

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

Die NSA-Abteilung ANT entwickelt Implantate für Handys und auch für Sim-Karten. Die Späh-Software für das erste iPhone namens DROPOUTJEEP etwa war im Jahr 2008, kurz nach der Markteinführung, noch in der Entwicklung. Sie sollte es erlauben, aus der Ferne Dateien vom Handy herunter- und andere darauf zu laden, SMS abzuzweigen, das Adressbuch auszulesen, Voicemail abzufangen, das Mikrofon und die Kamera nach Belieben zu bedienen, die aktuell benutzte Funkzelle zu ermitteln, den Aufenthaltsort des Besitzers mitzuteilen "und so weiter", wie es im Katalog heißt. Für spezielle Fälle entwickeln die ANT-Techniker auch modifizierte Handys, die wie normale Standardgeräte aussehen, aber diverse Informationen an die NSA weiterleiten – zum unbemerkten Austausch oder zur Weitergabe an Informanten und Agenten. 2008 waren Modelle von Eastcom und Samsung im Angebot – mittlerweile dürften weitere hinzugekommen sein.

DROPOUTJEEP ist ein Implantat für Apples iPhone-Betriebssystem iOS, das die Fernsteuerung über SMS oder Datendienste ermöglichen soll. Laut des NSA-Dokuments soll es diverse Möglichkeiten bieten: Dateien herunter- oder auf das Handy hochladen, SMS auslesen, Adressbuch auslesen, Voicemail abhören, Standortdaten erfassen, Mikrofon und Kamera unbemerkt einschalten, Funkzelle bestimmen. Anfang 2008 war es noch in der Entwicklung.

GOPHERSET: Ein Implantat für GSM SIM-Karten, das über verborgene Funktionen das Telefonbuch, Kurznachrichten (SMS) und das Protokoll ab- und eingehender Gespräche ausliest.

MONKEYCALENDAR ist eine Angriffs-Software, die es ermöglicht, SIM-Karten dazu zu bringen, Standortinformationen als verborgene SMS zu versenden.

TOTECHASER ist ein Implantat, das sich im Flashrom des Thuraya 2520 Satellitentelefon verbergen und Daten des eingebauten Windows CE über versteckte SMS-Funktionen weiterreichen soll.

TOTEGHOSTLY ist ein Implantat aus der STRAITBIZARRE-Familie der NSA, das die vollständige Fernsteuerbarkeit von Windows Mobile Phones ermöglicht. Es soll diverse Möglichkeiten bieten: Dateien herunter- oder auf das Handy hochladen, SMS auslesen, Adressbuch auslesen, Voicemail abhören, Standortdaten erfassen, Mikrofon und Kamera einschalten, Funkzelle bestimmen.

PICASSO ist ein modifiziertes Mobiltelefon, das über GSM-Netze als Ortungs- und Audiowanze agiert. Die Daten werden über USB-Schnittstelle oder verborgene SMS aus dem Gerät übertragen.

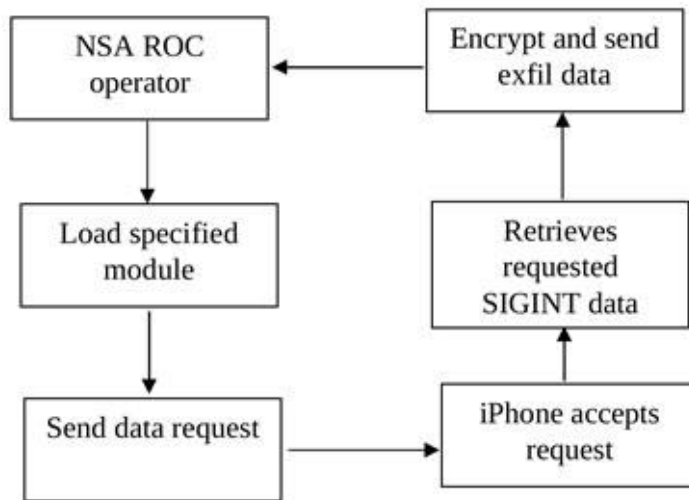


DROPOUTJEEP

ANT Product Data

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

10/01/08



(U//FOUO) DROPOUTJEEP – Operational Schematic

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

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

Unit Cost: \$ 0

Status: (U) In development

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

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

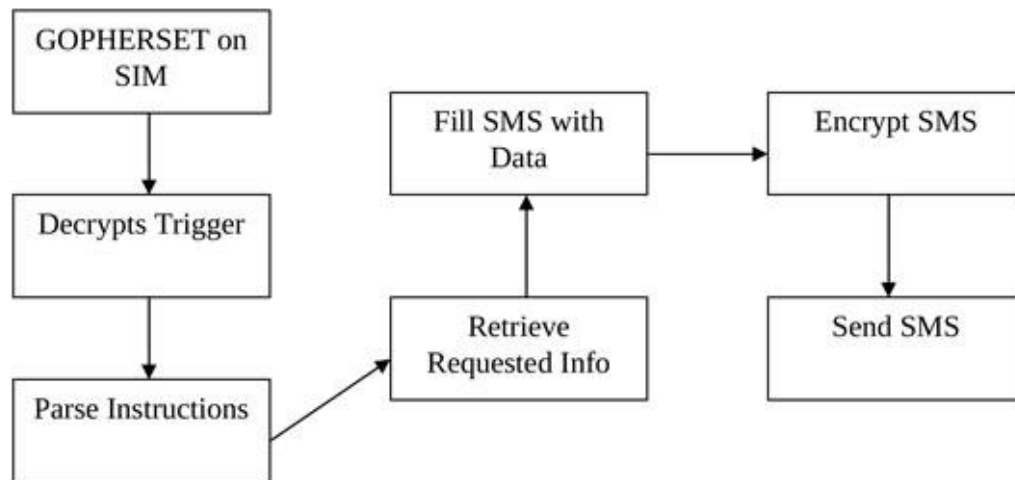


GOPHERSET

ANT Product Data

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

10/01/08



(U//FOUO) GOPHERSET – Operational Schematic

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

Unit Cost: \$0

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

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

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

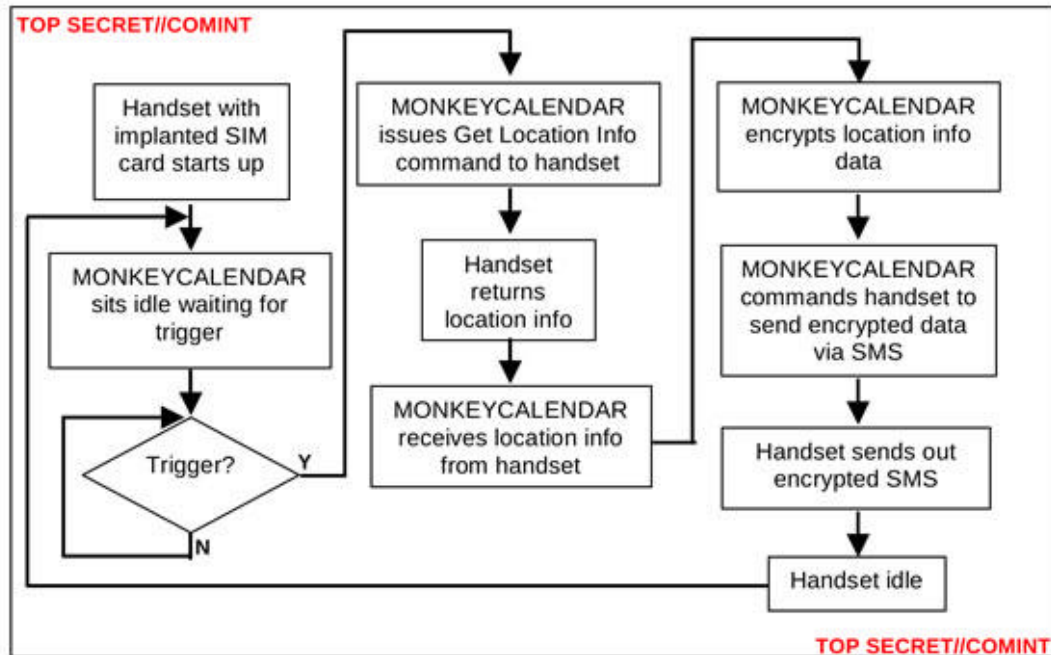


MONKEYCALENDAR

ANT Product Data

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

10/01/08



(U//FOUO) MONKEYCALENDAR – Operational Schematic

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

Unit Cost: \$0

Status: Released, not deployed.

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

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

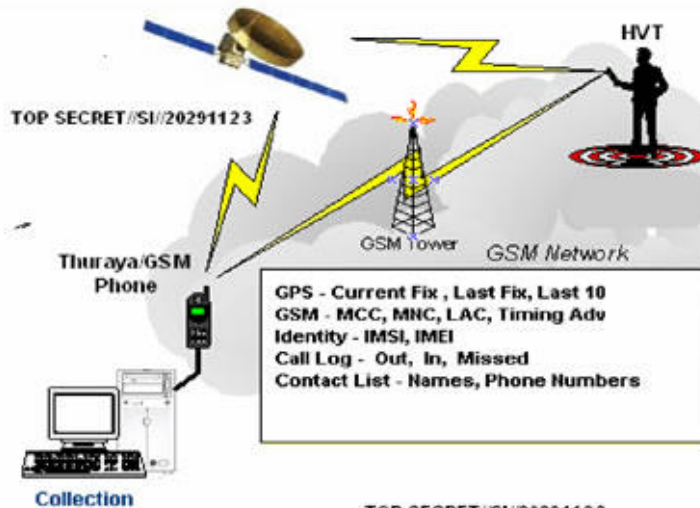


TOTECHASER

ANT Product Data

(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.

10/01/08



(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 TOTEHOSTLY implant is intended for a future version.

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

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

Unit Cost: \$

Status:

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

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

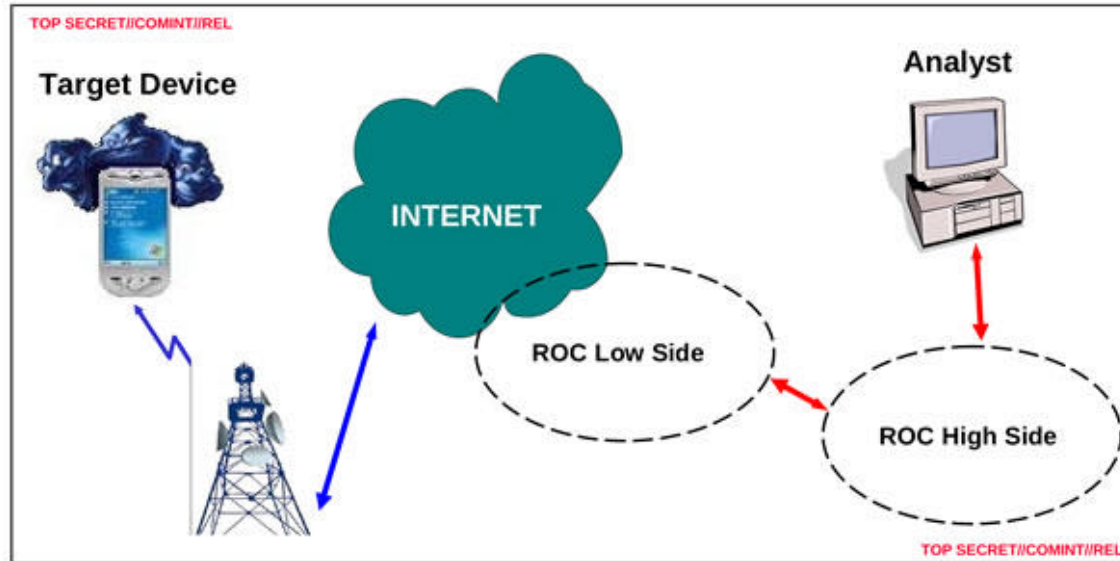


TOTEGHOSTLY 2.0

ANT Product Data

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

10/01/08



(U//FOUO) TOTEGHOSTLY – Data Flow Schematic

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

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

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

Unit Cost: \$0

Status: (U) In development

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

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



PICASSO

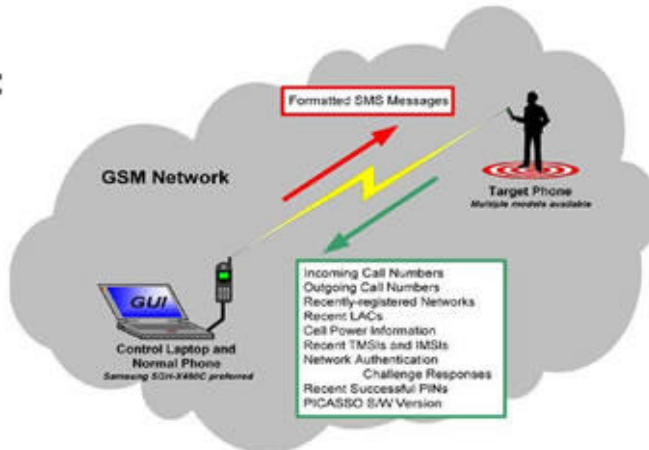
GSM HANDSET

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

06/20/08

(S//SI) Target Data via SMS:

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



(S//SI) PICASSO Operational Concept

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

Status: 2 weeks ARO (10 or less)

(S//SI//REL) Handset Options

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



Unit Cost: approx \$2000

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

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

