OWASP
LATAM TOUR
2014

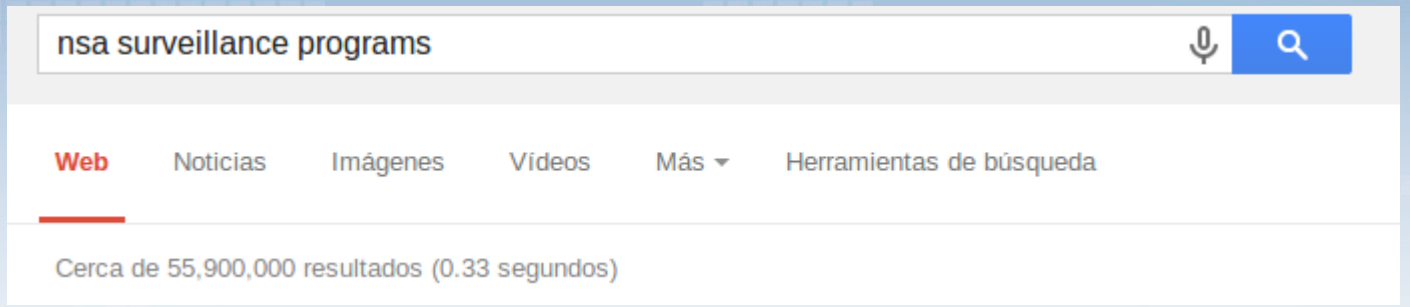
C0mun1c4nd0n0s 3n t13mp0s d3 NSA

OWASP
LATAM TOUR
2014

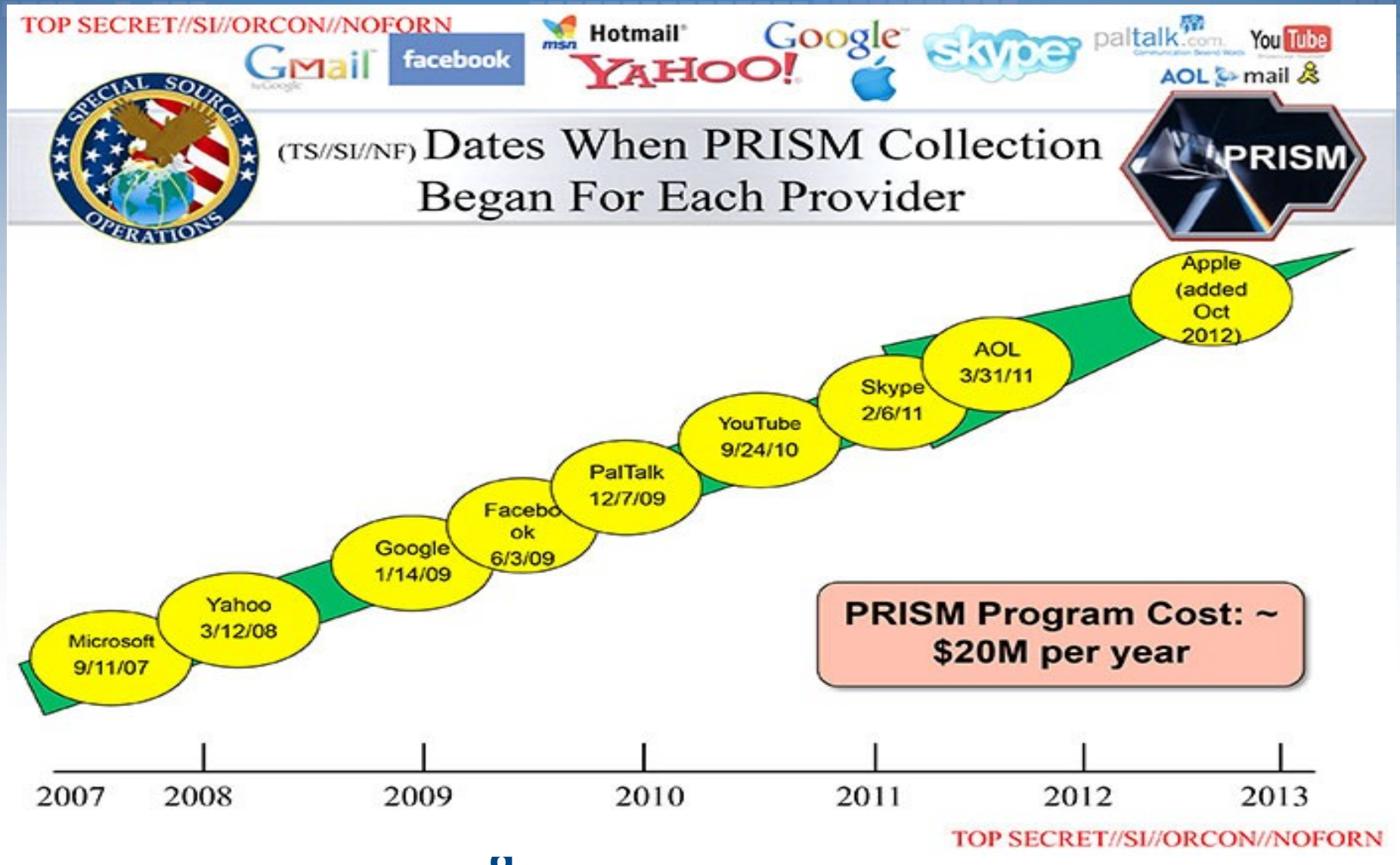
Camilo Galdos AkA Dedalo

Hacker, Security Researcher en algunos HoF, Running 2 Tor Relays - PHP, Python & Freedom Writter. CainaMrehpyC, **Paranoid** y No-Fear.

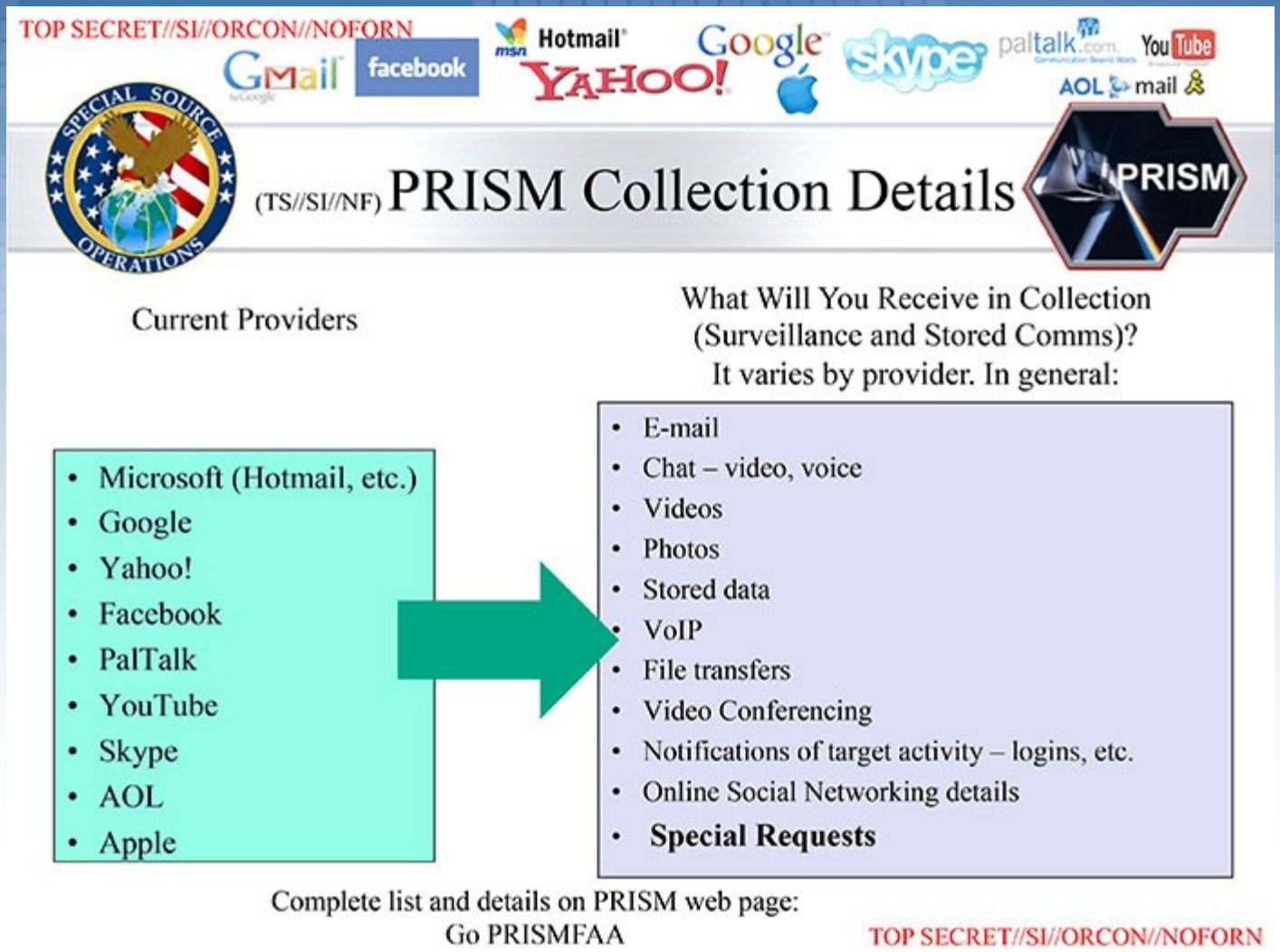
¿NSA?


nsa surveillance programs
Web
Noticias
Imágenes
Vídeos
Más
Herramientas de búsqueda
Cerca de 55,900,000 resultados (0.33 segundos)

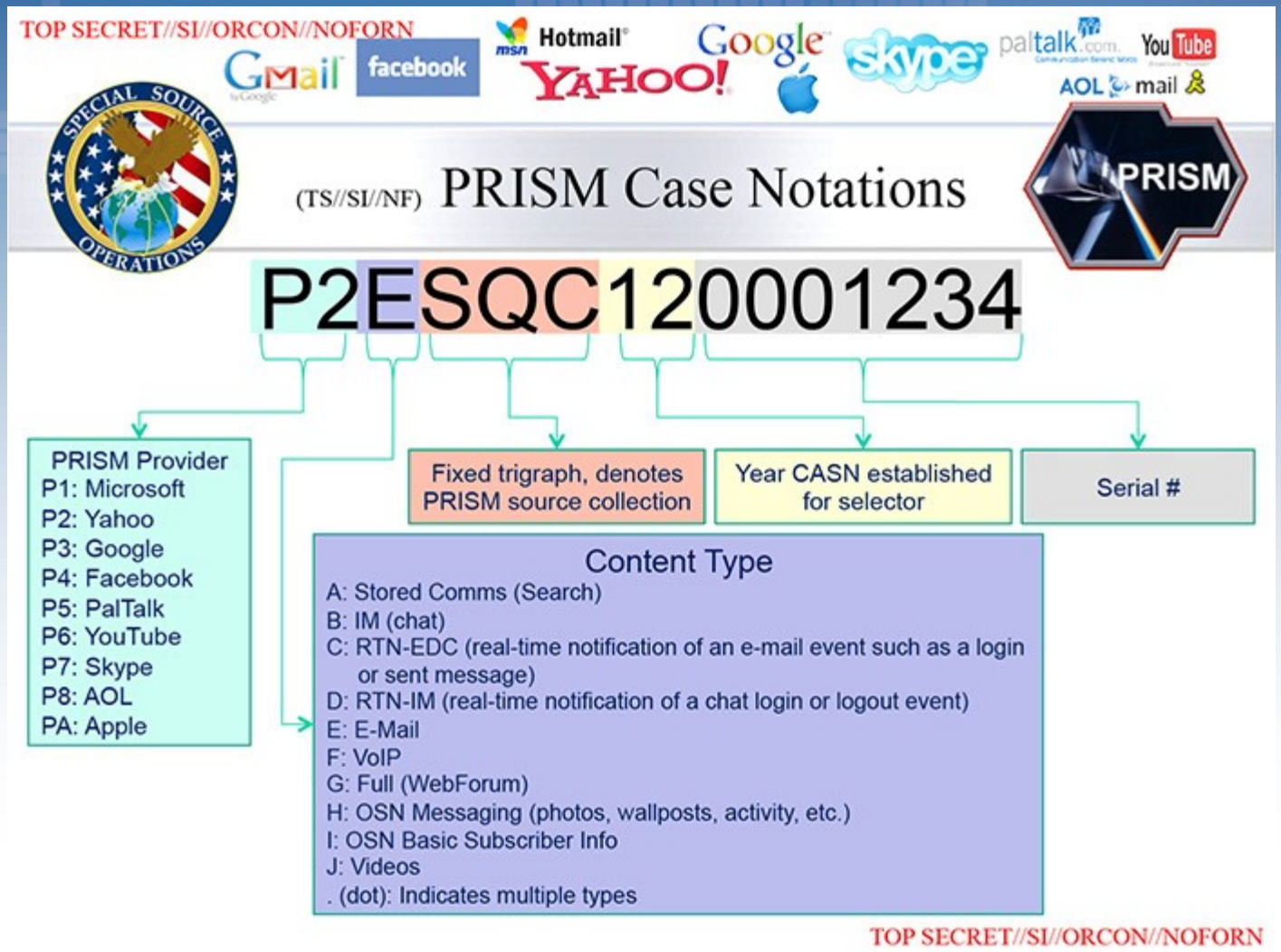
¿Como Empezó todo?



PRISM

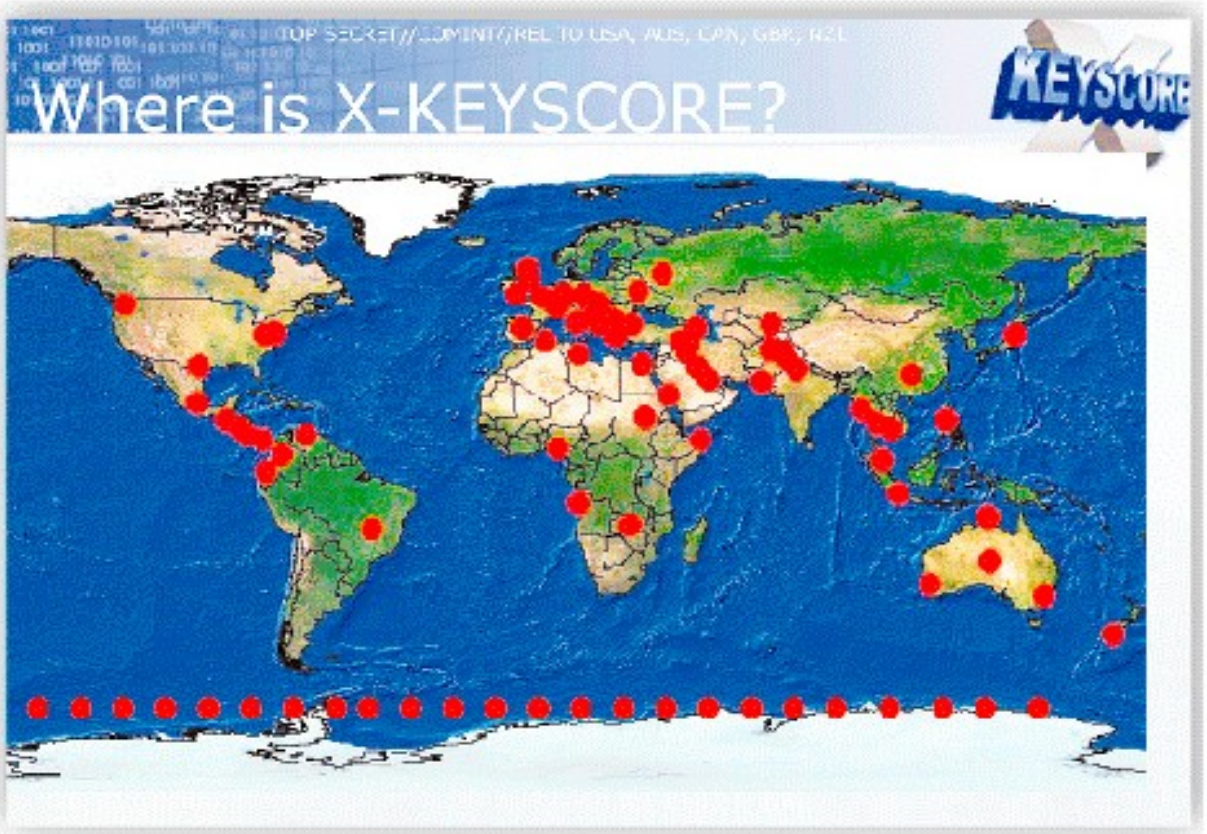

TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) PRISM Collection Details
PRISM
Current Providers
What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:
Microsoft (Hotmail, etc.)
Google
Yahoo!
Facebook
PalTalk
YouTube
Skype
AOL
Apple
E-mail
Chat – video, voice
Videos
Photos
Stored data
VoIP
File transfers
Video Conferencing
Notifications of target activity – logins, etc.
Online Social Networking details
Special Requests
Complete list and details on PRISM web page:
Go PRISMFAA
TOP SECRET//SI//ORCON//NOFORN

Formatos


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) PRISM Case Notations
PRISM
P2ESQC120001234
PRISM Provider
P1: Microsoft
P2: Yahoo
P3: Google
P4: Facebook
P5: PalTalk
P6: YouTube
P7: Skype
P8: AOL
PA: Apple
Fixed trigraph, denotes PRISM source collection
Year CASN established for selector
Serial #
Content Type
A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types
TOP SECRET//SI//ORCON//NOFORN

Todo Empeoró

Mapa de 2008 mostra o Brasil dentre os países bisbilhotados pelo programa X-Keyscore, que detecta a presença de estrangeiros através da língua usada em e-mails e telefonemas.



¿Como se voceó?

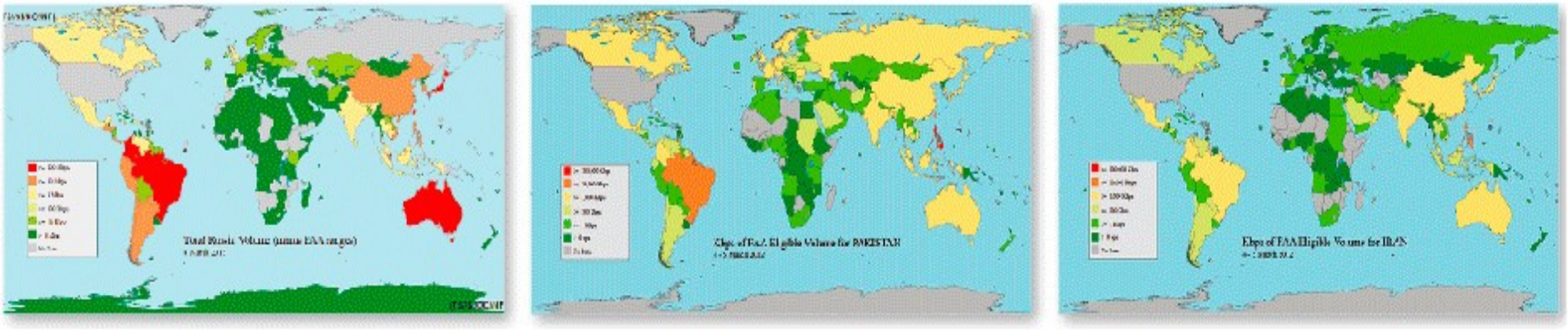
Para el norte y europa: The Guardian, The Washington Post, Der Spiegel, entre otros.

Al Grupo el Comercio, Grupo La Republica y Los Chichas les llegó al...

O Globo sacó cara por L.A

FAIRVIEW: PROGRAMA QUE AMPLIA CAPACIDADE DE COLETA DE DADOS

Mapas ilustram a quantidade de mensagens e telefonemas trocados por vários países do mundo com Rússia, Paquistão e Irã, compilados pelo programa Fairview, aparentemente nos dias 4 e 5 de março de 2013; países em vermelho, laranja e amarelo tiveram o maior número de mensagens rastreadas. Em todos os mapas, o Brasil se destaca entre os países da América Latina.



Estamos peor de lo que se piensa

Reporte de bug de windows

Example: Standard outbound Proxy log

6/30/13 - 3:44:17.000 PM
cloud-proxy.example.com XXX.XXX.XXX.XXX 80
http://watson.microsoft.com/StageOne/firefox_exe/21_0_0_4879/518ec3cc/xul_dll/21_0_0_4879/518ec306/c00000
05/001c9789.htm?LCID=4105&OS=6.1.7601.2.00010300.1.0.3.17514&SM=Acer&SPN=Aspire%20M3970&BV=P01-
A3&MRK=1025_ACER_ACER_AM1930&MID=0513D3D-CBA4-2339-9ABC-ABCDEFABCDEF microsoft.com cat

Event	Application crash report
IP Address	XXX.XXX.XXX.XXX
Application	Firefox.exe
Application version	21.0.0.4879
Crash location	518ec3cc
App library	Xul_dll
App library version	21.0.0.4879
Library crash location	518ec306
Crash reason	0xC0000005 (Access Violation)
App crash offset	001c9789
PC Info	Acer Aspire 1930 – Mid Tower running Windows 7 SP2
PC Windows Version #	6.1.7601.2.00010300.1.0.3.17514 (SP2)
PC Machine ID	0513D3D-CBA4-2339-9ABC-ABCDEFABCDEF

Apple está mas jodido

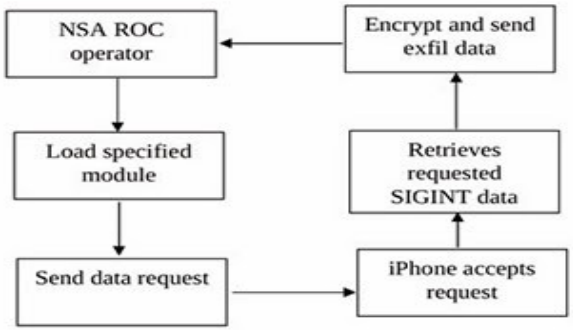
TOP SECRET//COMINT//REL TO USA, FVEY

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

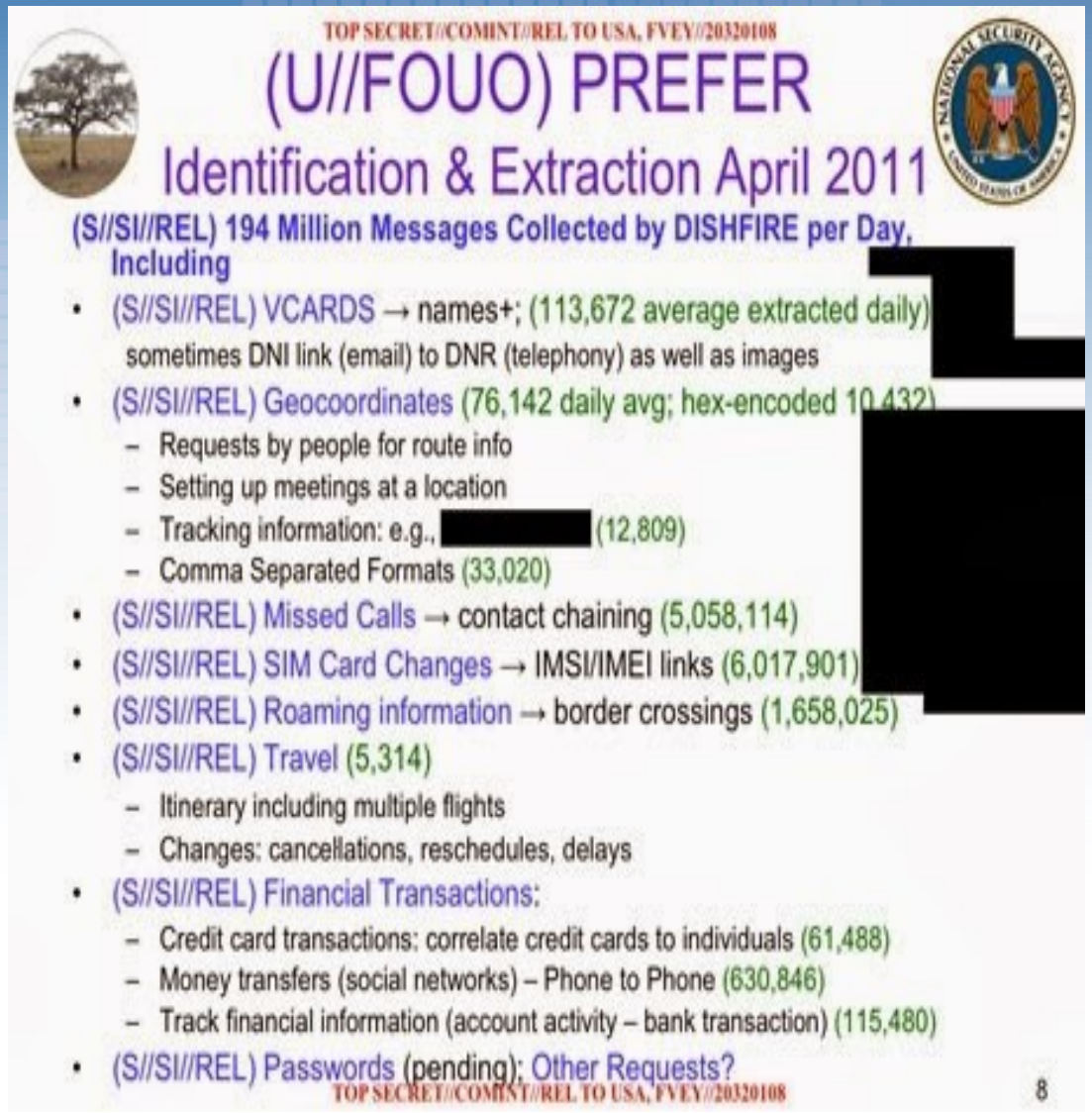
POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

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

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

OWASP LATAM TOUR 2014

Cuando la realidad no podía empeorar... 200M SMS x dia



TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(U//FOUO) PREFER

Identification & Extraction April 2011

(S//SI//REL) 194 Million Messages Collected by DISHFIRE per Day, Including

- (S//SI//REL) VCARDS → names+; (113,672 average extracted daily)
  sometimes DNI link (email) to DNR (telephony) as well as images
- (S//SI//REL) Geocoordinates (76,142 daily avg; hex-encoded 10,432)
  - Requests by people for route info
  - Setting up meetings at a location
  - Tracking information: e.g., [redacted] (12,809)
  - Comma Separated Formats (33,020)
- (S//SI//REL) Missed Calls → contact chaining (5,058,114)
- (S//SI//REL) SIM Card Changes → IMSI/IMEI links (6,017,901)
- (S//SI//REL) Roaming information → border crossings (1,658,025)
- (S//SI//REL) Travel (5,314)
  - Itinerary including multiple flights
  - Changes: cancellations, reschedules, delays
- (S//SI//REL) Financial Transactions:
  - Credit card transactions: correlate credit cards to individuals (61,488)
  - Money transfers (social networks) – Phone to Phone (630,846)
  - Track financial information (account activity – bank transaction) (115,480)
- (S//SI//REL) Passwords (pending); Other Requests?

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

8

OWASP LATAM TOUR 2014

¿Y los medios Peruanos?

Alan García figura en más de 100 informes de espionaje de Estados Un

Sabado, 29 de marzo de 2014 | 4:46 pm

Alan García: EEUU tiene más de 100 informes de espionaje sobre él

Sábado 29 de marzo del 2014 | 13:28

Semanario alemán Der Spiegel asegura que NSA creó base de datos de 122 jefes de

EE.UU. tiene más de 100 informes de espionaje sobre Alan García

Servicios secretos crearon base de datos especial con informes sobre 122 jefes de Estado y de gobierno en 2009

53 Comentarios | Me gusta 136 | Twittear 74 | +1 5 | Pin it 1

Der Spiegel: EEUU tiene más de 100 informes de espionaje sobre García

Sábado, 29 de Marzo 2014 | 4:40 pm

Ningún medio “respetable” adjunto la ppt

Y como se que los mata la curiosidad

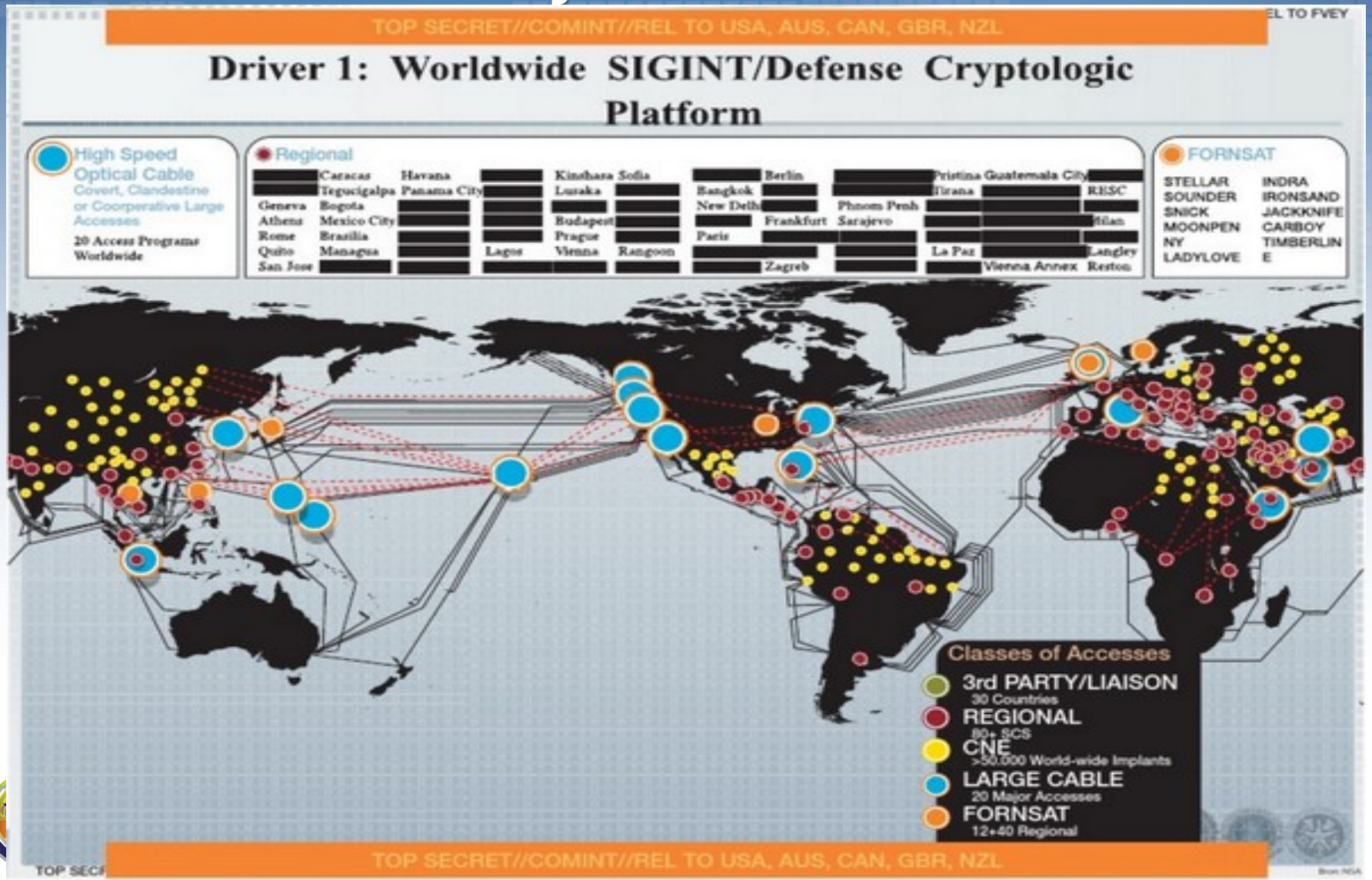
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

Machine vs. Manual Chief-of-State Citations

	Nymrod (machine-extracted) Citations				Last TKB Manual Update
	Name	Role	Code	Cites	
1	Abdullah Badawi	Malaysian Prime Minister	COS	> 100	10/15/2007
2	Abdullahi Yusuf	Somali President	COS	> 200	N/A
3	Abu Mazin	(Mahmud 'Abbas) PA President	COS	> 200	5/20/2009
4	Alan Garcia	Peruvian President	COS	> 100	N/A
5	Aleksandr Lukashenko	Belarusian President	COS	> 50	N/A
6	Alvaro Colom	Guatemalan President	COS	> 200	N/A
7	Alvaro Uribe	Colombian President	COS	> 700	N/A
8	Amadou Toumani Toure	Malian President	COS	> 50	N/A
9	Angela Merkel	German Chancellor	COS	> 200	N/A
10	Bashar al-Asad	Syrian President	COS	> 800	N/A
...	.....	.....	...		
122	Yuliya Tymoshenko	Ukrainian Prime Minister	COS	> 200	N/A

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

Pero... Perú también está jodido



Aquí comienza el surveillance peruano.

Un usuario no documentado

¿Backdoors en routers OLO SW(C|U)-9100?

17/02/2014 | Escrito por Nox

Deja tu cometario

Dos entradas en un día. !Esto es un record! :P.

¿Backdoors en routers OLO SW(C|U)-9100?

Este escrito es parte de los hallazgos que tuvieron fruto al analizar y hacerle ingeniería inversa a los *routers* Seowon Intech WiMAX SWC-9100 y SWU-9100.

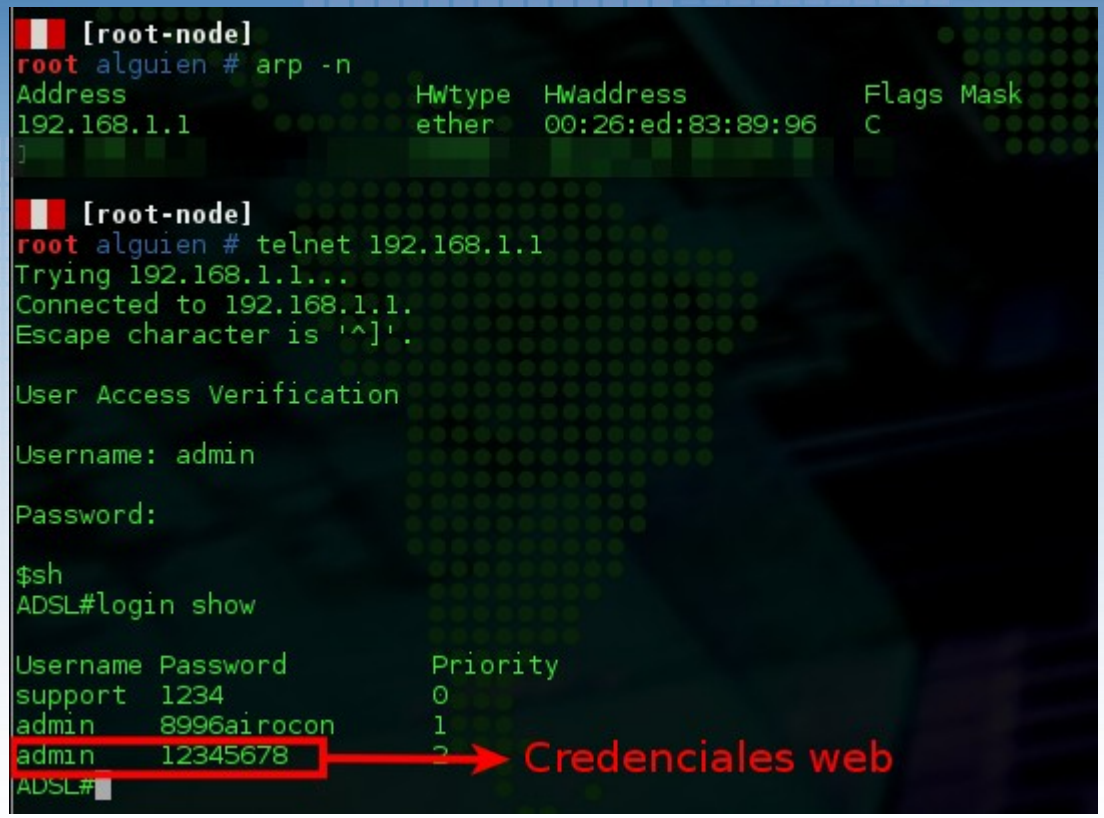
En el PDF enfatizo un usuario de la administración web que no existe en los manuales de usuario, que no está documentando y no puedes encontrar información al respecto, sin embargo, que puedes acceder a la administración web y puedes cambiar la contraseña del usuario documentado en el manual de usuario, "admin/admin" (usuario y contraseña respectivamente).

Espero que la lectura sea de su agrado.

Descarga: ¿Backdoors en routers OLO SW(C|U)-9100?

Saludos,
Nox.

Otro Usuario NO DOCUMENTADO



Un Acceso no documentado

CUANDO LA PUERTA ESTÁ ABIERTA: ROUTER ZTE ZXHN H108N

Miguel Guerra

Comunicador dedicado a la Seguridad Informática, Hacking, TIC y Marketing Corporativo.

57
SHARES

COMPARTIR | COMPARTIR | IMPRIMIR
TWITTEAR | ENVIAR

Continuamos con la revisión de router que miles de peruanos tienen instalados en sus hogares y empresas. Esta semana se verá la falla de seguridad en el router **ZTE ZXHN H108N**. Una vulnerabilidad realmente paranoica para quienes tengan este router de dos antenas en su poder, quedan prevenidos, cambien sus equipos o tomen las medidas necesarias para que no espien o intercepten sus comunicaciones.

Pidieron disculpas

Telefónica ratifica pleno respeto a la privacidad de la información

Frente al anuncio del hallazgo de una vulnerabilidad asociada a los **módems ZTE ZXV10 W300,** Telefónica enfatiza su pleno respeto a las leyes de privacidad de la información de todos sus clientes.

Esta vulnerabilidad, presentada recientemente en un porcentaje mínimo de su planta de módems con este fabricante, fue detectada en forma oportuna y se han tomado las medidas necesarias para su solución.

Telefónica recomienda a los usuarios que hayan adquirido sus propios módems a través de canales diferentes a la empresa, que apliquen las siguientes medidas para prevenir eventos similares:

- Restringir el acceso vía telnet desde la interface WAN.
- Deshabilitar el servicio SNMP".
- Llamar al servicio 104 para recibir la orientación correspondiente.

Lima, 5 de febrero de 2014

Algunos a medias

Desde el lunes 24 de marzo, está disponible la actualización del software para todos nuestros Router Móvil y Router Fijos. El proceso es automático; una vez que prendas tu dispositivo, las luces Wimax y Wifi comenzarán a parpadear por un lapso no mayor a 120 segundos y luego se reiniciará, no interrumpas ese proceso. No te preocupes por tu clave de Wifi, ninguna de tus configuraciones personales se verán afectadas. Si tienes dudas o deseas mayor asesoría, comunícate con nosotros al 01 7068000 o a atencionalcliente@olo.com.pe

Algo mas jalado de los pelos

- Para la interceptación de telefonía fija se ha contado con la participación de personal de supervisores y técnicos en actividad y ex trabajadores de la CPT y Telefónica del Perú, quienes recibían de la DIE los números telefónicos fijos por interceptar, obtenían del programa Omega de Telefónica la información técnica para identificar los pares telefónicos en las MAIN DISTRIBUTIONS FRAME FRAMS (MDF) e ingresaban a estos para hacer la desviación de la línea interceptada hacia los Puestos de Escucha.

Montesinos al SIN, haciendose cargo [illegible]
con las intervenciones telefónicas, accediendo a que el Coronel Roberto Huamán Azcurra infiltrara los elementos en las centrales que permitieron la interceptación de líneas fijas a nivel de Lima y provincias.

La Dirandro

Los secretos de Constelación

La interceptación se realiza desde el sexto piso del edificio de la Dirandro.

Desde hace más de dos años, unos 50 agentes de escucha trabajan las 24 horas del día en el sexto piso de la Dirandro con el apoyo de efectivos antidrogas e integrantes de las fiscalías contra el crimen organizado. Tienen permiso judicial y autorización de las empresas telefónicas. El sistema ha almacenado 1.024 gigabytes en audios que han permitido judicializar 99 casos e incautar 12 toneladas de droga.

Las conversaciones interceptadas son en su mayoría vinculadas al:

TERRORISMO, NARCOTRÁFICO Y CRIMEN ORGANIZADO

Comunicación establecida con un teléfono interceptado

El sistema captura la llamada **directamente desde la línea telefónica**, lo cual garantiza la fidelidad de lo interceptado.

El monitor

Es el efectivo que escucha las conversaciones. Cada uno cuenta con una clave de usuario.

Los audífonos del efectivo que escucha están adheridos a la pantalla.

El trámite previo a la interceptación

1 El oficial a cargo del caso recibe una lista de números telefónicos los cuales **expone ante el fiscal** para lograr que este formule un pedido de interceptación ante el juzgado.

Si el fiscal aprueba la intervención telefónica emite un acta al juez para su autorización.

2 El acta firmada retorna al fiscal y es allí cuando este **ingresa el número por interceptar** en el sistema.

999831_ _ _
9827580_ _

Números referenciales

3 El área de administración **configura el número,** previo aval de la compañía telefónica móvil y desde ese momento **se inicia la interceptación** del número celular.

El equipo no tiene CPU, trabaja directamente con el servidor y no cuenta con salidas USB ni similares.

¿Que programa usa constelación?

PEN-LINK, proporciona servicios policiales y organismos de inteligencia con el software de tecnología de última generación y sistemas para la interceptación, recogida, almacenamiento y análisis de las telefónicas-y las comunicaciones basadas en IP.

Software y sistemas de Pen-Link - Pen-Link 8, Lincoln y Xnet - son ampliamente reconocidos como estándares de la industria, con miles de Aplicación de la Ley y los usuarios con licencia de inteligencia de autoridades federales, estatales y locales en todo el mundo.

Sistemas de Pen-Link son ampliamente favorecidos, ya que no sólo destacan en la recogida de información y recogida en vivo, pero también traen a la luz un poderoso conjunto de herramientas de informes y análisis, el tipo de funcionalidad que es esencial en la perforación a través de gran cantidad de datos de hoy en día establece que revelar las relaciones que de otro modo podrían pasar desapercibidos.

Que mas trae Pen-Link

PRODUCTOS DE INTERCEPTACION EN TELEFONIA Y COMUNICACIONES

El Software **Pen-Link** cumple con toda su colección de las telecomunicaciones y de las necesidades de análisis:

- Registros históricos (peajes, CDRs)
- Plumas y Alambres
- De área amplia Red de Distribución
- Cell Phone Forensics
- Informes Potente, Gráficos y Mapas

Mas...

PRODUCTOS DE INTERCEPTACION EN INTERNET / IP BASADA EN SUS COMUNICACIONES

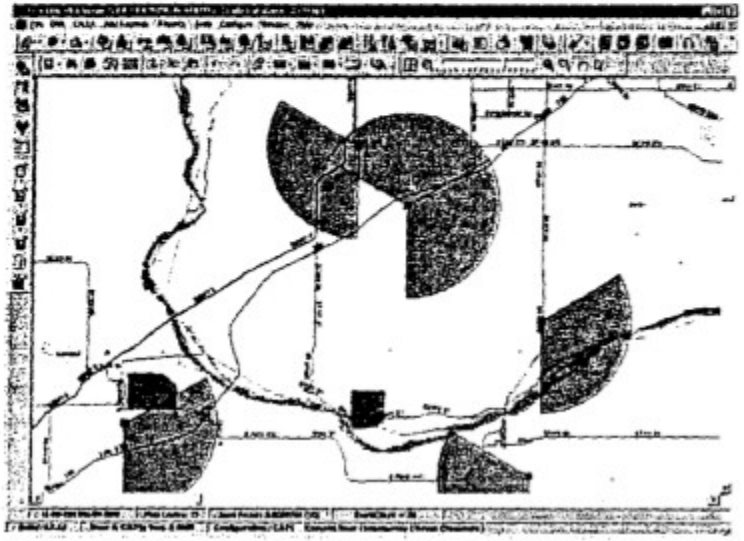
El Software **Pen-Link Xnet** reúne toda su colección de las comunicaciones basadas en IP (correo electrónico, redes sociales, etc.) y las necesidades de análisis:

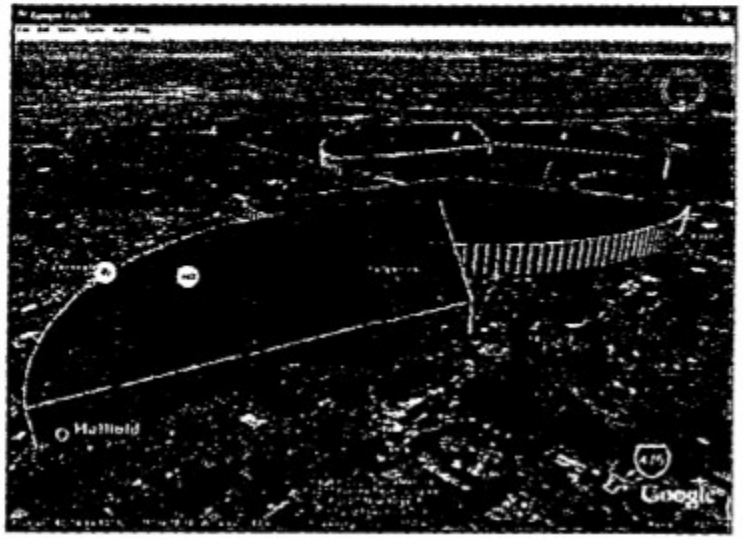
- Registros históricos Carga automática (por ejemplo, búsqueda de datos de warrants de los proveedores en línea)
- Carga automática de datos en paquetes
- Carga automática de los archivos de registro de varios elementos de la red
- Pens IP y Alambres
- Contenido decodificación y reconstrucción
- Informes Potente y Cartografía

Y entre la gama...

4.5.4 GIS Mapping

Where available, Geographical Information Systems (GIS) is an optional *add-on* to Pen-Link Software. Pen-Link provides GIS capabilities and will load the data. The mapping layers will need to be acquired locally. With the GIS functions, you can map any record or set of records that contain location information, including Call records, Cell Sites, Subscriber records, and Event records. Pen-Link will map locations based on street addresses or latitude and longitude (so it will work with most GPS Tracking units). Where available, the GIS functions can include center-line street data allowing you to zoom down to surface street level. Pen-Link's GIS capabilities are also compatible with ESRI shape file formats, so you can also load your own departmental data and image layers.





Como solicita la dirandro

FORMATO 02

ACTA Nº_______ DE INTERVENCIÓN, RECOLECCIÓN Y CONTROL DE COMUNICACIONES Y DOCUMENTOS PRIVADOS

- - - En el Distrito de San Isidro, Provincia de Lima, siendo las...............horas del día...........de..........de 20__, presentes en el Departamento Técnico Judicial – DIVINESP – DIRANDRO PNP el ....PNP...; Transcriptor/ Analista, el ....PNP..; Jefe/Coordinador del Grupo Técnico y el Dr (a). ....; Fiscal Adjunto Provincial (Recolector/Controlador) de la ....; actuando en observancia de la Ley Nº 27697 que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional del 10ABR2002 y su modificatoria Decreto Legislativo Nº 991 del 21JUL2007 y a mérito de la Resolución Judicial ...., emitida por el ....Juzgado .... de Justicia de ...., que resuelve .... , se procede a la recolección y control conforme se detalla a continuación: -------------

- - -El Personal PNP especializado indicado líneas arriba y el Señor Fiscal, proceden a verificar la recolección, luego de lo cual el Sr. Fiscal efectúa el control de la misma, desechando las comunicaciones o las partes de la comunicación que no tienen interés para efectos de la investigación, registrándose lo siguiente como relevante: --

Continuación

DATOS DE REGISTRO DE LA COMUNICACIÓN

LIID:		**Nombre/Número:**	
HASH (MD5):			

DATOS DE LA COMUNICACIÓN

Fecha:			
Hora Inicio:		**Duración:**	
Origen:		**Destino:**	
Medio utilizado:			
Interlocutores:			
Resumen:			
Transcripción:	**Se transcribe a continuación los fragmentos de audio que a consideración del Sr. Fiscal son relevantes para la presente investigación:- - - - - -** **00:00:00 "....."** **00:00:00** **00:00:00 "....."** **00:00:00**		
Observaciones:			

¿Y como me protejo de tanto espionaje?

Primero Las PCs

Dile ¡NO! A Windows y Apple

- Ubuntu -> Fixubuntu.com
- Debian
- Arch
- Fedora
- **Qubes**
- **Tails**

¿Cómo les escribo?

Skype -> Jitsi
Web XMPP -> Jabber
XMPP Clients -> Pidgin (Adium)
Crypto.Cat

¿Cómo mando mail?

Mozilla Thunderbird

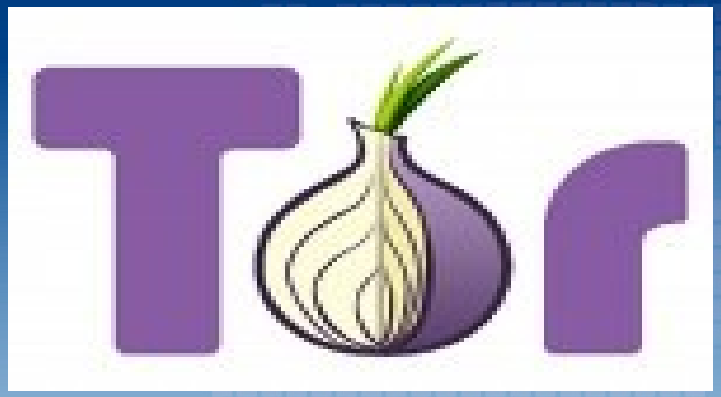
+

PGP

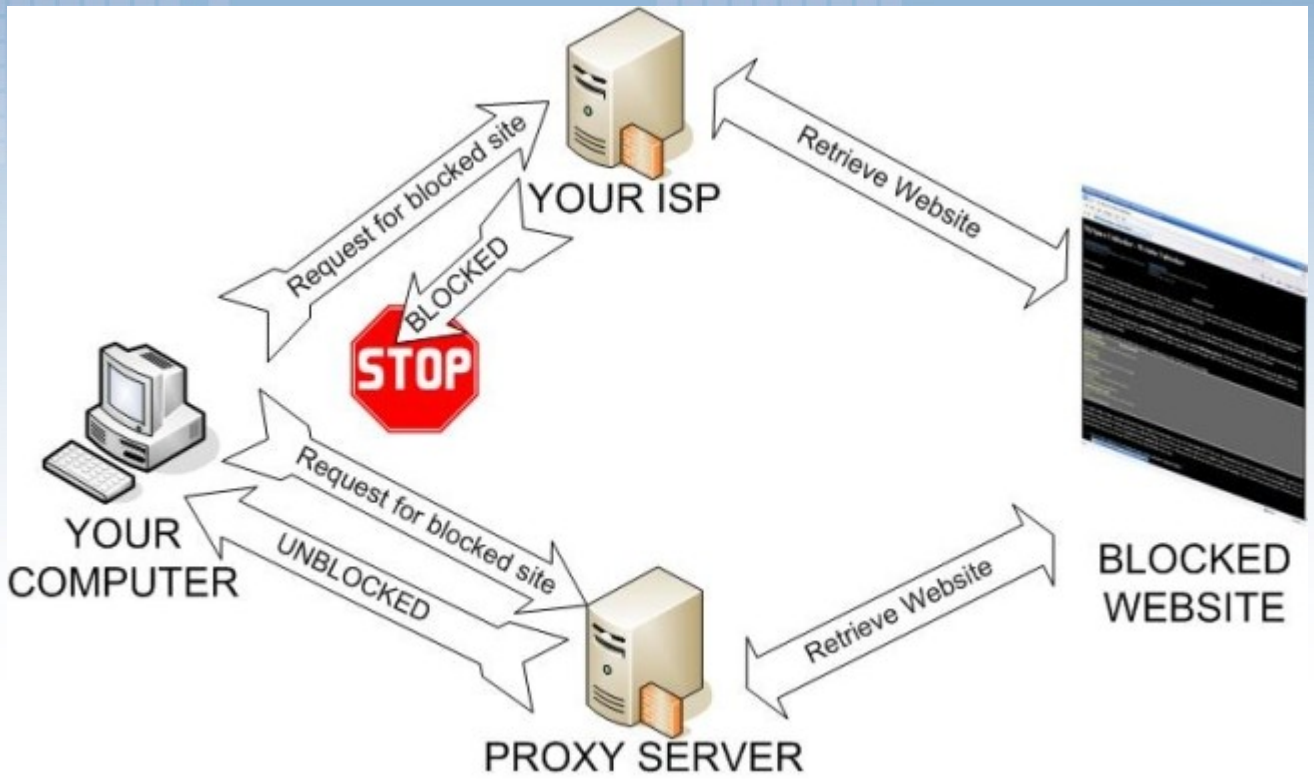
¿Cómo Navego?

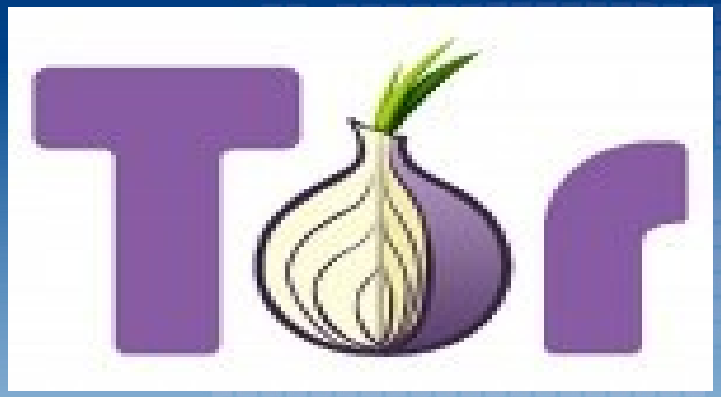
Usen Tor:

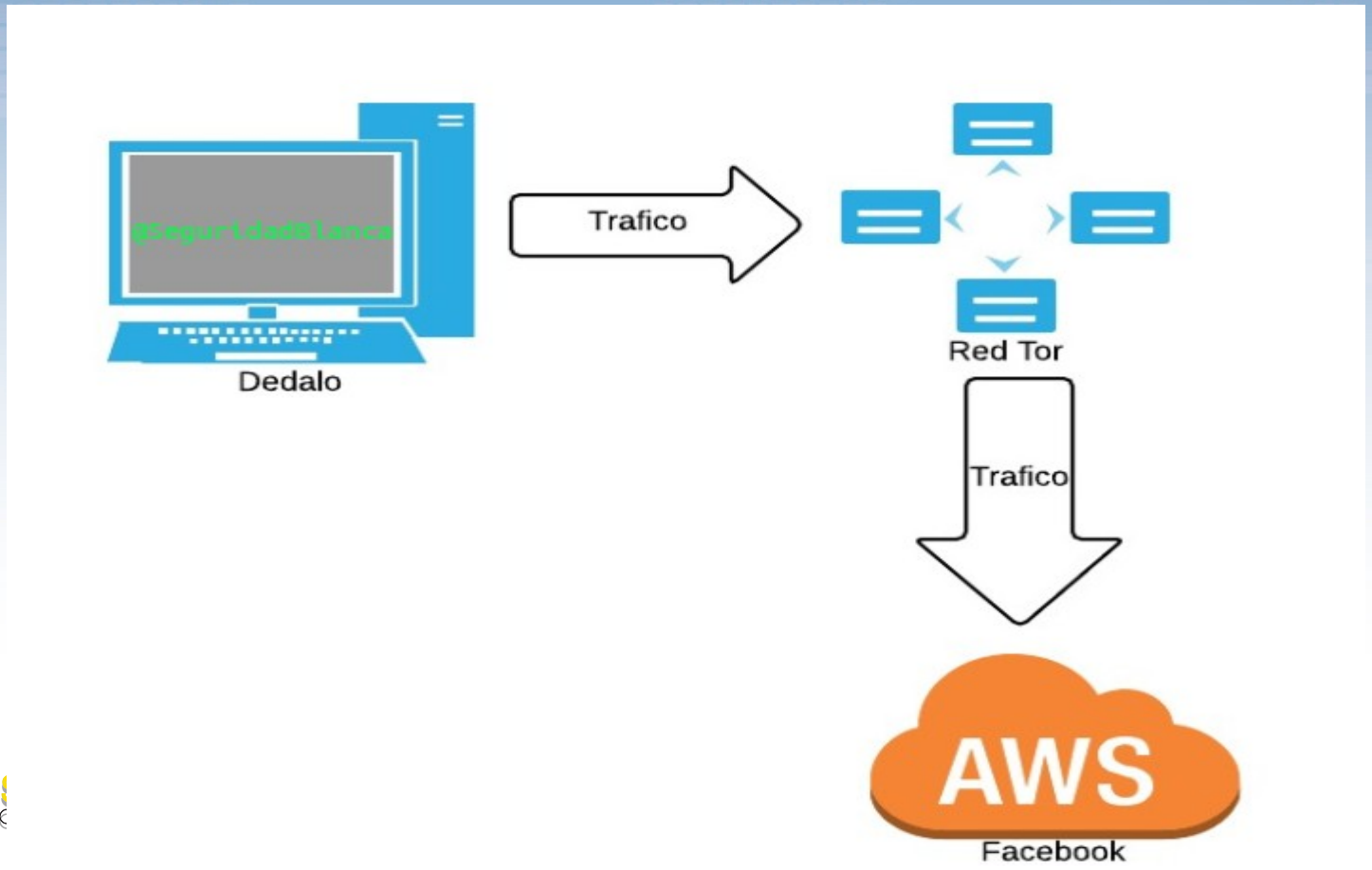
Tor Browser Bundle
Tormium



Tor Project es una red de servidores proxy que permite comunicaciones cifradas.


YOUR ISP
Request for blocked site
BLOCKED
STOP
Retrieve Website
YOUR COMPUTER
Request for blocked site
UNBLOCKED
Retrieve Website
BLOCKED WEBSITE
PROXY SERVER




@Seguridad@Lanca
Dedalo
Trafico
Red Tor
Trafico
AWS
Facebook

¿Smarfons?

¿Cómo Llamo?

Podemos usar Ostel o Redphone

RedPhone es una aplicación que se conecta a un servidor de voz sobre IP de manera cifrada para poder conversar con otro que tenga redphone sin ser interceptado.

¿Por donde escribo?

TextSecure o ChatSecure

TextSecure es una aplicación que permite enviar sms/mms/push de manera cifrada

ChatSecures es un cliente de mensajería por protocolo XMPP Cifrado por OTR.

Muy bonito todo pero...

¿Por que la Dirandro o la NSA quisieran algo de mi?

1.- ¿Por que debería hacerlo?

¿Por qué deben tener nuestras fotos, correos, llamadas, etc?

2.- Hoy eres nadie, mañana quien sabe.

Hoy puede que escribas a donde vas a comer menú todos los días, mañana esa información puede ser usada para saber donde estás.

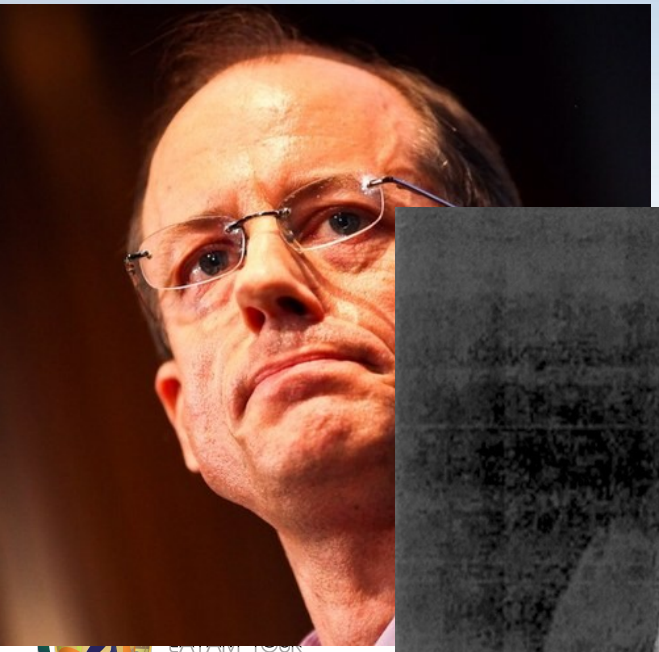
3.- Soy amigo de X

Si X te dijo algo que tu no quería saber o se equivoco al momento de mandar una conversación y la leyeron, puedes estar ya en la lista.

Cardenal Richelieu

Dame un texto de seis líneas escrito por el hombre mas honesto y encontraré algo para que lo cuelguen.

¿Que puedo hacer yo por mi Perú?



¿Como mas puedo apoyar?

- Programar
- Periodismo de Investigación
- Financiamiento
- Protestas

¿Como apoya Dedalo?

Programando

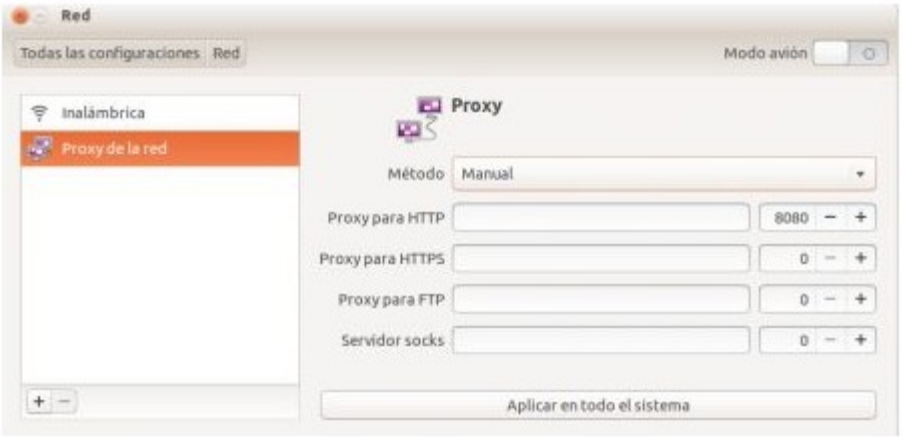
Tormium: Saliendo por tor con chromium

Por Dedalo el viernes 7 Febrero 2014, 11:46

InfoSec Tor

Bueno resulta que desde que comencé a buscar vulnerabilidades, noté que usar firefox para buscar xss basados en DOM, era un poco tedioso. Decidí quedarme pegado en chromium, no chrome porque en definitiva me gusta la idea de poder revisar el código fuente de la aplicación en busca de backdoors cuando yo quiera.

Pero cuando llegó el momento de la verdad y quise hacer que mi chromium saliera por TOR me encontré con este salvaje mensaje: Chromium está utilizando la configuración de proxy del sistema de tu equipo para conectarse a la red. Lo primero que pensé fue que era como firefox que podría cambiar la configuración a usar proxy puesto a mano. Pero cuando di click al boton para cambiar me saltó lo siguiente:



OWASP LATAM TOUR 2014

Apoyando el Periodismo

HACKEANDO LA METADATA DE TUS ARCHIVOS [PARTE 1]

Dedalo

Escritor de PHP, Python y Libertad...

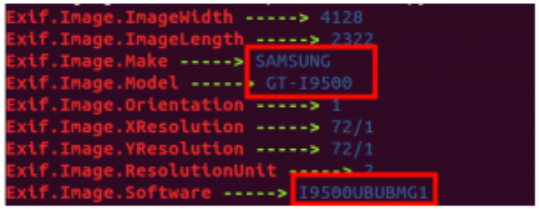
Ethical Hacker.

33 SHARES

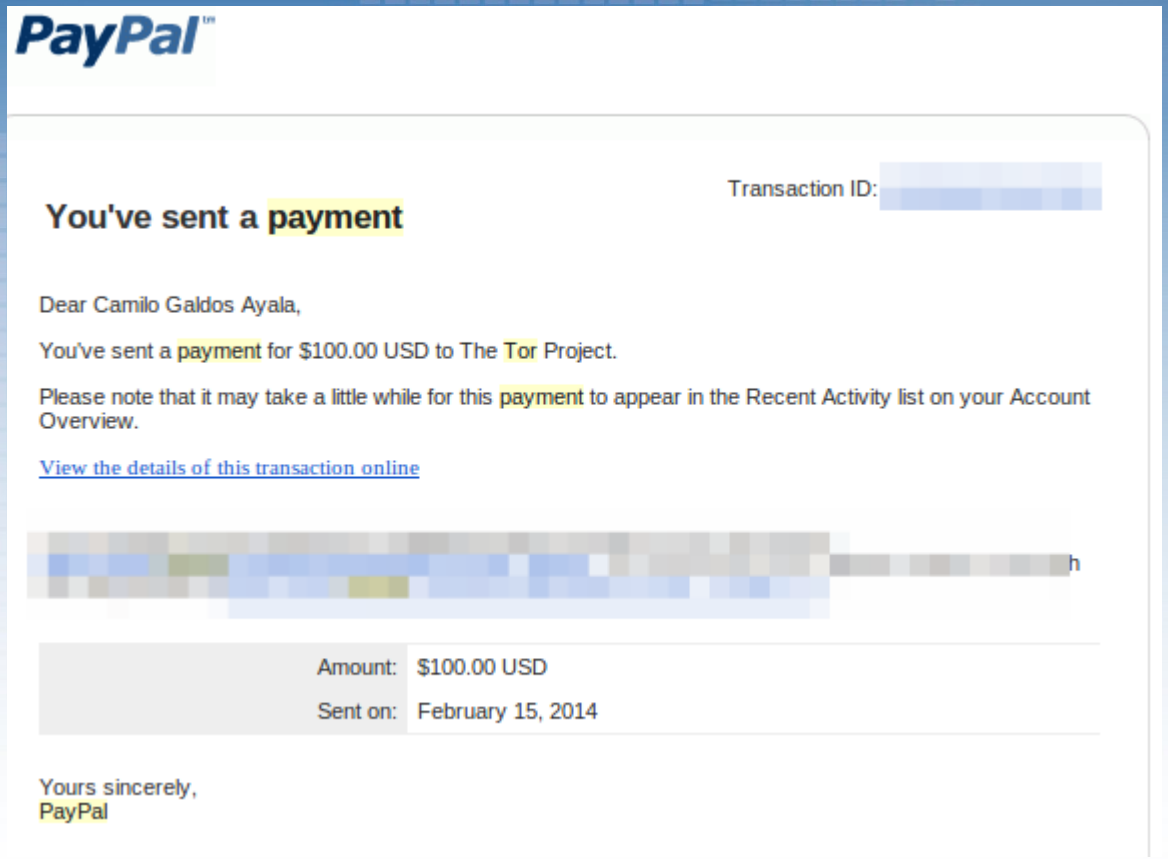
COMPARTIR | COMPARTIR | IMPRIMIR | TWITTEAR | ENVIAR

Metadata es la unión de dos palabras griegas que significan: ***"Mas allá de la información"***. ¿Y esto cómo influye en tu vida tecnologica? Resulta que cada vez que tomas una foto con tu camara o smartphone, en la foto se almacenará más información de la q puede ver a simple vista. Asi que cuidado que cuando compartes una imagen estés regalando datos como el dispositivo que tienes, tu ubicación, fechas y más.

En la Metadata o datos ocultos de una foto podrás observar: El Fabricante (Marca) del dispositivo con el que tomaste la foto, la versión modelo) del aparato, si la tomaste con flash, la hora y fecha en que se tomó, y si tienes el GPS activo, se podrá saber el lugar geográfico donde se captó la fotografía.



Financiando



PayPal™

Transaction ID:

You've sent a payment

Dear Camilo Galdos Ayala,

You've sent a payment for $100.00 USD to The Tor Project.

Please note that it may take a little while for this payment to appear in the Recent Activity list on your Account Overview.

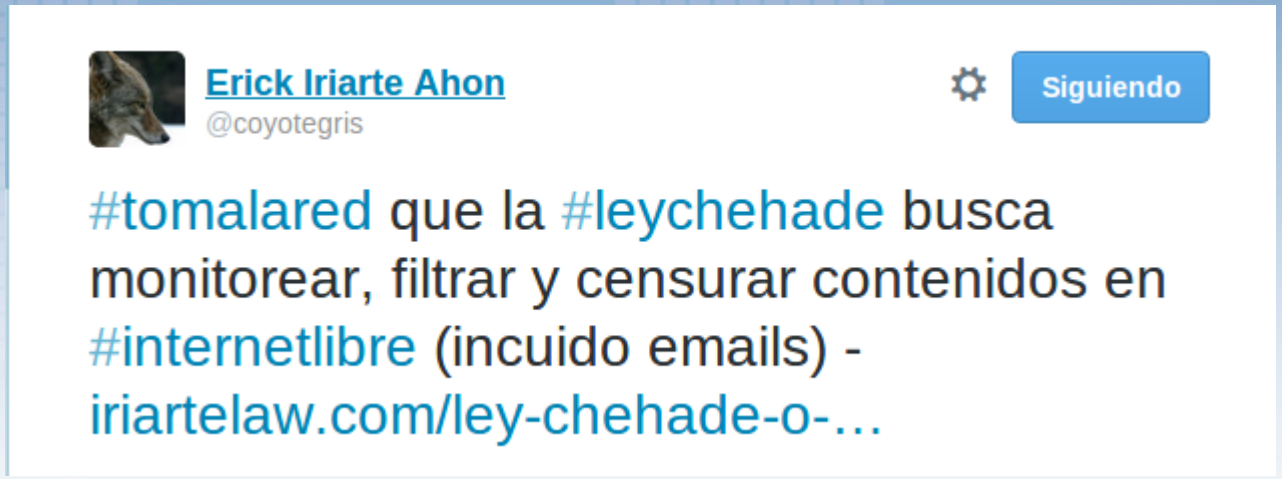
View the details of this transaction online

Amount:	$100.00 USD
Sent on:	February 15, 2014

Yours sincerely,
PayPal

Por su puesto... Protestando... No a las leyes de mierda.

#TomaLaRed
#InternetLibre



@SeguridadBlanca
me@dedalo.in
Blog.Dedalo.In

OWASP
LATAM TOUR
2014

Gracias!