Cazando sombras en la Dark Web

Raúl Beamud

Raúl Beamud

https://www.youtube.com/c/CiberINseguro

https://ciberinseguro.com

@raulbeamud | @ciberinseguro

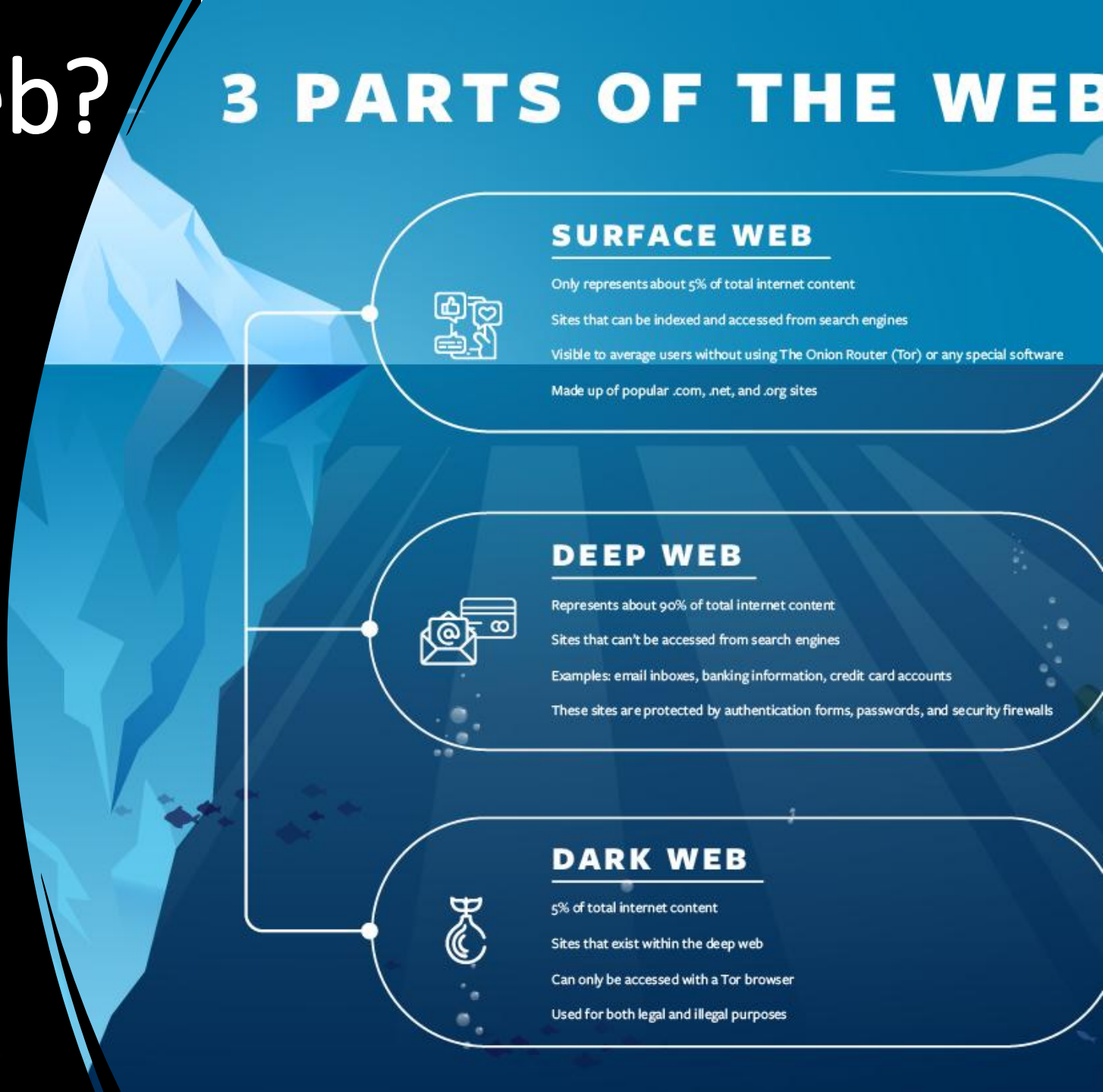
https://www.linkedin.com/in/raulbeamud/

Hacker Ético, con amplia experiencia y conocimiento en Pentesting, Red & Blue Team. Analista e Investigador de ciberseguridad. Certificado como Hacker Ético Experto, y como Perito Informático Forense. Con amplia experiencia en análisis de amenazas y vulnerabilidades, análisis de riesgos, auditorías de seguridad y cumplimiento normativo (LOPD, GDPR). Arquitecto de ciberseguridad en sistemas, aplicaciones y redes. Hardening de servidores. Seguridad en entornos Cloud. Delegado de Protección de Datos. Speaker en diferentes eventos, congresos y formaciones en materia de ciberseguridad. Mentor en la National Cyber League de la Guardia Civil.

¿Qué es la Dark Web?

¿Qué es la Dark Web?

Una parte oculta de Internet que no es accesible a través de los motores de búsqueda convencionales y requiere algún navegador especializado para acceder



Mitos y Realidades de la Dark Web

La Dark Web es solo para criminales

NO

La Dark Web es completamente anónima

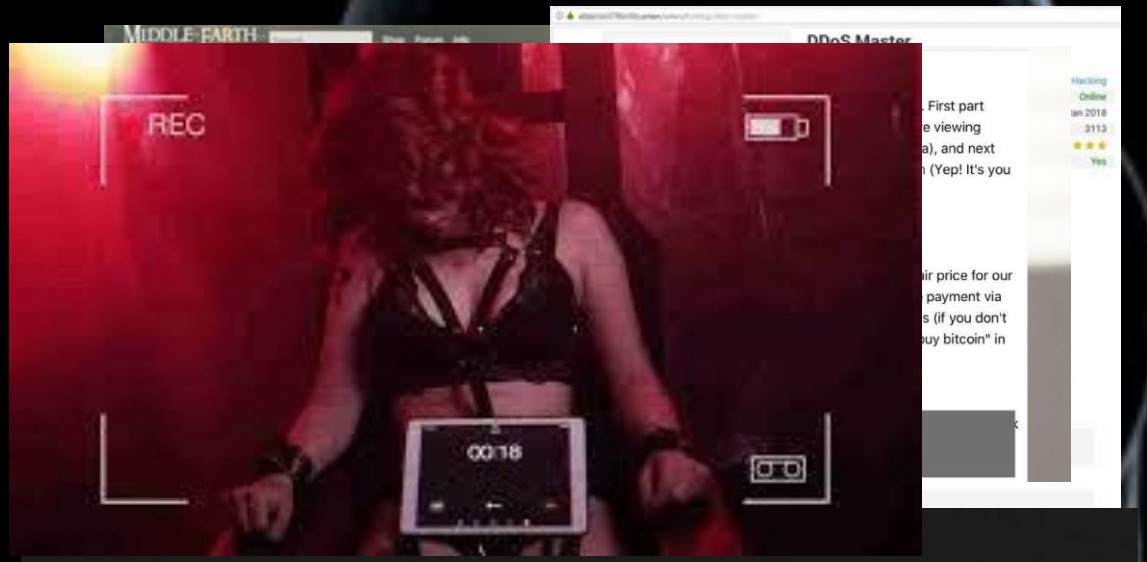
NO

La Dark Web y la Deep Web son lo mismo

NO

El Cibercrimen en la Dark Web

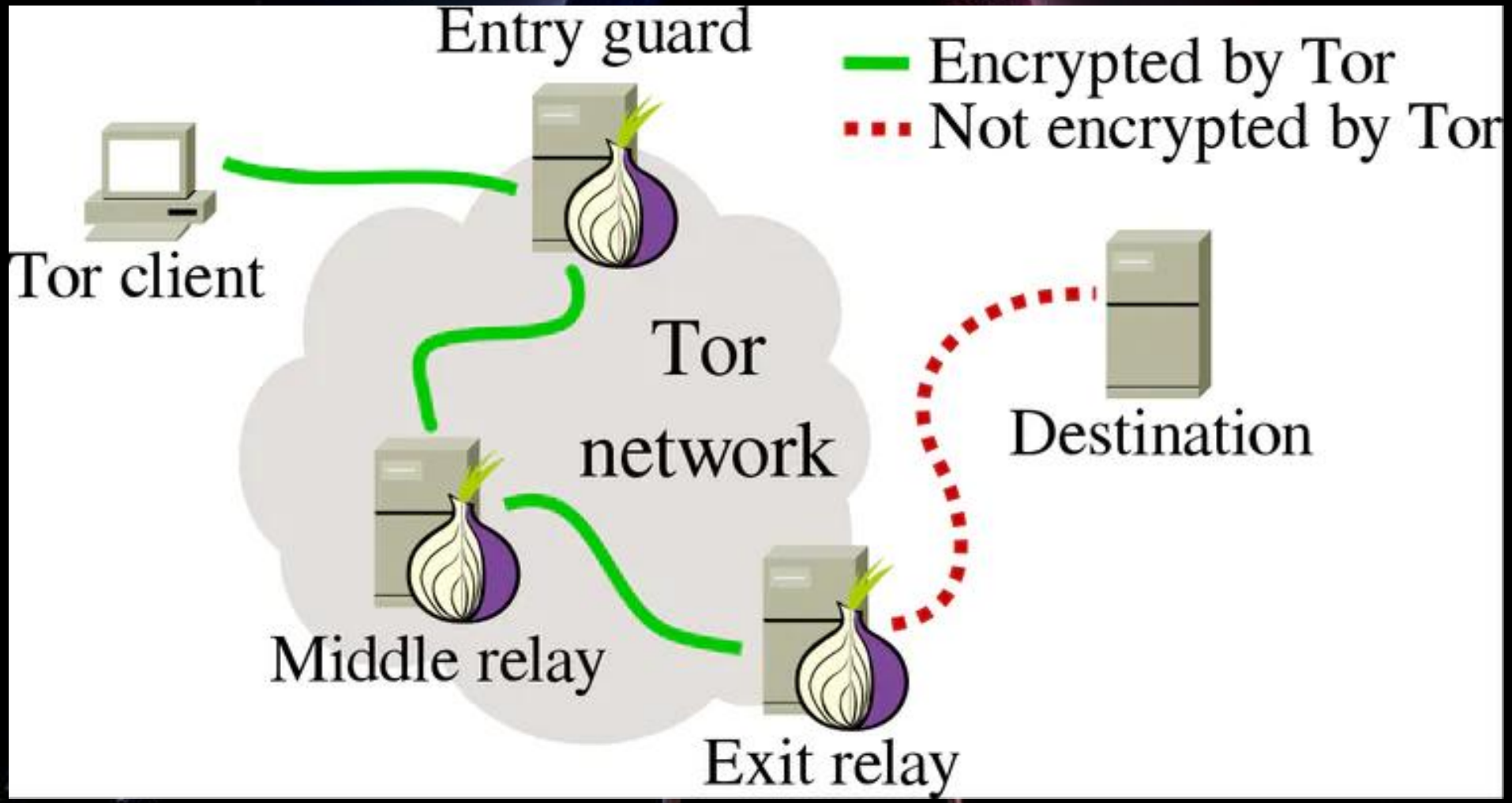
El Cibercrimen en la Dark Web



- Venta de drogas y sustancias ilegales
- Comercio de armas y explosivos
- Tráfico de información y datos robados
- Servicios de hacking y ataques cibernéticos
- Extorsión y chantaje
- Explotación y tráfico de seres humanos, incluyendo menores
- Acceso a contenidos ilegales y perturbadores

Técnicas y Herramientas para la caza de sombras

Análisis de tráfico en la Dark Web



Análisis de tráfico en la Dark Web

El análisis de tráfico implica la recopilación y examen de paquetes de datos que viajan a través de las redes en la Dark Web.

Permite identificar patrones, flujos de datos y ubicaciones de los cibercriminales, lo que ayuda a comprender mejor sus actividades y operaciones.

Durante el análisis, se examinan aspectos como las direcciones IP de origen y destino, los puertos utilizados, los protocolos involucrados y los patrones de comunicación.

El análisis de tráfico también puede incluir el estudio de metadatos, como la hora y la duración de las comunicaciones, para obtener más información sobre las actividades de los cibercriminales.

Explorando Fuentes abiertas (OSINT)

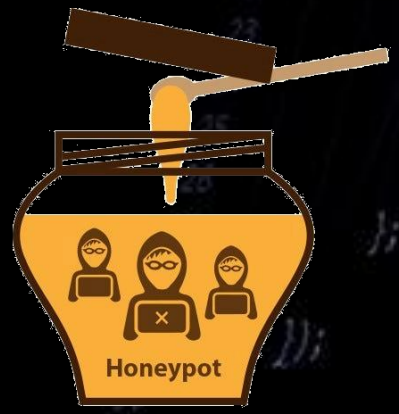
OSINT es una técnica de recolección de información que se basa en fuentes abiertas y accesibles públicamente en Internet.

Algunos ejemplos de fuentes abiertas utilizadas en OSINT, como redes sociales, foros de discusión, blogs, sitios web públicos, registros públicos y repositorios de código abierto.

La información recopilada de estas fuentes puede proporcionar detalles sobre las identidades, las relaciones y las actividades de los cibercriminales.

Honeypots en la Dark Web

Los honeypots son sistemas, redes o servicios diseñados específicamente para atraer a los cibercriminales y recopilar información sobre sus actividades y tácticas. Se colocan en la Dark Web para simular objetivos atractivos para los delincuentes.



Existen diferentes tipos de honeypots utilizados en la Dark Web, como honeypots de baja interacción, honeypots de alta interacción, honeynets y honeypages.

Inteligencia Artificial

Los algoritmos de IA pueden analizar grandes cantidades de datos y patrones para identificar comportamientos anómalos en la Dark Web.

La IA puede procesar y comprender el lenguaje natural utilizado en la Dark Web. Esto permite identificar palabras clave, frases o contextos que pueden indicar actividades ilegales, como la venta de drogas o la planificación de ciberataques.

Los sistemas de IA pueden clasificar y filtrar automáticamente el contenido de la Dark Web para identificar y eliminar sitios web o publicaciones que promuevan actividades ilegales.

La IA también puede utilizarse para analizar imágenes y videos encontrados en la Dark Web. Esto puede ayudar a identificar contenido ilegal, como imágenes de abuso infantil o actividades terroristas, y colaborar con las autoridades para su detección y eliminación.

Ingeniería Social

Creación de perfiles falsos en la Dark Web, presentándose como potenciales compradores o colaboradores en actividades ilegales.

Participar activamente en foros y comunidades en la Dark Web, se pueden establecer relaciones con cibercriminales y obtener información valiosa.

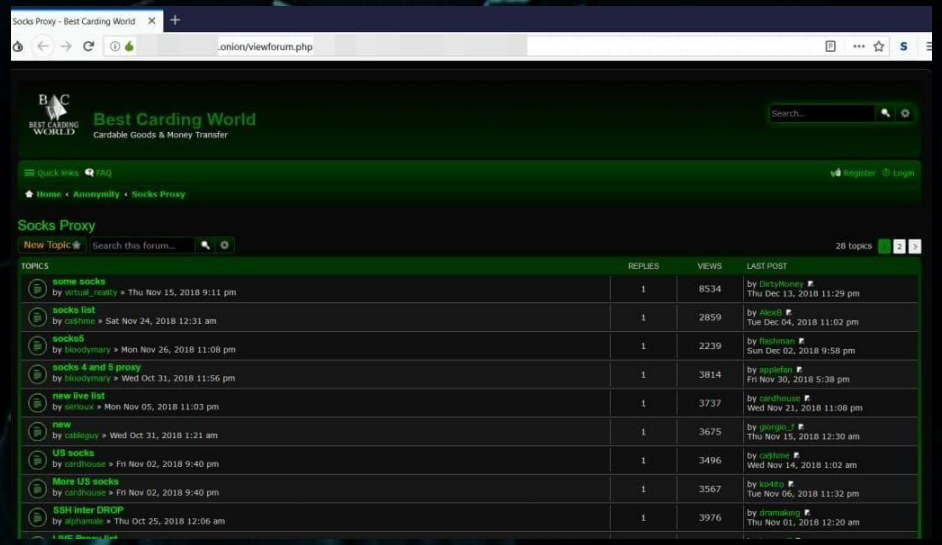
Se pueden utilizar identidades falsas para infiltrarse en grupos delictivos en la Dark Web.

Casos de éxito

Casos de Éxito

SILK ROAD

ANONYMOUS MARKET



Retos y Limitaciones

Retos y Limitaciones

- **Anonimato y cifrado**
- **Información limitada y sesgada**
- **Ética y privacidad**
- **Descentralización**
- **Velocidad de adaptación**
- **Recursos y habilidades especializadas**
- **Jurisdicciones y cooperación internacional**


GRACIAS!!!
APLAUDAN Y HAGAN PREGUNTAS FACILES...
memegen.es