¿QUIS CUSTODIET IPSOS CUSTODES?
¿QUIEN VIGILA A LOS VIGILANTES?

EL ROSTRO DE MATRIX

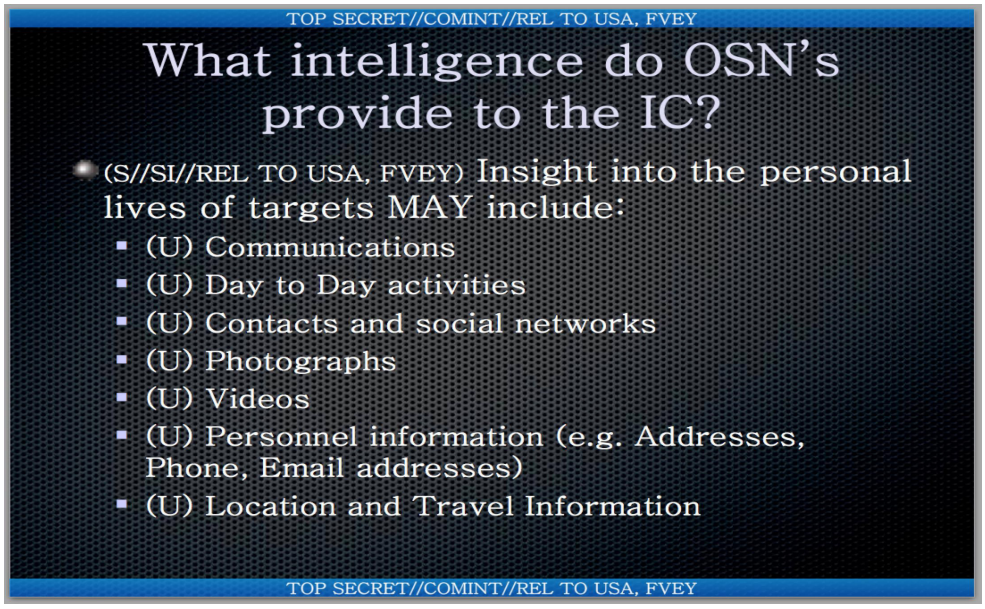
Parece adecuada la frase de Juvenal para nombrar a este documento, aterrador si miramos con frialdad las implicaciones que tienen las actividades de espionaje masivo y control que nos detalla; es estremecedor ver como los peores presagios hechos por los cypherpunks sobre internet en los 90 se han convertido en solidas realidades que proyectan sombras muy oscuras para los próximos años de existencia de la red, sus futuros desarrollos y asimismo el de la humanidad.
El usuario inconsciente de la red vive su vida digital en un **MATRIX** virtual, donde no se preocupa de nada mientras va sembrando pedacitos de su vida por toda la red, dejando constancia de que le gusta o no, a quien admira y a quien no, a quien votara y porque, que compra y donde lo hace, quien es su banco, que compra, a quien escribe y quien le escribe a el, sus gustos sexuales o deportivos... esta despreocupación solo posible en un “mundo feliz” es la norma, bien potenciada por autoridades de cualquier escalon jerarquico de la piramide que animan este tipo de conducta con evidentes fines de vigilancia y control.
Ahora bien, no vivimos en un mundo feliz, MATRIX es real, ese mundo soñado, no existe, lo real es el mundo de los metadatos, el espionaje masivo, las formulas de chantaje, la recopilación masiva de todo tipo de datos con fines comerciales por parte de grandes compañías, su activa cooperación con ejércitos y estados con fines de espionaje o guerra cibernética, ese es el verdadero rostro del mundo digital, oculto por Google, Facebook, Skype etc, etc.. el de enloquecidos pretorianos que han decidido criminalizar a todo aquel que use un ordenador o un telefono movil y escudandose en la prevencion de un posible terror, considerarle culpable y someterle a un control y vigilancia exhaustivos, estos pretorianos dan forma al MATRIX real, convirtiendo nuestra vida, sin muchos saberlo en algo muy parecido a la del Kafkiano Joseph K .

Métodos

Verdaderamente cuando E. Snowden desnudó a la NSA con sus revelaciones en

2013, no hizo nada mas que poner a la vista del publico y confirmar los temores y preocupaciones que gran parte de los usuarios conscientes de internet tenían, esto es la existencia de grandes redes de espionaje digital a nivel masivo, fomentadas y mantenidas por estados supuestamente "democráticos". Estos estados, sin ningún rubor consideran "culpables" a todos los usuarios de la red y los someten a una vigilancia y un control permanente e intensivo. Una tarea de espionaje que se extiende a toda la vida digital de ciudadanos de países de todo el mundo, criminalizados por los custodios de organizaciones de inteligencia estatales con objetivos imperialistas, empresariales y de clase.

Las revelaciones de Snowden y sus documentos nos hablan de varios niveles de actuación masiva conducida no solo por los órganos de seguridad de los USA, (la NSA), sino de los de países acólitos, como puede ser UK, Australia o Nueva Zelanda.
El acceso a los datos se produce con diferentes técnicas que abarcan varios estadios del movimiento, tratamiento de la información y su transporte por la red, esto es cubierto legalmente por una enmienda del acta [1]FISA del año 2008 , que fue renovada en Diciembre del 2012. La recopilación masiva de datos se produce con la cooperación de las grandes multinacionales o trust de la información y redes sociales, Facebook, Google, Microsoft, Yahoo, Skype, Apple etc, etc, por supuesto negada categóricamente en un principio y reconocida después con la boca pequeña, aludiendo a las obligaciones impuestas por las leyes. Asimismo se accede a información en bruto pinchando los cables transoceánicos de fibra óptica. Los sistemas abarcan la telefonía móvil, fija y todo tipo de movimiento digital y las cantidades de información generada son tan astronómicas que solo las pueden mantener para su estudio durante varios días(aquí hay contradicción en el n. de días según las fuentes).



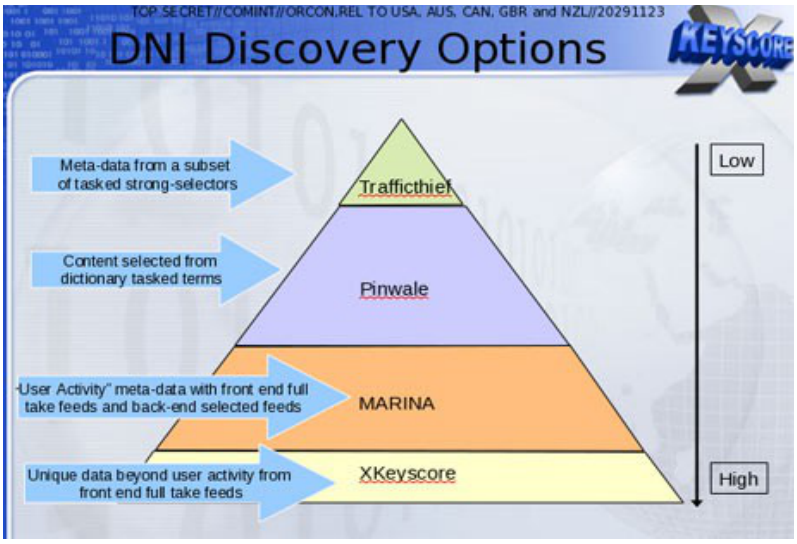
Para ello, en la actualidad la NSA cuenta con una plantilla cercana a los 40.000 empleados, un presupuesto reconocido de 10.800 millones de dólares y cerca de 500 programas –operativos o en fase de desarrollo– destinados a la vigilancia y el espionaje tecnológicos. Asimismo para estas operaciónes masivas de espionaje que abarcan a centenares de millones de personas la NSA se ha apoyado en compañias americanas L-3 Communications12, Tasc, Cytech

Services, SAIC, Raytheon o BAE Systems, que han producido maravillas de software como podremos comprobar en las siguientes paginas. Este informe no esta basado solo en los 20.000 documentos proporcionados por Snowden, sino en estudios internacionales, filtraciones interesadas o no y en documentos de Wikileaks, creando un cuadro bastante completo de estas actividades de espionaje masivo y metodico planteado por la NSA y el USCYBERCOM en el marco del UKUSA como una ciberguerra contra la humanidad en su conjunto, ya que todos somos su objetivo.
Vamos a comenzar analizando las herramientas que utilizan en su tarea de espionaje masivo contra “terroristas” como ud., su hija de 10 años o su compañero de trabajo....
Empezaremos con una de las estrellas: **Xkeyscore.**

El propósito del programa es permitir a los analistas buscar metadatos, contenidos de correos electrónicos, historiales de navegación, nombres, números de teléfono, direcciones IP, idioma y ciertas palabras claves de cualquier actividad que se haya realizado en Internet y funciona en el marco de UKUSA, una alianza de naciones de habla inglesa formada en 1946, con el propósito de recolectar información de inteligencia y formado por USA, UK, Canada, Australia y Nueva Zelanda.

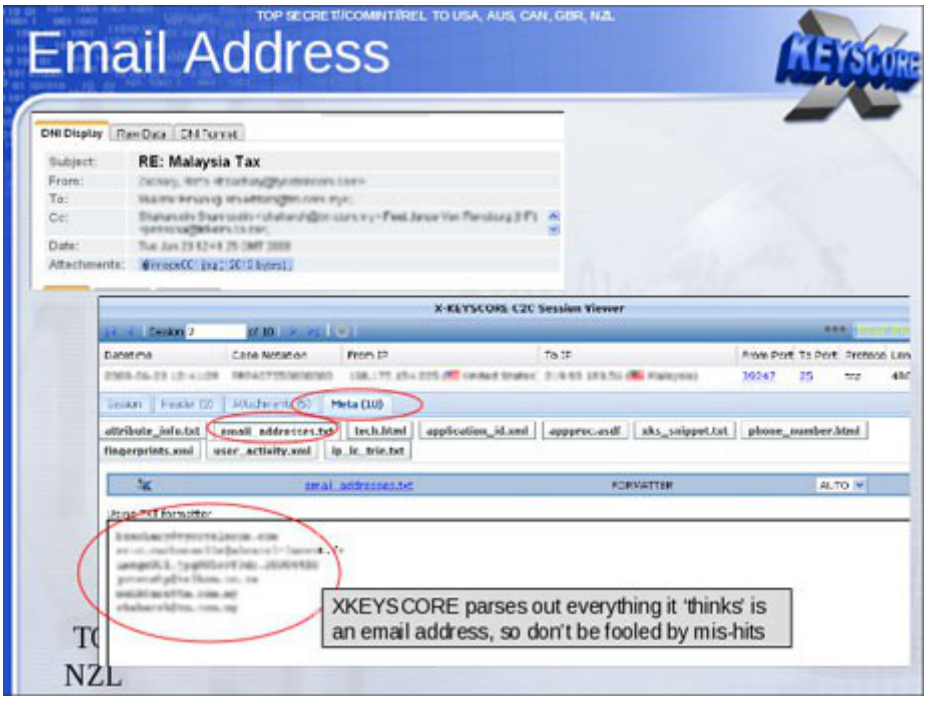
XKEYSCORE no recolecta los datos es una serie de interfaces de usuario con acceso a bases de datos, servidores y software que aunan ciertos tipos de metadatos que la NSA ha reunido ya mediante diferentes metodos , XKEYSCORE es una base mundial de esos metadatos. Estos datos son recopilados por una entidad denominada F6 y tambien FORNSAT y a veces con el acronimo SSO en los documentos de Snowden.

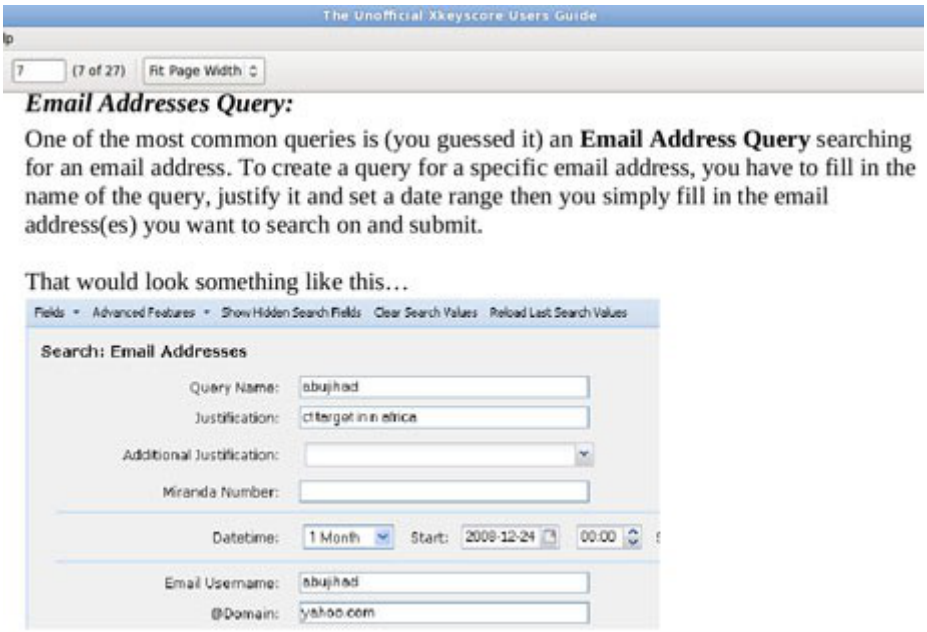
Capacidades de XKS



Como nos muestran los diagramas de presentacion del programa KEYSCORE es utilizado por todo el mundo los Metadatos de la Actividad de los usuarios se almacenan en la base de datos MARINA; el contenido leido y clasificado se retiene en la base de datos pinwale; para objetivos específicos y regulares, la base de datos TRAFFICTHIEF permite un analista tener un retrato muy claro y exacto de las actividades de Internet de cualquier persona en tiempo real o casi real, SI la NSA tiene los datos.
El programa abarca diferentes tipos de informacion proporcionada incidiendo sobre el protocolo HTTP.

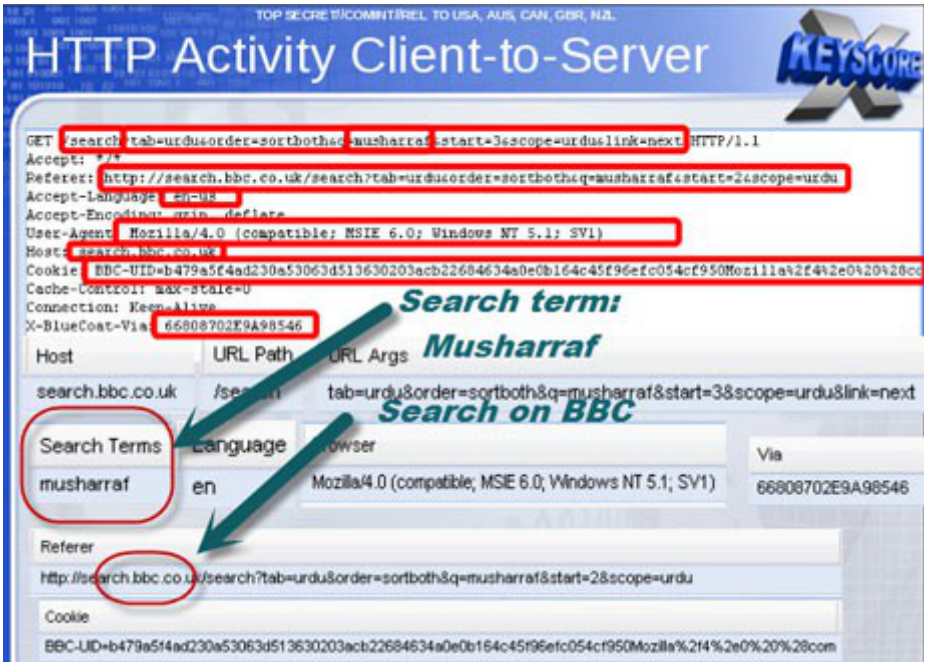
Busquedas en el correo electronico.





Como vemos refinando sus busqueda en varios campos del correo electronico los analistas pueden llegar a conclusiones no solo estudiando datos en bruto, como citas, o numeros de telefono, nombres u horarios, sino con idiomas utilizados, toponimias o argots locales.

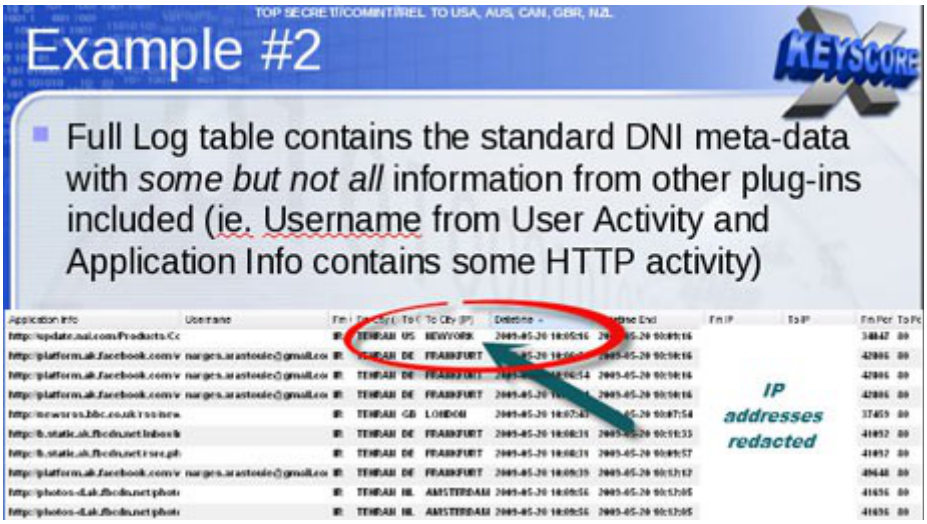
Busqueda por la actividad del protocolo HTTP.



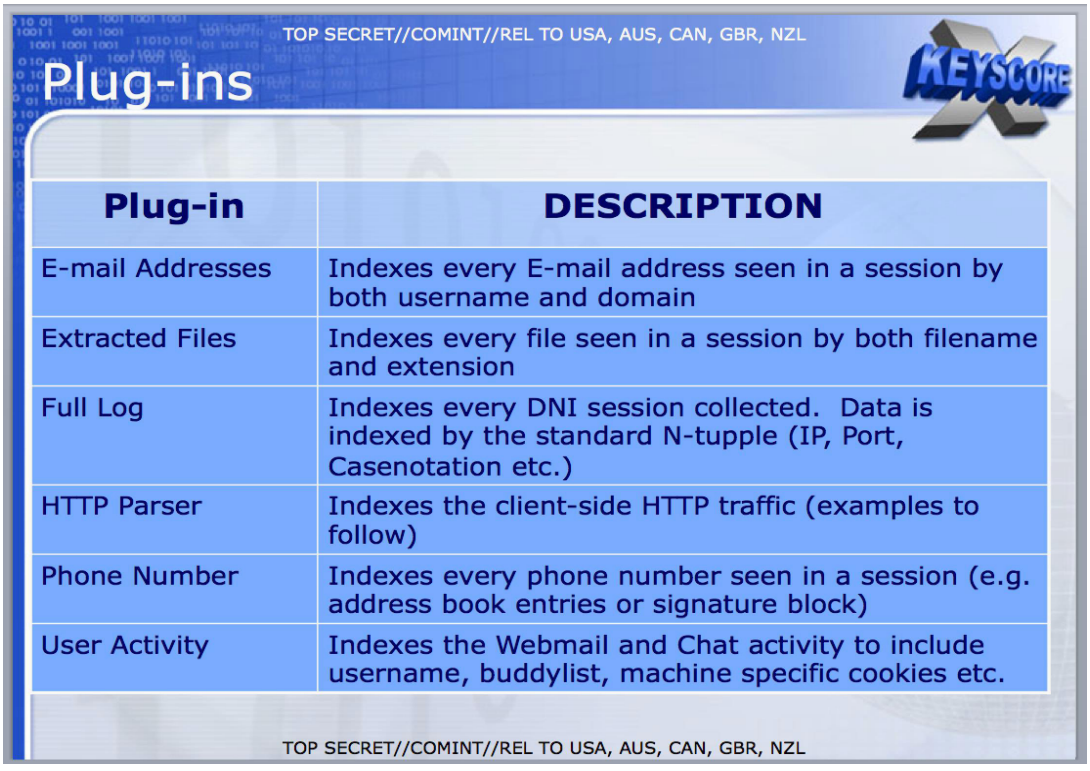
1. If you know the particular website the target visits. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.

Para realizar este tipo de operaciones se necesitan cantidades ingentes de datos que gracias a programas tan eficientes como XKS dan una capacidad de control sobre nuestras vidas a estos grupos de poder que supera con mucho las proyecciones mas pesimistas hechas en los tiempòs de Echelon. Sigamos un poco mas con XKS antes de pasar a otras herramientas tanto o mas utiles que este.

Los metadatos, la base del sistema de espionaje masivo.



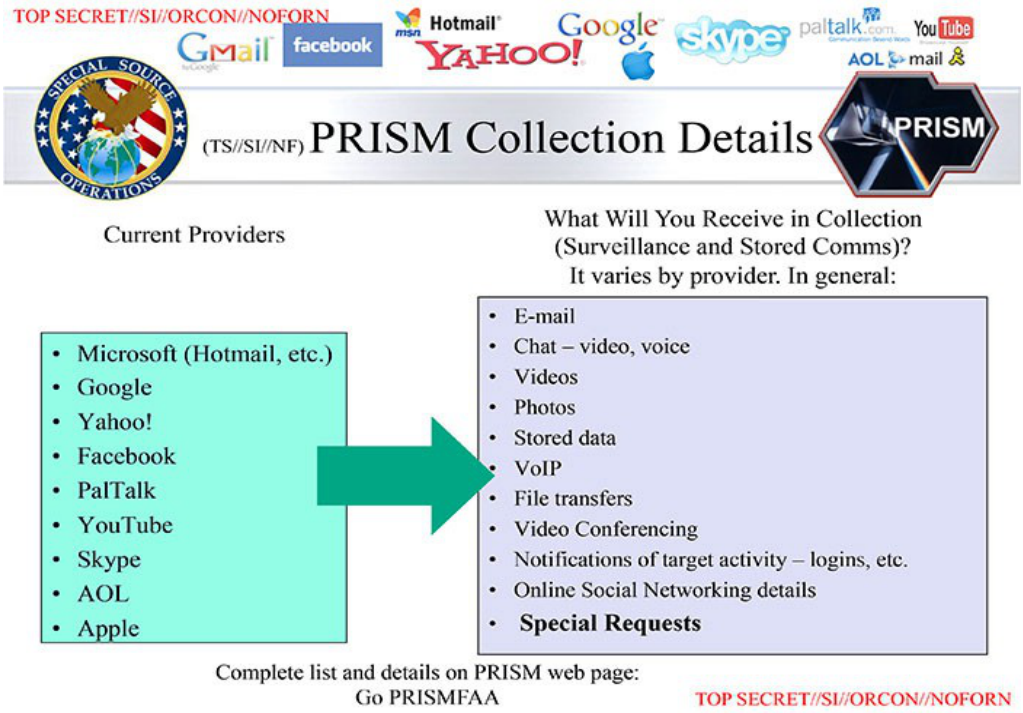
Los plugins del programa.



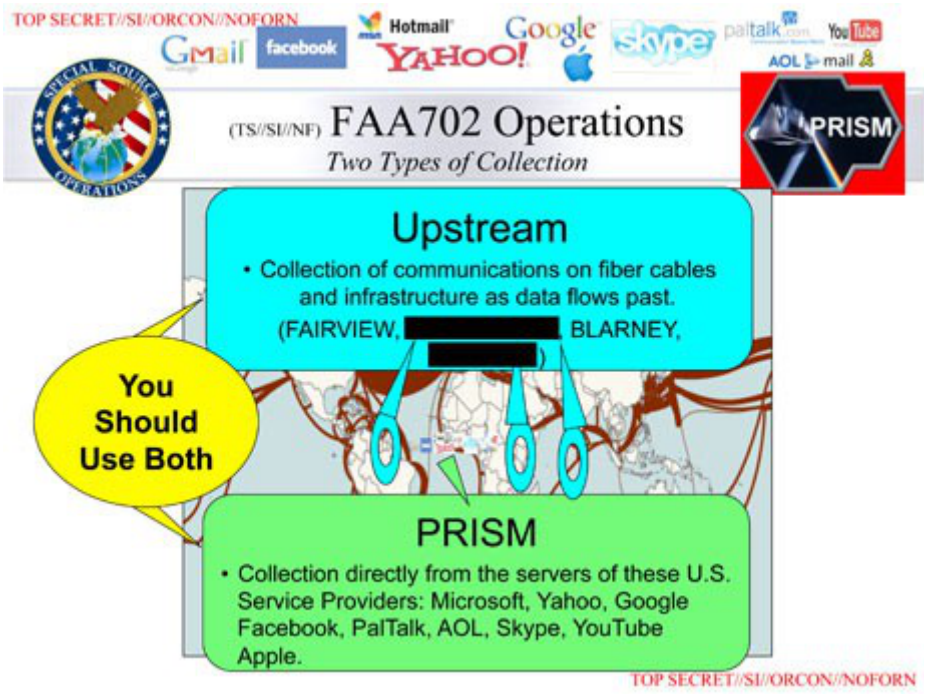
Si nos han sorprendido las capacidades de Xkeyscore, capaz de espiar nuestras actividades en las redes sociales, nuestros correos electronicos, nuestros historiales de navegacion o cualquier formulario rellenado donde en cualquier sitio web, a ver hasta donde llega nuestro asombro con las de otra de las revelaciones de E. Snowden, **PRISM**.

PRISM, tambien llamado US-984XN esta destinado a recolectar datos de personas que vivan fuera de los EUA y fue creado en el año 2007 bajo la presidencia de baby Bush, vamos a ver como funciona y de donde salen sus fuentes de datos, algo que provoco un pequeño escandalo el año 2013 cuando Snowden puso a disposicion de la sociedad a traves del periodico The Guardian estos estupendos diagramas secretos de la NSA.

Fuentes de PRISM.

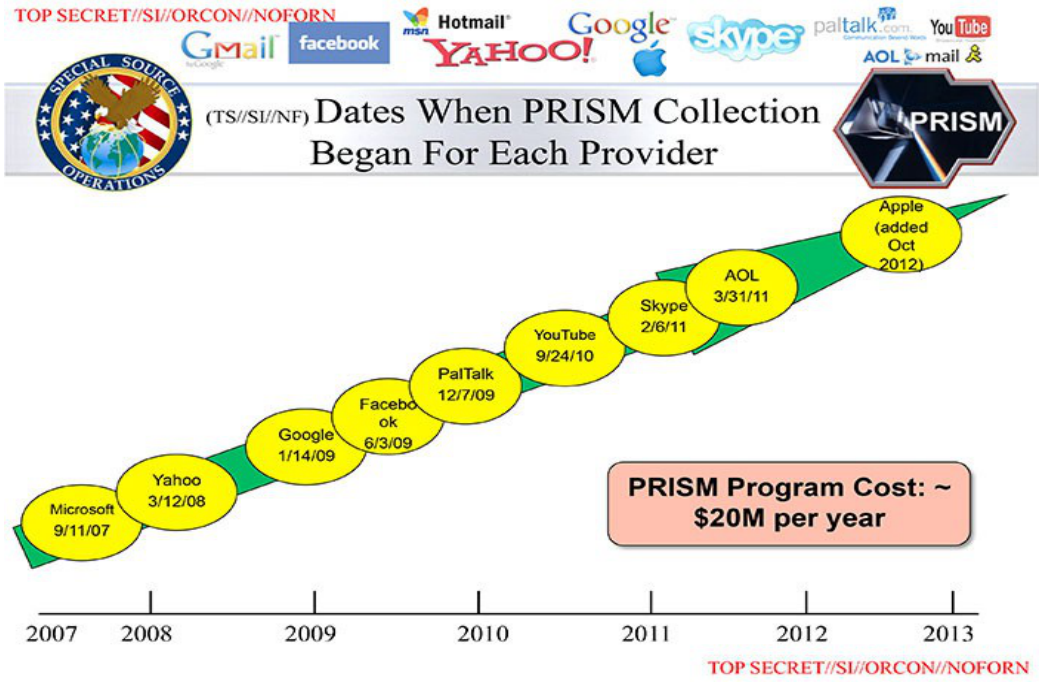


El diagrama completo de las fuentes de PRISM.

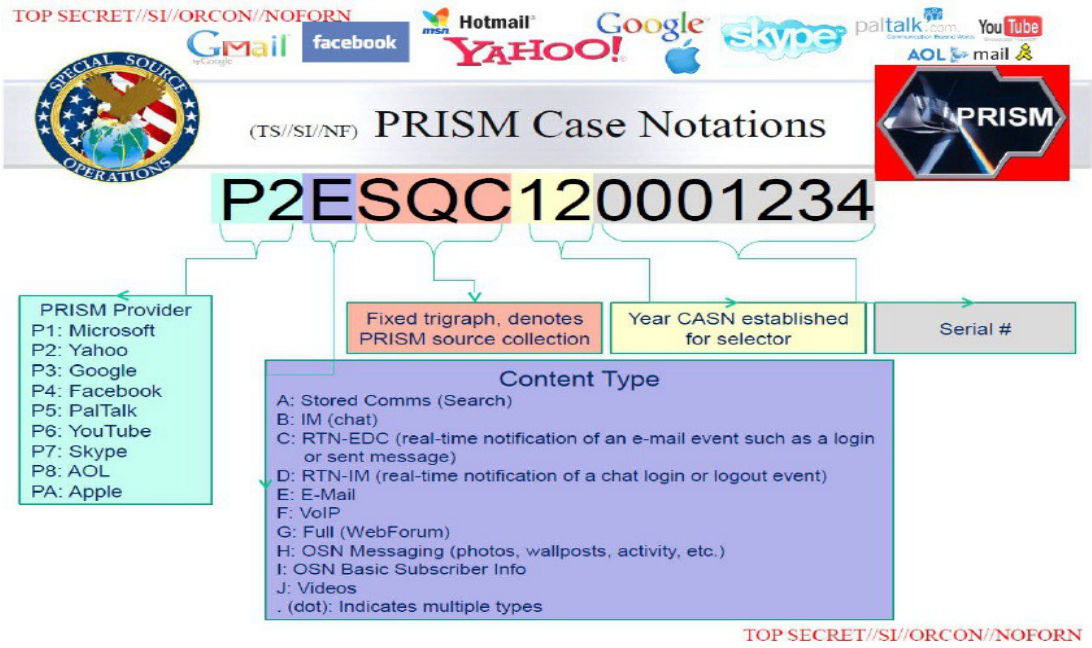


Los datos que supuestamente la NSA es capaz de obtener gracias a PRISM incluyen correos electrónicos, vídeos, chat de voz, fotos, direcciones IP, notificaciones de inicio de sesión, transferencia de archivos y detalles sobre perfiles en redes sociales.

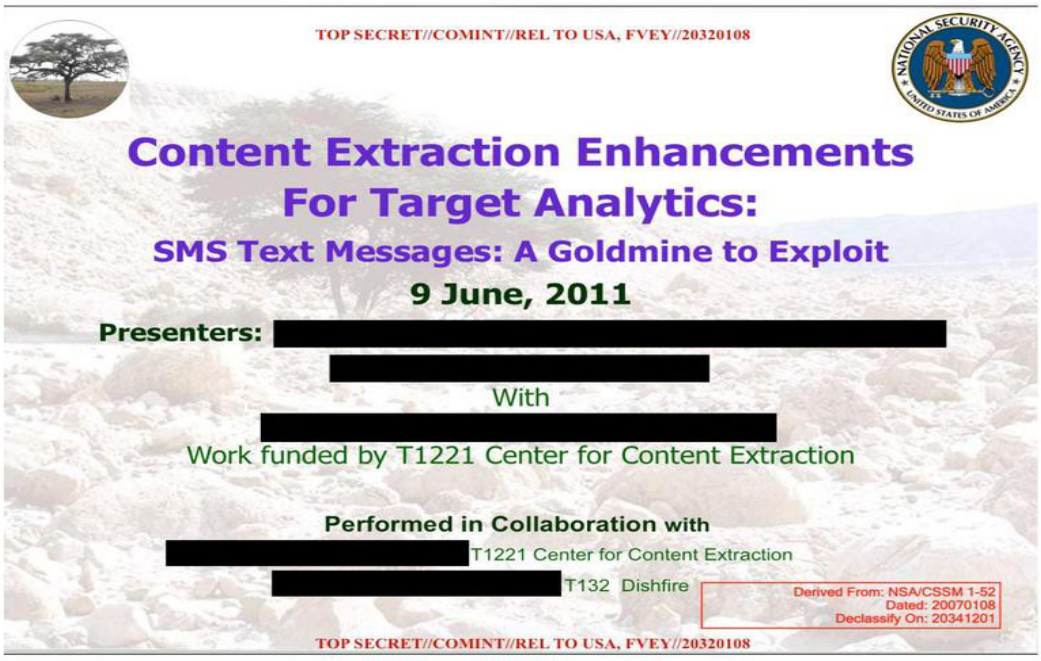
Fechas de comienzo de colaboracion con PRISM.



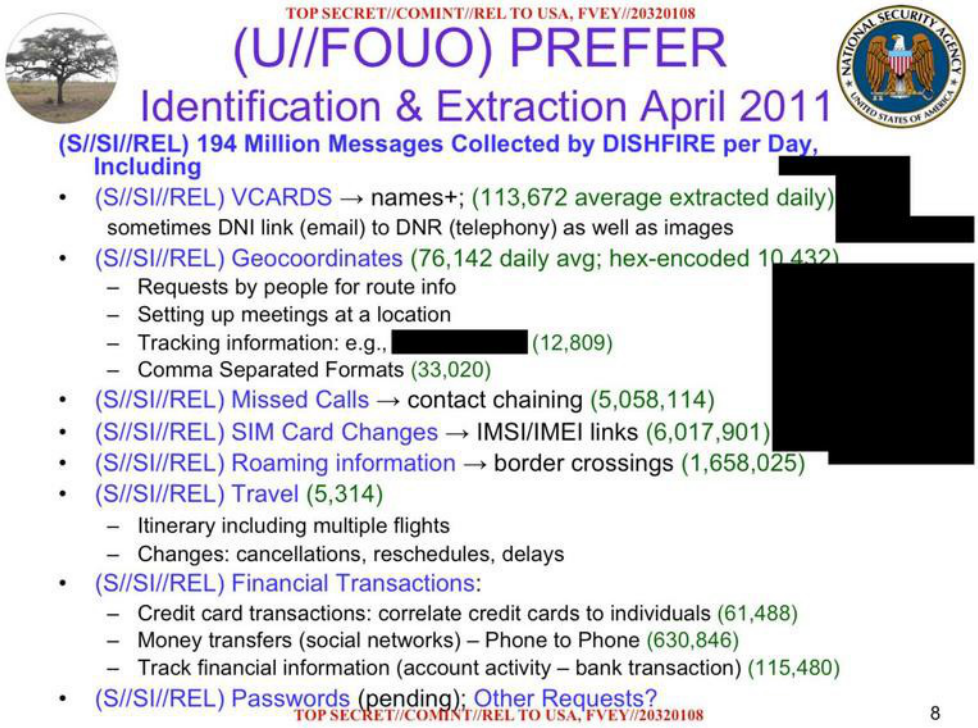
Nomenclatura de casos para PRISM.



Como podemos comprobar la colaboración de los grandes trust de internet es necesaria para el buen funcionamiento de **PRISM** y de toda la cadena de programas que se utilizan para el espionaje masivo, tanto de metadatos como de n. de teléfono e-mails, etc, etc.
Abundar mas sobre **PRISM**, no tiene objeto así que vamos a continuar en otra dirección lo que haremos con **DISHFIRE** un software que recopila sms.



Realmente no parece nada preocupante,¿ quien usa hoy en día el sms?, sin embargo el angelito es mas peligroso de lo que parece, el titulo de su presentación es realmente muy clarificador; una mina de oro que explotar
Aquí vemos la peligrosidad del ingenio.



'DISHFIRE' recopila "prácticamente todo lo que puede". ¿Qué quiere decir esto? Que básicamente se almacenan los mensajes sin criterio ninguno, entre la información que obtiene la NSA de estos mensajes, como queda claro en la presentacion, está la siguiente: datos de avisos de llamadas perdidas para analizar la red de contactos de cada número, datos de transacciones financieras (pagos con tarjetas asociados a números de teléfono a los que se envían avisos, informacion de roamming, llamadas perdidas, localizacion geografica, información automática que se envía a los teléfonos de los usuarios (por ejemplo, cambios en el horario de un vuelo, cambios de contraseña, etc.)
Los datos recopilados por **'DISHFIRE'** son procesados por "prefer", que los filtra y son almacenados, puede que durante años.
Evidentemente esto debe darnos que pensar, dada la cantidad de informacion recibida, pero vamos a seguir a buen ritmo, nos quedan algunas cosas que ver....

TURMOIL, TURBINE, FOXACID, QUANTUM

Entre los planes desquiciados de los custodios dedicados a la inteligencia/contrainteligencia en los USA y los miembros del UKUSA en general nos encontramos con planes para infectar docenas de millones de ordenadores con malware a traves del proyecto TURBINE que es parte de la colección de sistemas que incluye el sistema de vigilancia de la red TURMOIL que a su vez trabaja con XKeyscore , la infeccion se realizaria a traves de falsos servidores...pero TURBINE no es la unica plataforma de hackeo diseñada por la NSA ahi esta la arquitectura FOXACID una colección de servidores usados para infectar con software malicioso
Para engañar a los objetivos para que visiten un servidor FoxAcid, la NSA se basa en sus alianzas secretas con las empresas de telecomunicaciones de Estados Unidos. Como parte del sistema TURMOIL, la NSA pone servidores secretos, con nombre en código QUANTUM, en lugares clave de la red troncal

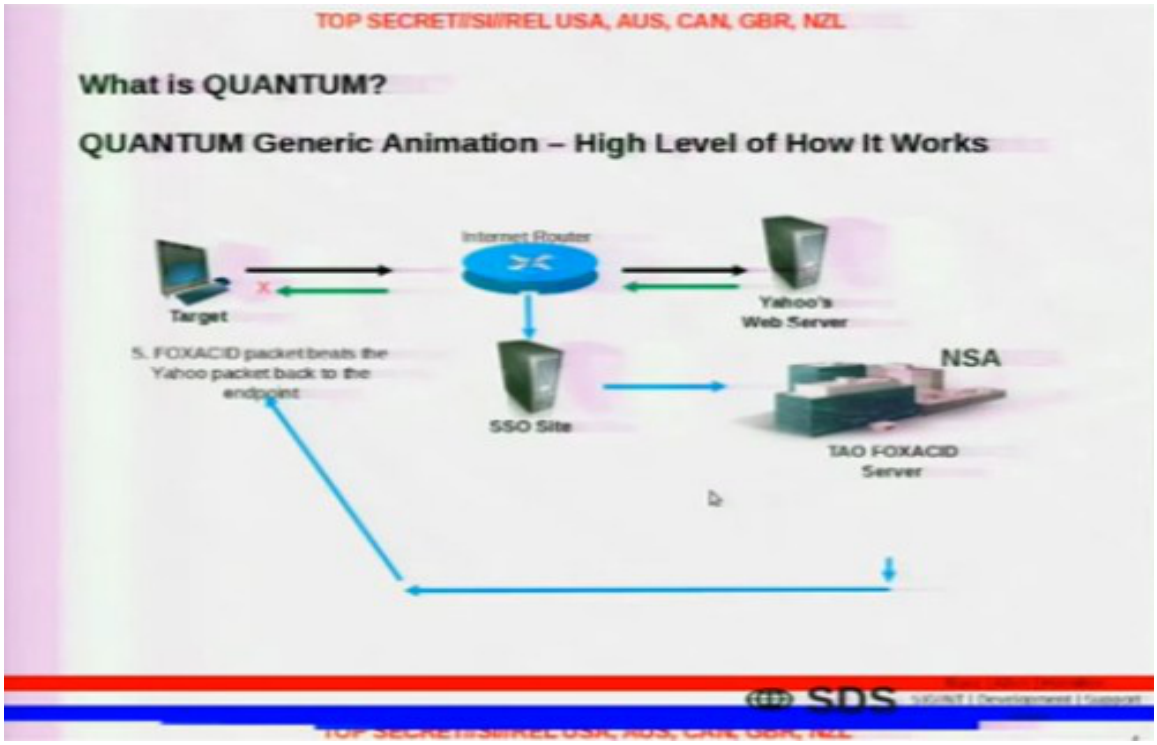
de Internet. Esta colocación asegura que puedan reaccionar más rápido que otros sitios web. Mediante la explotación de esa diferencia de velocidad, estos servidores pueden suplantar un sitio web que desea visitar “el objetivo” antes de que el sitio web legítimo puede responder, engañando con ello el navegador del destino para visitar a un servidor Foxacid . Las Plataformas FOXACID y Turbine proporcionan al operador de la NSA un menú en el que puede seleccionar múltiples opciones de ataque, de tal modo que los atacantes puedan elegir el ataque adecuado. Ambas arquitecturas están bajo el control de las operaciones del Tailored Access Operation (TAO), una unidad de hacking secreta de la NSA.

La plataforma Turbine descrita por la NSA en un documento secreto.

(TS//SI//REL) TURBINE manages the active implants that make up the Active SIGINT system.
Active SIGINT offers a more **aggressive** approach to SIGINT.
We retrieve data through intervention in our targets' computers or network devices. Extract data from machine. This is: Tailored Access Operations!

One of the greatest challenges for Active SIGINT/attack is **scale**. Human "drivers" limit ability for large-scale exploitation (humans tend to operate within their own environment, not taking into account the bigger picture)
The TURBINE infrastructure will allow the current implant network to scale to large size (millions of implants) by creating a system that does **automated control implants by groups** instead of individually.
Expert System (resource and operations manager) is like the **brain** it manages the applications and functions of implants.
Decides which tools should be provided to a given implant and executes the rules on how it should be used
Decisions of the expert system are passed to the **command and control modules**, which execute the decision against the appropriate set of implants.
Diode is a device that allows connectivity from the high side to the low side network without human intervention.

Algunos de los componentes de QUANTUM



TOP SECRET//COMINT//REL USA, FVEY

(U) There is More Than One Way to QUANTUM

TS//SI//REL

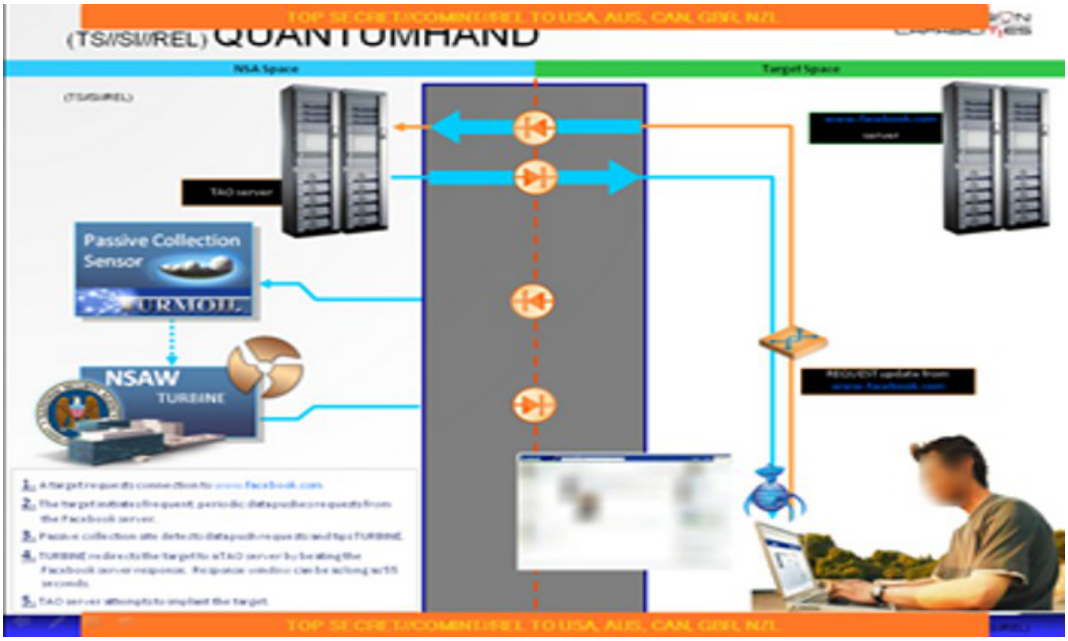
Name	Description	Inception Date	Status	Operational Success
CNE				
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**
CNA				
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live Tested	**N/A**
CND				
QUANTUMSMACKDOWN	Prevents target from downloading implants to DoD computers while capturing malicious payload for analysis.	Oct 2010	Live Tested	**N/A**

TS//SI//REL

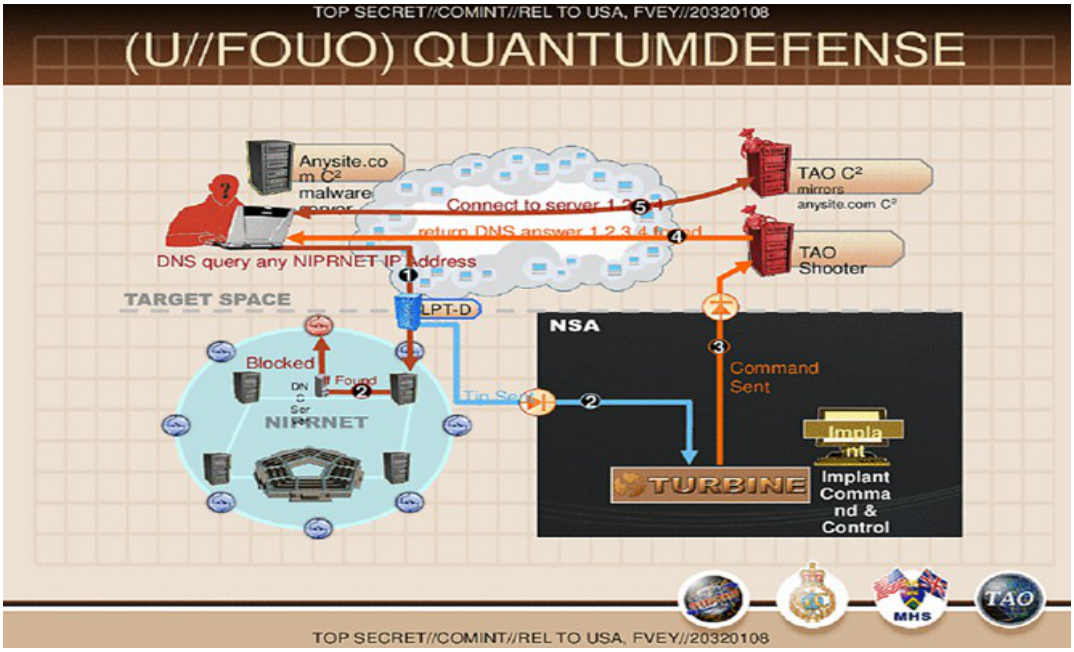
TOP SECRET//COMINT//REL USA, FVEY 1

Fijarse en QUANTUMHAND

(TS//SI//NF) QUANTUMTHEORY (QT) is a set of CNO Man-on-the-Side capabilities that involve real-time responses to passive collection. After the recent TURMOIL upgrade at SSO's SARATOGA access, TAO operators were able to run QUANTUMHAND which exploits the computer of a target accessing his facebook account. Briefly, when quantum is tipped that a target is using Facebook, quantum pretends to be the Facebook server and sends a response to the target. This fake response contains a link to TAO's FOXACID server, which implants the target's computer. In just a week, nearly 100 "shots" have been fired on 14 targets using QUANTUM from over 1300 tips received from SARATOGA. More targets are being added. This collaboration between TD, SSG, TAO, and SSO is another successful example of the emerging emphasis on Endpoint-Midpoint Integration.



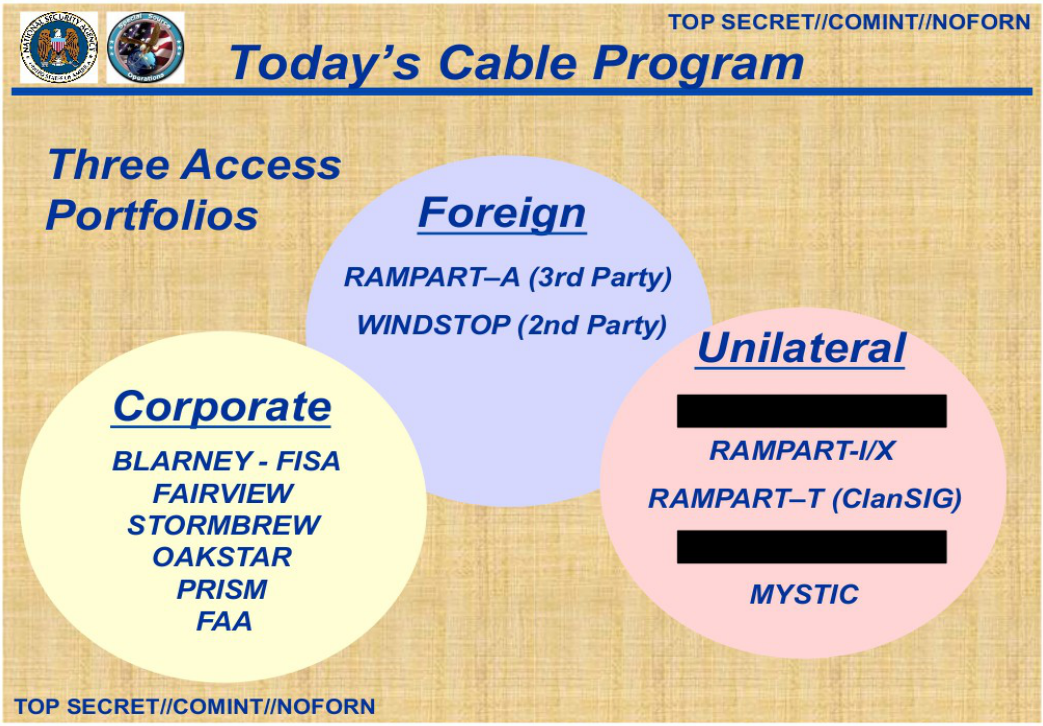
Como funciona el sistema.



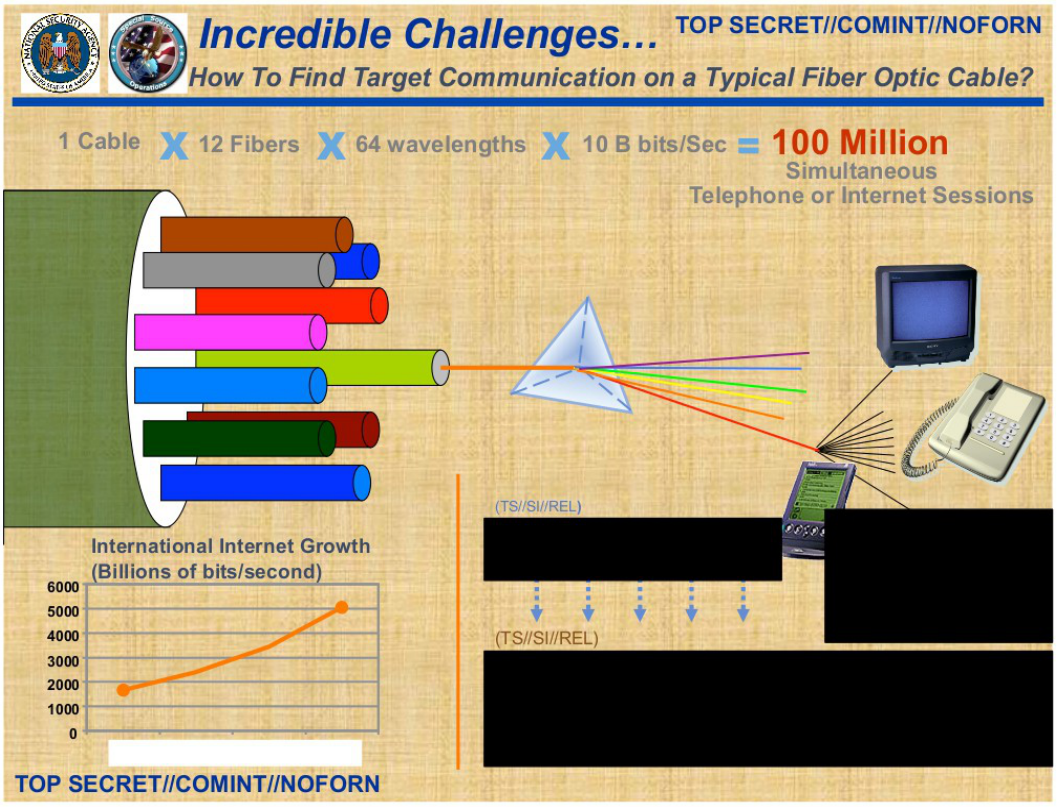
RAMPART

RAMPART, es un programa liderado por la NSA y compartido por varios estados vasallos de los USA, amen de los ya consabidos esbirros del UKUSA, RAMPART literalmente pincha los cables submarinos de fibra optica y lo graba todo.

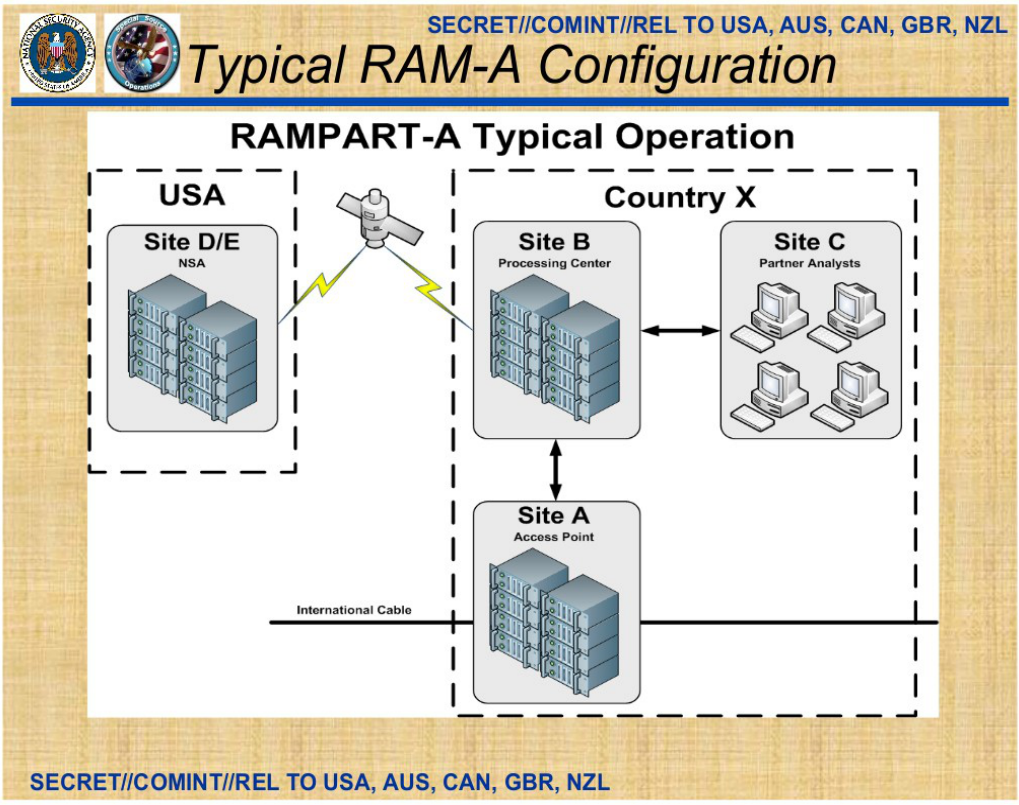
Aquí vemos la interrelacion de RAMPART con otros programas de la NSA



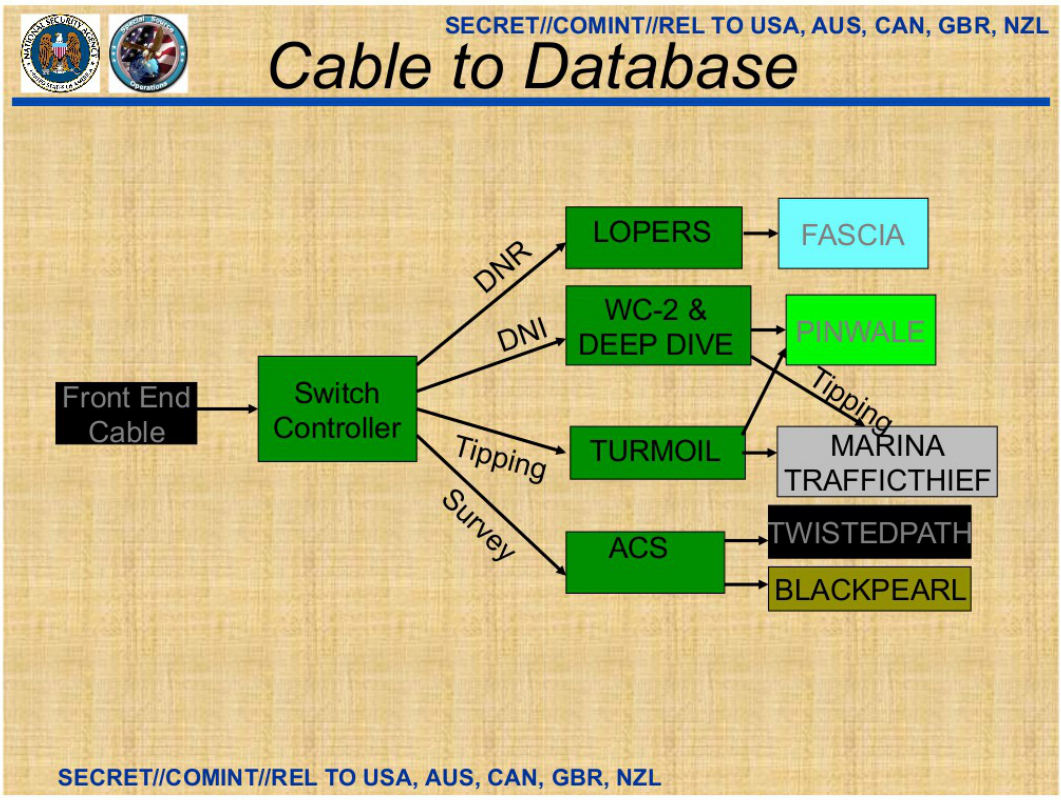
Las capacidades de RAMPART



Viaje de los datos robados por RAMPART



Destino final: las bases de datos de la NSA; MARINA, PINWALE etc, etc.



Los documentos uno tras otro nos muestran un espionaje indiscriminado a todos los ciudadanos sin ninguna distinción en absoluto y con una amoralidad que nos deja atónitos.
Podíamos seguir hablando de MYSTIC Y de RETRO, programas que según los documentos son capaces de grabar todas las conversación de un país durante un día... seguir con MUSCULAR o investigar los tratos de la NSA con proveedores de routers y otro hardware que es manipulado antes de llegar al destinatario, el programa BULLRUN que intenta romper los algoritmos de encriptacion y arrastrar a la industria del software a la creación de puertas traseras y toda una serie de programas de vigilancia masiva, pero seguir es baladí, estos documentos no dejan lugar a dudas sobre la realidad del espionaje masivo y a nivel mundial realizado por los órganos de seguridad e inteligencia de los USA en compañía de sus esbirros de menor calibre.
Sabemos cuando comenzó esta campaña mundial de espionaje masivo y sabemos que los encargados de llevarla a cabo viven en un mundo particular, diferente al de las personas decentes y normales, viven en 1984, están enfermos de fascismo y el espionaje al que intentan someter a todo aquel que se encuentre en el mundo digital nos habla claramente que no se están intentando defender de un supuesto enemigo terrorista, están intentando salvaguardar su régimen político y económico y quieren descubrir cualquier conato de respuesta tanto interior como exterior a su fascismo y a la locura asesina desencadenada por el capital neoliberal con los USA como espada

exterminadora y creadora del caos. El ciberespionaje y el control de las masas a través de su huella digital sin duda alguna ha sido convertido por estas organizaciones en uno de los perros de la guerra.

VIVIENDO EN MATRIX

El mundo en que vivimos es complejo, la humanidad nunca se había enfrentado a un problema semejante al que se nos plantea, el espionaje, la vigilancia y control a unos niveles inimaginables hace tan solo unos años y que los avances tecnológicos han puesto al alcance de la mano de estas agencias de información y seguridad, y con ello la pretensión de que desaparezca la privacidad en el mundo digital, pero definamos que queremos decir; **Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.** Esto dice la Real academia Española de la lengua sobre la palabra **PRIVACIDAD**, ***que se tiene derecho a proteger.***

La privacidad en el mundo digital.

La noción de privacidad en Europa es diferente a la que pueda haber en los USA un país en permanente estado de guerra, abanderado del capitalismo neoliberal y con durísimas leyes de excepción en vigor que permiten la detención de sus ciudadanos y de ciudadanos extranjeros sin informar a nadie de su detención y recluirlos de manera secreta sin juicio y hasta que algún juez de un tribunal secreto lo decida, en esencia y gracias a la ley Patriot([1]Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008) algo muy parecido a un régimen dictatorial e imperialista. Asimismo en la constitución americana no hay referencias a la privacidad Esto hace que los ciudadanos de los USA contemplen su privacidad de una manera diferente a la de otros países. El hecho es sin embargo que esta legislación y estas leyes estadounidenses se nos aplican a ciudadanos de otros países que nos encontramos indefensos legalmente ante estos atropellos.
Asimismo el Big data nos abruma con la publicidad no deseada y la venta de nuestros datos privados conseguidos de diferentes maneras, Google, Facebook, Skype y un largo etc, nos espían con tanta o mas intensidad que la NSA.
Y no nos olvidemos de la ciberdelincuencia que busca nuestros datos bancarios o de otro tipo para robarnos o chantajearnos.
Esta realidad nos plantea tres preguntas ¿Como debemos reaccionar? ¿Debemos defenderla? ¿Podemos hacer algo para defender nuestra intimidad y privacidad?

¿Como debemos reaccionar?

1. Al entender del autor de este documento, las pretensiones de organizaciones como la NSA de los USA, el FSB Ruso, el 国家安全部 (GuoJia anquan Bu) Chino u otros servicios de inteligencia y contraespionaje de controlar y espiar en forma masiva e indiscriminada a ciudadanos de todo el mundo son fruto de mentes enfermas y de un ansia de poder frenetico, malsano y malvado. No es de recibo que nos espíen, no es legal que lo hagan y no debemos aceptar de ninguna manera mansamente la situación mientras nos encogemos de hombros, cuando

estos individuos nos equiparan a terroristas o delincuentes comunes.

2. ¿Debemos defenderla?

Sin ninguna duda debemos poner todos los medios para ello, y el principal es nuestra actitud mental ante el atropello y el delito, dado que son delitos los que cometen estos organizaciones, empresas e individuos ¿Dejaríamos que alguien nos grabara en nuestros momentos mas íntimos? Seguro que no y para ello ponemos medios y protegemos nuestra intimidad, debemos darnos cuenta que aunque parezca inocente el mundo digital es un espejo del real y debemos actuar en consecuencia, no debemos dejar las puertas abiertas, no debemos mandar las cartas sin sobre, debemos tener cuidado con las cuentas bancarias, etc, etc,

3. ¿Podemos hacer algo para defender nuestra intimidad y privacidad?

Desde luego que podemos hacer algo por poner trabas a estas acciones delictivas, ilegales e inmorales. Debemos ser usuarios conscientes de nuestros derechos, tanto ante el big data que nos envuelve en MATRIX como al espionaje. Hay organizaciones repartidas por todo el mundo que luchan contra esta situación y que ponen todos sus medios, inteligencia y sinergias en extender los medios para que podamos defender nuestros derechos y provocar un cambio de actitud en el usuario. No soy ningún terrorista islámico sin embargo uso Tor habitualmente, como lo hacen los miembros de la NSA y el FSB, altos funcionarios, periodistas y un largo etc, cuando quieren tener privacidad en sus comunicaciones. No soy ningún terrorista islámico pero uso encriptacion en mis comunicaciones siempre que puedo, como hace cualquier usuario consciente o una persona que no desea que lean su correspondencia u documentos privados. No soy un terrorista islámico pero uso Tails cuando me apetece, para que no me llenen el navegador de publicidad no deseada, eso es mi derecho. Hay software, rutinas y costumbres que nos van a a ayudar a protegernos. Al final de este documento encontrara una serie de links de bastante utilidad.

En definitiva permitir que esta situación continúe en gran medida depende de nosotros, nuestras rutinas y nuestros deseos de proteger nuestra vida privada algo que es un derecho.

En este documento se ha hecho un resumen bastante sucinto principalmente de las actividades de la NSA y sus acólitos, se ha obviado el espionaje de las empresas y trust de la información y comunicación y el BIG DATA, algo que se hará en otro documento; dejo aquí algunos links a quien desee mejorar su privacidad y ciberseguridad.

https://www.torproject.org/ Pagina del proyecto Tor, anonimato en la navegacion.

https://www.securityinabox.org/es/seguridadportatil Gran cantidad de guias y utiles recursos para obtener privacidad en el pc y el **movi**l.

http://www.genbetadev.com/seguridad-informatica/manual-de-gpg-cifra-y-envia-datos-de-forma-segura Guia amable de Gpg en castellano.

http://www.genbetadev.com/seguridad-informatica/gpg-para-periodistas-por-cincinnatus-edward-snowden Un poco de historia....

http://www.kriptopolis.com/ Para los muy interesados.

https://tails.boum.org/ Un sistema que se lo pone muy dificil a los espias.

http://www.hacker10.com/internet-anonymity/list-of-the-best-tor-email-hidden-services/ Correo seguro.

Mialambre Octagon, 2014