NSA ANT USB, 30C3, Jacob Appelbaum, 30 December 2013

Für USB-Stecker hat die NSA-Abteilung ANT eine ganze Reihe von Computerwanzen im Angebot. Sie sind entweder als der USB-Anschluss einer Tastatur getarnt, oder aber als eine Art USB-Verlängerungsstecker, unbemerkt zwischen Maus-, Keyboard- oder einen anderen Anschluss und den Rechner selbst gesteckt wir Sie funken und empfangen entweder auf kurze Distanz ("Cottonmouth I") oder aber, auf dem Umweg über e weiteres Implantat, irgendwo im Rechner oder im Raum, über weitere Strecken ("Cottonmouth II", "Cottonmouth III"). Diese Implantate erlauben sowohl, den angezapften Rechner und sein Netzwerk zu überwachen, als auch Befehle auf den Rechner und ins gekaperte Netz zu schicken.

COTTONMOUTH-1 ist ein USB-Stecker-Implantat für das Abfangen von Kommunikation, Injizieren von Trojanern etc. Es kann sich über einen eingebauten Radiotransmitter mit anderen COTTONMOUTH-Implantaten verbinden.

COTTONMOUTH-2 ist ein USB-Implantat, das die Fernsteuerung eines Zielsystems ermöglicht. Es wird an Funkmodul gekoppelt, das im Rechnergehäuse versteckt ist und Zugriffe aus größerer Entfernung ermöglic

COTTONMOUTH-3 ist ein USB-Implantat zum Aufbau eines verdeckten Kommunikationsweges über Funkwellen mit Computern, die offline betrieben werden oder bei denen ein Angriff über die Netzschnittstell nicht praktikabel ist. Es wird an ein Funkmodul gekoppelt, das im Rechnergehäuse versteckt ist und Zugriffe aus größerer Entfernung ermöglicht oder sich mit anderen COTTONMOUTH-Modulen in der Nähe verbinde

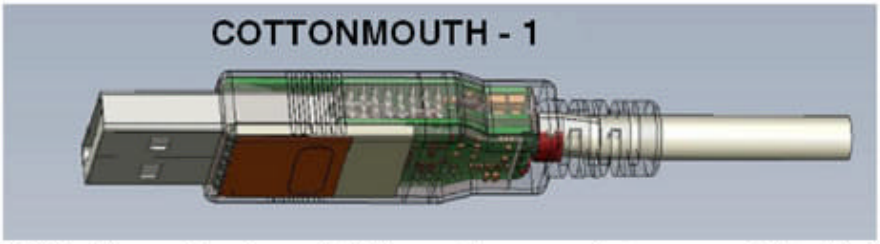
FIREWALK ist ein Hardware-Implantat in der Form einer Ethernet- oder USB-Buchse, das das Abfangen vo Daten und aktive Einschleusen von Angriffstools über Funk erlaubt.

COTTONMOUTH-I

ANT Product Data

08/05/08

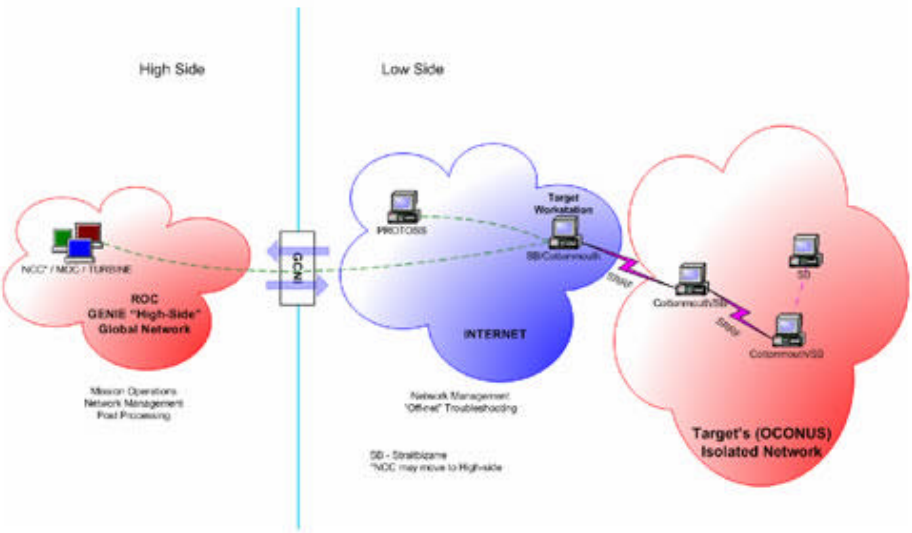
(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.



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

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

COTTONMOUTH CONOP
INTERNET Scenario



Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

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

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

COTTONMOUTH-II

ANT Product Data

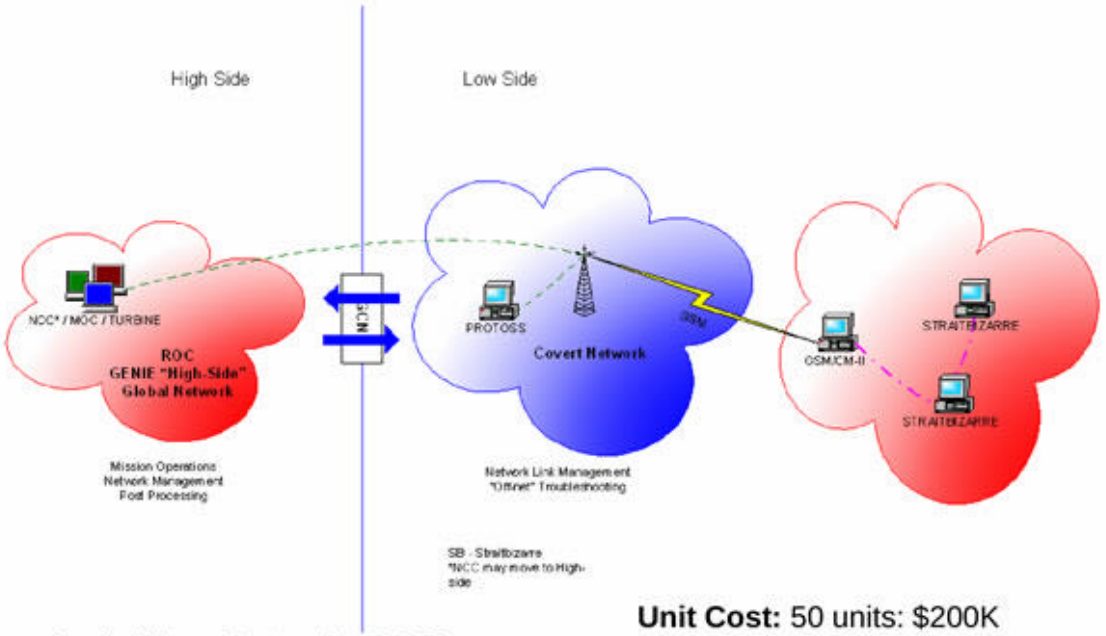
(TS//SI//REL) COTTONMOUTH-II (CM-II) is a Universal Serial Bus (USB) hardware Host Tap, which will provide a covert link over USB link into a targets network. CM-II is intended to be operate with a long haul relay subsystem, which is co-located within the target equipment. Further integration is needed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

08/05/08

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

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

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



Unit Cost: 50 units: $200K

Status: Availability – September 2008

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

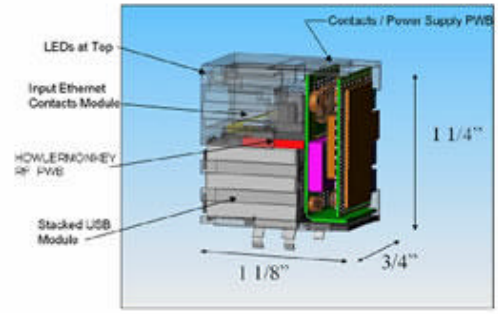
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

COTTONMOUTH-III

ANT Product Data

(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.

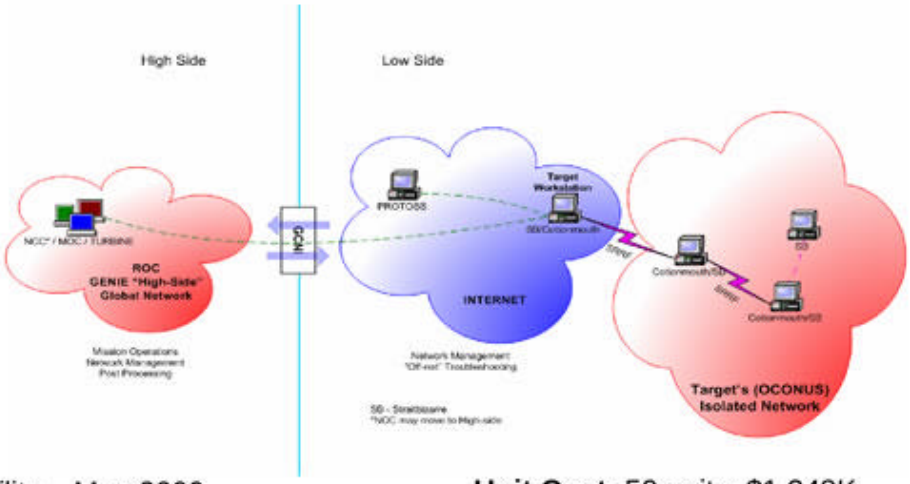
08/05/08



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

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

COTTONMOUTH CONOP
INTERNET Scenario



Status: Availability – May 2009

Unit Cost: 50 units: $1,248K

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

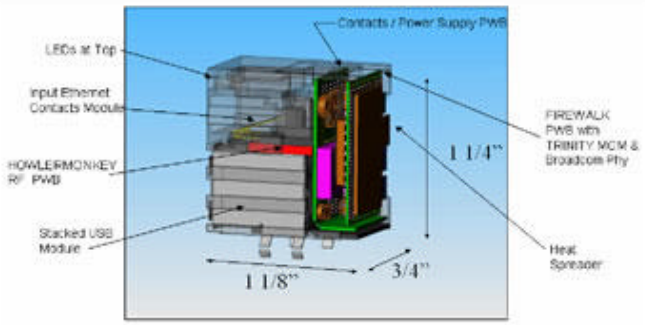
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

FIREWALK

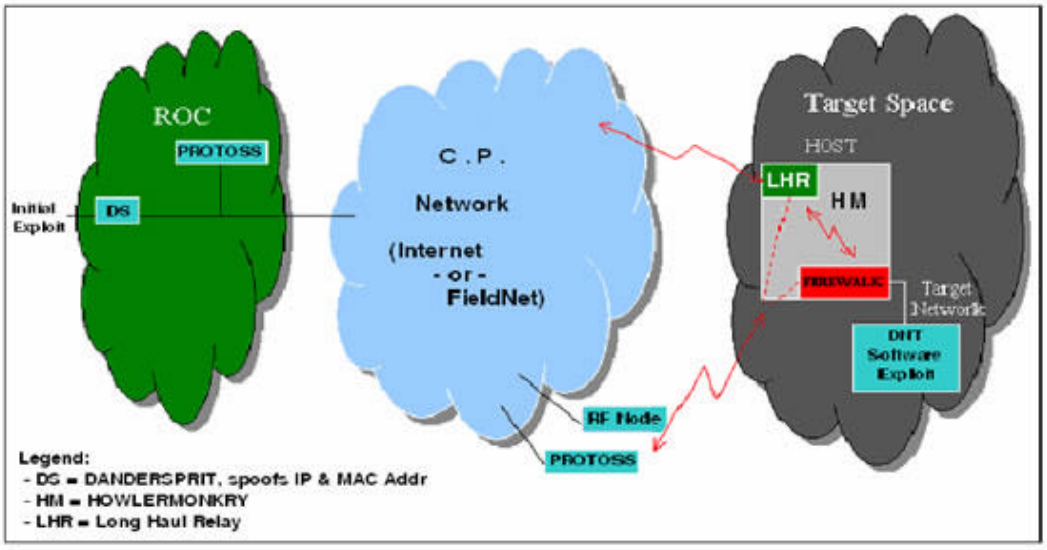
ANT Product Data

08/05/08

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



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



Status: Prototype Available – August 2008

Unit Cost: 50 Units $537K

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

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