Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

CARRERA DE ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO

TRABAJO FINAL DE ESPECIALIZACIÓN

Estudio descriptivo sobre la Darkweb como herramienta delictiva: Ciberdelincuencia en Argentina 2020/2023

AUTOR: ING. ALEJANDRO PEDRO BENABEN

DOCENTE DEL TALLER: MG. JOSÉ LUIS PIBERNUS

ABRIL 2022

Resumen

La presente investigación tiene como objetivo el estudio y análisis de las distintas metodologías que son utilizadas en la DarkWeb por los ciberdelincuentes. ¿Cómo utilizan los cibercriminales las ventajas que proporciona la web oscura?, ¿por qué la utilizan? ¿Cuáles son los beneficios para el anonimato que están disponibles y cuáles son los servicios y bienes que más frecuentemente se ofrecen por ese medio?

Estudiar las modalidades que se adoptan o encuentran en la web, es principalmente entender la posibilidad de anonimato y los servicios que se ofrecen para que una persona decida actuar criminalmente. Un malware específico en contra de otros usuarios, por ejemplo, el servicio de un Ransomware que tiene como fin encriptar archivos informáticos de una computadora para luego pedir un rescate económico a las víctimas. Modalidad que tuvo un gran crecimiento los últimos años y es considerada una de las principales amenazas según los reportes internacionales de ciberseguridad. Así lo afirma el informe: Allianz Risk Barometer (2022) Los Cyber incidentes o ataques están en primera posición en causas de interrupción de negocios. (pág., 3). Argentina fue víctima de ataques de este tipo, y se dieron a conocer con mayor influencia a partir de la pandemia por el Covid-19.

El presente trabajo deja ver la importancia del conocimiento, de las técnicas y las ventajas del anonimato en internet, utilizados por los ciberdelincuentes para operar criminalmente. Los aumentos de estas prácticas se ven en las fuentes de información y en los ataques a distintas empresas. ¿Se pueden tomar medidas preventivas contra estos ataques? Será la propuesta de este estudio ofrecer a los usuarios algunas recomendaciones.

La pandemia por el Covid-19 se desplegó con períodos de reclusión de todas las personas, provocando momentos de incertidumbre. Este fenómeno mundial hizo que se intensifique la utilización de internet para el uso de tareas diarias. Es evidente que en estos últimos años fuimos testigos del proceso de aceleración en adopción de nuevas tecnologías. Ya que la cotidianeidad empezó a pasar por estar conectados a internet.

Por esta razón y otras es que cada vez estudiamos, trabajamos y vivimos relacionados con la red. Creemos en la importancia de estudiar los riesgos, amenazas y las metodologías criminales que encontramos en la Dark Web para conocer de que se tratan estos perfiles ocultos en el ciberespacio.

La propuesta del presente trabajo es informar, prevenir o advertir sobre las nuevas técnicas y modalidades de los ciberdelincuentes. La cual consideramos fundamental para comprender e investigar los factores que implican el ciberespacio. El anonimato en internet es una herramienta, utilizada tanto en investigación por los analistas como los cibercriminales.

Palabras clave: *DarkWeb, ciberdelincuencia, Anonimato en internet, Argentina Covid-19, ciberinteligencia.*

Índice

Resumen 2
Índice 3
Índice de Figuras 4
1. Introducción 5
1.1 Justificación / Fundamentación 5
1.2 Planteamiento del problema 9
1.3 Objetivos 9
1.3 .1 Objetivo General 9
1.3.2 Objetivos Específicos 9
2. Marco teórico 10
2.1 La Deep y Dark web 10
2.2 Cibercrimen y ciberdelitos 14
2.3 Criminalística y criminología 17
3 Diagnóstico 19
3.1 Servicios de la Dark Web 19
3.1.1 Step by step (búsqueda en la DW) 20
4. Propuesta de intervención 28
5. Conclusiones 30
6. Referencias bibliográficas 33
7. Anexos 36

Índice de Figuras

Figura1: Funcionamiento de TOR Network…….07
Figura2: Acciones de la Deep Web…….....12
Figura3: Anatomía de Internet……..13
Figura4: Buscador Ahmia por TOR……..…….21
Figura5: Ransomware as a service….....22
Figura6 Pro hackers……23
Figura7 Curso de ransomware……24
Figura8 Billetera virtual……..25
Figura9 Oferta de armas…….....26
Figura10 Oferta de Opio……....27
Figura11 Oferta de Heroína……27
Figura12 ID y credenciales…….28

1. Introducción

1.1 Justificación / Fundamentación

La presente investigación enmarcada en un trabajo final integrador de la Especialización en Inteligencia y Crimen Organizado, explorará sobre las posibilidades que ofrece la Dark web para el crimen organizado. Dentro del desarrollo de la presente investigación el lector podrá familiarizarse no solo con el contenido que se encuentra en la web oculta, sino una guía paso a paso, de fácil acceso, como algunas recomendaciones para comenzar una investigación relacionada a la dar web y cibercrimen.

No solo se trata de mostrar materiales ilegales, se intenta desmentir con un sesgo social donde la Dark web es un lugar accesible solo para personas con altos conocimientos en informática. Demostrar lo contrario su fácil acceso es parte de la justificación de este trabajo. La Información suministrada es fundamental para la inteligencia estratégica que deberá en la época del cibercrimen estar cada vez más familiarizada con las transacciones y comercialización en la Deep y Dark web que explicaremos a continuación.

La Dark web es apenas una pequeñísima parte de la Deep web, esto es la parte de internet en la que se almacenan datos propietarios de personas y organizaciones.

Esto implica que el acceso a la Dark web está limitado a quienes ya conocen las URL a las que intentan acceder, sumado a esta privacidad y ocultamiento público de estas direcciones se agrega el navegador específico para la Dark web, como por ejemplo TOR (The Onion Router), cuyo propósito es impedir que se relacione la IP de origen con la IP de destino, ya que el mismo confía en saltos aleatorios antes de llegar a la dirección final.

¿Qué es la red Tor?

Sagun Samuel K (2020) “Tor and DarkNet 4 Donkeys a Practical Beginners Guide To The Secrets Of Deepweb” Tor es un acrónimo de The Onion Router (el enrutador cebolla, en castellano). Se trata de una red de comunicaciones que utiliza la técnica Onion Routing (enrutado de cebolla) para proteger el secreto, anonimato, seguridad y privacidad de los datos que circulan con estas comunicaciones. (Pag.111)

El Onion Routing utiliza distintos nodos. La información pasa encriptada de nodo a nodo. La dirección IP está protegida. Como son varios nodos, por eso se hace el símil con las capas de la cebolla. El objetivo, además, es que cada nodo descifre la información esencial para llegar a la web que se quiere consultar, y que solo el primer y último nodo sepan el origen y el destino.

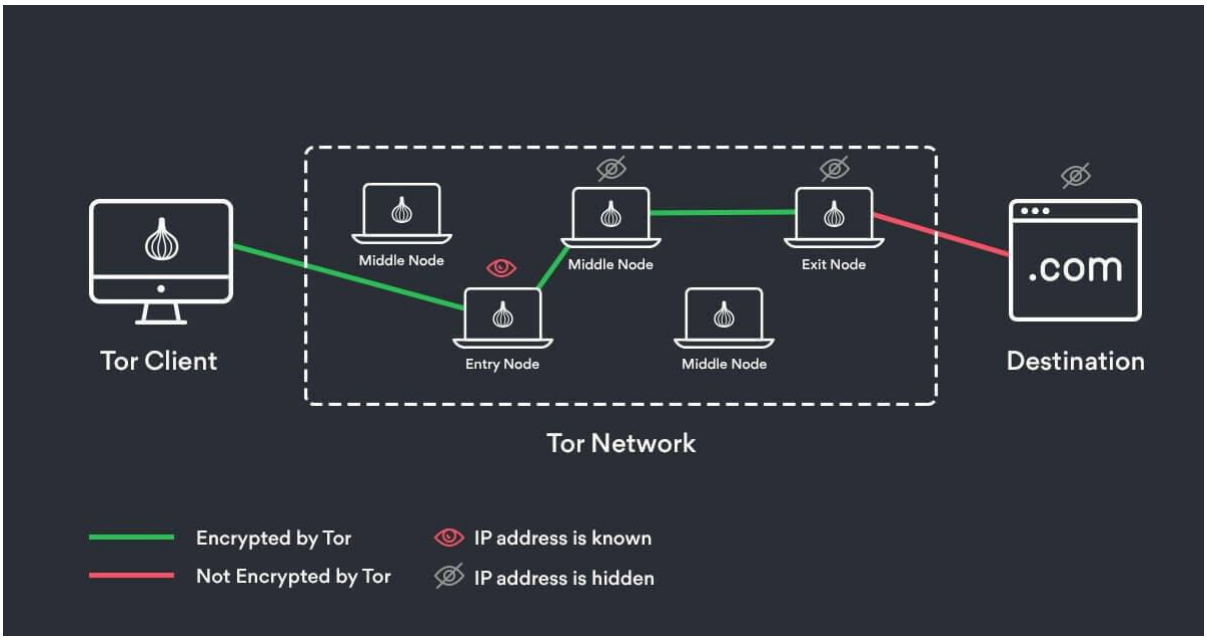


Fig. 1. Funcionamiento de TOR Network. Recuperado de TOR AND DARKNET (2020)

Este proceso, al ser más complejo, hace que la velocidad de acceso a una página web que se puede visitar con esta red sea más lenta.

¿Cómo usar y acceder a Tor?

Samuel K (2020) "Tor and DarkNet 4 Donkeys a Practical Beginners Guide To The Secrets Of Deepweb" Para acceder a la red Tor, existe un software específico: Tor Browser, un navegador que se puede descargar para cualquier sistema operativo. Es un navegador que, además de poder visitar las páginas web que ya podemos ver con otra red, también permite entrar a los enlaces de la dark web. Algunas de estas páginas funcionan con el dominio. onion. (Pág. 112).

Sion Retznik (2020) plantea Estos datos, indexados por un motor de búsqueda y a los que se accede a través de la World Wide Web (también llamada Surface Web), en realidad es solo una pequeña parte de Internet, es apenas una parte de la web que conocemos y utilizamos en los motores de búsqueda convencionales, Google, yahoo, Bing. Es por esto que la web oscura se diferencia de la web convencional mediante otra forma de conexión anónima y/u oculta. (Pág.10). Se necesita algún medio especial para el acceso como puede

ser el caso de TOR (the onion rúter) un software creado por la marina de EE. UU para ocultar la IP de los usuarios y de esta manera no poder determinar el origen de acceso a la web.

El propósito de la Marina al desarrollar TOR fue el de ofuscar la información para poder operar a través de la red de manera anónima, sin embargo, TOR fue rediseñado por particulares para permitir que ciudadanos en países cuyos gobiernos, controlaban y perseguían las opiniones disidentes vertidas en la red, pudieran tener un espacio seguro en donde operar. Esta misma seguridad pensada para permitir dar voz al oprimido da la posibilidad de desarrollar actividades ilegales o criminales por parte de los usuarios. Una gran parte del crimen convencional fue hacia el ciber espacio por su capacidad de anonimato casi absoluto.

Así fue como comenzaron a surgir en la Dark web comercios ilegales, relacionados al narcotráfico, venta de armas, material de abuso sexual infantil, entre otras. La que fue en su inicio un concepto de libertad para países que controlaban internet es hoy un mundo de ilegalidad que está disponible para cualquiera con los conocimientos mínimos para accederlo.

Los motivos por los cuales se decidió el tema de estudio se basan y sustentan en la relación entre la inteligencia estratégica y el crimen organizado con los medios de comunicación e intercambio de información. Todos los sistemas basados en protagonistas y antagonistas siempre han resaltado la importancia de tener comunicaciones seguras al tiempo que se tratan de vulnerar las del contrincante. La historia muestra muchos ejemplos de cómo el bando que mantiene impermeables sus medios de comunicación y lee la correspondencia ajena tiene una clara ventaja.

Hoy en día las redes criminales o cualquier ciudadano común podrían hacer uso de estas tecnologías, conectados a internet, que les harían evadir controles de las autoridades públicas, nacionales y trasnacionales.

Si la información es poder, conocer y analizar el lugar donde generalmente se apoyan los ciberdelincuentes, es lo propicio para el trabajo final de especialización.

Un analista de inteligencia conoce de HUMINT, OSINT, SOCMINT, Técnicas de Ingeniería Social, entre otras técnicas informáticas o físicas. Además, deberá contar con un buen nivel de conocimiento y de seguridad, si va a investigar en la web oscura, como proponemos mostrar paso a paso, para generan un anonimato seguro y adentrarnos en búsquedas dentro de la DARK y DEEP WEB.

Durante los últimos 20 años hemos visto la incesante penetración que ha tenido Internet en todos los ciudadanos de nuestro país. Programas gubernamentales como Conectar Igualdad, PC Abuelos y otros se convirtieron en la base del “achicando la brecha digital” entre las distintas clases sociales y grupos etarios.

Los bancos, comercios de electrodomésticos, supermercados y otros van reduciendo sus estructuras a medida que avanza la digitalización del ciudadano. Ya nadie quiere perder su tiempo en largas colas en dependencias gubernamentales, bancos o supermercados, hoy en día queremos hacer todo desde casa.

La pandemia de COVID-19 aceleró aún más este proceso de digitalización ciudadana. El miedo al virus COVID-19 y los decretos de "aislamiento social, preventivo y obligatorio y distanciamiento social, preventivo y obligatorio" aceleraron este cambio y hoy prácticamente todo se puede realizar de forma online.

Este cambio en el hábito de los ciudadanos trajo consigo la correspondiente mutación del crimen organizado llevándolo al campo de la virtualidad.

Es por ello que, vale la pena preguntarnos acerca de, cuán difícil es mutar hacia la ciberdelincuencia.

Nos preguntamos ¿Cuáles son las herramientas delictivas que ofrece la DarkWeb que está generando el incremento del cibercrimen?

Los largos periodos de aislamiento debidos a las medidas de profilaxis por la pandemia del COVID-19, fueron amenizados por la presencia masiva de la internet en los hogares, que nos permitió seguir relacionándonos y trabajando sin salir de casa. Durante los últimos dos años hemos sido testigos del aumento de la aceleración en el proceso de adopción de nuevas tecnologías. En nuestros días todo se hace a través de la red: trabajamos; estudiamos; compramos y pagamos bienes y servicios; nos entretenemos y relacionamos.

Según la revista internacional “Chaos” (2016) PAC 135, el surgimiento de la web oscura sirve como “vitrinas para la venta de productos y servicios ilícitos. Una cantidad creciente de actores se reparte un mercado altamente competitivo, en el cual los líderes son Ágora, Alphabay y Nucleus. La caída de Silk Road dio lugar al surgimiento de black markets similares, lo que concurre a la compleja construcción de un ecosistema criminal. Se trata de un espacio en el cual cada protagonista implementó estrategias innovadoras, con la finalidad de obtener más partes de mercado. Para lograrlo, los diferentes black markets suscitaron dinámicas de profesionalización y de especialización en sus productos (datos sutilizados, programas malintencionados, hardware, drogas, armas, documentos falsos, mercancías falsas, etc.)”1

[1]El surgimiento de un ecosistema criminal la: Dark Web y el Bitcoin los instrumentos del ciber-crimen. (2016). https://www.chaos-international.org/pac-135-el-surgimiento-de-ecosistema-criminal/?lang=es

1.2 Planteamiento del problema

Como pregunta de investigación y problema del presente TFI nos propusimos indagar sobre ¿Cuáles son las principales herramientas delictivas, utilizadas por cibercriminales en la DarkWeb observadas en organizaciones argentinas durante los años 2020/2023?

¿Cuál es el alcance a modo exploratorio utilizando TOR para navegar en la web oscura?

En el presente trabajo utilizaremos metodología de enfoque descriptivo y cualitativo. Este método implica un proceso de recolección de datos a través del estudio de bibliografía del área, publicaciones en la web, publicaciones académicas, entrevistas a especialistas y fuentes confiables. La investigación incluirá elementos de tipo descriptivo, incursionando en la red profunda para obtener información relacionada al crimen organizado. Seguiremos una guía paso a paso, navegando por TOR con la intención de obtener dicho material para realizar un diagnóstico y análisis de las posibles ofertas criminales en la Dark Web.

1.3 Objetivos

1.3.1 Objetivo General

Para motorizar nuestra investigación y como meta, nos propusimos el siguiente objetivo general: ¿qué herramientas delictivas llevan a un ciudadano a interactuar dentro de la DarkWeb con el objetivo de adquirir una actitud criminal en la red?

1.3.2 Objetivos Específicos

Para lograr el objetivo general, nos proponemos alcanzar los siguientes objetivos específicos:

1. Describir cómo se llega a la DarkWeb (DW) desde la Web Superficial mediante el uso de aplicaciones gratuitas.
2. Analizar herramientas que nos permitan movernos dentro de la DarkWeb.
3. Indagar sobre las actividades delictivas dentro de la DW.

2. Marco teórico

2.1 La Deep y Dark web

Para comenzar y dar sustento teórico y referencial, a nuestra investigación, creemos necesario conocer sobre lo que identificaremos primero como la Deep (profunda) y Dark (oscura) Web.

La Deep y Dark web no son iguales, aunque comparten sistemas parecidos. La internet profunda está compuesta por todo el contenido que no ha sido indexado por los motores de búsqueda convencionales como, Google, Yahoo, Bing, etc.

Digamos que no se esconde información si no que al no indexarse no se añade a Google u otros buscadores. Hay mucha información como dice Julián GL (2020) en su libro de Ciberpatrullaje: Metodologías para la Investigación en Internet: esta parte de Internet está compuesta por información y datos inofensivos, muy útiles para un investigador avispado.

Algunas de las cosas que pululan por aquí son:

- Emails: los correos electrónicos son privados (o deben serlo), por lo que Google no los indexa a su base de datos.
- Contenido dinámico: páginas web que sirven como respuesta a ciertos parámetros, como, por ejemplo, formularios online, datos de registro, encuestas, etc.
- Contenido de acceso restringido: todas aquellas páginas protegidas con contraseñas o con un Captcha (medida de seguridad basada en la dinámica pregunta-respuesta).
- Archivos y documentos: Pdf o Docs. que se hayan subido a la nube, también archivos con extensiones como .exe, .rar, .zip, etc.
- Páginas no enlazadas: páginas que han sido ocultadas intencionalmente a los ojos (o a las arañas) de Google, como por ejemplo páginas sin ningún tipo de enlace a otras webs.

- Redes internas: una gran parte de la Deep Web se compone de las redes internas y privadas de instituciones científicas y académicas. Se trata de bases de datos privadas utilizadas por las propias instituciones, y por lo tanto restringidas para personas ajenas.

Pero, además, una ventaja enorme que ofrece la Internet profunda es la posibilidad de comunicarse y compartir información permaneciendo en el anonimato (pág. 23, 24).

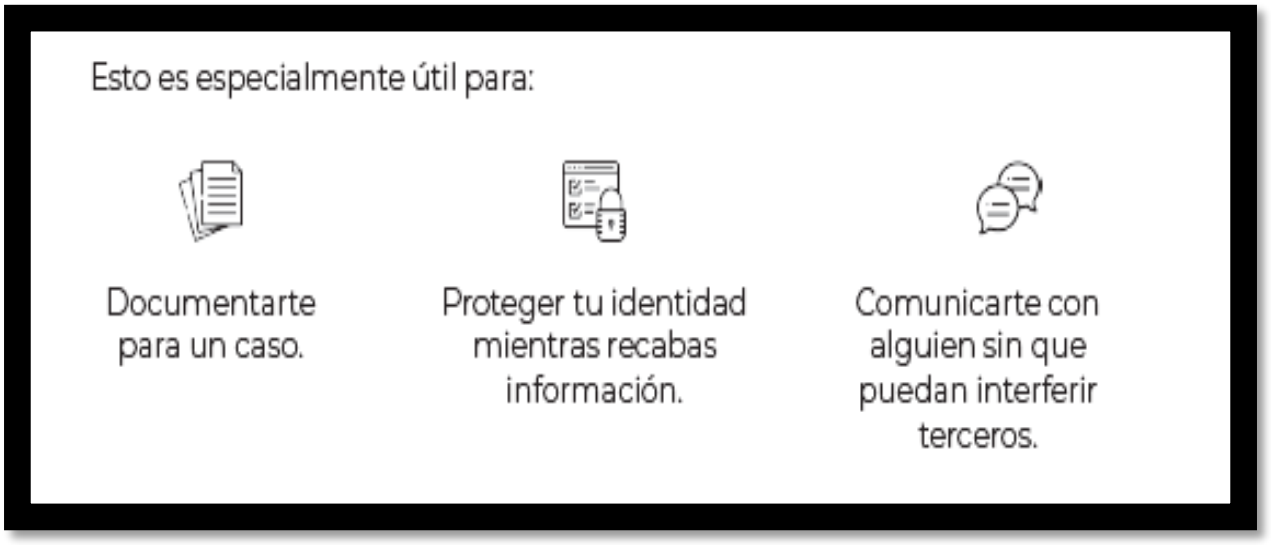


Figura 2 acciones de la Deep web. Libro: Ciberpatrulla: metodologías para la investigación en Internet (2020).

Ahora vamos a hablar un poco de la Dark Web y sus diferencias con las Deep Web. La principal diferencia es que la web oscura es un porcentaje muy pequeño de la Deep.

Como lo describe Julián LG (2020) de ciberpatrulla: La Internet oscura (o Dark Web) es un conjunto de redes paralelas a la Deep Web, que usan servidores y navegadores especiales para no dejar rastro y navegar de forma anónima (pag,26).

Por ejemplo:

- Periodistas que estén documentando un reportaje, protegiendo a la fuente.
- Activistas que quieran proteger su identidad.

- Ciudadanos de países con censura sobre Internet.
- Militares o cuerpos de seguridad encubiertos que necesiten comunicarse.
- Investigadores que necesiten información para un caso concreto.

Son estas las zonas oscuras en internet donde hay delitos desagradables, donde proliferan distintos ejemplos de cibercrimen, no solo el económico sino por ejemplo el intercambio de material de abuso sexual infantil en redes de pedofilia especialmente ocultas. En el artículo de la revista científica del Instituto de Ingenieros Eléctricos y Electrónicos IEEE Access , J, PASTOR-GALINDO, P, NESPOLI , GÓMEZ MÁRMOL AND G, MARTÍNEZ PÉREZ (2019) "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends" (La mina de oro aún no explotada de OSINT: Oportunidades, Desafíos abiertos y tendencias futuras) plantea: la Dark Web ofrece anonimato y privacidad a los usuarios que al utilizarlo ésta propiedad facilita que los criminales empleen este red para navegar, realizar sus búsquedas y publicar con fines ilegítimos ocultando su identidad. Por lo tanto, la Dark Web es una fuente ideal para aplicar OSINT y luchar contra el cibercrimen, el crimen organizado o las ciberamenazas. Sobre el otro lado, la persecución y desanonimización de estas personas son desafíos no triviales actuales para que OSINT funcione adecuadamente. (pág.3).

Es por esta razón, la importancia en el análisis de inteligencia contar con conocimiento del funcionamiento de estas web o redes ocultas. Si cada vez se utilizan más la inteligencia debe capacitar y concientizar a sus recursos humanos para saber el funcionamiento y como se debería investigar en la Deep y dark web.

Spadaro (2016) caracteriza a la Inteligencia como el proceso en "la búsqueda de la verdad oculta, desentrañando lo que ha sido disimulado deliberadamente tras una falsa significación" (pág.30). Es por esta intención tal cual plantea Ricardo Spadaro la importancia de generar noción y conocimiento en ciberseguridad para combatir e identificar el cibercrimen. En oportunidades es necesario llegar a pensar como un ciberdelincuente que nos permita llevar adelante una investigación favorable al investigador, por ejemplo, como pensar, "que haría para vender drogas o comprar un malware de tipo ransomware, mediante la dark web". En la figura siguiente se observan las 3 capas de internet.

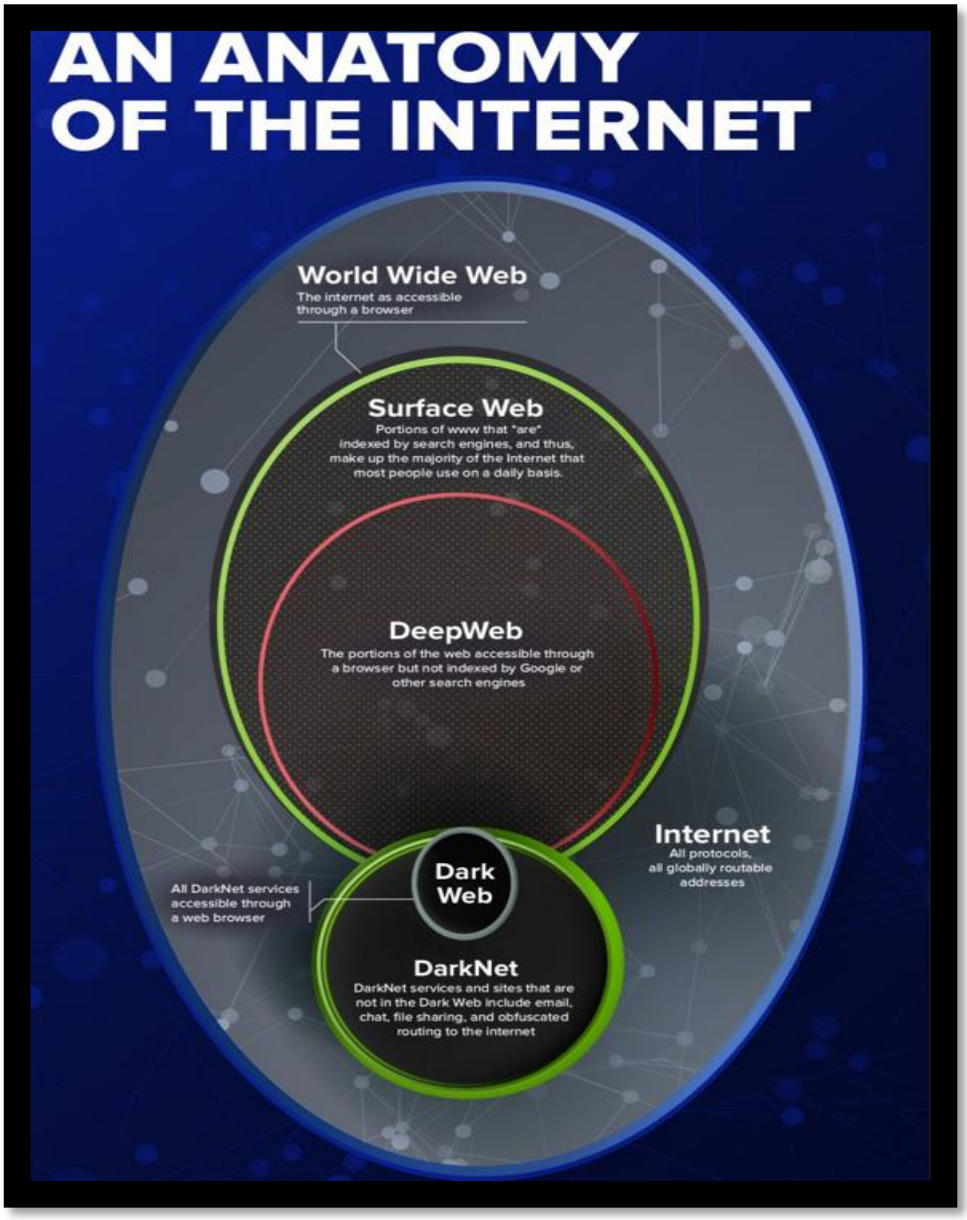


Fig. 3 Anatomía de internet. Arggone National Laboratory website (2022) Recuperado de: https://www.anl.gov/

Observando la figura n° 3; explica gráficamente las distintas capas de internet donde se observa el protocolo www (Word Wide Web) en el que generalmente navegamos o también denominada "Surface Web" identificada como la parte más pequeña de la red. Y así lo plantea la revista científica de ingenieros IEEE Access, J, PASTOR-GALINDO, P, NESPOLI, GÓMEZ MÁRMOL AND G, MARTÍNEZ PÉREZ (2019) The Not Yet

Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends: Actualmente hay un gran volumen de código abierto que vale la pena, son datos para ser analizados, correlacionados y vinculados. Esto incluye redes sociales, documentos e informes gubernamentales públicos, contenido multimedia en línea, periódicos e incluso la Deep web y Dark web, entre otros. En realidad, tanto el Deepweb y DarkWeb (este último circunscrito dentro del primero) contiene incluso más información que la Surface Web (es decir, la Internet conocida por la mayoría de los usuarios). Con el fin de poder acceder a estas redes, es necesario utilizar herramientas ya que sus contenidos no están indexados por la búsqueda tradicional de motores. (pág. 2). Por esta razón una de las maneras de acceder a las profundidades de la red es via TOR, the onion rúter.

2.2 Cibercrimen y ciberdelitos

En la reconocida revista de seguridad "Foreing Affairs Latinoamérica" el especialista Roberto de León Huerta (2020) afirma que hay discusiones abiertas en cuanto al ciberdelito; "hay discusiones en curso en foros especializados sobre ciberdelito, el impacto de las tecnologías en el desarrollo, gobernanza de internet y el desarrollo de normas técnicas para el uso del ciberespacio. Entre tanto, la proliferación de foros y la fragmentación de enfoques vuelven difícil alcanzar consensos y plantear un abordaje integral de esta agenda". (pag,53)

También llamado crimen por computadora, por el uso de una computadora como instrumento para lograr un fin ilegal, como ser: fraude, tráfico de material de abuso sexual infantil y propiedad intelectual, robo de identidades o violación a la privacidad. Según el informe de la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDYCI) "Recomendaciones para evitar ser víctima de ciberacoso en épocas de coronavirus (2020), plantea: Al hacer la denuncia por cualquier medio, nos permitís ayudarte a saber quién está del otro lado de la computadora (pág. 22), manifestando la necesidad de comenzar por una denuncia para investigar cada caso, además sugiere a los usuarios: Realiza un uso responsable y seguro de la computadora, utiliza la webcam únicamente con personas de máxima confianza (que conozcamos en el mundo real o físico). (pág., 15)

El cibercrimen, ha crecido en importancia a medida que las computadoras se han vuelto parte central del comercio, el entretenimiento y el gobierno. Según la Asociación

Argentina de Lucha Contra el Cibercrimen (2021), Se observa una leve disminución de casos consultados en el año 2021 con respecto al año 2020. vale destacar que a nuestro entender en el 2020 fue considerable la suba de casos respecto a los años anteriores , principalmente casos de fraude, robo de datos y extorción digital debido a qué ya la cuarentena estricta decretada en el país en el segundo y tercer trimestre, hizo que mucha gente tuviera que comenzar a trabajar a través de dispositivos informáticos en forma casi total, y en muchos casos sin los elementos de prevención ni la capacitación necesaria para prevenir las tipologías de delitos mencionados. en el 2021 un porcentaje importante normalizó su forma de trabajo habitual, otros lograron capacitarse en materia preventiva, como así también las diferentes campañas de concientización tanto gubernamentales, de organizaciones civiles y los medios de comunicación lograron en cierta forma un efecto positivo en la prevención.[2]

La Convención de las Naciones Unidas contra el Crimen Organizado Transnacional (2020) define como "grupo criminal organizado" a un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención, con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material. Además, según la ONU: "En el artículo 2(a) se específica que un "grupo criminal organizado" es:

- Un grupo de tres o más personas que no fue formado de manera aleatoria;
- Que ha existido por un periodo de tiempo;
- Actuando de manera premeditada con el objetivo de cometer un delito punible con, al menos, 4 años de encarcelamiento;
- Con el fin de obtener, directa o indirectamente, un beneficio financiero o material."[3]

[2] AALCC. (2021). ESTADISTICAS 2021
INFORME SOBRE CONSULTAS EN MATERIA DELITOS CONFIGURABLESA TRAVÉS DE INTERNET. https://www.cibercrimen.org.ar/2021/12/28/estadisticas-2021/
[3] UNODC.ORG. Crimen Organizados Transnacional. (2020). https://www.unodc.org/ropan/es/organized-crime.html

En la Argentina, según la Caracterización de la Criminalidad Organizada publicada por la página oficial del gobierno argentino "argentina.gob.ar" (2022), los delitos más comunes son: narcotráfico, tráfico de armas, venta ilegal de autopartes, contrabando de mercancía, lavado de dinero y los ciberdelitos.[4]

Según Sion Retznik (2018) en su libro "Hand-on Dark Web Analysis" la web oscura es un conjunto oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado. Se utiliza para mantener la actividad de Internet anónima y privada, lo que puede ser útil tanto en aplicaciones legales como ilegales. Si bien algunos lo usan para evadir la censura del gobierno, también se sabe que se utiliza para actividades altamente ilegales. Como lo afirman el autor del blog médium.com: "La Dark Web (o Darkweb) es una pequeña parte de la Deep Web (también inaccesible con un navegador web estándar). Se accede a Dark Web a través de la llamada DarkNet, que consta de muchos nodos anónimos distribuidos (como Tor, I2P y Freenet). (Pág. 15)

En cuanto a las Criptodivisas el autor Sion Retznik (2018). Uno de los temas importantes, al realizar transacciones con criptomonedas, es mantener la privacidad. Esto es hecho ofuscando el origen de bitcoins en una billetera bitcoin y la identidad/ubicación del receptor. La divisa alternativa o moneda digital que permite intercambiar valor a través de Internet con dificultad para rastrear por parte de las autoridades. (Pág. 28). A partir de esta modalidad es el comercio "ideal" y elegido por los ciberdelincuentes.

Según Jan Lansky (2020), una criptodivisa es un sistema que cumple las siguientes seis condiciones:

1. El sistema no necesita una autoridad central. Así, su estado es mantenido a través de un consenso distribuido.
2. El sistema mantiene todas las unidades y sus propietarios.
3. El sistema define si se pueden crear nuevas unidades.
4. Solo se puede asegurar la propiedad de una unidad a un usuario de manera criptográfica.

[4]Argentino.gob.ar (2022). Caracterizacion de la criminalidad organizada. https://www.argentina.gob.ar/seguridad/abordaje-crimen-organizado/criminalidad-organizada

5. El sistema permite las transacciones de unidades, en las cuales se cambia el propietario de dichas unidades. Una transacción solo puede ser efectuada si se puede probar el actual propietario de estas unidades.
6. Si se efectúan dos transacciones sobre las mismas unidades, el sistema solo ejecuta una de ellas.[5]

Este paraíso del anonimato podría motivar de alguna manera a delincuentes comunes o complejos a tratar de ingresar en la ciberdelincuencia. Sion Retzkin (2018) en su libro "Hand-on Dark Web Analysis" Dado que la Dark Web ofrece anonimato y seguridad, los delincuentes suelen utilizarla para protegerse ellos mismos y para evitar la captura. Aunque los organismos encargados de hacer cumplir la ley operan dentro del Dark Web, significa que impiden que todos los ciber-delincuentes participen en actividades delictivas. (pag.18)

2.3 Criminalística y criminología

Como auxiliares de la justicia es la investigación en criminalística la que debe buscar las pruebas o como vemos en el presente estudio, la evidencia digital de un delito. El doctor Dimas Oliveros Sifontes (1973) define la criminalística como conjunto de conocimientos aplicables a la búsqueda y el estudio material del crimen para llegar a su prueba. (Pág. 7).

Un cibercriminal no difiere a un criminal del mundo físico. Sin duda, algunas de las manifestaciones son nuevas, pero una gran cantidad de los delitos cometidos con o contra las computadoras sólo difiere en términos del medio utilizado. En el libro "El Rastro Digital del Delito: aspectos técnicos, legales, y estratégicos de la informática forense" (2016) sus autores concluyen en cuanto a la informática forense; la dinámica de la evolución humana y su avance tecnológico, han aportado un nuevo paradigma en la materia, generando nuevas escenas del crimen de características virtuales que concurren con las físicas ; nuevas escrituras que no son sobre soporte de papel y a la que no es posible aplicarles el método scopométrico que tan buenos resultados ha dado a la Documentología. La digitalización de la información ha hecho que ya no se deba buscar un rastro de una huella con un reactivo

[5] Ulab.es (2019) ¿Qué son las criptomonedas? https://ulab.es/que-son-las-criptomonedas/

químico o magnético, sino con complejas herramientas computacionales que buscan ese indicio escondido, ese rastro, en un código binarios que genera complejos laberintos digitales de información. (Pag.83). El delito es fundamentalmente el mismo, por lo que se trata de un delito reconocible cometido de una manera completamente diferente.

Los criminales del mundo real tienen la decisión de cometer delitos, por lo que, ante un cambio en el paradigma de los hábitos de los ciudadanos, es de suponer que los criminales tendrían la motivación para mutar hacia el cibercrimen.

Ahora bien, estudiar la conducta humana o sobre el porqué una persona decide cometer un cibercrimen es objeto de un estudio más extenso que no nos compete, pero si condiciona a la hora de hablar de cibercrimen y los distintos canales que encontramos en la Dark Web para llevarlos adelante. La criminología a su vez es el estudio de los móviles que llevaría a una persona a incurrir en la delincuencia, por ejemplo. “El Rastro Digital del Delito: aspectos técnicos, legales, y estratégicos de la informática forense” (2016): la definen como la ciencia que se encarga del estudio del delito como conducta humana y social, de investigar las causas de la delincuencia, de la prevención del delito y del tratamiento del delincuente, teniendo en su campo de acción tres ramas: la administración de justicia, la penitenciaría, y la prevención del delito, lo que se conoce como etiología del delito, aplicándose de manera práctica, aspectos pre-delincuentes y post-delincuentes.

3 Diagnóstico

3.1 Servicios de la Dark Web

A partir del presente trabajo de investigación se pretende evidenciar las oportunidades de un cibercriminal que navega por la web oscura. Inferimos que muchos de los servicios ofrecidos allí, son los que luego impactan tanto en las personas como en organizaciones público o privadas. Se saben que con la pandemia por Covid-19 las ciberamenazas aumentaron y tuvieron un impacto en un mundo desprevenido. Así lo manifiesta el reporte del banco Allianz (2022). "Risk Barometer, the most important businnes risk for the next 12 month and beyond, based on the insigth". los ciberataques son la principal pérdida económica para las empresas por encima de desastres naturales. (Pag.6).

Una de las principales amenazas son los malwares (virus informáticos) especialmente uno que se conocen como Ransomware, un software malicioso que encripta los archivos de la computadora para luego pedir dinero o generalmente criptodivisas a cambio de devolver dicha información secuestrada.

Tanto empresas privadas como organizaciones del Estado son víctimas a diario. Argentina cotidianamente lo sufre y lo confirman fuentes oficiales y periodísticas cada vez con más cotidianeidad, es un ataque detrás de otro. Respondiendo a nuestra pregunta problema de investigación ¿Cuáles son las principales herramientas delictivas, utilizadas por cibercriminales en la DarkWeb observadas en organizaciones argentinas durante los años 2020/2023?. Algunas dependencias estatales encontradas son: Ministerio Publico Fiscal[6]; CONICET[7], Senado de la Nación[8], Migraciones[9], Correo Argentino sufrió un ataque de tipo

[6] Diario Perfil (2021). "Un hackeo en el Ministerio Publico Fiscal generó preocupación en el poder judicial". https://www.perfil.com/noticias/politica/hackeo-ministerio-publico-fiscal-genero-preocupacion-poder-judicial.phtml
[7] Clarin (2022). "El conicet victima de ciberdelincuentes". https://www.clarin.com/tecnologia/conicet-victima-ciberdelincuentes-roban-datos-piden-dinero-devolverlos_0_LFRRFW39jx.html
[8] Clarin (2021) "El Senado de la Nación sufrio un cibeataque de tipo ransomware" https://www.clarin.com/tecnologia/senado-nacion-sufrio-ciberataque-ransomware-secuestran-datos-publicos_0_13uPrKQNd.html
[9] La Nación. (2020). "Migraciones: como fue el ataque de ransomware Netwalker y que datos revela" https://www.lanacion.com.ar/tecnologia/migraciones-como-fue-ataque-del-ransomware-netwalker-nid2446451/

phishing[10]. Es evidente la cantidad de ataques sufridos en argentina en los últimos años. La pandemia va terminando, pero estaríamos en condiciones de afirmar que esta modalidad de cibercrimen llegó para quedarse.

En este trabajo, hemos navegado mediante TOR en la Dark Web para observar: ¿qué oferta de servicios de ransomware encontramos? y ¿Cuáles son las posibilidades de compra y venta? que nos sugiere la web oscura.

3.1.1 Step by step (búsqueda en la DW)

1° paso buscador en TOR: AHMIA

Es un conocido buscador para la web profunda que se puede acceder con TOR browser. La imagen nos muestra una escalera de un subterráneo haciendo referencia a la web profunda, metaforizando lo que estaría por debajo de la superficie. El sitio web presenta un cartel de advertencia donde manifiesta que no aceptan material de abuso y que se puede acceder a su "lista negra" donde se indexan sitios prohibidos o denegadas e invita a los usuarios a reportar si se encuentran con material considerado abusivo.

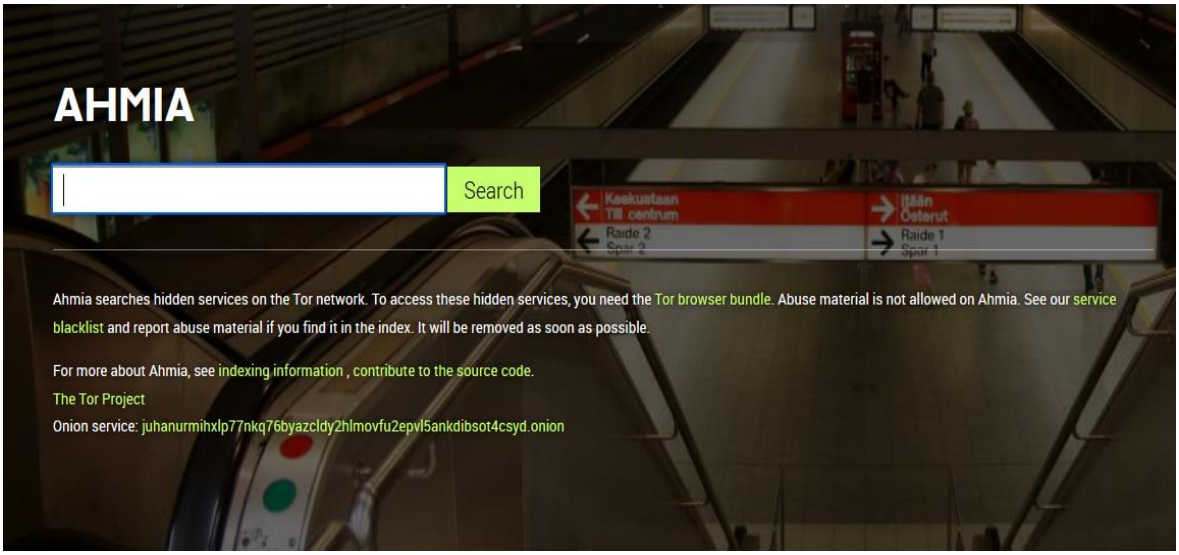


Fig. 4 Captura de pantalla del buscador AHMIA mediante TOR. Producción propia (2022)

[10] Correoargentino.com.ar. (2021). "Alerta: usan el nombre de Correo Argentino para una nueva estafa virtual" https://www.correoargentino.com.ar/alerta-usan-el-nombre-de-correo-argentino-para-una-nueva-estafa-virtual

2° paso: Búsqueda de servicios ransomware

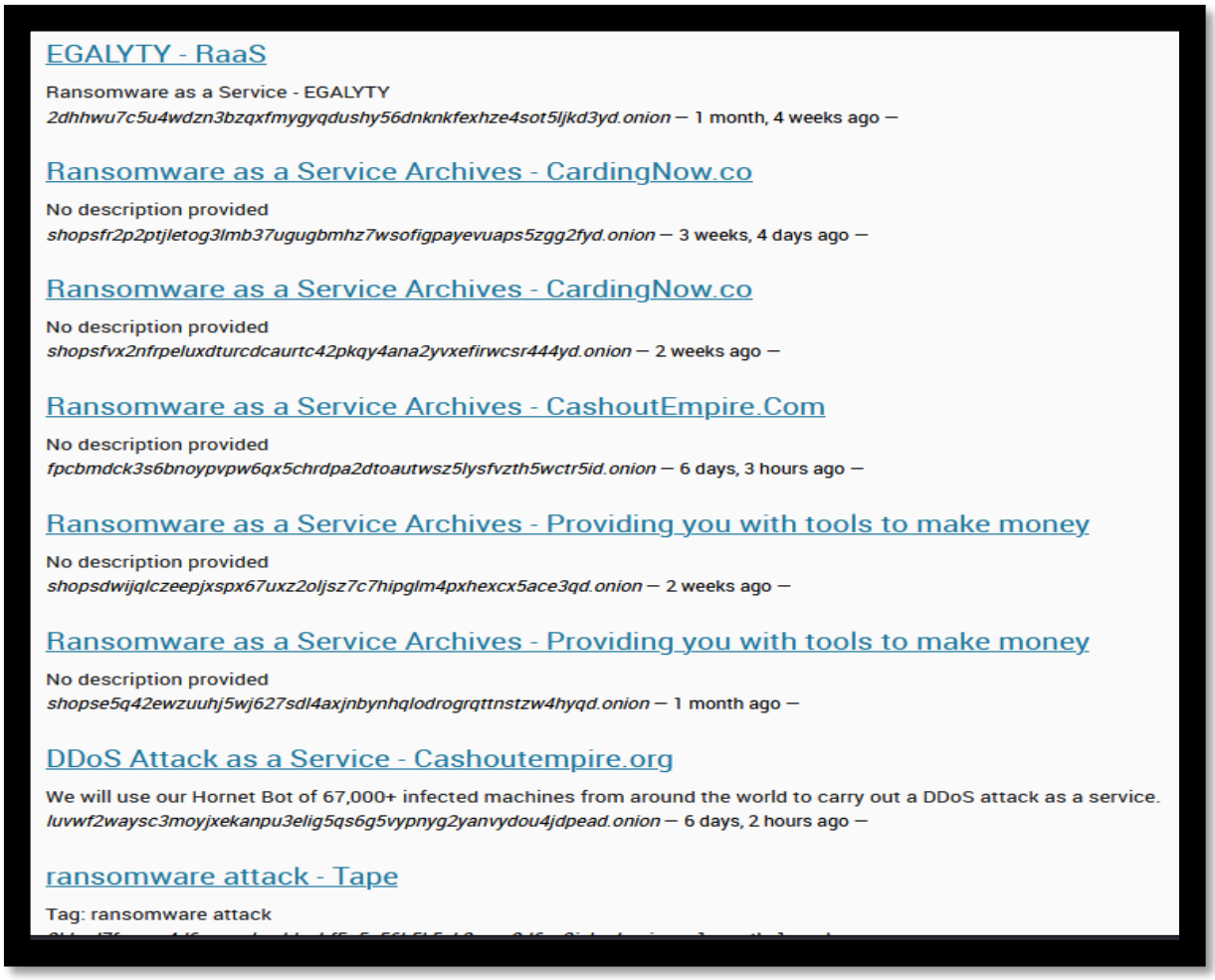


Fig. 5: *A partir de nuestro buscador se ingresó la palabra "Ransomware as a service", y se devolvió como resultado un número importante de anuncios sobre el servicio solicitado. Captura de pantalla propia (2022).*

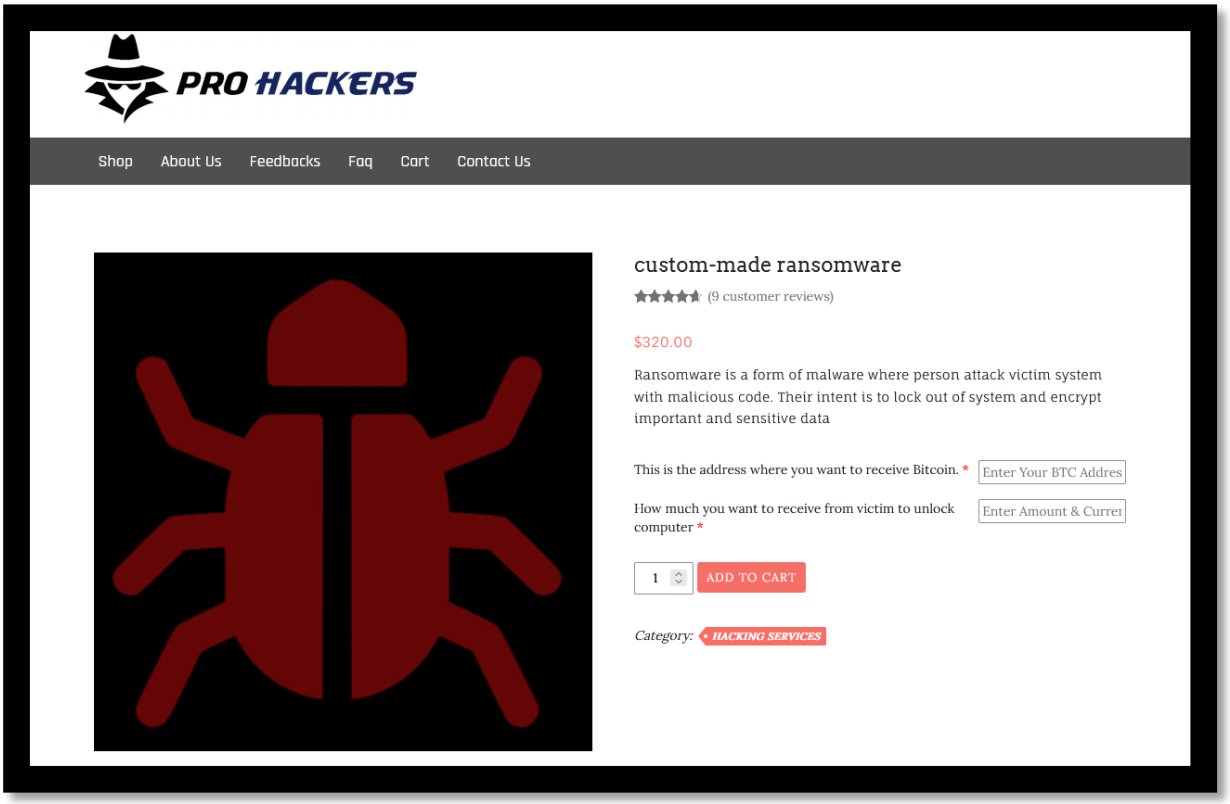


Fig. 6: Captura de pantalla "Pro hackers" (2022), donde se ofrece un Ransomware a medida del consumidor. Recuperado de http://r722lrlb2f4gat7djrogjttel4s6eumx7l4x6nd5xa7xlzjyazgjorid.onion/product/custom-made-ransomware/

Se adjunta la dirección (el onion) que difiere de las conocidas "www" de la Surf web, observamos otro tipo protocolo de URL que nos proporciona en este caso la herramienta TOR, otorgándonos de esta manera lo necesario para el correspondiente ingreso a los sitios de la web oscura. Sin más, en dos simples pasos.

Además, encontramos la venta de un curso para fabricar y aprender a encriptar archivos mediante Phyton, un tipo de lenguaje de programación. De esta manera tal como lo dice el título del curso se podría construir un propio ransomware (Building ransomware) La oferta es variada, interminable, y no solo se resume a la compra o venta de un software malicioso, es mucho más que eso. Se podría entender como una inducción o gran escuela para el ciberdelincuente, donde se puede generar las habilidades necesarias para comenzar a interactuar con las herramientas más utilizadas por los ciberdelincuentes.

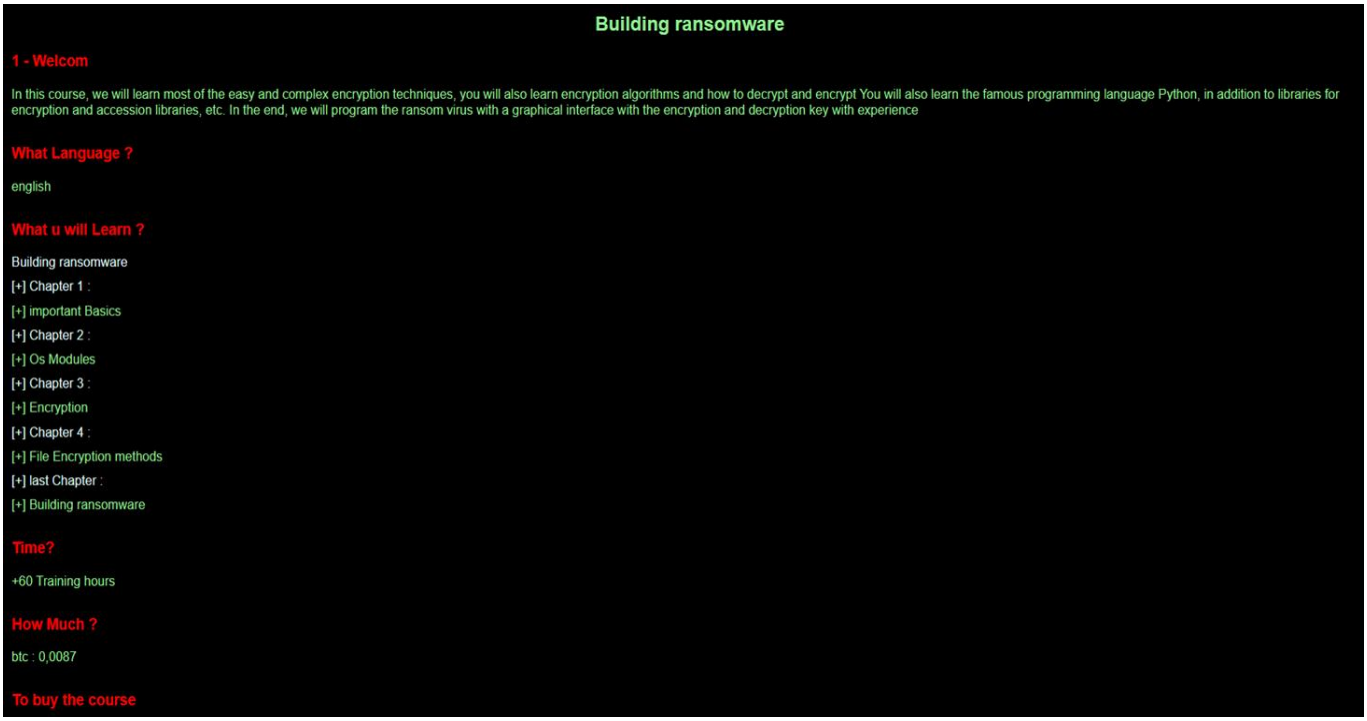


Fig. 7: Curso para aprender a fabricar tu propio ransomware en la DW. Captura de pantalla propia (2022).

Se puede ver que la oferta es variada donde no es complejo interactuar con el proveedor, ya que deja sus direcciones por los propios canales de mensajes encriptados.

Por supuesto que descargar archivos, ingresar divisas, comerciar o interactuar con los ciberdelincuentes es un riesgo. Para la muestra de las imágenes presentadas en el presente diagnostico se utilizó una máquina virtual a modo de protección personal del investigador. No se recomienda interactuar mediante estos canales por más que sea de fácil acceso ya que muchas veces son trampas de los propios cibercriminales para aprovecharse de las personas o las mismas fuerzas de seguridad montan sus falsos sitios para perseguir a delincuentes. Sin dudas sigue siendo un lugar oscuro, complejo y por lo tanto ideal para el crimen organizado.

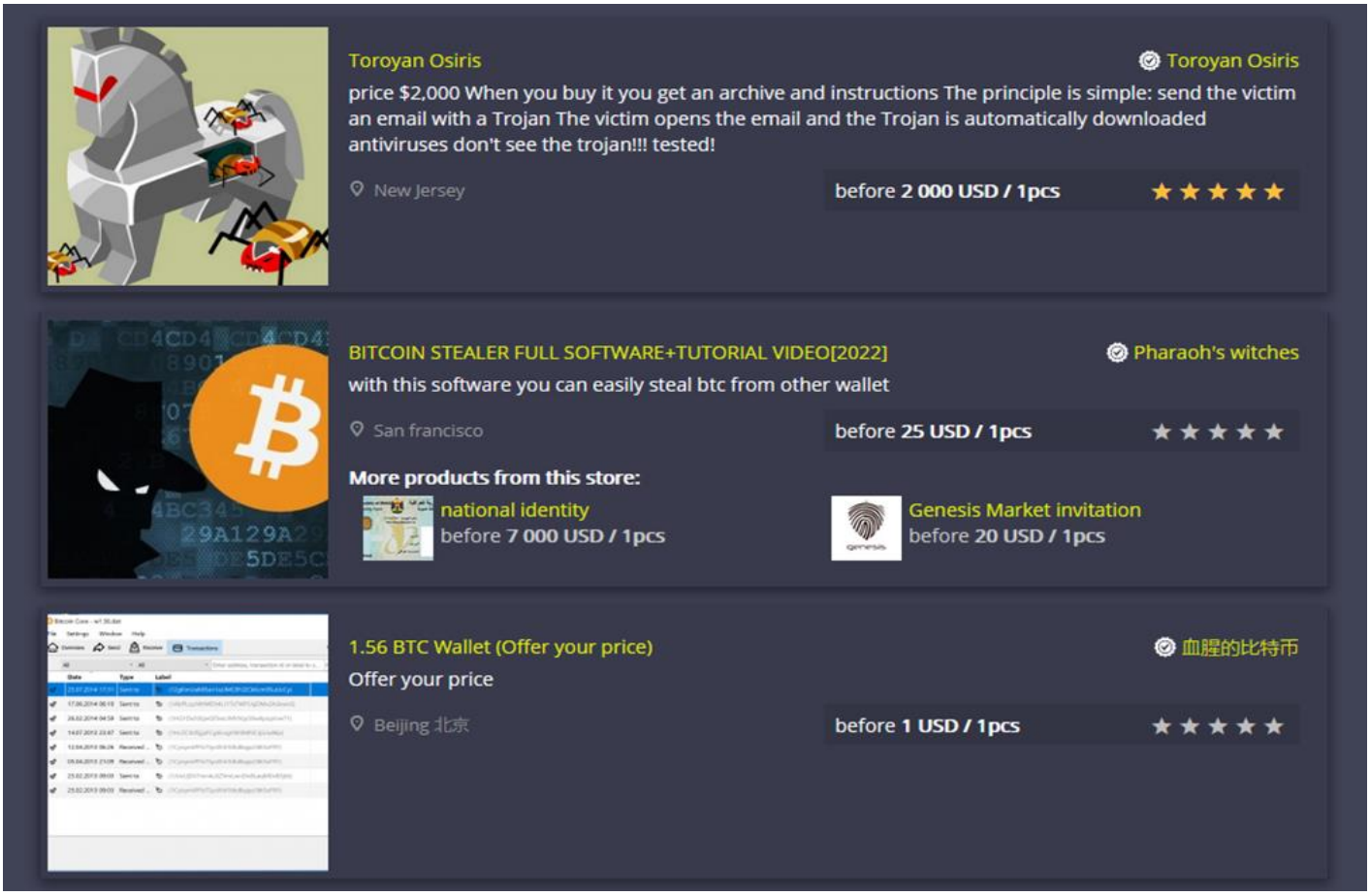


Fig. 8: Otros servicios de malware y billeteras virtuales en la DW. Captura de pantalla propia (2022).

Pero observemos un poco más, que ocurre si a nuestra búsqueda en dos pasos le agregamos la palabra “weapons” (armas en inglés). Observemos lo que nos devuelve la DW en este mercado.

ARMAS

En la imagen se puede observar un mercado ilegal de armas donde se destaca la oferta de un misil anti-tanque y otras variedades de armas.

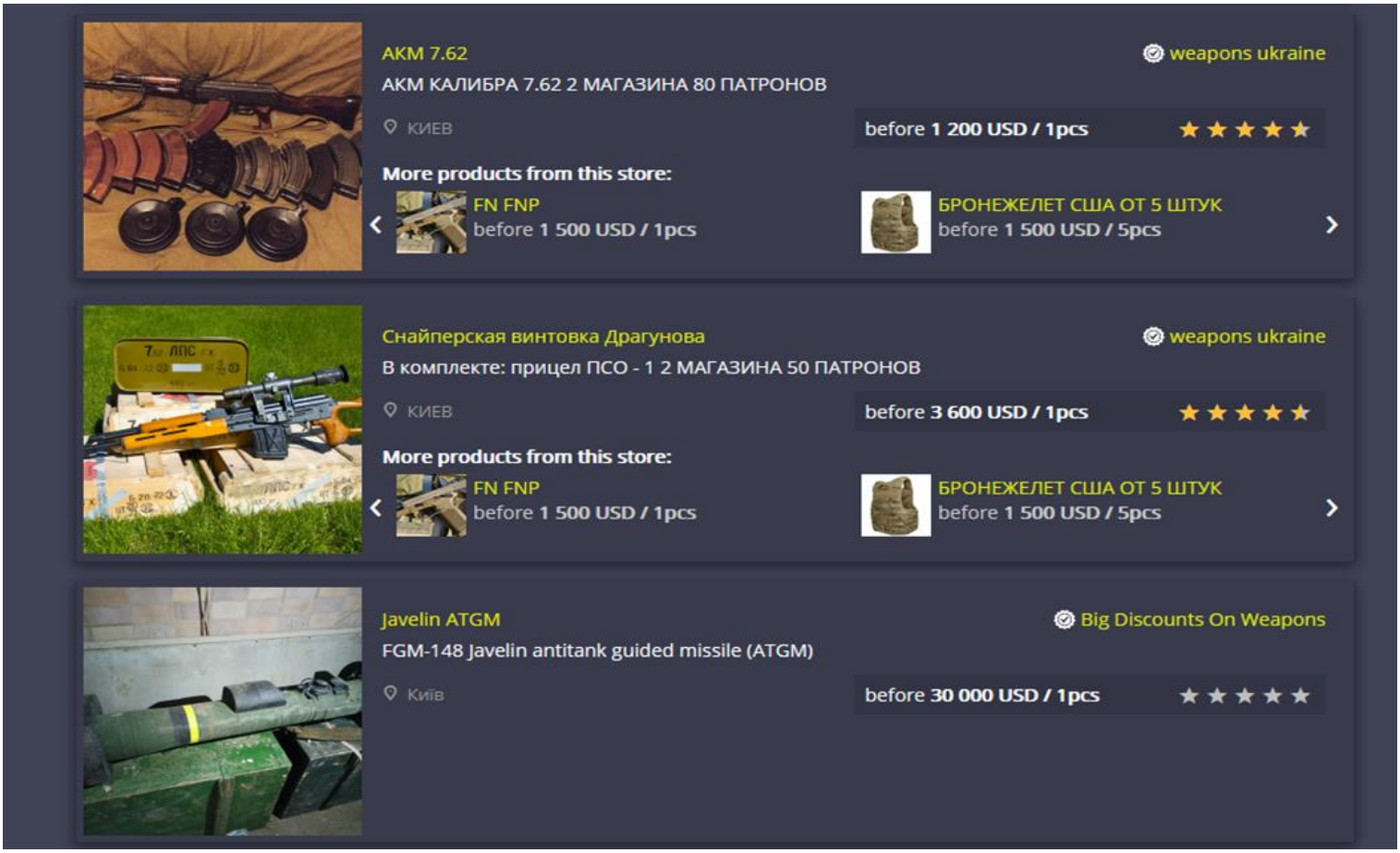


Fig. 9: Oferta de distintos tipos de armas. Captura de pantalla propia (2022).

DROGAS

Lo mismo sucede con las drogas. Se accede a una oferta de drogas poco convencionales para nuestro país, como opio de Irán, y heroína de Afganistán. Lo que podría ser un mercado interesante para un criminal local.

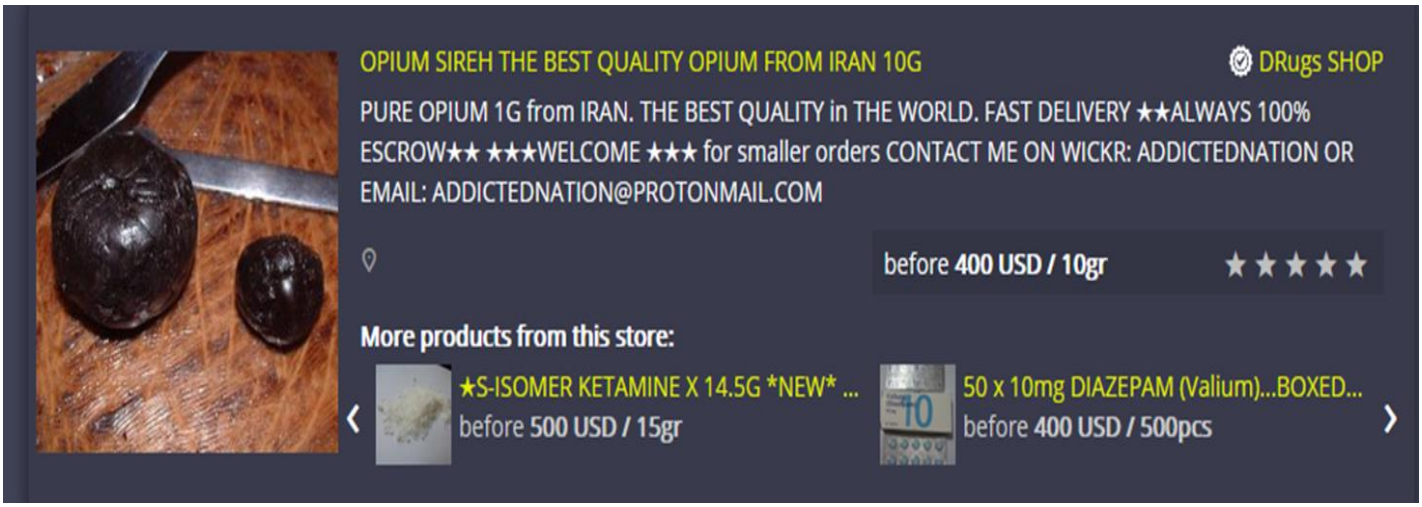


Fig. 10: Opio de supuesto origen iraní. Captura de pantalla propia (2022).

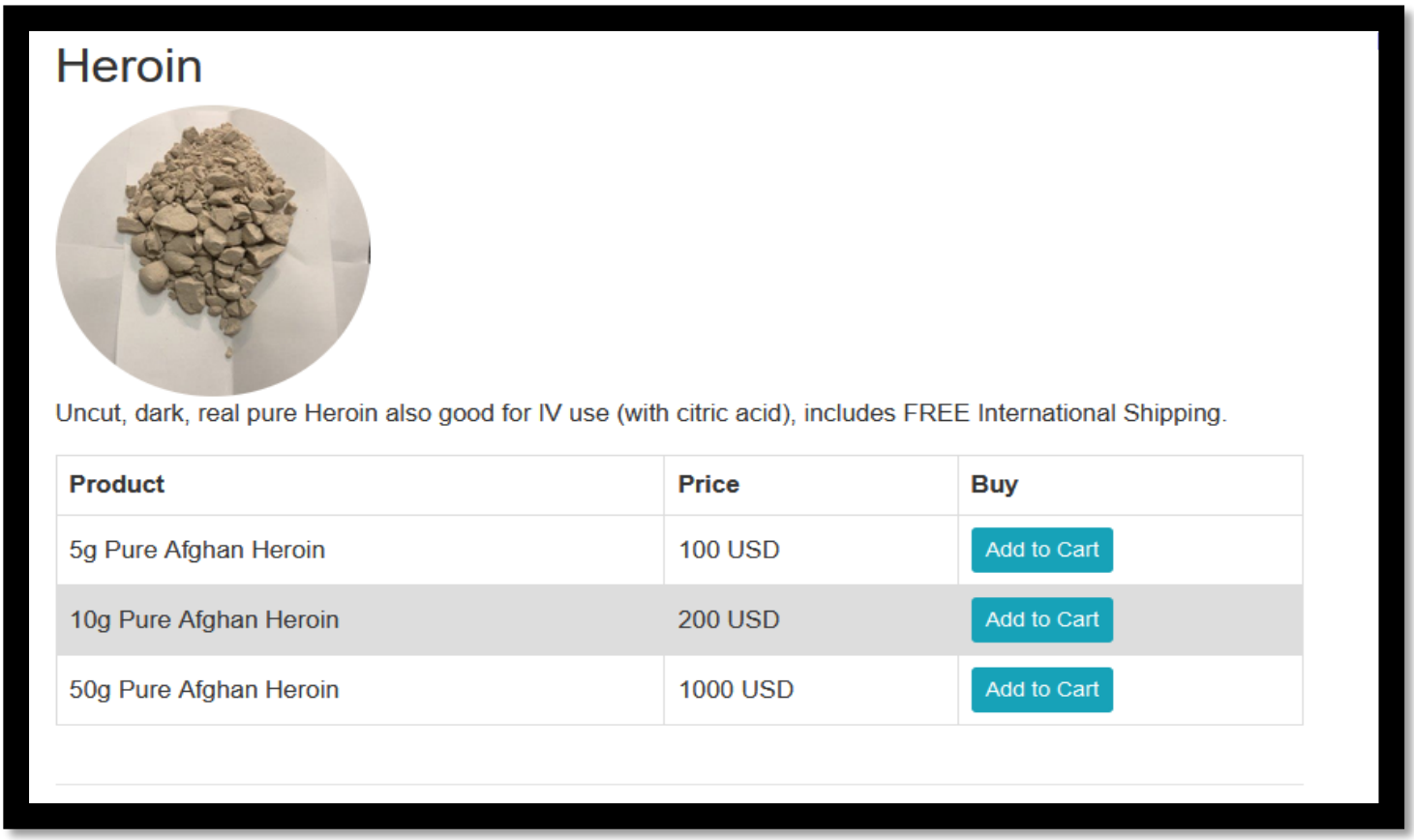


Fig. 11: Heroína de supuesto origen afgano. Captura de pantalla propia (2022).

IDENTIDADES Y CREDENCIALES

Como resultado vemos oferta de credenciales de residente de EE. UU (Green card), el ID identificación de un supuesto agente del FBI y acceso a una reconocida universidad.

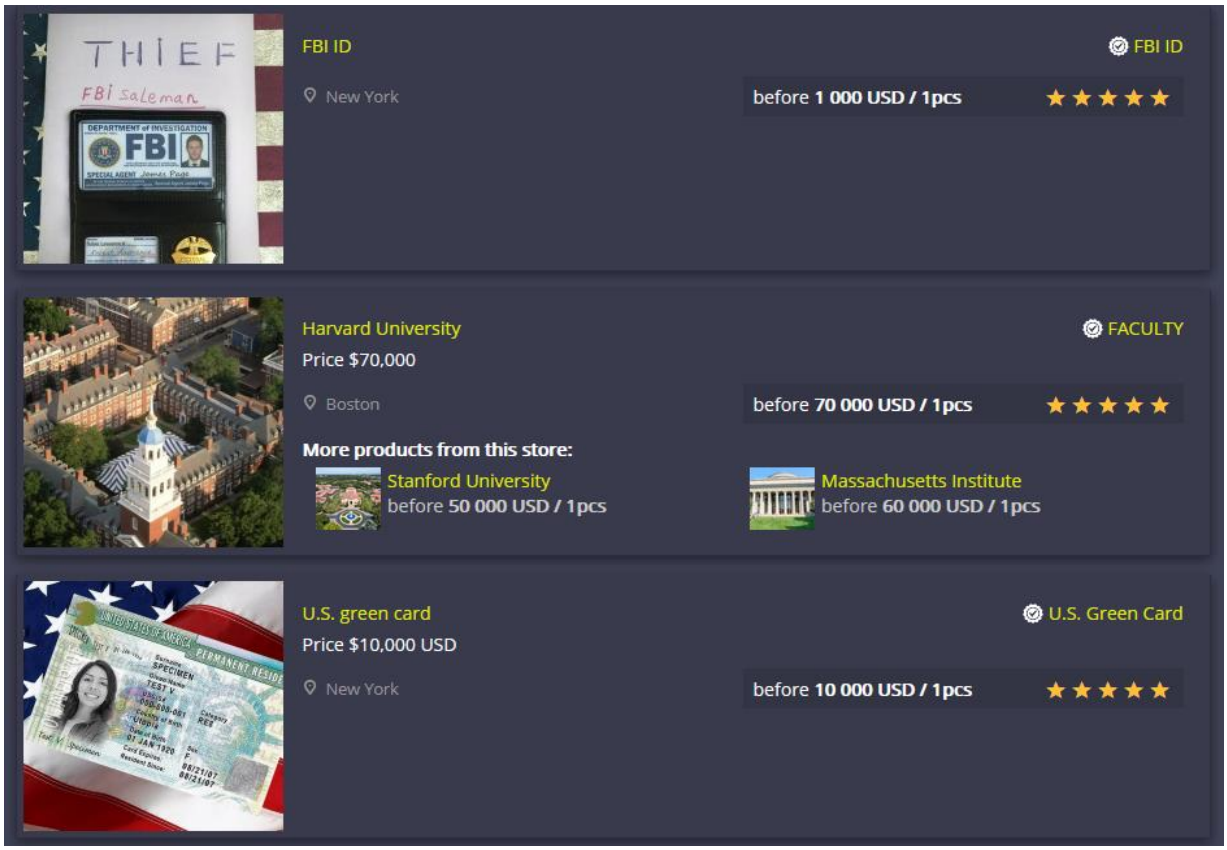


Fig. 12: Oferta de identidades y credenciales. Captura de pantalla propia (2022).

4. Propuesta de intervención

Problema a resolver

Creemos que uno de los principales problemas que rodea a la dark web (DW) es un "imaginario social" que circula alrededor de su nombre. Este imaginario se alimenta de desconocimiento, sesgos, mitos e historias peligrosas que en ocasiones impide hacer foco necesario en el problema. Si bien no realizamos una invitación abierta a navegar en un lugar donde conviven ciberdelincuentes, creemos que la comunidad de seguridad entienda que por navegar en la DW no se somete a riesgos altos. A partir de nuestra investigación se procura "desmitificar" la web oscura con la responsabilidad necesaria.

Estamos convencidos que, si cada vez más las fuerzas de seguridad o del orden público navegan con la prevención necesaria, se podrá dar un paso a favor de la lucha contra el Crimen Organizado. Creemos en la posibilidad de capacitación técnica de las FFSS. Pero deberá ser un esfuerzo conjunto con las fiscalías y jueces correspondientes. Comprender el funcionamiento como vimos en el presente estudio, es el primer paso, no requiere un gran conocimiento técnico, pero es un comienzo para ir aumentando la criticidad dependiendo de los intereses o skills de los analistas o especialistas en cibercrimen.

A modo de propuesta vamos a incentivar a un Proyecto de Capacitación de la Dark Web para la FFSS.

Estrategia a implementar

La propuesta en cuestión consiste en un Proyecto de Capacitación. La principal idea es formar a las fuerzas de seguridad en la utilización y navegación de la DW. De manera simple y rápida. Se enseñará la securización necesaria y al alcance de cualquiera persona. La idea es optimizar los tiempos y que luego de una clase teórica se inicie una práctica con los requisitos mínimos de seguridad. Además, con el fin de evidenciar la facilidad con la que una persona puede comenzar a incurrir en acciones delictivas mediante la DW.

Actividades a Desarrollar

Programa Federal de Capacitación de la Dark Web:

- 1° Clase teórica: Funcionamiento, casos y bibliografía acerca de la DW.
- 2° Clase práctica de securización personal: En este apartado se explicarán los requisitos para navegar de forma segura, acompañando al oficial de las fuerzas a que configure una VPN (Virtual Private Network), para que su tráfico de red pase por otro lado y el proveedor de internet no pueda saber a

qué sitios se está accediendo. A su vez que se instale en su PC terminal una máquina virtual. Se enseña a trabajar con máquinas virtuales para que la computadora de trabajo en caso de descargar un malware o sufrir un ataque no se vea afectada. Simulando un ambiente de laboratorio de prueba. Una máquina virtual emula un sistema operativo dentro de nuestra PC física.

- 3° Clase búsqueda en la Web Oscura: De acuerdo a los delitos de interés cada grupo buscará material relacionado al Crimen Organizado o cibercrimen.
- 4° Clase toma de contacto: Con la creación de una cuenta fake (usuario-email) el oficial de acuerdo a las posibilidades otorgadas por la autoridad de aplicación del presente programa, intentará contactarse y negociar con el ciberdelincuente.

Intervención y acciones de evaluación

A partir de lo expresado anteriormente se intenta contribuir al combate del cibercrimen. Es lógico que muchas de las practicas descriptas hoy se hagan. Es una realidad de la post Pandemia la falta de Recursos Humanos en tecnologías de la comunicación e información. Si cada vez aumentamos más el tráfico de las redes de internet nuestras vidas comienzan a desempeñarse por sistemas de comunicación, las fuerzas de seguridad no pueden estar por detrás, ya que de esta manera se alejaría más la brecha entre el know how del crimen organizado y las políticas de seguridad.

Con esta intención la propuesta de intervención es socializar el conocimiento, en este caso con la fuerza, pero también se pude extender al organismo que lo necesité como al sistema nacional de inteligencia, FFAA. La aplicación de estas habilidades en la red oscura es solo un puntapié inicial para las investigaciones en los distintos niveles observados en el marco teórico. Se puede combinar con otras figuras legales como la entrega controlado o directamente ingresar con perfiles falsos y estar años intentado detectar organización oculta como puede ser una red de pedofilia.

Las opciones son varias, pero sin duda que de cara al futuro se deberán realizar cada vez más relaciones del factor humano con la tecnología.

5. Conclusiones

Para finalizar el trabajo final de integración, nos proponemos responder las preguntas de investigación sobre: 1- ¿Cuáles son las principales herramientas delictivas, utilizadas por cibercriminales en la DarkWeb observadas en organizaciones argentinas durante los años 2020/2023? 2- ¿Cuál es el alcance a modo exploratorio utilizando TOR para navegar en la web oscura?

La investigación tuvo como fin analizar e identificar modalidades utilizada tanto por el Crimen Organizado como el ciberdelito. Retomando la cita de La Convención de las Naciones Unidas contra el Crimen Organizado Transnacional (2020) define como "grupo criminal organizado" a un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención, con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material. Además, según la ONU: "En el artículo 2(a) se específica que un "grupo criminal organizado" es:

- Un grupo de tres o más personas que no fue formado de manera aleatoria;
- Que ha existido por un periodo de tiempo;
- Actuando de manera premeditada con el objetivo de cometer un delito punible con, al menos, 4 años de encarcelamiento;
- Con el fin de obtener, directa o indirectamente, un beneficio financiero o material."[11]

Si en la definición se habla de 3 o más personas digamos que un ciberdelincuente que opera en soledad queda fuera de la definición de C.O, pero estaría íntimamente relacionado ya que sus mercancías pueden llegar a ser las mismas.

Ahora, para responder la pregunta n°1 en cuanto a las principales herramientas delictivas utilizadas en argentina 2020/2023 a partir de lo reportado, podríamos coincidir a

[11] UNODC.ORG. Crimen Organizados Transnacional. (2020). https://www.unodc.org/ropan/es/organized-crime.html

partir de búsquedas que los distintos tipos de malwares o software maliciosos especialmente diseñados para engañar, robar o estafar a las personas son muy utilizados. Creemos a que esto se debe a la facilidad de operar de manera remota y con un alto nivel de anonimato.

Si una gran parte de las instituciones del Estado están constantemente recibiendo ciber-ataques como ejemplificamos en el diagnóstico, podríamos concluir que es una forma novedosa y cómoda para los cibercriminales. Así lo plantea último reporte del Banco internacional Allianz (2022). "Risk Barometer, the most important businnes risk for the next 12 month and beyond, based on the insigth". los ciberataques son la principal pérdida económica para las empresas por encima de desastres naturales. (Pag.6). La ciberseguridad es un lugar que en los próximos años tendrá un gran desarrollo con la necesidad de trabajar con recursos humano creativo y novedosos en la actividad del ciberdelito. Cada vez que cambia una tecnología podríamos asegurar que hay nuevas vulnerabilidades para explotar. La capacitación y actualización constante será obligatoria para la seguridad de los sistemas de información y comunicación.

Así como no se forma un analista de inteligencia en uno pocos años lo mismo sucede con los analistas de ciberinteligencia. Muchas veces pensamos que los analistas de sistemas deben saber de ciberseguridad y no es así, es un error común. Muchas veces por falta de información, o por el simple hecho que su carrera profesional fue hacia otra parte de la organización. A la falta de programadores y desarrolladores que tiene argentina hoy, no estaría mal sumarle el faltante de especialistas en ciberseguridad. Eso no quiere decir que no existan si no que son trabajos difícilmente a cubrir como el de un programador senior.

Se necesita un abordaje en conjunto, desde sistemas, seguridad física e infraestructura y desarrollo para alcanzar buenos niveles de seguridad en una empresa de otra manera siempre estaremos corriendo detrás de las emergencias con pérdidas económicas en aumento. Este no es el objetivo de la anticipación estratégica en la que se centra las actividades de inteligencia.

Volviendo al primer interrogante, a simple vista son varias modalidades de estafas ya conocidas como el phishing, Ransonware, Carding, robo de identidad y varias más cambiantes como la actividad del humano. En cuanto al narcotráfico y tráfico de armas se sabe que en Argentina no sería la dark web el principal canal de ingreso ilegal. Por lo menos hasta ahora.

En cuanto a la segunda pregunta es el alcance exploratorio de la DW. Es infinito, como plantea la revista IEEE Access en una red infinita donde pasa muchísima información, aún más de la que usamos a diario donde ya nos bombardea una cantidad de información y data a diario difícil de manejar. Digamos que con TOR ingresamos a un mundo infinito donde la ilegalidad está al alcance de cualquier persona sin muchas habilidades informáticas. Lo cual sería conveniente entender, para proceder correctamente como planteamos en el programa hacia las fuerzas de seguridad y realizar seguimientos, mediciones, estadísticas. Es investigar para anticipar hechos o evidenciar modalidades delictivas.

Como ingeniero en sistemas y a modo personal; creo haber encontrado mucho más material y de manera más accesible, comparando con otros ingresos a la Dark Web hace 6 o 8 años. Lo que me deja una sensación que, si bien la dark web por sí sola no genera o forma un criminal, las condiciones están dadas para generar costumbre o una cultura ciber – delictiva en general. Se tendrán que seguir realizando investigaciones y capacitando recursos humanos para tener reportes acertados de cómo prevenir o combatir en la red. En el presente y futuro próximo.

A su vez las limitaciones estarán dadas por el conocimiento, la responsabilidad y la inteligencia (en este caso como capacidad de resolver problemas) de las personas que decidan o tomen decisiones sobre ciberseguridad. Las inversiones en tecnología son costosas y las administraciones deberán ajustarse a los tiempos que transcurren. La inteligencia estratégica sabe, hace muchos años que las ciberamenazas llegaron para quedarse y es una herramienta civil y también bélica en casos de conflictos transnacionales.

6. Referencias bibliográficas

Allianz (2022). “Risk Barometer, the most important businnes riskfor the next 12 month and beyond, based on the insigth”. Allianz Globa Corporate.

GL, J. (2020). “Ciberpatrulla: Metodología OSINT para investigar en internet. Todas las claves de este sistema de investigación” España; Madrid. Flaticon.com.

Mitnick, K. (2007) “El Arte de la Intrusión: como ser un hacker o evitarlos”. Alfaomega, Ra-Ma. Madrid.

Shelby, James PH. D (2020) The Dark Web Guide For Beginners: The Master Guide To Using Dark Web And Know All Everything You Need About Exploiting The Dark Web

Spadaro, J.R. (2016). Inteligencia Aplicada, crimen trasnacional y derecho público. Buenos Aires: Autores de Argentina

Retzkin, S. (2018). Hands-On Dark Web Analysis: Learn what goes on in the Dark Web, and how to work with it. Birmingham B3 2PB, UK.

De León Huerta, R. (2020) “La dimensión de la ciberseguridad”. Revista: Foreign affairs Latinoamérica. Volumen 20, N° 4. México.

Eddison, Leonard (2018) Tor And The Deep Web: The Complete Guide To Stay Anonymous In The Dark Net

K., Samuel (2020) Tor And Darknet 4 Donkeys A Practical Beginner's Guide To The Secrets Of Deepweb, Internet And The Web. Pda Publishing.

Norton, Jared (2020) Tor And The Dark Net: Learn To Avoid NSA Spying And Become Anonymous Online (Dark Net, Tor, Dark Web, Tor Books Book 1)

Oliveros Sifonte, D. (1973). Manual de Criminalística. Monte Ávila Editores, Caracas: Venezuela.

Revistas Académicas y sitios web:

IEEE Access (2019) Pastor-Galindo. J; Naspoli, p; Gomez Marmol, F; Martinez Perez, G.
The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. Departament of information and Comunications Eingenieering. University of Murcia, Spain.

Recuperado de:
El surgimiento de un ecosistema criminal la: Dark Web y el Bitcoin los instrumentos del ciber-crimen. (2016). https://www.chaos-international.org/pac-135-el-surgimiento-de-ecosistema-criminal/?lang=es
UNODC.ORG. Crimen Organizados Transnacional. (2020). https://www.unodc.org/ropan/es/organized-crime.html
Argentino.gob.ar (2022). Caracterizacion de la criminalidad organizada. https://www.argentina.gob.ar/seguridad/abordaje-crimen-organizado/criminalidad-organizada
Médium.com. (2022). Deep Web vs. Dark Web vs. Darknet: ¿Cuál es la diferencia?
https://medium.com/@darkenergyarticles/deep-web-vs-dark-web-vs-darknet-what-is-the-difference-b9f2b4a4dc7f

Ministerio Público Fiscal. (2020) UFEDICY: Informe: Atención Coronavirus Covid-19.
https://mpfciudad.gob.ar/

the TOR Project. (2022).
https://www.torproject.org/

Sitio de la Dark Web:
Ahmia:
Recuperado de, Link onion:
http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/

Hidden wiki

Recuperado de: https://hidden.wiki/

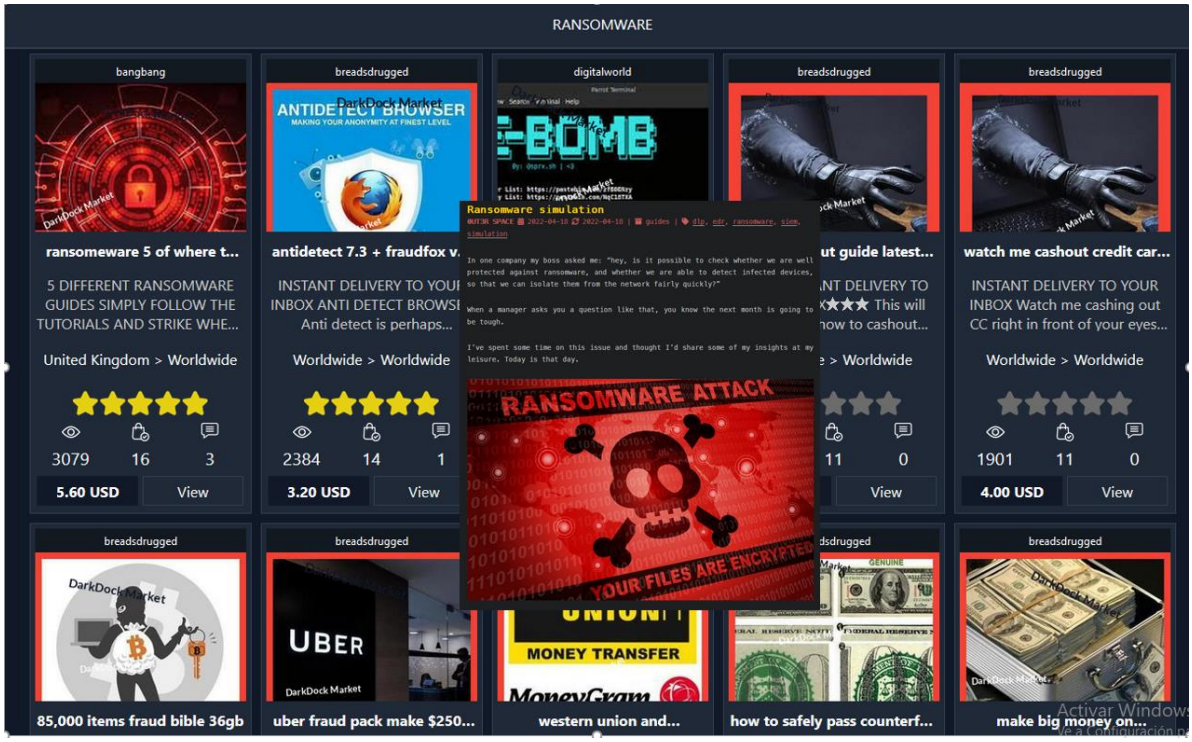
Pro hacker (2022) “ransomware a medida”

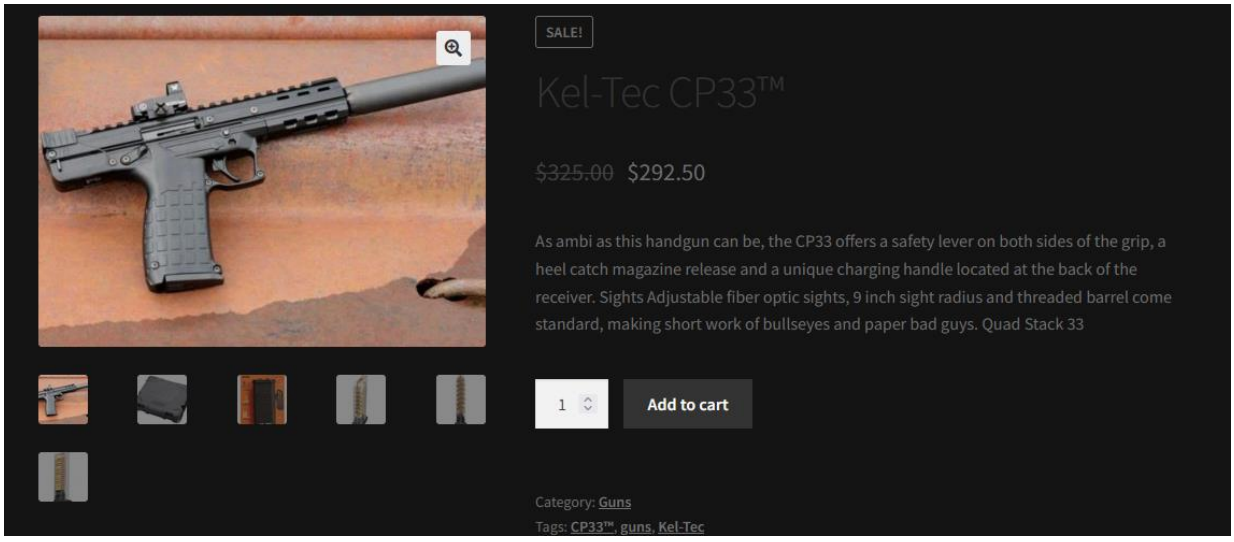
Enlace onion TOR:

http://r722lrlb2f4gat7djrogjttel4s6eumx7l4x6nd5xa7xlzjyazgjorid.onion/product/custom-made-ransomware/

7. Anexos

A continuación, y a modo ilustrativo se adjuntan más imágenes de los resultados obtenidos en las búsquedas de la Dark Web. Todas son de capturas de pantalla propias (2022).





TheHidden.Wiki TOR Onion Directory

Verified Dark Web Links 2022

Hidden Wiki

Hidden Wiki has been the directory for TOR onion links for the past decade, listing only verified dark web links.

Last Updated on **June 2022.**

Install TOR Browser from http://torproject.org/

Uncensored Hidden Wiki can be accessed using wiki47qgn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion

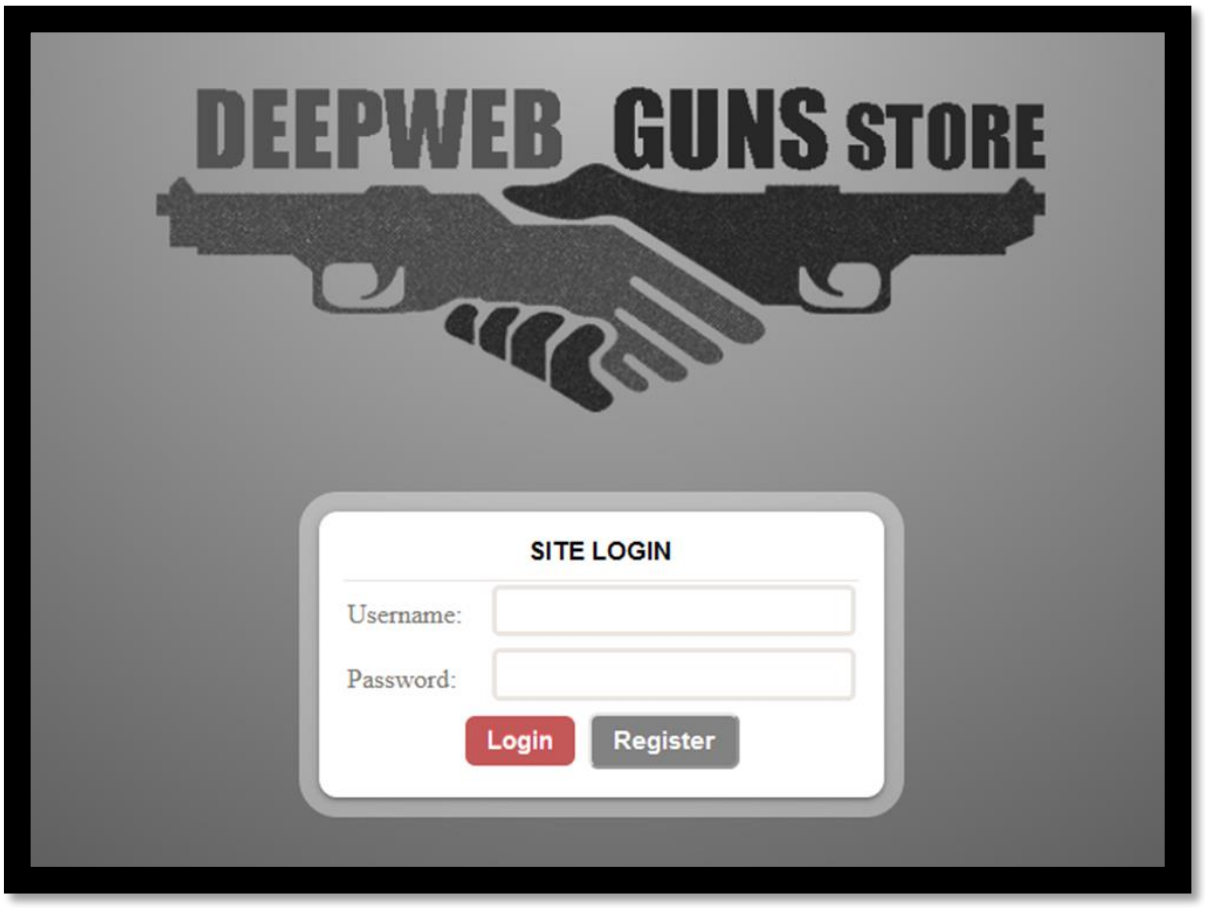
Take a minute and check our scam list to know more about dark web scammers.

Hidden Search Engines

- http://oniondxjxs2mzjkbz7ldlflenh6huksestjsisc3usxht3wqgk6a62yd.onion/ - OnionIndex Search Engine
- http://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/ - DuckDuckGo Search Engine
- http://3bbad7fauom4d6sgppalyqddsqbf5u5p56b5k5uk2zxsy3d6ey2jobad.onion/ - OnionLand Search
- http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onion/ - tordex
- http://xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion/ - Torch
- http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/ - Ahmia
- http://metagerv65pwclop2rsfzg4jwowpavpwd6grhhlvdgsswvo6ii4akgyd.onion/ - MetaGer - German Search

Commercial Markets

- http://blackma6xtzkajcy2eahws4q65ayhnsa6kghu6oa6sci2ul47fq66jqd.onion/ - BlackMart
- http://caribcc5jik7maeqfit7h34af7ntatggbmlfhyxjnqnrhij7gjt5vtid.onion/ - Caribbean Cards
- http://abraxasdegupusel.onion/ - Abraxas - offline
- http://psyshopshweetovp4em654waimmcjsf7eqifwe2d4qhnluk2b24r6dqd.onion/ - Psy Shop - Drugs Market
- http://cardzilevs4j4nj6uswfwf35oxnp64yrrtazjgap2w3vgoz2pwkp6sqd.onion/ - Cardzilla
- http://million5utxgrxru4rgmjwn7jji6bf44jkdqn3xyav6md5ebwy5l2ryd.onion/ - 21 Million Club



If you do not know what you are doing here, get out.

We have been active during the Agora, Evolution, Silkroad 3 era, then continued through Alphabay and Nucleus, and even the late Dream Market and also Wallstreet, with the same successful concept: High quality drugs combined with an extremely discreet and fast shipping. Extremely stealth shipping from our multiple warehouses!

Our email - thepsyshop@onionmail.org

We specialise in legally grown strains of dispensary quality. All our products are imported directly to guarantee you the highest quality from some of the best growers in the world. We reflect this in our prices and believe that ensuring quality of product is far more important than cheap prices. We are professionals, not street dealers, we do our utmost to deliver on our promises on time, every time.

Any of our long term customers will know this, We want to let you know that when ordering with us you are getting the very best. Sometimes this means that this is reflected in the price. We are not the cheapest but we like to think we have the BEST price to quality ratio.

Cannabis Buds

We are experienced professional cannabis growers who place emphasis on the medicinal value rather than the quantity we produce. FREE International Shipping.

Cart
Cannabis Buds
Cocaine
Heroin
MDMA
LSD

Cocaine

We offer High Quality Cocaine 90%+ with FREE International Shipping.

Product	Price	Buy
2g High Quality Cocaine	90 USD	Add to Cart
5g High Quality Cocaine	180 USD	Add to Cart
10g High Quality Cocaine	360 USD	Add to Cart

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Solicitud de evaluación de TRABAJO FINAL DE ESPECIALIZACIÓN (TFE)	Código de la Especialización **E 97**
Nombre y apellido del alumno **Alejandro Pedro Benaben**	Tipo y N° de documento de identidad
Año de ingreso a la Especialización - Ciclo	Fecha de aprobación del TFE en el Taller

Título del Trabajo Final

Estudio descriptivo sobre la DarkWeb como herramienta delictiva: Ciberdelincuencia en Argentina 2020/2023

Solicitud del docente a cargo del Taller

Comunico a la Dirección de la Especialización que el Trabajo Final bajo mi tutoría se encuentra satisfactoriamente concluido. Por lo tanto, solicito se proceda a su evaluación y calificación final.

.UBAeconómicas |posgrado
ENAP Escuela de Negocios y Administración Pública

Ing. Carlos Federico Amaya
Subdirector de la Maestría en Ciberdefensa y Ciberseguridad
c-amaya@hotmail.com

Datos de contacto del Tutor

Correo electrónico	Teléfonos
c-amaya@hotmail.com	

Se adjunta a este formulario:

- Trabajo Final de Especialización impreso (indicar cantidad de copias presentadas)
- CD con archivo del Trabajo Final en formato digital (versión Word y PDF)
- Certificado analítico

Fecha	Firma del alumno

Form. TFE v1

PRESENTAR EN LA RECEPCIÓN DE LA ESCUELA DE ESTUDIOS DE POSGRADO

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

INFORME DE EVALUACIÓN DE TFI DE LA ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO

INTERVENCIÓN DEL PROFESOR, INGENIERO ESPECIALISTA CARLOS AMAYA - DOCENTE DE LA MATERIA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

1. Conocimiento del tema (Breve apreciación respecto al marco teórico utilizado sobre el tema de investigación):
   El Ing. Alejandro Benaven ha demostrado en este trabajo un profundo conocimiento del tema

2. Actualización del Diagnóstico (como espacio vinculante entre el marco teórico y la información obtenida de la realidad respecto a la problemática abordada).
   Ha sabido explicar la temática en forma de fácil y amena lectura, lo que demuestra un amplio conocimiento teórico práctico.

3. Pertinencia y coherencia de la propuesta de intervención.
   Absoluta

4. Breve juicio del TFI (4 o 5 renglones)
   En pocas palabras puedo expresar que no solo leí e interpreté un escrito técnico-práctico. He leído un artículo donde se relata de forma amena y con calidad docente, una actividad que pocos profesionales se animan a explorar.
   Propongo a las autoridades académicas de la especialidad, incluir esta temática en la currícula de la cursada, pero en lo posible dictada por tan distinguido profesional, y ya como ESPECIALISTA.
   Sería muy difícil encontrar una personalidad que cumpla con las condiciones de analista de inteligencia, que cuente a la vez con la experiencia en la temática desarrollada en el presente trabajo.

5. Propuesta de calificación numérica (1 al 10; 6 es de aprobación), para ser considerada por el Director de la Especialización como nota final de graduación como especialista.
   Sobresaliente - 10 (diez)

INTERVENCIÓN DEL PROFESOR DE TALLER DE TRABAJO FINAL INTEGRADOR, Mg JOSE LUIS PIBERNUS:

- El TFI evaluado, reúne los procedimientos de metodología de investigación exigidos para el nivel académico de la carrera.

- Cumple con la Guía de la FCE establecida para TFE y con el Reglamento de Posgrado de la UBA.
- En su desarrollo, demuestra expertise en el área específica, que le permitió hacer un recorrido explicativo sobre la temática investigada; siendo totalmente innovador respecto a otras investigaciones de nuestra carrera.
- Se advierte una excelente integración de contenidos de distintas áreas del posgrado, que le dan un excelente anclaje disciplinar, todo ello frente al complejo problema del uso de las redes por parte de la criminalidad organizada, y específicamente las posibilidades que ofrece la web oscura o la internet profunda.
- La propuesta de intervención es totalmente coherente con el diagnóstico presentado.
- Propuesta de Calificación: **Sobresaliente, diez (10).**

INFORME FINAL DE EVALUACIÓN DEL DIRECTOR DE LA ESPECIALIZACIÓN EN INTELIGENCIA ESTRATEGICA Y CRIMEN ORGANIZADO:

He leído, con satisfacción, el aporte del Ingeniero Alejandro Benaben destinado, como sugiere, a una capacitación del sistema de seguridad de un modo visiblemente práctico. Llega a esa propuesta luego de indagar técnicamente el acceso y navegación en redes frecuentemente usadas para el delito y sobre las que pesa una cortina de equívocos y precariedades de conocimiento. Las fuentes que consulta indican que ha prestado atención a las preguntas de investigación que se propuso y a los objetivos enunciados del presente TIF, correctamente alcanzados.
Destaco que, durante el desarrollo de la especialización, su participación ha sido continuamente de excelencia, incluso formulando observaciones, con las que he coincidido respecto de aspectos curriculares en el ámbito de las TICs y que hemos receptado.
Ratifico las calificaciones que preceden.

Calificación: Sobresaliente (10). - Con mención de difusión al Ministerio de Seguridad de la Nación como aportes desde la Universidad a la capacitación técnica del sistema de seguridad.

Dr. José Ricardo Spadaro
Dir Esp en Icia Est y Crim Org
(097) – ENAP-FCE-UBA

Universidad de Buenos Aires
Facultad de Ciencias Económicas

Escuela de Estudios de Posgrado