ASÍ ACCEDE LA NSA A TU GMAIL

Intentamos explicar de manera sencilla cómo funcionan los 2 programas del Gobierno de EEUU que recogen nuestros datos en Internet.

Alberto Sicilia

Crédito de la imagen: The White House

Durante las últimas semanas hemos conocido muchos detalles sobre los programas de espionaje del gobierno de EEUU a través de su Agencia de Seguridad Nacional (la NSA).

Snowden ha desvelado diversos programas de espionaje: escuchas a líderes mundiales, recolección masiva de llamadas

telefónicas, acuerdos entre agencias de inteligencia de diferentes países, etc.

En este post vamos a intentar explicar en detalle cómo funcionan los 2 programas de espionaje que recogen nuestra información en Internet (y, en particular, cómo acceden a los correos de Gmail).

Dos programas de espionaje secretos: PRISM y MUSCULAR

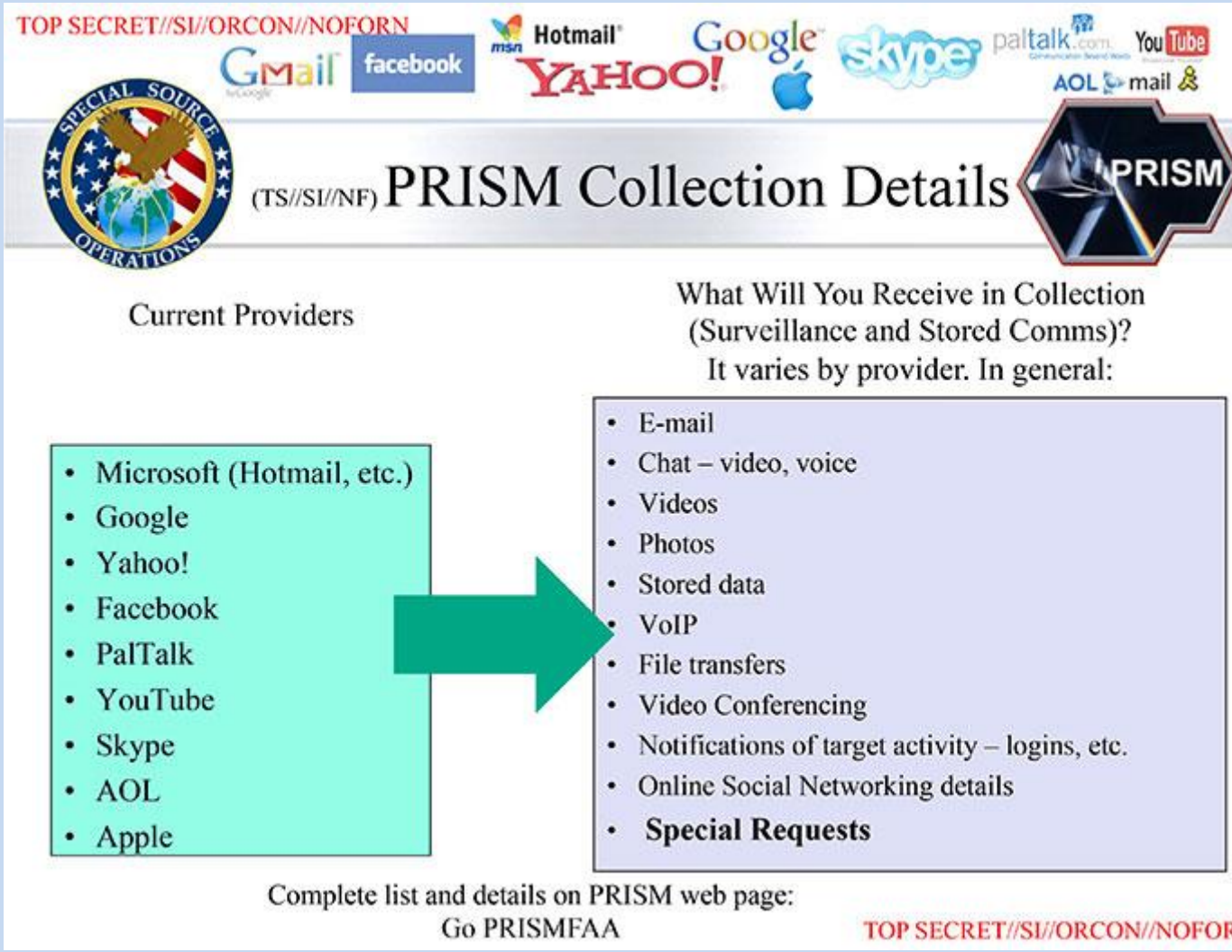
Según los documentos de Snowden, existen 2 programas principales para recoger información de Internet: PRISM y MUSCULAR.

Aunque los objetivos de ambos programas son similares, el funcionamiento de ambos es muy diferente. Así que empecemos por el principio.

¿Qué es PRISM?

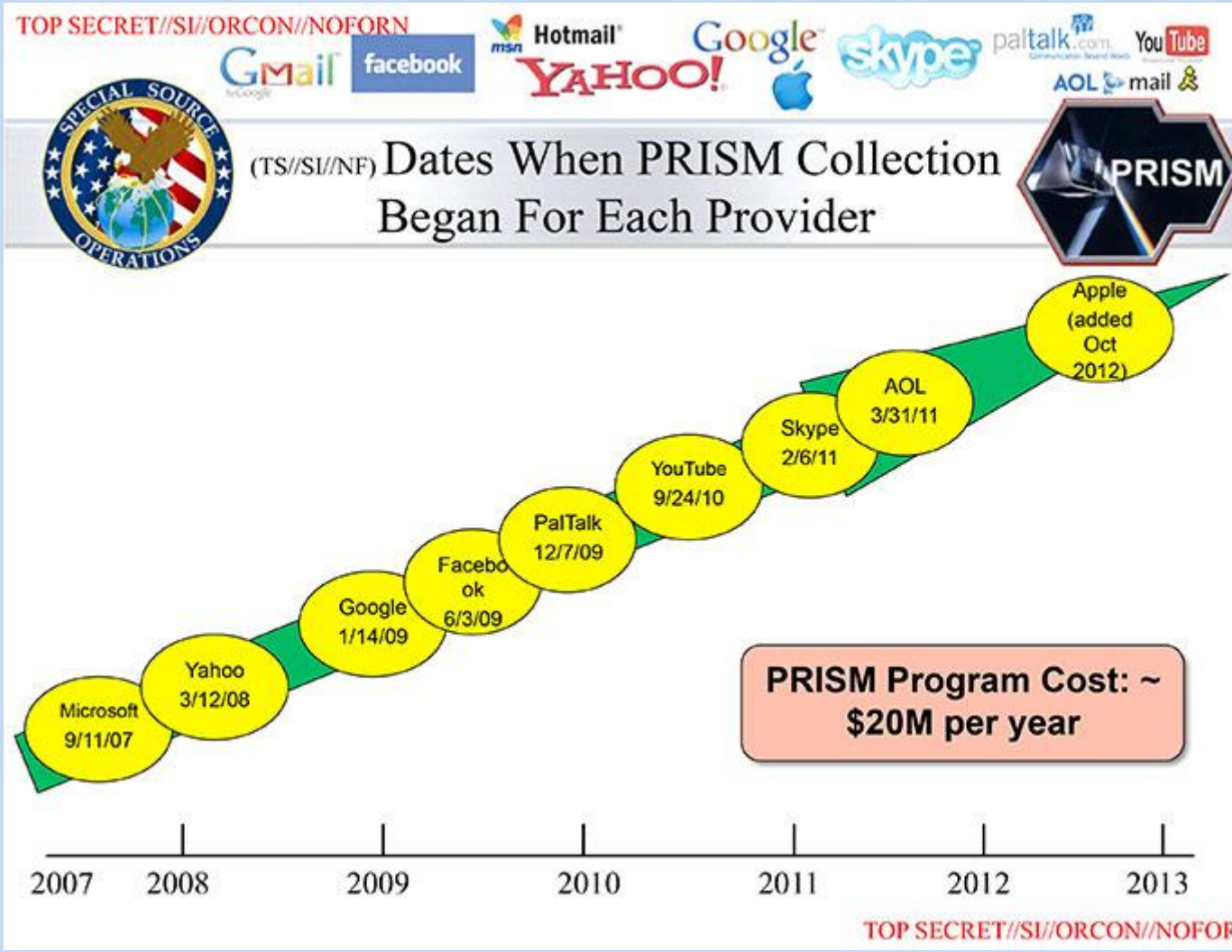
PRISM es un programa de recolección de datos que realiza la NSA con la colaboración directa de las grandes compañías de Internet.

En este documento "Top Secret" desvelado por Snowden aparecen las compañías que colaboraban en PRISM. Están todas las importantes: Microsoft, Google, Yahoo, Facebook, Skype, Apple, etc.



Crédito de la imagen: The Washington Post

En este otro documento, la NSA detalla el año en el que esas compañías empezaron a colaborar en PRISM:



Crédito de la imagen: The Washington Post

¿Cómo accede la NSA a los datos a través de PRISM?

PRISM recolecta datos de 2 maneras: una "semi-legal" y otra "completamente ilegal".

PRISM "semi-legal"

El gobierno norteamericano, en principio, no puede espiar a sus ciudadanos. La Cuarta Enmienda a la Constitución estadounidense establece que el Gobierno necesita una orden judicial para investigar a un ciudadano.

Pero conseguir una orden judicial no resulta ningún problema para la NSA. Las obtiene a través de un tribunal secreto -pero legal- llamado FISC (Foreign Intelligence Survelliance Court). Este tribunal sólo admite al abogado que representa al Gobierno y nunca publica sus decisiones.

Desde el año 2003, los senadores de EEUU se quejan de que "no tienen ni idea de cómo funciona el tribunal porque sus procedimientos legales son también secretos para ellos".

En la práctica, esta corte es una triquiñuela legal para circunvalar la cuarta enmienda. Para que os hagáis una idea: el año pasado, la NSA y el FBI solicitaron 1.800 órdenes de investigación. El 98.9% fueron aprobadas por el tribunal.

Una vez la NSA obtiene su orden judicial, las compañías de Internet están obligadas a entregar los datos.

Ah, y por cierto, si no eres ciudadano norteamericano, no estás protegido por la cuarta enmienda.

PRISM "completamente ilegal"

Además de la triquiñuela legal anterior, los documentos de Snowden desvelan otra faceta de PRISM completamente ilegal (sin orden judicial ninguna) y que se realiza con la completa colaboración de las compañías de Internet.

Para entender cómo funciona es interesante analizar las palabras del representante de Facebook cuando se filtraron los primeros documentos:

"Cuando el Gobierno pide a Facebook datos sobre individuos, nosotros sólo entregamos los estrictamente requeridos por la

ley" [lo que hemos hablado antes del PRISM semi-legal]. "Nunca permitimos un acceso directo a nuestros servidores".

Atención a la última frase. Los periodistas de The Washington Post, estudiando otros documentos de Snowden publicados semanas después, encontraron la trampa lingüística que esconde.

En truco era el siguiente: en efecto, las compañías "no permitían un acceso directo" a sus servidores. Pero lo que hacían era copiar datos de sus servidores a otros servidores (que técnicamente no eran suyos aunque estuviesen dentro de sus instalaciones) a los que sí tenía acceso la NSA. ¡Toma malabarismo lingüístico con la expresión "acceso directo"!

Hasta aquí hemos hablado de PRISM. Ahora vamos a ver otro programa que utiliza la NSA para acceder a nuestros datos (y en particular a Gmail) y que se llama MUSCULAR.

MUSCULAR o cómo acceder al Gmail de manera sencilla

Seguramente os habréis dado cuenta que cuando os conectáis a Gmail, en vuestra barra del navegador aparece "httpS://" en vez de "http://" (diferencia en la letra "S"). Básicamente, lo que esto quiere decir es que la conexión entre vuestro ordenador y el servidor de Google está encriptada con el protocolo seguridad SSL/TSL.

Si alguien "pinchase el cable" que va desde vuestro ordenador hasta Google, no podría leer el email que acabáis de enviar porque la información viaja encriptada.

Evidentemente, Google no está formado por un sólo servidor. Cuando os conectáis a Google, en realidad os estáis conectando al servidor que hace de "puerta de entrada" de Google.

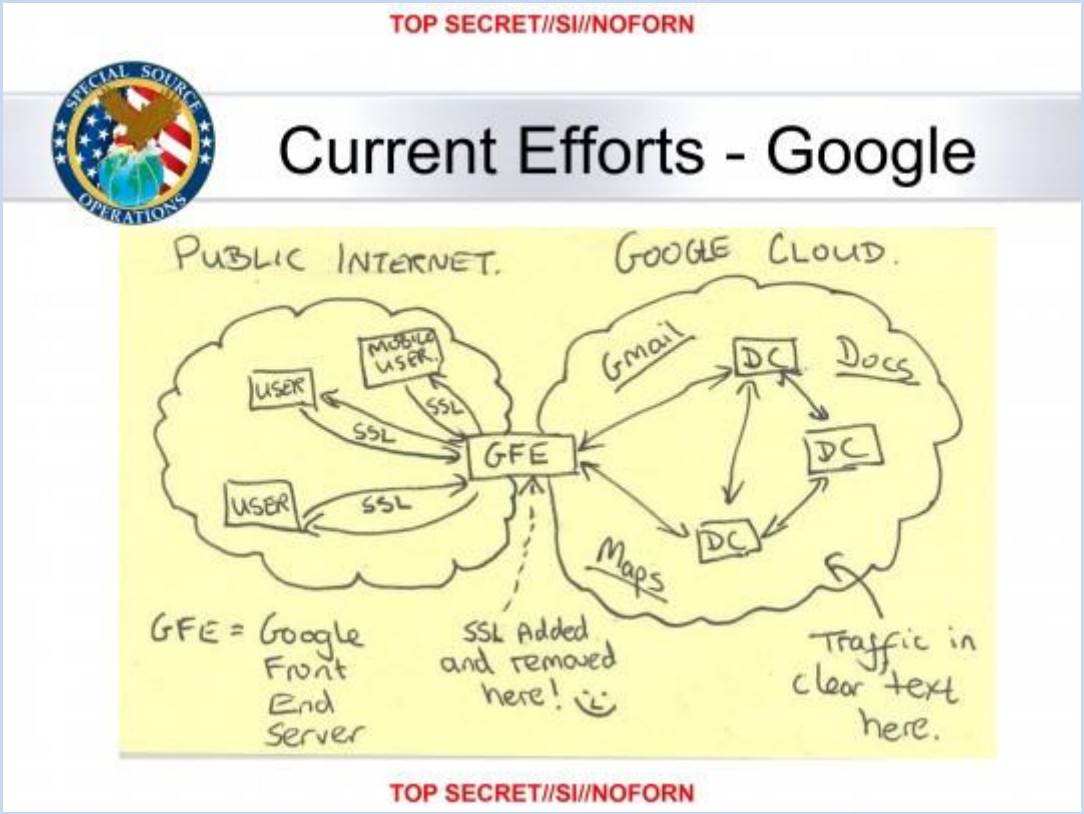
La conexión entre vuestro ordenador y "la puerta de entrada" de Google es segura.

Una vez vuestro email llega a Google, la compañía los copia en muchos servidores a la vez. Así, si por ejemplo, se cae uno de sus centros de datos, vosotros podéis seguir accediendo a Gmail.

Problema: las conexiones entre los centros de datos de Google no están encriptadas.

MUSCULAR es el programa de la NSA que pincha los cables entre los centros de datos de Google (o Yahoo) para leer los emails.

Quizás es más sencillo entenderlo con este otro documento de la NSA desvelado por Snowden:



Crédito de la imagen: The Washington Post

En la nubecita de la izquierda están las conexiones entre los usuarios y Google. Como véis las flechitas tienen escrito "SSL". Es decir, las conexiones son seguras.

En la nubecita de la derecha están las conexiones internas entre los servidores de Google. Ahí ya no tienen escrito "SSL". Es decir, las conexiones aquí no son seguras.

Entre las dos nubecitas, está el cuadrito "GFE", la puerta de entrada a Google. Aquí está indicado que el protocolo de seguridad "SSL" desaparece una vez entras en Google. ¡ATENCIÓN a la carita sonriente!

Como podéis ver en este mapa, Google tiene centros de datos repartidos por todo el mundo:

Crédito de la imagen: Google

Muchos de esos centros de datos están conectados entre sí por fibra óptica propia. Con MUSCULAR, la NSA pinchaba esos cables y tenía acceso a todos los datos que circulaban sin encriptar.

Todos estos detalles se los debemos a la enorme valentía de Edward Snowden y al trabajo de análisis que han realizado durante meses los compañeros de The Guardian yThe Washington Post.