Раскрыт список «жучков» АНБ США для техники Cisco, Huawei и Juniper. ФОТО

Безопасность версия для КПК

10.01.14, Пт, 17:46, Мск, Текст: Сергей Попсулин /

Каталог включает жучки для межсетевых экранов Cisco, Huawei и Juniper, серверов Dell PowerEdge, SIM-карт, кабелей USB, LAN и VGA, прототип жучка для iPhone и т. д. Помимо жучков, в каталог входит оборудование, предназначенное для прослушки.

Читайте также:

Новая версия Trojan.Mods способна добывать Bitcoin

Ведущий мировой разработчик шифров снизил их надежность за взятку $10 млн от властей США

Троян-добытчик биткоинов раскрывает имя своего создателя

Германское издание Spiegel опубликовало 48 страниц каталога «жучков» АНБ США (Агентства национальной безопасности), предназначенных для внедрения и перехвата данных в оборудовании известных американских и азиатских производителей. Каталог датирован 2008-2009 г.г.

Каталог включает программные жучки для межсетевых экранов Cisco (линейка PIX 500, модели ASA 5505, 5510, 5520, 5540 и 5550), Huawei (линейки Eudemon 200, 500 и 1000) и Juniper (Netscreen ns5xt, ns25, ns50, ns200, isg1000, nsg5t, SSG 320M, 350M, 520, 520M и 550M).

В каталог также входят программные жучки для SIM-карт, используемых в сетях GSM. Они позволяют извлекать контакты, SMS-сообщения, историю звонков и геолокационные данные с телефона и отправлять их на заданный мобильный номер по SMS.

В каталоге также представлены аппаратные жучки для USB- и LAN-кабелей (перехватывают данные), VGA-кабелей (позволяют перехватывать видеосигнал, идущий с ПК на монитор), жучки для компьютеров и прочих вычислительных систем на базе Windows, Linux, FreeBSD и Solaris, мобильных устройств на Windows Mobile, а также для серверов Dell PowerEdge (1950, 2950) и HP ProLiant 380DL G5, системы имитации базовых станций сотовой связи и модифицированные телефоны Samsung и других производителей с интегрированной системой прослушки.

Разработкой всех жучков занимается подразделение ANT. Сотрудники АНБ могут заказывать у него жучки, которые им необходимы для слежки. Большинство жучков бесплатны, однако есть и платные - стоимость варьируется до $250 тыс. (столько стоит решение для развертывания готовых мобильных сетей).

Некоторые жучки находятся в разработке: например, программный жучок для Apple iPhone. Он должен позволить удаленно записывать и извлекать файлы со смартфона, получать список SMS-сообщений, список контактов, доступ к голосовой почте, микрофону, камере и информации о текущих координатах абонента. Управление жучком предлагается осуществлять с помощью SMS-команд или посредством GPRS-соединения.

Список жучков и оборудования

RAGEMASTER - жучок для перехвата видеосигнала на монитор
JETPLOW - жучок для межсетевых экранов Cisco
HALLUXWATER - жучок для межсетевых экранов Huawei
FEEDTROUGH - жучок для межсетевых экранов Juniper
GOURMETTROUGH - жучок для межсетевых экранов Juniper
SOUFFLETROUGH - жучок для межсетевых экранов Juniper
DROPOUTJEEP - жучок для Apple iPhone (разрабатывается)
GOPHERSET - жучок для SIM-карт
MONKEYCALENDAR - жучок для SIM-карт
TOTECHASER - жучок для мобильного телефона Thuraya 2520
TOTEGHOSTLY 2.0 - жучок для устройств на базе Windows Mobile
PICASSO - комплект модифицированных мобильных телефонов Samsung и Eastcom
CROSSBEAM - GSM-модуль
CANDYGRAM - имитатор базовой станции сети GSM
CYCLONE Hx9 - решение для развертывания сети сотовой сети
EBSR - оборудование для сотовой связи
ENTOURAGE - оборудование для сотовой связи
GENESIS - модифицированный мобильный телефон
NEBULA - решение для развертывания сети сотовой сети
TYPHON HX - оборудование для сотовой связи
WATERWITCH - устройство для выявления координат мобильных телефонов
CTX4000 - портативный радар
LOUDAUTO - передатчик звука
NIGHTWATCH - портативный компьютер для сканирования сигналов
PHOTOANGLO - система радаров
TAWDRYYARD - передатчик
GINSU - жучок для вычислительных систем на базе Windows
IRATEMONK - жучок для персональных компьютеров

SWAP - жучок для персональных компьютеров
WISTFULTOLL - жучок для персональных компьютеров
HOWLERMONKEY - передатчик
JUNIORMINT - мини-ПК
MAESTRO-II - мини-ПК
SOMBERKNAVE - жучок для локальных сетей
TRINITY - мини-ПК
HEADWATER - жучок для роутеров Huawei
SCHOOLMONTANA - жучок для роутеров Juniper
SIERRAMONTANA - жучок для роутеров Juniper
STUCCOMONTANA - жучок для роутеров Juniper
DEITYBOUNCE - жучок для серверов Dell
GODSURGE - жучок для серверов Dell
IRONCHEF - жучок для серверов HP
SURLYSPAWN - передатчик
COTTONMOUTH-I - жучок для соединений USB
COTTONMOUTH-II - жучок для соединений USB
COTTONMOUTH-III - жучок для соединений USB
FIREWALK - жучок для соединений LAN
NIGHTSTAND - оборудование связи

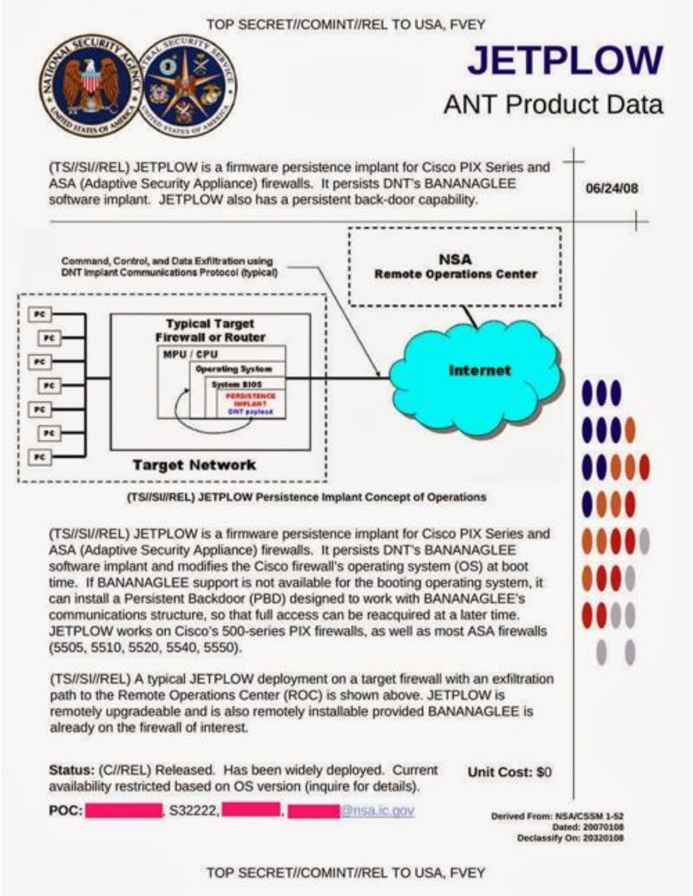
Жучки АНБ созданы таким образом, чтобы они могли продолжать работать после перезагрузки и даже обновления прошивки оборудования. Внедрение осуществляется с помощью различных уязвимостей, технических интерфейсов, BIOS, загрузочных секторов и т. п.

Вендоры отреагировали на публикацию Spiegel, отрицая наличие любых форм сотрудничества со спецслужбами. Старший вице-президент, глава по безопасности Cisco Джон Стюарт (John Stewart) заявил, что компания не сотрудничает с государственными органами и не помещает в свое оборудование бэкдоры. Он также сказал, что в настоящее время экспертам Cisco неизвестны какие-либо уязвимости в решениях компании, которые могли быть использованы для внедрения бэкдоров.

Российский офис Cisco на вопросы CNews не ответил.

В российском офисе Samsung на запрос издания CNews ответили следующим образом: «Samsung следует законодательным нормам тех стран, в которых ведет бизнес. В настоящее время мы ведем процесс сертификации жестких дисков, которые будут поставляться на территорию РФ. До завершения процесса сертификации, официальных поставок жестких дисков Samsung на территории России не будет».

Системы для контроля над сетевыми экранами



TOP SECRET//COMINT//REL TO USA, FVEY

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

(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).

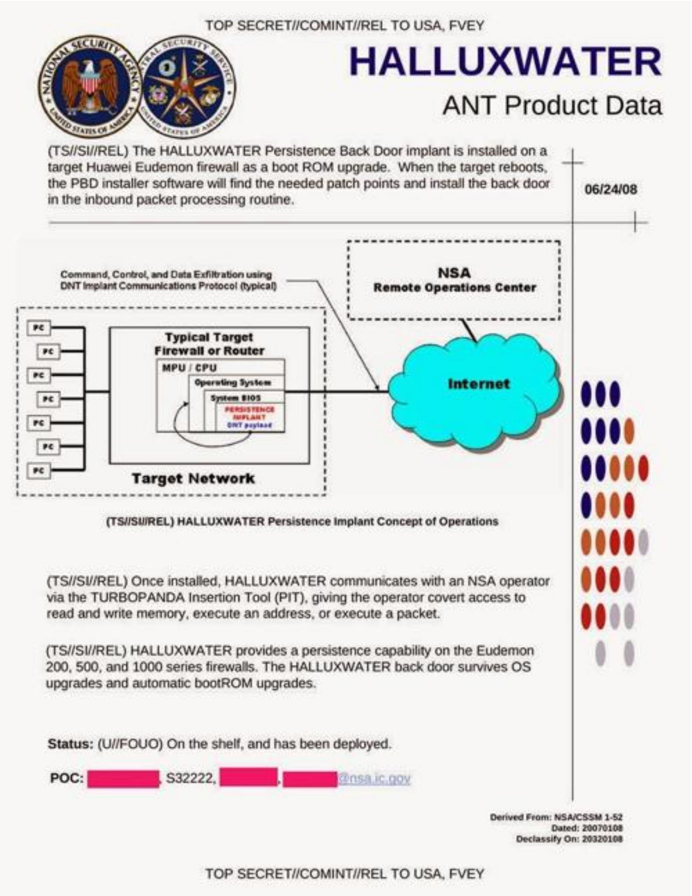
Unit Cost: $0

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

JETPLOW, программный «жучок» для межсетевых экранов Cisco



TOP SECRET//COMINT//REL TO USA, FVEY

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.

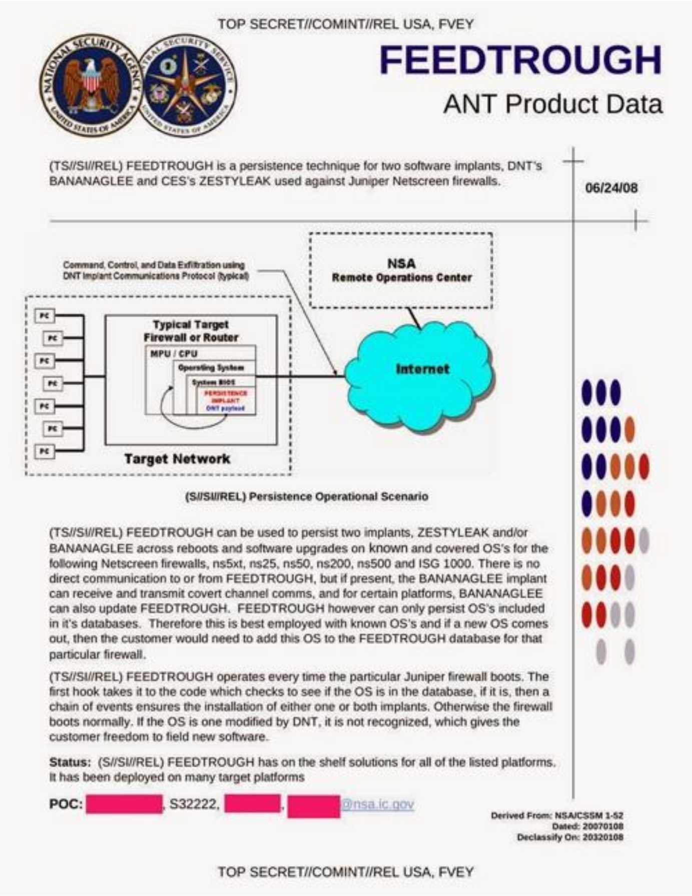
Status: (U//FOUO) On the shelf, and has been deployed.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

HALLUXWATER, бэкдор для межсетевых экранов Huawei Eudemon, Netscreen, ISG 1000



TOP SECRET//COMINT//REL USA, FVEY

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.

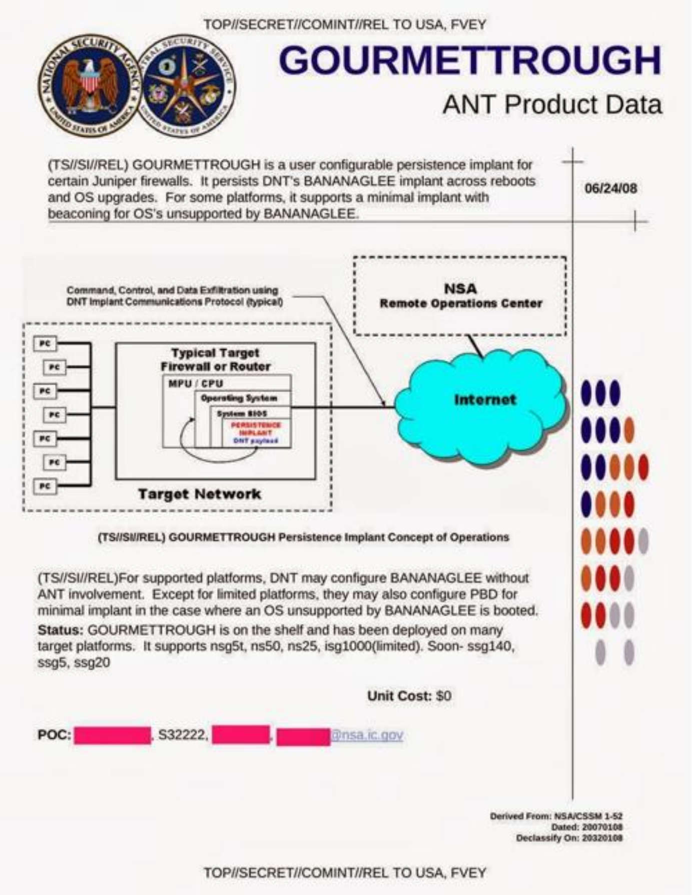
Status: (S//SI//REL) FEEDTROUGH has on the shelf solutions for all of the listed platforms. It has been deployed on many target platforms

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

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

TOP SECRET//COMINT//REL USA, FVEY

FEEDTROUGH, программный «жучок» для межсетевых экранов Juniper Netscreen N5XT, NS25, NS50, NS200, NS500, ISG1000



TOP//SECRET//COMINT//REL TO USA, FVEY

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

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT
DNT payload
Internet
Target Network

(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

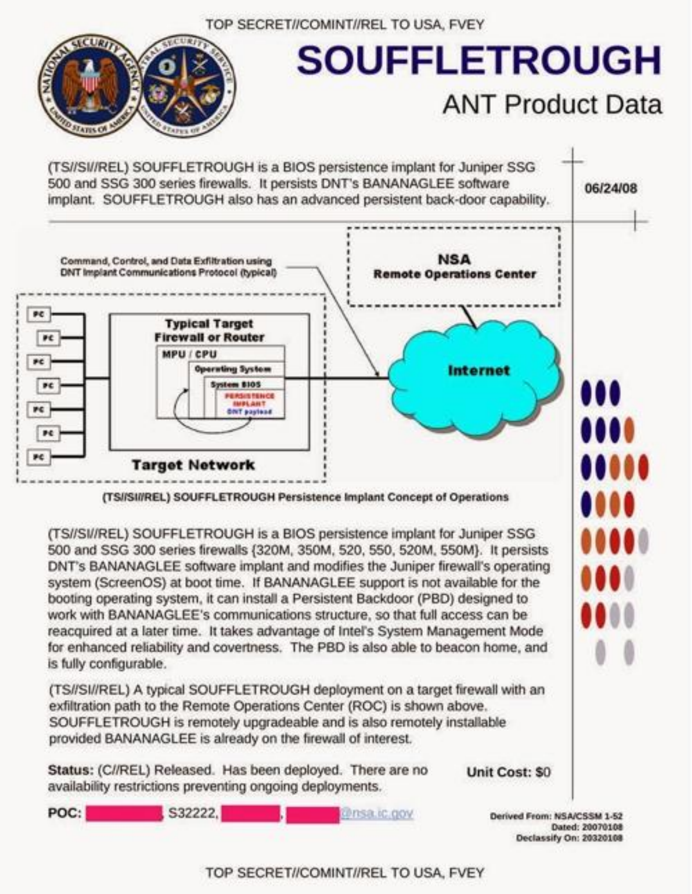
Unit Cost: $0

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

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

TOP//SECRET//COMINT//REL TO USA, FVEY

GOURMETTROUGH, программный «жучок» для межсетевых экранов Juniper NSG5T, NS50, NS25, ISG1000, SSG140, SSG5, SSG20



TOP SECRET//COMINT//REL TO USA, FVEY

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

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT
DNT payload
Internet
Target Network

(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

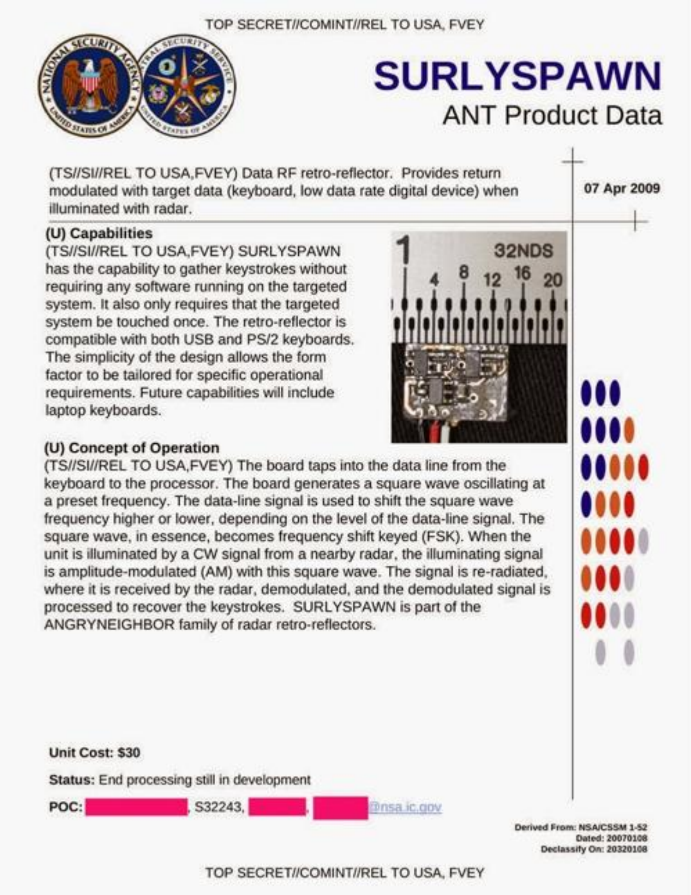
POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY

SOUFFLETROUGH, бэкдор для BIOS межсетевых экранов Juniper SSG30x/SSG50x

Устройства слежения за клавиатурой



TOP SECRET//COMINT//REL TO USA, FVEY

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

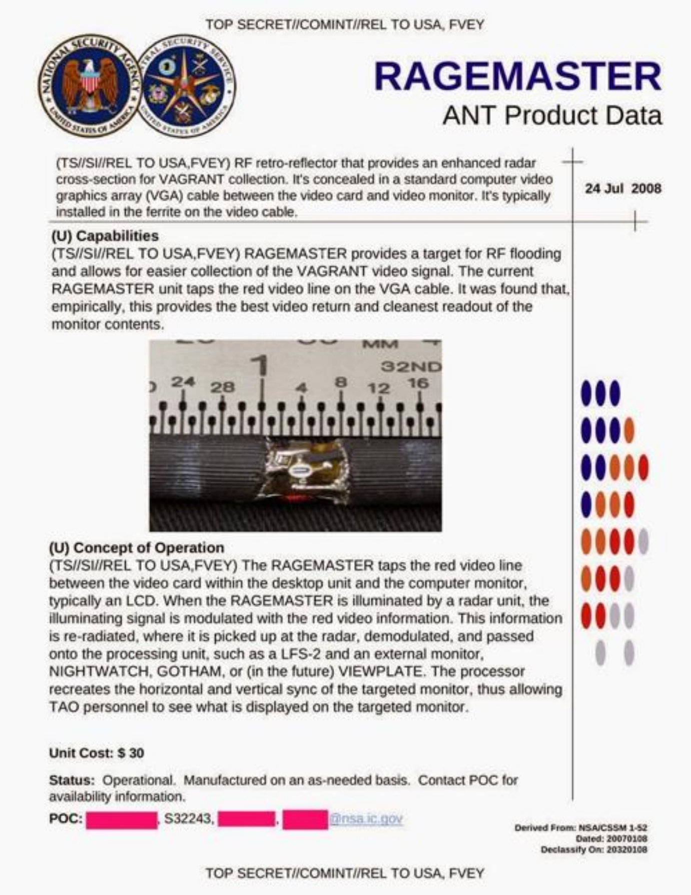
POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY

SURLYSPAWN, аппаратный «жучок» для отслеживания клавиатурных нажатий с передачей данных по радиоканалу

Системы перехвата изображения



TOP SECRET//COMINT//REL TO USA, FVEY

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.

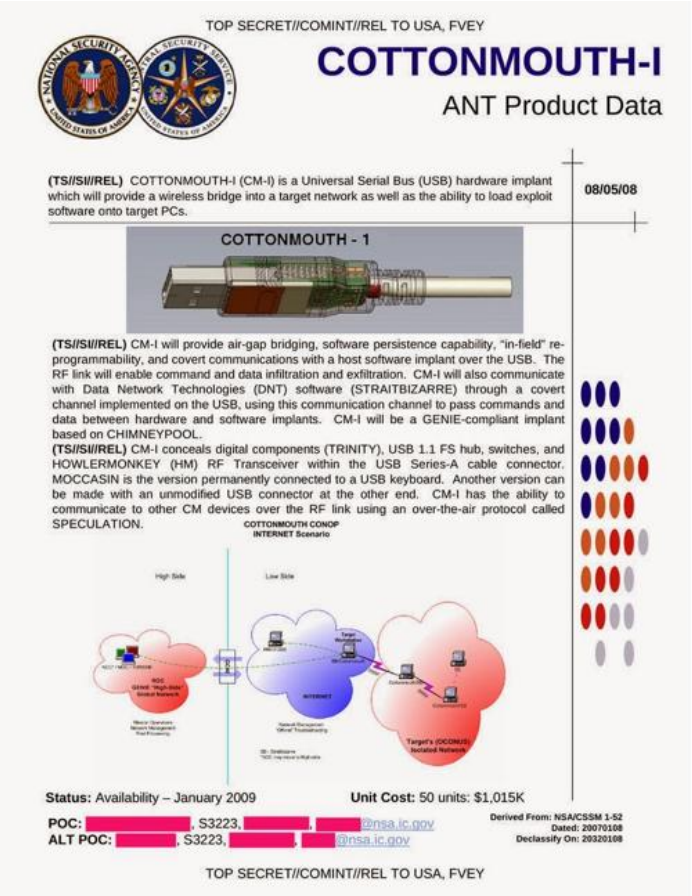
POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY

RAGEMASTER, аппаратный «жучок» для перехвата сигнала с экранов VGA

«Жучки» для портов USB и Ethernet



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(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.

08/05/08

COTTONMOUTH - 1

(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

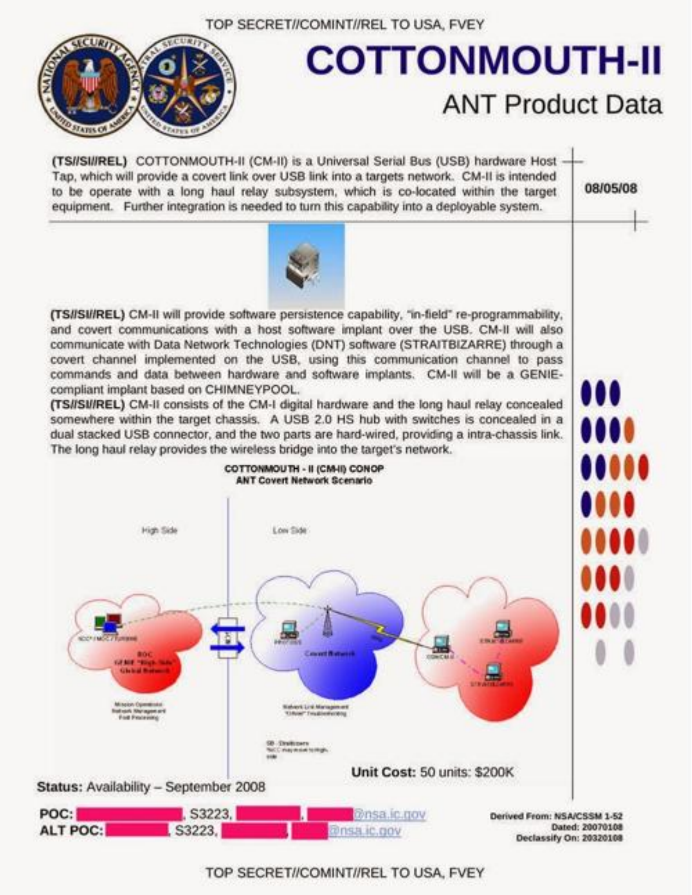
Unit Cost: 50 units: $1,015K

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

TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I, аппаратный «жучок» для перехвата данных и инъекции троянов через USB-порт, способный передавать данные по радиоканалу



TOP SECRET//COMINT//REL TO USA, FVEY

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

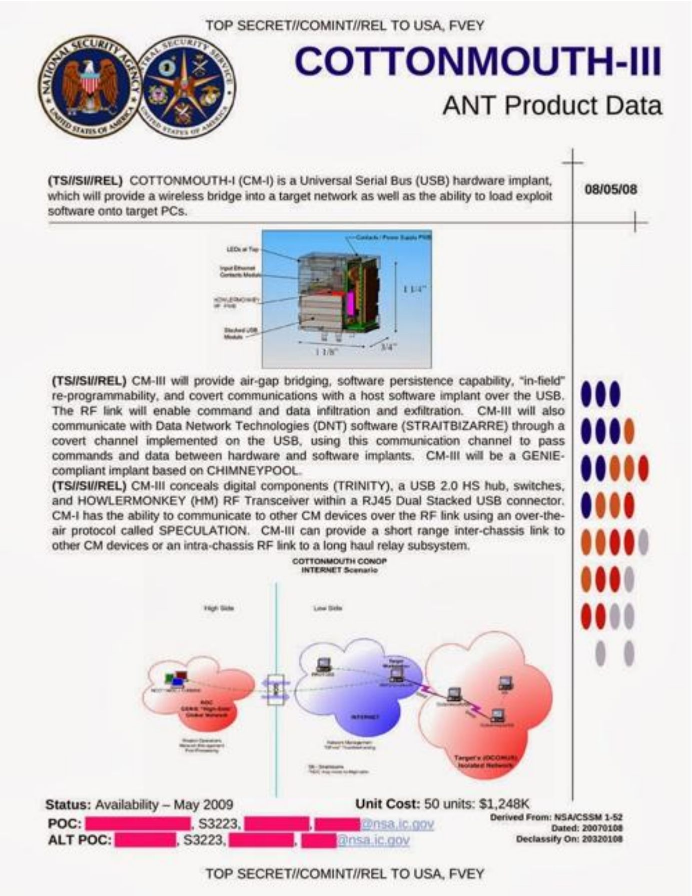
Status: Availability – September 2008

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

TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-II, аппаратный «жучок» для удаленного доступа и контроля над целевой системой через USB-порт


LEDs at Top
Input Ethernet Contacts Module
HOWLERMONKEY RF PWB
Stacked USB Module
Contacts / Power Supply PWB
1 1/4"
1 1/8"
3/4"
COTTONMOUTH CONOP
INTERNET Scenario
High Side
Low Side
ROC
INTERNET
Target's (OCONUS) Isolated Network

TOP SECRET//COMINT//REL TO USA, FVEY

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.

Status: Availability – May 2009

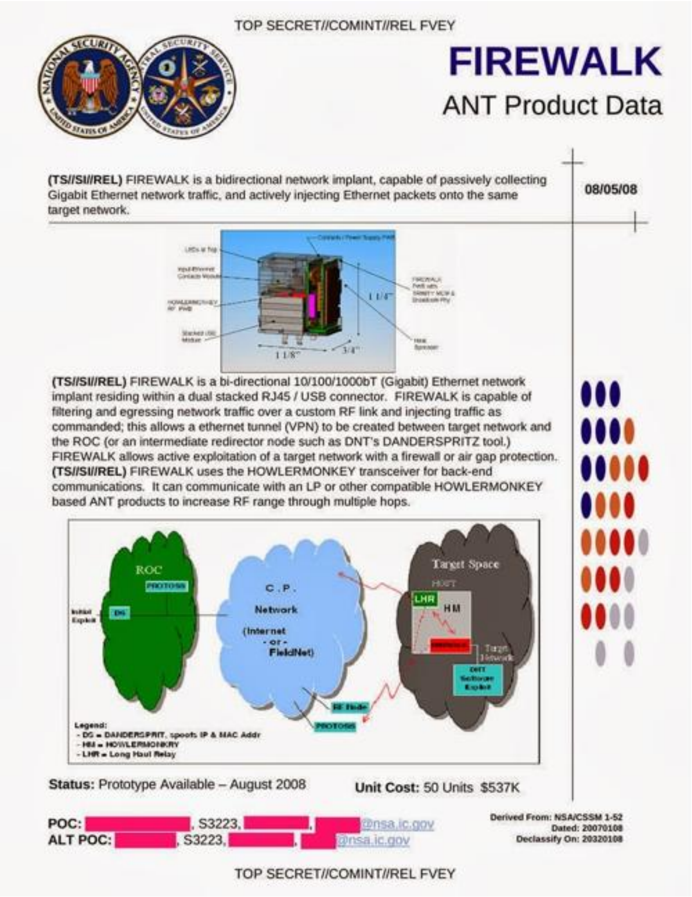
Unit Cost: 50 units: $1,248K

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

TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-III, аппаратный «жучок» для организации радиоканала к другим устройствам COTTONMOUTH. Устанавливается на USB-порт


LEDs at Top
Input Ethernet Contacts Module
HOWLERMONKEY RF PWB
Stacked USB Module
Contacts / Power Supply PWB
FIREWALK PWB with TRINITY MCM & Broadcom Phy
Heat Spreader
1 1/4"
1 1/8"
3/4"
ROC
PROTOSS
Initial Exploit
DG
C.P.
Network
(Internet
- or -
FieldNet)
Target Space
HOST
LHR
HM
Target Network
DNT Selector Exploit
RF Node
PROTOSS
Legend:
- DG = DANDERSPRIT, spoofs IP & MAC Addr
- HM = HOWLERMONKRY
- LHR = Long Haul Relay

TOP SECRET//COMINT//REL FVEY

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

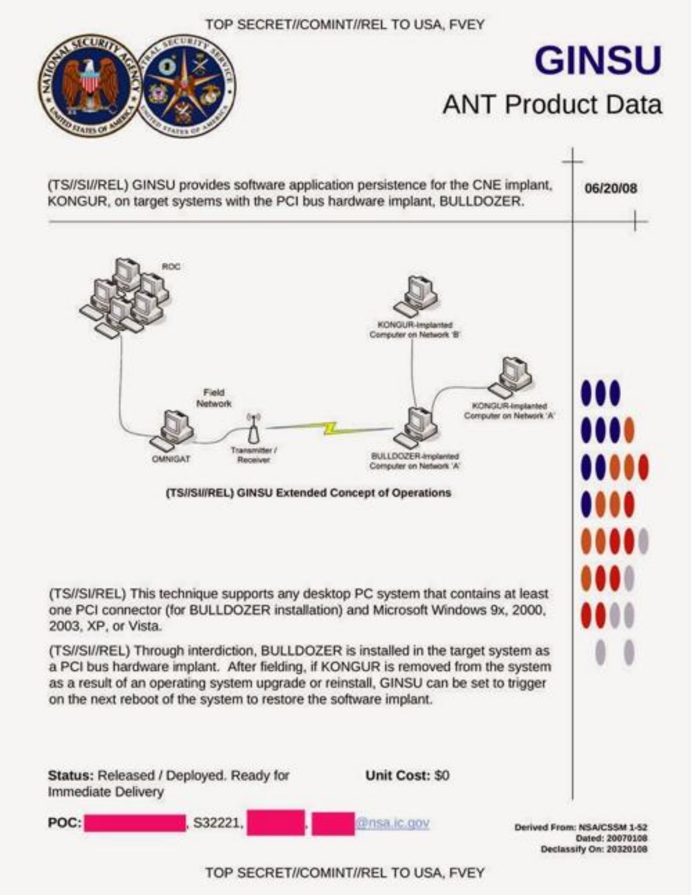
POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

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

TOP SECRET//COMINT//REL FVEY

FIREWALK, аппаратный «жучок» для перехвата и инъекции пакетов в порты USB и Ethernet

Аппаратные «жучки» для ПК



TOP SECRET//COMINT//REL TO USA, FVEY

GINSU

ANT Product Data

(TS//SI//REL) GINSU provides software application persistence for the CNE implant, KONGUR, on target systems with the PCI bus hardware implant, BULLDOZER.

06/20/08

ROC
KONGUR-implanted Computer on Network 'B'
Field Network
KONGUR-implanted Computer on Network 'A'
OMNIGAT
Transmitter / Receiver
BULLDOZER-implanted Computer on Network 'A'

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

(TS//SI//REL) This technique supports any desktop PC system that contains at least one PCI connector (for BULLDOZER installation) and Microsoft Windows 9x, 2000, 2003, XP, or Vista.

(TS//SI//REL) Through interdiction, BULLDOZER is installed in the target system as a PCI bus hardware implant. After fielding, if KONGUR is removed from the system as a result of an operating system upgrade or reinstall, GINSU can be set to trigger on the next reboot of the system to restore the software implant.

Status: Released / Deployed. Ready for Immediate Delivery

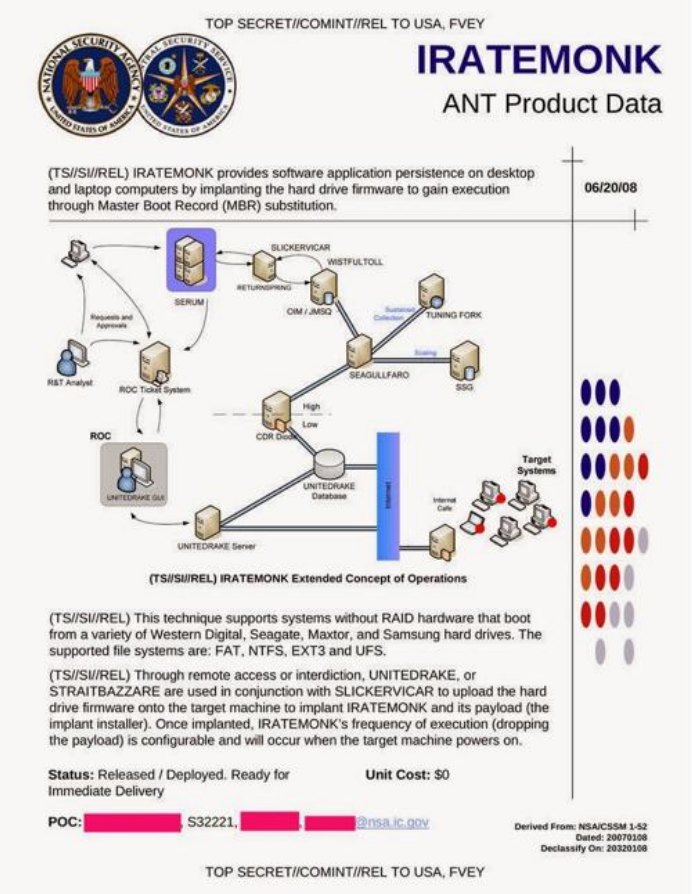
Unit Cost: $0

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

GINSU, программный «жучок» для шины PCI для ОС Windows 9x, XP, 2000, 2003, Vista



TOP SECRET//COMINT//REL TO USA, FVEY

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

SLICKERVICAR
WISTFULTOLL
RETURNSPRING
SERUM
OIM / JMSQ
Sustained Collection
TUNING FORK
Requests and Approvals
Staging
R&T Analyst
ROC Ticket System
SEAGULLFARO
SSG
High
Low
ROC
CDR Diode
Target Systems
UNITEDRAKE GUI
UNITEDRAKE Database
Internet
Internet Cafe
UNITEDRAKE Server

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

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK'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

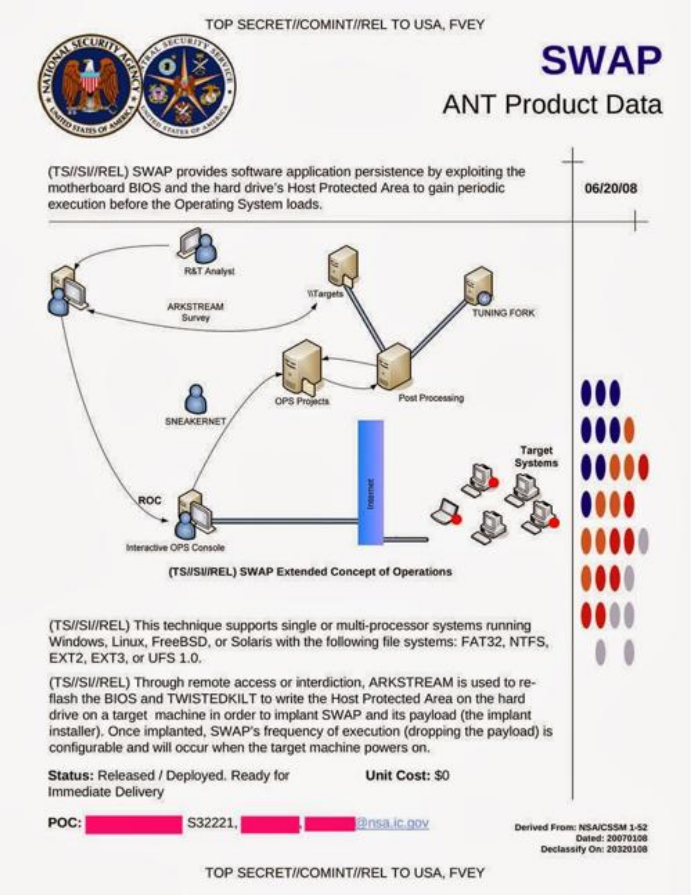
Unit Cost: $0

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

IRATEMONK, программный «жучок» для Western Digital, Seagate, Maxtor, Samsung



TOP SECRET//COMINT//REL TO USA, FVEY

SWAP

ANT Product Data

(TS//SI//REL) SWAP provides software application persistence by exploiting the motherboard BIOS and the hard drive's Host Protected Area to gain periodic execution before the Operating System loads.

06/20/08

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

(TS//SI//REL) This technique supports single or multi-processor systems running Windows, Linux, FreeBSD, or Solaris with the following file systems: FAT32, NTFS, EXT2, EXT3, or UFS 1.0.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS and TWISTEDKILT to write the Host Protected Area on the hard drive on a target machine in order to implant SWAP and its payload (the implant installer). Once implanted, SWAP'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

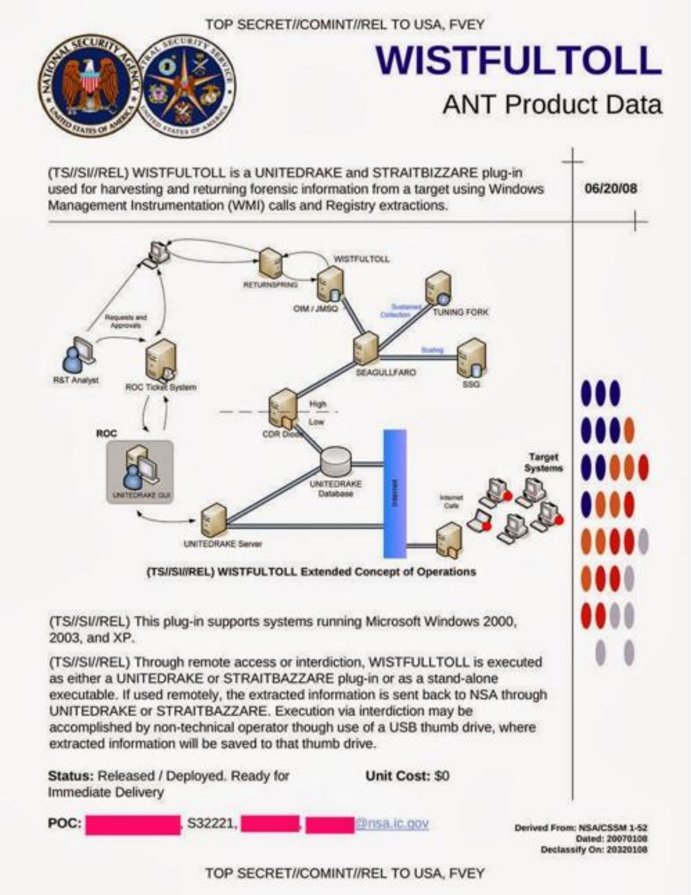
Unit Cost: $0

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

SWAP, программный «жучок» для ОС Windows, FreeBSD, Linux, Solaris



TOP SECRET//COMINT//REL TO USA, FVEY

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

(TS//SI//REL) This plug-in supports systems running Microsoft Windows 2000, 2003, and XP.

(TS//SI//REL) Through remote access or interdiction, WISTFULLTOLL is executed as either a UNITEDRAKE or STRAITBAZZARE plug-in or as a stand-alone executable. If used remotely, the extracted information is sent back to NSA through UNITEDRAKE or STRAITBAZZARE. Execution via interdiction may be accomplished by non-technical operator though use of a USB thumb drive, where extracted information will be saved to that thumb drive.

Status: Released / Deployed. Ready for Immediate Delivery

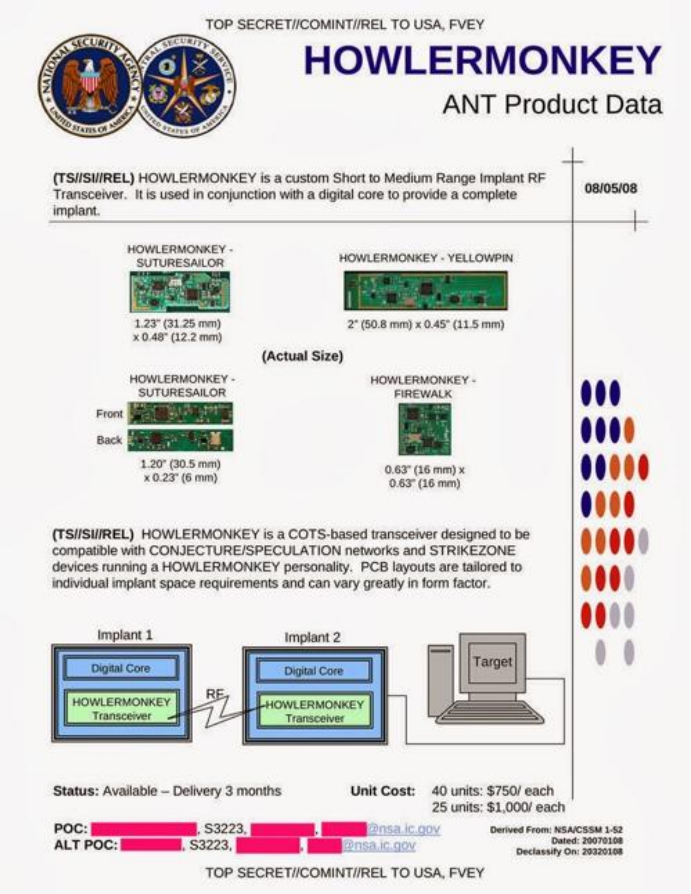
Unit Cost: $0

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

WISTFULTOLL, «жучок» для управления ОС Windows с помощью технологии Windows Management Instrumentation (WMI)



TOP SECRET//COMINT//REL TO USA, FVEY

HOWLERMONKEY

ANT Product Data

08/05/08

(TS//SI//REL) HOWLERMONKEY is a custom Short to Medium Range Implant RF Transceiver. It is used in conjunction with a digital core to provide a complete implant.

HOWLERMONKEY - SUTURESAILOR
1.23" (31.25 mm) x 0.48" (12.2 mm)
HOWLERMONKEY - YELLOWPIN
2" (50.8 mm) x 0.45" (11.5 mm)
(Actual Size)
HOWLERMONKEY - SUTURESAILOR
Front
Back
1.20" (30.5 mm) x 0.23" (6 mm)
HOWLERMONKEY - FIREWALK
0.63" (16 mm) x 0.63" (16 mm)

(TS//SI//REL) HOWLERMONKEY is a COTS-based transceiver designed to be compatible with CONJECTURE/SPECULATION networks and STRIKEZONE devices running a HOWLERMONKEY personality. PCB layouts are tailored to individual implant space requirements and can vary greatly in form factor.

Status: Available – Delivery 3 months

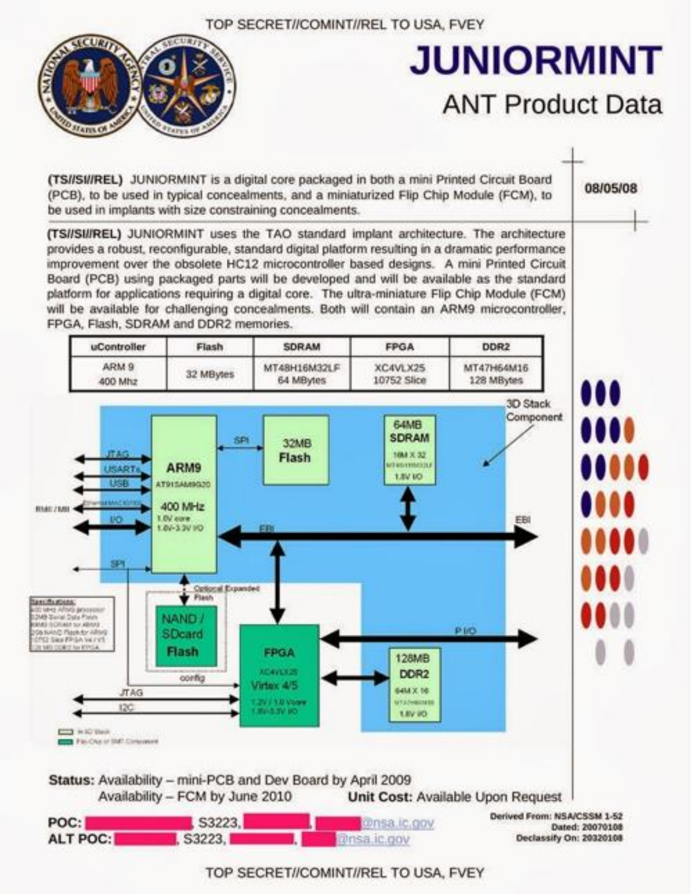
Unit Cost: 40 units: $750/ each
25 units: $1,000/ each

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

TOP SECRET//COMINT//REL TO USA, FVEY

HOWLERMONKEY, аппаратный «жучок» для приема-передачи радиосигнала и дистанционного управления ПК



TOP SECRET//COMINT//REL TO USA, FVEY

JUNIORMINT

ANT Product Data

08/05/08

(TS//SI//REL) JUNIORMINT is a digital core packaged in both a mini Printed Circuit Board (PCB), to be used in typical concealments, and a miniaturized Flip Chip Module (FCM), to be used in implants with size constraining concealments.

(TS//SI//REL) JUNIORMINT 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 mini Printed Circuit Board (PCB) using packaged parts will be developed and will be available as the standard platform for applications requiring a digital core. The ultra-miniature Flip Chip Module (FCM) will be available for challenging concealments. Both will contain an ARM9 microcontroller, FPGA, Flash, SDRAM and DDR2 memories.

uController	Flash	SDRAM	FPGA	DDR2
ARM 9 400 Mhz	32 MBytes	MT48H16M32LF 64 MBytes	XC4VLX25 10752 Slice	MT47H64M16 128 MBytes

Status: Availability – mini-PCB and Dev Board by April 2009
Availability – FCM by June 2010

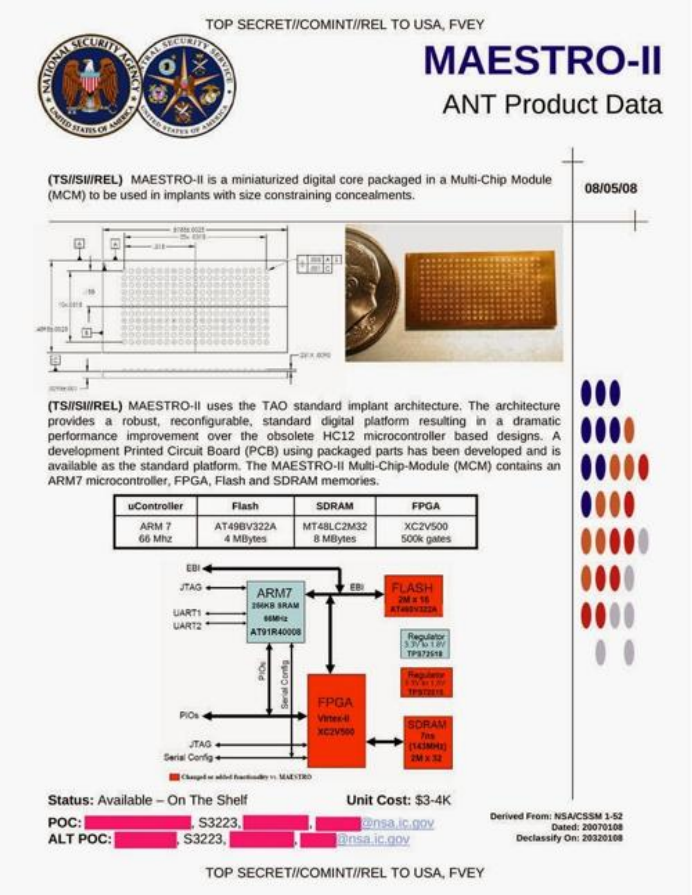
Unit Cost: Available Upon Request

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

TOP SECRET//COMINT//REL TO USA, FVEY

JUNIORMINT, аппаратный «жучок» - микро-ПК на основе процессора ARM9



TOP SECRET//COMINT//REL TO USA, FVEY

MAESTRO-II

ANT Product Data

08/05/08

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

(TS//SI//REL) MAESTRO-II 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 MAESTRO-II Multi-Chip-Module (MCM) contains an ARM7 microcontroller, FPGA, Flash and SDRAM memories.

uController	Flash	SDRAM	FPGA
ARM 7 66 Mhz	AT49BV322A 4 MBytes	MT48LC2M32 8 MBytes	XC2V500 500k gates

Status: Available – On The Shelf

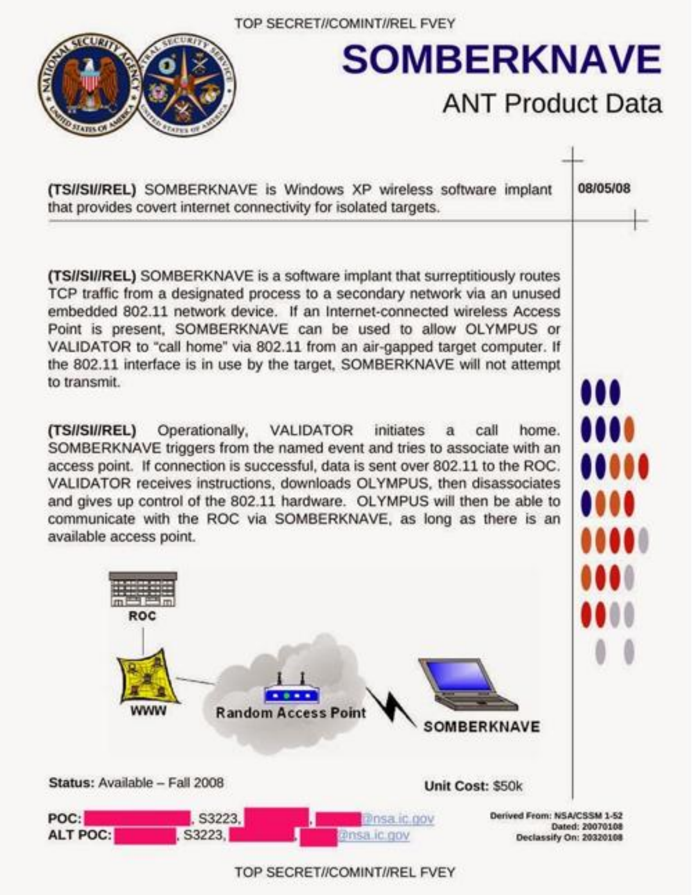
Unit Cost: $3-4K

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

TOP SECRET//COMINT//REL TO USA, FVEY

MAESTRO-II, аппаратный «жучок» - микро-ПК на основе процессора ARM7



TOP SECRET//COMINT//REL FVEY

SOMBERKNAVE

ANT Product Data

08/05/08

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

(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.

Status: Available – Fall 2008

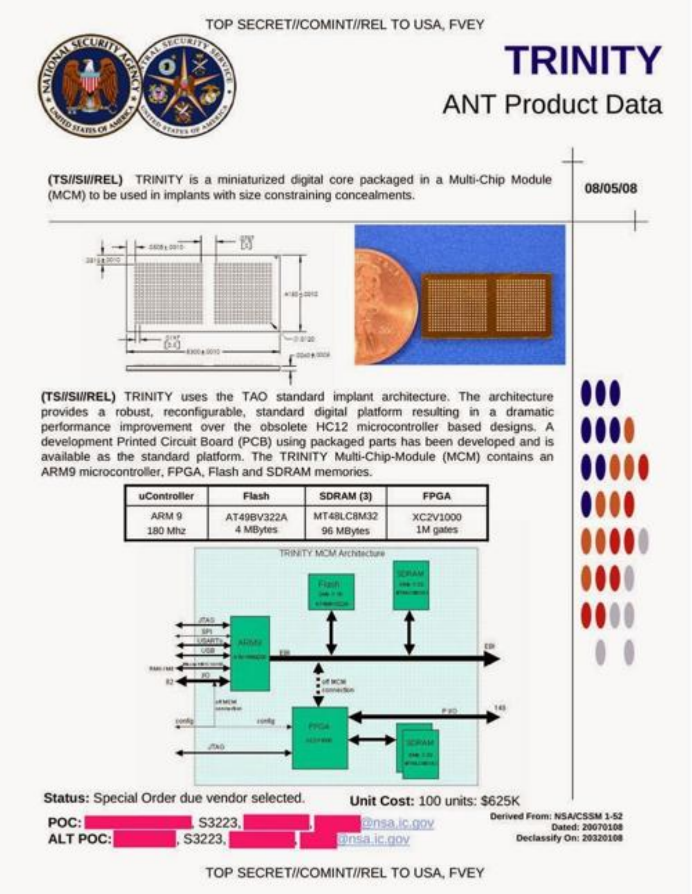
Unit Cost: $50k

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

TOP SECRET//COMINT//REL FVEY

SOMBERKNAVE, программный «жучок» для Windows XP, подключающийся к устройствам АНБ с помощью Wi-Fi



TOP SECRET//COMINT//REL TO USA, FVEY

TRINITY

ANT Product Data

(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.

08/05/08

(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

Status: Special Order due vendor selected.

Unit Cost: 100 units: $625K

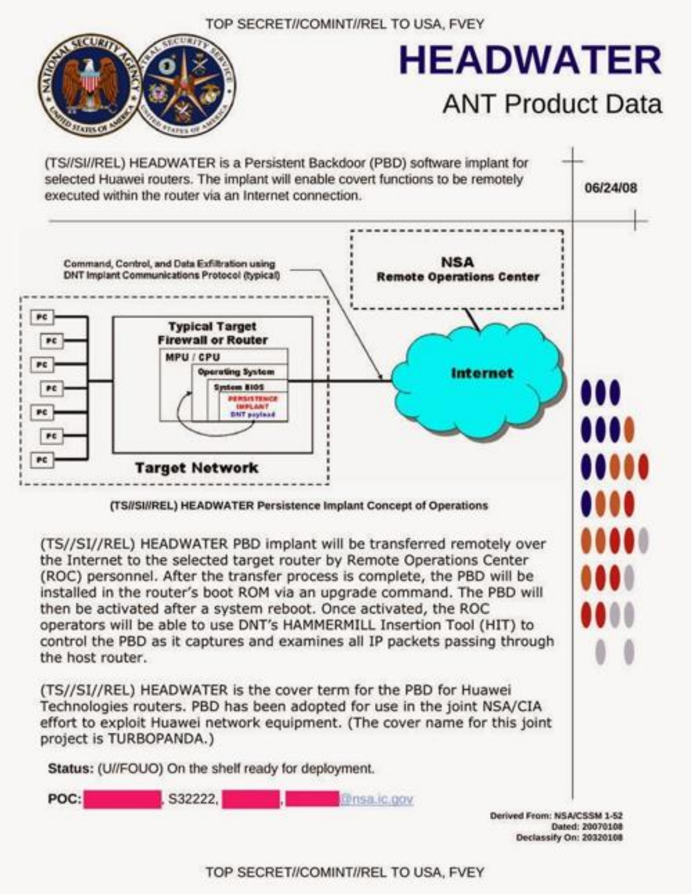
POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY

TRINITY, аппаратный «жучок», свободно конфигурируемый микро-ПК на основе ARM9

Аппаратные «жучки» для маршрутизаторов



TOP SECRET//COMINT//REL TO USA, FVEY

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

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
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) 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.)

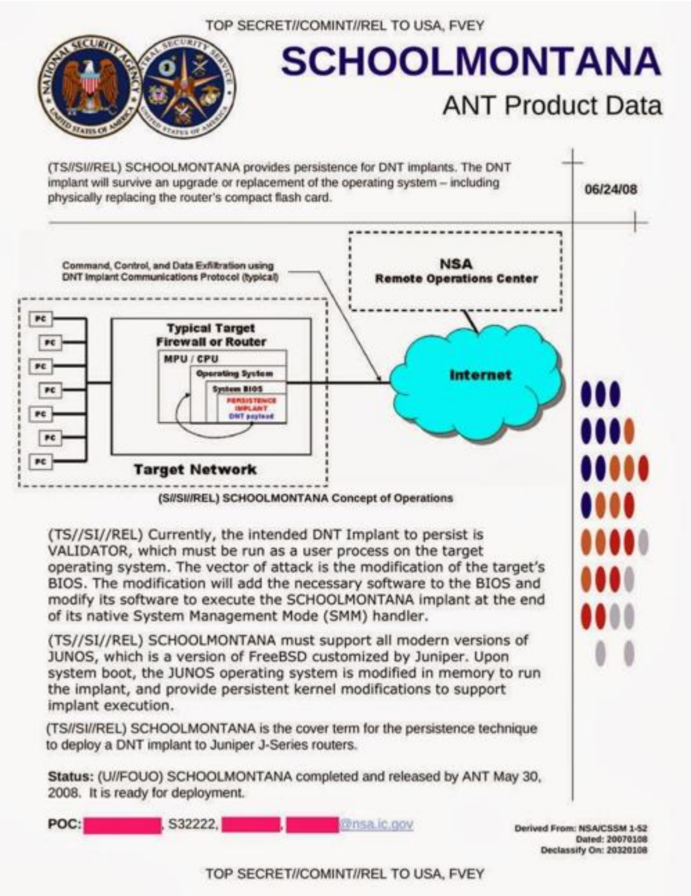
Status: (U//FOUO) On the shelf ready for deployment.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

HEADWATER, программный бэкдор для удаленного управления маршрутизаторами Huawei, удаленно устанавливаемый в Boot ROM



TOP SECRET//COMINT//REL TO USA, FVEY

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

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
Internet
PC
PC
PC
PC
PC
PC
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT
DNT payload
Target Network

(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.

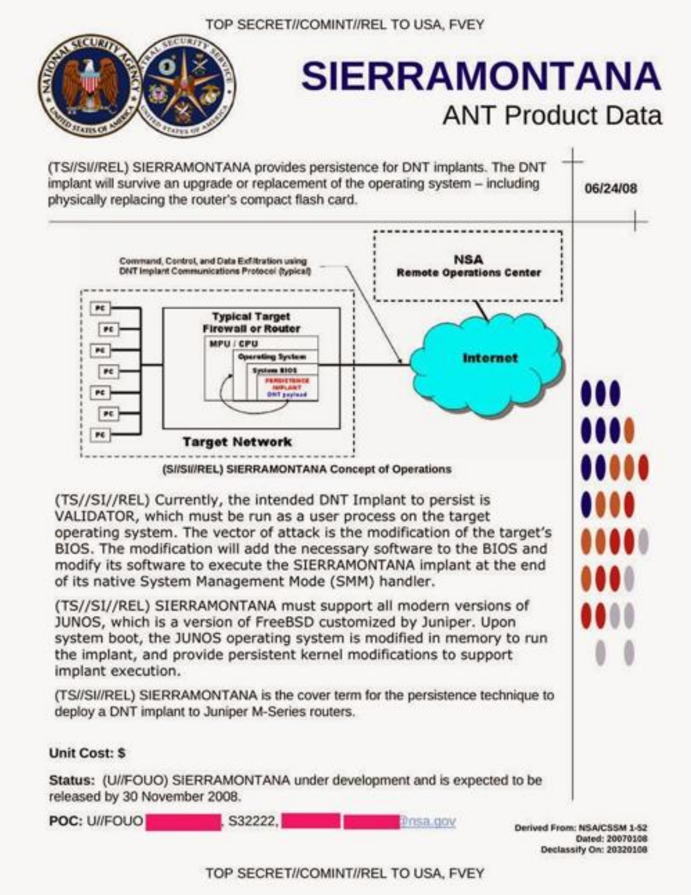
Status: (U//FOUO) SCHOOLMONTANA completed and released by ANT May 30, 2008. It is ready for deployment.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

SCHOOLMONTANA, программный «жучок» для BIOS маршрутизаторов Juniper J-серии



TOP SECRET//COMINT//REL TO USA, FVEY

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

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
Internet
PC
PC
PC
PC
PC
PC
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT
DNT payload
Target Network

(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: $

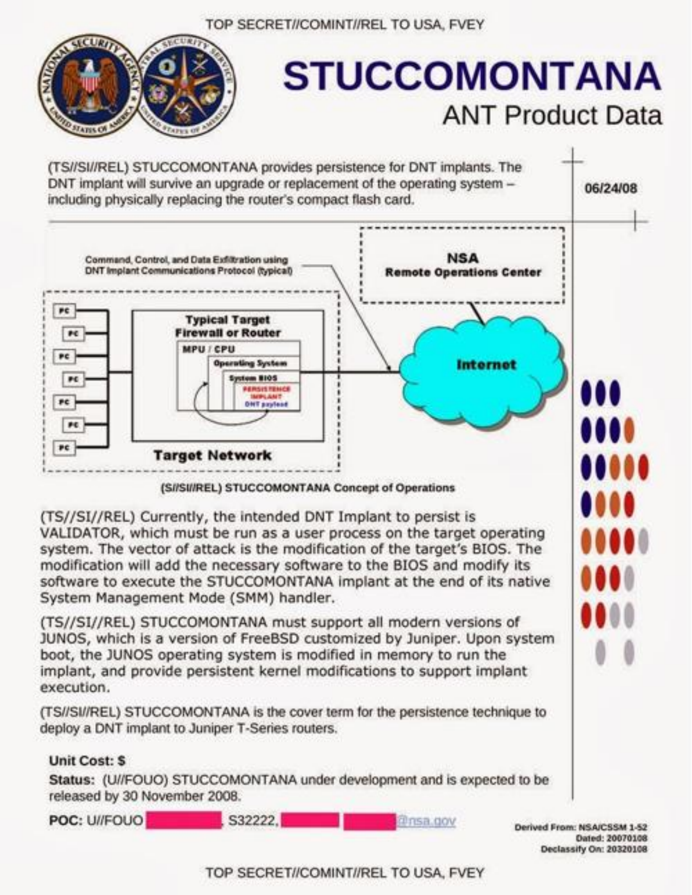
Status: (U//FOUO) SIERRAMONTANA under development and is expected to be released by 30 November 2008.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

SIERRAMONTANA, программный «жучок» для BIOS маршрутизаторов Juniper M-серии



TOP SECRET//COMINT//REL TO USA, FVEY

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

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)
NSA
Remote Operations Center
PC
PC
PC
PC
PC
PC
PC
Typical Target Firewall or Router
MPU / CPU
Operating System
System BIOS
PERSISTENCE IMPLANT
DNT payload
Internet
Target Network

(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.

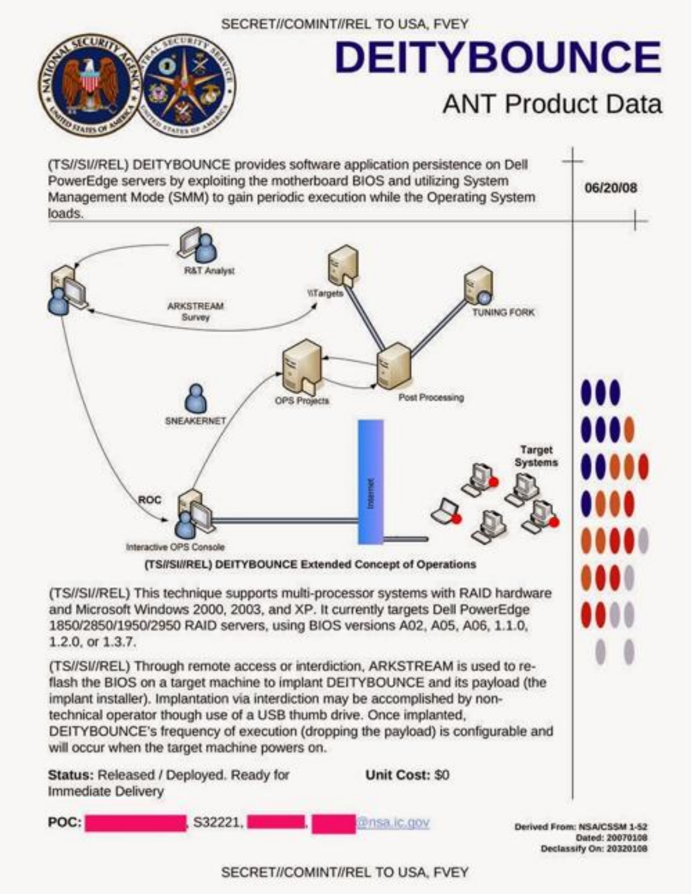
POC: U//FOUO [redacted], S32222, [redacted] [redacted]@nsa.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY

STUCCOMONTANA, программный «жучок» для BIOS маршрутизаторов Juniper T-серии

Аппаратные закладки для серверов



SECRET//COMINT//REL TO USA, FVEY

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

R&T Analyst
\\Targets
TUNING FORK
ARKSTREAM Survey
OPS Projects
Post Processing
SNEAKERNET
Target Systems
ROC
Internet
Interactive OPS Console

(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

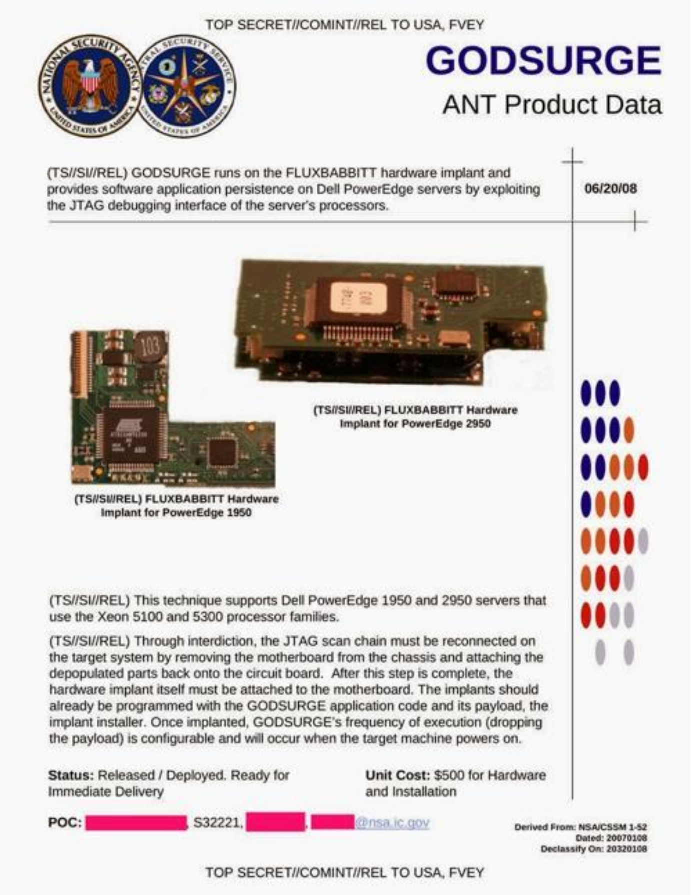
Unit Cost: $0

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

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

SECRET//COMINT//REL TO USA, FVEY

DEITYBOUNCE, программный «жучок» для BIOS серверов Dell PowerEdge 1850/2850/1950/2950 (BOIS A02,A05, A06, 1.1.0, 1.2.0, 1.3.7)



TOP SECRET//COMINT//REL TO USA, FVEY

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

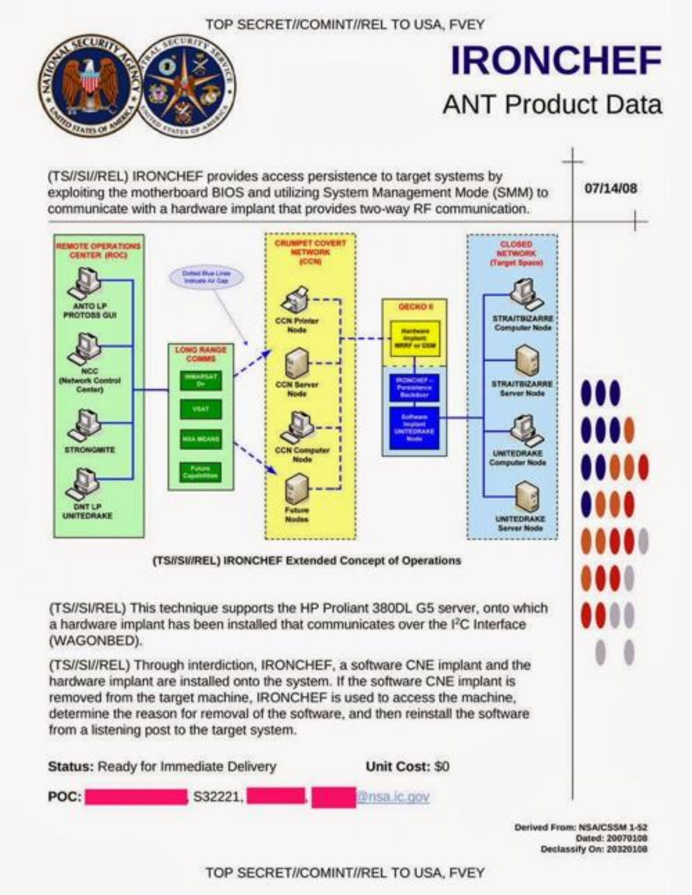
Unit Cost: $500 for Hardware and Installation

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

GODSURGE программный «жучок» для аппаратного «жучка» FLUXBABBITT. Используется для серверов Dell PowerEdge 1950/2950



TOP SECRET//COMINT//REL TO USA, FVEY

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

REMOTE OPERATIONS CENTER (ROC)
ANTO LP PROTOSS GUI
NCC (Network Control Center)
STRONGMITE
DNT LP UNITEDRAKE
Dotted Blue Lines Indicate Air Gap
LONG RANGE COMMS
INMARSAT D+
VSAT
NSA MEANS
Future Capabilities
CRUMPET COVERT NETWORK (CCN)
CCN Printer Node
CCN Server Node
CCN Computer Node
Future Nodes
GECKO II
Hardware Implant MRRF or GSM
IRONCHEF – Persistence Backdoor
Software Implant UNITEDRAKE Node
CLOSED NETWORK (Target Space)
STRAITBIZARRE Computer Node
STRAITBIZARRE Server Node
UNITEDRAKE Computer Node
UNITEDRAKE Server Node

(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^{2}C 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

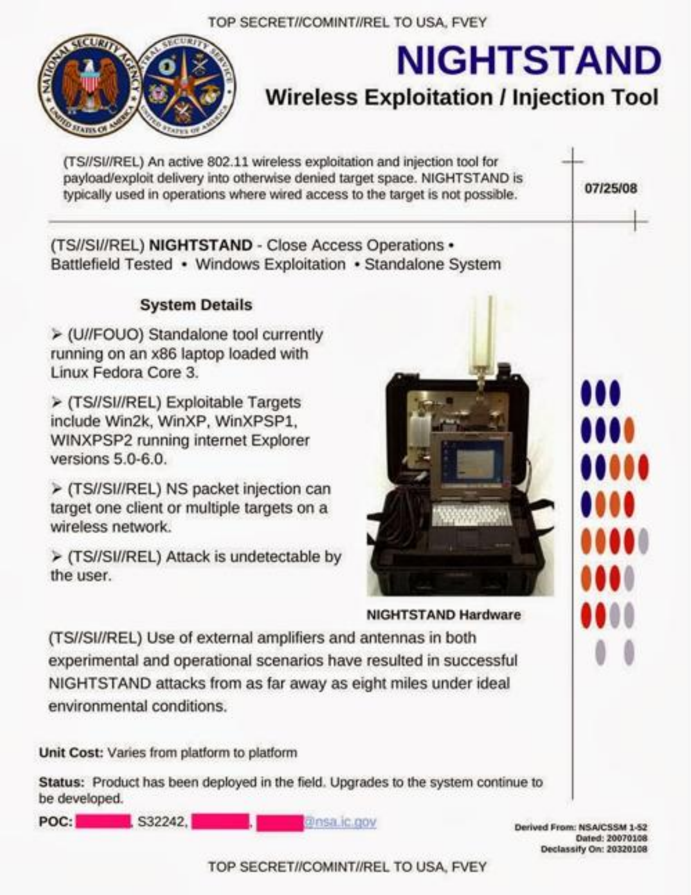
POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY

IRONCHEF, «жучок» для HP Proliant 380DL G5

Решения для атак на Wi-Fi сети



TOP SECRET//COMINT//REL TO USA, FVEY

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

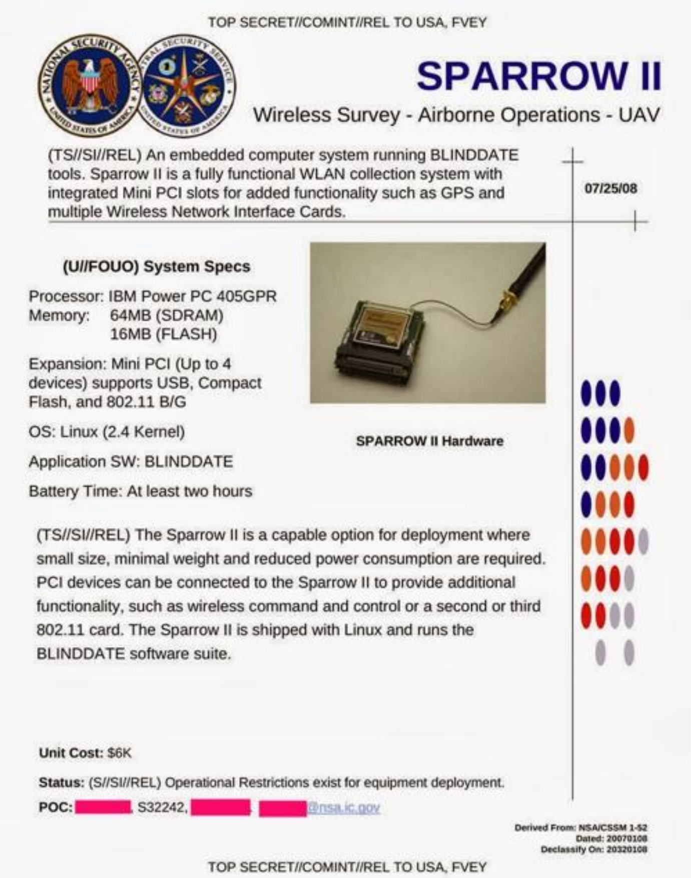
Status: Product has been deployed in the field. Upgrades to the system continue to be developed.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

NIGHTSTAND, устройство для внедрения пакетов в сети Wi-Fi



TOP SECRET//COMINT//REL TO USA, FVEY

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.

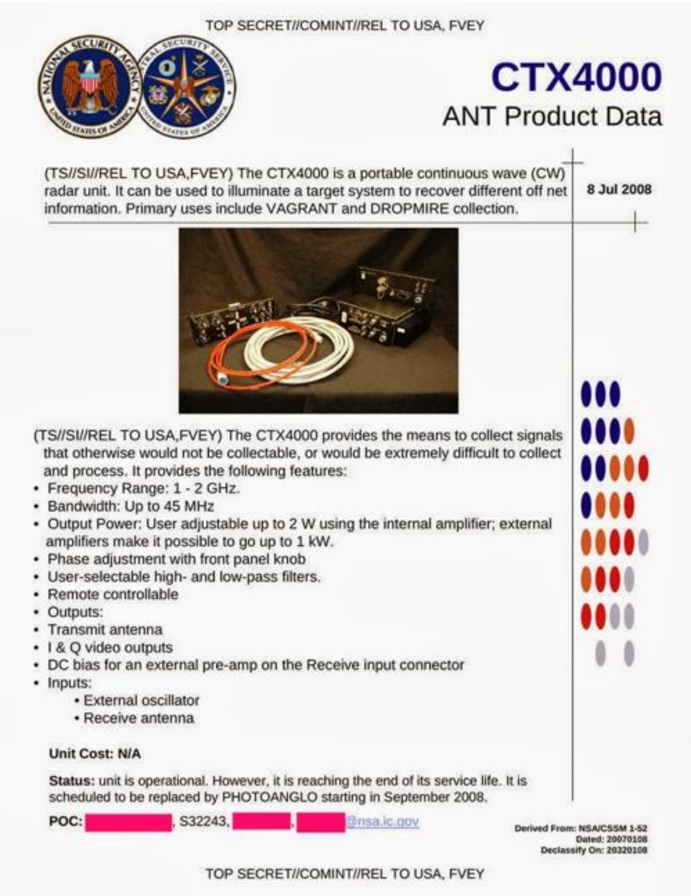
POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY

SPARROW II, устройство для взлома сетей Wi-Fi

Устройства для обнаружения и снятия информации с «жучков»



TOP SECRET//COMINT//REL TO USA, FVEY

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

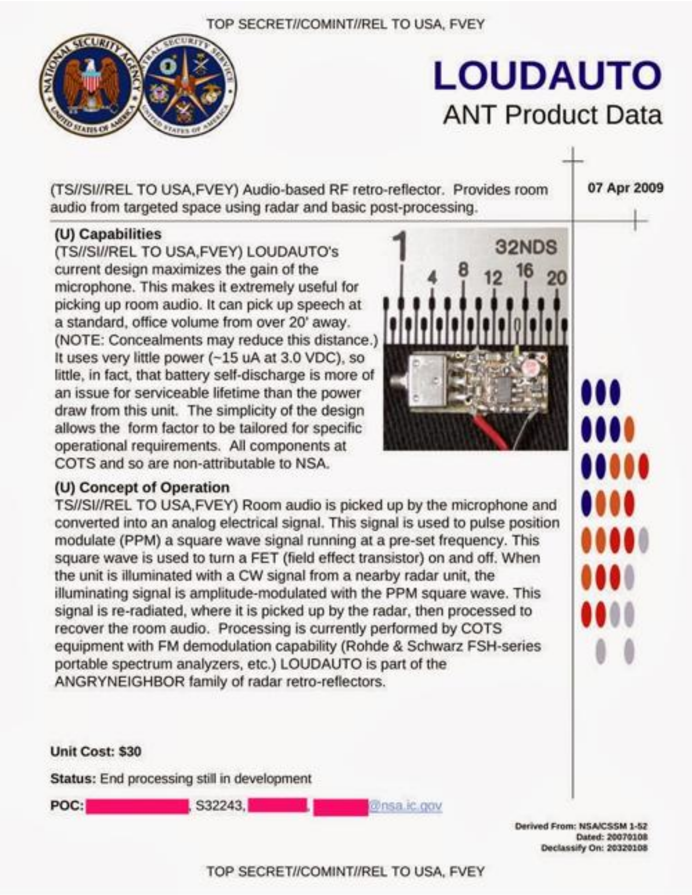
Status: unit is operational. However, it is reaching the end of its service life. It is scheduled to be replaced by PHOTOANGLO starting in September 2008.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

CTX4000, устройство непрерывного анализа и получения сигналов от аппаратных «жучков» VAGRANT и DROPMIRE



TOP SECRET//COMINT//REL TO USA, FVEY

LOUDAUTO

ANT Product Data

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

07 Apr 2009

(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

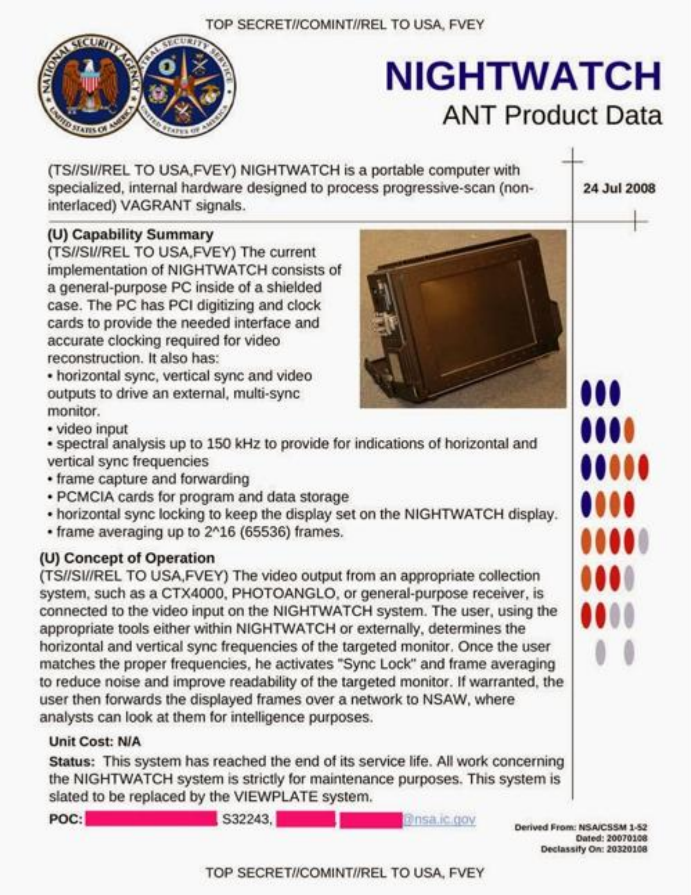
Status: End processing still in development

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

LOUDAUTO, устройство для записи звуковой информации



TOP SECRET//COMINT//REL TO USA, FVEY

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

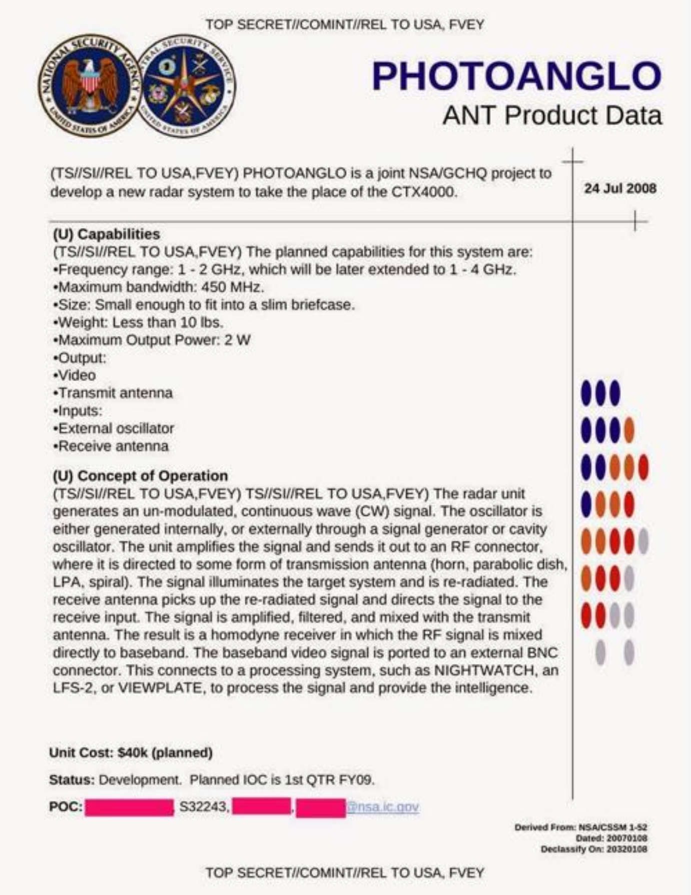
Status: This system has reached the end of its service life. All work concerning the NIGHTWATCH system is strictly for maintenance purposes. This system is slated to be replaced by the VIEWPLATE system.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

NIGHTWATCH - система реконструкции сигнала «жучка» VAGRANT с выводом на монитор



TOP SECRET//COMINT//REL TO USA, FVEY

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)

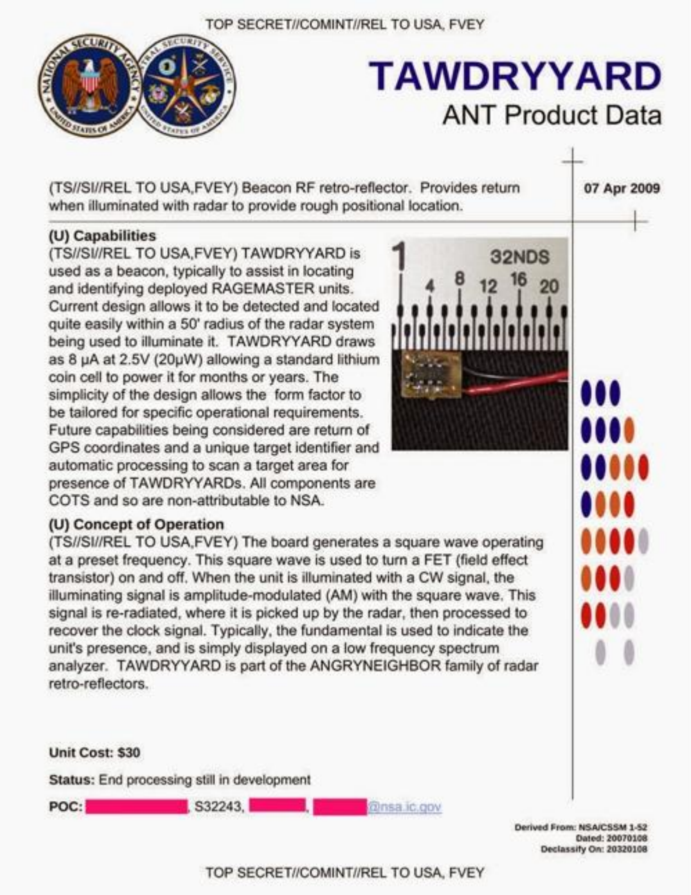
Status: Development. Planned IOC is 1st QTR FY09.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

PHOTOANGLO, обновленная версия устройства CTX4000



TOP SECRET//COMINT//REL TO USA, FVEY

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

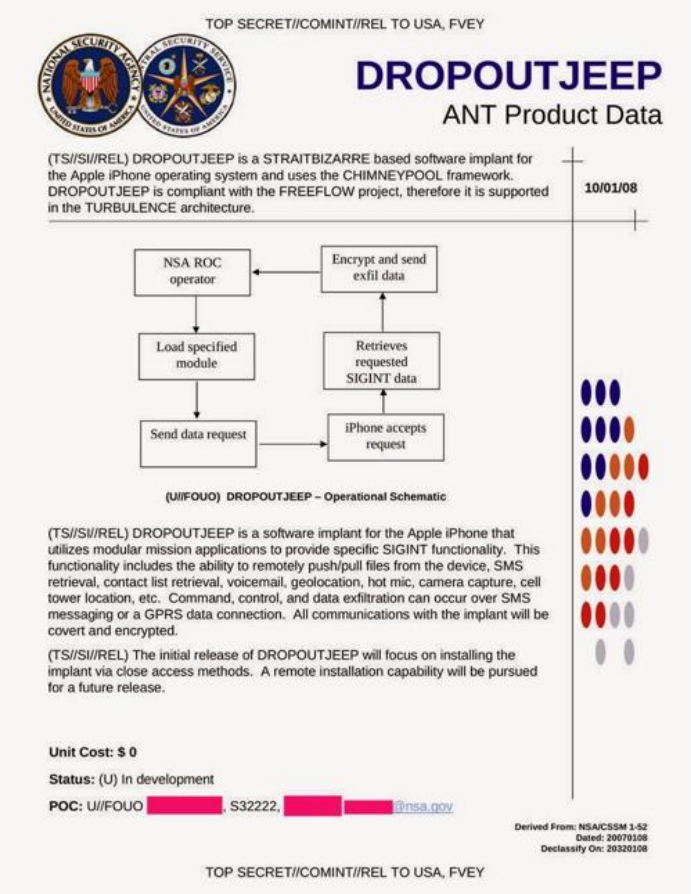
POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY

TAWDRYYARD, аппаратный модуль для поиска «жучков»

Системы для скрытного управления мобильными телефонами



TOP SECRET//COMINT//REL TO USA, FVEY

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

NSA ROC operator
Load specified module
Send data request
iPhone accepts request
Retrieves requested SIGINT data
Encrypt and send exfil data

(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

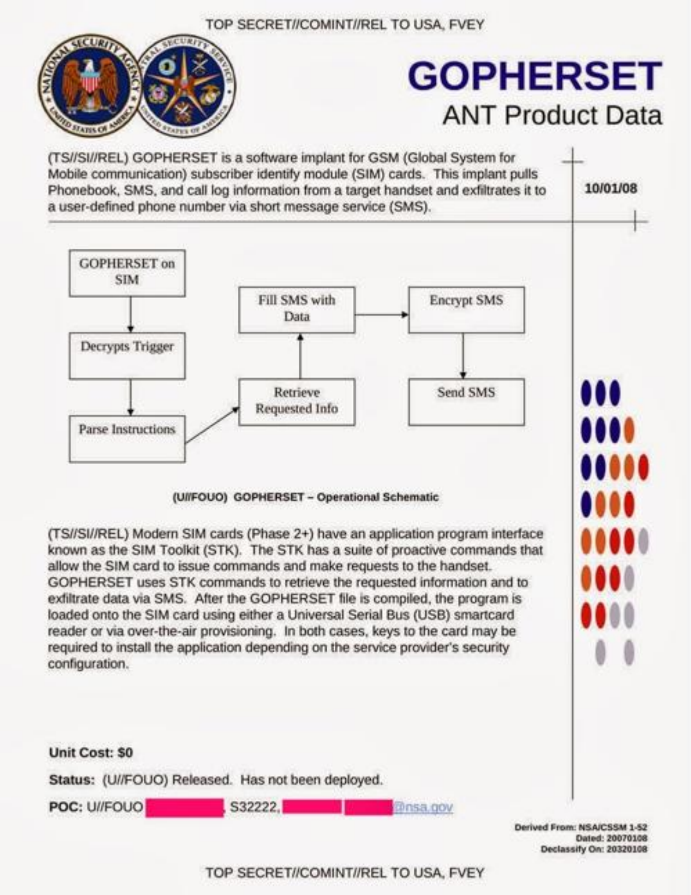
Status: (U) In development

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

DROPOUTJEEP, программный «жучок» для операционной системы iOS (iPhone) для перехвата SMS, голосовой почты, данных о местоположении, контроля над микрофоном и камерой



TOP SECRET//COMINT//REL TO USA, FVEY

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

GOPHERSET on SIM
Decrypts Trigger
Parse Instructions
Retrieve Requested Info
Fill SMS with Data
Encrypt SMS
Send SMS

(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

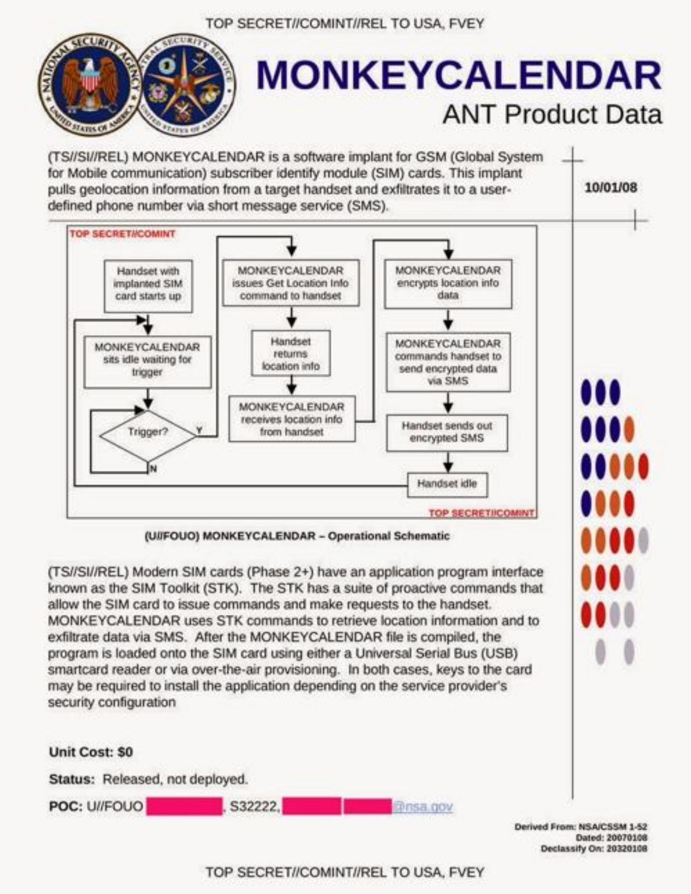
Status: (U//FOUO) Released. Has not been deployed.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

GOPHERSET, «жучок» SIM-карт в GSM-устройствах



TOP SECRET//COMINT//REL TO USA, FVEY

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

TOP SECRET//COMINT
Handset with implanted SIM card starts up
MONKEYCALENDAR sits idle waiting for trigger
Trigger?
Y
N
MONKEYCALENDAR issues Get Location Info command to handset
Handset returns location info
MONKEYCALENDAR receives location info from handset
MONKEYCALENDAR encrypts location info data
MONKEYCALENDAR commands handset to send encrypted data via SMS
Handset sends out encrypted SMS
Handset idle
TOP SECRET//COMINT

(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

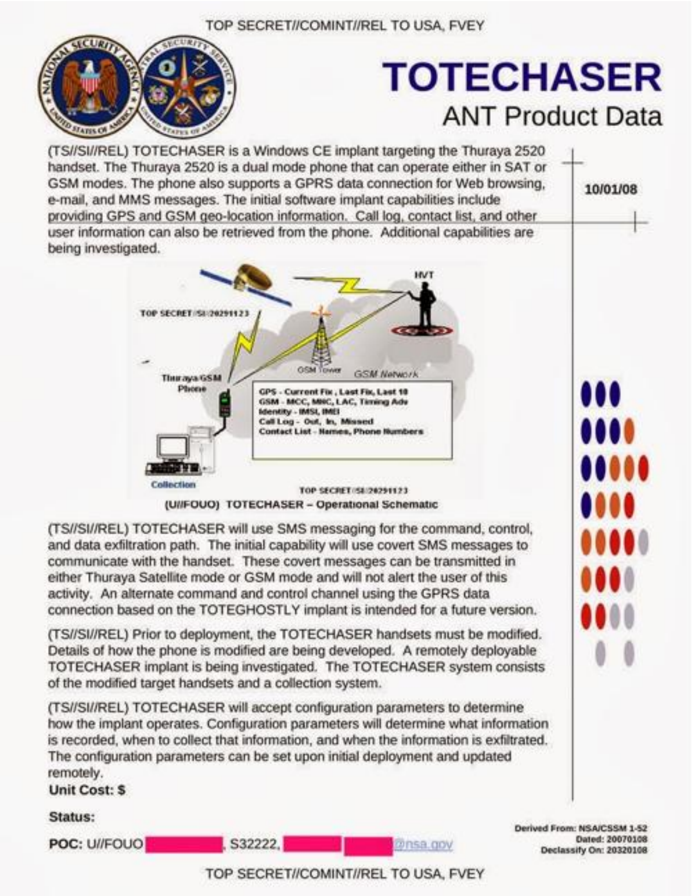
Status: Released, not deployed.

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

MONKEYCALENDAR, программный «жучок» для тайной отправки SMS о местоположении устройства



TOP SECRET//COMINT//REL TO USA, FVEY

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.

GPS - Current Fix , Last Fix, Last 10
GSM - MCC, MNC, LAC, Timing Adv
Identity - IMSI, IMEI
Call Log - Out, In, Missed
Contact List - Names, Phone Numbers

(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: $

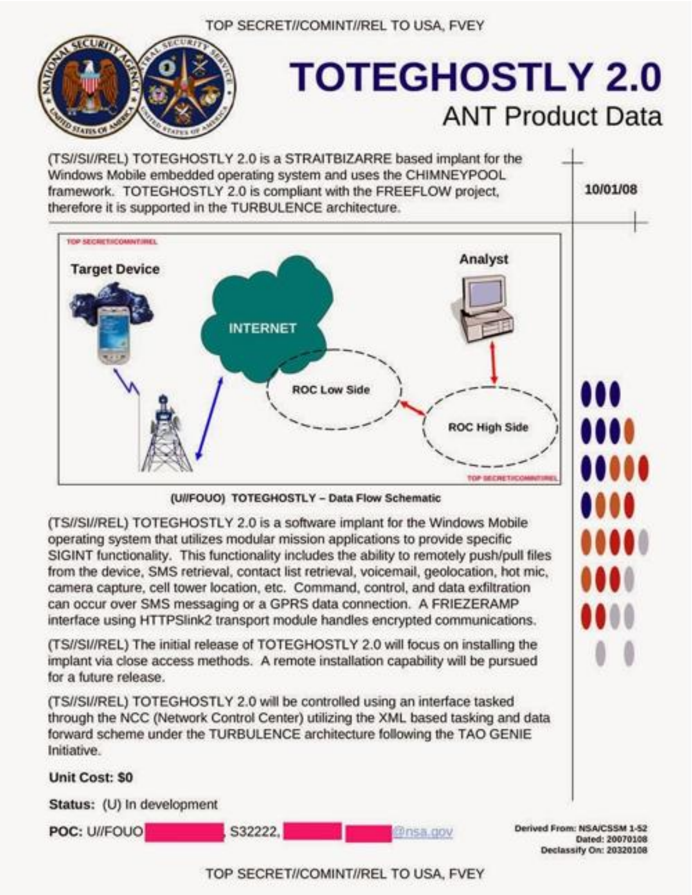
Status:

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

TOTECHASER, программный «жучок» для спутникового телефона Thuraya 2520 (ОС Windows CE) для скрытной передачи данных по каналу SMS



TOP SECRET//COMINT//REL TO USA, FVEY

TOTEGHOSTLY 2.0

ANT Product Data

10/01/08

(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.

TOP SECRET//COMINT//REL
Target Device
INTERNET
Analyst
ROC Low Side
ROC High Side
TOP SECRET//COMINT//REL

(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

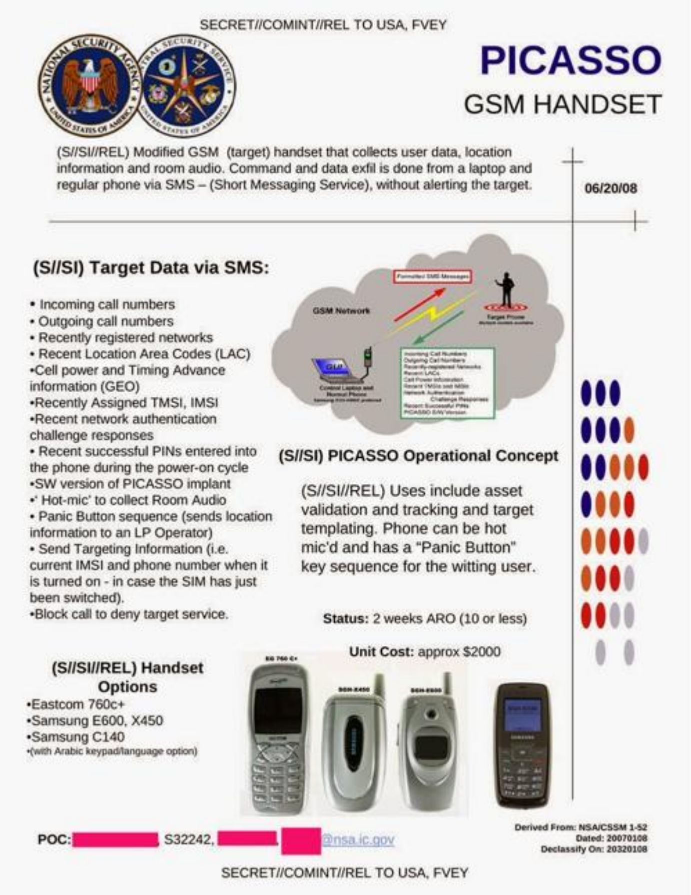
Status: (U) In development

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

TOTEGHOSTLY 2.0, программный «жучок» для устройств на Windows Mobile, позволяющий скрытно скачивать и загружать файлы, читать SMS, голосовую почту, собирать данные об местоположении, управлять микрофоном и камерой



SECRET//COMINT//REL TO USA, FVEY

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)

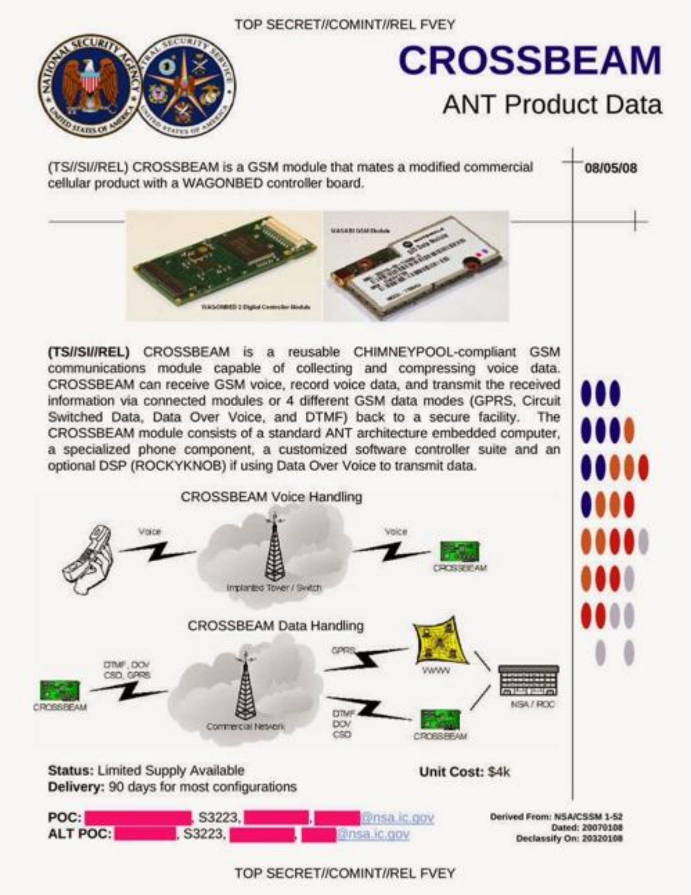
POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

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

SECRET//COMINT//REL TO USA, FVEY

PICASSO, модифицированные GSM-устройства для скрытного сбора данных о местоположении и звонках владельца

Устройства для контроля и отслеживания мобильных телефонов



TOP SECRET//COMINT//REL FVEY

CROSSBEAM

ANT Product Data

(TS//SI//REL) CROSSBEAM is a GSM module that mates a modified commercial cellular product with a WAGONBED controller board.

08/05/08

WAGONBED 2 Digital Controller Module

(TS//SI//REL) CROSSBEAM is a reusable CHIMNEYPOOL-compliant GSM communications module capable of collecting and compressing voice data. CROSSBEAM can receive GSM voice, record voice data, and transmit the received information via connected modules or 4 different GSM data modes (GPRS, Circuit Switched Data, Data Over Voice, and DTMF) back to a secure facility. The CROSSBEAM module consists of a standard ANT architecture embedded computer, a specialized phone component, a customized software controller suite and an optional DSP (ROCKYKNOB) if using Data Over Voice to transmit data.

CROSSBEAM Voice Handling

CROSSBEAM Data Handling

Status: Limited Supply Available
Delivery: 90 days for most configurations

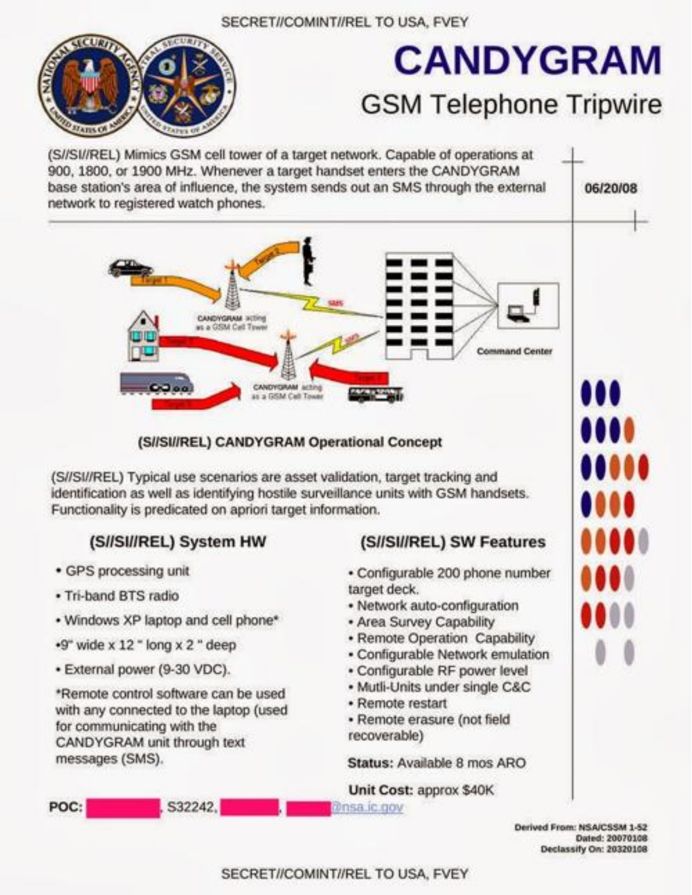
Unit Cost: $4k

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

TOP SECRET//COMINT//REL FVEY

CROSSBEAM - «жучок» для внешнего доступа к данным, передаваемым GSM-телефоном



SECRET//COMINT//REL TO USA, FVEY

CANDYGRAM

GSM Telephone Tripwire

(S//SI//REL) Mimics GSM cell tower of a target network. Capable of operations at 900, 1800, or 1900 MHz. Whenever a target handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones.

06/20/08

Target 1
Target 2
SMS
CANDYGRAM acting as a GSM Cell Tower
SMS
CANDYGRAM acting as a GSM Cell Tower
Command Center

(S//SI//REL) CANDYGRAM Operational Concept

(S//SI//REL) Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets. Functionality is predicated on apriori target information.

(S//SI//REL) System HW

- GPS processing unit
- Tri-band BTS radio
- Windows XP laptop and cell phone*
- 9" wide x 12 " long x 2 " deep
- External power (9-30 VDC).

*Remote control software can be used with any connected to the laptop (used for communicating with the CANDYGRAM unit through text messages (SMS).

(S//SI//REL) SW Features

- Configurable 200 phone number target deck.
- Network auto-configuration
- Area Survey Capability
- Remote Operation Capability
- Configurable Network emulation
- Configurable RF power level
- Mutli-Units under single C&C
- Remote restart
- Remote erasure (not field recoverable)

Status: Available 8 mos ARO

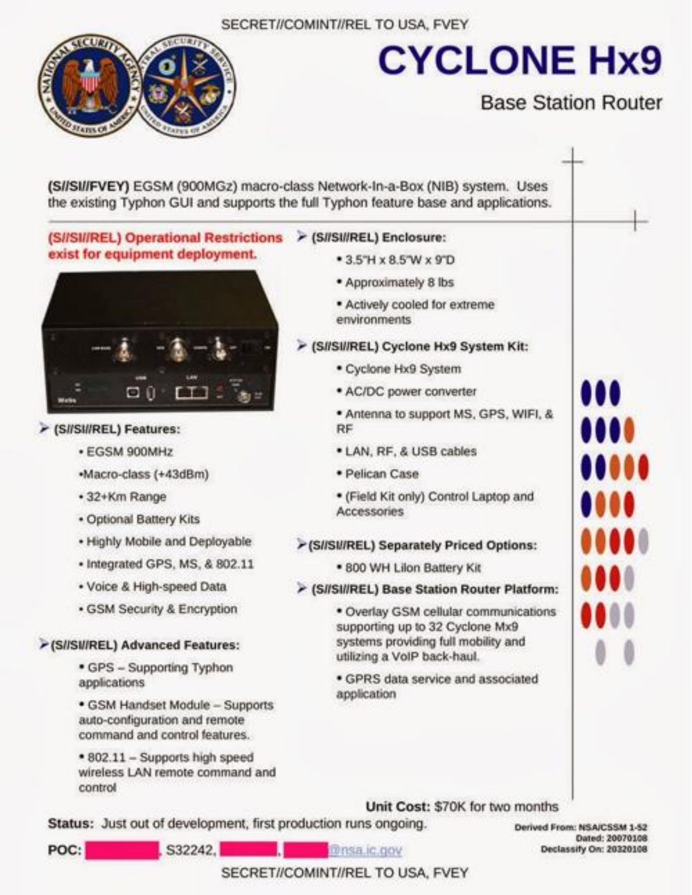
Unit Cost: approx $40K

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

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

SECRET//COMINT//REL TO USA, FVEY

CANDYGRAM - ложная базовая станция GSM, применяемая для определения местонахождения объекта и отправки скрытых SMS



SECRET//COMINT//REL TO USA, FVEY

CYCLONE Hx9

Base Station Router

(S//SI//FVEY) EGSM (900MGz) macro-class Network-In-a-Box (NIB) system. Uses the existing Typhon GUI and supports the full Typhon feature base and applications.

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

➢ **(S//SI//REL) Features:**

- EGSM 900MHz
- Macro-class (+43dBm)
- 32+Km Range
- Optional Battery Kits
- Highly Mobile and Deployable
- Integrated GPS, MS, & 802.11
- Voice & High-speed Data
- GSM Security & Encryption

➢ **(S//SI//REL) Advanced Features:**

- GPS – Supporting Typhon applications
- GSM Handset Module – Supports auto-configuration and remote command and control features.
- 802.11 – Supports high speed wireless LAN remote command and control

➢ **(S//SI//REL) Enclosure:**

- 3.5"H x 8.5"W x 9"D
- Approximately 8 lbs
- Actively cooled for extreme environments

➢ **(S//SI//REL) Cyclone Hx9 System Kit:**

- Cyclone Hx9 System
- AC/DC power converter
- Antenna to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories

➢ **(S//SI//REL) Separately Priced Options:**

- 800 WH LiIon Battery Kit

➢ **(S//SI//REL) Base Station Router Platform:**

- Overlay GSM cellular communications supporting up to 32 Cyclone Mx9 systems providing full mobility and utilizing a VoIP back-haul.
- GPRS data service and associated application

Unit Cost: $70K for two months

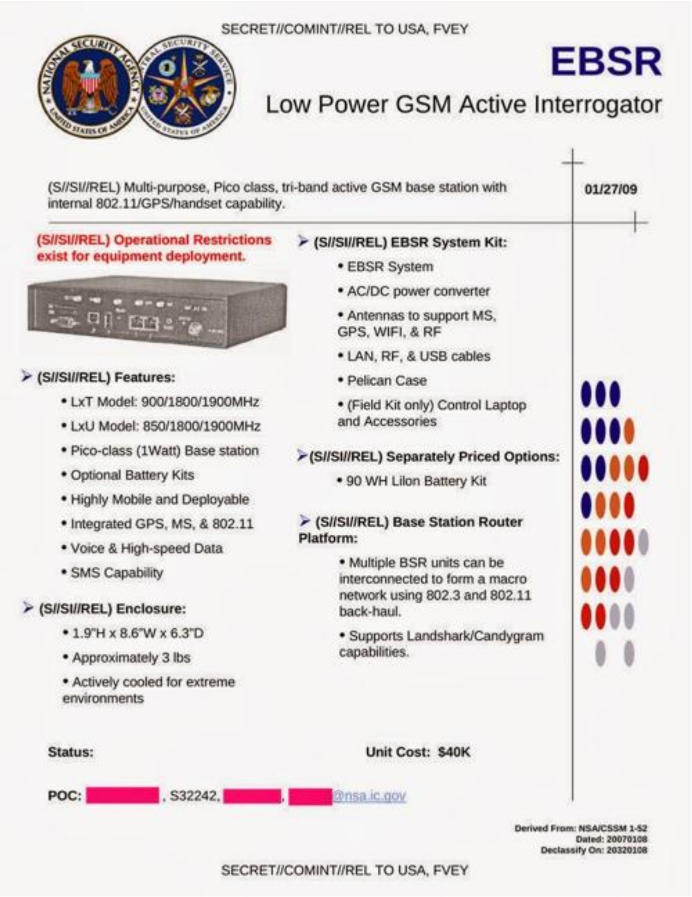
Status: Just out of development, first production runs ongoing.

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

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

SECRET//COMINT//REL TO USA, FVEY

CYCLONE HX9, ложная базовая станция GSM, применяемая для прослушивания сотовых телефонов и перехвата данных



SECRET//COMINT//REL TO USA, FVEY

EBSR

Low Power GSM Active Interrogator

(S//SI//REL) Multi-purpose, Pico class, tri-band active GSM base station with internal 802.11/GPS/handset capability.

01/27/09

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

- (S//SI//REL) Features:
  - LxT Model: 900/1800/1900MHz
  - LxU Model: 850/1800/1900MHz
  - Pico-class (1Watt) Base station
  - Optional Battery Kits
  - Highly Mobile and Deployable
  - Integrated GPS, MS, & 802.11
  - Voice & High-speed Data
  - SMS Capability
- (S//SI//REL) Enclosure:
  - 1.9"H x 8.6"W x 6.3"D
  - Approximately 3 lbs
  - Actively cooled for extreme environments

- (S//SI//REL) EBSR System Kit:
  - EBSR System
  - AC/DC power converter
  - Antennas to support MS, GPS, WIFI, & RF
  - LAN, RF, & USB cables
  - Pelican Case
  - (Field Kit only) Control Laptop and Accessories
- (S//SI//REL) Separately Priced Options:
  - 90 WH LiIon Battery Kit
- (S//SI//REL) Base Station Router Platform:
  - Multiple BSR units can be interconnected to form a macro network using 802.3 and 802.11 back-haul.
  - Supports Landshark/Candygram capabilities.

Status:

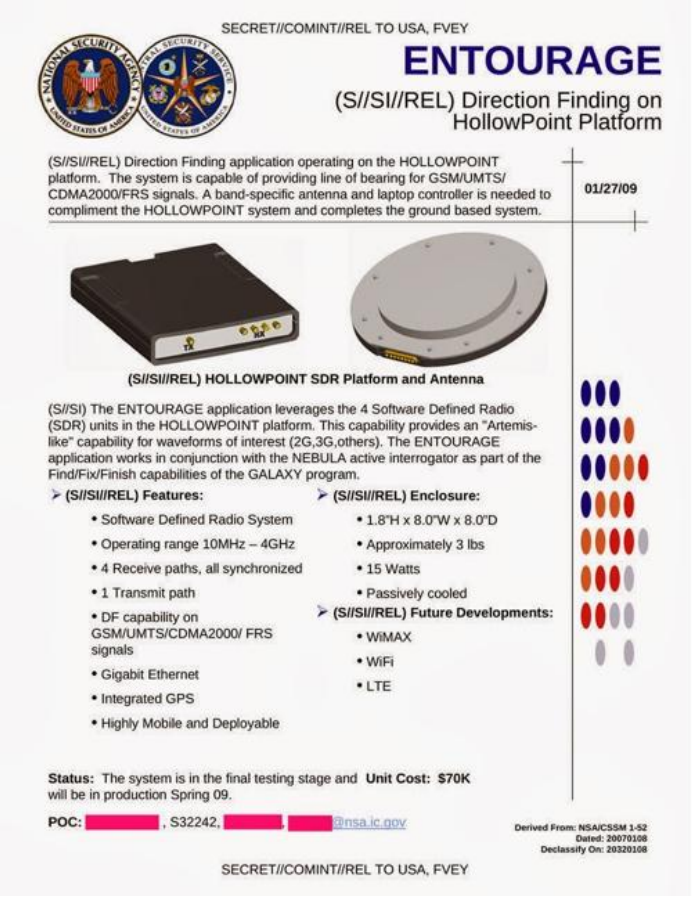
Unit Cost: $40K

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

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

SECRET//COMINT//REL TO USA, FVEY

EBSR, ложная базовая станция GSM



SECRET//COMINT//REL TO USA, FVEY

ENTOURAGE

(S//SI//REL) Direction Finding on HollowPoint Platform

(S//SI//REL) Direction Finding application operating on the HOLLOWPOINT platform. The system is capable of providing line of bearing for GSM/UMTS/CDMA2000/FRS signals. A band-specific antenna and laptop controller is needed to compliment the HOLLOWPOINT system and completes the ground based system.

01/27/09

(S//SI//REL) HOLLOWPOINT SDR Platform and Antenna

(S//SI) The ENTOURAGE application leverages the 4 Software Defined Radio (SDR) units in the HOLLOWPOINT platform. This capability provides an "Artemis-like" capability for waveforms of interest (2G,3G,others). The ENTOURAGE application works in conjunction with the NEBULA active interrogator as part of the Find/Fix/Finish capabilities of the GALAXY program.

- (S//SI//REL) Features:
  - Software Defined Radio System
  - Operating range 10MHz – 4GHz
  - 4 Receive paths, all synchronized
  - 1 Transmit path
  - DF capability on GSM/UMTS/CDMA2000/ FRS signals
  - Gigabit Ethernet
  - Integrated GPS
  - Highly Mobile and Deployable

- (S//SI//REL) Enclosure:
  - 1.8"H x 8.0"W x 8.0"D
  - Approximately 3 lbs
  - 15 Watts
  - Passively cooled
- (S//SI//REL) Future Developments:
  - WiMAX
  - WiFi
  - LTE

Status: The system is in the final testing stage and will be in production Spring 09.

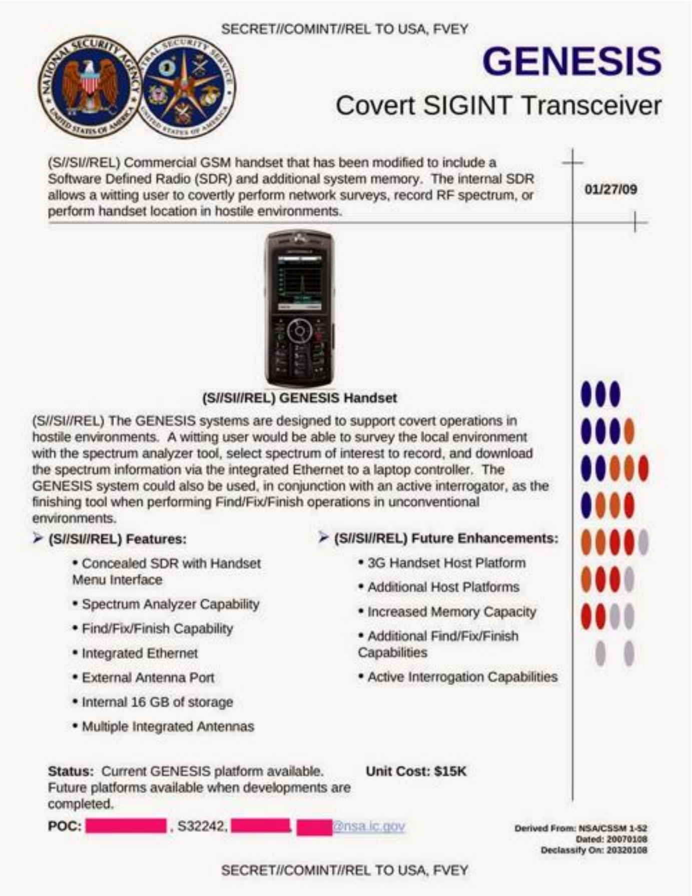
Unit Cost: $70K

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

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

SECRET//COMINT//REL TO USA, FVEY

ENTOURAGE, устройство для поиска и определения местоположения телефонов GSM и 3G



SECRET//COMINT//REL TO USA, FVEY

GENESIS

Covert SIGINT Transceiver

(S//SI//REL) Commercial GSM handset that has been modified to include a Software Defined Radio (SDR) and additional system memory. The internal SDR allows a witting user to covertly perform network surveys, record RF spectrum, or perform handset location in hostile environments.

01/27/09

(S//SI//REL) GENESIS Handset

(S//SI//REL) The GENESIS systems are designed to support covert operations in hostile environments. A witting user would be able to survey the local environment with the spectrum analyzer tool, select spectrum of interest to record, and download the spectrum information via the integrated Ethernet to a laptop controller. The GENESIS system could also be used, in conjunction with an active interrogator, as the finishing tool when performing Find/Fix/Finish operations in unconventional environments.

➢ (S//SI//REL) Features:

- Concealed SDR with Handset Menu Interface
- Spectrum Analyzer Capability
- Find/Fix/Finish Capability
- Integrated Ethernet
- External Antenna Port
- Internal 16 GB of storage
- Multiple Integrated Antennas

➢ (S//SI//REL) Future Enhancements:

- 3G Handset Host Platform
- Additional Host Platforms
- Increased Memory Capacity
- Additional Find/Fix/Finish Capabilities
- Active Interrogation Capabilities

Status: Current GENESIS platform available. Future platforms available when developments are completed.

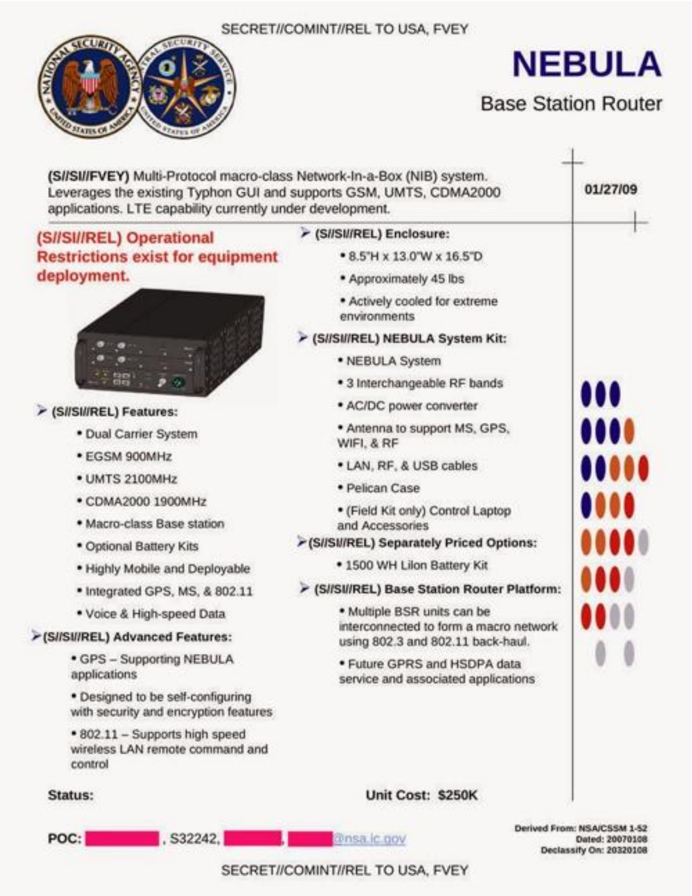
Unit Cost: $15K

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

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

SECRET//COMINT//REL TO USA, FVEY

GENESIS, модифицированный сотовый телефон с анализатором спектра GSM и 3G сетей для радиоразведки



SECRET//COMINT//REL TO USA, FVEY

NEBULA

Base Station Router

(S//SI//FVEY) Multi-Protocol macro-class Network-In-a-Box (NIB) system. Leverages the existing Typhon GUI and supports GSM, UMTS, CDMA2000 applications. LTE capability currently under development.

01/27/09

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

➢ (S//SI//REL) Features:

- Dual Carrier System
- EGSM 900MHz
- UMTS 2100MHz
- CDMA2000 1900MHz
- Macro-class Base station
- Optional Battery Kits
- Highly Mobile and Deployable
- Integrated GPS, MS, & 802.11
- Voice & High-speed Data

➢ (S//SI//REL) Advanced Features:

- GPS – Supporting NEBULA applications
- Designed to be self-configuring with security and encryption features
- 802.11 – Supports high speed wireless LAN remote command and control

➢ (S//SI//REL) Enclosure:

- 8.5"H x 13.0"W x 16.5"D
- Approximately 45 lbs
- Actively cooled for extreme environments

➢ (S//SI//REL) NEBULA System Kit:

- NEBULA System
- 3 Interchangeable RF bands
- AC/DC power converter
- Antenna to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories

➢ (S//SI//REL) Separately Priced Options:

- 1500 WH LiIon Battery Kit

➢ (S//SI//REL) Base Station Router Platform:

- Multiple BSR units can be interconnected to form a macro network using 802.3 and 802.11 back-haul.
- Future GPRS and HSDPA data service and associated applications

Status:

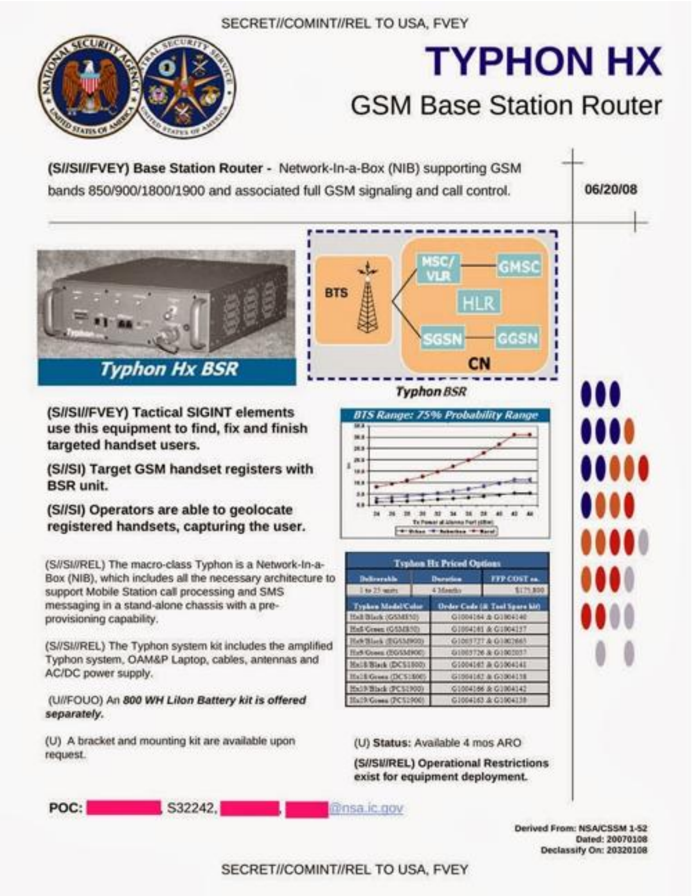
Unit Cost: $250K

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

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

SECRET//COMINT//REL TO USA, FVEY

NEBULA, ложная базовая станция для сетей EGSM, UMTS, CDMA2000



SECRET//COMINT//REL TO USA, FVEY

TYPHON HX

GSM Base Station Router

(S//SI//FVEY) Base Station Router - Network-In-a-Box (NIB) supporting GSM bands 850/900/1800/1900 and associated full GSM signaling and call control.

06/20/08

Typhon Hx BSR
BTS
MSC/VLR
GMSC
HLR
SGSN
GGSN
CN
Typhon BSR
BTS Range: 75% Probability Range
0.0
5.0
10.0
15.0
20.0
25.0
30.0
35.0
24
26
28
30
32
34
36
38
40
42
44
Tx Power at Antenna Port (dBm)
Urban
Suburban
Rural

(S//SI//FVEY) Tactical SIGINT elements use this equipment to find, fix and finish targeted handset users.

(S//SI) Target GSM handset registers with BSR unit.

(S//SI) Operators are able to geolocate registered handsets, capturing the user.

(S//SI//REL) The macro-class Typhon is a Network-In-a-Box (NIB), which includes all the necessary architecture to support Mobile Station call processing and SMS messaging in a stand-alone chassis with a pre-provisioning capability.

(S//SI//REL) The Typhon system kit includes the amplified Typhon system, OAM&P Laptop, cables, antennas and AC/DC power supply.

(U//FOUO) An ***800 WH LiIon Battery kit is offered separately.***

(U) A bracket and mounting kit are available upon request.

Typhon Hx Priced Options		
Deliverable	Duration	FFP COST ea.
1 to 25 units	4 Months	$175,800

Typhon Model/Color	Order Code (& Tool Spare kit)
Hx8/Black (GSM850)	G1004164 & G1004140
Hx8/Green (GSM850)	G1004161 & G1004137
Hx9/Black (EGSM900)	G1003727 & G1002665
Hx9/Green (EGSM900)	G1003726 & G1002057
Hx18/Black (DCS1800)	G1004165 & G1004141
Hx18/Green (DCS1800)	G1004162 & G1004138
Hx19/Black (PCS1900)	G1004166 & G1004142
Hx19/Green (PCS1900)	G1004163 & G1004139

(U) **Status:** Available 4 mos ARO

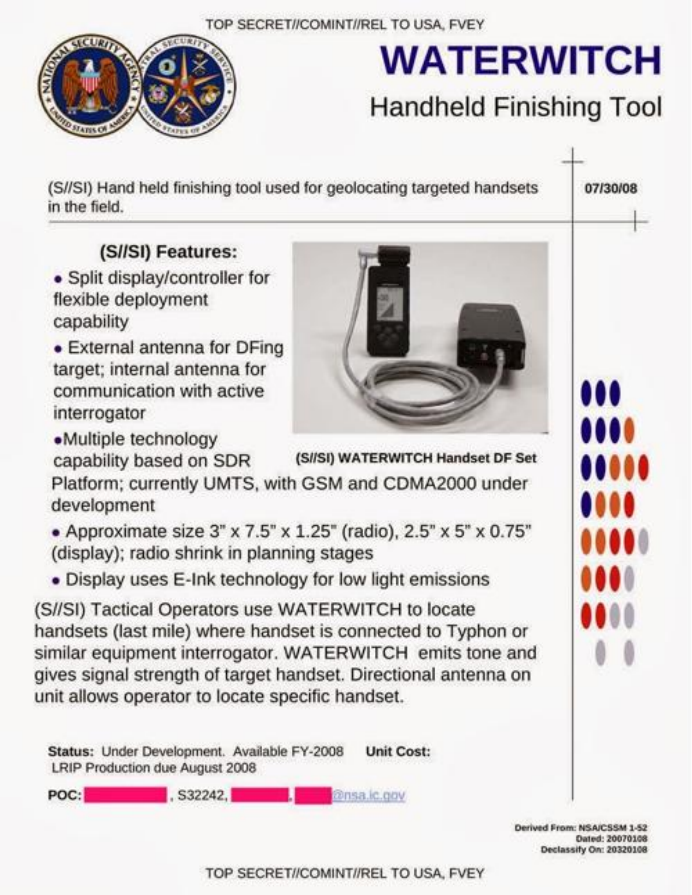
(S//SI//REL) Operational Restrictions exist for equipment deployment.

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

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

SECRET//COMINT//REL TO USA, FVEY

TYPHON HX, ложная базовая станция для сетей GSM 850/900/1800/1900 МГц



TOP SECRET//COMINT//REL TO USA, FVEY

WATERWITCH

Handheld Finishing Tool

(S//SI) Hand held finishing tool used for geolocating targeted handsets in the field.

07/30/08

(S//SI) Features:

- Split display/controller for flexible deployment capability
- External antenna for DFing target; internal antenna for communication with active interrogator
- Multiple technology capability based on SDR Platform; currently UMTS, with GSM and CDMA2000 under development
- Approximate size 3" x 7.5" x 1.25" (radio), 2.5" x 5" x 0.75" (display); radio shrink in planning stages
- Display uses E-Ink technology for low light emissions

(S//SI) WATERWITCH Handset DF Set

(S//SI) Tactical Operators use WATERWITCH to locate handsets (last mile) where handset is connected to Typhon or similar equipment interrogator. WATERWITCH emits tone and gives signal strength of target handset. Directional antenna on unit allows operator to locate specific handset.

Status: Under Development. Available FY-2008 **Unit Cost:**
LRIP Production due August 2008

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

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

TOP SECRET//COMINT//REL TO USA, FVEY

WATERWITCH, устройство для определения местоположения мобильных телефонов