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

Router sind spezielle Rechner, die das interne Netzwerk eines Unternehmens oder eines Internet-Providers knüpfen helfen, aber auch Internet-Traffic weiterleiten und verarbeiten. Die NSA-Abteilung ANT hat dem Katalog zufolge, der dem SPIEGEL vorliegt, Implantate für Profi-Router von mindestens zwei Herstellern im Angebot: Juniper und Huawei. Ob es weitere ANT-Produkte für solche Geräte gibt, ist unbekannt. Die ANT-Implantate für Router verstecken sich im Bios, also der untersten Software-Ebene des jeweiligen Geräts. Da stellt sicher, dass sie sogar dann weiterarbeiten und andere Späh-Software nachladen können, wenn der Rechner neu gestartet oder sogar ein neues Betriebssystem aufgespielt wird. Die Router, deren Typbezeichnungen im Katalog auftauchen, sind für kleine, mittlere und große Unternehmen konzipiert – ein auch für die Rechenzentren von Internet- und Mobilfunkanbietern.

Huawei Router
Das chinesische Unternehmen Huawei gehört mittlerweile zu den weltgrößten Herstellern von Netzwerkausrüstung. Im zweiten Quartal 2013 lag Huawei dem Marktforschungsunternehmen Infonetics zufolge auf Platz 2, was den Umsatz mit Routern und Switches für Mobilfunk- und Internet-Provider angeht hinter Cisco und vor Juniper.

HEADWATER ist eine permanente Backdoor (PBD) für Huawei Router, die resistent gegenüber Firmware Updates im Boot-ROM verbleiben und so die Fernsteuerung des Geräts ermöglichen soll.

Juniper J-Series
Juniper-Router der Serie J sind für den Einsatz in Unternehmen gedacht, sie verbinden Server und Desktop Rechner mit dem Unternehmensnetzwerk und dem Internet.

SCHOOLMONTANA sind Software-Implantate für Serie-J-Router der Firma Juniper.

Juniper M-Series
Juniper-Router der Serie M sind für Unternehmen und Service-Provider gemacht. Sie kommen also auch in den Rechenzentrum von Firmen zum Einsatz, die anderen Unternehmen und Privatkunden Internetanschlüs zur Verfügung stellen.

SIERRAMONTANA ist ein Software-Implantat für Juniper-Router der M-Serie, das sich laut des NSA-Dokuments resistent gegenüber Softwareupdates im Bios einnistet.

Juniper T-Series
Die Router der Serie T werden dem Hersteller Juniper zufolge von "führenden Service-Providern eingesetzt um große Festnetz-, Mobil-, Video- und Cloud-Netzwerke zu betreiben".

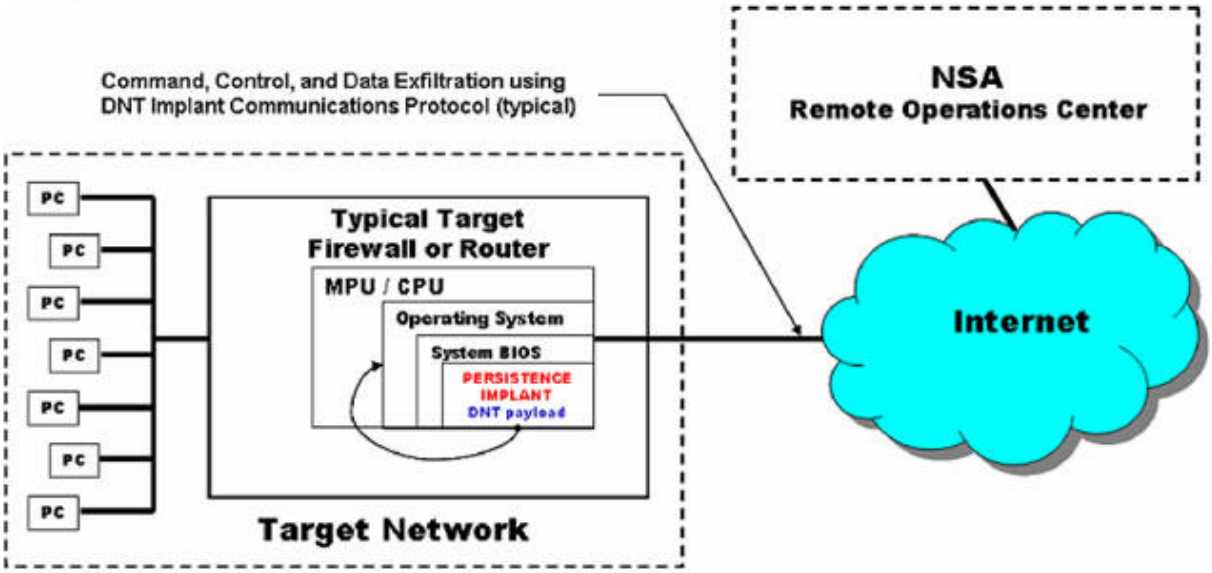
STUCCOMONTANA ist offenbar ein Implantat für Juniper T-Series-Router, das als Bios-Modifikation auch Softwareupdates überstehen soll.

HEADWATER

ANT Product Data

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

06/24/08



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

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

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

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

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

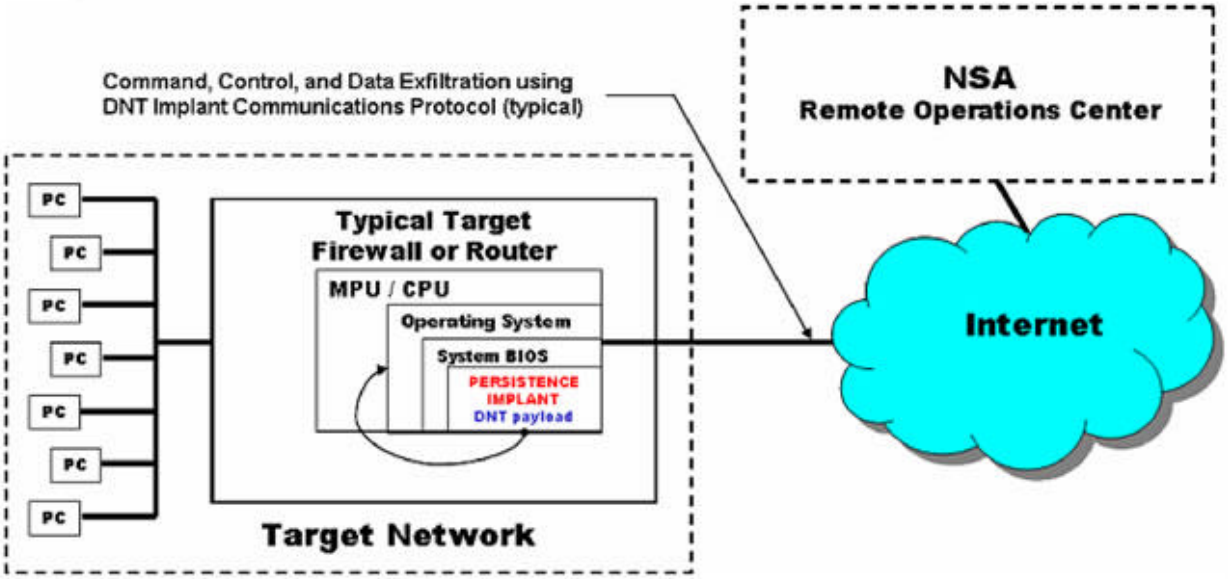
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SCHOOLMONTANA

ANT Product Data

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

06/24/08



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

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

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

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

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

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

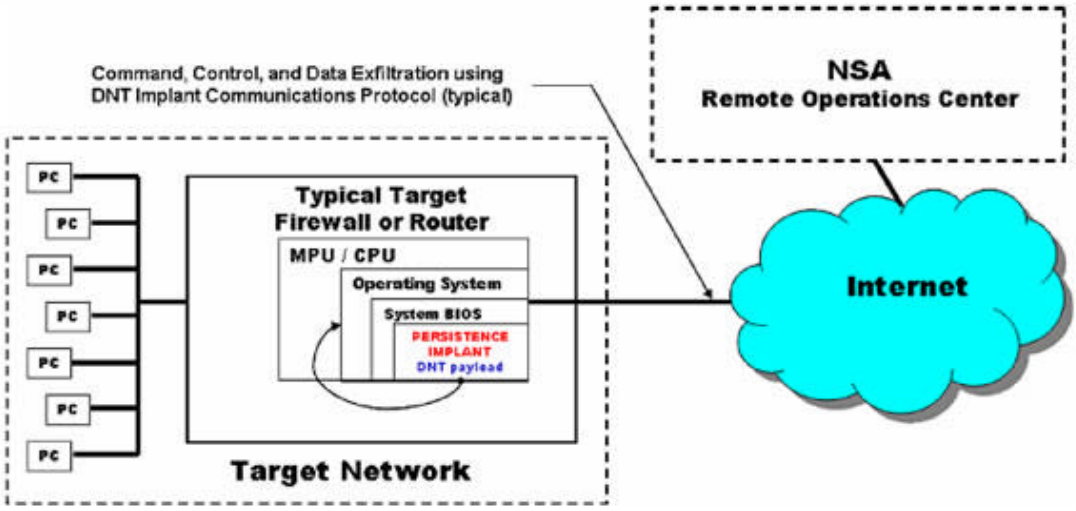
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SIERRAMONTANA

ANT Product Data

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

06/24/08



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

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

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

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

Unit Cost: $

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

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

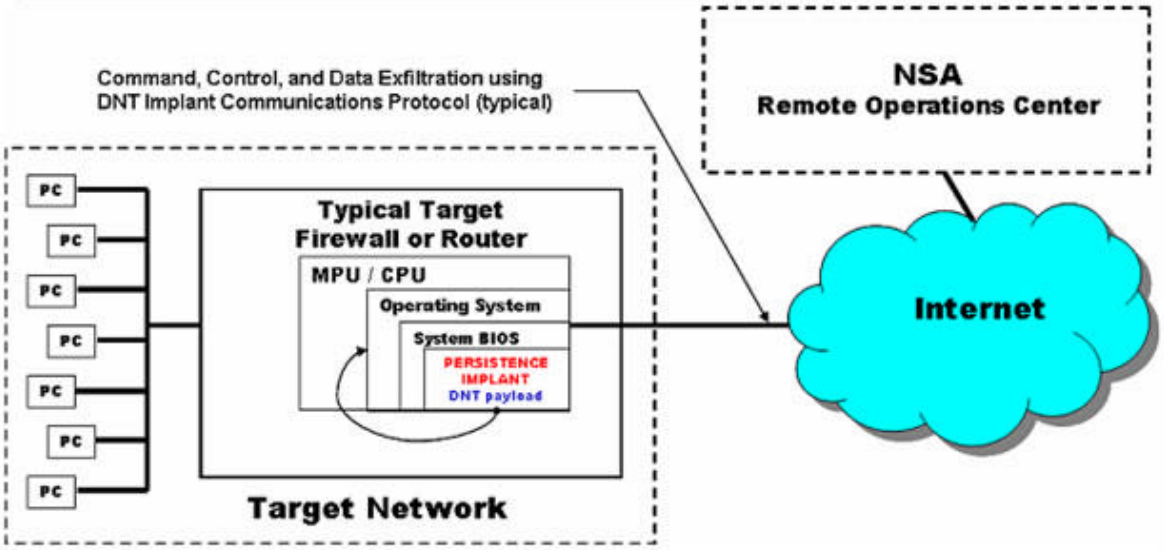
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

STUCCOMONTANA

ANT Product Data

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

06/24/08



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

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

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

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

Unit Cost: $

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

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

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