

Evil 3 full analysis

**Ciberterrorismo, ADVANCED
PERSISTENCE THREATS (APT'S) & DEEP
WEB**



OWASP

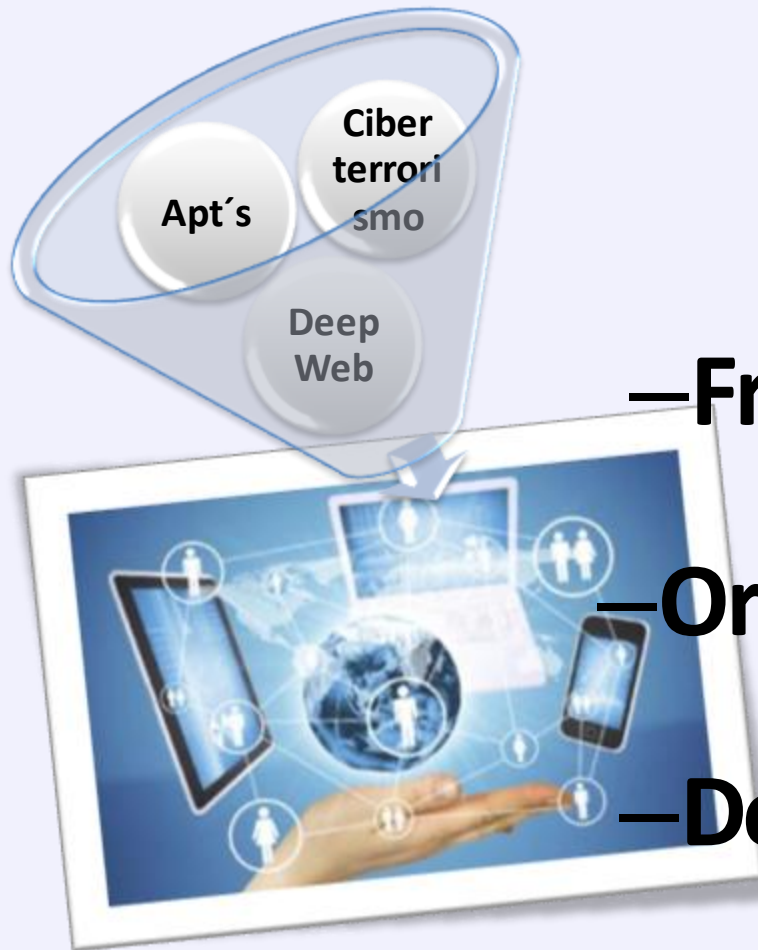
The Open Web Application Security Project



- Christian Vila



¿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:



OWASP

The Open Web Application Security Project

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

Los Británicos tenían su propia operación de espionaje y ya habían

PENTÁGONO 12 ENERO 2015

ISIS hackeó las cuentas de Twitter y YouTube

central

ase militar estadou
microblogging dio de baja la cuenta

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

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

[Anonymous publica 2.500 cuentas de Twitter vinculadas al Ejército Islámico](#)

El colectivo
hacer pút
prometido
acontecido

del robo de secretos. "Son

GOOGLE Y OTRAS 34 COMPAÑÍAS SUFRIERON ROBO DE INFORMACIÓN

"Operación Aurora", el ciberataque más sofisticado de la historia

El hackeo involucró a Microsoft, a través del Internet Explorer, y al gobierno de donde se creó salió parte del problema.

Robar dinero en Internet es muy barato

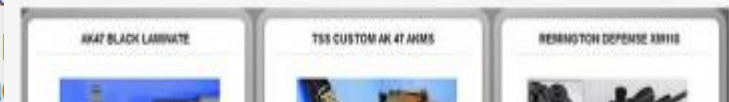
¿CUÁNTO CUESTA EN LA DEEP WEB UNA TARJETA DE CRÉDITO ROBADA?

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

Deep Web: Comprar un Kalashnikov desde casa

S COM
sto, de
ación
y Esta
lado y retrasado el programa nuclear iraní.

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



Deep web: el universo paralelo de Internet

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

- Advanced persistent threat=> **Malware**
- APT=> **Malware+avanzado** (programadores poseen skills avanzados en ataques: **experiencia más conocimiento**)
- APT=> **Malware+avanzado+persistente** (ataque que persiste **quedando latente y monitoreando** hasta que se cumplan 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)



- No infectan de forma aleatoria sino **que tienen objetivos específicos:**
 - Gobiernos
 - Compañías
 - Personas
 - Host
 - Redes
 - Plantas industriales
 - Dispositivos (IOT)



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

1- APT, análisis técnico casos reales

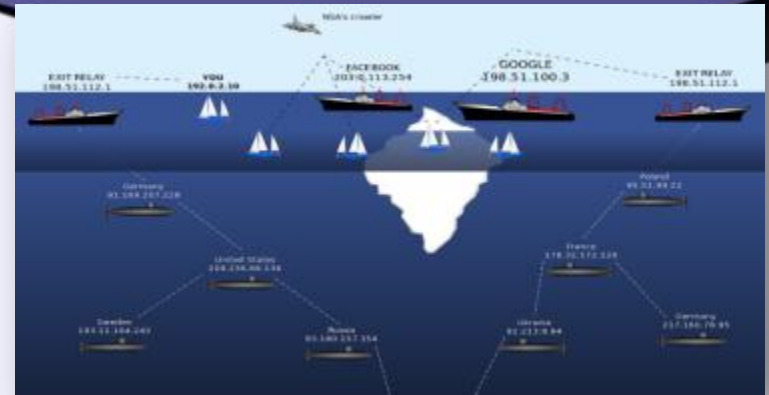


- **Caso NetTraveler**
 - Objetivo: **Espionaje**
 - Víctimas dirigidas: **350** víctimas de alto perfil en **40** Gobiernos (agencias de gobierno, diplomáticos, contratista de las fuerzas armadas) específicamente activistas tibetanos y uigures, compañías petroleras, centros e institutos de investigación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



- Caso **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 (RW)
 - Instala keyloggers
 - Modifica parámetros y archivos del sistema operativo (Rootkits)
 - Genera conexiones externas protegidas (VPN), envía archivos recogidos vía http y ftp

2 - Deep web




- Deep Web (internet profunda)
- Invisible Web (internet invisible)
- Dark Web (internet oscura)
- Hidden Web (internet oculta)
- 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 deep web se aloja 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 (Fuente: Wikipedia)

2 - Deep Web, requisitos



Configuración de la red Tor

 **BROWSER**

Antes de que se conecte a la red Tor, necesita proporcionar información sobre la conexión a Internet de este equipo


¿Cuál de las siguientes opciones describe mejor su situación?

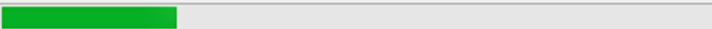
Me gustaría conectarme directamente a la red Tor.
Esto funcionará en la mayoría de las situaciones.

La conexión a Internet de este equipo está censurada o proxificada.
Necesito ajustar la configuración del repetidor puente(bridge) o de otro tipo.


Para obtener ayuda, contacte con help@rt.torproject.org

Estado de Tor

 **Conectando con la red de Tor**
Cargando el estado de la red



Espere mientras se establece una conexión con la red de Tor.



¡Felicidades!

Este navegador está configurado para usar Tor.

[Probar las preferencias de red Tor](#)

2 - Deep Web ¿Qué hay?



Contact | Alphabay Market x +

zdfvqospmrbvzdn3.onion/contact.php

Search

Logged in as **tresiano**
Current balance: **BTC 0.0000**
Autoshop Logout

USD 415.20 CAD 554.74 EUR 381.58 AUD 565.73 GBP 274.75

HOME SALES MESSAGES (1) LISTINGS BALANCE ORDERS FEEDBACK FORUMS CONTACT

Home

tresiano
Joined: Aug 6, 2015
Trust level: Level 1
Total sales: USD 0.00
Total orders: USD 0.00

Search: Search

⚠ We highly recommend that you disable Javascript when viewing the marketplace for better security.

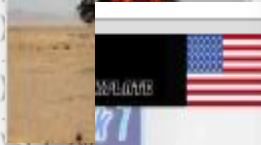
Featured Listings

[CARDING-UNIVERSITY] Jump From Noob to Pro Carder [Live Mentorship] [CUVE] # 648 - Fraud -	[MS] Whole Foods Market eGIFT CARD * 30% of the price balance* no carder # 44570 - Digital - Expedien	USA HIGH LEVEL CC - Check store for more! # 4004 - CVV & Cards - st0n3d Buy: USD 8.50	[FE 50%] Modafinil 200mg - 100x # 33184 - Other - Angelina Buy: USD 53.15	[FE 100%] [Bulk] 100 GRAM of high quality MDMA (80%+) (ESCROW) # 34503 - MDMA - Qualibwhite

2 - Deep Web



- ¿qué hay?



CZ Scorpion Evo 3 Semi-Auto

Barrel Length 7.75" Caliber 9mm Capacity 10+1 Will be shipped completely disas:



10 rounds 7.62x39mm Ammunition FULL ESCROW

For sale are 10 rounds of Wolf 7.62x39mm, better quality images: <http://www0.xup.in/executeimg.php?fid=16599966> Please ask for discounts for larger quantities. I send from Austria to th avoid customs. You will receive the Tracking-ID on the date of shipment with a PGP encrypted messa is ...

Sold by **deschek1337** - 1 sold since Dec 3, 2015

Vendor Level 1

Trust Level 4

	Features		Features
Product class	Physical package	Origin country	Austria
Quantity left	1 items	Ships to	Europe
Ends in	Never	Payment	Escrow



- **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).
- **Despacho de los objetos vendidos:**
 - se despachan desde 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.

3 – Ciberterrorismo

Definiciones

- **Ciberterrorismo:** **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)



3 – Ciberterrorismo

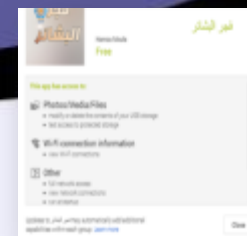
Principales Actores:

- **Terroristas:** ETA, ISIS, FARC, HAMAS, IRA...
 - Reclutamiento + Propaganda + Financiación + Comunicaciones
- **Gobiernos:** USA, China, Rusia, Alemania, Inglaterra, Israel, Corea...
 - Inteligencia + Espionaje + Sabotaje
- **Hacktivistas:** Anonymous, Lulzsec...
 - Propaganda.
- **Ciberdelincuentes:** Phishers, crackers, spammers, exploiters...
 - \$\$\$\$\$\$\$\$\$\$\$\$\$\$
- **Hackers profesionales:**
 - \$\$\$\$\$\$\$\$\$\$

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 más 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**
 - 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:**



Tecnologías utilizadas por **Gobiernos: #1** ESPIONAJE, PRISM



- PRISM es un programa de **vigilancia electrónica** considerado confidencial -hasta snowden!- 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 USA accedió a registros de **más de 35 líderes mundiales**.
- Las fuentes emplean grandes compañías de como Microsoft, Google, Apple y Facebook que entregan acceso a esa información.
- El programa tiene como objetivos a **aquellos ciudadanos estadounidenses que viven fuera de USA**, y se incluyen a **los ciudadanos estadounidenses que mantienen contacto con personas que habitan fuera de las fronteras de ese país**.
- Los datos que 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 -privados- sobre perfiles en redes sociales**.

3 – Ciberterrorismo

Análisis técnico de los ataques

Tecnologías utilizadas por **Gobiernos: #2** SABOTAJE,

Código Malware para sistemas scada

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



Tecnologías utilizadas por **Gobiernos: # 3**

Directamente **contratar hackers**

- El nombre del proyecto ultra secreto del Pentágono es **Plan X** y con él los “**cibersoldados**” podrán **obtener un espectro completo de las “cibercapacidades” y más opciones para los presidentes**, actuará en alianza con los comandantes militares y con el servicio secreto NSA.





Algunas **Afirmaciones** para tener en cuenta:

- 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 Gobiernos **reconocieron haber utilizado apt’s para sabotajes y espionaje**.
- Los **terroristas contratan Ciberdelincuentes y hacktivistas que utilizan apt’s con malware comprado en la deep web**.
- Los **Gobiernos contratan hackers que utilizan apt’s con malware comprado en la deep web**.

-



OWASP

The Open Web Application Security Project

- en memoria de Carlos Tori , Ethical Hacker -



- Gracias -

Christian Vila

ISEC GLOBAL Inc.

christian.vila@isec-global.com

@infosecurityvip

www.isec-global.com

www.infosecurityvip.com