

Rastros digitales

Seguridad para colectivos
e individuos



ReD

Cofundador de Hacklabs

Apasionado de la tecnología

Defensor de la privacidad



¿Por qué hacer una charla
sobre rastros digitales?



¿Por qué hacer una charla
sobre rastros digitales?



Participantes

- Pasivos
 - Individuos / Colectivos
- Activos
 - Empresas de servicios en Internet
 - Proveedor internet (isp)
 - Compañías / Lugar de trabajo
 - Gobiernos
 - Cuerpos del estado
 - Vecino jeta



Protección

- Antivirus
- Antispyware
- Firewall (cortafuegos)
- Antirootkits



¡Yo no tengo nada que ocultar!



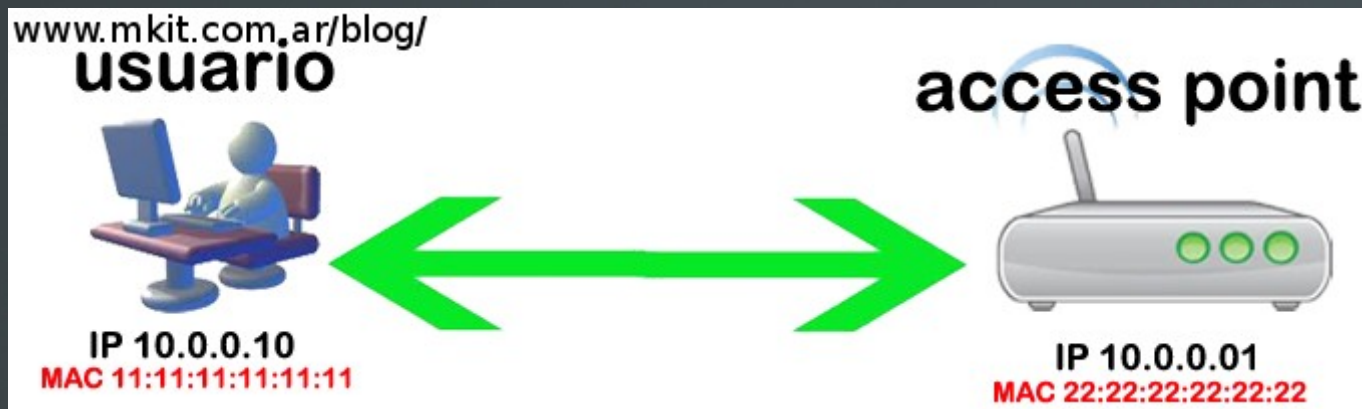
Wifi

- Vecino sin Internet
- Herramientas:
 - Wlan decrypter WLAN_XXXX
 - Jazztel decrypter JAZTELL_XXXX
 - Wlanreaver
 - Wifiway
- No sólo perdemos ancho de banda



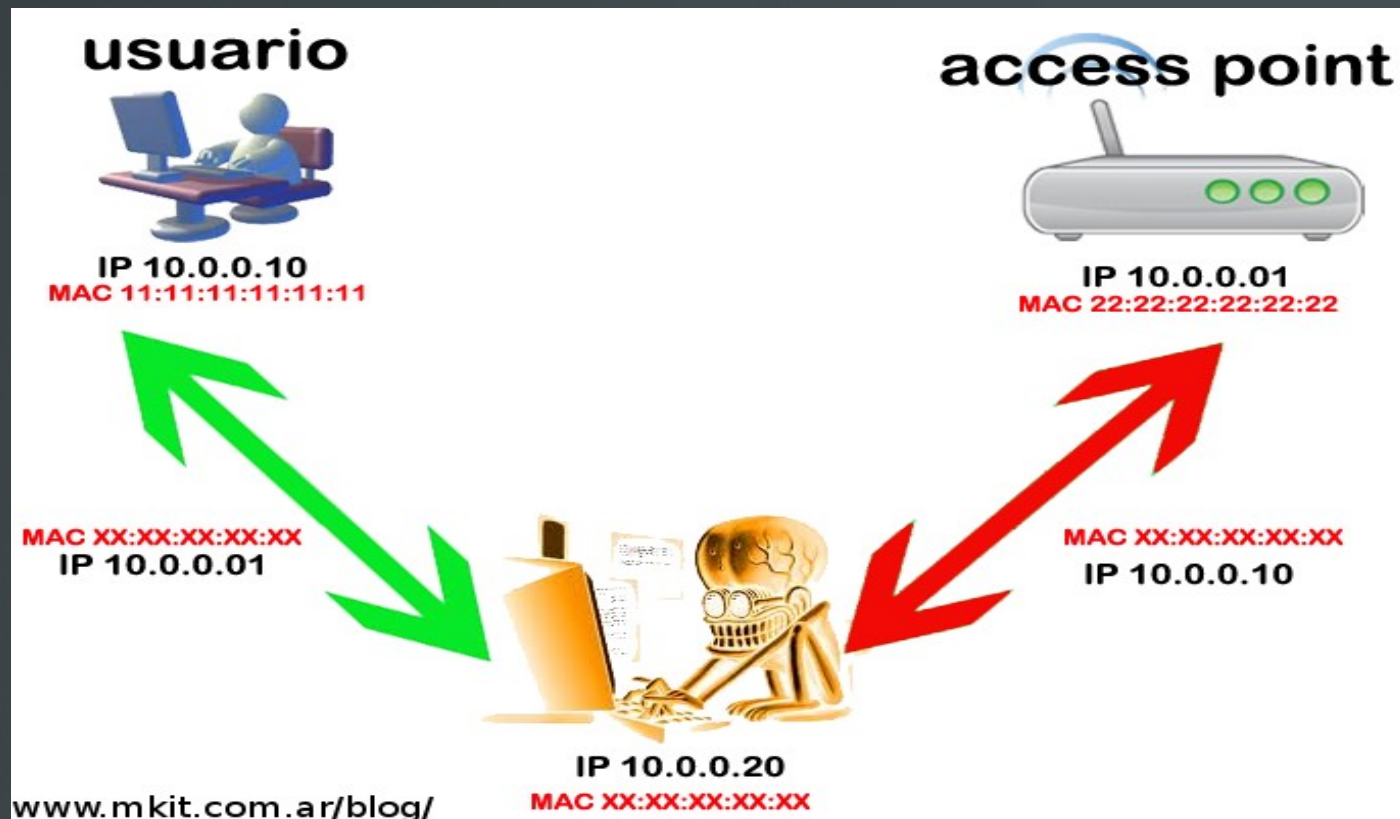
Wifi

- Acceso a todo nuestro tráfico a través de un ataque Man In The Middle (MITM)



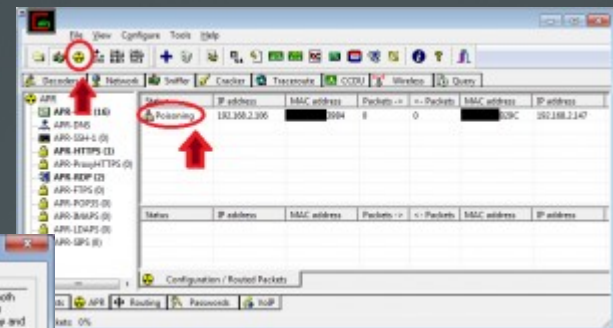
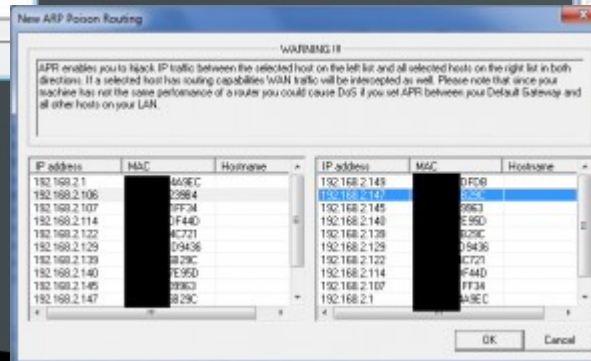
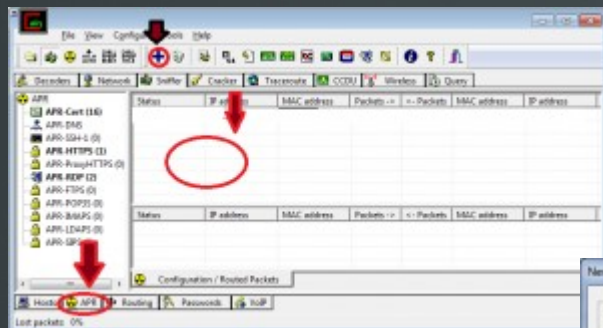
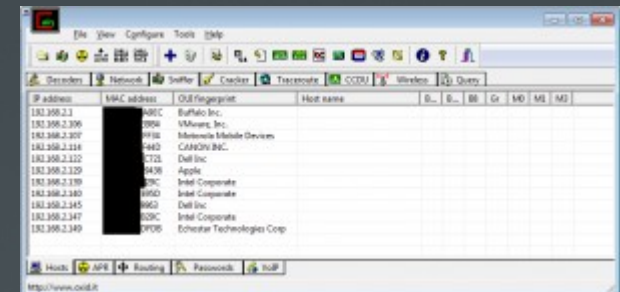
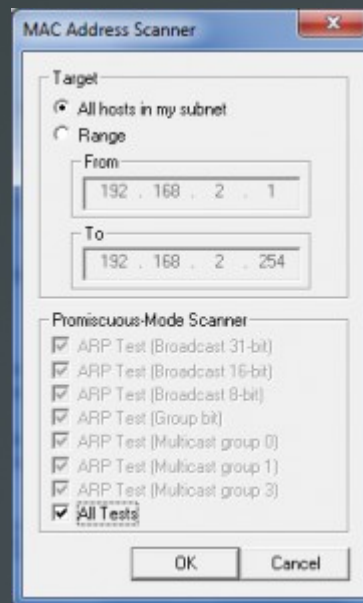
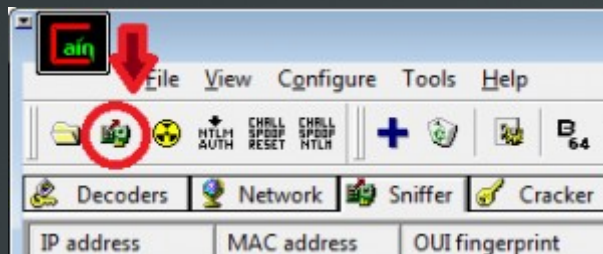
Wifi

- Acceso a todo nuestro tráfico a través de un ataque Man In The Middle (MITM)



Wifi

■ MITM con Cain & Abel en 6 pasos



Wifi

- Webs con o sin certificados (SSLStrip)
- Emails
- Conversaciones
- Etc.



Wifi

- Rastros más allá del alcance de la wifi
- Bases de datos con ESSID, BSSID y potencia
 - Nombre , Mac (xx:xx:xx:xx:xx:xx) y Distancia
- Localizar un equipo sin GPS



Wifi

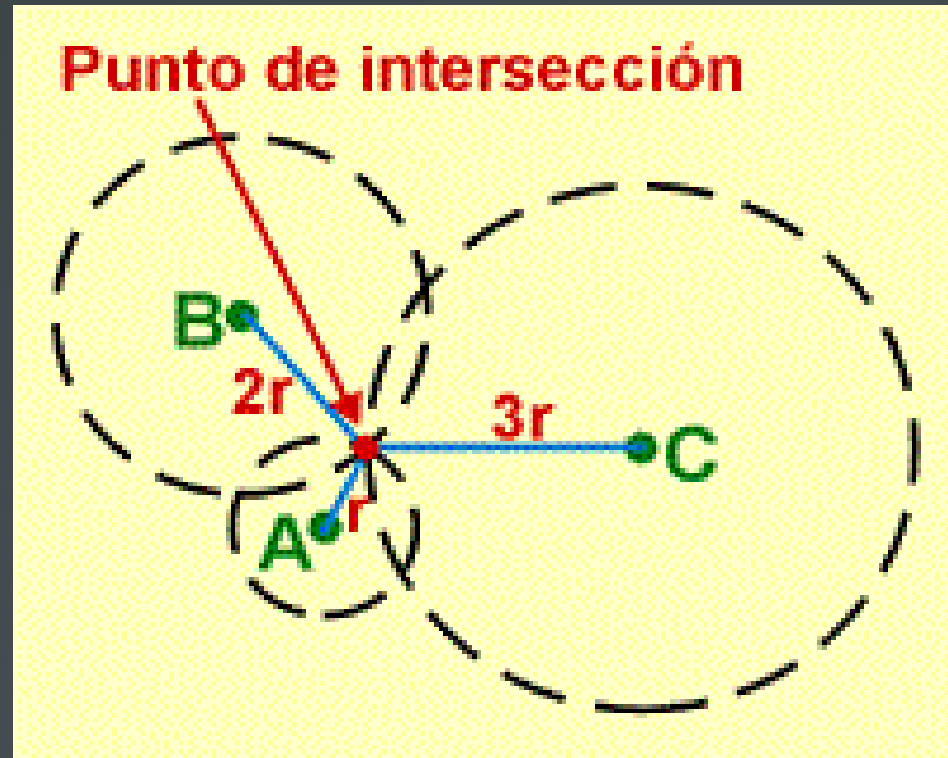


Discreción Ninja



Wifi

Triangulación



Wifi

- Google tuvo problemas legales
- Solución añadir _nomap al nombre ap
- Impacto real muy bajo



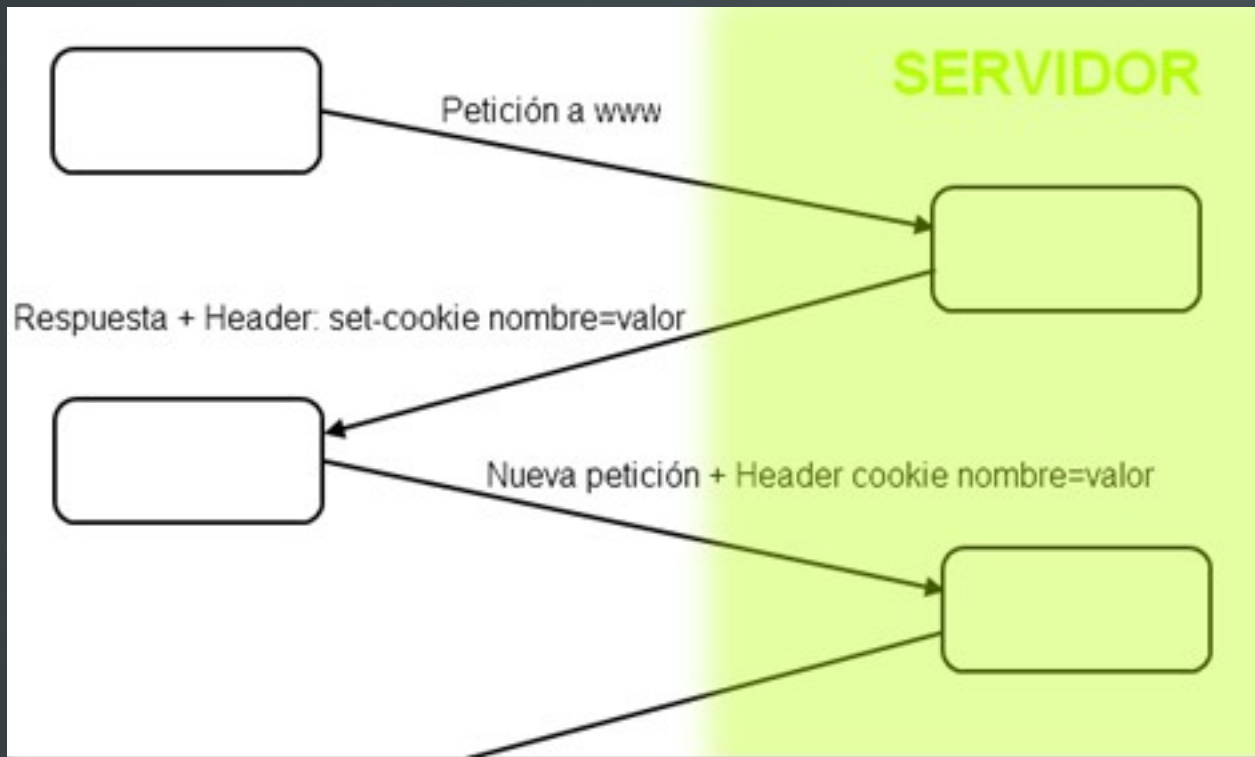
Wifi

- Protección:
 - Extensión HTTPS Everywhere
 - Ocultar el ESSID
 - Utilizar WPA2 con contraseñas complejas
 - Filtrar por mac
 - Reducción rangos IP
 - Detectar intrusos:
 - Suricata (Linux)
 - AirSnare (Windows)



Cookies

- Se almacenan en el equipo
- Guardan parejas nombre y valor



Cookies

- Dos funciones:
 - Seguimiento dentro de una web
 - Conseguir hábitos de navegación



Cookies

- Protección:
 - Usar navegación privada
 - Eliminación desde navegador
 - Darse de baja (opt-out)
www.networkadvertising.org
 - Usar plugin de borrado:
 - Objection (flash)
 - Cookie monster.



Super Cookies

- Se pueden borrar pero se regeneran
- Se almacena en:
 - Como cookie estandar
 - Como cookie de flash
 - Con los métodos de almacenaje de HTML 5
 - En cache a través de eTags



Super Cookies

- Se pueden instalar incluso en el modo incógnito
- Hacen oídos sordos a Do Not Track
- El servicio no está en una sola web, sino en todas las que usen el mismo sistema de estadísticas



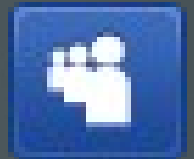
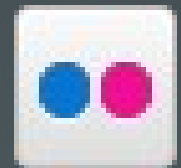
Super Cookies

- Protección:
 - Extensión Better Privacy



Redes sociales

- Información pública para todos:
 - Trabajos
 - Seguros...
- Cruce de información para sacar:
 - Orientación sexual
 - Afilaciones políticas
 - Creencias religiosas
 - Problemas de salud...



Redes sociales

Geotagging

- Opción activa de geotag
- Peligro por detección de hábitos:
 - Colegios
 - Parque...



Redes sociales

Geotagging

- Protección:
 - Desactivar geotags
 - Desactivar geolocalización tanto GPS, GPS-A y Wifi



Redes sociales

Rastreo de Facebook

- Primera visita a Facebook:
 - Si te registras te manda 2 cookies.
 - Sólo visita 1 (la que identifica tu pc)
- Pagina con botón "me gusta" u otro plugin te carga en la cookie la página y fecha exacta
- Mantienen los registros de tus últimos 90 dias de actividad en sus servidores



Redes sociales

Cuentas anonimas Facebook

- Versión móvil (**m.facebook.com**) permite buscar usuarios anónimos de forma indirecta
- No válida correctamente el formulario
- Permite el análisis por medio de bots



Redes sociales

Cuentas anónimas Facebook

facebook

Identify Your Account

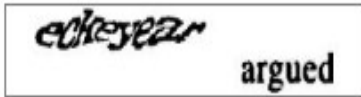
We Couldn't Find Your Account

- The email you entered does not belong to any account. Make sure that it is typed correctly. You may also try again using any other email, username or mobile phone number associated with your account.

facebook

Security Check

Security Check



Submit Try another

Redes sociales

Cuentas anónimas Facebook

- Respuesta de Facebook

”NO aseguramos que la información de los usuarios no pueda ser recolectada de forma automática por un bot u otro proceso”
- Existen mecanismos de protección que no se usan.
Captcha...



Informacion privada Facebook

- Univ. Columbia Británica prueba 8 semanas,
- 102 bots simuladores de humanos
- 5023 usuarios atacados
- 80% de los usuarios pueden ser infiltrados, incluyendo amigos de amigos
- Se envio 3Gb y se recibió aproximadamente 250Gb
- Facebook ha calificado esta investigación como exagerada y poco ética



Redes sociales

Análisis forense de Facebook

- Valkyrie-X Security Research Group publicaron un documento de análisis forense de facebook
- Se puede recuperar las charlas, comentarios en el muro, eventos, grupos...
- Recopilan datos de perfiles móviles



Redes sociales

Imágenes Facebook

- Toda imagen tiene un identificador
- Imágenes privadas o públicas son accesibles sin cuenta de Facebook
- Todas las imágenes se guardan en host externos

<https://fbcdn-sphotos-a.akamaihd.net/hphotos-ak-snc3/>
<http://sphotos.ak.fbcdn.net/hphotos-ak-snc3/hs395.snc3/>
<https://s-hphotos-ash4.fbcdn.net/>
<https://fbcdn-sphotos-a.akamaihd.net/hphotos-ak-snc4/>
<https://fbcdn-photos-a.akamaihd.net/hphotos-ak-ash4/>
<https://s-hphotos-snc6.fbcdn.net/>



Redes sociales

Imágenes Facebook

24124_100199166687607_1000000000000000001_2078_4000612_n.jpg

- Campos del identificativo
 - 24124; 5 dígitos que identifica el album
 - 100199166687607; 15 dígitos para id de foto
 - 1000000000000000001; 9 dígitos después 100000, no se usa y sólo tiene que ser superior a 0
 - 2078; Sin uso, si lo cambias sigue funcionando
 - 4000612; Número unico de la foto, uso desconocido



Redes sociales

Imágenes Facebook

- Imagen en Facebook

24124_100199166687607_10000000000000001_2078_4000612_n.jpg

- Imagen accesible públicamente

https://s-hphotos-ash4.fbcdn.net/24124_100199166687607_10000000000000001_2078_4000612_n.jpg



Redes sociales

- Protección:
 - Extensión Priv3 (botones seguir, +1, me gusta...)



Redes sociales

- Protección:

*”Uno es dueño de lo que calla
y esclavo de lo que habla”*

Sigmund Freud



Búsquedas en Internet

- Google usa 57 variables en identificar equipo
- Edición de contenidos digitales (censura "positiva")



Búsquedas en Internet



- Crisis in Egypt
- Protests of 2011
- Lara Logan



- Travel, Vacations
- Egypt Daily News
- CIA World Factbook

Los "Secretos" de Google Y Facebook

Scott's Search

Egypt ⌵ ⌵

About 100,000,000 results (0.34 seconds)

Crisis in Egypt
Videos in Egypt have been muted but will not be silenced. Listen.
humanityfirst.org/Egypt/

Egypt - Wikipedia, the free encyclopedia ⌵ ⌵
Egypt officially the Arab Republic of Egypt, is a country mainly in North Africa, with the Sinai Peninsula forming a land bridge in Southwest Asia. ...
Hosni Mubarak - Ancient Egypt - Female genital cutting - History of modern Egypt
en.wikipedia.org/wiki/Egypt - Cached - Similar

Egypt News - The Protests of 2011 - The New York Times ⌵ ⌵
World news about Egypt and the protests of 2011. Breaking news and archival information about its people, politics and economy from The New York Times.
nytimes.com - World - Countries and Territories - Foreign

Egypt Travel, Tours, Vacations, Ancient Egypt from Tour Egypt ⌵ ⌵
Information for travelers, resources on history, monuments and activities.
www.touregypt.net - Cached - Similar

News for Egypt
 **Why Lara Logan Was Likely to Return to Egypt** ⌵ ⌵
1 hour ago
By Charlotte Triggs AP Lara Logan had already had one troubling experience in Egypt before last Friday's "brutal and sustained" sexual assault. ...
People Magazine - 1000 related articles - Shared by 20+
In Egypt, renewed hope for gender equality ⌵ ⌵
USA Today - 2011's most stories - Shared by 3+
[Readline updates for Egypt 2011](#)

Egypt Daily News - Egypt News

Daniel's Search

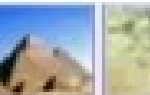
Egypt ⌵ ⌵

About 101,000,000 results (0.10 seconds)

Egypt - Wikipedia, the free encyclopedia ⌵ ⌵
Egypt officially the Arab Republic of Egypt, is a country mainly in North Africa, with the Sinai Peninsula forming a land bridge in Southwest Asia. ...
Hosni Mubarak - Ancient Egypt - Female genital cutting - History of modern Egypt
en.wikipedia.org/wiki/Egypt - Cached - Similar

Egypt Travel, Tours, Vacations, Ancient Egypt from Tour Egypt ⌵ ⌵
Information for travelers, resources on history, monuments and activities.
www.touregypt.net - Cached - Similar

Egypt Daily News - Egypt News ⌵ ⌵
Egypt Daily News, covering Egypt News, Arab news, Middle East news and World News.
Egyptian Culture, Egyptian recipes, Egyptian food, Egyptian art, ...
www.egyptdailynews.com/ - Cached - Similar

Images for Egypt - Egypt Images
    

Egypt - CIA - The World Factbook ⌵ ⌵
Feb 1, 2011 ... It features a map and brief descriptions of geography, economy, government, and people.
<https://www.cia.gov/library/publications/the-world-factbook> - Cached - Similar

Egypt State Information Service ⌵ ⌵
Official government site provides information on the country's government, politics, culture, history, economy and tourism. (Arabic, English, French)

Búsquedas en Internet

- Protección:
 - Extensión GoogleSharing
 - Extensión TrackMeNot
 - Activar Do No Track



Navegadores

- Facilitan datos de máquina, S.O. entre otros
 - <https://panopticlick.eff.org/>
- La navegación privada sigue sin cubrir:
 - Certificados digitales
 - Consultas DNS; ipconfig /displaydns
 - Páginas swapeadas



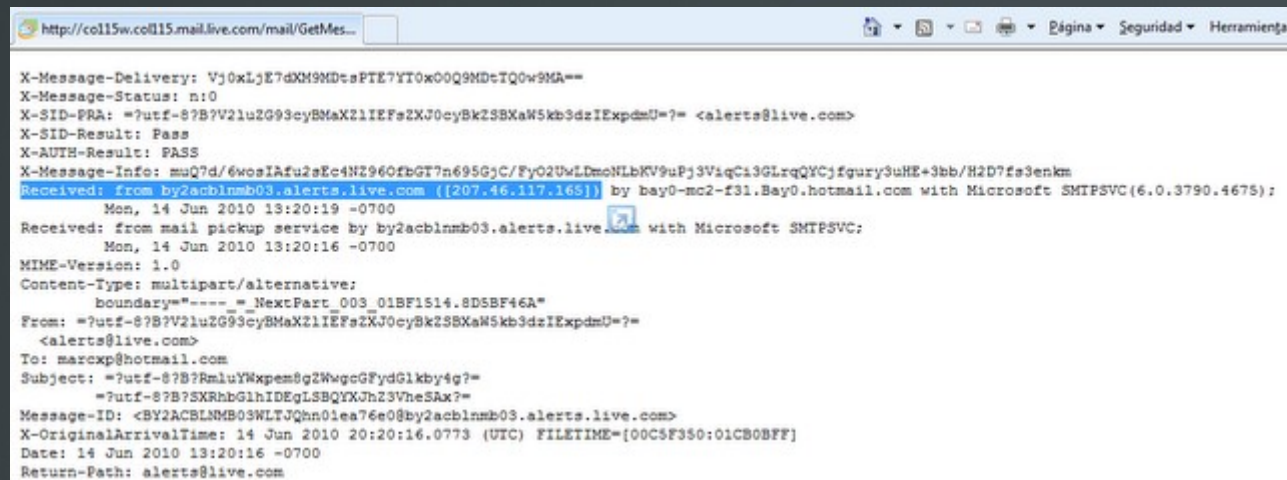
Voz ip

- Skype. Sistema de cifrado vulnerable en la negociación a un MITM
- Facilidad de acceso a escuchas a gobiernos
- "Error" de funcionamiento permitió:
 - Acceder al tráfico p2p
 - Localizar al usuario geofraficamente por ip
 - Se podía realizar sin conocimiento del usuario



Correos

- Análisis de las cabeceras de los correos



The screenshot shows a web browser window displaying the raw header of an email. The address bar shows a URL from a live.com mail service. The header text includes various fields such as X-Message-Delivery, X-Message-Status, X-SID-FRA, X-SID-Result, X-AUTH-Result, X-Message-Info, Received, MIME-Version, Content-Type, From, To, Subject, Message-ID, X-OriginalArrivalTime, Date, and Return-Path. The email is from an alerts@live.com domain and was received on June 14, 2010.

```
http://coll5w.col115.mail.live.com/mail/GetMes...
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTE7YT0xO0Q9NDtTQ0w9MA==
X-Message-Status: n:0
X-SID-FRA: =?utf-8?B?V2luZG93cyBMaXZlIEFsZXJ0cyBkZSBXaW5kb3dzIEExpdmU=? <alerts@live.com>
X-SID-Result: Pass
X-AUTH-Result: PASS
X-Message-Info: msQ7d/6wosIAfu2sEc4NZ96OfbGT7n695GjC/FyO2UwLDmoNLbKV9uPj3ViqC13GLrqQYCjfgury3uHE+3bb/H2D7fs3enkm
Received: from by2acblnmb03.alerts.live.com ([207.46.117.165]) by bay0-mc2-f31.Bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675);
    Mon, 14 Jun 2010 13:20:19 -0700
Received: from mail pickup service by by2acblnmb03.alerts.live.com with Microsoft SMTPSVC;
    Mon, 14 Jun 2010 13:20:16 -0700
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_NextPart_003_01BF1514.8D5BF46A"
From: =?utf-8?B?V2luZG93cyBMaXZlIEFsZXJ0cyBkZSBXaW5kb3dzIEExpdmU=? <alerts@live.com>
To: marcxp@hotmail.com
Subject: =?utf-8?B?RmluYWxpem8gZWwgcGFydG1kby4g?=
    =?utf-8?B?SXRhbg1hIDEgLSBQYXJhZ3VheSAx?=>
Message-ID: <BY2ACBLNMB03WLTJQm01ea76e08by2acblnmb03.alerts.live.com>
X-OriginalArrivalTime: 14 Jun 2010 20:20:16.0773 (UTC) FILETIME=[00C5F350:01CB0BFF]
Date: 14 Jun 2010 13:20:16 -0700
Return-Path: alerts@live.com
```

- Análisis estadísticos del contenido de los mails

Correos

- Protección
 - Uso de cifrado en los correos (gpg y enigmail)
 - Buscar servidores mas comprometidos



RASTOS LOCALES

Metadatos

- Datos dentro de los ficheros
 - Fecha creación
 - Dispositivo que lo creó
 - Información de quien lo creó
 - Posibles dispositivos cercanos (recursos red...)



RASTOS LOCALES

Metadatos

- Ejemplos de problemas:
 - Las imagenes (exif) guardan una miniatura de la imagen grande, si tratas la grande la pequeña no
 - Cartas de queja con el nombre y apellidos de quien la originó



PARTICIPANTES ACTIVOS

Empresas

- Gamma internacional Tecnología espía que permitía al gobierno infectar computadoras objetivo para monitorear conversaciones de los usuarios.
- Hacking team da acceso a las autoridades a través de sus productos a los equipos y teléfonos inteligentes, activar micrófonos, realizar fotos por cámaras. Enviar imágenes, mails, contraseñas para su posterior inspección.



Anecdotas

- Experimentos Universidad Carnegie Mellon
 - **5000** fotos perfil citas anónimas vs **280.000** que se encuentra en la búsqueda de perfiles Facebook. Resultado **500** de identificaciones positivas
 - **93** fotos webcam voluntarios vs **250.000** facebook Resultado **31** de identificaciones positivas
 - Cruce de datos publicos de los voluntarios vs perfiles facebook. Resultado **1** afición y casos de **5** primeros dígitos S.S.



Anecdotas

- Jerry Lucas, presidente de la compañía detrás de ISS World, opina que Gamma Internacional y Hacking Team deberían ser capaces de vender esta tecnología a cualquiera que así lo desee “La vigilancia que ofrecemos en nuestras conferencias está disponible para cualquier país del mundo. ¿Qué algunos países utilizan esta tecnología para suprimir principios políticos? Sí, yo diría que probablemente sí. Pero ¿quiénes son los proveedores para decir que la tecnología está siendo utilizado para el bien o para el mal?”



Anécdotas

- Peticiones de datos de usuarios realizada a google publicado en su último informe.
 - 5.950 EEUU
 - 1.739 Francia
 - 1.273 Reino Unido
 - 1.060 Alemania
- Para nada los países que se esperan como sospechosos habituales



PARTICIPANTES ACTIVOS

Anécdotas

- ISS WORLD (Inteligencia de Soporte de Sistemas) reunión de los gobiernos de todo el mundo para discutir como aprovechar la tecnología a favor de una vigilancia mas estricta para los ciudadanos.
- Se realizan varias al año por todos los continentes



Anécdotas

- Algunas de las 63 charlas ISS world latinoamerica:
- Amenazas de Redes Sociales: Desafíos y Soluciones para la Monitorización de Comunicación y Análisis de Inteligencia
- SMS, ¡Fuente Olvidada de Inteligencia!
- Voz Biométrica- Identificación de Orador en Investigaciones Penales e Inteligencia
- Cómo Extraer Datos de un Teléfono que sea bloqueado y protegido con PIN usando un XRY de Micro Systemation



Anécdotas

- Un Sistema Furtivo Basado en Spyware para Atacar, Infectar y Monitorizar Computadoras y Smartphones
- Búsqueda-Cruzada Eficiente en la Inteligencia de Múltiples Fuentes
- Análisis de Patrones Comunicativos – Detectar lo que sus blancos están intentando esconder
- Intrusión Gubernamental IT: Técnicas Aplicadas de Hacking usadas por Agencias Gubernamentales



¡Yo no tengo nada que ocultar!



GRACIAS POR VUESTRA ATENCIÓN

red@nosoloaulas.com



Anexos (Herramientas)

- Wlanreaver
<http://mir.cr/ZPSMOGQH>
- Wlan Decrypter
<http://www.seguridadwireless.net/archivos/wlandecrypter-1.3.2.tar.gz>
- Jazztel decrypter
<http://www.box.com/shared/rsbhautkoy>
- Wifiway
<http://www.wifiway.org/>
- Cain & abel
<http://www.oxid.it/cain.html>
- Sslstrip
<http://www.thoughtcrime.org/software/sslstrip/>



Anexos (Herramientas)

- Suricata

<http://www.openinfosecfoundation.org/index.php/download-suricata>

- Aircrack-ng

<http://home.comcast.net/~jay.deboer/aircrack-ng/download.html>

- Gpg

<http://www.gnupg.org/>

- Enigmail

<http://enigmail.mozdev.org/home/index.php.html>



Anexos (Extensiones)

- Https everywhere
<https://www.eff.org/files/https-everywhere-1.2.2.xpi>
- Objection
http://downloads.mozdev.org/objection/objection-0_3_5-fx.xpi
- Cookie monster
<https://addons.mozilla.org/firefox/downloads/latest/4703/addon-4703-latest.xpi?src=dp-btn-primary>
- Better privacy
<https://addons.mozilla.org/firefox/downloads/latest/6623/addon-6623-latest.xpi?src=cb-dl-popular>
- Googlesharing
<http://www.googlesharing.net/download.html>
- TrackMeNot
<https://addons.mozilla.org/firefox/downloads/latest/3173/addon-3173-latest.xpi?src=dp-btn-primary>



Anexos

- Documetal los "Secretos" de Google Y Facebook
<https://www.youtube.com/watch?v=wGq3HWILr6k>
- Algunas paginas para mantenerse informado:
 - <http://www.xombra.com>
 - <http://www.securitybydefault.com/>
 - <http://unaaldia.hispasec.com/>

