

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

Hardware-Firewalls sind spezielle Rechner, die zwischen das interne Netzwerk eines Unternehmens oder eines Internet-Providers und das Internet geschaltet werden. Sie sollen Hacker-Angriffe, Denial-of-Service-Attacken und Spam abhalten – und gleichzeitig die Mitarbeiter des Unternehmens, die sich über eine VPN-Verbindung (Virtual Private Network) ins Unternehmensnetz einloggen, durchlassen. Die NSA-Abteilung AN hat laut den Dokumenten Hardware- und Software-Implantate für die Hardware-Firewalls aller großen Hersteller entwickelt: Cisco, Juniper und Huawei. Auf diese Weise werden die eigentlich als digitaler Schutzwall gedachten Computer dieser Hersteller offenbar zu Einfallstoren für die NSA-Hacker gemacht. Die meisten der ANT-Implantate für Firewalls sollen sich im Bios verstecken, also der untersten Software-Ebene des jeweiligen Geräts. Das stellt sicher, dass sie sogar dann weiterarbeiten und andere Spähsoftware nachladen können, wenn der Rechner neu gestartet oder sogar ein neues Betriebssystem aufgespielt wird.

Cisco PIX-Serie, Cisco ASA-Serie

Die Produkte der PIX-Reihe des US-Herstellers Cisco waren Hardware-Firewalls für, je nach Modell, kleine und mittlere Unternehmen oder aber große Unternehmen und Service-Provider. Die Herstellung dieser Modellreihe wurde 2008 eingestellt. Nachfolger sind die Produkte der ASA-Serie, die für Unternehmen unterschiedlicher Größe und für Rechenzentren konzipiert sind.

JETPLOW: Laut dieses NSA-Dokuments ein Software-Implantat für Cisco PIX- und ASA-Firewalls, das dauerhafte Hintertüren installiert.

Huawei Eudemon Serie

Die Hardware-Firewalls der Eudemon-Serie des chinesischen Herstellers Huawei sind sowohl für kleine und mittlere Unternehmen (200er-Serie) wie für Service-Provider und große Unternehmen (1000er-Serie) konzipiert. 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. Huawei-Technik wird beispielsweise auch bei O2, Vodafone und der Deutsche Telekom eingesetzt.

HALLUXWATER ist offenbar eine Hintertür (Backdoor) für Huawei Eudemon Firewalls in Form eines Software-Implantats, das im Boot-Rom verborgen wird.

Juniper Netscreen / ISG 1000

Die größeren Modelle der Netscreen-Serie des Herstellers Juniper und die Firewalls der ISG-Serie sind Herstellerangaben zufolge sowohl für den Einsatz bei Internet-Service-Providern als auch bei Mobilfunkanbietern geeignet.

FEEDTROUGH ist ein Software-Implantat, das Fremdzugriffe auf die Juniper Firewall Modelle N5XT, NS25, NS50, NS200, NS500, ISG1000 ermöglichen soll.

Juniper SSG, Netscreen G5, Netscreen 25 und 50, SSG-Serie

Die Juniper-SSG-Modelle sind Hardware-Firewalls für kleine und mittlere Unternehmen sowie für den Einsatz in Zweigstellen größerer Unternehmen.

GOURMETTROUGH: Ein konfigurierbares Implantat für eine Reihe von Juniper Firewalls, wie das NSA-Dokument zeigt.

SOUFFLETROUGH ist ein im Bios verborgenes Implantat für Juniper SSG300- und SSG500-Geräte, das eine permanente Hintertür (PBD) herstellen soll.

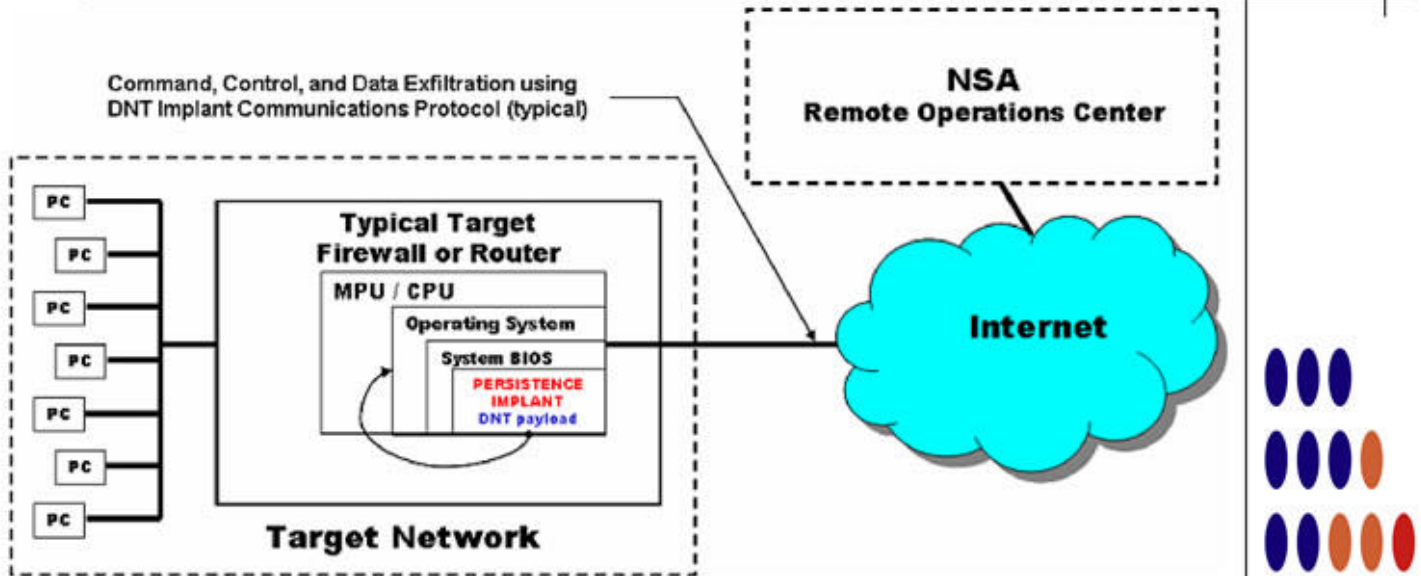


JETPLOW

ANT Product Data

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

06/24/08



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

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

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

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

Unit Cost: \$0

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

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

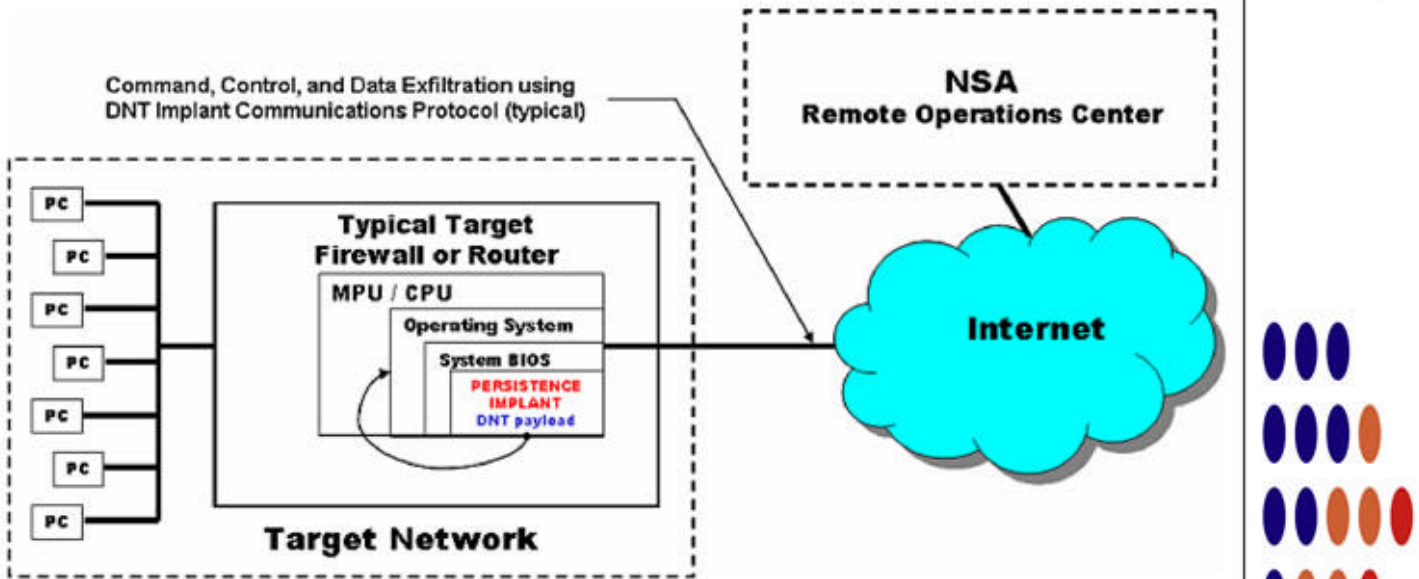


HALLUXWATER

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

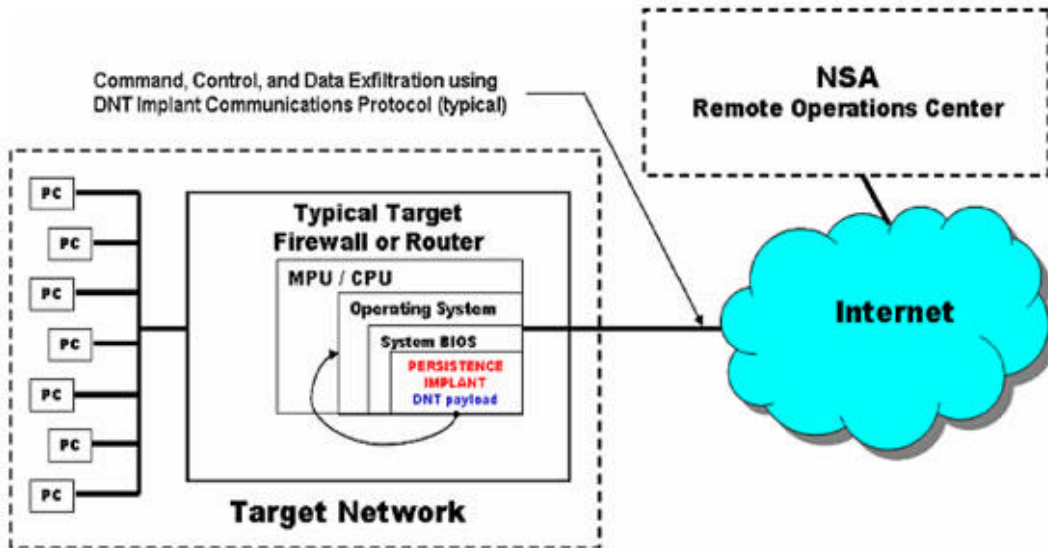


FEEDTROUGH

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

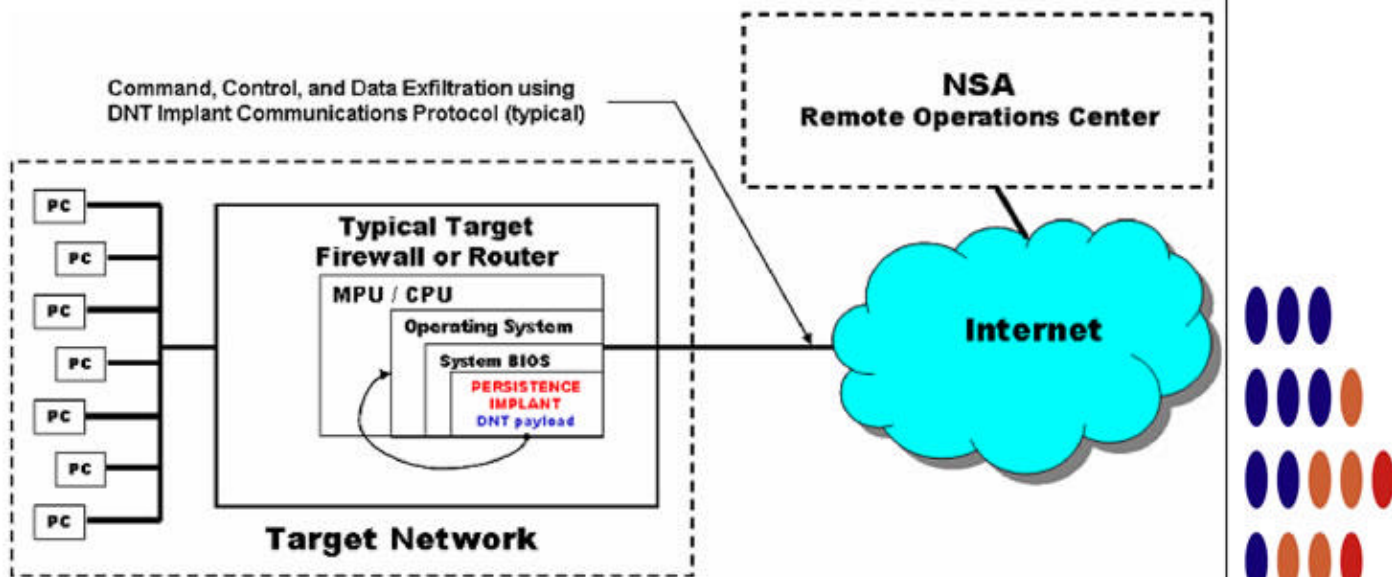


GOURMETTROUGH

ANT Product Data

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

06/24/08



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

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

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

Unit Cost: \$0

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

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

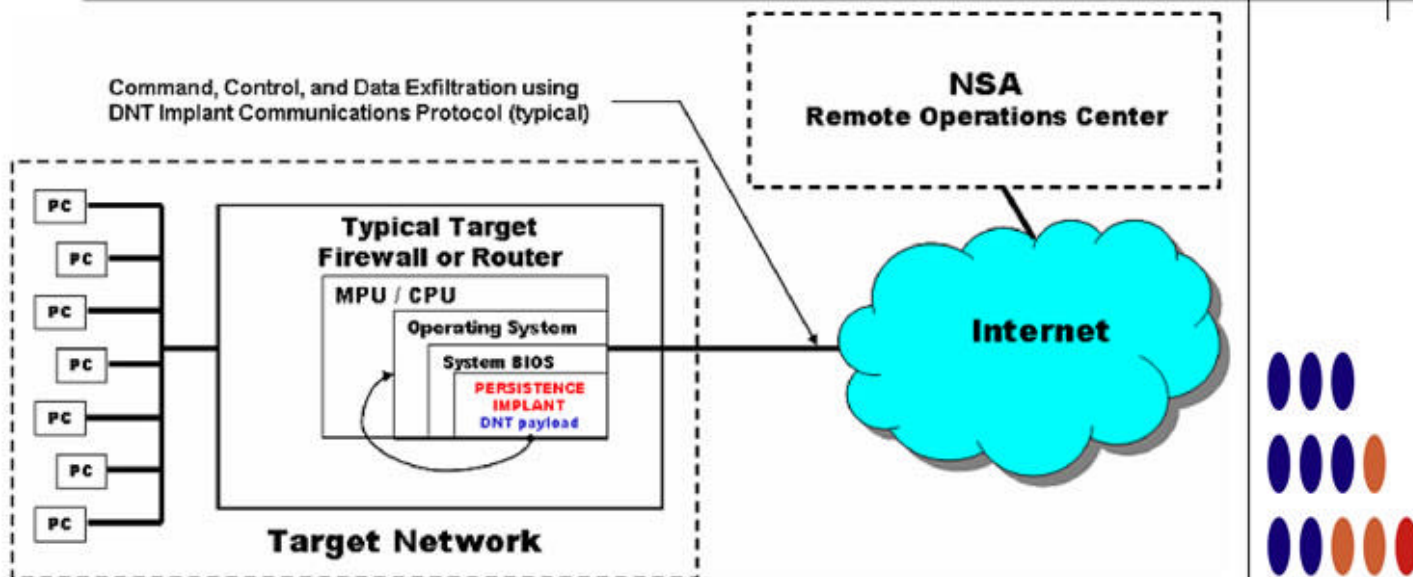


SOUFFLETROUGH

ANT Product Data

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

06/24/08



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

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

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

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

Unit Cost: \$0

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

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