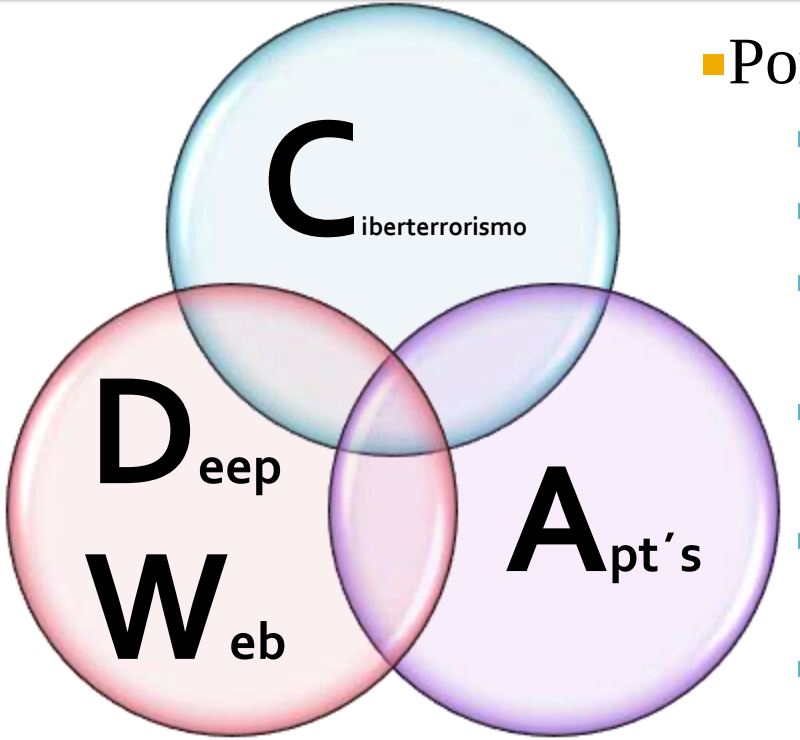
Evil 3 full analisys Ciberterrorismo, advanced persistence treats (apt´s) & DEEP WEB

Actualización técnica que incluye un análisis profundo de las tres amenazas más peligrosas del 2016, panorama de la situación actual sobre ciberdelitos, hacktivismo, ciberguerras; los ataques actuales y los ataques de siempre.

¿Porqué Ciberterrorismo +Deep web + Apt´s?



- Porque son los tres más:
  - Intrusivos
  - Destructivos
  - Frecuentes (Estadísticas de los principales ataques)
  - Organizados (Grupos masivos, Gobiernos reclutando)
  - Desarrollados técnicamente (malware+hardware+hackers)
  - Mediáticos:

Evil 3 - News

Operación TEMPORA deja a la NSA como niños en el parque.

Los Britanicos tenían su propia operación de espionaje y ya habían

PENTÁGONO 12 ENERO 2015

ISIS hackeó las cuentas de Twitter y YouTube d

entral de

base militar estadounidense

microblogging dio de baja

El director del FBI acusó a China de hackear compañías de EEUU

Anonymous publica 2.500 cuentas de

Islámico

El colectivo de hackers enmarcado e

GOOGLE Y OTRAS 34 COMPAÑÍAS SUFRIERON ROBO DE INFO

"Operación Aurora", el ciber

Se muda el Estado Islámico a la Deep Web

19 noviembre, 2015 | 3:58 pm

Agencias | NorteDigital

Tras las amenazas de Anonymous, el grupo terrorista empezó a tomar medidas preventivas y mudó sus operaciones cibernéticas a la red Tor

Robar dinero en Int

¿CUÁNT

UNA TARJETA DE CRÉDITO ROBADA?

PR Newswire

The Advanced I

Expected to Gro

Billion by 2020

DUBLIN, Dec. 01, 2015 /PR

Research and Markets (http

addition of the "Advanced P

offering.

Over the past decade, adva

unsophisticated malware att

solution such as SIEM, next

years.

Israel y EEUU crearon el virus que dañó el programa nuclear iraní

gusano Stuxn

Muchos comentarios en la prensa y silencio absoluto

supuesto, de los servicios secretos israelíes (Mosad)

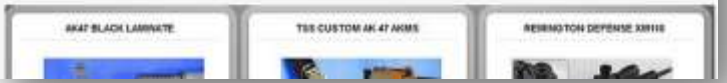
información publicada por el diario 'The New York T

Israel y Estados Unidos como los responsables del vi

ha dañado y retrasado el programa nuclear iraní.

Kalashnikov desde casa

Una muestra de armamento en venta en la DeepWeb Guns Store. Un bitcoin se cambia por unos 305€



Deep web

Más allá del contenido que está al alcance de los buscadores tradicionales, hay una red global profunda 500 veces más grande; controversia por los mercados ilegales y la circulación de bitcoins

1- Advanced persistence treats

- Definiciones
- Objetivos
- Ciclo de vida
- Análisis técnico casos reales
- Conclusiones

1

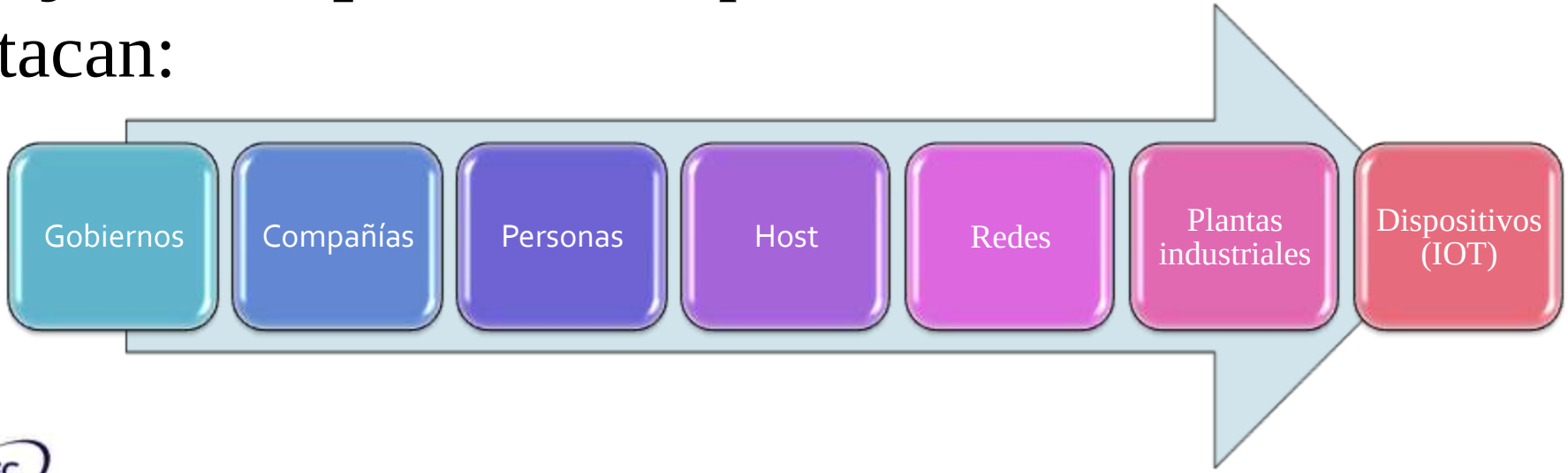
1- APT - Definiciones

- Advanced persistent threat=>**Malware**
- APT=>**Malware+avanzado** (programadores poseen skills avanzados en ataques, experiencia más conocimiento)
- APT=>**Malware+avanzado+persistente** (queda latente monitoreando hasta ciertas circunstancias)
- APT=>**Malware+avanzado+persistente+amenaza** (objetivos bien claros con ataques dirigidos y organizados)

APTs are lions wearing insider sheep's clothing, (Fuente: Vormetric para Infosecurity 2016 - Santo Domingo)

1- APT - Objetivos

- No infectan de forma aleatoria sino **que tienen objetivos específicos,** dependiendo del malware atacan:



1- APT – Ciclo de vida

- Algunos ejemplos: theflame, stuxnet, medre, nettraveler, aurora, duqu, cosmicduke, finspy, hacking team rcs, machete, redoctober, ice fog, cozyduke, black energy, animl farm, kimsuky, regin, the mask, desert falcons…
- **Sería imposible analizar todos** pero hay algunos denominadores en común, todos cumplen con ciertas tareas o etapas **–ciclo de vida-**

1- APT – Ciclo de vida

1. PLANIFICACIÓN & RECONOCIMIENTO
2. DESARROLLO DE MALWARE
3. INFECCION
4. OCULTAMIENTO Y PROPAGACION
5. ATAQUE Y CONSOLIDACION
6. BORRADO DE RASTRO O AUTODESTRUCCIÓN

¿a qué se parece?

1- APT – Análisis técnico casos reales

- Caso #1: NetTraveler
  - Objetivo: **Espionaje**
  - Víctimas dirigidas: **350 víctimas de alto perfil en 40 Estados Nacionales** (agencias de gobierno, diplomáticos, contratista de las fuerzas armadas) específicamente activistas tibetanos y uigures, compañías petroleras, centros e institutos de investigación científica, compañías privadas, gobiernos e instituciones gubernamentales, embajadas y contratistas del ejército

1- APT – Análisis técnico casos reales

- Caso #1: NetTraveler (cont…)
  - Método de Infección: **spear-phishing** con adjuntos infectados (distintos idiomas, sectores, regiones)
  - Vulnerabilidades explotadas:
    - CVE-2010-3333: Microsoft Office Could Allow **Remote Code Execution**
    - CVE-2012-0158: Microsoft Windows Common Controls ActiveX Control **Remote Code Execution**

1- APT – Análisis técnico casos reales

- Caso #1: NetTraveler (cont…)
  - Comportamiento **similar a todo malware**: Se carga en memoria modificando y agregando datos en registros, librerías del sistema operativo, etc..
  - ¿Cómo persiste?, lanza **múltiples ataques**:
    - Instala Backdoors
    - Fuga de documentos office, pdf, corel, autocad, configuración
    - Instala keyloggers
    - Modifica parámetros y archivos del sistema operativo
    - Genera conexiones externas protegidas (VPN), envía archivos recogidos vía http y ftp

1- APT – Análisis técnico casos reales

- Caso #2: Stuxnet
  - Objetivo: **Sabotaje**
  - Víctimas dirigidas: Este malware fue diseñado para infectar a equipos Windows y afectar a únicamente a **sistemas SCADA**, infraestructuras industriales controladas con el software **WinCC (Siemens).**

1- APT – Análisis técnico casos reales

- Caso #2: Stuxnet (cont…)
  - Método de Infección: vulnerabilidad de **auto-ejecución de archivos** en dispositivos de almacenamiento USB. Luego ampliaba sus capacidades a **worm** -gusano- al propagarse en distintos medios del sistema scada.
  - Vulnerabilidades expotadas: dos vulnerabilidades **0day de windows**; cola de impresión & file share server.

1- APT – Análisis técnico casos reales

- Caso #2: Stuxnet (cont…)
  - ¿Cómo persiste?, lanza distintos ataques:
    - Se autoejecuta y autopropaga (**worm**).
    - Aprovecha las dos vulnerabilidades 0 day de wincc **para escalar privilegios** en los equipos infectados. (https://en.wikipedia.org/wiki/WinCC)
    - Se **actualiza** a través de p2p. (botnets p2p!: https://en.wikipedia.org/wiki/Gameover_ZeuS, https://en.wikipedia.org/wiki/ZeroAccess_botnet)
    - **Muta su código** agregando nuevas funcionalidades o métodos de evasión.
    - Utiliza **rootkits firmados digitalmente** para evadir antivirus.

1- APT – Conclusiones

USUARIOS

- Escanear archivos antes de abrirlos, desconfiar de orígenes desconocidos.
- Actualización de SO, antivirus, anti…
- Todas las recomendadas para evitar malware

IT & IS

- Auditar conexiones (Firewall) especialmente en perímetros externos.
- Auditar privilegios de acceso a recursos, servidores, etc.
- Analizar los logs de los IDS buscando comportamientos anómalos de host.
- Captura de paquetes en busca de tráfico anómalo.
- Pentest + estrategias de defensa.

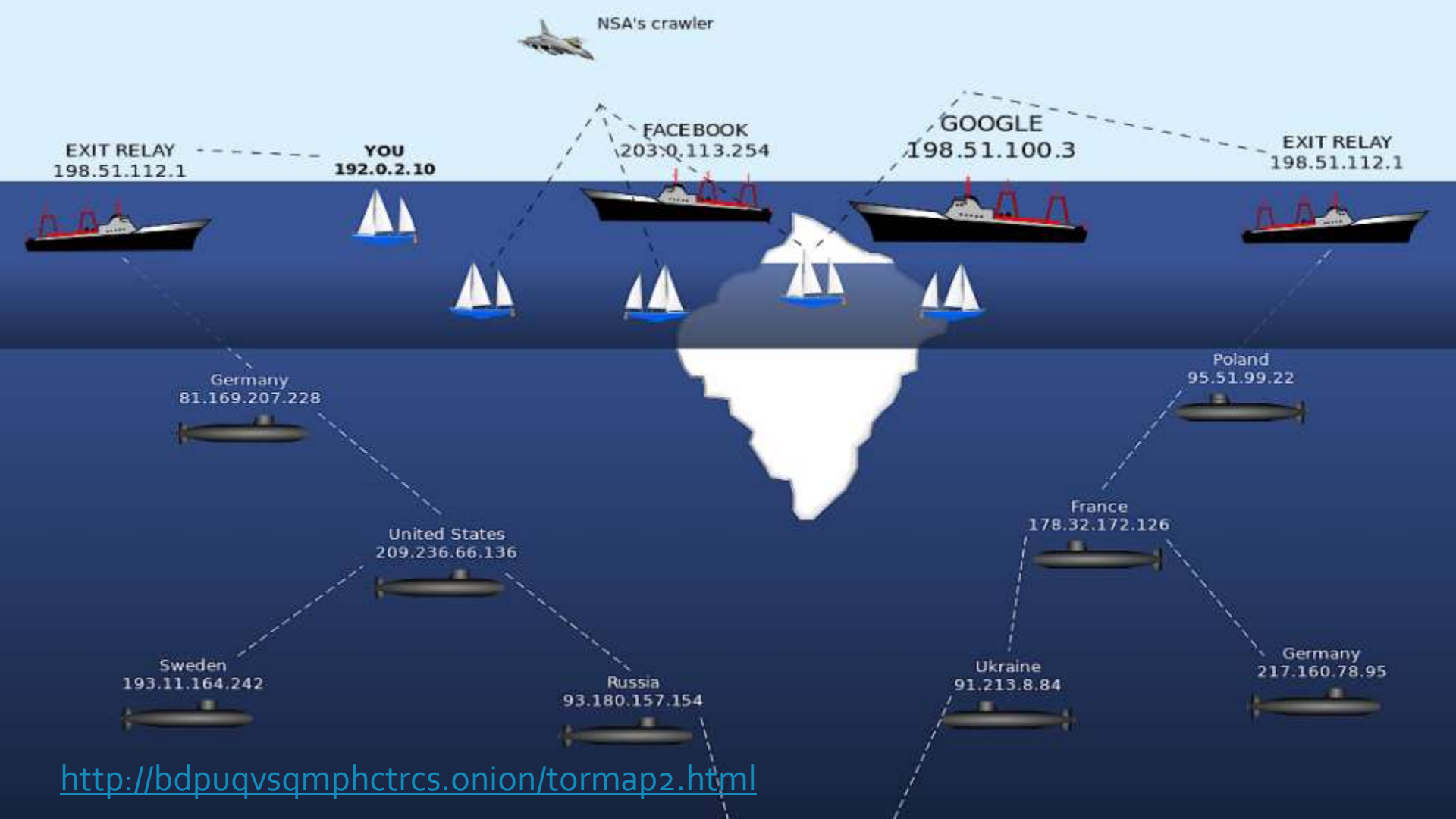
2 - Deep web

- Deepweb (internet profunda)
- Invisible Web (internet invisible)
- Deep Web (internet profunda)
- Dark Web (internet oscura)
- Hidden Web (internet oculta)

2

2 - Deep web

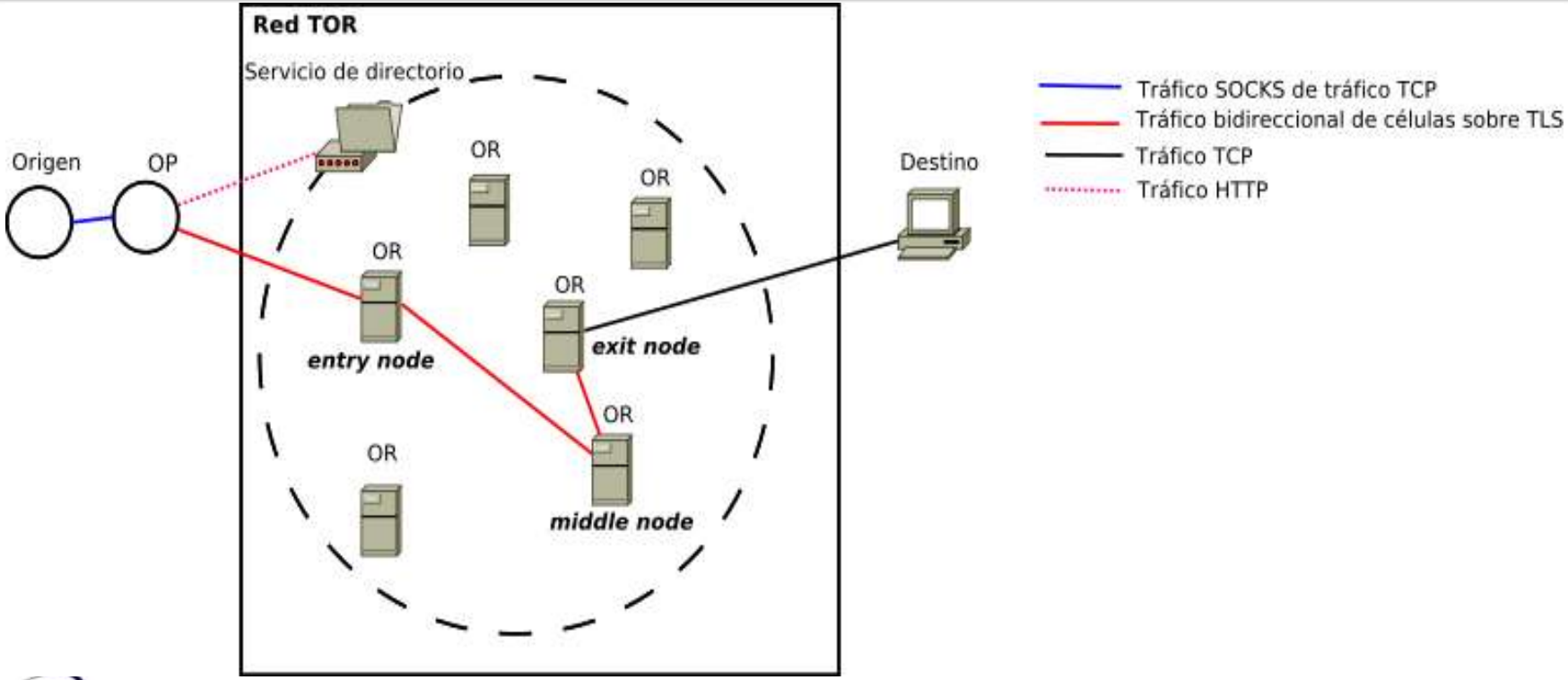
- Se conoce así a **todo el contenido de internet que no forma parte de la internet superficial**, es decir, de las páginas indexadas por las redes de los motores de búsqueda de la red.
- La mayor parte de la información encontrada en la internet profunda está en sitios **generados dinámicamente** y para los motores de búsqueda tradicionales es difícil hallarla.
- Es un **refugio para la delincuencia** debido al contenido ilícito que se encuentra en ella (Wikipedia)


NSA's crawler
EXIT RELAY
198.51.112.1
YOU
192.0.2.10
FACEBOOK
203.0.113.254
GOOGLE
198.51.100.3
EXIT RELAY
198.51.112.1
Germany
81.169.207.228
Poland
95.51.99.22
United States
209.236.66.136
France
178.32.172.126
Sweden
193.11.164.242
Russia
93.180.157.154
Ukraine
91.213.8.84
Germany
217.160.78.95
http://bdpuqvsqmphctrcs.onion/tormap2.html

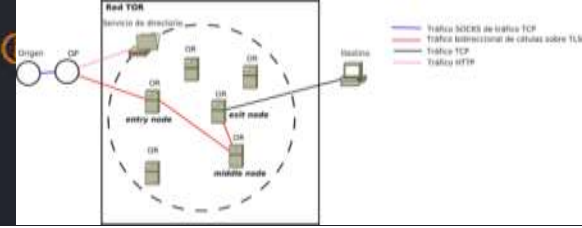
2 - Deep web - TOR

- Tor propone el uso de **encaminamiento de cebolla** de forma que los mensajes viajen desde el origen al destino a través de una **serie de routers especiales llamados 'routers de cebolla'** (en inglés onion routers)
- Proxy + cifrado + web hosting dinámicas
- Tor cifra la información a su entrada y la descifra a la salida de dicha red. (en los extremos qué ocurre?)
- https://www.torproject.org/
- https://check.torproject.org/?lang=es_ES

2 - Deep web - TOR



2 - Deep web - TOR



- **Web Servers**: Existen servicios que **ocultan la localización (por ejemplo, la dirección IP) de quien provee el servicio** (Ej. un servicio web accesible sólo desde la red de encaminamiento de cebolla).
- **Nodos OR o simplemente OR** (del inglés *Onion Router*): Funcionan como **encaminadores** y en algunos casos además como servidores de directorio (DNS) de una especie de servicio de mantenimiento.
- **Nodos OP o simplemente OP** (del inglés *Onion Proxy*): Los usuarios finales ejecutan un **software local que hace la función de nodo OP** y que su función es obtener información del servicio de directorio, establecer circuitos aleatorios a través de la red y manejar conexiones de aplicaciones del usuario.
- El **servicio de directorio** publica una base de datos que asocia a cada OR. Fuente Wikipedia

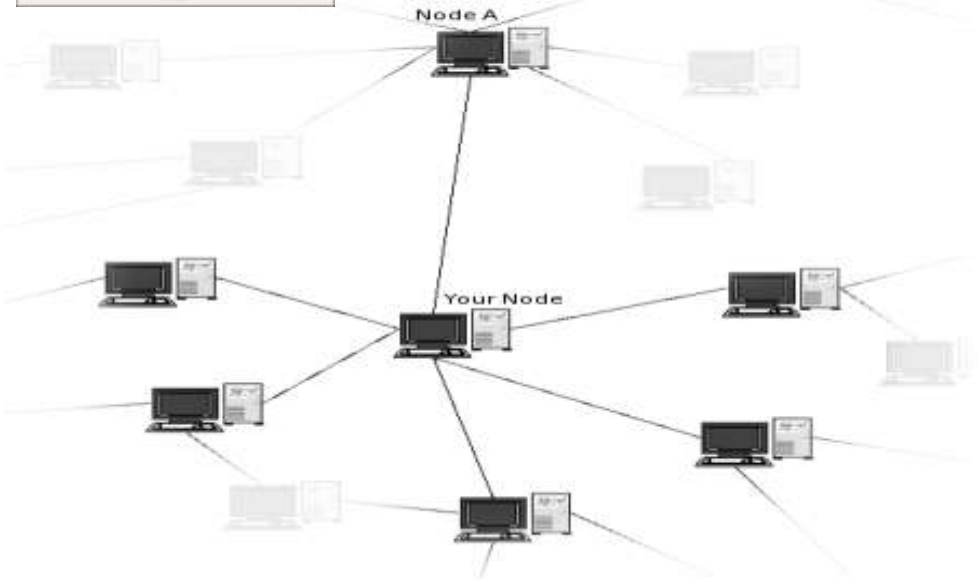
2 - Deep web - requisitos

https://check.torproject.org/?lang=es_ES

https://www.torproject.org/

2 - Deep web - requisitos

Freenet



https://freenetproject.org/index.html#home

I2P

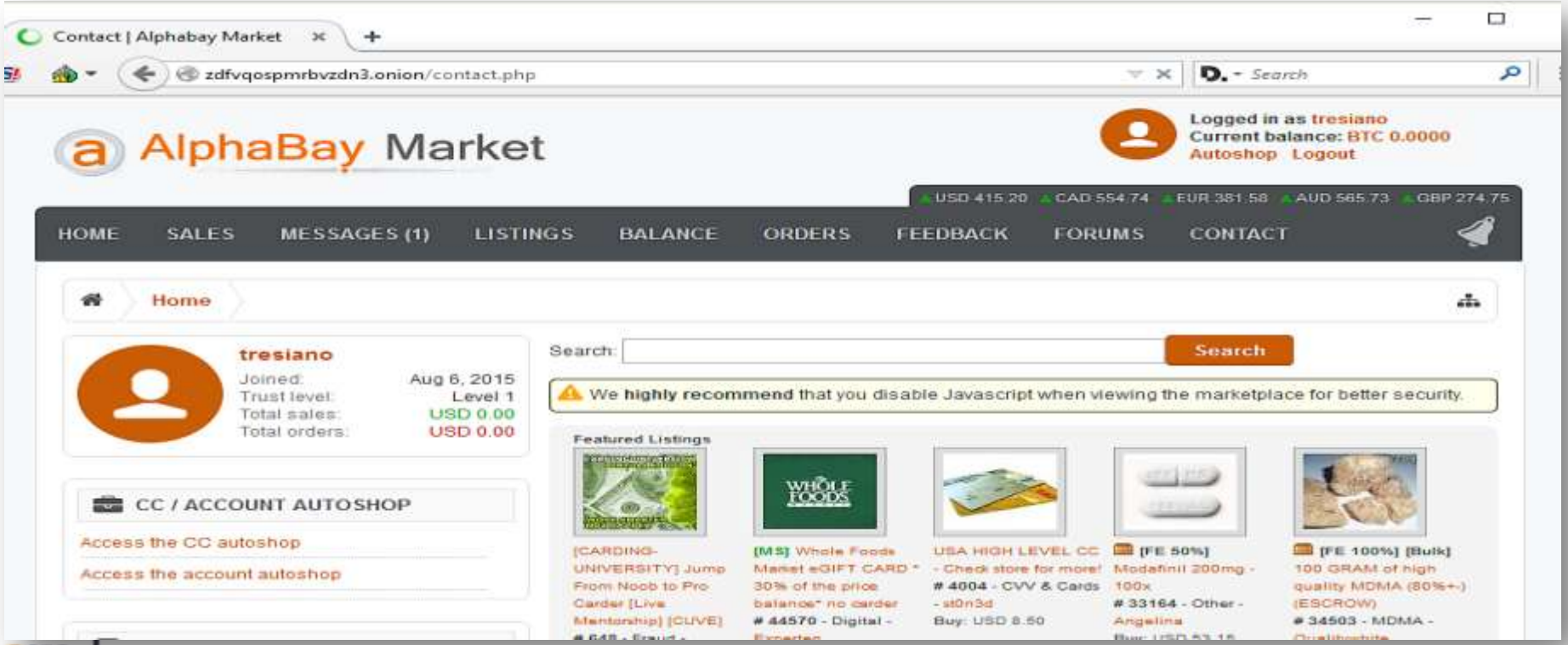
https://geti2p.net/es/

http://mainstreamlos.blogspot.fr/search?updated-min=2015-01-01t00:00:00%2B01:00&updated-max=2016-01-01t00:00:00%2B01:00&max-results=50

2 - Deep web - ¿qué hay?

- Mensajería anónima o protegida:
  - Swiss email
  - Anonymous E-mail service
  - SMS4TOR – Self destructing messages
  - NoteBin – Create encrypted self-destructing notes
  - [TorBox] The Tor Mail Box
- Algunos mercados electrónicos de artículos prohibidos:
  - Tor Market Board – Anonymous Marketplace Forums
  - UK Guns and Ammo
  - AlphaBay
  - Hidden BetCoin
  - Project Evil

2 - Deep web – Caso alphabay



2 - Deep web

- ¿qué hay?

BlackShades RAT 5.5.1 + User Guide

Item # 22902 - Botnets & Malware / Botnets & Malware - shonajaan (5524)

Views: 10688 / **Bids:** Fixed price

Quantity left: Unlimited (2121 automatic items)

Office Exploit Builder v3

Office Exploit Builder v3 cracked

Sold by AGENT3500ZERO - *21* sold since *Jul 4, 2015* Vendor Level 2 Trust Level 4

42 items available for auto-dispatch

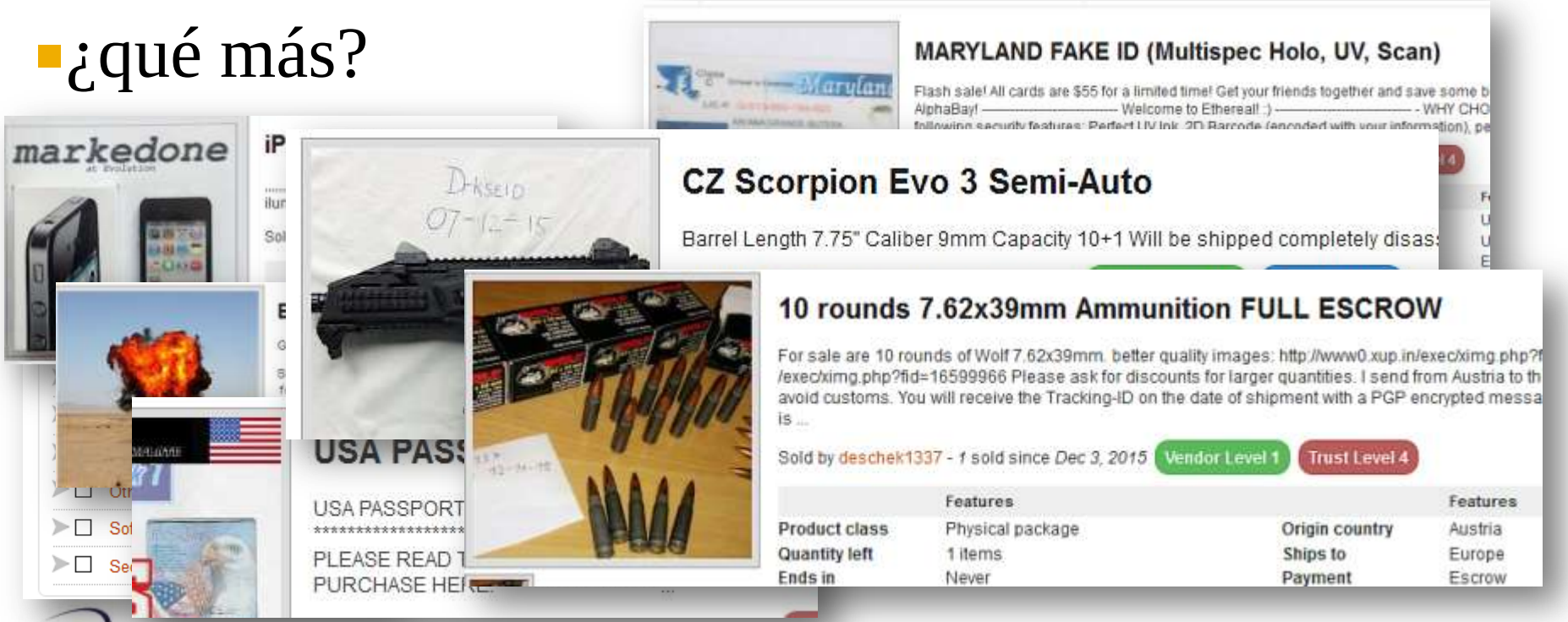
	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Views: 10207 / **Bids:** Fixed price

Quantity left: Unlimited

2 - Deep web

- ¿qué más?



2 - Deep web

- http://oasisnvwltxvmqqz.onion/welcome
- http://oasisnvwltxvmqqz.onion/64

- rolear en argentina: http://oxwugzccvk3dk6tj.onion/argentina/catalog.html
- listador parazite: http://kpynyvym6xqi7wz2.onion/links.html
- Listador yas: http://bdpuqvsqmphctrcs.onion/

2 - Deep web

- HANSA LINK: http://hansamkt2rr6nfg3.onion/affiliate/894
- AlphaBay Link: http://pwoah7foa6au2pul.onion/affiliate.php?ref=outraged
- Valhalla Link: http://valhallaxmn3fydu.onion/register/SWuR
- Dream Link: http://lchudifyeqm4ldjj.onion/?ai=71553

2 - Deep web – Caso alphabay

- Diferentes protecciones

2 - Deep web – Conclusiones

- **Medios de Pago**:
  - **Bitcoins** en principio, después con las mismas **tarjetas clonadas** vendidas ahí o cualquier otras formas de pago digitales que no puedan ser rastreados (cuentas mulas).
- **Expedición de los objetos vendidos**:
  - Se despachan en los **depósitos de correos de origen** y los retiros se realizan en los depósitos de **los correos de destino,** en algunos casos se reciben en los domicilios.
- **Análisis Delictual:**
  - Son **delitos difíciles de rastrear** y más difícil aún de generar **el valor probatorio** para iniciar una demanda penal.
  - Las policías, las judicaturas **no están preparadas** todavía.
  - Todo esto se complica más **si el delito es transnacional:** pornografía infantil y jailbait, publicación de delitos en vivo homicidios, suicidios, violaciones, ejecuciones.

2 - Deep web – Caso Skypetorsion

- **Hecho:** ABR 2016, usuario desprevenido realiza video conferencia hot con una persona (skype/wapp/face), luego de varias sesiones, recibe muestreo de los videos por diferentes medios (mail, sms, llamadas telefónicas) distintos a los utilizados y comienza extorsión -amenazas de publicar videos, de enviárselos a familiares y conocidos, etc.- pidiendo un pago a través de western union a cuentas de costa de marfil.

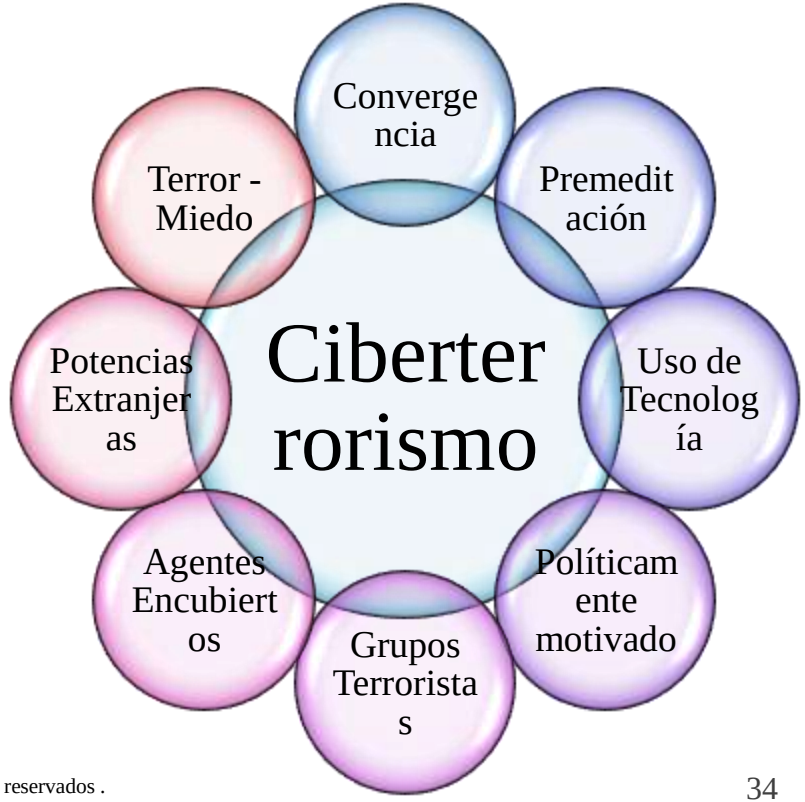
3 - Ciberterrorismo

- Naturaleza y Motivaciones
- Análisis técnico de los ataques:
  - Tecnologías
  - Métodos
  - Víctimas - Objetivos
- Recomendaciones

3 – Ciberterrorismo - Naturaleza

¿de qué estamos hablando? Definiciones:

- **Convergencia** del ciberespacio con el terrorismo. (Barry Collin - Institute for Security and Intelligence/USA)
- Ataque **premeditado** y **políticamente motivado** contra información, sistemas, programas y datos informatizados no combatientes, **por parte de grupos terroristas o agentes encubiertos de potencias extranjeras**. (Mark Pollit – FBI/USA)
- Uso de **medios de tecnologías** de información, comunicación, informática, electrónica o similar con el propósito de **generar terror o miedo generalizado** en una población, clase dirigente o gobierno. (Wikipedia) https://en.wikipedia.org/wiki/Cyberterrorism



3 – Ciberterrorismo - Naturaleza

Actores del Ciberterrorismo

- **Terroristas**: grupos terroristas; ETA, ISIS, FARC, HAMAS, IRA…
- **Estados Nacionales**: USA, China, Rusia, Alemania, Francia, Inglaterra…
- **Hacktivistas**: Anonymous, Lulzec…
- **Ciberdelincuentes**: Phishers, crackers, spammers…
- **Hackers profesionales**

3 – Ciberterrorismo - Motivaciones

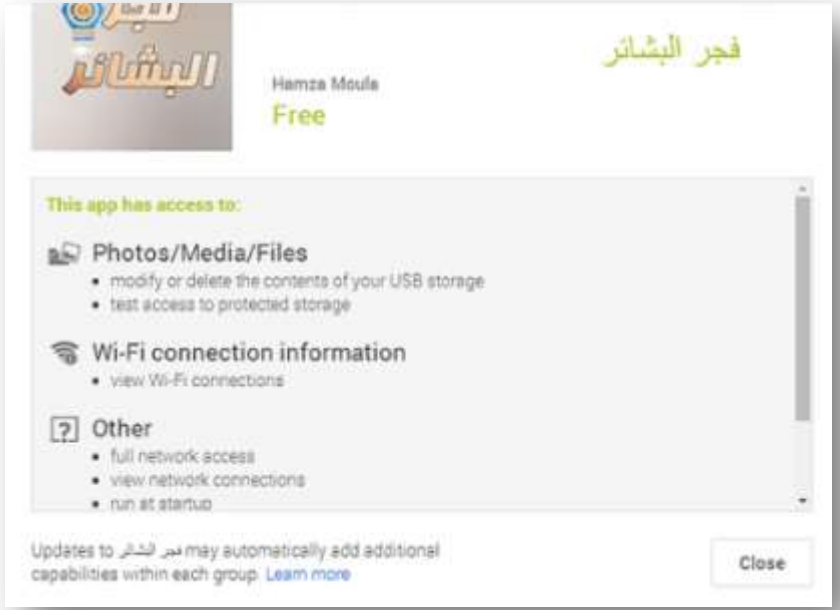
- **Terroristas**: Reclutamiento + Propaganda + Financiación + Comunicaciones
- **Estados Nacionales**: Inteligencia + Espionaje + Sabotaje
- **Hacktivistas**: Propaganda
- **Ciberdelincuentes**: $$$$ - Beneficios económicos.
- **Hackers**: $$$$ - lo mismo pero para los gobiernos!

3 – Ciberterrorismo - Análisis técnico de los ataques

Tecnologías utilizadas por TERRORISTAS:

- Uso de **criptografía** para las comunicaciones principalmente Telegram y Snapchat - aplicaciones de mensajería instantánea.
- Protegen con **cifrado y esteganografía los activos digitales** (comunicaciones, archivos, etc.)
- **Borrado de rastros**, con Snapchat los mensajes se eliminan, transmiten fotos y videos de todo tipo.
- **Propaganda y Reclutamiento**: desarrollaron una estrategia a través de Redes Sociales Públicas; ej: Twitter usan app The Dawn of Glad Tidings

3 – Ciberterrorismo - Análisis técnico de los ataques



- Tecnologías utilizadas por **TERRORISTAS**:

#1 CASO DAWN

- The Dawn of Glad Tidings (Twitter app)
- De la misma forma que el **mobile malware,** se publican app´s en los appstores mas populares.
- Las app´s instaladas **recolectan información privada** y configuran el móvil con **permisos no requeridos e innecesarios** para el juego.
- Resultado: info para reclutamiento + botnet

3 – Ciberterrorismo - Análisis técnico de los ataques

- Tecnologías utilizadas por **TERRORISTAS**:

#1 CASO DAWN (cont…)

- Posterior al signup comienza a **enviar tuits** en la cuenta del usuario como **propaganda**
- **Links, hashtags e imágenes** son tuiteadas por **todos los usuarios infectados a la vez** por lo que se convierte en tuit viral
- Por ejemplo en la invasión de ISIS a Mosul se realizaron al **menos 40k tuits con este contenido:**

3 – Ciberterrorismo - Análisis técnico de los ataques

Otras Tecnologías utilizadas por **TERORISTAS**: intentan tercerizar actividades a usuarios distraídos, cuentas comprometidas o pagan por malware:

- Incluyen **campañas organizadas de hashtags** en los que **utilizan a sus seguidores** y **sus usuarios comprometidos** a través de **botnets** para viralizar las campañas multiplicando sus tuits en un promedio de 70 retuits por cada tuit.
- Incluyen **cuentas árabes populares como @ActiveHashtags** para promover sus tuits.
- Copian **técnicas de marketing:** por ejemplo hashtag #CatsOfJihad los combatientes subieron a las redes sociales fotografías de sus mascotas junto a rifles, pistolas o incluso granadas, afirmando que compartían con ellos su afición por asesinar infieles.
- **Contratan hacktivistas y Ciberdelincuentes** para propaganda / reclutamiento online

3 – Ciberterrorismo - Análisis técnico de los ataques

Tecnologías utilizadas por **Estados Nacionales**:

- **Espionaje** a través de las comunicaciones digitales: PRISM/TEMPORA (gracias Snowden!)
- **Sabotaje** con Código Malware para sistemas scada - Supervisory Control and Data Acquisition / Siemens - para **atacar infraestructuras:**
  - control de oleoductos
  - plataformas petroleras
  - centrales eléctricas
  - centrales nucleares
  - instalaciones industriales.
- Directamente **contratan hackers.** (algunos hasta con antecedentes penales)

Tecnologías utilizadas por Estados Nacionales: #1 Caso PRISM (cont…)

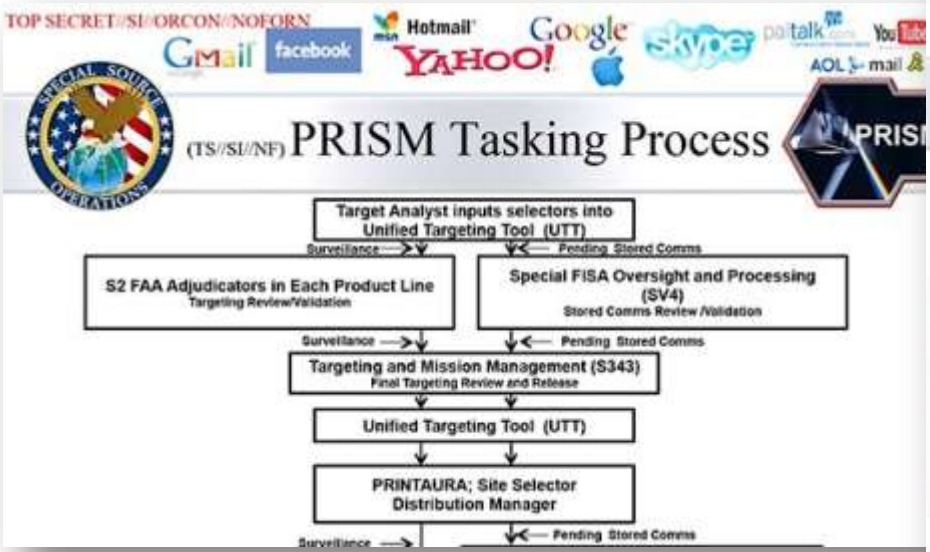
- PRISM es un programa de **vigilancia electrónica** considerado confidencial a cargo de la Agencia de Seguridad Nacional (**NSA**) de los Estados Unidos desde el 2007.
- El alcance de PRISM es tan grande que incluso los Estados Unidos podría haber **espiado a más de 35 líderes mundiales.**
- Se emplea como un medio para la vigilancia a fondo de las comunicaciones y otros datos almacenados: registros obtenidos de **dispositivos de voz, texto, vídeo y datos**
- Las **fuentes emplean grandes compañías de como Microsoft, Google, Apple y Facebook que entregan acceso a esa información**.

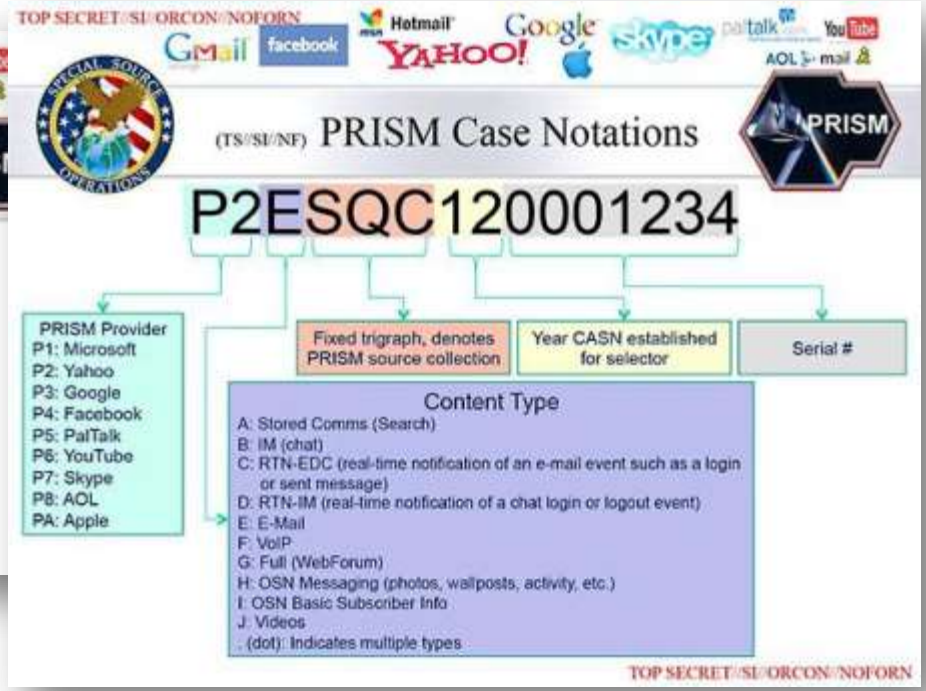
Tecnologías utilizadas por Estados Nacionales: #1 **Caso PRISM (cont…)**

- El programa tiene como objetivos **a aquellos ciudadanos que vivan fuera de Estados Unidos**, aunque también se incluyen a **los ciudadanos estadounidenses** que hayan **mantenido contactos con personas que habitan fuera de las fronteras** del país.
- 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**.

3 – Ciberterrorismo - Análisis técnico de los ataques

- Tecnologías utilizadas por Estados Nacionales: **#1 Caso PRISM**





Tecnologías utilizadas por **Estados Nacionales**: #2

Código Malware para sistemas scada

- Supervisory Control and Data Acquisition -SCADA- para atacar infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales.
- Flame y Stuxnet (APT´s)

3 – Ciberterrorismo - Análisis técnico de los ataques

Tecnologías utilizadas por **Estados Nacionales**:

3 Directamente contratar hackers.

- El nombre del proyecto ultra secreto
podrán detectar en tiempo real cualqui
- El objetivo de este proyecto **-obtene**
opciones para los presidentes, actuar
servicio secreto NSA.

La ciberguerra que prepara el Pentágono

Johannes Schmitt-Tegge | 24 de Noviembre de 2015 | 12:00

El organismo de defensa estadounidense entrena a soldados para combatir en la "inmensidad digital de Internet". Se trata de un proyecto para la lucha contra los ataques de hackers a la red de computadoras del gobierno.

3 - Ciberterrorismo

Recomendaciones: Si bien no existen aplicaciones anti ciberguerras, o anti espionaje o anti ciberterrorismo; podemos evitar alguna de esas prácticas invasivas de la privacidad.

1. Proteger las comunicaciones de voz con herramientas como **Cryptophone, Blackphone.**
2. Proteger las comunicaciones escritas –chats- con **Telegram, Cryptocat, Wickr**.
3. Proteger las correos electrónicos con firma digital utilizando herramientas como **OpenGPG**, no sólo permite **autenticidad** sino que también otorga **confidencialidad a través de cifrado asimétrico.**

3 - Ciberterrorismo

4. Utilizar **servicios en la nube que permitan protocolos cifrados** o montar los servicios expuestos a internet a través de **VPN** – virtual private networks.
5. Para los casos de navegación anónima existen **proxys y navegadores que cifran la navegación** por ejemplo Tor.
6. Para evitar localizaciones **quitarle los metadatos a los archivos publicados** en internet por ejemplo imágenes, documentos que publican en sitios públicos, edes sociales, etc.
7. Recuerde que también se deben considerar todas estas medidas en los dispositivos móviles.

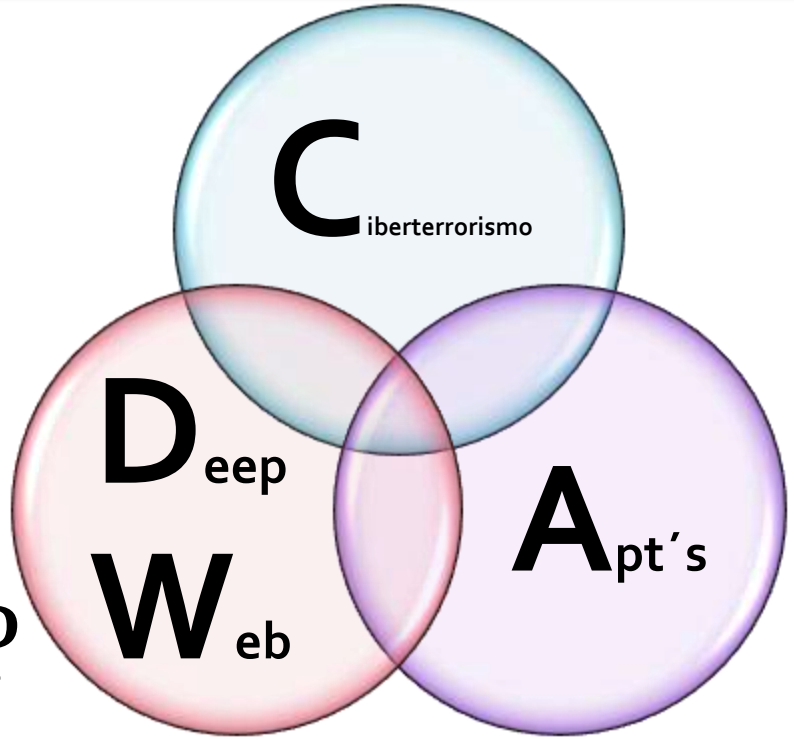
Conclusiones

Algunas Afirmaciones:

- Deep Web **permite** delitos de **distinto tipo**.
- Deep Web está “sospechosamente” **organizada y protegida.**
- En Deep Web se vende **malware** que es utilizado para **APT**.
- APT´s tienen estructuras “sospechosamente” que persiguen **metodologías similares a los estándares de seguridad.**
- Los estados nacionales **reconocieron haber utilizado apt´s para sabotajes y espionaje**.
- Los **terroristas contratan ciberdelincuentes y hacktivistas** que utilizan apt´s con malware comprado en deep web.
- Los **estados nacionales contratan hackers** que utilizan apt´s con malware comprado en deep web.

Ciberterrorismo +Deep web + Apt´s

- Estados
- Terroristas
- Hacktivistas
- Hackers
- Ciberdelincuentes, phishers, crackers, spammers…
- ¿existe sinergia?



- Gracias -

Christian Vila

christian.vila@isec-global.com
ISEC GLOBAL Inc.
www.isec-global.com