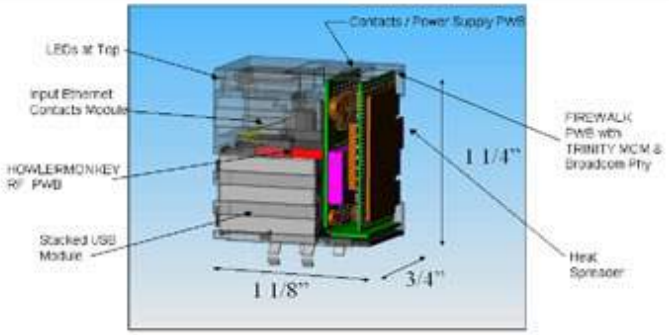
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

FIREWALK

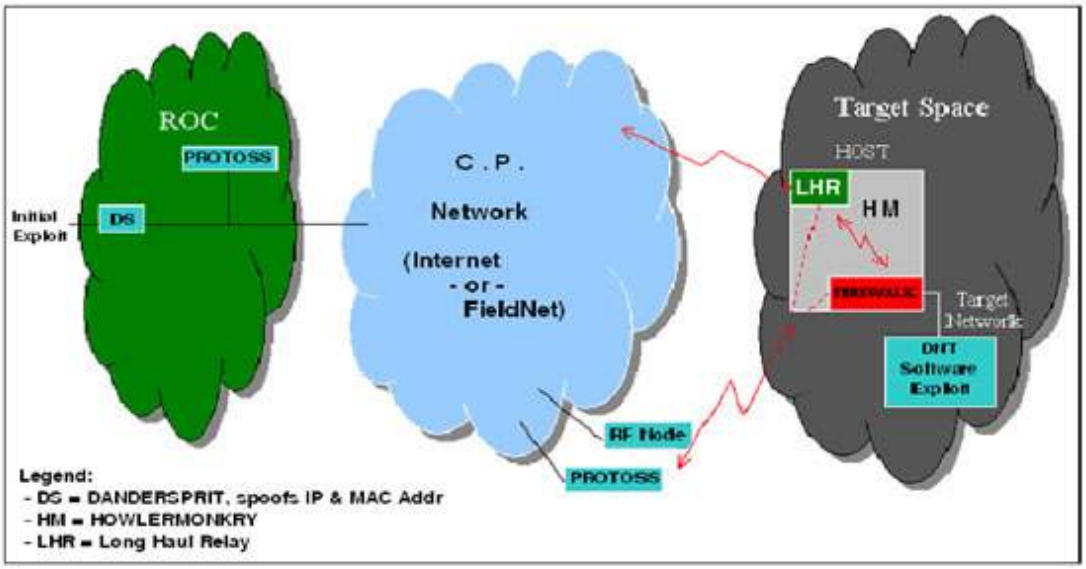
ANT Product Data

08/05/08

(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.



(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.



Status: Prototype Available – August 2008

Unit Cost: 50 Units $537K

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

CTX4000

ANT Product Data

(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

8 Jul 2008

(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- Frequency Range: 1 - 2 GHz.
- Bandwidth: Up to 45 MHz
- Output Power: User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.
- Phase adjustment with front panel knob
- User-selectable high- and low-pass filters.
- Remote controllable
- Outputs:
- Transmit antenna
- I & Q video outputs
- DC bias for an external pre-amp on the Receive input connector
- Inputs:
    - External oscillator
    - Receive antenna

Unit Cost: N/A

Status: unit is operational. However, it is reaching the end of its service life. It is scheduled to be replaced by PHOTOANGLO starting in September 2008.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

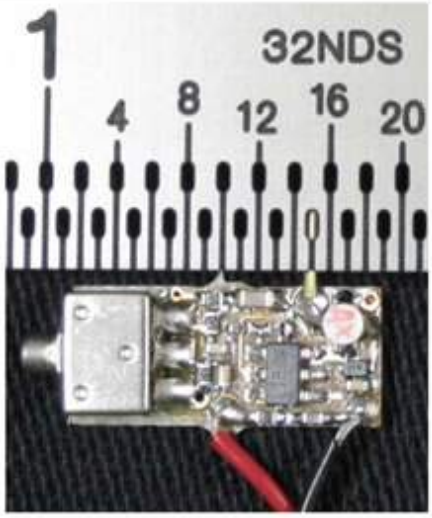
LOUDAUTO

ANT Product Data

07 Apr 2009

(TS//SI//REL TO USA,FVEY) Audio-based RF retro-reflector. Provides room audio from targeted space using radar and basic post-processing.

(U) Capabilities



(TS//SI//REL TO USA,FVEY) LOUDAUTO's current design maximizes the gain of the microphone. This makes it extremely useful for picking up room audio. It can pick up speech at a standard, office volume from over 20' away. (NOTE: Concealments may reduce this distance.) It uses very little power (~15 uA at 3.0 VDC), so little, in fact, that battery self-discharge is more of an issue for serviceable lifetime than the power draw from this unit. The simplicity of the design allows the form factor to be tailored for specific operational requirements. All components at COTS and so are non-attributable to NSA.

(U) Concept of Operation

TS//SI//REL TO USA,FVEY) Room audio is picked up by the microphone and converted into an analog electrical signal. This signal is used to pulse position modulate (PPM) a square wave signal running at a pre-set frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal from a nearby radar unit, the illuminating signal is amplitude-modulated with the PPM square wave. This signal is re-radiated, where it is picked up by the radar, then processed to recover the room audio. Processing is currently performed by COTS equipment with FM demodulation capability (Rohde & Schwarz FSH-series portable spectrum analyzers, etc.) LOUDAUTO is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

Unit Cost: $30

Status: End processing still in development

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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 Hardware

(TS//SI//REL) Use of external amplifiers and antennas in both experimental and operational scenarios have resulted in successful NIGHTSTAND attacks from as far away as eight miles under ideal environmental conditions.

Unit Cost: Varies from platform to platform

Status: Product has been deployed in the field. Upgrades to the system continue to be developed.

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

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

NIGHTWATCH

ANT Product Data

(TS//SI//REL TO USA,FVEY) NIGHTWATCH is a portable computer with specialized, internal hardware designed to process progressive-scan (non-interlaced) VAGRANT signals.

24 Jul 2008

(U) Capability Summary

(TS//SI//REL TO USA,FVEY) The current implementation of NIGHTWATCH consists of a general-purpose PC inside of a shielded case. The PC has PCI digitizing and clock cards to provide the needed interface and accurate clocking required for video reconstruction. It also has:

- horizontal sync, vertical sync and video outputs to drive an external, multi-sync monitor.
- video input
- spectral analysis up to 150 kHz to provide for indications of horizontal and vertical sync frequencies
- frame capture and forwarding
- PCMCIA cards for program and data storage
- horizontal sync locking to keep the display set on the NIGHTWATCH display.
- frame averaging up to 2^16 (65536) frames.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The video output from an appropriate collection system, such as a CTX4000, PHOTOANGLO, or general-purpose receiver, is connected to the video input on the NIGHTWATCH system. The user, using the appropriate tools either within NIGHTWATCH or externally, determines the horizontal and vertical sync frequencies of the targeted monitor. Once the user matches the proper frequencies, he activates "Sync Lock" and frame averaging to reduce noise and improve readability of the targeted monitor. If warranted, the user then forwards the displayed frames over a network to NSAW, where analysts can look at them for intelligence purposes.

Unit Cost: N/A

Status: This system has reached the end of its service life. All work concerning the NIGHTWATCH system is strictly for maintenance purposes. This system is slated to be replaced by the VIEWPLATE system.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

PHOTOANGLO

ANT Product Data

(TS//SI//REL TO USA,FVEY) PHOTOANGLO is a joint NSA/GCHQ project to develop a new radar system to take the place of the CTX4000.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) The planned capabilities for this system are:

- •Frequency range: 1 - 2 GHz, which will be later extended to 1 - 4 GHz.
- •Maximum bandwidth: 450 MHz.
- •Size: Small enough to fit into a slim briefcase.
- •Weight: Less than 10 lbs.
- •Maximum Output Power: 2 W
- •Output:
- •Video
- •Transmit antenna
- •Inputs:
- •External oscillator
- •Receive antenna

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) TS//SI//REL TO USA,FVEY) The radar unit generates an un-modulated, continuous wave (CW) signal. The oscillator is either generated internally, or externally through a signal generator or cavity oscillator. The unit amplifies the signal and sends it out to an RF connector, where it is directed to some form of transmission antenna (horn, parabolic dish, LPA, spiral). The signal illuminates the target system and is re-radiated. The receive antenna picks up the re-radiated signal and directs the signal to the receive input. The signal is amplified, filtered, and mixed with the transmit antenna. The result is a homodyne receiver in which the RF signal is mixed directly to baseband. The baseband video signal is ported to an external BNC connector. This connects to a processing system, such as NIGHTWATCH, an LFS-2, or VIEWPLATE, to process the signal and provide the intelligence.

Unit Cost: $40k (planned)

Status: Development. Planned IOC is 1st QTR FY09.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

PICASSO

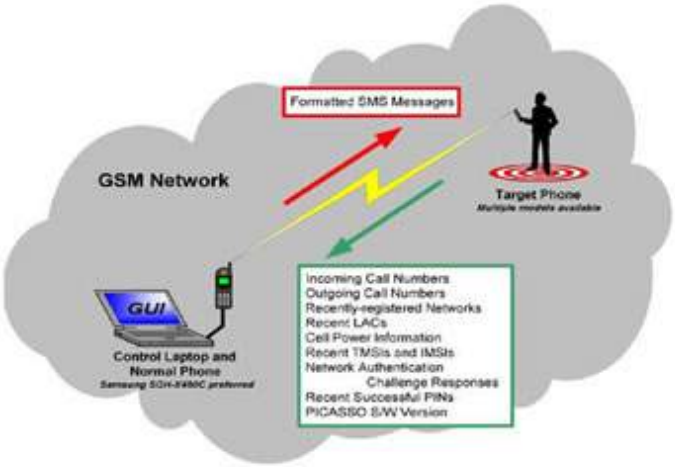
GSM HANDSET

(S//SI//REL) Modified GSM (target) handset that collects user data, location information and room audio. Command and data exfil is done from a laptop and regular phone via SMS – (Short Messaging Service), without alerting the target.

06/20/08

(S//SI) Target Data via SMS:

- Incoming call numbers
- Outgoing call numbers
- Recently registered networks
- Recent Location Area Codes (LAC)
- Cell power and Timing Advance information (GEO)
- Recently Assigned TMSI, IMSI
- Recent network authentication challenge responses
- Recent successful PINs entered into the phone during the power-on cycle
- SW version of PICASSO implant
- ' Hot-mic' to collect Room Audio
- Panic Button sequence (sends location information to an LP Operator)
- Send Targeting Information (i.e. current IMSI and phone number when it is turned on - in case the SIM has just been switched).
- Block call to deny target service.



(S//SI) PICASSO Operational Concept

(S//SI//REL) Uses include asset validation and tracking and target templating. Phone can be hot mic'd and has a "Panic Button" key sequence for the witting user.

Status: 2 weeks ARO (10 or less)

Unit Cost: approx $2000

(S//SI//REL) Handset Options

- Eastcom 760c+
- Samsung E600, X450
- Samsung C140
- (with Arabic keypad/language option)

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

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

RAGEMASTER

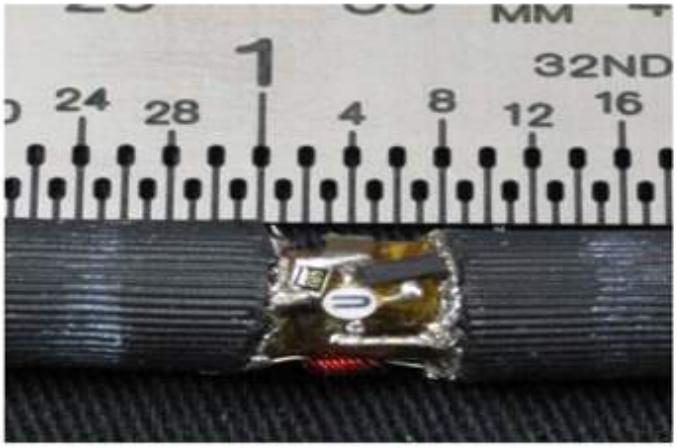
ANT Product Data

(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.

24 Jul 2008

(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.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: $ 30

Status: Operational. Manufactured on an as-needed basis. Contact POC for availability information.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

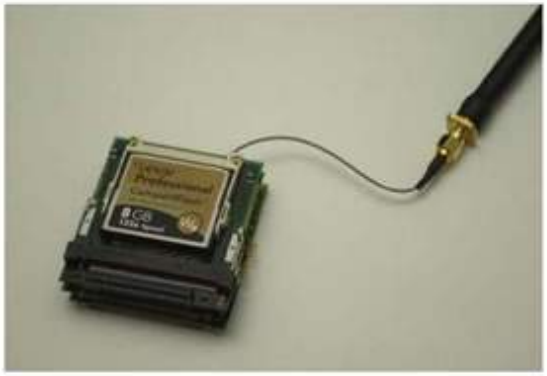
Processor: IBM Power PC 405GPR
Memory: 64MB (SDRAM)
16MB (FLASH)

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

(TS//SI//REL) The Sparrow II is a capable option for deployment where small size, minimal weight and reduced power consumption are required. PCI devices can be connected to the Sparrow II to provide additional functionality, such as wireless command and control or a second or third 802.11 card. The Sparrow II is shipped with Linux and runs the BLINDDATE software suite.

Unit Cost: $6K

Status: (S//SI//REL) Operational Restrictions exist for equipment deployment.

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

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SURLYSPAWN

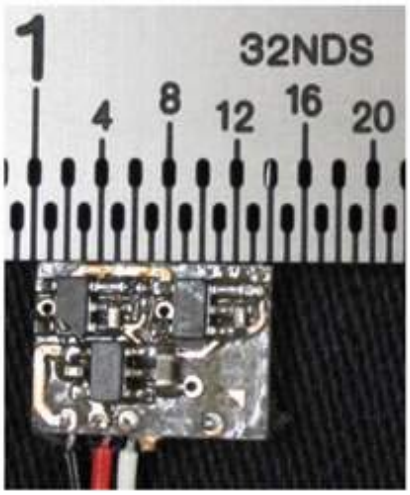
ANT Product Data

(TS//SI//REL TO USA,FVEY) Data RF retro-reflector. Provides return modulated with target data (keyboard, low data rate digital device) when illuminated with radar.

07 Apr 2009

(U) Capabilities

(TS//SI//REL TO USA,FVEY) SURLYSPAWN has the capability to gather keystrokes without requiring any software running on the targeted system. It also only requires that the targeted system be touched once. The retro-reflector is compatible with both USB and PS/2 keyboards. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities will include laptop keyboards.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board taps into the data line from the keyboard to the processor. The board generates a square wave oscillating at a preset frequency. The data-line signal is used to shift the square wave frequency higher or lower, depending on the level of the data-line signal. The square wave, in essence, 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 signal is re-radiated, where it is received by the radar, demodulated, and the demodulated signal is processed to recover the keystrokes. SURLYSPAWN is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

Unit Cost: $30

Status: End processing still in development

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

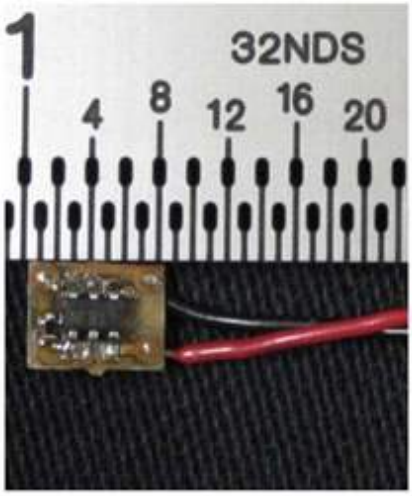
TAWDRYYARD

ANT Product Data

(TS//SI//REL TO USA,FVEY) Beacon RF retro-reflector. Provides return when illuminated with radar to provide rough positional location.

07 Apr 2009

(U) Capabilities



(TS//SI//REL TO USA,FVEY) TAWDRYYARD is used as a beacon, typically to assist in locating and identifying deployed RAGEMASTER units. Current design allows it to be detected and located quite easily within a 50' radius of the radar system being used to illuminate it. TAWDRYYARD draws as 8 µA at 2.5V (20µW) allowing a standard lithium coin cell to power it for months or years. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities being considered are return of GPS coordinates and a unique target identifier and automatic processing to scan a target area for presence of TAWDRYYARDs. All components are COTS and so are non-attributable to NSA.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board generates a square wave operating at a preset frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal, the illuminating signal is amplitude-modulated (AM) with the square wave. This signal is re-radiated, where it is picked up by the radar, then processed to recover the clock signal. Typically, the fundamental is used to indicate the unit's presence, and is simply displayed on a low frequency spectrum analyzer. TAWDRYYARD is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

Unit Cost: $30

Status: End processing still in development

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108