Técnicas de OSINT para la evaluación de la superficie de ataque

Jhon Heyder Murillo Mejia

Master Ciberseguridad y Privacidad

Seguridad Empresarial

Nombre Tutor/a de TF
Manuel Jesús Mendoza Flores
Profesor/a responsable de la asignatura
Manuel Jesús Mendoza Flores

13 de junio del 2023

Universitat Oberta de Catalunya

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Técnicas de OSINT para la evaluación de la superficie de ataque*
Nombre del autor:	*Jhon Heyder Murillo*
Nombre del consultor/a:	*Manuel Jesus Mendoza Flores*
Nombre del PRA:	*Manuel Jesus Mendoza Flores*
Fecha de entrega :	*06/2023*
Titulación o programa:	Master en Ciberseguridad y Privacidad
Área del Trabajo Final:	*M1.849 - TFM-Seguridad empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*OSINT, Cibercriminal Mitre&Attack*

Resumen del Trabajo

La finalidad de este trabajo es evidenciar y/o reflejar el trabajo y conocimiento adquirido a lo largo del estudio del master en ciberseguridad y privacidad y reflejar la información e investigación llevada a cabo para realizar la evaluación de la superficie de exposición de una organización.

En el presente trabajo se pretende abordar el uso de técnicas y métodos utilizados actualmente en ciberinteligencia, para llevar acabo la recopilación y/o investigación de la posible información expuesta de una organización, que permita ser utilizada como un vector de entrada a amenazas digitales, al identificar las posibles amenazas, el trabajo reflejara su relación con las principales técnicas y tácticas utilizadas por cibercriminales para la materialización de estas y posteriormente, esta relación permitirá abordar una serie de pasos o guías que llevaran a la organización a tomar medidas mitigatorias de las mismas, de igual manera, el trabajo será realizado haciendo uso de recursos o fuentes libres disponibles en internet los cuales serán registrados y anexados como evidencia

Abstract

The purpose of this work is to demonstrate and/or reflect the work and knowledge acquired during the study of the master's degree in cybersecurity and privacy and to reflect the information and research carried out to carry out the evaluation of the exposure surface of a organizing.

This paper aims to address the use of techniques and methods currently used in cyberintelligence, to carry out the collection and/or investigation of the possible exposed information of an organization, allowing it to be used as an entry vector to

digital threats, when identifying possible threats, the work will reflect its relationship with the main techniques and tactics used by cybercriminals to materialize these and subsequently, this relationship will allow to address a series of steps or guides that will lead the organization to take mitigating measures thereof, in the same way, the work will be done making use of resources or free sources available on the internet which will be registered and annexed as evidence

Índice

Lista de figuras

Índice de Tablas

1. Introducción

1.1. Contexto y justificación del Trabajo

A lo largo de los siglos la civilización han evidenciado el desarrollo de medios de comunicación más avanzados que han surgido como parte de la necesidad de satisfacer aspectos como la interacción social, el intercambio cultural y el intercambio de bienes o servicios, también se ha usado en ocasiones como instrumento logístico en los cuerpos de seguridad de cada nación y como medio de protección y/o guerra entre países, al ir avanzando los medios y tecnologías de comunicación se generan diferentes tipos de información que al ser usada por terceros pueden o no afectar positiva o negativamente a una organización, comunidad y/o nación. Es por eso que hoy en día es imperativo la protección de la información, dentro de los métodos de protección se incluye la vigilancia de un espacio virtual llamado **ciberespacio** el cual se puede considerarse como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física[1] es en este ciberespacio que hoy en día se evidencia la interacción de actores como hackers o cibercriminales que usan la información disponible en el ciberespacio para realizar un reconocimiento previo de sus víctimas y así realizar ciberataques, con el ánimo de mitigar o monitorear esta actividad nace la ciberinteligencia y sus técnicas de investigación asociadas como el OSINT.

La Ciberinteligencia puede definirse en dos palabras en **Ciber** e **Inteligencia**, **Ciber** prefijo, creado por acortamiento del adjetivo cibernético, que forma parte de términos relacionados con el mundo de las computadoras u ordenadores [2] e **inteligencia** (Capacidad de entender o comprender) [3]. de igual manera, Existe una enseñanza del filósofo militar sunt-zu que puede aclarar un poco el concepto o base de la inteligencia, en el ámbito militar **sun-tzu decía** "**Si conoces al enemigo y te conoces a ti mismo, no debes temer el resultado de cientos de batallas. Si te conoces a ti mismo, pero no al enemigo, por cada victoria que ganes también sufrirás una derrota. Si no conoces ni al enemigo ni a ti mismo, sucumbirás en cada batalla**"[4] como se ha indicado la ciberinteligencia puede ser definida como el espacio virtual en el que se realizan actividades para comprender y entender las acciones de un enemigo o actor del ciberespacio ya sea para uso militar o no, es por eso que en este trabajo se pretende mostrar las técnicas que pueden ser utilizadas en el ciberespacio para obtener inteligencia de una organización a través de métodos de investigación como OSINT, la información obtenida puede ser utilizada positivamente o negativamente por los diferentes actores del ciberespacio, hacker, cuerpos de seguridad, países y empresas, cada actor involucrado puede obtener información privilegiada que posteriormente se transforme o materialice en posibles amenazas digitales para la organización objetivo.

1.2. Objetivos del Trabajo

- Identificar y evaluar la superficie de exposición de la organización "ETB (Empresa de Teléfonos de Bogotá) por medio del uso de metodologías de inteligencia como OSINT que permita reconocer en primera instancia los activos expuestos y la información que pueda ser de utilidad para un cibercriminal.

- Categorizar y clasificar la información recopilada a partir de su naturaleza, de tal manera que se logre proporcionar un contexto más identificativo que permita identificar los posibles riesgos o aspectos negativos que tiene la organización y su posible uso ante posibles amenazas digitales conocidas por parte de los adversarios o cibercriminales.

- Por medio de la información recopilada y tipificada se elaborará un proceso de inteligencia de amenazas que permitirá valorar la superficie de exposición de la organización e identificar los posibles vectores de ataques comúnmente utilizados por los cibercriminales generando de esta manera información que permita la toma de decisiones enfocada a proteger la integridad, disponibilidad y confidencialidad de la organización, evitando de esta manera la materialización futuras amenazas.

- Enmarcar por medio de la matriz de Mitre&Attack los posibles vectores de ataqué previamente definidos, generando de esta manera enriquecimiento a la inteligencia de las amenazas identificadas con el fin de sugerir y recomendar medidas preventivas.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

En el presente Trabajo Final de Master, se ha procurado ser objetivo e imparcial en las observaciones y citaciones del mismo, manteniendo un lenguaje que sea lo más entendible posible, sin ningún sesgo cognitivo que permita desviar la objetividad de lo planteado en el mismo.

En el desarrollo del presente trabajo estará alineado a la **dimensión de la sostenibilidad,** ya que en la investigación, ejecución y resultados son enteramente sin usar ningún recurso físico que tenga un impacto significativo sobre el medio ambiente, puesto que el trabajo se concentra en demostrar carencias de seguridad a través de una evaluación digital a los activos de una organización haciendo uso de medios tecnológicos, los cuales permiten una mayor eficiencia en el estudio a realizar y sin utilizar recursos naturales u orgánicos que afecten al medio ambiente.

En cuanto a la dimensión de **comportamiento ético y responsabilidad social** se puede contemplar un impacto negativo sobre el uso que pueda llegar a tener por terceras personas sobre la información contenida en el presente documento, ya que a

pesar de que la información anexa es pública, sigue siendo una recopilación importante que puede conducir al lector a producir ideas negativas y/o maliciosas que sean de utilidad para el daño de la organización o que permitan ser utilizadas como guía para otros fines, para mitigar este impacto el trabajo contempla anexar la información más delicada como un documento anexo y contempla la limitación de información clasificada como confidencial como es el caso de datos de ubicación, salarios, estado de salud estados financieros entre otros.

En la **dimensión de diversidad y género y derechos humanos,** el TFM propuesto puede contemplar información técnica que sea identificada como útil para el desarrollo del TFM sin importar la distinción de género, sin embargo, puede abarcar información de propiedad intelectual o llegar a identificar información corporativa a pesar de esto, el presente documento tratara de mitigar este impacto abordando todos los aspectos en la misma medida con el fin de utilizar la información necesaria para el desarrollo de los objetivos.

1.4. Enfoque y método seguido

Dentro de la revisión de trabajos previos y experiencia laboral propia, el TFM consistirá en brindar un contexto base de los métodos de investigación y recopilación de inteligencia actuales como el **OSINT** el cual puede ser aplicado a cualquier ámbito de investigación que involucre fuentes de información abierta, de igual manera, al trabajar con técnicas como OSINT se hará uso del concepto del ciclo de inteligencia que nos permitirá tener una metodología o pasos para aplicar las técnicas de OSINT a la hora de evaluar la **superficie de exposición**.

Por otro lado, el uso de las técnicas y herramientas abordadas en el presente trabajo, han sido utilizadas por diferentes investigadores y profesionales en la industria, sin embargo, el presente trabajo está enfocado en guiar y usar formas efectivas por medio del uso de la herramienta de **spiderfoot**, el cual es un framework de trabajo que permitirá integrar varias fuentes de información en una sola herramienta, permitiendo de esta manera la centralización de la información y sin tener problemas en cuanto su análisis y su descentralización, el cual es uno de los principales problemas a la hora de investigar o recopilar información.

La herramienta spiderfoot nos permitirá concentrarnos en la rápida búsqueda de información expuesta en fuentes abiertas previamente integradas al software el cual estará instalado sobre un sistema libre, generando de esta manera una solución completamente de código abierto para la generación de inteligencia y evaluación de superficie de exposición de la empresa ETB. una vez se pueda identificar los principales activos con la herramienta procederemos a concentrarnos y ahondar aún más en cada activo expuesto identificado, haciendo uso de las técnicas de OSINT pero en fuentes distintas a las ya utilizadas.

1.5. Planificación del Trabajo

#	Actividad	Inicio	Fin	Duración
Planificación				
1	Realizar anteproyecto(definición de alcance, objetivos ..)	01/03/2023	13/03/2023	12
Investigación				
2	Revisión de literatura para la definición de antecedentes que permita conocer el aporte de otros trabajos	13/03/2023	05/04/2023	23
3	Investigación sobre OSINT	13/03/2023	05/04/2023	23
4	Investigación sobre el framework Spiderfoot	13/03/2023	05/04/2023	23
5	Investigación sobre el ciclo de inteligencia de amenazas	29/03/2023	05/04/2023	7
6	Búsqueda de amenazas digitales comúnmente utilizadas en organizaciones a través de informes de tendencias o reportes anuales de amenazas de empresas de seguridad	12/04/2023	17/05/2023	35
7	Investigación sobre la matriz Mitre&Attack	19/04/2023	17/05/2023	28
Ejecución				
7	Instalación del entorno de trabajo y el framework Spiderfoot	13/03/2023	22/03/2023	9
8	Ejecución y puesta en marcha del entorno de trabajo y fuentes adicionales para la recopilación de información	13/03/2023	17/05/2023	65
9	Identificación de activos expuestos como marcas, IP dominios, redes sociales	13/03/2023	05/04/2023	23
	Definición de amenazas y sus respectiva relación con Mitre&Attack	12/04/2023	17/05/2023	35
Conclusión o finalización				
10	Redacción de las recomendaciones o controles sugeridos	24/05/2023	13/06/2023	20
11	Redacción de la conclusiones	07/06/2023	13/06/2023	6
12	Elaborar video y presentación	14/06/2023	20/06/2023	6

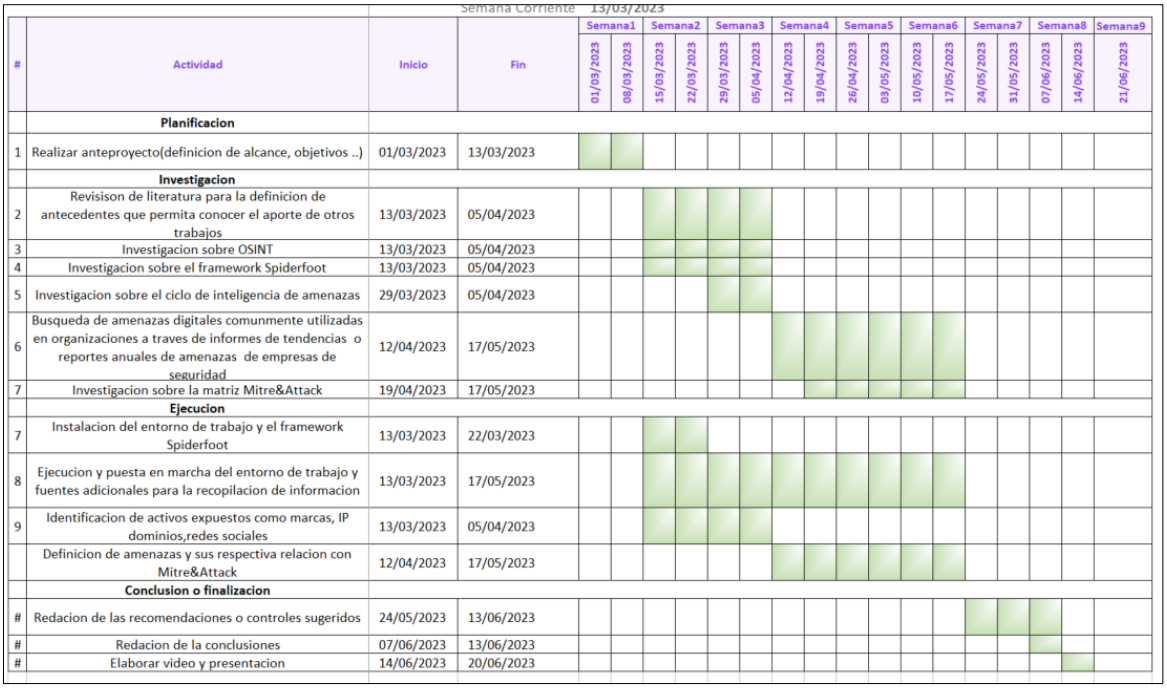


Ilustración 1 Diagrama de Grant

1.6. Breve sumario de productos obtenidos

El resultado de la investigación del presente trabajo permitirá conocer una forma general de evaluación de superficie de exposición que servirá como guía para futuras investigaciones, el producto final será una entrega donde se vea el análisis, evaluación y recomendaciones de los resultados de los escaneos realizados en la herramienta spiderfoot, estos ítem estarán inmersos en el mismo trabajo de investigación además de lo comentado anteriormente se registrara como abordar o identificar una superficie de exposición y como identificar amenazas asociadas a los activos expuestos con sus principales recomendaciones o mitigaciones

1.7. Breve descripción de los otros capítulos de la memoria

2. Motivación

Hoy en día las organizaciones y/o personas no son conscientes de lo importante que es mantener la información restringida o limitada a quien autoricemos o queramos es por esto que este trabajo representa para mí una visión de las maneras en que actualmente los grupos cibercriminales pueden llegar a utilizar la información tanto como personal como de las empresas para llevar a cabo hechos delictivos como extorsión, daño reputacional, perdidas económicas entre otros, mi motivación personal radica en la experiencia laboral que he tenido al constatar el uso de esta información en diferentes ámbitos y nace con el fin de poder mostrar las deficiencias en la protección de datos y activos que actualmente tiene las organizaciones con el fin de generar conciencia ante

sus directivos para que se realice un mayor control de los datos que se exponen y del papel que tiene como actores en la protección de datos.

3. Riesgos

- Se identifica un posible riesgo en la actividad de instalación del entorno de trabajo y de la instalación del framework spiderfoot

En ocasiones puede ocurrir fallos de incompatibilidad entre librerías o paquetes de instalación es por esto que he decidido como base del sistema operativo la distribución de kali que está basado en debían Linux, esta implementación me ha funcionado en muchas aplicaciones de investigación en mi ámbito laboral de igual manera para mitigar el riesgo asociado a la instalación del framework podemos utilizar la guía de instalación de la página oficial https://intel471.com/attack-surface-documentation#installing

- Se identifica el riesgo en las búsquedas de la organización elegida, puede que no se identifique información suficiente

Para mitigar este riesgo se realizara una búsqueda inicial de la empresa objetivo con el fin de identificar posibles activos expuestos, de igual manera, se tiene en cuenta la elección de la organización basado en un contexto local y comercial en el que actualmente está la organización, como visión general he evidenciado que la empresa pública de teléfonos de Bogotá (ETB) ha tenido un crecimiento exponencial en sus operaciones en la ciudad de Bogotá esto me permite suponer una exposición mayor de su marca por ende la hace más susceptibles a exposición de información

- Se identifica el riesgo de no cumplir con el resultado esperado en cuanto a la relación o identificación de amenaza potenciales

Es posible que al terminar la investigación la información identificada no sea tan relevante como se esperaba, sin embargo, dependerá del momento, análisis y fuentes que se utilicen para obtención de la información, con el fin de mitigar el riesgo se propone seguir las con la metodología de investigación escogida.

4. Estado del arte

Se puede decir que la ciberinteligencia surge como una necesidad ante el crecimiento de un nuevo espacio digital llamado ciberespacio en donde convergen todos los desarrollos tecnológicos afines al crecimiento cultural y social de la sociedad actual, el uso de estas tecnologías emergentes como redes sociales, celulares, aplicaciones móviles, telecomunicaciones entre otros desarrollos, ha generado que la sociedad pase de un ambiente de interacción física a una interacción más digital, al compartir más información cada día por este medio, la información se convierte en un activo vital para las personas y la sociedad, es por esto que la información juega un papel muy importante en la sociedad y en las naciones, como dijo el político filósofo **Sir Francis Bacon** (1561-1622) "**el conocimiento es poder**" esta frase aplica mucho en el ámbito militar, ya que el uso de tecnologías en el ámbito militar hace que se amplíe su conocimiento sobre el enemigo por ende es imprescindible el uso de la ciberinteligencia y las técnicas de recopilación de información como OSINT para el conocimiento de actuales y futuras amenazas, lo anterior se adapta a lo definido por El Centro de Tecnologías Emergentes de la Universidad Carnegie Mellon, quien define la ciberinteligencia como "**La adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye la toma de decisión**" [5]

No solo en el ámbito militar se identifican amenazas, en las sociedades más modernas se evidencia la aparición del cibercrimen que hace uso del internet para cometer o generar nuevos delitos que anteriormente no se conocían como el **ciberespionaje**, **suplantación de identidad digital**, **robó de información**, secuestro de información como el **ransomware**, a medida que nuevos métodos de cibercrimen surgían o se creaban, nacían de la misma forma bandas cibercriminales que los cometían llamados APT(amenazas avanzadas persistentes).

Teniendo en cuenta lo expuesto anteriormente, las técnicas de recopilación de información como OSINT nacen como una solución a la fase de recopilación de la inteligencia de amenazas para aquellos organismos o personas que requieran actuar proactivamente frente a ciberamenazas.

5. Metodología

En ciberinteligencia es imprescindible hablar del proceso o ciclo de inteligencia, el cual de acuerdo al Centro nacional de inteligencia de España, el Ciclo de Inteligencia está compuesto por todas aquellas actividades que, de forma ordenada, persiguen la transformación de información en bruto en inteligencia[6]

Se contempla seguir como metodología, el ciclo de inteligencia definido por el centro nacional de inteligencia(CNI) asociado al CERT de España, el cual indica 5 fases o pasos a seguir para generar inteligencia.

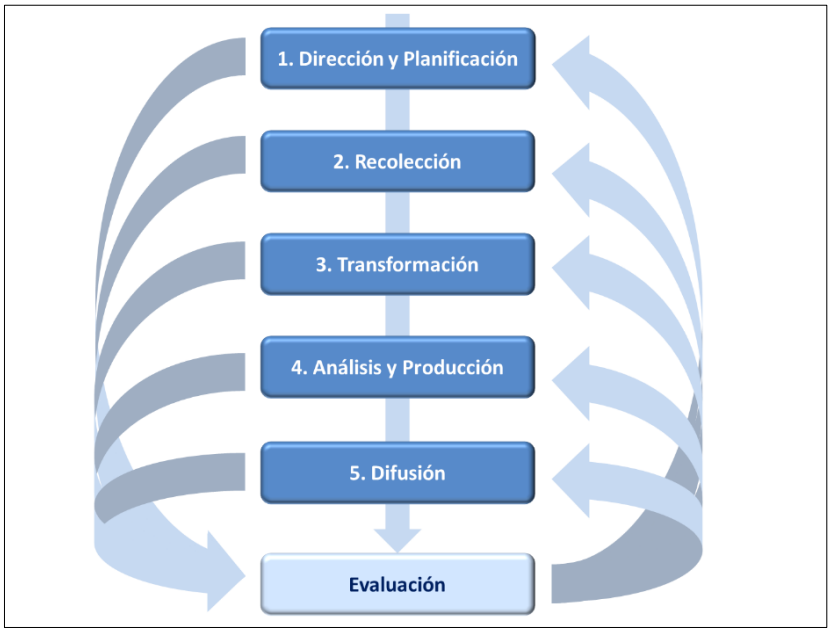


Ilustración 2 Ciclo de Inteligencia

tomada de https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html

Para el presente TFM no se abarcarán todas las fases de la ilustración 2, ya que se trabajará en las 4 principales fases

5.1. Definición de pasos o proceso a realizar para el cumplimiento de los objetivos

En la primera fase de **dirección y planificación** se optará por definir la empresa objetivo, para este caso se realizara una búsqueda inicial en donde se explorara el contexto o industria a la que pertenece y se tendrá en cuenta su exposición de marca, la cual puede estar relacionada con la cantidad de reconocimiento o interés que se tenga para la persona del común y/o interés comercial, de igual manera, el foco de atención estará en demostrar y concientizar la superficie de exposición de la empresa objetivo con el fin de demostrar el impacto que puede llegar a tener para la empresa en materia de ciberseguridad ante ciberamenazas.

La segunda fase contempla la **recopilación inicial y gradual de información** que se obtenga del objetivo, en esta fase definiremos los principales activos expuestos, se aplicara las técnicas de OSINT conocidas para la recopilación y consolidación de activos expuestos como la búsqueda de IP o dominios asociados a partir del nombre de la organización, las redes sociales, exposición de la marca y sedes físicas, a esto lo llamamos comprender la superficie de exposición.

En la tercera fase la **transformación y enriquecimiento de la data** obtenida, con el fin de establecer una matriz de relevancia en la que se indique el tipo o categoría de cada activo y directa relación con posibles amenazas, esto se lograra con una investigación previa de amenazas o vectores de ciberataques que comúnmente utilizan los cibercriminales.

En la fase de **análisis y producción** procederemos a relacionar las amenazas identificadas en cada uno de los activos expuestos con sus posibles vectores de ataque y relacionándolos con las técnicas y tácticas de la matriz de Mitre&Attack con el fin de reconocer las posibles mitigaciones o recomendaciones asociadas

5.2. Recursos empleados

- **Software de virtualización** para la recreación del ambiente aislado y seguro que permitirá anonimizar el proceso de investigación y evitar dejar registro de huella personal del investigador

- Entorno o **framework** de trabajo **Spiderfoot**, esta herramienta de uso libre y privado nos permitirá recopilar y centralizar la mayoría de información posible de la empresa objetivo

- **Cuenta de correo electrónico**, para el uso de API de conexión y acceso a recursos abiertos de suscripción

- Fuentes o **técnicas de OSINT** que apoyen a la búsqueda de información pasiva de la empresa objetivo, las fuentes de investigación pueden abarcar tanto la web superficial como la deepweb

- Framework y/o Matriz de **Mitre&attack**, https://attack.mitre.org/resources/working-with-attack/

- Herramienta de citas bibliográficas https://app.bibguru.com/p/ba590349-8f6a-438b-91f5-e889422b316e

- Herramienta online de apoyo en la redacción del trabajo https://languagetool.org/editor/new

- **Anonym8**: herramienta de anonimizacion para búsquedas en la red Tor

5.3. Fase de Dirección y planificación

Se procede a registrar los hallazgos y a contextualizar el propósito principal de la **Empresa de Teléfonos de Bogotá (ETB)** esta empresa legalmente constituida en Bogotá Colombia, nació el 28 de agosto de 1884 como una empresa de servicios de teléfonos para Bogotá, capital de Colombia, a lo largo de los años se convirtió en una empresa pública con presencia en todo el territorio colombiano convirtiéndose en la mayor operadora de teléfonos de Bogotá, posteriormente sus servicios abarcaron la telefonía móvil e internet, sin embargo, a medida que otras operadoras hacían presencia en el país, ETB mantenía su organización sin ningún cambio significativo al pasar los años y cambios de gobierno en el país, ETB entre el año 2014 y 2023 incrementó su oferta de servicios y capital convirtiéndola en una de las operadoras o ISP que mayor ha tenido crecimiento en los últimos años, este crecimiento va asociado normalmente a enfocar los esfuerzos en la oferta de servicios, el reconocimiento de la marca y superficie de exposición de igual forma, también va asociado a posibles deficiencias en materia de ciberseguridad, debido al conocimiento y contexto local que tengo de la organización, se elige la empresa ETB como un objetivo para el presente TFM.

Ilustración 3 Logo de la empresa ETB

Página oficial de ETB https://etb.com/

A continuación, se relaciona algunas citas de medios digitales que describen el progreso y desarrollo de ETB y que dan un mayor contexto de la organización objetivo, para el presente TFM.

Como contexto anexo a lo anterior ETB, fue escogida como la compañía con mejor servicio al cliente del país según una encuesta realizada por Datexco que consulto a 12 ciudades del país [7]

ETB se propone como meta abarcar el 80% de clientes conectados del país aumentando la presencia del servicio de internet por medio de fibra óptica según lo publicado por el medio digital de portafolio https://www.portafolio.co/negocios/empresas/etb-le-apunta-a-tener-80-de-sus-clientes-conectados-con-fibra-579058 , esto nos indica una inversión de capital y cobertura en servicios provocando un rápido reconocimiento de la marca haciéndola que sea más probable a ser atacada por los cibercriminales

Todos estos datos nos permiten identificar a ETB como una empresa con un amplio reconocimiento público, por ende, un buen candidato para realizar este TFM

Como se mencionó anteriormente ETB es una empresa que nació en Bogotá, Colombia y ha venido creciendo su cobertura de servicios, sin embargo, como empresa de telecomunicaciones de gran expansión también es posible que sea afectada por ciberamenazas como en otras compañías de gran reconocimiento, esta hipótesis se encuentra apoyada en numerosos artículos como

- El medio digital **virtualpro.co** https://www.virtualpro.co/noticias/empresas-colombianas-a-invertir-mas-en-ciberseguridad- en el que indica los resultados de encuestas de seguridad realizadas por la empresa de auditoria EY, donde se ve reflejada una falta de inversión significante comparada con las emergentes amenazas que se han ido desarrollando

- De igual forma, se evidencia en la publicación del medio digital **cio.com (https://cio.com.mx/empresas-en-latinoamerica-no-priorizan-la-seguridad-cibernetica-al-iniciar-procesos-de-transformacion-digital-estudio-ey/)** que indica que, a lo largo de la implementación de los procesos relacionados con transformación digital no se involucran o priorizan proceso de ciberseguridad.

- Por otro lado, se ha identificado en el sitio https://ncsi.ega.ee/ncsi-index/?order=rank un ranking de los países y su posición en materia de ciberseguridad para afrontar ataques, Colombia aparece en el lugar **66** como se puede observar en la ilustración 4, esta medición es tomada y explicada en el sitio https://ncsi.ega.ee/methodology/ en él se indica los siguientes ítems

    1. Identificación de niveles nacionales de ciberamenazas
    2. Identificación de medidas y capacidades de ciberseguridad
    3. Selección de aspectos importantes y medibles
    4. Desarrollo de indicadores de ciberseguridad
    5. Agrupación de indicadores de ciberseguridad

Las fuentes de información tomadas para esta evaluación en el ranking son tomadas desde

- Actos legales
- Documentos oficiales
- Sitios web oficiales

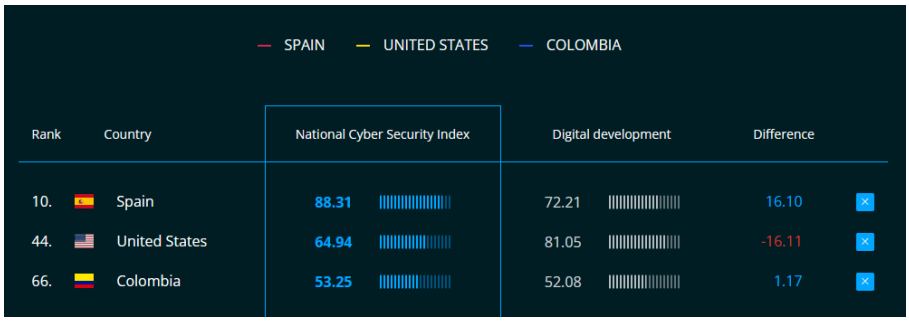


Ilustración 4 Ranking de países y su estado de ciberseguridad mundial

Todas estas estadísticas y valoraciones por firmas de auditoría, han servido como soporte y base por optar una organización colombiana para el presente TFM

5.4. Fase de Recopilación de información

OSINT es considerado como un proceso de inteligencia, por ende considera métodos o técnicas de recopilación de información para investigar un objetivo, estas técnicas son construidas generalmente por cada investigador, las técnicas pueden ser encontradas en algunos libros o blogs como pasos o playbooks para cada uno de los posibles caminos a investigar, como por ejemplo el proceso para investigar a partir de un **correo, usuario, dominio** entre otros, en el presente trabajo relacionaremos algunos enlaces de flujos de trabajo (playbook) que sirvieron como guía para la elaboración de nuestro propio playbook en este TFM

Algunos pasos propuestos para el presente trabajo son plasmados a partir de la experiencia laboral y que consideramos generales a la hora de investigar en fuentes abiertas, de igual manera estos pasos fueron construidos con ayuda de las siguientes fuentes de información

- Michael Bazzell,Capitulo 24,Open_Source_Intelligence_Techniques-Lite,Sexta Edicion, Library of Congress Cataloging-in-Publication Data, febrero del 2018, Página 443, Available from: https://bigdata-ir.com/wp-content/uploads/2021/02/Open_Source_Intelligence_Techniques-Lite.pdf
- Técnicas de inteligencia de código abierto (OSINT) para prevenir el fraude [Internet]. SEON ES. SEON; 2022 [cited 2023 Mar 20]. Available from: https://seon.io/es/recursos/guias/tecnicas-osint-para-prevenir-fraude/
- Julian Gutieerez,Metodologia Osint para Investigar en internet, ,tercera edición, ediciones ciberpatrulla,2021, Available from https://es.scribd.com/document/585579439/eBook-Metodologia-OSINT-Para-Investigar-en-Internet#
- OSINT dojo [Internet]. OsintDojo.github.io. [cited 2023 Apr 16]. Available from: https://www.osintdojo.com/

Otras fuentes de ayuda utilizadas para la construcción de los pasos fueron

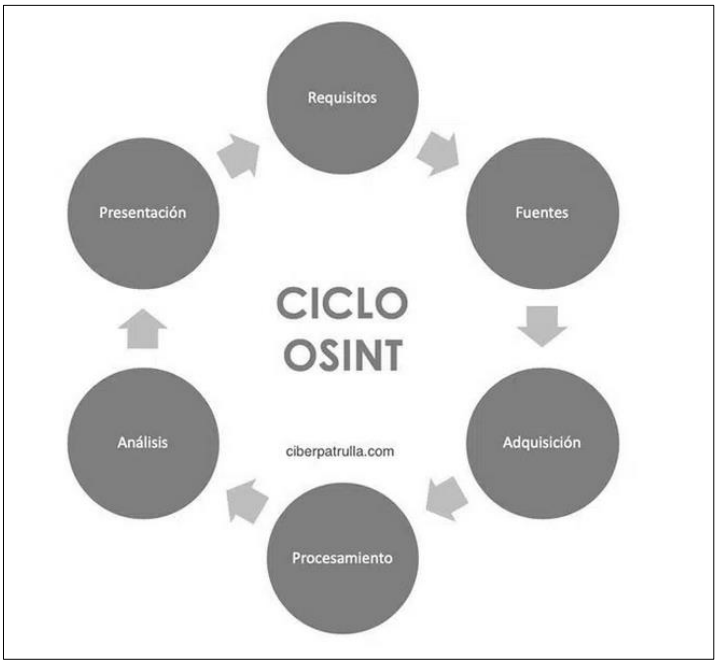


Ilustración 5 Ciclo de OSINT

tomada de https://ciberpatrulla.com/que-es-osint/#%F0%9F%91%89_Proceso_OSINT_fases_del_sistema_de_obtencion_de_informacion

6. OSINT y fase de recopilación para el presente trabajo

Tomando como referencia las fuentes citadas y los pasos del ciclo de OSINT, procedimos a formular algunos pasos para nuestra investigación.

Pasos

1. Anonimizarían del entorno y huella digital (crear cuenta de correo)
2. Realizar búsquedas con información base o conocimiento inicial (nombre de la empresa, dominio)
3. Escoger módulos o fuentes en Spiderfoot
4. Búsqueda y transformación de la información obtenida en cada módulo (fuentes de spiderfoot)
5. Análisis de los activos recopilados y sus correspondientes amenazas y/o vulnerabilidades y como estas afectan al negocio
6. Relación de amenazas y activos con sus respectivas Tácticas y Técnicas (TTP) de la matriz Mitre&attack
7. Recomendaciones y conclusiones por cada TTP

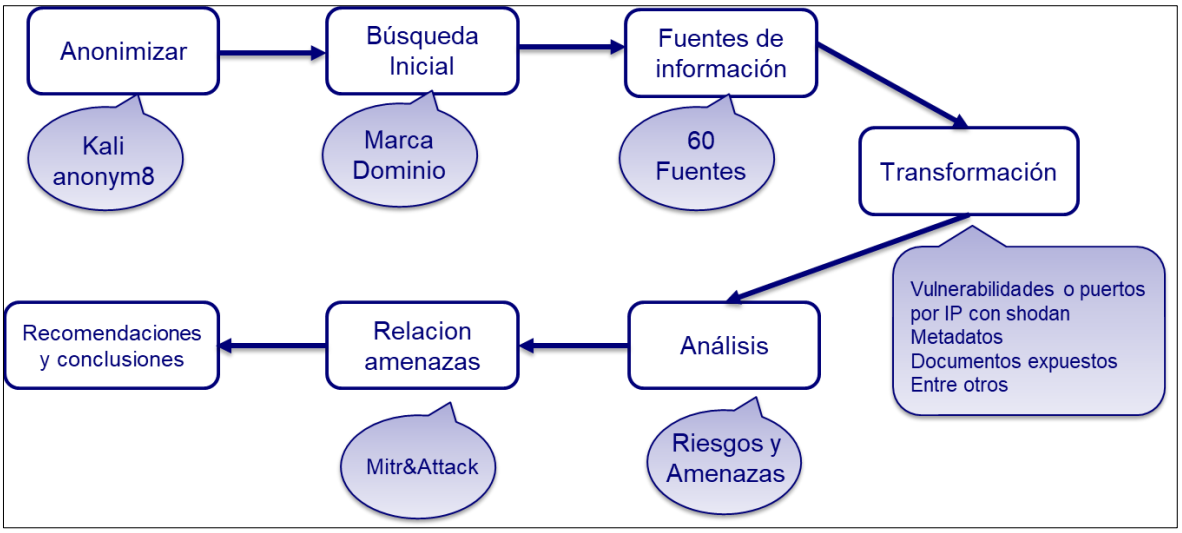


Ilustración 6 Playbook de investigación

6.1. Paso 1

En todo proceso de investigación, el investigador debe permanecer en una figura que permita ser anónimo ante su objetivo con el fin de que el objetivo no conozca las intenciones del investigador ni su identidad, el **anonimato** es usado en estas investigaciones con el fin de mantener y garantizar el proceso de investigación sin que afecte la integridad del investigador ni la de su investigación, es por esto que en este paso se describen las medidas optadas para anonimizar el entorno de investigación o entorno de trabajo.

Muchas fuentes de investigación requieren del uso de suscripción a sus servicios a través de cuentas de correo, por ende se recomienda crear una cuenta de correo gratuita en algunas de las siguientes plataformas **protonmail, Hotmail** y **Gmail**, para nuestro caso hemos creado un correo gratuito en Gmail, se debe tener en cuenta que al crear el correo no debe ser asociado con nuestra verdadera identidad es por esto que se recomienda crear un alias o un seudónimo que no permite tener una relación directa con nuestra identidad, una vez hemos creado nuestro correo procedemos a acondicionar nuestro entorno de trabajo.

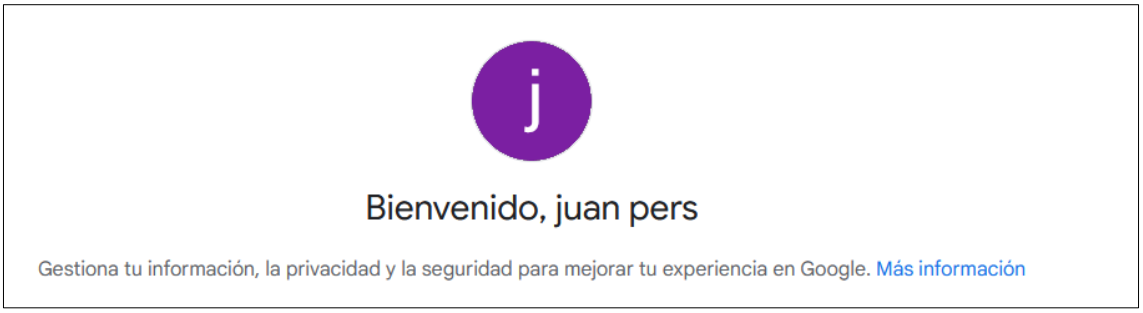


Ilustración 7 correo Gmail con el alias “juan pers”

Para el acondicionamiento de nuestro entorno de trabajo hemos instalado el sistema operativo **KALI Linux** sobre una máquina virtual que nos permite de una manera más ágil contar con mayores herramientas y una base compatible con múltiples herramientas

Otra de las opciones que podemos utilizar para anonimizar o convertir una navegación más privada en nuestro entorno es el uso de scripts como **Anonsurf**, **Proxychain y Anonym8** para nuestro caso hemos escogido **Anonym8** este script se caracteriza por tener reglas de firewall y la configuración de proxy dinámico y estático de igual manera nos permite reconfigurar nuestro sistema para que la conexión de red sea a través de la red TOR o a través de proxy anónimos, esto se lleva a cabo con el fin de evitar ser identificado a través de alguna huella digital o registro de conexión, ya que el proceso de recolección de información conlleva a un registro de conexiones en algunos casos activas sobre las fuentes en las que estamos trabajando.

6.2. Paso 2

Antes de empezar a investigar debemos de considerar las siguientes preguntas o pasos que estarán alineadas con la fase de recopilación de información

¿Cuál es el propósito de la búsqueda sobre el objetivo?

Debemos preguntarnos con qué propósito u objetivo nos ayudara aplicar las técnicas OSINT en nuestra investigación, para nuestro caso se trata de una investigación enfocada a validar activos tecnológicos o digitales expuestos de la organización que es nuestro principal objetivo y que tengan algún riesgo ante ciberamenazas, los objetivos que podemos definir como punto de partida son

activos digitales como

- Dominios
- Dirección IP
- Correos
- Exposición de documentos y marca

Se parte de la información inicial disponible como el nombre de la organización y página principal

- Marca o nombre de la empresa ETB
- etb.com
- Empresa de teléfonos de Bogotá (ETB)

6.3. Paso 3

¿Porque escoger spiderfoot para OSINT?

Spiderfoot es uno de los framework más reconocidos en el ámbito laboral y de investigación, ya que actualmente cubre la necesidad de monitorear la superficie de exposición de una organización, actualmente existen otras herramientas de código abierto como **Maltego** y **Data hunter** que ayudan al proceso de recopilación de información, sin embargo, **Spiderfoot** cuenta con características que las hace única como integrar más de **200** fuentes de información en su mayoría de uso libre y de integración por API que permite monitorear los activos de información expuestos a internet de una organización, al ser una herramienta automatizada que integra un servidor web para la interacción gráfica, permite para el analista o investigador tener mayor eficiencia en la recopilación de información y mantener un constante monitoreo sobre los activos del cliente

Para mayor información de esta herramienta es posible encontrarla en https://intel471.com/attack-surface-documentation#what-can-i-do-with-spiderfoot

Teniendo en cuenta la información inicial disponible en el paso 2 se procede a instalar el framework de Spiderfoot y posteriormente a validar las opciones que ofrece, el proceso de instalación de anexa al presente trabajo como **Anexo1**

Las opciones de búsqueda de Spiderfoot son basadas en

- **By Use Case**

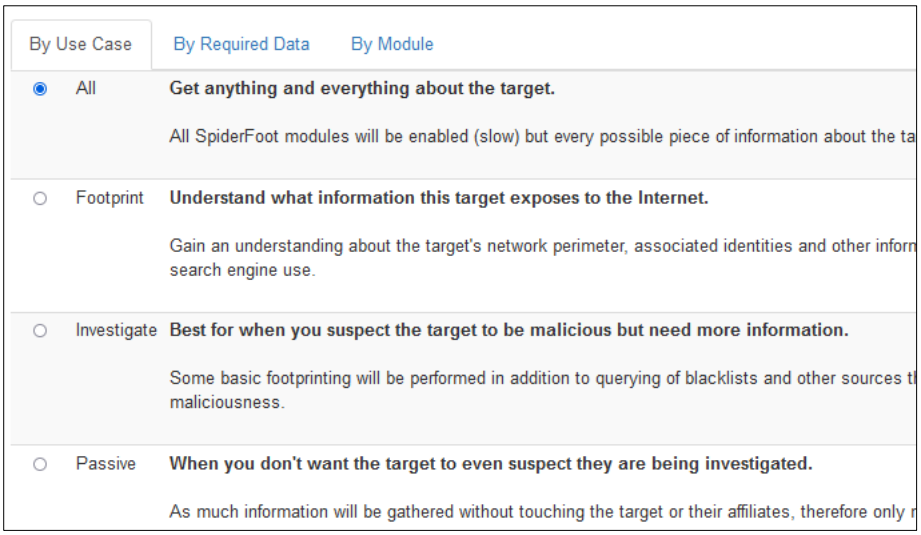


Ilustración 8 Opciones SpiderFoot

Estas opciones contemplan

- **All:** esta opción permite activar todos los módulos incluyendo búsquedas activas y en repositorios de información de malware o fuentes de inteligencia de amenazas
- **Footprint:** esta opción está más focalizada a la búsqueda de información expuesta de un objetivo
- **Investigate:** opción para búsqueda sobre una amenaza en concreto como un grupo cibercriminal o el nombre de un malware
- **Passive:** opción que solo activa módulos para búsqueda pasiva, contempla la búsqueda de información sin que el objetivo deduzca una actividad de recopilación de información es decir sin dejar registro sobre búsquedas directas en el cliente como escaneos de puestos entre otros

➢ by data required

Como opciones adicionales de búsqueda tenemos por datos solicitados (**by data required**) que contempla la búsqueda por tipos de activos o tipos de información como dirección IP, dominios, registros, correos entre otros

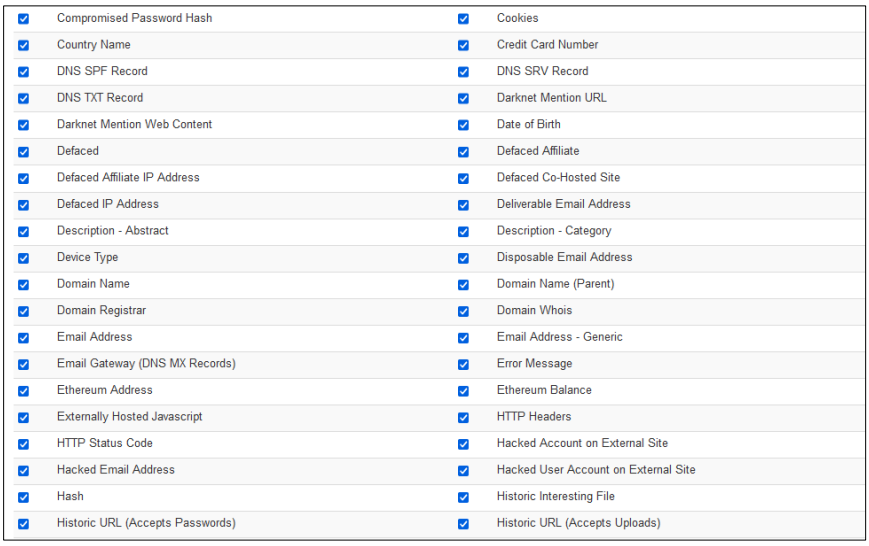


Ilustración 9 Tipo de data SpiderFoot

➢ By Module

La tercera opción es por **módulos** o fuentes de información, esta opción es la más recomendable desde mi punto de vista ya que proporciona mayor información acerca de los módulos o fuentes a trabajar y de los posibles resultados que obtendríamos, de igual manera, un investigador o analista de ciberinteligencia ahorraría mayor tiempo al escoger fuentes confiables, el cual será el propósito de esta investigación.

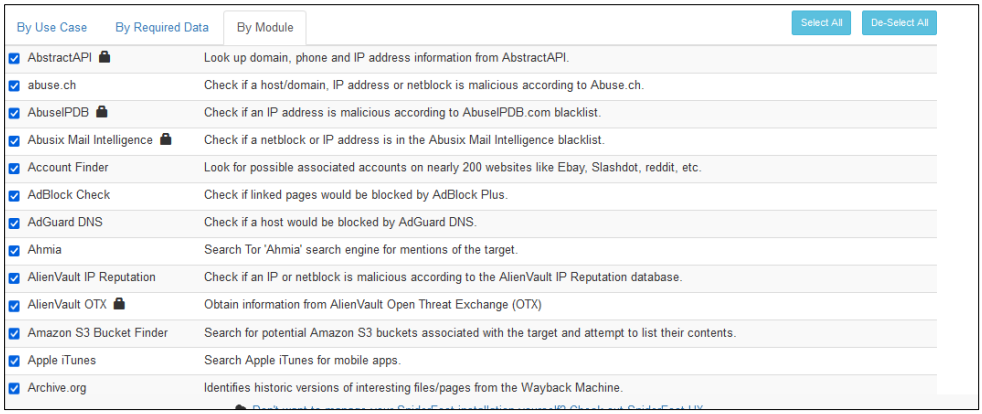


Ilustración 10 Modulos SpiderFoot

Antes de seleccionar los módulos o fuentes requeridas para nuestra búsqueda debemos tener claro que existen 2 tipos de escenarios o espacios en internet para recopilar información, existe un espacio de "**Surface web**" que indica todo el contenido que es indexable, esto quiere decir todo el contenido que ha sido previamente asociado a uno o múltiples servidores plenamente identificables y anexos o identificados por motores de búsqueda es decir de fácil acceso y búsqueda y la "**Deep web** y **darkweb"** que se refiere a todo el contenido anónimo y de difícil identificación, ya que no existe una identificación sobre el origen exacto del contenido y en muchas veces el origen de las conexiones es anónimo frente al receptor esto quiere decir que el contenido no es fácilmente identificable o indexado.

Para nuestra investigación realizaremos la búsqueda en los 2 escenarios

Búsqueda en la Surface web

No todas las fuentes o módulos de Spiderfoot son adecuados para nuestra investigación, debido a que las fuentes recopilan diferentes tipos de información que puede ser o no útil para identificar activos expuestos, teniendo en cuenta esto nos enfocaremos en elegir las primeras fuentes o módulos para la recopilación de información que más nos convengan para una búsqueda sobre la web superficial o web indexable.

Para la elección de fuentes que nos que proporcione información de utilidad se procedió a realizar una validación de las cerca de 200 módulos que alberga spiderfoot, se opta por escoger principalmente aquellos módulos que no tengan restricción de API y que permitan ser invocadas sin ninguna previa configuración, estas fuentes se caracterizan por ser completamente libres y sin necesidad de realizar una suscripción por correo o pago, posteriormente se procede a descartar aquellas fuentes que no aportan valor a la búsqueda como fuentes enfocadas en identificar indicadores de compromiso y fuentes que requieran algún método de pago, de igual manera, se descartan los módulos que requieren de herramientas preinstaladas como Nmap que conllevan una carga para el aplicativo.

Inicialmente se utilizaron **39** fuentes para llevar a cabo la investigación, sin embargo, se evidencia demoras en el escaneo y errores en las solicitudes de búsquedas de las herramientas, una vez se realiza una nueva validación de las fuentes se procedió a retirar y seleccionar nuevas fuentes teniendo como resultado **60** fuentes seleccionadas para un nuevo escaneo esto permitió obtener resultados más rápidamente

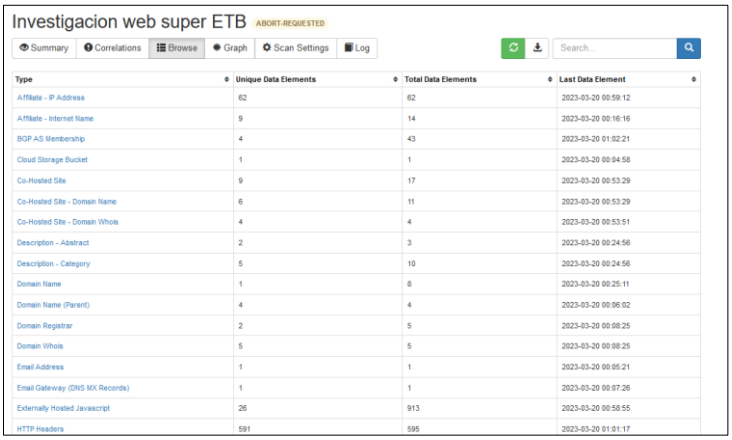


Ilustración 11 Evidencia de escaneo inicial y sus errores

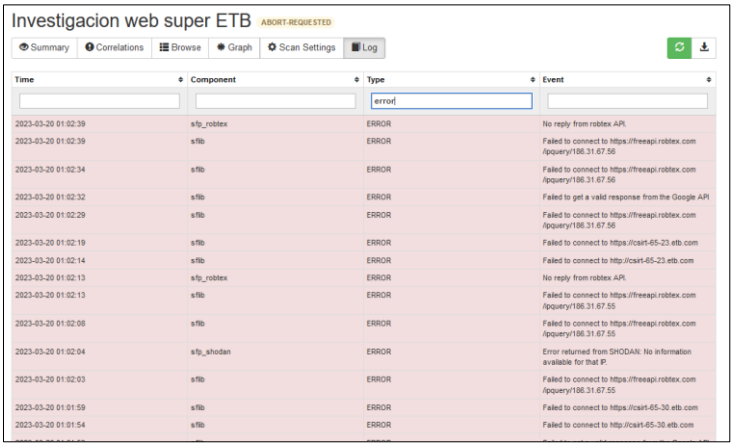


Ilustración 12 Evidencia Errores

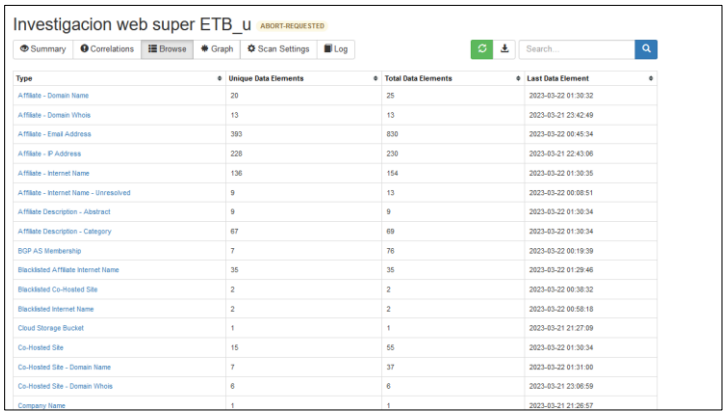


Ilustración 13 Escaneo de prueba adicional

Resultados de la validación de las fuentes

Después de leer y visitar la documentación de la mayoría de las fuentes se optó por elegir **60** fuentes de información para esta elección se tuvo que realizar pasos como

- Lectura y análisis de cada modulo
- Validación de API en la página oficial
- Validación de resultados realizando escaneo de prueba a través de la herramienta Spiderfoot
- Validación de obsolescencia y registro de cambios sobre algunas herramientas, en algunas fuentes de OSINT puede ocurrir volatilidad de la información y formas de recopilar, ya que continuamente las tecnologías de integración por API para realizar búsquedas cambian por ajustes en los desarrollos como es el caso de Facebook, twitter e Instagram

Se anexa el detalle de las fuentes seleccionadas como **Anexo 2**

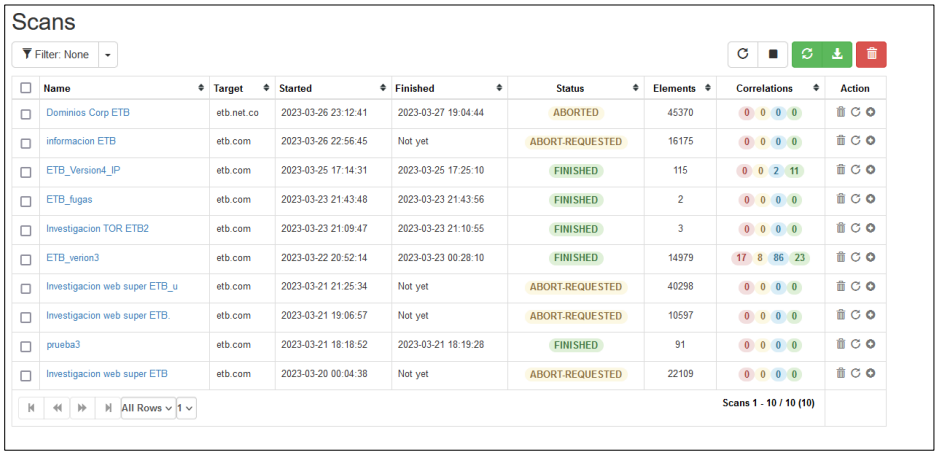


Ilustración 14 Escaneos SpiderFoot Realizados

En la ilustración 14 se relaciona el detalle de los escaneos realizados y cantidades de registros realizados en SpiderFoot para el presente TFM

6.4. Paso 4

Documentar el resultado de cada herramienta utilizada, aquí realizaremos el proceso de **filtrado** o de validación de la información en el cual se validará, cual es la información de utilidad que tendrá valor para la investigación y que tenga una menor cantidad de **falsos positivos**, este punto es importante para la investigación, ya que puede existir información falsa o incierta, en este proceso también se procederá a aplicar el proceso de inteligencia de amenazas llamado **transformación de la información** el cual generara como resultado el listado de los activos de información tipificados o categorizados permitiendo conocer de esta manera una visión general de la superficie de exposición

Después de la pruebas y escaneo previos realizados se escogieron 2 escaneos el primero corresponde al dominio **etb.com** y el segundo escaneo corresponde al dominio **etb.net.co**, los resultados de los 2 escaneos se anexan al presente documento.

El primer escaneo fue lanzado el 22/03/2023 a las 21:25 Pm al cabo de 2-3 horas aproximadamente se obtuvo un total de **14979** registros, las fuentes elegidas para el escaneo son registradas en el **Anexo 2**

El segundo escaneo fue lanzado el 27/03/2023 a las 19:04 al cabo de 12 horas el escaneo fue detenido debido a que había fuentes de información que tomaban más tiempo de lo debido y la cantidad de registros ya era suficiente para el trabajo, este escaneo fue lanzado debido a que después de un proceso de filtrado se identifica el dominio **etb.net.co** en el primer escaneo, al cabo de las 12 horas se obtienen **45370** registros, las fuentes elegidas para el escaneo son registradas en el **Anexo 3**

Ilustración 15 Resultado escaneo dominio etb.com

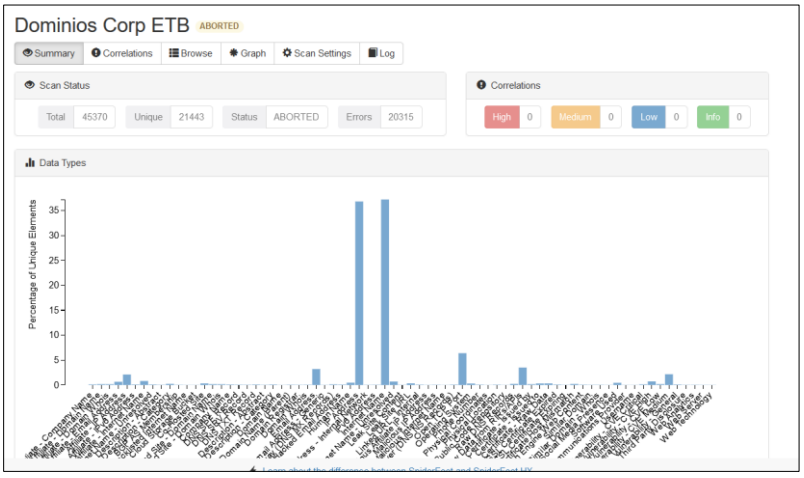


Ilustración 16 Resultados escaneo dominio etb.net.co

Como método o herramienta de análisis de los registros se procedió a utilizar la herramienta de Microsoft, llamada **Excel** la cual permite importar la información obtenida

por SpiderFoot en formato **csv**, este formato de datos fue abierto en programa de Excel y se procedió a realizar una validación de cada uno de los registros haciendo uso de los filtros y opciones de tabla dinámica de Excel

Módulos	Cantidad	Módulos	Cantidad
sfp_virustotal	**5367**	sfp_tool_dnstwist	**88**
sfp_dnsresolve	**2755**	sfp_filemeta	**83**
sfp_intelx	**1483**	sfp_intfiles	**82**
sfp_shodan	**1356**	sfp_similar	**62**
sfp_email	**745**	sfp_dns_for_family	**46**
sfp_dnsneighbor	**606**	sfp_phone	**44**
sfp_dnsbrute	**515**	sfp_hunter	**20**
sfp_sslcert	**390**	sfp_hostio	**8**
sfp_psbdmp	**311**	sfp_webanalytics	**4**
sfp_leakix	**262**	sfp_abstractapi	**4**
sfp_whois	**208**	sfp_yandexdns	**3**
sfp_duckduckgo	**191**	SpiderFoot UI	**2**
sfp_dnsraw	**147**	sfp_azureblobstorage	**1**
sfp_dnsdumpster	**99**	sfp_github	**1**
sfp_urlscan	**96**	Total general	**14979**

Tabla 1 Registros Primer escaneo dominio etb.com

Módulos	Cantidad	Módulos	Cantidad
sfp_dnsresolve	15382	sfp_phone	26
sfp_dnsneighbor	8153	sfp_skymem	26
sfp_shodan	7048	sfp_urlscan	22
sfp_dnsbrute	6280	sfp_dnscommonsrv	14
sfp_virustotal	5179	sfp_citadel	13
sfp_email	810	sfp_hostio	7
sfp_sslcert	783	sfp_tool_dnstwist	5
sfp_intelx	641	sfp_webanalytics	4
sfp_dnsraw	201	sfp_openbugbounty	4
sfp_hunter	129	sfp_abstractapi	4
sfp_names	121	sfp_stackoverflow	2
sfp_dnsdumpster	106	SpiderFoot UI	2
sfp_company	91	sfp_dns_for_family	1
sfp_robtex	88	sfp_similar	1
sfp_whois	84	sfp_github	1
sfp_duckduckgo	84	sfp_azureblobstorage	1
sfp_arin	29	Total general	45370
sfp_psbdmp	28		

Tabla 2 Registros Segundo escaneo dominio etb.net.co

Nota: para mayor entendimiento y presentación de los resultados de los escaneos realizados, se procede a presentarlos unidos a partir de este apartado

6.4.1. Procesos de Transformación de la información recopilada

1. Filtros para obtener una información base
2. Descartar información no relevante
3. Retirar duplicados
4. Validación los resultados de las fuentes o módulos nuevamente
5. Filtrar nuevamente para obtener nuevos registros
6. Correlacionar registros de otras fuentes con registros de fuentes de base o referencia
7. Validación Final de los resultados o porcentaje de utilidad de los datos

Una vez tenemos los resultados en Excel se procede a realizar el **filtrado** ya sea por medio de la información contenida en los registros obtenidos en cada módulo, en primera instancia se eligieron aquellas fuentes de información que registran información de **IP's, dominios y subdominios**, las fuentes escogidas inicialmente son

- Dnsresolve
- Dnsbrute
- Dnsdumpster
- ssl_cert

las fuentes elegidas contaban con una gran cantidad de registros, con el fin de identificar la información de interés más fácilmente, se procedió a:

- Descartar dominios que empiezan con **csirt** ya que después de un previo análisis de los registros, estos dominios no aportaban al proceso de inteligencia y eran ambiguos por no tener una relación directa o clara con el Core corporativo de la organización, estos dominios correspondían con la prestación del servicio

- Se procede a **retirar registros duplicados** para dejar valores únicos

- Se descartan dominios que empezaban con **static-*** y **Dinamic** ya que ETB al ser un prestador de servicios de internet proporciona estos domininios a los clientes de ETB con IP estatica y IP dinamica respectivamente.

Se descartan las siguientes fuentes ya que no aportaban a la identificacion de una **IP dominio y subdominio** del objetivo que permitiera continuar con la investigacion

- sfp_dnsbrute
- sfp_dnsdumpster

Finalmente se relacionan **56** IP y dominios resultantes en la **tabla 14** del **Anexo 4**

La relación de IP y dominios nos proporciona una visión de los activos operativos mas importantes que tiene la organización de igual manera, nos proporciona una base para futuras búsquedas, ya que tendremos de alguna manera una lista blanca para identificar los verdaderos positivos en las demás fuentes con su respectiva IP.

Siguiendo el mismo proceso de filtrado y la relación de los activos bases de **dominios e IP's**, se procedió a realizar una búsqueda de activos de información adicionales que nos pueden ayudar a determinar la superficie de exposición de la organización, los tipos de activos que podemos obtener a partir de las IP's y dominios son

1. Vulnerabilidades o puertos por IP con shodan
2. Metadatos
3. Documentos expuestos
4. Activos expuestos en cloud
5. Dominios similares
6. Correos corporativos
7. Repositorios con información expuesta de ETB
8. Tecnologías utilizadas por los portales

6.4.2. Vulnerabilidades o puertos por IP con shodan

Al realizar el cruce en Excel de las IP's públicas relacionadas en el **Anexo 4** con los **8.344** registros obtenidos del módulo de shodan, se identifica como resultado **443** registros de los cuales **388** son vulnerabilidades y **55** son puertos expuestos de los activos más representativos de ETB

Activos	Criticas	Altas	Baja	Media	General	Total general
promociones.etb.com (181.49.168.205)	2	19	6	108	12	147
tiendaetb.etb.com (40.118.164.51)				1		1
comunicaciones.etb.net.co (200.69.107.121)		8	3	49	3	63
gesdocetbapp02.etb.net.co (190.24.81.200)		8	3	49	4	64
gestion.etb.net.co (200.69.107.215)	1	1		3		5
gestiondocumental.etb.net.co (190.24.81.138)		8	3	42	2	55
smtp-cronos.etb.net.co (200.69.107.97)	2			1		3
tuxston.etb.net.co (200.69.107.151)		8	2	36	4	50
Total general	5	52	17	289	25	**388**

Tabla 3 Relación de Vulnerabilidades por activo

Por otro lado, obtenemos del cruce de la información con shodan, la cantidad de **puertos expuestos** por cada IP relacionados en la **tabla 14** del **Anexo 5**

6.4.3. Registros relacionados con Metadatos

Los metadatos son huellas digitales o datos incrustados en cada archivo que generamos que relacionan información básica de la tecnología, fecha y autor del archivo, esta metadata la podemos obtener con Spiderfoot gracias al módulo de **sfp_filemeta** que permite descubrir metadatos a partir de documentos expuestos, los metadatos obtenidos de los archivos expuesto de ETB son

Usuario o autor del archivo	Tecnología o Software utilizado
ADRIANA PATRICIA PEREZ RODRIGUEZ	Microsoft Word 2016
Broq	Microsoft Word 2010
Cuenta Corporativa Generica Prestamo	Microsoft Word para Microsoft 365
EUGENIA LONDOÃ‘O VALLEJO	Microsoft Word para Office 365
LAURA ESTHER PRIETO RAMOS	Adobe InDesign CS6 (Macintosh)
MARIA YOLANDA MEDINA CANO	Microsoft PowerPoint® para Microsoft 365
Omar Guevara	Microsoft PowerPoint® 2016
WEBMASTER	
YAMIL OTILIO FORERO CIFUENTES	
carlcric	
martdiar	
lilirojs	
Brayan Morales	
JORGE ALEJANDRO SANCHEZ USAQUEN	
OBJETO	

Tabla 4 Metadatos de ETB

6.4.4. Documentos expuestos

Registros relacionados con **Documentos expuestos** con su respectivo hipervínculo

Se identifica **57** documentos expuestos en las URL identificadas con el módulo de Spiderfoot llamado **sftp_infiles**, los documentos recopilados se registran en la **tabla 16** del **Anexo 5**

6.4.5. Activos en la nube

Por medio del módulo de **sfp_azureblobstorage** de Spiderfoot obtenemos los siguientes activos clasificados como equipos cloud

- https://etb.blob.core.windows.net

6.4.6. Dominios similares

Spiderfoot cuenta con un módulo llamado **similar** y **dnstwist** que nos proporciona información de los posibles dominios similares a los dominios de etb.com y etb.ent.co, ya que estos dominios pueden generar ciertas amenazas que se detallaran posteriormente en los resultados

En la **tabla 5** se puede apreciar los **65** dominios similares identificados

Dominios similares			
zetb.com	etbp.com	hetb.com	etb1.com
yetb.com	etbo.com	getb.com	erb.com
xetb.com	etbn.com	fetb.com	eetb.com
wtb.com	etbm.com	ezb.com	detb.com
wetb.com	etbl.com	eyb.com	cetb.com
vetb.com	etbk.com	etv.com	betb.com
tetb.com	etbi.com	ettb.com	aetb.com
setb.com	etbg.com	etn.com	8etb.com
retb.com	etbf.com	etbz.com	7etb.com
petb.com	etbe.com	etby.com	2etb.com
oetb.com	etbd.com	etbx.com	et.net.co
netb.com	etbc.com	etbw.com	etb.co
metb.com	etbb.com	etbv.com	etc.net.co
letb.com	etba.com	etbu.com	eth.net.co
ketb.com	etb5.com	etbt.com	wtb.net.co
jetb.com	etb3.com	etbs.com	
ietb.com	etb2.com		

Tabla 5 Dominios similares a etb.com

6.4.7. Correos Corporativos

Spiderfoot cuenta con **8** módulos para obtener información relacionada con correos corporativos y así obtener información de correos de posibles víctimas, los módulos utilizados son

- sfp_intelx
- sfp_hunter
- sfp_skymem
- sfp_citadel
- sfp_email
- sfp_arin
- sfp_names
- sfp_host.io

Debido a la gran cantidad de correos recopilados en los escaneos se procede a relacionar **728** correos de los dominios etb.com y etb.net.co en el **Anexo 6**

6.4.8. Repositorios

Spiderfoot cuenta con varios módulos que recopilan información expuesta, relacionada con el cargue de información en repositorios públicos donde las personas suelen compartir contenido con otros usuarios, este tipo de información en ocasiones puede contener información confidencial que puede representar una amenaza para la organización.

Módulos de Spiderfoot usados para la recopilación de repositorios

- sfp_psbdmp
- sfp_psbdmp
- sfp_github

Se identifican **227** repositorios por parte de Spiderfoot, después de un previo análisis de disponibilidad y respuesta del sitio, se relacionan **29** repositorios que aún siguen activos en el **Anexo 7**

6.4.9. Tecnologías identificadas

Se identifica **12** tecnologías en **7** dominios y subdominios por medio del módulo urlscan

Portal	Dato
blog.etb.com	openresty
etb.com	Apache
	Microsoft-IIS/10.0
	Microsoft-IIS/8.0
	Microsoft-IIS/8.5
info.etb.com	Apache
	Microsoft-IIS/8.0
mietb.etb.com	Microsoft-IIS/10.0
	Microsoft-IIS/8.5
mietbeyg.etb.com	Microsoft-IIS/8.0
montesquieu.etb.com	Microsoft-IIS/8.0
tienda.etb.com	Microsoft-IIS/10.0

Tabla 6 Tecnologías Identificadas

6.4.10. Activos o información de Deep y Darkweb

Se procede a realizar la búsqueda a través de los módulos en spiderfoot sin embargo, no se identifica información, esto ocurre porque las formas de buscar en la darkweb tiene un método diferente ya que, muchas palabras exactas como etb o etb.com no son indexables o no se relacionan o comentan en la Deep con el nombre de la organización, si no, con alias o seudónimos que a veces son comentados en foros privados, la estructura de algunos sitios y el acceso a ellos no permite una búsqueda automatizada es por esto que es necesario el uso de herramientas de terceros como **onionsearch, Torch, Ahmia,duckduckgo** entre otros

Resumen de activos y % de Utilidad

Se relaciona un breve resumen de la cantidad de registros identificados por spiderfoot por cada activo buscado y su porcentaje de información útil identificada para la evaluación de superficie de exposición

Activos	Registros	Activos resultantes	Porcentaje
Dominios y IP	25527	56	0,20%
Puertos y vulnerabilidades	8344	443	5%
Metadatos	83	23	28%
documentos	82	22	27%
Azure	1	1	100%
Dominios similares	156	65	42%
Correos	4281	728	17%
repositorios	227	29	13%
Tecnologias	118	12	10%

Tabla 7 Resumen de la cantidad de activos

6.5. Análisis de la Información recopilada

Una vez es recopilada la información y transformada debemos de tratarla o usarla para comprender su respectivo uso ante posibles amenazas

Para esta fase responderemos preguntas como

- ¿Para qué me sirve conocer mis activos?
- ¿Qué información revela cada activo que pueda perjudicar mi organización?
- ¿Cómo puede convertirse mis activos expuestos en vectores de acceso?
- ¿Cuáles son las amenazas que pueden afectar a mis activos?
- ¿Cómo me puedo proteger ante las amenazas identificadas?
- ¿Qué aspectos de mi organización puede afectar estas amenazas?
- ¿Qué riesgos organizacionales pueden surgir a partir de las amenazas? identificadas que afecten al negocio?

Para contestar las anteriores preguntas debemos de conocer de antemano las principales amenazas que afectan hoy en día los activos expuestos de una organización, para esto tenemos que abordar la evaluación de la **superficie de exposición** de una organización desde un ámbito donde podamos identificar cuantas **vulnerabilidades o vectores de acceso** se tiene a partir de las amenazas más comúnmente identificadas en los últimos años por fabricantes y cuerpos de seguridad, para esto procedemos a referenciar algunos informes de tendencias de amenazas y los principales vectores de acceso comúnmente utilizados, como resultado se listara una serie de vulnerabilidades y vectores de acceso comunes que posteriormente servirán como base para la relación de los activos identificados

Al validar los informes de tendencia de amenazas más actuales nos encontramos con el informe de amenazas a la ciberseguridad de la cámara colombiana de informática y telecomunicaciones (https://www.ccit.org.co/estudios/informe-evaluacion-retos-y-amenazas-a-la-ciberseguridad/) en donde indica una serie de amenazas entre ellas se encuentran **fuga de datos personales**, **suplantación de sitios digitales** (phishing) y **ransomware** todas estas amenazas ha venido aumentando en los últimos años en Colombia y en todo el mundo a raíz de la pandemia sufrida entre el 2020 y el 2021 en todo el mundo, los cibercriminales ha identificado una amplia superficie de ataque con estas amenazas debido a que muchos trabadores hacían uso de más canales digitales durante la pandemia, fortaleciendo de esta manera las técnicas de ingeniería social utilizadas

Por otro lado, el instituto nacional de ciberseguridad de España INCIBE ha publicado en su blog un artículo mencionando el top de vectores de acceso más comunes como los son:

- Phishing
- Vulnerabilidades Web
- Credenciales por defecto
- Insiders
- Debilidades en la cadena de suministro

A partir de los enlaces a reportes anexos y el análisis de cada uno de ellos se proporciona un listado de las amenazas y vectores de acceso más comunes utilizados por los cibercriminales y que pueden relacionarse con los activos recopilados en el **capítulo 6.4**

Reportes anexos

- https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-redes-de-tel-2022-2.pdf
- https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

- https://www.incibe.es/protege-tu-empresa/blog/los-10-vectores-ataque-mas-utilizados-los-ciberdelincuentes
- https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf
- https://www.ibm.com/downloads/cas/3VANOMEA
- https://ciberseguridad.com/guias/recursos/superficie-ataque/
- https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

7. Vectores de ataques y amenazas más comunes

7.1. Correo electrónico

Amenazas derivadas de correo electrónico

- **Phishing**: Técnica o métodos utilizados por cibercriminales que hacen uso del nombre o dominio de la empresa para suplantar y engañar herramientas y personas por medio de la elaboración de correos sofisticados y de esta manera distribuir malware
- **Spearphishing**: Tipo de phishing que comúnmente se caracteriza por suplantar contenido de sitios web de la organización o proveedores, con el fin de obtener credenciales, normalmente enfocados a objetivos específicos o fines específicos
- **Business Email Compromise (BEC)**: Tipo de phishing que por medio de técnicas psicológicas intenta obtener la confianza de su objetivo suplantando a organizaciones o proveedores con el fin de obtener información corporativa y/u obtención de recursos monetarios

7.2. Personas

Amenazas derivadas de las personas

- **Insiders**: amenaza comúnmente asociada a las actividades cibercriminales realizadas por un empleado en contra de su organización como la implementación de código malicioso, la extracción de información para su venta, corromper o destruir información corporativa, este vector está asociado en ocasiones a amenazas externas a los insiders con el fin de que estos realicen acciones por otros, esto ocurre por tener una **identidad digital expuesta:** esta amenaza ocurre por revelar información personal en fuentes públicas y que no son de confianza o de uso gubernamental o empresarial como redes sociales, la información revelada puede abarcar amenazas subsecuentes como suplantación de identidad, fraude o extorsión por información expuesta o por vida personal expuesta como familiares
- **Suplantación de identidad:** es una de las amenazas más comúnmente vistas hoy en día, en este tipo de amenazas se registra robo monetario por cuentas

bancarias, compra de artículos sin conocimiento del titular o sin validación de la identidad, involucramiento en actos delictivos sin conocimiento

- **Revelación involuntaria de código o software** (metadatos): esta amenaza suele registrarse por los mismos empleados de una organización ya que, no cuentan con buenas prácticas o controles de aseguramiento de la información que no permitan la revelación de información involuntaria en repositorios de desarrollo o publicación de archivos sobre sitios web posibilitando obtener información confidencial o privada de la organización como IP, usuarios, claves entre otros

7.3. Exposición de información

Amenazas derivadas de la exposición

- **Puertos o servicios expuestos:** en ocasiones al publicar un servicio sobre un activo digital en una red pública, es posible que publiquemos información relacionada con posibles versiones de tecnología vulnerable o información interna como información de esquemas o infraestructura interna, al habilitar puertos que no se requieren públicamente se abre una brecha o acceso más a un cibercriminal
- **Documentos expuestos:** amenaza o vector de acceso que permite recopilar información del contexto de la organización y su posible estado financiero, en ocasiones la información de financiera o información de uso comercial o de protección comercial, esta información se considera vital para la organización, ya que al obtener dicha información de manera pública es posible reconocer vulnerabilidades en productos o la organización, que pueda ser de utilidad para cibercriminales u otras organizaciones

7.4. Fugas de datos

Para comprender un poco mejor estas amenazas a continuación detallamos algunos problemas derivados de la fuga de datos

- Afectaciones o implicaciones legales
- Multas millonarias
- Suspensiones de operaciones
- Pérdida de clientes
- Desventaja corporativa

7.5. Malware

Amenazas relacionadas con el malware

- **Ransomware**: malware que se caracteriza por encriptar la información de un sistema y solicitar rescate para su des-encriptación
- **Backdoor:** malware o configuración realizada sobre un sistema o tecnología que permita mantener persistencia o acceso posterior a un sistema vulnerado

- **MalDoc:** tipo de malware ampliamente usado en campañas de phishing con el fin de aprovechar vulnerabilidades en archivos ofimáticos como Word y Excel

7.6. Otras amenazas

Cadenas de suministro

Las amenazas que clasifican en esta categoría son reconocidas por aprovechar vulnerabilidades que generalmente son generadas en la cadena de producción de una tecnología o en la capa de desarrollo o implementación de un producto, es en esta categoría podemos evidenciar fallas propias de tecnologías implementadas o creadas por terceros como solarwinds, Microsoft, fortinet y Cybeark

Fuerza bruta

Estos ataques comúnmente utilizan listas de palabras de usuarios o de contraseñas que son probados de manera automatizada sobre sistemas de login o de acceso con el fin de poder acceder a ellos

- Contraseñas por defecto
- Credenciales filtradas
- **Passwordspray:** diccionario de contraseña sin usuario

Ddos

Ataque de denegación de servicio, este tipo de amenazas se caracteriza por su efecto de producir indisponibilidad en los servicios que afecta, este ataque consiste en realizar grandes cantidades de peticiones a un puerto de red o servicio con el fin de sobrecargar la capacidad de respuesta y de esta manera producir su fallo

Suplantación de identidad

- Insuficiencia de seguridad en redes sociales
- Control de la privacidad personal o corporativa

Vulnerabilidades Tecnológicas

- Puertos abiertos y servicios expuestos
- Ejecución de código remoto RCE
- Vulnerabilidades web(OWASP)

Botnet

Conjunto de equipos infectados con malware que permite su control remoto con el fin de realizar tareas específicas como Denegación de servicio (Ddos)
Transferencia de zona DNS

Ataque o amenaza que consiste en suplantar o copiar los registros de DNS que actualmente consulta un usuario, al lograr este tipo de ataques se puede conocer la infraestructura interna y lograr re direccionar solicitudes a otros sitios remotos

Vishing

Tipo de phishing que consiste en realizar engaños a través de medios telefónicos con el fin de obtener información personal y posteriormente realizar actividades delictivas como fraude o robo de identidad

Smishing

Esta amenaza es similar a la anterior con la diferencia de que se realiza campañas de envío de información fraudulenta a través de mensajes de texto con el fin de robar o sustraer información a través de enlaces maliciosos

8. Paso 5-Resultados

Análisis y Amenazas de los activos identificados

Para el tratamiento de la información anteriormente recopilada en el paso 4 analizaremos que información puede ser de relevancia por los atacantes que permita ser utilizada por alguna de las amenazas o vectores de acceso mencionadas en el **capítulo 7 vectores de ataque**, para esto haremos una relación de los activos digitales descubiertos con las amenazas, con el fin de comprender un poco más el grado de exposición de la organización.

Algunos de los pasos seguidos en este apartado consisten en agregar enriquecimiento a la información tomando en cuenta los siguientes ítems

- Un filtrado mayor sobre los datos
- Validación de información con otras fuentes o con su posible relación en la operación de TI
- El posible uso de otras herramientas para obtener más información
- La validación de la información obtenida en fuentes abiertas como google para tener mayor contexto
- La validación de cada uno de los registros filtrados con el fin de conocer su posible uso por cibercriminales (amenazas)
- Validación del Tipo de información expuesta (publica o reservada)
- Técnicas para evitar falsos positivos como revisiones de los documentos y la validación de puertos y tecnologías
- La identificación de posibles riesgos asociados al análisis de los activos digitales basados en el siguiente enlace https://opmintegral.com/empresa-estrategia-y-proyectos/tipos-de-riesgos-empresariales/

8.1. Dominios y IP

Análisis de activos del anexo 4

Cada dominio, subdominio y dirección IP asociada puede convertirse en un vector de acceso a continuación relacionaremos el análisis de los activos del **anexo 4** y sus posibles vectores de acceso identificados y que pueden ser usados por un cibercriminal.

Análisis realizado a puertos y dirección IP

De los puertos expuestos en el **anexo 5**, se recopilan todos aquellos puertos comunes en las direcciones IP publicas identificadas, obteniendo de esta manera **34** direcciones IP públicas únicas y sus respectivos puertos, estos se evidencian en la **tabla 15** del **anexo 5**

Se identifican **15** puertos comunes en las **34** IP's relacionados en la tabla 8, dentro de los puertos comunes se encuentran expuesto los siguientes servicios

Puerto	Servicio
25	SMTP
53	DNS
80	HTTP
81	HTTP
83	HTTP
84	HTTP
96	dixie
443	https
995	POP3
5443	SPSS telefonia
6443	HTTPS kubernets
8080	HTTP
8083	Vcenter
8443	Controladora wifi o HTTPS
9443	Vmware

Tabla 8 Puertos y servicios identificados

para esta identificación se usó el sitio **https://www.speedguide.net/**

Cada puerto tiene asociado un servicio expuesto y dependiendo del tipo de servicio esto puede tener mayor riesgo de ser atacado o tener mayor grado de exposición. Los puertos que son comúnmente atacados por los cibercriminales son aquellos que tiene vulnerabilidades en sus protocolos de funcionamiento como los puertos

Puerto	Servicio
22	SSH
21	FTP
3389	RDP
137	Netbios
139	Netbios
445	SMB

Tabla 9 Puertos comunes de ataque

A pesar que ETB no contenga los puertos más comúnmente atacados no significa que no tenga amenazas probables asociadas a los puertos analizados

Otro de los vectores de acceso que se puede mencionar es la identificación por parte de spiderfoot relacionada en la **ilustración 17**, en la que indica que se descubrieron dominios gracias a que muchos de ellos compartían el mismo certificado de seguridad web ssl con dominios de terceros, esta característica es conocida como **certificados ssl multiples** o **Certificados SSL de varios dominios** la cual contempla vulnerabilidades que permiten realizar ataques como MIM(hombre en el medio) interceptación de la comunicación, según el medio digital https://www.kaspersky.es/blog/residual-certificates-mitm-dos/16840/

Ilustración 17 Análisis de la herramienta sobre dominios

Amenazas identificadas en los activos

Los dominios pueden tener las siguientes **amenazas** de acuerdo a la información relacionada en el **anexo 4**

- **Certificados ssl múltiples** y amenaza MIM (Man in the middle)
- Sitios web que permitan el cargue de archivos como **reverse Shell** o **Backdoor**
- Ataques conocidos a servidores DNS**,** como **transferencia de zona DNS**
- **Transferencia de zona DNS**
- **DDOs (denegación de servicio)**

Riesgos que podrían impactar al negocio al materializarse una amenaza

- Riesgos tecnológicos
- Riesgo reputacional

8.2. Vulnerabilidades identificadas en los activos expuestos (Direcciones IP)

Otro análisis realizado asociado a los **dominios** e **IP** son las vulnerabilidades, estas son identificadas por el módulo de **Shodan** de manera pasiva, esto lo logra shodan gracias a la identificación de la versión del servicio asociado al puerto expuesto, esta información nos ayuda a comprender cuales son los activos de mayor riesgo y los activos que tiene mayor probabilidad de ser atacados

Análisis de las Vulnerabilidades identificadas

Dentro de las vulnerabilidades identificadas en la **tabla 3** se identifica que el activo con mayor probabilidad de sufrir un ataque es el dominio **promociones.etb.com** con IP **181.49.168.205** debido a que cuenta con **147** vulnerabilidades de las cuales **21** de ellas están entre altas y críticas, analizando las vulnerabilidades presentes se identifica que están asociadas a servicios o aplicaciones como Openssl, Apache y PHP

Otro de los activos con mayor riesgo de ser atacado son los activos

- comunicaciones.etb.net.co
- gesdocetbapp02.etb.net.co

debido a que cuentan con 63 y 64 vulnerabilidades respectivamente cada uno

Amenazas

Dentro de las amenazas o ataques que pueden hacer uso de estas vulnerabilidades se encuentran

- Ejecución de código remoto
- Phishing
- Malware
- Vectores de acceso por medio de vulnerabilidades clasificadas por el OWASP - Vulnerabilidades web(OWASP) (cadena de suministro)
- Fuga de datos

Riesgos asociados

- Riesgos tecnológicos
- Riesgo reputacional

8.3. Metadatos

En los metadatos podemos apreciar tecnologías actualmente utilizadas por la organización, esta información permite a un cibercriminal identificar las posibles vulnerabilidades asociadas a cada software o programa utilizado por la organización con el fin de elaborar ataques de ingeniería social como phishing las vulnerabilidades más comunes, asociadas a las tecnologías identificadas en los metadatos de la **tabla 4** son

Tecnología o Software utilizado	Vulnerabilidades
Microsoft Word 2016	CVE-2022-30190 CVE-2023-21716 CVE-2017-0199 CVE-2021-40444
Microsoft Word 2010	CVE-2022-30190 CVE-2023-21716 CVE-2017-0199 CVE-2021-40444
Microsoft Word para Microsoft 365	CVE-2022-30190
Adobe InDesign CS6 (Macintosh)	CVE-2018-4928
Microsoft PowerPoint® para Microsoft 365	CVE-2021-40444
Microsoft PowerPoint® 2016	CVE-2023-21716

Tabla 10 Tecnologías y vulnerabilidades identificadas

Por otro lado, se identifica nombres de usuario en la tabla 4, por medio de estos es posible realizar ataques como **passwordspray** o fuerza bruta al conocer usuarios internos

Amenazas

- Passwordspray
- Fuerza bruta
- Vulnerabilidades Tecnológicas (cadenas de suministro)
- Phishing

Riesgos asociados

- Riesgo de seguridad y fraude
- Riesgos tecnológicos

8.4. Documentos expuestos

Se identifican **57** documentos expuestos en **3** URL

- http://montesquieu.etb.com
- https://etb.com

- https://pruebasetb.etb.com

al validar los documentos se evidencia que existen documentos internos de la organización como

- 2022-05-03_TRANSMISIÓN DE CONTENIDOS CANAL CARACOL.xlsx
- 2022-05-05_BASE SUSPENSIÓN PREVENTIVA ENTE REGULADOR.xlsx
- 2022-05-16_CUENTAS RETENIDAS FTTX.xls
- 2022-01-16_HOJA DE VIDA TRAMITES FIJA FTTX _Y COBRE_.xlsx
- 2022-02-18_MATRÍZ PARRÃFOS RESPUESTA PQR V73.xlsm
- 2022-03-23_GUIÓN CAMPAÑAS MÓVILES.xlsx
- 2022-04-01_GUIÓN DE POSVENTAS ETB HOGARES.xlsx
- 2022-04-01_SIMULADOR DE TARIFAS HOGARES Y MIPYMES.xlsx

Estos documentos registran información de la operación interna de la organización, de igual manera, se evidencia la exposición de datos personales de clientes empresariales como de personas naturales, esta exposición es muy grave ya que actualmente en Colombia existe la **ley de protección de datos personales, 1581** que dictamina las directrices de este tipo de faltas por parte de las organizaciones, de igual manera esta información es aprovechada por la competencia o por cibercriminales para realizar campañas de ingeniería social

Amenazas

- Phishing
- vishing
- smishing
- suplantación de identidad
- Fuga de datos o filtración de datos

Riesgos asociados

- Riesgo reputacional
- Riesgo de cumplimiento
- Riesgo competitivo
- Riesgo económico

8.5. Activos de nube Cloud

Para este apartado se identifica un activo en la nube correspondiente con un posible servicio o activo de la solución azure de Microsoft, para este tipo de activos es posible que sufra las mismas amenazas que un activo publicado o expuesto en la infraestructura propia de la organización a continuación se detallan las amenazas y riesgos identificados

Amenazas

- cadena de suministro
- passwordspray

Riesgos

- Riesgos operativos
- Riesgo de seguridad y fraude

8.6. Dominios Similares

Análisis de la información de la **tabla 5,** los dominios encontrados por spiderfoot como similares al dominio etb.com y etb.net.co son dominios que se suelen registran por cibercriminales con el objetivó de suplantar al dominio original esto se realiza como una técnica psicológica de engaño, algunas de estas técnicas son **Typosquatting** y **combosquatting** esto con el fin de realizar campañas de ingeniería social como phishing y/o afectar negativamente la marca de la organización, los dominios que soporten sitios similares al sitio original se suelen tomar como dominios maliciosos que pueden ser utilizados para campañas de propagación de malware o para robo de información de clientes y/o usuarios

Al analizar cada uno de los dominios se identifica que existen **13** dominios que no tiene relación con ETB y **52** dominios que no están en uso

Amenazas

- Phishing tipo BEC
- Phishing
- Spearphishing
- Malware
- Fuga de información

Riesgos asociados

- Riesgos operativos
- Riesgo de seguridad y fraude

8.7. Análisis de Correos electrónicos

Al realizar el análisis de los correos identificados del **anexo 6,** se evidencia que es posible llevar a cabo varias técnicas de investigación que permitan profundizar en la superficie de exposición de ETB, ya que en este apartado se cuenta con una gran cantidad de correos electrónicos, una buena opción para comenzar a profundizar es validar que correos tienen alguna relación con alguna posición o cargo de importancia dentro de la organización como por ejemplo, un ingeniero de TI, un contador, un gerente entre otros, otra opción viable de investigación es realizar una búsqueda de correos

electrónicos asociados a posibles perfiles en redes sociales con el fin de realizar ataques de ingeniería social, de igual manera también es posible validar en fugas masivas de información pública alguna relación de correos electrónicos y de esta manera identificar posibles credenciales filtradas o expuestas, como se puede observar existen varias maneras para profundizar en los posibles vectores de acceso a partir de correos electrónicos

Algunas herramientas que puede servir para las técnicas de investigación mencionadas son

- Maltego
- Profil3r
- Hunter.io
- h8mail

Al analizar los **728** correos del **anexo 6** se identifica que muchos de los correos registraban **números** dentro del alias o nombre del correo, normalmente los correos asociados al personal interno de una organización, no cuentan con estos números, por ende, se procede a excluir estos registros por medio de un filtro en Excel y así obtenemos **215** correos posiblemente asociados a empleados de la organización, los cuales pueden ser útiles por cibercriminales para realizar ataques, se anexan los correos resultantes como **anexo 8**

Por medio de herramientas como **h8mail** se procede a analizar los **215** correos anteriormente extraídos con el fin de identificar relaciones con fugas masivas o información expuesta relacionada, una vez se logró ejecutar la herramienta en el entorno de trabajo se logró identificar **29** correos que pueden estar relacionados con fugas masivas de datos, por ende es posible encontrar información de credenciales expuestas de estos usuarios generando de esta manera más vectores de acceso, se anexa los **29** correos electrónicos como **anexo 9**

Amenazas

- Fuga de información
- Phishing
- Spearphishing
- Vishing y Smishing
- suplantación de identidad

Riesgos asociados

- Riesgo reputacional
- Riesgo de cumplimiento
- Riesgo competitivo
- Riesgo económico

8.8. Análisis de repositorios

Se validó cada uno de los repositorios del **anexo 7** y se identifica que solo **29** repositorios se encontraban activos o accesibles, de estos repositorios se evidencia información que solo relacionaba enlaces a canales de televisión en internet, no se llegó a encontrar ningún tipo de información relevante en este apartado que represente alguna amenaza, sin embargo, en algunas ocasiones se logra identificar información como credenciales o API expuestas

Amenazas

- No se identifican para este activo digital

Riesgos asociados

- Riesgo reputacional
- Riesgo de cumplimiento
- Riesgo competitivo
- Riesgos tecnológicos

8.9. Análisis de los activos relacionados a tecnologías

Al igual que los metadatos spiderfoot cuenta con un módulo llamado **urlscan** que identifica la tecnología web de los dominios y subdominios de la organización al conocer estas tecnologías es posible conocer las vulnerabilidades relacionadas con dichas tecnologías, en este caso al analizar la **tabla 6** se logró identificar **5** tecnologías de desarrollo de sitios web y sus versiones.

- Apache
- Microsoft-IIS/10.0
- Microsoft-IIS/8.0
- Microsoft-IIS/8.5
- openresty

el conocimiento de estas tecnologías puede conllevar a amenazas como

- Vulnerabilidades web(OWASP) Cadena de suministro

Riesgos asociados

- Riesgo competitivo
- Riesgos tecnológicos

Una vez hemos identificados las amenazas o posibles vectores de acceso en la superficie de exposición de la organización procedemos a mapear estas amenazas en una matriz o framework que permita comprender las técnicas y tácticas utilizadas para lograr materializar estas amenazas, para esto hacemos uso de la matriz de **Mitre&Attack**

Se relaciona como **anexo 10**, el resumen de los datos analizados y recopilados en el **capítulo 8** de resultados

9. Paso 6- Matriz de MITRE&ATTACK

De acuerdo a la página oficial (https://attack.mitre.org/), Mitre&Attack es una base de conocimiento global de tácticas y técnicas de adversarios basada en observaciones del mundo real, el conocimiento de estos ataques permite el modelado de amenazas en diferentes sectores y fabricantes de ciberseguridad

Esta base de conocimiento alberga una matriz para identificar más fácilmente las técnicas y tácticas que usan los grupos de amenazas avanzadas (APT), estas técnicas y tácticas se han logrado identificar por medio de las investigaciones de algunos fabricantes de seguridad como trendmicro, karpersky y fortinet entre otros haciendo uso de las huellas o artefactos que estos grupos dejan en sus ataques

La matriz de Mitre&Attack cuenta con **14** tácticas y **224** técnicas para recrear o comprender los vectores de acceso de los grupos cibercriminales

Tácticas	Técnicas
Reconocimiento	10
Recursos desarrollados	7
Acceso inicial	9
Ejecución	13
Persistencia	19
Estalación de privilegios	13
Evasión de defensas	42
Acceso credencial	17
Descubrimiento	30
Movimiento lateral	9
Colección	17
Comando y control	16
Ex filtración	9
Impacto	13

Tabla 11 Tacticas y tecnicas

La matriz de Mitre&Attack cuenta con un framework vía web que nos ayuda a identificar más rápidamente estas tácticas y técnicas, para nuestro TFM relacionaremos cada una de las amenazas identificadas en los activos digitales del **capítulo 8** con las respectivas técnicas y tácticas utilizadas por los cibercriminales, describiendo de esta manera el comportamiento de los principales cibercriminales, teniendo en cuenta esto obtendremos mayor comprensión de la **superficie de exposición** e inteligencia sobre nuestro posibles enemigos, entre más conozcamos del enemigo seremos más efectivos en aplicar medidas de protección ante sus posibles ataques.

A continuación, se relacionan las técnicas y tácticas identificadas para cada amenaza relacionada en los resultados del **capítulo 8**

Para identificar las técnicas en Mitre&Attack podemos hacer uso de la siguiente página https://attack.mitre.org/ y en el buscador ingresamos el nombre de las amenazas y/o ataques, la página identificara las posibles técnicas y tácticas utilizadas y posteriormente se marcaran en el mapa o matriz online que se puede encontrar https://mitre-attack.github.io/attack-navigator/

9.1. Relación de Tácticas y Técnicas

Activo	Amenaza	Tactica	Tecnica
Dominios y IP	Certificados SSL (MIM)	Acceso credenciales	T1557
	Cargue de backdoor	Persistencia	T1505.003
	Ddos	Recursos desarrollados	T1584.005
	DNS	Recursos desarrollados	T1584.002
Vulnerabilidades	RCE(ejecucion de codigo remoto	Ejecución	T1059
	Phishing	Acceso inicial	T1566
	Malware	Recursos desarrollados	T1587.001,T1588
	Web attack(owasp)cadena de suministro	Acceso inicial	T1195
	Fuga de datos(data leak)	Ex filtración	T1020,T1041,T1567
Metadatos	passwordspray	Acceso credenciales	T1110.003
	fuerza bruta	Acceso credenciales	T1110
	cadena de suministro	Acceso inicial	T1195
	Phishing	Acceso inicial	T1566
Documentos Expuestos	Phishing	Acceso inicial	T1566
	Vishing	Acceso inicial	T1566
	Smishing	Acceso inicial	T1566
	Suplantación de identidad	Recursos desarrollados	1586.001,1586.002
	Fuga de datos(data leak)	Ex filtración	T1020,T1041,T1567
	exposición de información	Colección	T1602
Nube	cadena de suministro	Acceso inicial	T1195

	passwordspray	Acceso credenciales	T1110.003
Dominios similares	Phishing (BEC)	Acceso inicial	T1566
	Phishing	Acceso inicial	T1566
	Spearphishing	Acceso inicial	T1566
	Malware	Recursos desarrollados	T1587.001,T1588
	Fuga de datos(data leak)	Ex filtración	T1020,T1041,T1567
Correos electrónicos	Fuga de datos(data leak)	Ex filtración	T1020,T1041,T1567
	Phishing	Acceso inicial	T1566
	Spearphishing	Acceso inicial	T1566
	Vishing	Acceso inicial	T1566
	Smishing	Acceso inicial	T1566
	Suplantación de identidad	Recursos desarrollados	1586.001,1586.002
Repositorios	No se identifica en los activos	No se identifica en los activos	No se identifica en los activos
Tecnologias	cadena de suministro	Acceso inicial	T1195

Tabla 12 Amenazas, Activos y Tacticas y Tecnicas

Matriz con las técnicas marcadas

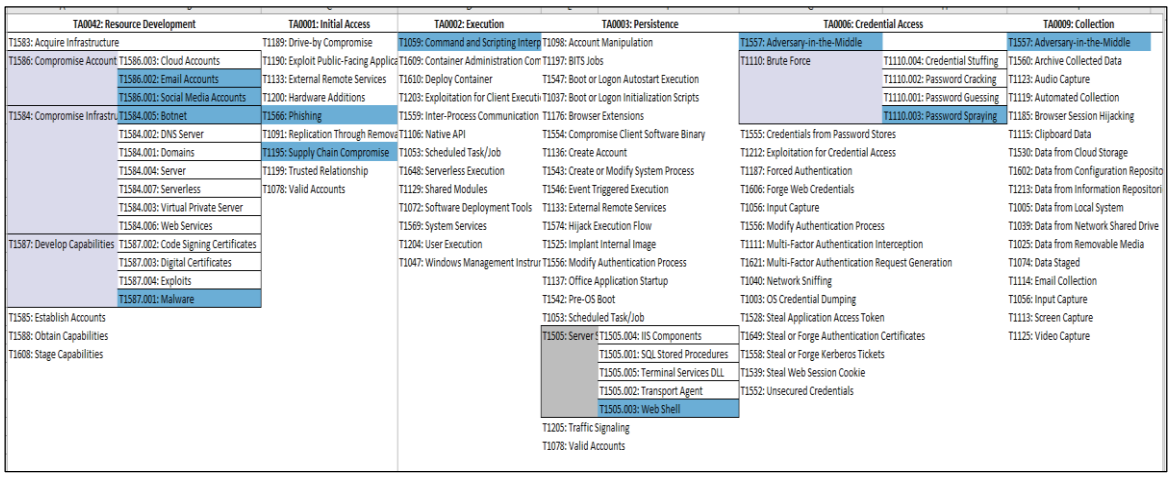


Ilustración 18 Tecnicas MItre&Attack identificadas

9.2. Paso 7 y Recomendaciones

Para cada técnica identificada anteriormente en la matriz Mitre&Attack existe un apartado para mitigarla o detectarla que nos permitirá tomar acciones preventivas y reactivas ante las posibles técnicas identificadas, a continuación en la **tabla 13**, se detallaran cada uno de las posibles acciones y controles a seguir para cada técnica identificada

Nombre	Tecnica	Control o Mitigación
Adversary-in-the-Middle	T1557	Implementar controles de encriptación en las comunicaciones limitar acceso a los recursos de red implementar sistemas de detección de intrusos Segmentación de red
Backdoor webshell	T1505.003	control de cuentas de usuario hardening de servidores implementar sistemas de protección de aplicaciones web como WAF(web aplicación Firewall implementar sistemas de detección de intrusos en endpoint
Botnet	T1584.005	implementar sistemas de detección de intrusos en endpoint Concientización o entrenamiento de usuario final
DNS server	T1584.002	hardening de servidores Implementar sistemas de seguridad avanzados en DNS como DNSSEC
Remote comand control	T1059	Implementar procesos de testing de código o proceso de desarrollo seguro implementar sistemas de protección de aplicaciones web como WAF(web aplicación Firewall mantener procesos de parchado y de gestión de vulnerabilidades
Phishing	T1566	Concientización o entrenamiento de usuario final Implementar proceso de análisis de phishing implementar sistemas de protección de correo tanto en nube como localmente implementar sistemas de detección de intrusos en endpoint
Malware	T1588	Implementar sistemas de administración de eventos implementar sistemas de protección a nivel de endpoint como antivirus o EDR
Cadena de suministro	T1195	mantener procesos de parchado y de gestión de vulnerabilidades Implementar sistemas de administración de eventos
Exfiltracion	T1020 T1041 T1567	Implementar procesos de cacería de amenazas a través de manejo de eventos de diferentes herramientas Implementar sistemas de administración de eventos implementar sistemas de protección a nivel de endpoint como antivirus o EDR implementar sistemas de DNS centralizado

Password spray	T1110.003	Implementar sistemas de administración de eventos implementar sistemas de doble factor de autenticación 2FA implementar sistemas de control de acceso y de autenticación de usuarios como AD y PAM implementar políticas de contraseñas
Fuerza bruta	T1110	Implementar sistemas de administración de eventos implementar sistemas de doble factor de autenticación 2FA implementar sistemas de control de acceso y de autenticación de usuarios como AD y PAM implementar políticas de contraseñas
Compromiso de redes sociales	T1586.001	Concientización o entrenamiento de usuario final implementar sistemas de doble factor de autenticación 2FA
Compromiso de cuentas de correo	T1586.002	Concientización o entrenamiento de usuario final implementar sistemas de doble factor de autenticación 2FA
Configuración repositorios	T1602	políticas o controles que regulen el acceso a los recursos de nube y de código publicados políticas de clasificación de la información

Tabla 13 Recomendaciones Mitre&Attack

Recomendaciones Generales

- Mantener un servicio o proceso que permita el monitoreo de la superficie de exposición que conforme analistas y herramientas el cual debe gestionarse continuamente y debe pertenecer al sistema de gestión de seguridad de la organización

- Mantener planes de respuesta incidentes y manejo de datos enfocados a las comunicaciones y el tratamiento de la información confidencial con el fin de evitar incumplimientos legales y daños reputacionales

Conclusiones y trabajos futuros

Conclusiones

- A lo largo de la realización del presente TFM se optó por seguir una metodología definida por CNI la cual nos ayudó a orientar para la realización de la búsqueda y transformación de la información, sin embargo, el presente trabajo género a partir de investigaciones previas una metodología en forma de **playbook** que se concentró en la evaluación de la superficie de exposición de la organización objetivo, esta metodología plantea una guía que sirve como base para futuras investigaciones, el playbook generado plantea una nueva forma para la evaluación e identificación de la superficie de exposición de igual manera el playbook involucra la experiencia e inteligencia relacionada a la evaluación actual de una organización, cumpliendo de esta manera de forma transversal los objetivos planteados

- Se identificó que a pesar de existir una metodología como la mencionada anteriormente, es imprescindible tener aspectos técnicos y culturales por parte del investigador, que permitan la generación de la **inteligencia de amenazas**, los aspectos que se pueden recalcar para dicho fin son, idioma de la información identificada, tener un contexto local de la organización objetivo, conocimiento técnico en TI y ciberseguridad, experiencia o pensamiento crítico, estos aspectos son importantes debido a que la metodología permite la **extracción y transformación** de la información, sin embargo, el **enriquecimiento** la genera el poder cognitivo de correlacionar las diferentes fuentes de información que se tengan con el fin de brindar una evaluación que permita la toma de decisiones

- se identifican algunos limitantes en el software spiderfoot como que no permite excluir términos en las búsquedas, no permite búsquedas puntuales de activos como una IP o un dominio, limitación del control sobre la ejecución del escaneo, a pesar de las limitantes del software y las limitantes que tiene la metodología, se logra correlacionar las amenazas identificadas con los activos identificados en la organización, comprendiendo de esta manera la **superficie de exposición** de la organización, ya que se logra cuantificar las vulnerabilidades o vectores de acceso a los que está expuesta la organización y se logra identificar las diferentes técnicas y tácticas de dichos vectores.

- Las técnicas y tácticas identificadas son el resultado del aporte del **enriquecimiento de la información** recopilada, que permitiría a una organización tomar decisiones preventivas y reaccionar oportunamente a las amenazas por consiguiente consideramos cumplido los objetivos con la relación a las técnicas y tácticas y a las respectivas recomendaciones.

- Se puede concluir que el uso de una sola herramienta (spiderfoot) en las investigaciones OSINT no conduce a que obtengas información de inteligencia necesaria para la evaluación de la superficie, es necesario en ocasiones hacer uso de herramientas adicionales y de técnicas propias o adquiridas por experiencia para reconocer la información de valor en los activos de una organización.

- Dentro de la metodología se contempla aspectos técnicos y de búsqueda alternativos que no se basan en ningún método estándar conocido, estos métodos fueron introducidos para el cumplimiento de los objetivos dentro de los métodos empleados se menciona la incorporación de **técnicas de anonimizacion** y la contextualización o referencia a fuentes poco convencionales como la **darkweb**, esta última técnica es mencionada como una opción para futuros trabajos de investigación ya que, la herramienta automatizad no genero un buen resultado en este aspecto y no se contempla dentro del alcance del presente trabajo incorporar una técnica o metodología para la búsqueda de información en la darkweb.

Futuras investigaciones

- La ciberinteligencia y OSINT para el Threat Hunting
- Técnicas y/o metodologías de Investigación en la darkweb
- Evaluación de la superficie de exposición con fuentes de inteligencia artificial
- Investigación OSINT para el terrorismo
- Investigaciones OSINT para localización de una persona secuestrada
- OSINT como herramienta para entrenamientos de Capture the Flag (CTF)
- OSINT como herramienta para detección de fraude

10. Glosario

- **Hackers:** definición dada a las personas con grandes habilidades y altos conocimientos en ciberseguridad
- **Cibercriminales:** personas o grupos de personas con altos conocimientos en ciberseguridad que usan sus conocimientos en esta rama para realizar actos delictivos que van en contra de la ley
- **OSINT:** acrónimo utilizado en el documento que se define como Open Source Intelligence o inteligencia de fuentes abiertas
- **Ciberataques:** Proceso o evento que es llevado en contra de un activo tecnológico u organización con el fin de interrumpir su operación o llevar acciones delictivas
- **Amenaza:** toda acción que se aprovecha de una vulnerabilidad
- **Amenazas digitales:** en el contexto de este trabajo se refiere a todas aquellas técnicas utilizadas para aprovechar las vulnerabilidades externas que se puedan encontrar en el ciberespacio a partir de la información obtenida para llevar acabo ciberataques
- **Mitre&Attack:** es una base de conocimiento accesible a nivel mundial de tácticas y técnicas del adversario basadas en observaciones del mundo real. La base de conocimientos de ATT&CK se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad. [8]
- **Framework:** entorno de trabajo que enmarca conjunto de características que permite lograr un proceso u objetivo
- **Spiderfoot:** Herramienta desarrollada para llevar a cabo investigaciones de tipo OSINT
- **Activos:** todo aquel elemento tecnológico como un servidor, un firewall o un equipo que tenga alguna función tecnológica para la empresa como impresoras, estaciones de trabajo, cámaras etc…
- **Playbook:** flujo de pasos que describen un proceso o la solución de un problema
- **Dark web:** termino asociado a los sitios web registrados en servidores o redes que no son indexable o reconocidos por buscadores reconocidos como goolge.com
- **API:** interfaz de programación de aplicaciones que permite la interacciones entre aplicaciones, permitiendo de esta manera consumir o adquirir por medio de instrucciones dadas información de una aplicación
- **Vulnerabilidad:** es un fallo o una ausencia de configuración asociada a una tecnología o funcionalidad de alguna herramienta que permite ser utilizada como vector de acceso a un sistema
- **ISP:** Proveedor de servicios de internet, este término es asociado a las organizaciones que prestan servicios de internet
- **Typosquatting:** es el término asociado a los dominios que se crean con errores ortográficos comunes para la suplantación del dominio real, estos son técnicas de diseño de dominios utilizadas por cibercriminales
- **Combosquatting:**amenaza o técnica de engaño utilizada para crear dominios similares al dominio real

11. Bibliografía

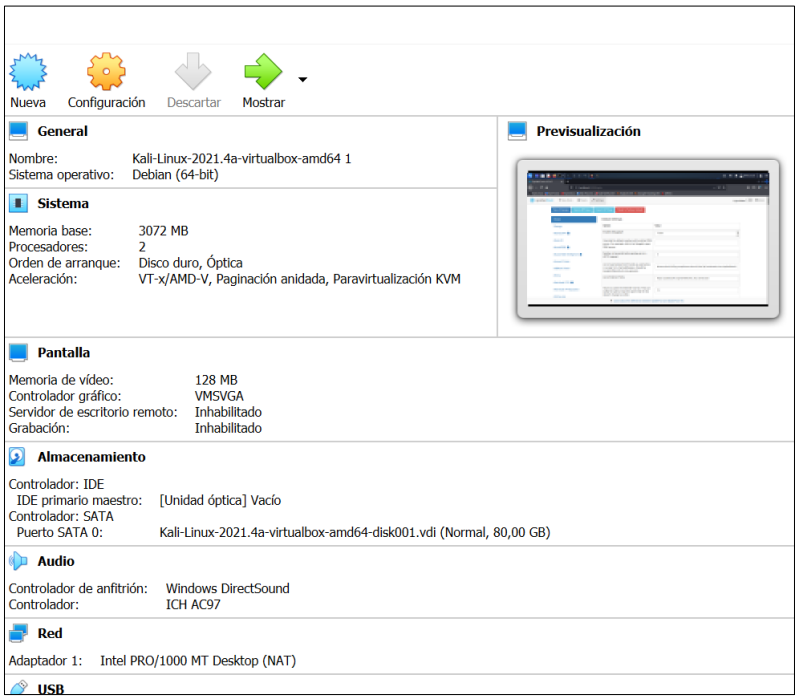
- Bejarano MJC. Alcance y ámbito de la seguridad nacional en el ciberespacio. Cuadernos de estrategia [Internet]. 2011 [citado el 7 de marzo de 2023];(149):47–82. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3837251 **[1]**
- Rae.es. [citado el 7 de marzo de 2023]. Disponible en: https://www.rae.es/dpd/ciber- **[2]**
- Rae.es. [citado el 7 de marzo de 2023]. Disponible en: https://dle.rae.es/inteligencia **[3]**
- Juárez C. Las 110 mejores frases de Sun Tzu (El Arte de la Guerra) [Internet]. Psicologiaymente.com. 2019 [citado el 7 de marzo de 2023]. Disponible en: https://psicologiaymente.com/reflexiones/frases-sun-tzu **[4]**
- Alumnos A. ¿Qué es y para qué sirve la Ciberinteligencia? [Internet]. LISA Institute. [cited 2023 Mar 14]. Available from: https://www.lisainstitute.com/blogs/blog/ciberinteligencia-que-es-y-para-que-sirve **[5]**
- Criptológico C. SIN CLASIFICAR [Internet]. Cni.es. [cited 2023 Mar 14]. Available from: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html **[6]**
- Semana. Encuesta reconoce a ETB como empresa con mejor servicio al cliente [Internet]. Revista Semana. 2009 [cited 2023 Mar 17]. Available from: https://www.semana.com/encuesta-reconoce-etb-como-empresa-mejor-servicio-cliente/78883/ **[7]**
- MITRE ATT&CK® [Internet]. Mitre.org. [citado el 12 de marzo de 2023]. Disponible en: https://attack.mitre.org/ **[8]**

12. Anexos

12.1. Anexo 1

Para esta fase debemos de realizar la preparación de nuestro entorno

Procederemos a instalar nuestro entorno de trabajo, para esto utilizamos el virtualizador de virtualbox el cual nos ayuda a crear máquinas virtuales sobre un equipo físico permitiéndonos independizar y ejecutar programas sin ningún riesgo sobre la maquina física



máquina virtual creada

Características

Se procede a instalar como sistema operativo base un debian 5.14 con la distribución conocida como kali Linux la cual se Puede descargar desde https://www.kali.org/get-kali/

Características

- 3 GB memoria RAM
- 2 núcleos
- 80 GB

Instalación del framework de trabajo spiderfoot como herramienta general para la búsqueda de información

Spiderfoot en un entorno de trabajo que recopila información de cerca de 100 fuentes de información permitiendo su búsqueda a través de la integración de API de terceros y

centralizando la información encontrada en fuentes abiertas de los activos expuestos de una organización

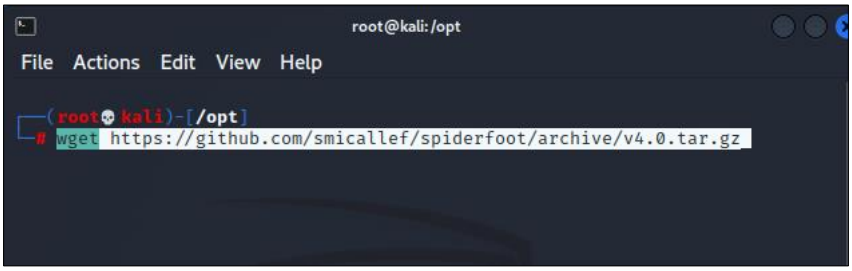
https://intel471.com/attack-surface-documentation

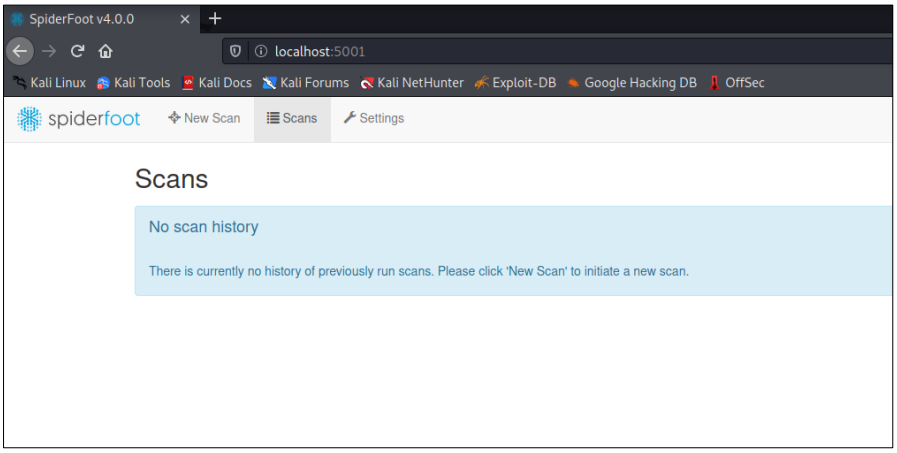
para su instalación en el entorno de trabajo se procede a seguir los pasos del repositorio oficial

https://github.com/smicallef/spiderfoot

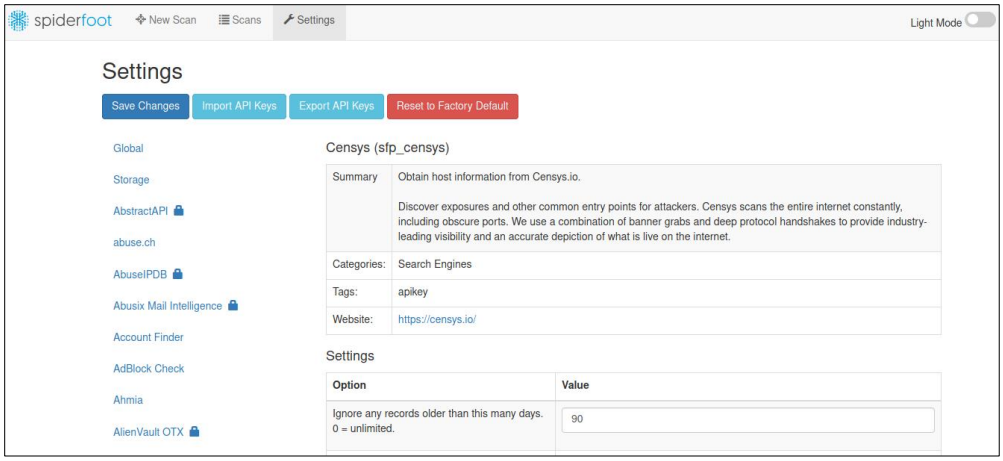
pasos para la instalación

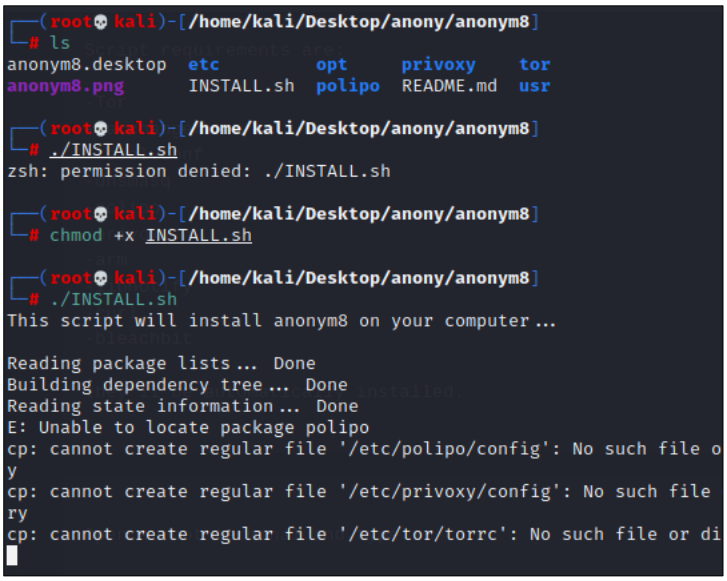
- wget https://github.com/smicallef/spiderfoot/archive/v4.0.tar.gz
- tar zxvf v4.0.tar.gz
- cd spiderfoot-4.0
- pip3 install -r requirements.txt
- python3 ./sf.py -l 127.0.0.1:5001





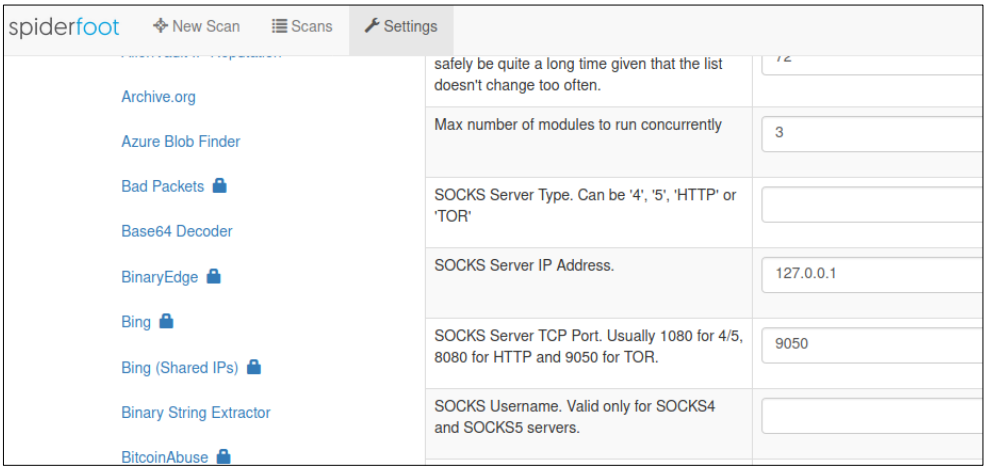
Con el fin de que spiderfoot pueda operar o realizar búsquedas debemos definirles conexiones por medio de API a motores de búsqueda





Instalación anonym8anon

Configuración búsqueda Proxy TOR



12.2. Anexo 2

Fuentes utilizadas en los escaneos

Nombre Fuente	Requiere API	Enfoque u objetivo de la fuente
AbstractAPI	SI	Dominio, teléfono y dirección IP
ARIN	NO	Registro ARIN (dominios)
Censys	SI	Direcciones IP
Azure Blob Finder	NO	Buscador de blobs de azure
Account Finder	NO	Cuentas de usuario o correo
CommonCrawl	NO	informacion de contenido web
DNS brute force	NO	IP's dominios
DNS Common SRV	NO	IP's dominios
DNS Family	NO	IP's dominios
DNS look SIDE	NO	IP's dominios
DNS raw records	NO	IP's dominios
DNS resolver	NO	IP's dominios
DNS zone transfer	NO	IP's dominios
DNSDumpster	NO	IP's dominios
Duckduckgo	NO	Motor de busqueda(correos,enlaces,dominios)
E-Mail Address Extractor	NO	Email
EmailFOrmat	NO	Email
F-Secure Riddler.io	NO	Hostname
File metadata	NO	Extraccion de metadata
Github	NO	Exposicion de informacion(dominios,documentos,etc..)
Greynoise	SI	IP, dominios
Host.io	SI	Informacion de dominios
Onyphe	SI	Valida vulnerabilidades
Hunter.io	SI	Email, hostname
Instagram	NO	redes sociales
IntelligenceX	SI	Informacion de fugas masivas de activos de informacion
Interesting file finder	NO	Documentos
Junk file finder	NO	Documentos
Keybase	NO	dominios y usuarios
LeakIX	SI	Informacion de fugas masivas de activos de informacion
Leak-lookup	SI	Informacion de fugas masivas de activos de informacion
Multiproxy.org	NO	IP's
Open bugbounty	NO	Vulnerabilidades
Openpasive dns satabase	NO	Dominios
Openphish	NO	base de datos de phishing dominios
Page information	NO	informacion general
Phishtank	NO	base de datos de phishing dominios
Phone Number Extractor	NO	Numeros de telefono
Psbdmp	NO	Email, dominios

SecurityTrails	SI	Dominios DNS
searchcode	NO	busqueda de repositorios de codigo
Shodan	SI	Direcciones IP, dominios, puertos abiertos y vulnerabilidades
Pastebin	SI	Repositorio de informacion general y codigo
Ssl Certificate Analyzer	NO	Certificados de paginas HTTPS
Urlscan.io	NO	validacion tecnologias web por medio de solicitudes
Web analitycs extractor	NO	Registros de analitycs
Whois	NO	Informacion dominio
Yandex	NO	Informacion general
Virus total	SI	Informacion de dominio, IP
Similar Domain Finder	NO	Busqueda de dominios similares
SlideShare	NO	Busqueda de informacion
Social network	NO	Redes sociales
Skymem	NO	Email
StackOverflow	NO	Dominios
Tool - DNSTwist	Ruta local	Busqueda de dominios similares
Tool - TruffleHog	Ruta local	Busuqueda en repositorios de informacion
Trumail	NO	Email
Twitter	NO	redes sociales
Wikileaks	NO	Fugas masivas
Wikipedia Edits	NO	Articulos nombres

12.3. Anexo 3

Fuente Utilizada en el escaneo 2

Nombre Fuente	Requiere API	Enfoque u objetivo de la fuente
AbstractAPI	SI	Dominio, teléfono y dirección IP
ARIN	NO	Registro ARIN (dominios)
Censys	SI	Direcciones IP
Azure Blob Finder	NO	Buscador de blobs de azure
Account Finder	NO	Cuentas de usuario o correo
CommonCrawl	NO	informacion de contenido web
DNS brute force	NO	IP's dominios
DNS Common SRV	NO	IP's dominios
DNS Family	NO	IP's dominios
DNS look SIDE	NO	IP's dominios
DNS raw records	NO	IP's dominios
DNS resolver	NO	IP's dominios
DNS zone transfer	NO	IP's dominios
DNSDumpster	NO	IP's dominios
Duckduckgo	NO	Motor de busqueda(correos,enlaces,dominios)
E-Mail Address Extractor	NO	Email

EmailFOrmat	NO	Email
F-Secure Riddler.io	NO	Hostname
File metadata extractor	NO	Extraccion de metadata
Github	NO	Exposicion de informacion(dominios,documentos,etc..)
Greynoise	SI	IP, dominios
Host.io	SI	Informacion de dominios
Onyphe	SI	Valida vulnerabilidades
Hunter.io	SI	Email, hostname
Instagram	NO	redes sociales
IntelligenceX	SI	Informacion de fugas masivas de activos de informacion
Interesting file finder	NO	Documentos
Junk file finder	NO	Documentos
Keybase	NO	dominios y usuarios
LeakIX	SI	Informacion de fugas masivas de activos de informacion
Leak-lookup	SI	Informacion de fugas masivas de activos de informacion
Multiproxy.org	NO	IP's
Open bugbounty	NO	Vulnerabilidades
Openpasive dns satabase	NO	Dominios
Openphish	NO	base de datos de phishing dominios
Page information	NO	informacion general
Phishtank	NO	base de datos de phishing dominios
Phone Number Extractor	NO	Numeros de telefono
Psbdmp	NO	Email, dominios
SecurityTrails	SI	Dominios DNS
searchcode	NO	busqueda de repositorios de codigo
Shodan	SI	Direcciones IP, dominios, puertos abiertos y vulnerabilidades
Pastebin	SI	Repositorio de informacion general y codigo
Ssl Certificate Analyzer	NO	Certificados de paginas HTTPS
Urlscan.io	NO	validacion tecnologias web por medio de solicitudes
Web analitycs extractor	NO	Registros de analitycs
Whois	NO	Informacion dominio
Yandex	NO	Informacion general
Virus total	SI	Informacion de dominio, IP
Similar Domain Finder	NO	Busqueda de dominios similares
SlideShare	NO	Busqueda de informacion
Social network	NO	Redes sociales
Skymem	NO	Email
StackOverflow	NO	Dominios
Tool - DNSTwist	Ruta local	Busqueda de dominios similares
Tool - TruffleHog	Ruta local	Busuqueda en repositorios de informacion
Trumail	NO	Email
Twitter	NO	redes sociales
Wikileaks	NO	Fugas masivas

Wikipedia Edits	NO	Articulos nombres
Company Name Extractor	NO	Informacion
Human Name Extractor	NO	nombres
Robtex	NO	IP's
Web Server Identifier	NO	Tencologias
Sublist3r PassiveDNS	NO	Subdominios

12.4. Anexo 4

Tabla de dominios e IP’s

Direccion IP	Dominio
67.199.248.14	bit.etb.com
74.114.154.18	blog.etb.com
3.224.141.128	culturainteligente.etb.com
201.245.171.129	fibraoptica.etb.com
162.223.232.73	info.etb.com
162.223.232.73	m.infosms.etb.com
52.160.40.218	mietb.etb.com
201.245.171.130	mietbeyg.etb.com
201.245.171.130	montesquieu.etb.com
201.245.171.130	moviendofibras.etb.com
200.69.125.10	ns1-auth.etb.net.co
201.244.1.170	ns2-auth.etb.net.co
201.245.171.129	ofertas.etb.com
199.7.202.165	omp.info.etb.com
199.7.205.148	omptrans.info.etb.com
40.118.164.51	pagos.etb.co
181.49.168.205	promociones.etb.com
52.160.40.218	proxytienda.azurewebsites.net
201.245.171.131	pruebasetb.etb.com
52.160.40.218	tienda.etb.com
40.118.164.51	tiendaetb.etb.com
201.245.171.129	www.etb.com
40.118.164.51	suma.etb.co
201.245.171.130	terceros.etb.com
186.155.31.121	cloudetbcasm.etb.net.co
186.155.31.122	cloudetb.etb.net.co
186.155.31.123	replicationcasm.etb.net.co
186.155.31.124	replication.etb.net.co
186.29.143.1	correo.smtpnew.etb.net.co
190.24.81.138	gestiondocumental.etb.net.co
190.24.81.200	gesdocetbapp02.etb.net.co
190.27.245.3	smtp-avas1.etb.net.co
190.27.245.4	smtp-avas02.etb.net.co

200.69.107.11	mx1.voip.etb.net.co
200.69.107.121	comunicaciones.etb.net.co
200.69.107.14	smtp-cronos.etb.net.co
200.69.107.151	tuxston.etb.net.co
200.69.107.16	smtp-atlas.etb.net.co
200.69.107.18	smtp-atlas.etb.net.co
200.69.107.215	gestion.etb.net.co
200.69.107.220	gestionuetb.etb.com.co
200.69.107.35	blog.etb.net.co
200.69.107.44	smtp-atlas.etb.net.co
200.69.107.49	smtp-atlas.etb.net.co
200.69.107.61	smtp-atlas.etb.net.co
200.69.107.63	smtp-cronos.etb.net.co
200.69.107.9	smtp-atlas.etb.net.co
200.69.107.94	servicios.voip.etb.net.co
200.69.107.97	smtp-cronos.etb.net.co
200.69.125.10	ns1-auth.etb.net.co
200.69.125.18	etb-medidor2.etb.net.co
201.244.1.170	ns2-auth.etb.net.co
201.245.171.130	etb.net.co
201.245.171.51	intranet.etb.com.co
201.245.194.209	tenantprueba.etb.net.co
201.245.202.42	controladorawifietb.etb.net.co

Tabla 14 Dominios e IP's

12.5. Anexo 5

Dominio	Cantidad puertos
info.etb.com(162.223.232.73)	2
promociones.etb.com (181.49.168.205)	2
proxytienda.azurewebsites.net (52.160.40.218)	2
tiendaetb.etb.com (40.118.164.51)	9
blog.etb.net.co (200.69.107.35)	2
cloudetb.etb.net.co (186.155.31.122)	1
cloudetbcasm.etb.net.co (186.155.31.121)	1
comunicaciones.etb.net.co (200.69.107.121)	1
controladorawifietb.etb.net.co (201.245.202.42)	1
correo.smtpnew.etb.net.co (186.29.143.1)	1
etb-medidor2.etb.net.co (200.69.125.18)	3
gesdocetbapp02.etb.net.co (190.24.81.200)	2
gestion.etb.net.co (200.69.107.215)	1
gestiondocumental.etb.net.co (190.24.81.138)	3
gestionuetb.etb.com.co (200.69.107.2209	2
intranet.etb.com.co (201.245.171.51)	1
mx1.voip.etb.net.co (200.69.107.11)	1

ns1-auth.etb.net.co (200.69.125.109)	1
ns2-auth.etb.net.co (201.244.1.170)	1
replication.etb.net.co (186.155.31.124)	1
replicationcasm.etb.net.co (186.155.31.123)	1
servicios.voip.etb.net.co (200.69.107.94)	4
smtp-atlas.etb.net.co **200.69.107.16** **200.69.107.18** **200.69.107.44** **200.69.107.49** **200.69.107.61** **200.69.107.9**	6
smtp-avas02.etb.net.co (190.27.245.4)	1
smtp-avas1.etb.net.co (190.27.245.3)	1
smtp-cronos.etb.net.co **200.69.107.14** **200.69.107.63** **200.69.107.97**	3
tuxston.etb.net.co (200.69.107.151)	1
Total general	55

Tabla 15 Relación de puertos expuestos por activo

Archivos Expuestos
2018-01-01_MATRÍZ PARRÁFOS RESPUESTA PQR V 47.xlsm
2020-04-14_CAMBIO DE SUSCRIPTOR CONTIGENCIA COVID-19..pdf
2021-10-06_BASE EXTENSOR WIFI TIPO ROUTER $0.xlsx
2021-12-21_BASE CLIENTES RETOMA DE EQUIPOS.xlsx
2021-12-21_MATRIZ MANEJO DE PQR.xlsx
2022-01-14_HOJA DE VIDA TRAMITES MOVIL.xlsx
2022-01-16_HOJA DE VIDA TRAMITES FIJA FTTX _Y COBRE_.xlsx
2022-02-18_MATRÍZ PARRÃ• FOS RESPUESTA PQR V73.xlsm
2022-03-23_GUIÓN CAMPAÑAS MÓVILES.xlsx
2022-04-01_GUIÓN DE POSVENTAS ETB HOGARES.xlsx
2022-04-01_SIMULADOR DE TARIFAS HOGARES Y MIPYMES.xlsx
2022-04-05_BASE CAMPAÑA CARTERA ABRIL.xlsx
2022-04-08_BASE CLIENTES INACTIVOS.xlsx
2022-05-03_CUENTAS RETENIDAS FTTX.xls
2022-05-03_TRANSMISIÓN DE CONTENIDOS CANAL CARACOL.xlsx
2022-05-05_BASE SUSPENSIÓN PREVENTIVA ENTE REGULADOR.xlsx
2022-05-16_CUENTAS RETENIDAS FTTX.xls
2022-05-17_DOCEABA BASE CLIENTES RETOMA DE EQUIPOS.xlsx
2022-06-01_GUIONES CAMBIO DE TECNOLOGIA DE IPTV A DUO OTT.xlsx
2022-07-05_PARRILLA DIRECTV GO FULL ESPECIAL.xlsx
2022-09-17_GUION VENTAS ETB MÓVIL_.xlsx
2022-10-10_CAMBIO DE TECNOLOGIA DE IPTV A DÃšO OTT.pdf
2022-11-22_GUION VENTAS ETB MÓVIL.xlsx

2022-11-22_OFERTA_ETB TOTAL.pdf
GUION DE PROTOCOLO.xlsx
01-08-2022-TyC-Moviles-victimas-fuerzas-publicas-Bogota-y-Nacional.pdf
2022-07-01-TyC-Hogares-Oferta-Single-internet.pdf
modelo_poder_ETB_para_menores_de_edad.pdf
Archivo20160608114723546875O.pdf
Archivo20170308070610484375O.pdf
Archivo20180911114503443380O.pdf
Archivo20210423045737305637O.pdf
Archivo20220310071743052012O.pdf
Carta-Alza-tarifas-REV-GALC-03-07-2018-v3.pdf
Cobro-de-reconexion-revision-regulacion-v3.pdf
Factores_de_Limitacion_de_velocidad_Fijo_171227.pdf
Factores_de_Limitacion_de_velocidad_MÃ³vil_171227.pdf
Mantenimientos.pdf
Politicas_gestion_trafico.pdf
Procedimiento_y_tramite_de_PQR_171227.pdf
TDT.pdf
bloqueo_equipos.pdf
Lineas_de_AtenciOn_al_Cliente.pdf
Contrato-Bogota-Noviembre.PDF
Manual_G-2425G-A.pdf
ADSL-HG531.pdf
RECIPROCAS_CORTE_MARZO_2021.xlsx
Reciprocas-Marzo-2020-WEB-ETB.xlsx
Reciprocas_Diciembre_2020_Web_ETB.xlsx
Reciprocas_Junio_2020_Web_ETB.xlsx
Reciprocas_Junio_2021_Web_ETB.xlsx
Reciprocas_Septiembre_2020_Web_ETB.xlsx
Reciprocas_Septiembre_2021_Web_ETB.xlsx
normatividad.pdf
Reporte-integrado-2018.pdf
Reporte_Integrado_2019.pdf
Mantenimiento.pdf

Tabla 16 Documentos expuestos en dominios ETB

12.6. Anexo 6

Correos recopilados por de etb.com

05nfarmer@etb.com	inversionistas@etb.com	velandias@etb.com	tecnigen_sales@etb.net.co	promotoracon@etb.net.co
05nfarmer@etb.com	jeff@etb.com	willcart@etb.com	tecnica@etb.net.co	promero@etb.net.co

12345qqq@etb.com	jeffmann@etb.com	wilsdiac@etb.com	tavoplus13@etb.net.co	proceditor@etb.net.co
1@etb.com	jorgpenn@etb.com	www.cp@etb.com	taforero@etb.net.co	presquim@etb.net.co
1msum0n2o@etb.com	joseortm@etb.com	www.zaidepilef@etb.com	systimax@etb.net.co	prados@etb.net.co
904@etb.com	juankdiaz1976@etb.com	ypoyrvwt@etb.com	sunseacompany@etb.net.co	postmaster@etb.net.co
acgronp@etb.com	juanosps@etb.com	0186aqua@etb.net.co	sunomina@etb.net.co	posnoviciado@etb.net.co
adesystem@etb.com	kely.riveral@etb.com	yneiragyg@etb.net.co	subgerente.gsxxi@etb.net.co	porras_synergy@etb.net.co
afca10@etb.com	legon@etb.com	ymejia@etb.net.co	suaza@etb.net.co	pmchaves@etb.net.co
agboolaav@etb.com	leleon@etb.com	ym@etb.net.co	strattovisual@etb.net.co	pmcarloslozanogui@etb.net.co
alalvarez@etb.com	luis.ibanezp@etb.com	yl@etb.net.co	starclub@etb.net.co	plazaja@etb.net.co
alfontorresa@etb.com	luisa88@etb.com	yeyolo@etb.net.co	ssantanab@etb.net.co	plaza_gerencia@etb.net.co
alom@etb.com	luisgarc@etb.com	yeilael@etb.net.co	srjowcat@etb.net.co	plaza_comercial@etb.net.co
alvarosm48@etb.com	luisgarl@etb.com	yaroca49@etb.net.co	sonia.orgsolarte@etb.net.co	pinedaalejandro@etb.net.co
alyep@etb.com	luisjimg@etb.com	worldmedical@etb.net.co	solucionei@etb.net.co	phonemasterhogares@etb.net.co
asuntos.contenciosos@etb.com.co	magaye@etb.com	wilsonherrera@etb.net.co	softeldigital@etb.net.co	petrochin@etb.net.co
autoservicio@etb.com	maofeta@etb.com	william.gomez@etb.net.co	smachine@etb.net.co	pclase@etb.net.co
bitacora@etb.com	maosexy@etb.com	william.alonso@etb.net.co	sitiosweb66@etb.net.co	paulgutierrez@etb.net.co
cafelagiraldo@etb.com	marcoji@etb.com	wilbeth@etb.net.co	sinfintranslate@etb.net.co	patsando8@etb.net.co
caldascom@etb.com	marialuisa@etb.com	wd21@etb.net.co	sinergiahumana@etb.net.co	patolaya@etb.net.co
cares@etb.com	marthazuluaga@etb.com	watazea8631@etb.net.co	sigrafsistemas@etb.net.co	parmodiesel@etb.net.co
cbaquero@etb.com	maxivale@etb.com	vyanken@etb.net.co	seturcolltda@etb.net.co	pacocol@etb.net.co
comercialbethel@etb.com	miguel@etb.com	vivaciudadania@etb.net.co	servisyv@etb.net.co	pablofer@etb.net.co
danntap@etb.com	montsalud@etb.com	virtin@etb.net.co	servisistemasara@etb.net.co	p.gassnbuenabentura@etb.net.co
darreina@etb.com	morris@etb.com	vipsergio@etb.net.co	servimedsistemas@etb.net.co	oyabubezoe4546@etb.net.co
dfs235@etb.com	muebleslums@etb.com	victor_vinas@etb.net.co	servicial@etb.net.co	osmejia@etb.net.co
documentosdigitales@etb.com	mundocuriosoltda@etb.com	victor_duque@etb.net.co	sereguer@etb.net.co	oryot@etb.net.co
dplastimec@etb.com	neilagamez@etb.com	viagabogota@etb.net.co	sepecol@etb.net.co	orientcolombia@etb.net.co
dreadesign@etb.com	nestor.pronatec@etb.com	verde51@etb.net.co	seguridad@etb.net.co	operamaltda@etb.net.co
emmi12@etb.com	nexcall@etb.com	ventasproelec@etb.net.co	saranm49@etb.net.co	olympo@etb.net.co
etb@etb.com	nig@etb.com	ventas@etb.net.co	santiagochanchi@etb.net.co	olupya2939@etb.net.co

eugenia.londonov@etb.com	nnc@etb.com	vaom@etb.net.co	sangregoriocota@etb.net.co	olivasoc@etb.net.co
example@etb.com	no@etb.com	vamoscolombiadp@etb.net.co	sandra.morales7@etb.net.co	ojrc@etb.net.co
fd@etb.com	notiene@etb.com	valeriomejia@etb.net.co	sandra.acero@etb.net.co	ojosalher@etb.net.co
fege@etb.com	omarmarr@etb.com	uvechyaozansa@etb.net.co	sacevedom@etb.net.co	ohchavezv@etb.net.co
flash@etb.com	omartorj@etb.com	urano1@etb.net.co	rygmarketing@etb.net.co	oggonzalez@etb.net.co
franping@etb.com	osmoge@etb.com	umesume3973@etb.net.co	rusbel.ramirez@etb.net.co	oepynuiz8326@etb.net.co
fredtafm@etb.com	pcmat@etb.com	ukaruko9587@etb.net.co	ruben.ardila@etb.net.co	oanaafuaa1314@etb.net.co
gerenciatecnoinsumos@etb.com	peteralbiero@etb.com	u3dd@etb.net.co	rosario_marinos@etb.net.co	o_geovanny@etb.net.co
german40@etb.com	planen@etb.com	turinter@etb.net.co	roggerrodriguez@etb.net.co	o.jacome@etb.net.co
giovarcarl@etb.com	plastivalle@etb.com	tsasa@etb.net.co	rodrigopesantez@etb.net.co	novocolombia@etb.net.co
giovsanl@etb.com	redessa@etb.com	trujillof@etb.net.co	restur@etb.net.co	novc@etb.net.co
gpvega@etb.com	redzipper@etb.com	tripleg@etb.net.co	redsoft_ltda@etb.net.co	nicolasp@etb.net.co
gricol@etb.com	rglogistic@etb.com	tractocarga@etb.net.co	recalca@etb.net.co	nicew@etb.net.co
hacienda@etb.com	rosamper@etb.com	toteu@etb.net.co	rafaelmatrinez@etb.net.co	nhoraegonzalez@etb.net.co
helena.gordillop@etb.com	sandherzing@etb.com	tjose.guerreroh@etb.com.co	rafael.lozano@etb.net.co	ngodoy@etb.net.co
hernvenr@etb.com	sasas@etb.com	titopuchettih@etb.net.co	rafael.carvajal@etb.net.co	netcom.ing@etb.net.co
indumerca@etb.com	teofromc@etb.com	timothy@etb.net.co	quinitron@etb.net.co	nelsonposso@etb.net.co
info@etb.com	tora@etb.com	terrazzo@etb.net.co	qiautomation@etb.net.co	nelsonberrio1@etb.net.co
infonukak@etb.com	universal@etb.com	temv@etb.net.co	pyscia@etb.net.co	nelsonberrio@etb.net.co

Correos recopilados de etb.net.co

navegandocolombia@etb.net.co	lucky.j@etb.net.co	jorge.pardo@etb.net.co	igraipb@etb.net.co	germancallejps@etb.net.co
nasatur@etb.net.co	lucia_rodriguez@etb.net.co	jorge.mejia.m@etb.net.co	ignaciojimenez@etb.net.co	gerenciaphone@etb.net.co
mys_ltda@etb.net.co	lucas79@etb.net.co	jomarc@etb.net.co	igleco@etb.net.co	gerenciapegaso@etb.net.co
mstv@etb.net.co	lrincon@etb.net.co	joforero@etb.net.co	igecon_ltda@etb.net.co	gerenciagamma@etb.net.co
mq_agerencia@etb.net.co	logisticatrial@etb.net.co	joetaya@etb.net.co	iezecy1809@etb.net.co	gerenciacasamia@etb.net.co
mppubling@etb.net.co	logisticaltd@etb.net.co	jnova@etb.net.co	ideasdulces@etb.net.co	gerencia_acr@etb.net.co
movimientosufi@etb.net.co	logistica@etb.net.co	jmrodriguez@etb.net.co	icyecol@etb.net.co	gerardoinieto@etb.net.co

motomartltda@etb.net.co	loeonardoperezm@etb.net.co	jmoncayor@etb.net.co	hwilches@etb.net.co	generar@etb.net.co
morencar@etb.net.co	linazuluaga@etb.net.co	jmauricio.cruzr@etb.net.co	hunibviviendaltda@etb.net.co	genealcol@etb.net.co
moonlabstudio@etb.net.co	lfcvlav@etb.net.co	jmarquez@etb.net.co	humanidadvigent@etb.net.co	gcalderon@etb.net.co
monica.ospina@etb.net.co	leonardoangarita@etb.net.co	jm@etb.net.co	hsolano@etb.net.co	ganaderiapampas@etb.net.co
mobiliario@etb.net.co	leobel@etb.net.co	jlpuentes@etb.net.co	horacio.ayala@etb.net.co	gamoreno@etb.net.co
mlquintero@etb.net.co	leobautista@etb.net.co	jizapata@etb.net.co	hmorales57@etb.net.co	gaitancamilo@etb.net.co
miramco@etb.net.co	lbessudo@etb.net.co	jimmyfrodriguez@etb.net.co	hmorales@etb.net.co	gagiraldo@etb.net.co
miltonchavezg@etb.net.co	lab-vet@etb.net.co	jimmy_zambrano@etb.net.co	hmg@etb.net.co	gabriel.benavides@etb.net.co
mikhail@etb.net.co	lab_vet@etb.net.co	jhiro@etb.net.co	hevega@etb.net.co	fzamorac@etb.net.co
miguelangulob@etb.net.co	kolorprint@etb.net.co	jgomez.ccbiz@etb.net.co	herring.4720@etb.net.co	fvh@etb.net.co
miguel.cortes@etb.net.co	knoxbeer@etb.net.co	jforero_univ@etb.net.co	hernanlopeza@etb.net.co	franciscoforero@etb.net.co
microprocol@etb.net.co	kmisistemas@etb.net.co	jestebangf@etb.net.co	hernan.mendoza@etb.net.co	focui@etb.net.co
mgutierrezd@etb.net.co	klarita@etb.net.co	jepena@etb.net.co	hermea@etb.net.co	finjifcuti@etb.net.co
metavalbogota@etb.net.co	kikemercado@etb.net.co	jennyromero@etb.net.co	herloz@etb.net.co	fincarestrepo@etb.net.co
mescobar1@etb.net.co	kemiplas@etb.net.co	jdmedina@etb.net.co	herder@etb.net.co	ffsolucionesipc@etb.net.co
menteactiva@etb.net.co	karing@etb.net.co	jdgrazziani@etb.net.co	henrycely@etb.net.co	festivaltours@etb.net.co
mecato@etb.net.co	kairos.7@etb.net.co	jcmorales@etb.net.co	helpdesketb@etb.com.co	fernandoperry49@etb.net.co
mecanica@etb.net.co	jzarate@etb.net.co	jcflorez@etb.net.co	heliosanchez@etb.net.co	felixmontes@etb.net.co
mcca@etb.net.co	justinadrianhi@etb.net.co	jcarvajal@etb.net.co	harvesttime@etb.net.co	felipepolo@etb.net.co
mcamacho@etb.net.co	julman@etb.net.co	jcabrera@etb.net.co	haroma@etb.net.co	felipe.estrada@etb.net.co
mbastidas@etb.net.co	julio_avila@etb.net.co	javiercomunicaciones@etb.net.co	hamunera@etb.net.co	fds@etb.net.co
mayolediciones@etb.net.co	julio.delgado@etb.net.co	jatoca@etb.net.co	guipinzon@etb.net.co	fcubides@etb.net.co
maurosfood@etb.net.co	juliansolerolarte@etb.net.co	jamesacevedo@etb.net.co	guillermopena7@etb.net.co	famecal1@etb.net.co
mauricio.mm@etb.net.co	julianbedoya@etb.net.co	jairoparra@etb.net.co	gsegovia@etb.net.co	eventosanato@etb.net.co
matco@etb.net.co	jufranco@etb.net.co	jaimeiba@etb.net.co	grupomidas@etb.net.co	escuelacorporativa@etb.com.co
marzuza@etb.net.co	juanpico@etb.net.co	jaguarmg@etb.net.co	grupocrltda@etb.net.co	escorcia@etb.net.co
markaproduccion3@etb.net.co	juanp.gomez@etb.net.co	iwssuba@etb.net.co	grinter@etb.net.co	ernesthernandez@etb.net.co
marioqop1805@etb.net.co	juanmurra.comfia@etb.net.co	ivanrosero@etb.net.co	grant@etb.net.co	eoleki2024@etb.net.co
marialuisap@etb.net.co	juanmontero17@etb.net.co	ivanpallares@etb.net.co	grandesconstructores@etb.net.co	encuestasfg@etb.net.co

mariaguardiola48@etb.net.co	juanmac@etb.net.co	ivanchopa@etb.net.co	graflex.gerencia@etb.net.co	e-maileerg@etb.net.co
margaritagnecco@etb.net.co	juankarlos@etb.net.co	ismac_ong@etb.net.co	gpulido@etb.net.co	ejsgcoomulgar@etb.net.co
marco_forero@etb.net.co	juank@etb.net.co	ipadmin@etb.net.co	gonzalo.garcia@etb.net.co	ehodson@etb.net.co
marcemendoza@etb.net.co	juana.duquea@etb.net.co	inquieto@etb.net.co	gmanriqueb@etb.net.co	egesa@etb.net.co
maranata11@etb.net.co	jsdmasivos@etb.net.co	ingmama@etb.net.co	gladysp@etb.net.co	efewipo6749@etb.net.co
mailbox@etb.net.co	jqsoftware@etb.net.co	ingesetronics@etb.net.co	giuseppe.f@etb.net.co	eerg@etb.net.co
mag49@etb.net.co	jpmejia@etb.net.co	inescol@etb.net.co	giro.agenciacreativa@etb.net.co	edugobor@etb.net.co
mafapaez@etb.net.co	jpassega@etb.net.co	import_ortizo@etb.net.co	giraldoga@etb.net.co	edgarh_velandia@etb.net.co
macrodigital@etb.net.co	josecoca@etb.net.co	impel@etb.net.co	giovannicajas@etb.net.co	edgarespitia@etb.net.co
macanguro@etb.net.co	jose_pabon@etb.net.co	imatex@etb.net.co	giffunip@etb.net.co	edgar.velandia@etb.net.co
luzmonroym@etb.net.co	jorgevanegas55@etb.net.co	imapack@etb.net.co	gfischer@etb.net.co	edfuturo@etb.net.co
luisk1233@etb.net.co	jorgerubiano@etb.net.co	iicia7572@etb.net.co	gerproyectos@etb.net.co	edesaesp@etb.net.co
luisf.pardo@etb.net.co	jorgegalepos@etb.net.co	ihqbiogenex@etb.net.co	germmeja@etb.net.co	edenia@etb.net.co
luisalberto2006@etb.net.co	jorgebustamante@etb.net.co	ihixijut5415@etb.net.co	germantenza@etb.net.co	edelec@etb.net.co

edecoltda@etb.net.co	darusanc@etb.net.co	comercialgjaiber@etb.net.co	carolinaduran@etb.net.co	alfonsorojas@etb.net.co
edcmail@etb.net.co	danielhdez@etb.net.co	comercial_granja@etb.net.co	carmencriado@etb.net.co	alexseb@etb.net.co
edal@etb.net.co	daniel.colorado@etb.net.co	colsaclimitada@etb.net.co	carlosmartinezg@etb.net.co	alex.alfo...@etb.net.co
ed.valencia@etb.net.co	daferautomotriz@etb.net.co	coex@etb.net.co	carlosjr@etb.net.co	alejo.archila@etb.net.co
ectricol_gerenc@etb.net.co	daedcot@etb.net.co	codereslta@etb.net.co	carlosbernal@etb.net.co	alberto.reyes@etb.net.co
ecruzmar@etb.net.co	dacooperaciones@etb.net.co	cocovi@etb.net.co	carlosbarajas@etb.net.co	ajtamayo@etb.net.co
ecorescate@etb.net.co	dacoadm@etb.net.co	cocoh@etb.net.co	carlos.augusto@etb.net.co	ajromero@etb.net.co
ecol@etb.net.co	dackar@etb.net.co	cocelca@etb.net.co	carlorjo@etb.net.co	agutimarketing@etb.net.co
ecoinsa@etb.net.co	dac@etb.net.co	cocel@etb.net.co	carled@etb.net.co	agrocar@etb.net.co
ecofloraltda@etb.net.co	d2click@etb.net.co	cobroker@etb.net.co	carfaja@etb.net.co	aeropostalvta@etb.net.co
ecochem@etb.net.co	d_marzinter@etb.net.co	cobando@etb.net.co	canamo@etb.net.co	aerointer@etb.net.co
ecobosques@etb.net.co	d_lechepersonal@etb.net.co	coas51@etb.net.co	camilocornejo@etb.net.co	aerocontabilidad@etb.net.co
ecoambientales@etb.net.co	d_edalo@etb.net.co	coarquing@etb.net.co	calier_pharma@etb.net.co	adriana75@etb.net.co

ecnifil@etb.net.co	d_81ltda@etb.net.co	coanco@etb.net.co	caherna@etb.net.co	adorsa@etb.net.co
ecingeniero@etb.net.co	d.gonzalez@etb.net.co	coacredito@etb.net.co	c6e6dd0a.119b1084@etb.net.co	acnsever@etb.net.co
eci100@etb.net.co	d.ce@etb.net.co	cnovoa@etb.net.co	bycomp@etb.net.co	abuse@etb.net.co
duquesilvio@etb.net.co	cyrgo@etb.net.co	cnn_vehiculos@etb.net.co	bltravel@etb.net.co	9211_____0505@etb.net.co
ducast@etb.net.co	cypresad@etb.net.co	cnn_inversiones@etb.net.co	bioagrarius@etb.net.co	4014405b.336a0582@etb.net.co
drsmabogados@etb.net.co	cypres@etb.net.co	cnml@etb.net.co	biccoleg@etb.net.co	4012ed93.66571df@etb.net.co
dlozano@etb.net.co	cypltda@etb.net.co	cnegrelli@etb.net.co	belensamper@etb.net.co	4012eb25.fe6a753f@etb.net.co
distri666@etb.net.co	cyphercolombia@etb.net.co	cncacao@etb.net.co	b.garcia@etb.net.co	40129042.f32b2775@etb.net.co
dirsetronics@etb.net.co	cypet@etb.net.co	cnc@etb.net.co	axel2012@etb.net.co	401150f2.dd53c69a@etb.net.co
directorosnj@etb.net.co	cypc@etb.net.co	cnasistemas@etb.net.co	avimarcotnorte@etb.net.co	3fe90fb4.9faedff0@etb.net.co
diradmonsulicor@etb.net.co	cymltda@etb.net.co	cmztanpatank@etb.net.co	avimarcotcentro@etb.net.co	3fd69fb7.b67f4226@etb.net.co
dimed@etb.net.co	cykabogados@etb.net.co	cmvila@etb.net.co	avelinorodriguez@etb.net.co	3fd69ed9.9ddea1bd@etb.net.co
dillmann@etb.net.co	cygltda@etb.net.co	cmroman@etb.net.co	atlcely@etb.net.co	3fd379a4.3e5937aa@etb.net.co
diegorobles@etb.net.co	cygauditores@etb.net.co	cmrb60@etb.net.co	asdecafe@etb.net.co	29daebfb.6e45e8d4@etb.net.co
diegoparramarti@etb.net.co	cycltda@etb.net.co	cmpatriciamv@etb.net.co	ascolcirugia@etb.net.co	123.uupk@etb.net.co
diegomartin@etb.net.co	cycbancainv@etb.net.co	cmotorsa@etb.net.co	ascapc.i@etb.net.co	
diegomar60@etb.net.co	cyaltda@etb.net.co	cmontana@etb.net.co	arviajes@etb.net.co	
diegoforero@etb.net.co	cya@etb.net.co	cmoliz@etb.net.co	aruedace@etb.net.co	
diegocardenas@etb.net.co	cvgerencia@etb.net.co	clientescjv2009@etb.net.co	arcansas@etb.net.co	
diegoboteroyasoc@etb.net.co	curioso@etb.net.co	cleutoto@etb.net.co	araimep3404@etb.net.co	
diegoarenas@etb.net.co	curibec@etb.net.co	ckerguel@etb.net.co	araguatos@etb.net.co	
diego007@etb.net.co	crvd@etb.net.co	cimac@etb.net.co	aqualab_ltda@etb.net.co	
diego_beltran@etb.net.co	cristian.mrbrands@etb.net.co	ciconalex@etb.net.co	andresogc2010@etb.net.co	
diego_barragan@etb.net.co	crenova@etb.net.co	chuertasunas@etb.net.co	andresgonzaleznospam@etb.net.co	
diego.gomez@etb.net.co	cqmercaworld@etb.net.co	chrdivulgar@etb.net.co	andresgonzalez@etb.net.co	
diear@etb.net.co	cpjmspscol@etb.net.co	choconta@etb.net.co	andresfg@etb.net.co	
didemas@etb.net.co	cosmoderm@etb.net.co	chantallmb@etb.net.co	anatolia@etb.net.co	
didactimedios@etb.net.co	corpogen@etb.net.co	ceramosb@etb.net.co	anacarreira@etb.net.co	
didactica@etb.net.co	corfinanzasltd@etb.net.co	centrodonbosco@etb.net.co	amtmercaworld@etb.net.co	

dicsonltd@etb.net.co	copulido@etb.net.co	cenfordes@etb.net.co	ambrombogota@etb.net.co
dicsonhidraulica@etb.net.co	cooericsson.con@etb.net.co	cemendoza@etb.net.co	alvarobaquero@etb.net.co
dicon@etb.net.co	convers_c@etb.net.co	cedhitours@etb.net.co	alvaro.herrera@etb.net.co
dicomtelsa@etb.net.co	contubix@etb.net.co	ce3d76f1.10507a1b@etb.net.co	almacenparamo@etb.net.co
dicolnox@etb.net.co	consulmexcol@etb.net.co	cduqueb@etb.net.co	alimu.ventas@etb.net.co
dealonline@etb.net.co	consulado100@etb.net.co	castellanosi@etb.net.co	aliciamunoz@etb.net.co
dcordoba@etb.net.co	conchas@etb.net.co	cascabel@etb.net.co	alicia_ramos@etb.net.co
davidgg@etb.net.co	comerciali.reina@etb.net.co	carrenogerencia@etb.net.co	alfymad@etb.net.co

12.7. Anexo 7

Relación de repositorios activos identificados

https://github.com/melezov/etb
https://pastebin.com/1jnu3hQX
https://pastebin.com/1LXajK1X
https://pastebin.com/1W7ZgFDZ
https://pastebin.com/2zMkzB2z
https://pastebin.com/39wpEZvC
https://pastebin.com/3CcpLPgE
https://pastebin.com/3dfXh3eL
https://pastebin.com/3TeQA8yX
https://pastebin.com/4qbpd2HW
https://pastebin.com/756q9sNR
https://pastebin.com/7wkdGpfQ
https://pastebin.com/8Sufu1sT
https://pastebin.com/8tFQgKqh
https://pastebin.com/BECQF3hw
https://pastebin.com/Cj4eDN9Z
https://pastebin.com/CMhw7pAC
https://pastebin.com/E1v8fdje
https://pastebin.com/FAMt1gng
https://pastebin.com/HMeh32x3
https://pastebin.com/jBjnFtKB
https://pastebin.com/KviUXBwr
https://pastebin.com/NqsHZFS7
https://pastebin.com/QCvytC31
https://pastebin.com/QTsRYBW4
https://pastebin.com/R3pWg7Y8
https://pastebin.com/T0ReH2Db
https://pastebin.com/WHknM9Me

https://pastebin.com/Xg04KBzz

12.8. Anexo 8

Resultados de filtrar los correos electrónicos

acgronp@etb.com	luisjimg@etb.com	pclase@etb.net.co	servimedsistemas@etb.net.co	vyanken@etb.net.co
adesystem@etb.com	magaye@etb.com	pcmat@etb.com	servisistemasara@etb.net.co	wilbeth@etb.net.co
agboolaav@etb.com	maofeta@etb.com	peteralbiero@etb.com	servisyv@etb.net.co	willcart@etb.com
alalvarez@etb.com	maosexy@etb.com	petrochin@etb.net.co	seturcolltda@etb.net.co	william.alonso@etb.net.co
alfontorresa@etb.com	marcoji@etb.com	phonemasterhogares@etb.net.co	sigrafsistemas@etb.net.co	william.gomez@etb.net.co
alom@etb.com	marialuisa@etb.com	pinedaalejandro@etb.net.co	sinergiahumana@etb.net.co	wilsdiac@etb.com
alyep@etb.com	marthazuluaga@etb.com	planen@etb.com	sinfintranslate@etb.net.co	wilsonherrera@etb.net.co
asuntos.contenciosos@etb.com.co	maxivale@etb.com	plastivalle@etb.com	smachine@etb.net.co	worldmedical@etb.net.co
autoservicio@etb.com	miguel@etb.com	plaza_comercial@etb.net.co	softeldigital@etb.net.co	yeilael@etb.net.co
bitacora@etb.com	montsalud@etb.com	plaza_gerencia@etb.net.co	solucionei@etb.net.co	yeyolo@etb.net.co
cafelagiraldo@etb.com	morris@etb.com	plazaja@etb.net.co	sonia.orgsolarte@etb.net.co	yl@etb.net.co
caldascom@etb.com	muebleslums@etb.com	pmcarloslozanogui@etb.net.co	srjowcat@etb.net.co	ym@etb.net.co
cares@etb.com	mundocuriosoltda@etb.com	pmchaves@etb.net.co	ssantanab@etb.net.co	ymejia@etb.net.co
cbaquero@etb.com	neilagamez@etb.com	porras_synergy@etb.net.co	starclub@etb.net.co	yneiragyg@etb.net.co
comercialbethel@etb.com	nelsonberrio@etb.net.co	posnoviciado@etb.net.co	strattovisual@etb.net.co	ypoyrvwt@etb.com
danntap@etb.com	nelsonposso@etb.net.co	postmaster@etb.net.co	suaza@etb.net.co	
darreina@etb.com	nestor.pronatec@etb.com	prados@etb.net.co	subgerente.gsxxi@etb.net.co	
documentosdigitales@etb.com	netcom.ing@etb.net.co	presquim@etb.net.co	sunomina@etb.net.co	
dplastimec@etb.com	nexcall@etb.com	proceditor@etb.net.co	sunseacompany@etb.net.co	
dreadesign@etb.com	ngodoy@etb.net.co	promero@etb.net.co	systimax@etb.net.co	
eugenia.londonov@etb.com	nhoraegonzalez@etb.net.co	promotoracon@etb.net.co	taforero@etb.net.co	
example@etb.com	nicew@etb.net.co	pyscia@etb.net.co	tecnica@etb.net.co	
fd@etb.com	nicolasp@etb.net.co	qiautomation@etb.net.co	tecnigen_sales@etb.net.co	
fege@etb.com	nig@etb.com	quinitron@etb.net.co	temv@etb.net.co	

flash@etb.com	nnc@etb.com	rafael.carvajal@etb.net.co	teofromc@etb.com	
franping@etb.com	no@etb.com	rafael.lozano@etb.net.co	terrazzo@etb.net.co	
fredtafm@etb.com	notiene@etb.com	rafaelmatrinez@etb.net.co	timothy@etb.net.co	
gerenciatecnoinsumos@etb.com	novc@etb.net.co	recalca@etb.net.co	titopuchettih@etb.net.co	
giovarcarl@etb.com	novocolombia@etb.net.co	redessa@etb.com	tjose.guerreroh@etb.com.co	
giovsanl@etb.com	o.jacome@etb.net.co	redsoft_ltda@etb.net.co	tora@etb.com	
gpvega@etb.com	o_geovanny@etb.net.co	redzipper@etb.com	toteu@etb.net.co	
gricol@etb.com	oggonzalez@etb.net.co	restur@etb.net.co	tractocarga@etb.net.co	
hacienda@etb.com	ohchavezv@etb.net.co	rglogistic@etb.com	tripleg@etb.net.co	
helena.gordillop@etb.com	ojosalher@etb.net.co	rodrigopesantez@etb.net.co	trujillof@etb.net.co	
hernvenr@etb.com	ojrc@etb.net.co	roggerrodriguez@etb.net.co	tsasa@etb.net.co	
indumerca@etb.com	olivasoc@etb.net.co	rosamper@etb.com	turinter@etb.net.co	
info@etb.com	olympo@etb.net.co	rosario_marinos@etb.net.co	universal@etb.com	
infonukak@etb.com	omarmarr@etb.com	ruben.ardila@etb.net.co	uvechyaozansa@etb.net.co	
inversionistas@etb.com	omartorj@etb.com	rusbel.ramirez@etb.net.co	valeriomejia@etb.net.co	
jeff@etb.com	operamaltda@etb.net.co	rygmarketing@etb.net.co	vamoscolombiadp@etb.net.co	
jeffmann@etb.com	orientcolombia@etb.net.co	sacevedom@etb.net.co	vaom@etb.net.co	
jorgpenn@etb.com	oryot@etb.net.co	sandherzing@etb.com	velandias@etb.com	
joseortm@etb.com	osmejia@etb.net.co	sandra.acero@etb.net.co	ventas@etb.net.co	
juanosps@etb.com	osmoge@etb.com	sangregoriocota@etb.net.co	ventasproelec@etb.net.co	
kely.riveral@etb.com	p.gassnbuenabentura@etb.net.co	santiagochanchi@etb.net.co	viagabogota@etb.net.co	
legon@etb.com	pablofer@etb.net.co	sasas@etb.com	victor_duque@etb.net.co	
leleon@etb.com	pacocol@etb.net.co	seguridad@etb.net.co	victor_vinas@etb.net.co	
luis.ibanezp@etb.com	parmodiesel@etb.net.co	sepecol@etb.net.co	vipsergio@etb.net.co	
luisgarc@etb.com	patolaya@etb.net.co	sereguer@etb.net.co	virtin@etb.net.co	
luisgarl@etb.com	paulgutierrez@etb.net.co	servicial@etb.net.co	vivaciudadania@etb.net.co	

12.9. Anexo 9

Resultados de h8mail

Target	Type	Data
documentosdigitales@etb.com	HUNTER_PUB	13
cbaquero@etb.com	HUNTER_PUB	13
dfs235@etb.com	HUNTER_PUB	13
dreadesign@etb.com	HUNTER_PUB	13
904@etb.com	HUNTER_PUB	13
cares@etb.com	HUNTER_PUB	13
acgronp@etb.com	HUNTER_PUB	13
alvarosm48@etb.com	HUNTER_PUB	13
emmi12@etb.com	HUNTER_PUB	13
bitacora@etb.com	HUNTER_PUB	13
danntap@etb.com	HUNTER_PUB	13
1@etb.com	HUNTER_PUB	13
alalvarez@etb.com	HUNTER_PUB	13
1msum0n2o@etb.com	HUNTER_PUB	13
alyep@etb.com	HUNTER_PUB	13
dplastimec@etb.com	HUNTER_PUB	13
autoservicio@etb.com	HUNTER_PUB	13
alom@etb.com	HUNTER_PUB	13
cafelagiraldo@etb.com	HUNTER_PUB	13
agboolaav@etb.com	HUNTER_PUB	13
afca10@etb.com	HUNTER_PUB	13
adesystem@etb.com	HUNTER_PUB	13
caldascom@etb.com	HUNTER_PUB	13
asuntos.contenciosos@etb.com.co	HUNTER_PUB	80
12345qqq@etb.com	HUNTER_PUB	13
darreina@etb.com	HUNTER_PUB	13
alfontorresa@etb.com	HUNTER_PUB	13
comercialbethel@etb.com	HUNTER_PUB	13
05nfarmer@etb.com	HUNTER_PUB	13

12.10. Anexo 10

Activo	Activos	vectores de acceso identificados	Amenazas	Amenaza	Riesgos
Dominios y IP	34 IP con puertos expuestos	15 servicios unicos	4	Certificados SSL (MIM)	Riesgos tecnológicos Riesgo reputacional
				Cargue de backdoor	
				Ddos	
				DNS	
Vulneravilidades	147 vulnerabilidades	21 vulnerabilidades criticas altas	5	RCE(ejecucion de codigo remoto	Riesgos tecnológicos Riesgo reputacional
				Phishing	

				Malware Web attack(owasp)cadena de suministro Fuga de datos(data leak)	
Metadatos	6 tecnologias	12 vulnerabilidades	4	passwordspray fuerza bruta cadena de suministro Phishing	Riesgo de seguridad y fraude Riesgos tecnológicos
Documentos Expuestos	57 documentos publicos	3 URL	6	Phishing Vishing Smishing Suplantación de identidad Fuga de datos(data leak) exposición de información	Riesgo reputacional Riesgo de cumplimiento Riesgo competitivo Riesgo económico
Nube	1	0	2	cadena de suministro passwordspray	Riesgos operativos Riesgo de seguridad y fraude
Dominios similares	65	13 no tienen relacion 52 no estan en uso	5	Phishing (BEC) Phishing Spearphishing Malware Fuga de datos(data leak)	Riesgo de seguridad y fraude Riesgos operativos
Correos electrónicos	728	215 correos validos o veeridicos 29 expuestos en data leak	5	Fuga de datos(data leak) Phishing Spearphishing Vishing Smishing Suplantación de identidad	Riesgo reputacional Riesgo de cumplimiento Riesgo competitivo Riesgo económico
Repositorios	29	0 informacion relevante	0	No se identifica en los activos	Riesgo reputacional Riesgo de cumplimiento Riesgo competitivo Riesgos tecnológicos
Tecnologias	12	5 valores unicos	1	cadena de suministro	Riesgo competitivo Riesgos tecnológicos
Total	1079	365	32		