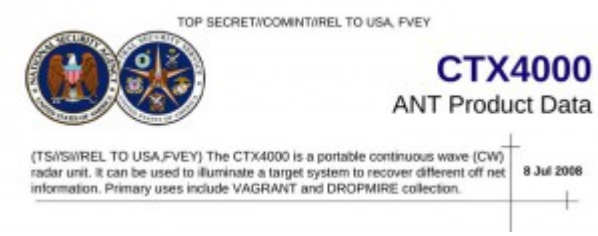
TOP SECRET: La tecnología con la que espía la NSA



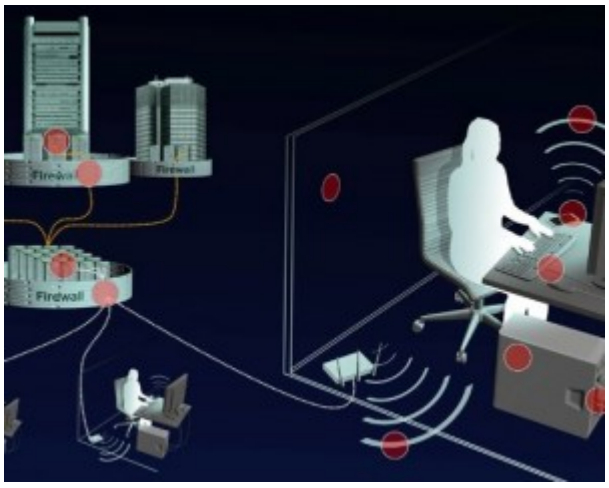
La monitorización masiva de toda la sociedad a través de internet y los dispositivos móviles no sorprende a nadie.

Aunque el revuelo se haya montado de igual forma debido a confirmación de la gravedad del asunto y a su exposición pública. Como para vencer hay que conocer al enemigo, haremos un repaso por **la tecnología con la que espía la NSA** en dos entregas que te dejarán boquiabierto.

El forzado héroe moderno es un tipo sin poderes especiales ni habilidad hollywoodense para esquivar balas mientras sortea obstáculos rescatando a la chica linda en sus brazos. El héroe moderno es un tipo como Edward Snowden, que de un día para otro dejó todo lo que tenía y actuando de la manera menos conveniente para él, le avisó al mundo que había visto algo que no estaba bien. La NSA nos espiaba a través del proyecto PRISM, y si bien todo el mundo ya daba por sentado que la CIA y EEUU siempre tenían un ojo en internet y las telecomunicaciones, la confirmación documentada fue escandalosa. Lamentablemente, como el poder de confrontación social está demasiado solapado por las comodidades que brinda el *status quo*, el pedido de explicaciones y la protesta se diluyó en cuestión de semanas. Lo que quedó sí fue el saber más público sobre las acciones de la NSA y un tenue interés por hallar formas de comunicarse y navegar en la red sin que nuestra privacidad sea tan violada.

El centro de espionaje de la NSA

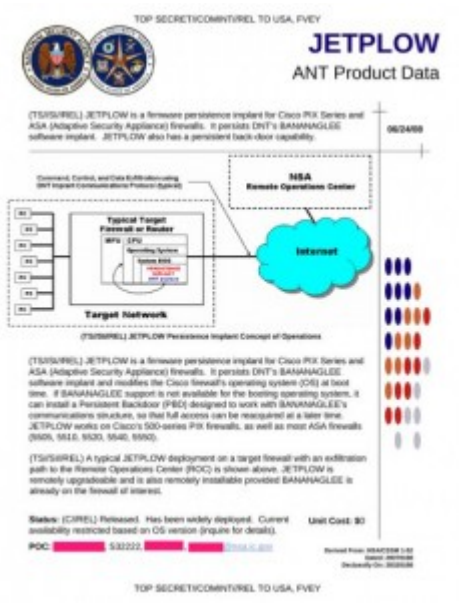
Miles de sitios han tomado por las astas el tema y han detallado la forma en la que se maneja este organismo fanático del chismerío tecnológico de alto costo y alcance, pero para comprender mejor qué es lo que se sabe hasta el momento sobre la NSA y sus métodos de espionaje, es bueno repasar la última información disponible conseguida por el periódico Der Spiegel para analizar qué alternativas reales tenemos a la hora de evadirla. A continuación entonces, haremos un resumen y te contaremos con qué aparatos cuenta la NSA para espiarnos y en qué gasta secretamente su presupuesto el país que dice ser la policía del mundo.



Las formas de espiar de la NSA

Implantes ANT para crear back doors

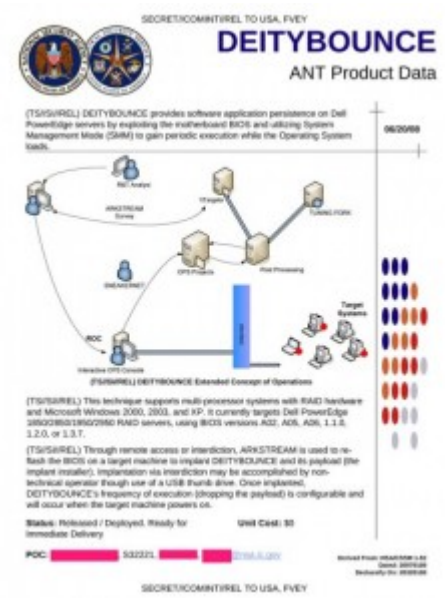
Los firewalls o cortafuegos tienen la finalidad de evitar la piratería, los ataques cibernéticos, el spam o los ataques de denegación de servicio, pero aprovechados por la NSA, los firewalls han servido de puerta de entrada a las redes de empresas y particulares. La división ANT de la NSA ha desarrollado “implantes” de hardware y software para servidores de seguridad de todos los principales fabricantes (Cisco, Juniper y Huawei) transformando a nuestro ordenador en un blanco inerme ante los **ataques de la NSA**. La mayoría de los implantes de firewall de ANT funcionan ocultándose a sí mismos en el BIOS o firmware del dispositivo. Esto asegura que el implante todavía será capaz de funcionar y mantenerse activo por más que se formatee el disco y se reinstale un nuevo sistema operativo. Especialmente diseñado para los routers Cisco PIX y ASA-Serie, los implantes persistentes Jetplow de la ANT creaban back-doors para que la NSA los aprovechase a su antojo a la hora de investigar a alguien.



Atravesando Firewalls con implantes ANT

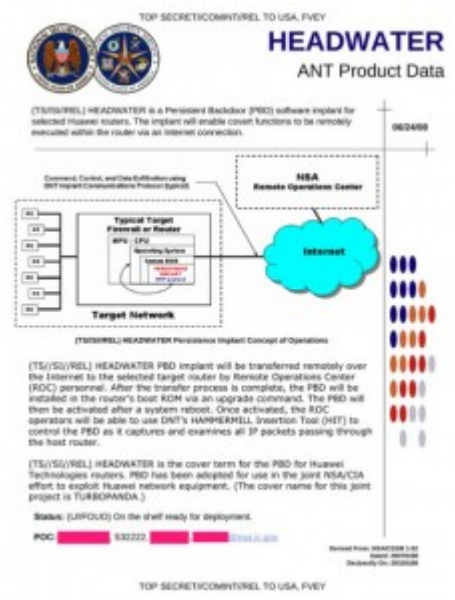
Servidores y routers

Según el catálogo presentado por la revista de investigación Der Spiegel, la división de ANT de la NSA hace varios implantes de hardware y software para servidores realizados por un puñado de fabricantes, incluyendo Dell y Hewlett-Packard. Un implante de software llamado “DEITYBOUNCE”, por ejemplo, se oculta dentro de la BIOS de los servidores Dell PowerEdge. Esta posición privilegiada permite que el implante haga funcionar o instale más software espía. Los implantes de hardware para servidores Dell y HP se deben instalar en un proceso que la NSA llama “interdicción”, en el que agentes interceptan un equipo mientras que se está entregando a su comprador, manipulan el hardware y luego lo devuelven a la ruta de entrega prevista como si no hubiera pasado nada. Dentro de estos implantes también tenemos a IRONCHIEF que está diseñado para los servidores Proliant, de HP.



Servidores infectados

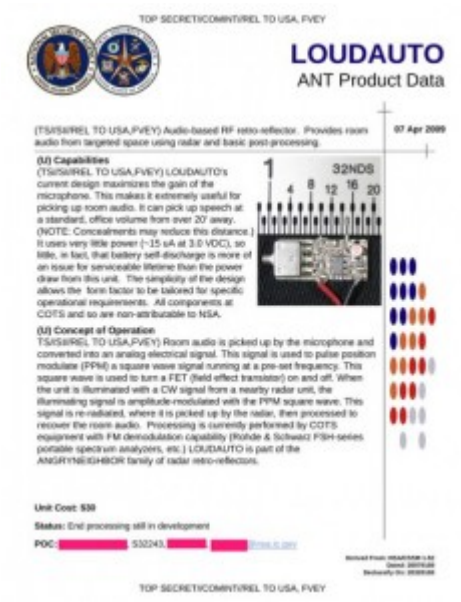
Los implantes creados para routers tienen dos fabricantes como objetivos (¿o cómplices?). Ambas marcas son Juniper y la china Huawei, y los modelos afectados por este implante llamado Headwater son hogareños o empresariales de distintas capacidades. Este implante es se instala en el router Huawei y produce un backdoor permanente que se esconderá en la boot ROM del dispositivo, siendo resistente a actualizaciones y pudiéndose ejecutar y maniobrar de forma remota a través de internet enviando paquetes de información a la NSA con todas las direcciones IP que pasan por él. Otro implante es el SCHOOLMONTANA, que a su vez también es un producto de la ANT. Éste provee persistencia para los implantes DNT, haciéndolo sobrevivir a actualizaciones o remplazaos del sistema operativo. Para terminar, otros dos implantes son el SIERRAMONTANA, que puede hacer instalar software en el BIOS y el STUCCOMONTANA, que se enfoca en los routers Juniper-T.



Headwater para interceptar IPs que pasan por un router

Vigilancia de ambientes con micrófonos

La división ANT de la NSA ha desarrollado toda una gama de equipos para ver y escuchar lo que sucede dentro de las habitaciones sin tener que instalar dispositivos de escucha en ellos. La mayor parte de este procedimiento implica una combinación de implantes de hardware que emiten una señal muy poco visible, y una unidad de radio dirigida, desde fuera, en el espacio que está siendo monitoreada. Las ondas de radar reflejadas se cambian a la señal emitida por el implante oculto en el espacio objetivo, por lo que es posible la captura de la ubicación de un objeto específico en la habitación. El nombre de ANT para esta familia de equipos de vigilancia compuesto por una combinación de implantes de hardware y la detección por radar es “ANGRYNEIGHBOR.”


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.

32NDS

(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] 532243, [redacted]

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

Escucha y graba conversaciones para enviarlas a la NSA

Luego está la unidad de radar CTX4000, que puede revelar las señales emitidas por los dispositivos tales como impresoras láser, aunque no contienen un implante. La NSA llama a este sistema “DROPMIRE”, y los documentos internos muestran que se ha utilizado, por ejemplo, para espiar a las oficinas de los representantes de la UE en Washington. También está LOUDAUTO, que es un micrófono oculto para enviar transmisiones de conversaciones reflejadas grabadas. NIGHTWATCH es un sistema para reconstruir señales de monitor de sistemas objetivos.


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: NA

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], 932243, [redacted], [redacted]@nsa.ic.gov

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

CTX4000 analiza las ondas capturadas por los micrófonos

PHOTOANGLO es un sistema avanzado de radar que detecta reflexiones de señales de onda continua permitiendo que el ANGRYNEIGHBOR reciba desde una distancia más grande. Por último se encuentra en TAWDRYYARD, que es un módulo de hardware que retro-refleja señales de radar entrantes y permite localizar diferentes objetos y señales dentro de una habitación, incluso detrás de paredes.

Redes LAN inalámbricas

La ANT de la NSA también desarrolla métodos para obtener acceso a las redes LAN inalámbricas desde el exterior, lo que les permite aprovechar estas redes y plantar su propio software en ellas. El sistema “NIGHTSTAND”, por ejemplo, puede inyectar de forma remota los paquetes deseados en el tráfico

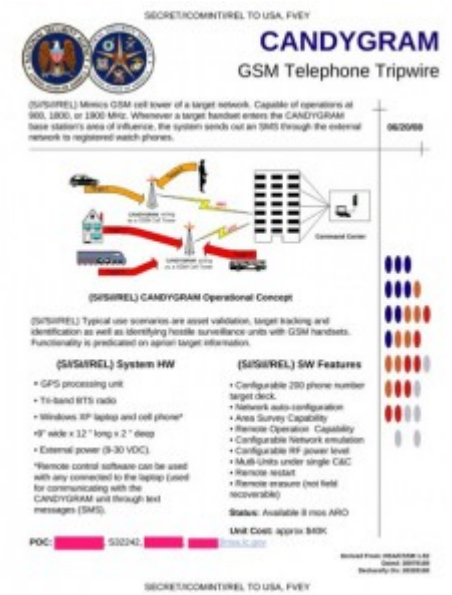
de datos de estas redes inalámbricas usando el estándar 802.11. Luego está el sistema “SPARROW III”, diseñado para mapear redes LAN inalámbricas desde el aire. El sistema es lo suficientemente pequeño para ser montado en un avión no tripulado (UAV) o dron.

Espionaje vía LAN inalámbrica

Redes de telefonía móvil

En relación a la vigilancia y seguimiento de los teléfonos móviles, la división ANT de la NSA tiene toda una gama de productos que atacan a los modelos de teléfonos móviles especialmente equipados que permiten hacer un seguimiento físico a otro teléfono móvil y estaciones de base GSM totalmente equipada capaz de hacerse pasar por las antenas de telefonía móvil oficial de un operador de red, y así

monitorear y grabar conversaciones o mensajes de texto desde teléfonos móviles dentro de su rango. Hay un dispositivo llamado “CANDYGRAM” que funciona como un “tripwire de teléfono” que envía un mensaje de texto a un centro de mando en cuanto ciertos usuarios de teléfonos móviles entran en su área de cobertura. De esta manera se pueden rastrear personas específicas portando un teléfono y saber su ubicación.



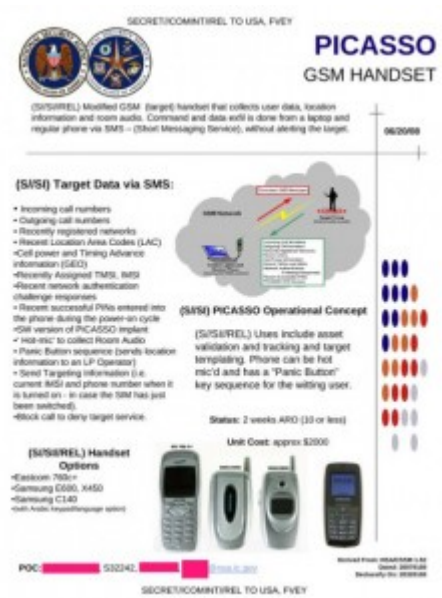
Redes móviles

En este rubro encontramos a CROSSBEAM, un implante que se puede instalar en una notebook para interceptar comunicaciones móviles y dar acceso remoto. ENTOURAGE es un dispositivo para detectar móviles a través de las coordenadas del GPS GENESIS funciona como un móvil normal pero que sirve como un analizador del espectro y parámetros de la red a la cual está asociado. WATERWITCH funciona como un sistema de

geolocalización de móviles cercanos y luego hay varias bases y estaciones móviles de GMS y 3G.

Móviles

Los teléfonos inteligentes han sido de gran ayuda para la investigación de la NSA, ya que recopilan mucha información del usuario en un mismo y explotable medio. Uno de los proyectos de la ANT es DROPOUTJEEP, un implante de spyware que fue diseñado para la primera versión de los iPhones. Este software espía tenía por objetivo hacer posible la descarga o subida de archivos de forma remota a un teléfono móvil. También servía para permitir que la NSA desviara mensajes de texto, navegase por la libreta de direcciones del usuario, interceptara mensajes de voz, activara el micrófono del teléfono y la cámara a su antojo, además de determinar la ubicación actual del usuario, entre otras cosas. Los técnicos de ANT también desarrollan teléfonos móviles modificados, para su uso en casos especiales. Estos móviles se parecen a los dispositivos normales, estándar, pero transmiten varias piezas de información a la NSA automáticamente y se pueden intercambiar con el teléfono de un objetivo. En 2008, ANT tenía modelos de Eastcom y Samsung que se ofrecen, y probablemente ha desarrollado modelos adicionales.



Móviles interceptados

Entre los implantes y herramientas tenemos GOPHERSET, que era un implante para las tarjetas SIM GSM que usaba funciones ocultas para espiar la libreta de teléfonos, los SMS y el logfile de llamadas entradas y salientes. MONKEYCALENDAR es un software que ataca a las SIM y hace que transmitan la geolocalización del móvil a través de mensajes de texto. TOTECHASER es un implante para flashrom que transfiere datos de Windows CE al centro de mando vía mensajes de texto ocultos. PICASSSO es una serie de teléfonos GSM modificados para recolectar información del usuario a través de la interface USB. Por último tenemos a TOTEGHOSTLY 2.0, un implante que provee acceso remoto y control a los teléfonos móviles con sistema operativo de Windows.

es recién la primera de dos partes en las que develaremos todos los aparatos y tecnologías con las que espía la NSA descubiertas hasta el momento gracias a la investigación del excelente periódico alemán Der Spiegel.

Fuente: La WEB.