Estudio de la detección de ciberataques de estenografia para evitar ingreso de software malicioso y evitar pérdidas de información en la cámara de comercio de Barrancabermeja

Estudiante

Jairo Alberto Moreno Jaraba

Asesor

Mauricio Ochoa Sana

Monografía Para Grado

Universidad nacional abierta y a distancia - UNAD

Escuela de ciencias básicas, tecnología e ingeniería

Especialización en redes de nueva generación

Barrancabermeja

2023

Contenido

Lista de Figuras

Lista de tablas

Resumen

Este trabajo se centra en identificar técnicas existentes de detección de software malicioso que se oculta por medio de Esteganografía para evitar la pérdida de información en laempresa cámara de comercio de Barrancabermeja, algo que es esencial trabajarlo no solo en los dispositivos finales sino también dentro de las redes, en especial las de nueva generación.

Existe un creciente interés por el conocimiento, difusión y utilización de la Esteganografía, dinamizada por el avance tecnológico de los sistemas computacionales. La Esteganografía es una ciencia que se perfila como tecnología de punta en los procesos de ocultamiento de información. Facilita el tránsito de archivos con buenos niveles de seguridad en la privacidad de los mensajes. Permite aplicar técnicas para ocultar información en imágenes, sonidos y canales encubiertos.

La cámara de comercio de Barrancabermeja cuenta con instrumentos de control los cuales contienen aparte de la base de datos de empresas y personas naturales, una base de datos de empleados y contratistas, consecutivo de correspondencia, inventario de activos; y estos a su vez, contienen registros de información no reservada o clasificadas de empleados y contratistas, registros de comunicaciones, enviadas, internas y recibidas, registro de información, activos y suministros entre otros. La cámara cuenta con una administración del departamento de sistemas el cual es el encargado de velar por esta información que es recopilada y guardada en el servidor.

La Cámara de Comercio reconoce abiertamente la importancia de la seguridad de la información, así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes

que afecten el normal funcionamiento de los procesos. La Seguridad de la Información en la Cámara de Comercio, tiene como objetivo proteger la información de una gran variedad de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el riesgo, reducir los impactos por incidentes de seguridad, generar oportunidades de negocio y para dar cumplimiento legal, contractual y regulatorio; el debido cuidado en el manejo de la información, permitirá a la Cámara de Comercio mantener relaciones de confianza con sus clientes actuales y futuros. Esta problemática será manejada socializando a los funcionarios de la Cámara de Comercio de Barrancabermeja las técnicas en contra de delitos informáticos que pueden afectar toda información que reposa en esta empresa.

Abstract

The current proposal focuses on identifying existing techniques for detecting malicious software that is hidden by stenography to avoid loss of information in the Barrancabermeja Chamber of Commerce company, something that is essential to work not only on end devices butalso within networks, especially new generation ones.

There is a growing interest in the knowledge, diffusion and use of steganography, stimulated by the technological advance of computer systems. Steganography is a science that is emerging as state-of-the-art technology in information concealment processes. It facilitates the transit of files with good levels of security in the privacy of messages. It allows applying techniques to hide information in images, sounds and covert channels.

The Barrancabermeja Chamber of Commerce has control instruments which contain, apart from the database of companies and natural persons, a database of employees and contractors, consecutive correspondence, inventory of assets; and these, in turn, contain records of non-reserved or classified information of employees and contractors, communications records, sent, internal and received, record of information, assets and supplies among others. The camera has an administration of the systems department which is in charge of ensuring this information is collected and stored on the server.

This problem will be managed by sharing with the officials of the Barrancabermeja Chamber of Commerce the techniques against computer crimes that can affect all information that rests in this company.

Introducción

La globalización de la tecnología ha hecho que todos los usuarios del mundo hagan uso diario de dispositivos electrónicos móviles o fijos, y para obtener conectividad con el mundo se hace necesario el uso de redes incluidas las NGN (redes de nueva generación), lo anterior preocupa el aseguramiento y veracidad de la información que dentro de los mismos circula. El mal uso de estos equipos y redes por desconocimiento o por ignorancia permite que la información esté expuesta y sufra afectaciones de modificación, secuestro o pérdida de esta. Uno de los medios más comunes en la actualidad que se usa como medio para camuflar virus, ramsonware u otro software malicioso es la esteganografía, muchos usuarios pueden ver una simple imagen como inofensiva, pero dentro de su código se oculta algún tipo de programa que podría afectar la integridad de la información y darse lugar a que se cometa un delito informático como lo dice la Ley 1273 de 2009 de Colombia. Desafortunadamente este tipo de archivos pueden viajar igualmente por las redes de comunicación, sin importar el tipo.

Dentro de las redes de información, se habla de la esteganografía, en la cual el objetivo es ocultar información por medio de los mismos protocolos que trabajan las redes.

“La esteganografía de red hace uso de canales encubiertos para transferir información, un canal encubierto se puede definir como un canal que cumple otros propósitos para los que no fue hecho, en este caso, enviar información de manera secreta” (Hernández López, 2013).

En el presente trabajo se realizó un análisis de las posibles soluciones para prevención de esteganografía dentro de las empresas, con la finalidad de asegurar la información dentro de estas. La estructura de este documento hará un recorrido sobre algunos conceptos generales de la

esteganografía y las redes NGN, posteriormente se encontrará con el desarrollo y resultados de este trabajo.

La evolución del sector hacia las redes convergentes o Redes de Nueva Generación NGN es de gran detalle por la sociedad de la información, ya que esta evolución implica infraestructura para el transporte de la información y para la conectividad de las personas. La convergencia de servicios, aplicaciones y dispositivos impulsa esta tendencia y con ello los ataques a esta infraestructura tecnológica.

Justificación

En la actualidad la era de la digitalización y más aún los servicios en la nube han hecho que las empresas y las personas tengan algún dispositivo que los conecte a las redes y por medio de ella pueden trabajar, hacer un poco de ocio, ver televisión y muchas más cosas. Este hecho hace que los riesgos estén presentes, más aún lejos del costo del software y del hardware, lo más importante y costoso dentro de estos dispositivos es la información que manejan las empresas y los usuarios. De ahí que, incluso en Colombia existe la ley 1273 de 2009 “de la protección de la información y de los datos” que tipifica los delitos informáticos.

Por lo tanto, es importante que se involucre el tema de la seguridad informática y estar conscientes de su relevancia, para así empezar a dejar de pensar en los ciberataques como un escenario lejano. En la actualidad por medio del uso de la esteganografía se oculta software malicioso para afectar la información de las empresas y los usuarios. Todo lo anterior debido a que día a día se presentan más casos de ataque a empresas, y la gran mayoría de usuario tiene un conocimiento muy básico de manejo de computadores y esto hace que se busque estrategias para que se puedan bloquear estos ataques antes de que lleguen al usuario final.

Planteamiento del problema

Durante la observación e indagación de algunas situaciones informáticas se mostró que el riesgo de software malicioso dentro de las empresas está latente, a lo largo del tiempo se evidencia que algunas entidades están preparadas para asumir dichas intromisiones, otras les ha costado recuperar su información, hasta su capital humano y económico por las evidentes afectaciones al ser víctimas de esta situación; en este caso se ha tomado en referencia el reporte de la empresa Telstra, en el cual indican que el 59% de las empresas por lo menos una vez al mes fueron afectadas por algún tipo de amenaza (Telstra, 2021), esto afectando su rendimiento y productividad.

Teniendo como punto de partida las innumerables herramientas que existen actualmente para detectar los ataques de seguridad a las empresas podemos mencionar una de los más altos desafíos de estas técnicas el cual es la esteganografía, la cual permite poner mensajes ocultos dentro de algunos que están mucho más visibles al usuario. Cabe resaltar la importancia de capacitar a los trabajadores en el uso correcto de las herramientas informáticas ya que la ignorancia de los usuarios al no conocer los cuidados básicos en seguridad pueden generar situaciones que a largo, mediano y corto plazo crean situaciones que amenazan la seguridad de la entidad y todo esto al hacer mal uso de sus respectivos equipos y redes que le proporciona la empresa.

La situación en la actualidad posterior a la pandemia según el periódico el País, a mayo del 2020 reportó que casi seis millones de personas están trabajando desde casa, esto ha generado que mucha de la información de las empresas se está trabajando desde equipos en esos lugares, los cuales no se sabe si cuentan con la seguridad que la empresa tiene dentro de sus instalaciones, además del riesgo en el uso de equipos compartidos dentro de sus hogares. Por ello es necesarios

verificar también el riesgo de esteganografía dentro de los servicios en la nube que tengan las empresas.

Un ejemplo claro de esto lo reporta el sitio web Cyclonis quienes manifiestan que los investigadores de la empresa Kaspersky, emplean la esteganografía para realizar ataques, donde por medio de un correo electrónico, envían un archivo de Excel, el cual al ejecutarlo y habilitar los permisos, se ejecutan macros ocultos que cargan un script, el que después de ejecutarse, también descarga una imagen de un sitio seguro, pero que igual al abrirla trae consigo otro script que ejecuta un programa que lo utilizan para robar credenciales de inicio de sesión de Windows (Duran, 2021).

Evidenciando lo antes mencionado existen las redes NGN las cuales brindarán más conectividad y servicios a los usuarios finales, pero todo esto nos lleva al siguiente cuestionamiento ¿Estará el mundo listo para salvaguardar la información de ataques que utilicen métodos de esteganografía para ocultar código malicioso y que dañe o secuestre la información de los equipos?, es una pregunta que debe ser resuelta por los usuarios que hacen uso constante de las herramientas tecnológicas.

Llevando todo esto a un contexto más cercano enfocaremos este proyecto en una empresa a nivel nacional con sucursal en la ciudad de Barrancabermeja-Santander la cual esta denominada como Cámara de comercio de Barrancabermeja, en dicha dependencia se maneja información de todas las empresas que tienen registro mercantil, adjuntado en bases de datos, documentos, entre otros de los usuarios de estas empresas; ¿Estará la cámara de comercio lista para salvaguardar la información de ataques que utilicen métodos de esteganografía para ocultar códigos maliciosos y que dañe o secuestre la información de los equipos? ¿Qué tan preparada

esta esta entidad para responsabilizarse de las perdidas, si no tienen los conocimientos y las herramientas para que no sea robada la información de los usuarios?

En manos de los directivos, personas que manejan dicha información y del buen uso de las herramientas informáticas como antes se mencionó, está la seguridad de que el sistema no pueda ser dañado por personas ajenas a la entidad.

Es por lo antes mencionado que se plantea la siguiente pregunta en esta monografía ¿Cómo puede salvaguardar la información digital de sus usuarios la cámara de comercio de Barrancabermeja?

Objetivos

Objetivo general

Identificar técnicas existentes de esteganografía que están afectando la seguridad de la información de los usuarios de la cámara de comercio de Barrancabermeja

Objetivos específicos

Identificar las diferentes técnicas de seguridad de información usadas para la Esteganografía.

Reconocer los sistemas de seguridad existentes más usados necesarios para proteger la información de las Redes NGN.

Comparar los sistemas de detección de esteganografía de la cámara de comercio de Barrancabermeja con la sede principal de las cámaras de comercio.

Estado del arte

Marco Conceptual

Se hace necesario el conocimiento de los términos o conceptos que soportan la propuesta, los cuales son: Esteganografía, Estegoanálisis, Criptografía, Objeto Contenedor, Estego-Objeto, Adversario.

Esteganografía

La esteganografía, es descrita en muchos artículos como un Arte de ocultar información debido a su uso en la historia. (Observatorio de la Seguridad de la Información, 2012).

Estegoanálisis

El Estegoanálisis es la técnica que se usa para recuperar mensajes ocultos o para impedir la comunicación por esteganografía.

Criptografía

Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

Objeto Contenedor

Se trata de la entidad que se emplea para portar el mensaje oculto.

Estego-objeto

Se trata del objeto contenedor más el mensaje encubierto.

Adversario

Son todos aquellos entes a los que se trata de ocultar la información encubierta.

Aspectos generales

La esteganografía bien del griego στεγανος steganos, "cubierto" u "oculto", y γραφος graphos, "escritura" el cual aplica técnicas que permiten ocultar mensajes u objetos, dentro de otros, a esto se les llama portadores. Con esto, establecen un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal. (Navas, 2010)

En la actualidad el tema de la Esteganografía es de curiosidad de muchas personas, tanto expertos en seguridad informática como en los mismos hackers, quienes tal vez se han beneficiado más de esto. El poder ocultar información dentro de un archivo que parece seguro, es un atractivo para los últimos y se ha prestado para que realicen sus ciber ataques a nivel mundial. Incluso se presentan video de herramienta como Kali Linux, la cual le permite explorar estas posibilidades a cualquier usuario con conocimientos básicos de informática.

Pilares de la esteganografía

La esteganografía es una rama la cual se basa en criterios de seguridad para camuflar información, como:

> Medio, Invisibilidad (Imperceptibilidad), Robustez, Capacidad de embebido, Usabilidad, Seguridad.

Tipos de Esteganografía

"Podemos tomar una clara definición de lo que es la esteganografía "La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos dentro de otros, llamados portadores, de modo que no se perciba su existencia."." (Esteganografía, 2017)

De acuerdo a la pasar de los años la esteganografía se clasifica en:

Esteganografía Clásica

Esteganografía Moderna

Esteganografía avanzada

Esteganografía y sus aplicaciones modernas

Entre los distintos usos que puede llegar a tener la tecnología cabe recalcar que el propósito siempre será el de ayudar a las personas para poder agilizar las tareas cotidianas, mediante la construcción de programas, sitios web, aplicaciones, software, etc. Existen un sinfín de herramientas en el mercado que pueden agilizar nuestras tareas cotidianas, pero con el surgimiento de las tecnologías, también surgieron personas inescrupulosas que se aprovechan de algunas vulnerabilidades que hay dentro de la tecnología, y sacan provecho de dicha vulnerabilidad. (Villa, 2015)

"Entre los programas y aplicaciones, el objeto más preciado ya no es lo físico como casas o autos, ahora con la llegada de la tecnología nuestra información personal se ha convertido en una mina de oro, el cual puede ser utilizado para hechos delictivos. Muchas de las herramientas

tienden a vulnerar nuestros datos, las aplicaciones que piden acceso a nuestra información personal para poder ser más personalizadas.” (Villa, 2015)

Diferencia entre esteganografía y criptografía

“El objetivo de este módulo es estudiar las diferentes disciplinas y técnicas que pueden plantear problemas durante la investigación en informática forense y pericial, como son la esteganografía, para la ocultación de la información, la criptografía, como proceso de codificación o de cifrado para mantener en secreto datos e informaciones y otras técnicas denominadas anti forenses, por ejemplo, para la limpieza u ofuscación de la información:

La esteganografía estudia y aplica técnicas para la ocultación de información, mensajes u objetos, dentro de otros, llamados portadores, de modo que no sea fácil percibir su existencia.” (Esteganografía, 2010)

Por otra parte, la criptografía tiene por objetivo mantener en secreto datos, informaciones, mensajes, etc. durante su almacenamiento o su transmisión.

Técnicas esteganografías

Normalmente se conoce que por lo general se oculta información en imágenes, pero existen muchas más técnicas de esteganografía como son:

Esteganografía pura

Esteganografía de clave secreta

Esteganografía en texto

Esteganografía en sistemas operativos y ficheros

Esteganografía en formato de ficheros

Esteganografía hardware

Esteganografía en tecnologías web

Esteganografía en protocolos de comunicación

Esteganografía en contenido multimedia

Esteganografía en imágenes

Se han presentado varias técnicas para la esteganografía de texto árabe en la literatura académica existente (Hakak et al., 2019). Estos estudios previos se pueden clasificar según las características del idioma árabe que utilizaron en su técnica de esteganografía, incluidos caracteres adicionales, signos diacríticos, Unicode, bordes afilados y letras puntiagudas (Khan, 2014).

(Shahreza y Shahreza, 2006) sugirió un enfoque para ocultar mensajes secretos en texto árabe mediante el uso de caracteres puntiagudos. En su trabajo, los bits secretos (la versión binaria de un mensaje secreto) se procesaban uno a uno. Si el bit es "1", el punto se desplaza ligeramente hacia arriba, mientras que nada más cambia si el bit es "0". Sin embargo, la capacidad de este método es muy baja y está limitada en cuanto a su solidez, ya que los mensajes secretos ocultos se perderían después de volver a escribirlos o cambiar la fuente.

Gutub y Fattani (2007) abordaron las limitaciones en el trabajo de Shahreza y Shahreza (2006) al insertar Kashida antes o después de letras puntiagudas y no puntiagudas, en lugar de solo letras puntiagudas. Este desarrollo eliminó el riesgo de perder datos secretos por cambios de fuente. Además, esta técnica mejoró la seguridad del texto, ya que se pueden agregar

múltiples Kashida antes o después de un carácter dentro del mismo documento o párrafo sin llamar la atención. Sin embargo, este método sufría de baja capacidad ya que no todos los caracteres tienen puntos (Gutub y Alaseri, 2019a). Por lo tanto, cuando un bit secreto era 1, era necesario anular muchas palabras en la oración para buscar un carácter puntiagudo donde se pudiera insertar Kashida.

Alhusban (2017) también desarrolló una técnica para ocultar partes secretas insertando Kashida entre letras puntiagudas o no puntiagudas. Este proceso de incrustación se basó en dos tablas, cada una de las cuales define cómo se debe agregar Kashida en cuatro permutaciones posibles de pares de bits secretos (00, 01, 10, 11). La primera mitad de las palabras en el texto de la portada siguieron las reglas definidas en la primera tabla y la segunda mitad de las palabras siguieron las reglas definidas en la segunda tabla. Esta técnica se basaba en la inserción de Kashida entre caracteres conectados para ocultar fragmentos secretos, lo que significa que no se utilizaron muchos caracteres no conectados, como caracteres aislados y espacios en blanco. Además, se anularon muchos caracteres cuando las letras no coincidían con el caso del Kashida insertado, que representaba dos bits. Como resultado, la capacidad de este método no alcanzó el 2%.

Tipos de antivirus

Los Antivirus preventivos se caracterizan porque analizan la entrada y salida de todos los datos en tu ordenador con la finalidad de interceptar posibles amenazas, anticipándose a la infección del equipo por parte de programas maliciosos. Están instalados en la memoria interna del ordenador y en ocasiones pueden llegar a ralentizar el funcionamiento del mismo.

Los antivirus identificadores son como su propio nombre indica, son antivirus que exploran el sistema operativo de tu ordenador con la finalidad de identificar posibles virus existentes en el mismo. Rastrean secuencias de bytes de códigos específicos e intentan identificar comportamientos extraños o patrones fuera dentro de lo común dentro de los programas existentes.

Los Antivirus descontaminadores son cuando el virus ya se encuentra identificado en nuestro ordenador, el antivirus de tipo descontaminador se encarga de eliminar esta infección. Tiene algunas funciones similares a los antivirus identificadores.

Tipos de antivirus según su objetivo específico

No todos los antivirus están diseñados para contraatacar un mismo tipo de virus, por ello es importante que identifiques los tipos de antivirus que existen según su objetivo específico:

Firewall o cortafuegos

El firewall (cortafuegos en español) controla la entrada y la salida de datos de tu ordenador y bloquea «como un muro» toda aquella actividad que le resulte dudosa. Actúa de forma preventiva. Actualmente podemos identificar 3 tipos de firewall distintos: los servidores proxy, los filtros de capa de red (o de paquete) y los cortafuegos de capa de aplicación.

Antipop-up

Este es un antivirus muy simple que se encarga únicamente de evitar que algunas webs abran de forma automática ventajas emergentes que puedan resultar molestas al navegar por Internet.

Antispyware o antiespías

Este antivirus tiene el objetivo de detectar y eliminar programas espías que se hayan instalado en nuestro equipo sin nuestro consentimiento. La finalidad de estos programas espías maliciosos y silenciosos es recabar información sobre el usuario (contraseñas, hábitos de navegación, etc.) para pasarla de forma ilegal a terceros.

Antispam

Su objetivo específico es el que identificar emails de dudosa procedencia y mandarlos directamente a la bandeja de spam. Prácticamente todos los proveedores de servicios de correo electrónico, como son Gmail, Hotmail, Yahoo! etc. cuentan con sus propios sistemas Antispam.

Antimalware

Los antimalware están diseñados para analizar, detectar, prevenir y eliminar software malicioso en nuestros equipos, es decir, malware. No es una simple herramienta (como sí puede serlo un antipop-up), sino que es un programa más completo que normalmente ya incorpora varias de las funciones de los antivirus mencionados en esta lista.

Antivirus online y antivirus offline

Todos aquellos antivirus que no necesitan ser instalados en tu equipo, sino que actúan únicamente a través de Internet se clasifican como antivirus online. Si no requieren Internet para ser ejecutables, son antivirus offline.

Antivirus pasivo y antivirus activo

Si el antivirus sólo actúa cuando el usuario lo solicita, entonces hablamos de un antivirus de tipo pasivo. Por el contrario, si el antivirus actúa de forma autónoma sin necesidad de que el usuario le dé una orden específica, entonces hablamos de un antivirus de tipo activo.

Tipos de antivirus según la marca

Existen múltiples marcas de antivirus para ordenador, pero como no podemos mostrártelos todos, a continuación mencionamos los 15 mejores antivirus por marcas:

Tabla 1: Antivirus

Kaspersky (Recomendado por Incuatro)		ESET(recomendado por incuatro**)**	Norton	AVG
PC Tools		BitDefender	Avast	McAfee
Panda		Webroot	Trend Micro	BullGuard
Avira		Sophos	Fortinet	

Marco teórico

La esteganografía de red se centra en el transporte de información que se da en la Comunicación entre el emisor y el receptor, su objetivo principal es ocultar la información en Canales encubiertos de un protocolo de red, estos canales son campos de la cabecera del Protocolo que no son utilizados o que al insertar datos no afectan su funcionalidad, la Información pasa desapercibida ante terceras personas, esta información puede ser Mensajes textuales, datos, comandos o alguna señal que tenga significado para el receptor. (Solano Solano, 2018).

La evolución en las redes de computadoras en los últimos años ha ocasionado el desarrollo de nuevos servicios, pero también de manera simultánea han surgido nuevas amenazas para los sistemas que se encuentran interconectados. Un canal de comunicación es el medio que se utiliza para transmitir un mensaje de un emisor hacia un receptor. Los canales encubiertos también llamados covert channel son una manera de crear una comunicación oculta que puede vulnerar la integridad de un sistema; dicho concepto fue introducido por primera vez en el año de 1973 por Lampson. La definición de Lampson, describe un canal encubierto como uno que se utiliza para la transmisión de información, pero que no está diseñado ni destinado para las comunicaciones. (Lampson, 1973).

En los últimos años, los rápidos desarrollos de Internet, las tecnologías de comunicación digital y los multimedia han permitido a los usuarios transferir datos digitales de manera eficiente a través de redes mundiales. Como resultado, proteger los datos confidenciales de estas personas, en particular cuando esos datos se transmiten a través de una red abierta, se ha vuelto más desafiante. Numerosos investigadores y organizaciones se han esforzado por encontrar métodos de seguridad que puedan proteger los datos secretos para que no sean detectados

durante la transmisión, incluida la criptografía, la marca de agua y la esteganografía (Mohamed, 2014).

Un ejemplo claro y más actualizado se dio a conocer por la BBC que observó como usaban un emoji de una zanahoria el cual traía un código secreto en internet para camuflar contenido anti vacunas, BBC ha observado varios grupos, entre ellos uno con cientos de miles de miembros, en los que aparece este emoji naranja en lugar de la palabra "vacuna". Los algoritmos de Facebook tienden a enfocarse en palabras en lugar de imágenes. En este tipo de grupos se comparten informaciones no verificadas de personas que supuestamente han sufrido daños o han muerto por las vacunas.

Otro ejemplo se ha descubierto una campaña contra usuarios de Windows, desde BleepingComputer, se ha descubierto una campaña por parte del grupo de hackers 'Witchetty', utiliza el logo de Windows para ocultar un malware de puerta trasera. La empresa de seguridad Symantec ha descubierto este nuevo ataque de ciberespionaje lanzado en febrero de 2022 fue dirigida a dos gobiernos en Oriente Medio y África. Según Bleeping computer “el ataque comienza cuando los actores de amenazas obtienen acceso inicial a una red al explotar Microsoft Exchange ProxyShell (CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207) y ProxyLogon (CVE-2021-26855 y CVE- 2021-27065) cadenas de ataque para colocar webshells en servidores vulnerables.” Cuando consiguen acceso pueden abrir archivos y directorios, iniciar o cerrar procesos, modificar el registro de Windows, descargar archivos y mucho más. Todo a través de un proxy que les permite utilizar cualquier equipo infectado de forma remota.

El uso de la esteganografía de red permite desarrollar aplicaciones esteganográficas sutiles que sean capaz de poder establecer canales de comunicación encubiertos sobre el conjunto de protocolos TCP/IP.

Clasificación de canales encubiertos

Los canales encubiertos pueden clasificarse de acuerdo al mecanismo de ocultación en:

Canales encubiertos de almacenamiento

Son aquellos canales en los que el proceso de la comunicación secreta entre el emisor y el receptor se lleva a cabo alterando el valor de las variables de un recurso compartido o un atributo almacenado o transmitido. Como ejemplo de este tipo de canales se tiene: la alteración en ciertos campos que no son utilizados en la cabecera de un protocolo de comunicación, o la modificación de los colores que componen a cada uno de los píxeles de una imagen en un archivo.

Canales encubiertos de temporización

Son aquellos canales en los que el proceso de la comunicación secreta entre el emisor y el receptor se lleva a cabo modificando el período de tiempo de ejecución de un determinado proceso o tarea. Como ejemplo de este tipo de canales se tiene: el tiempo de uso de la unidad central de proceso (CPU) o el tiempo de comienzo de un proceso.

Características de los canales encubiertos

Los canales encubiertos presentan ciertas características los cuales son: Por su Capacidad la cual es la cantidad de información que puede ser transmitida a través del canal, por Ruido la cual es la cantidad de perturbaciones que pueden interferir con la información mientras es transmitida a través del canal, por Modo de transmisión el cual puede ser síncrona, donde la transferencia de información es controlada por una señal de reloj, de otro modo es asíncrona. La capacidad es una parte muy importante de la calidad global de un canal. Desde el punto de vista de seguridad, un canal de mayor capacidad hará posible que más información se filtre.

Condiciones para canales encubiertos: Existen algunas condiciones que deben cumplirse para que sea posible la existencia de canales encubiertos: Potencial para la comunicación el cual se requiere al hecho de que entre el emisor y el receptor se pueda efectuar una comunicación, restricción sobre la comunicación la cual no está permitida una comunicación entre el emisor y el receptor en circunstancias normales debido a la política de Seguridad, existencia de una variable o recurso compartido esto debe haber algún recurso compartido de manera general dentro del sistema de comunicación entre emisor y el receptor, acceso pleno sobre la variable o recurso compartido en un recurso compartido debe ser visible ante el remitente y el receptor. También el remitente debe ser capaz de alterar el recurso de alguna manera, y el receptor debe ser capaz de notar dicho cambio, la capacidad para sincronizar donde el emisor y el receptor deben ser capaces de sincronizar sus operaciones a fin de que la transmisión tenga lugar, la entidad llamada cámara de comercio de Barrancabermeja: Las Cámaras de Comercio en Colombia son organizaciones privadas de carácter gremial y sin ánimo de lucro, que cumplen por delegación legal algunas funciones públicas, como la administración de los registros públicos. En otras palabras, una Cámara de Comercio representa un grupo de empresas y comerciantes de una región, que colaboran organizadamente.

Tabla 2: Características y funciones de la entidad

Características	Funciones
Promueven la competitividad y la formalización, impulsan el desarrollo de las regiones, sirven como órgano de consulta en	Las Cámaras de Comercio ejercen las funciones señaladas en el artículo 86 del Código de Comercio, y en las demás normas legales y reglamentarias. Las cuales se citan a

temas económicos e información comercial de los registros.

Adicionalmente, las Cámaras de Comercio promueven y mantienen la libertad de empresa necesaria, para mantener el crecimiento y progreso del país. En Colombia, existe una red de 57 Cámaras de Comercio, trabajando agremiadas, a través de Confecámaras, que liberan iniciativas para el fortalecimiento de las empresas y para el desarrollo de las comunidades en todo el territorio nacional.

continuación: (Art. 4 Decreto 2042/2014 – reglamentario de la Ley 1727 de 2014)

Servir de órgano consultivo del Gobierno nacional y, en consecuencia, estudiar los asuntos que este someta a su consideración y rendir los informes que le soliciten sobre la industria, el comercio y demás ramas relacionadas con sus actividades.

Adelantar, elaborar y promover investigaciones y estudios jurídicos, financieros, estadísticos y socioeconómicos, sobre temas de interés regional y general, que contribuyan al desarrollo de la comunidad y de la región donde operan. Administración de los registros públicos delegados. Actuación como órgano consultivo ante el Gobierno. Elaboración de estudios de interés general para el desarrollo de la comunidad. Certificación de la costumbre mercantil. Arbitraje, conciliación y amigable composición. Participación en exposiciones y recintos feriales. Ferias y

	exposiciones. Promoción de la formalización y capacitación. Información comercial con datos de otras fuentes. Información comercial de los registros.

Tabla 2: Características vs Funciones de la Cámaras de Comercio.

Las Cámaras han asumido por encargo del Gobierno Nacional, la administración del Registro Público Mercantil de las empresas y entidades sin ánimo de lucro, como también, de proponentes y otros registros.

Con lo anterior, quiere decir que las Cámaras asesoran a empresarios y comerciantes a formalizarse, y los acompañan a cumplir con todos los requisitos legales para que puedan operar con toda tranquilidad y con su información protegida.

Esto les permite tanto a los pequeños como grandes negocios ser más visibles y generar empleo de calidad. Además de tener estos beneficios por estar formalizadas, las empresas que renuevan cumplidamente su registro cada año, pueden beneficiarse de diferentes servicios de fortalecimiento y asesoría, para hacerse más competitivas.(https://www.ccbarranca.org.co/ccbar/)

Utiliza una Infraestructura tecnológica asociada a la red de información comercial AICO, cuyo objetivo es fomentar el intercambio de información comercial con el fin de incrementar el comercio entre los países miembros de la Asociación. Debido a la gran disparidad tecnológica en los países Latinoamericanos y del Caribe y en las entidades mismas. Se hace necesario conocer su capacidad de procesamiento informático y de telecomunicaciones para determinar el tipo de estrategia que se utilizará para la conexión a la red de cada uno de ellos.

Figura 1: Imagen frontal Edificio de la Cámara de comercio de Barrancabermeja 1

Tomada de: (google maps, 2022)

Tabla 3: Comparación con otras ciudades

Barrancabermeja	**Bogotá (sede principal)**
La cámara de comercio de Barrancabermeja, cuenta en sus instalaciones con 60 equipos de cómputo de los cuales la información contenida allí, es protegida mediante la utilización del antivirus ESET NOD32. Cabe resaltar que la base de datos de la cámara de comercio de Barrancabermeja	La cámara de comercio de Bogotá, como sede principal de Colombia cuenta en sus instalaciones con 840 equipos de cómputo, tiene implementada una política de seguridad de la información el cual responsabiliza a la Coordinación de Planeación e Innovación – Seguridad de

tiene como sede la ciudad de Bogotá. Es por esto que en Barrancabermeja para proteger los documentos inmediatos se utiliza este antivirus empresarial.	la Información de la Cámara de Comercio de Bogotá velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos,
Todos los funcionarios de la Cámara de Comercio de Barrancabermeja son responsables del manejo de la información en condiciones de seguridad, el cumplimiento de las políticas y de los controles implementados por la organización, así como de detectar las oportunidades de mejora, reportar incidentes de seguridad e implementar las acciones correctivas o preventivas a que haya lugar, para asegurar un proceso permanente de mejora en la Gestión de la Seguridad de la Información.	procedimientos, instructivos y formatos específicos alineados al estándar internacional ISO 27001 y sus normas derivadas además de los otros marcos generalmente aceptados como: COBIT, ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la Regulación Vigente.

Tabla 2: Comparación Cámara de comercio de Barrancabermeja con la cámara de Comercio sede principal.

Concientización a funcionarios: Este trabajo tiene como objetivo principal identificar técnicas existentes de esteganografía que están afectando la seguridad de la información de los usuarios de la cámara de comercio de Barrancabermeja por ello una vez identificado estas técnicas debe ser socializadas con todos los funcionarios de esta empresa ya que son responsables del manejo de la información en condiciones de seguridad, ya que no hay técnica

más eficaz que el entendimiento de lo que podría llegar a ser un problema si no se toman medidas con anterioridad.

Figura 2:

Capacitación a los funcionarios en las instalaciones de la cámara de comercio de Barrancabermeja 2.

Fuente: (moreno, 2022)

Figura 3

Capacitación a los funcionarios en las instalaciones de la cámara de comercio de Barrancabermeja 3.

Fuente: (moreno, 2022)

Figura 4

Capacitación a los funcionarios en las instalaciones de la cámara de comercio de Barrancabermeja 4.

Fuente: (moreno, 2022)

Antivirus: Eset nod32

Figura 5

Portada producto para la venta del antivirus

Fuente: (antivirus eset, 2022)

Figura 6

Comparación evaluación de características entre antivirus en el mercado

Producto Antivirus	Evaluaciones aprobadas
ESET NOD32	**61**
Symantec Antivirus	53
Kaspersky Antivirus	49
Sophos	49
Norman Security Suite	41
McAfee VirusScan	41
F-Secure	37
Alwil Avast!	35
FRISK F-Prot	26
BitDefender	21
Trend Micro	16
Microsoft Security Essentials	1
Panda	1

Fuente: (antivirus eset, 2022)

Además, ESET NOD32 Antivirus tiene las certificaciones de CheckMark sobre Anti-Spyware Desktop y Anti-Spyware Installed, las cuales garantizan la eficacia de la solución en ofrecer una total protección ante este tipo de malware.

Figura 7

Propaganda de venta del antivirus Eset por sus características

Fuente: (eset antivirus, 2022)

Figura 8

Firmware desde la BIOS

Fuente: (hard zone, 2022)

Un claro ejemplo de lo que es un firmware avanzado es la BIOS/UEFI de nuestras placas base. Gracias a ellas, la placa puede hacer funcionar nuestro PC, pero también gracias a ella, podemos configurar muchos aspectos de nuestros sistemas de manera diferente a lo que sería la configuración de serie del mismo.

Figura 9

Actualización del sistema operativo en proceso

Fuente: (hard zone, 2022)

Se debe hacer la debida actualización de este pero no antes de la actualización del sistema operativo ya que si se realiza antes no podrá decir si el software nuevo viene contaminado.

La diferencia principal entre un driver y el firmware es que el primero se ejecuta en el PC mientras que el segundo lo hace en el propio hardware de manera directa. El firmware además puede trabajar de manera conjunta con el driver, pasando parámetros importantes para el correcto funcionamiento y la seguridad del dispositivo o componente en cuestión.

Comparación con otros antivirus: En el mercado comercial informático de hoy en día existe una gran competencia de confiabilidad en cuestión de brindar seguridad a la información y entre estos tenemos los antivirus Eset y Kaspersky. Kaspersky tuvo un impacto mayor en la utilización de la CPU cuando no se realizó ningún análisis al 46%, en comparación con ESET, que fue del 32%. Las otras pruebas mostraron que ESET usó menos recursos que Kaspersky, lo que significa que el impacto en mi PC fue menor que el de Kaspersky. ESET NOD32 es el único

antivirus que combina cuatro características imprescindibles para la protección antimalware de hoy en día: velocidad de exploración, bajo impacto, eficiencia y eficacia en la detección de amenazas conocidas y rapidez en el reconocimiento de códigos maliciosos desconocidos. Su principal característica es la protección proactiva multicapa que detecta y neutraliza todas las amenazas digitales, incluidos virus, ransomware, rootkits (acceso y control remoto), gusanos y programas espía. También protege contra técnicas que buscan evadir la detección y bloquea ataques y exploits dirigidos.

Otro ejemplo de comparación es entre ESET NOD32 y el Smart Security, el cual si el equipo no cuenta con antispam ni con firewall, y además se encuentra expuesto al riesgo de pérdida física o robo, la suite de seguridad ESET Smart Security tiene mayores características anteriormente nombradas.

La cámara de comercio de Barrancabermeja utiliza antivirus como protección el antivirus ESET ya que es uno de los motores antimalware más seguros del mercado actual, y ofrece varias herramientas antivirus potentes para evitar que sus usuarios sean hackeados. Su escáner de virus utiliza la heurística avanzada y el aprendizaje automático para detectar el malware cifrado y las amenazas de día cero.

Seguridad en redes NGN y Esteganografía: La Esteganografía de protocolos utiliza ciertas características de algún protocolo de red para ocultar información, haciendo uso de canales encubiertos que son canales de comunicación que puede ser explotado por un proceso de transferencia de información de manera que viola la política de seguridad de un sistema. Esta investigación realiza un estudio sobre la esteganografía como medio para proteger la información, también se hace un análisis sobre la esteganografía de protocolos así como sobre las diferentes técnicas para explotarlos.

Medios que facilitan y mejoran los canales de envío de información; estos canales serían las Redes de nueva generación NGN definidas por el Grupo de Estudio 13 del Sector de Normalización de la Unión Internacional de Telecomunicaciones (UIT –T) en la Recomendación Y.2001 “Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS (Quality of Service), y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Por ello existen diversos métodos para crear canales encubiertos sobre TCP (Protocolo de Control de Transmisión)/IP (dirección del Protocolo de Internet), por ello la esteganografía sobre protocolos de red tiene diversas opciones y accesos poder ocultar información de manera que pase desapercibida ante la presencia de terceras personas. Aunque el uso de técnicas esteganográficas para proteger la información ha ido aumentando debido a los grandes beneficios que ofrece.

La esteganografía en protocolos de red se conoce también como esteganografía de red, la cual se dedica a ocultar la información haciendo uso de ciertas características de los protocolos de red. La esteganografía de red hace uso de canales encubiertos para transferir información, un canal encubierto se puede definir como un canal que cumple otros propósitos para los que no fue hecho, en este caso, enviar información de manera secreta. Por otra parte los ADS, son una característica particular del Sistema de Archivos de Nueva Tecnología (NTFS por sus siglas en inglés, New Technology File System), y son considerados un método para ocultar información. “GABRIELA HERNÁNDEZ LÓPEZ”

Sistemas de seguridad existentes más usados necesarios para proteger la información de las Redes NGN: Las tecnologías relacionadas con Internet están cambiando con el paso del tiempo, es decir, que las tecnologías se están volviendo avanzadas. La red convergente es una

infraestructura de red donde la comunicación de datos, voz y video se puede transmitir a través de la misma red. Según el concepto de red convergente no es nuevo. Este concepto se introdujo en la década de 1980 cuando la Red Digital de Servicios Integrados (RDSI) estaba en etapas de desarrollo. Pero cuando se implementó la RDSI, no fue fácil hacerlo como se decía para transmitir voz con datos en las redes telefónicas existentes. También describe la migración de la red existente hacia Convergencia que había una necesidad de que la voz también se enviara con paquetes de datos. Así fue posible, IP fue la plataforma para este propósito. VoIP se adoptó para transferir paquetes de voz y datos en Internet. Las redes convergentes proporcionan transferencia de datos a altas velocidades pero con una seguridad perfecta. La técnica de entrega de paquetes para Internet es el Protocolo de Internet (IP). Según IP solo fue diseñado para el transporte de datos, no de voz. IP depende del Protocolo de control de transmisión (TCP) para mejorar su confiabilidad.

Se discuten tres puntos de vista para la convergencia: convergencia de servicios de usuario, convergencia de dispositivos y convergencia de redes. En la convergencia de servicios de usuario, se pueden proporcionar diferentes servicios a través de diferentes redes a los mismos usuarios y a diferentes dispositivos. Mientras que en la convergencia de dispositivos, los dispositivos comunes admiten varios tipos de acceso. Por último, la convergencia de la red se refiere a proporcionar diferentes servicios a los usuarios, a varios tipos de acceso, teniendo en cuenta la rentabilidad y la calidad del servicio. El Protocolo de Internet (IP) se está introduciendo en las áreas de comunicación. El desarrollo de la tecnología conduce al aumento del ancho de banda y apoya la movilidad que permite verdaderos servicios convergentes. El desafío revisado aquí está relacionado con el entorno empresarial. Algunos aspectos de la convergencia podrían afectar los planes comerciales del operador de la red. Los operadores de red tendrán la capacidad

de adoptar rápidamente el nuevo entorno. Aquí la vista de red convergente se describe de otra manera.

Tradicionalmente, las soluciones de seguridad podían implementarse fácilmente después de diseñar e implementar una red porque todo lo que se necesitaba era asegurar perímetros fijos y monitorear el tráfico predecible y los flujos de trabajo que se movían entre servidores de red estáticos y dispositivos externos conocidos. Pero las nuevas demandas han ejercido una presión cada vez mayor sobre este modelo. Hoy en día, todos los componentes de la red, independientemente de su distribución, deben funcionar como un único sistema integrado. Y al mismo tiempo, la mayoría de esos elementos también deben verse como un discreto. A la red Como resultado, la interoperabilidad entre los elementos de la red dinámica es esencial. Pero también lo es proteger las transacciones, las aplicaciones y los flujos de trabajo que se mueven de cualquier lugar a cualquier lugar. Entonces, lo que debe suceder a nivel de la red es que la conectividad y la funcionalidad de la red deben combinarse perfectamente con la seguridad. De esa manera, cuando los datos se mueven de un lugar a otro, a través y entre dispositivos que están en constante movimiento, deben integrarse con la inspección, el cifrado y la aplicación de políticas que son igual de ágiles.

Debido a que las redes ahora tienen muchos bordes, es imposible crear el tipo de límite defendible único que la mayoría de las herramientas de seguridad heredadas fueron diseñadas para defender. En cambio, las aplicaciones y los flujos de trabajo ahora pueden abarcar múltiples entornos en una sola transacción, lo que significa que la seguridad debe aplicarse de manera consistente en los bordes de la LAN, WAN , la nube y los usuarios remotos . Y las conexiones dinámicas entre estos entornos también deben ser confiables y seguras. Independientemente del dispositivo que se utilice, cualquier usuario de cualquier perímetro debe poder conectarse de

forma segura a cualquier otro perímetro o conjunto de perímetros en cualquier momento y desde cualquier ubicación.

Para asegurar una red convergente, se analizan algunas medidas de seguridad. El primero es proteger la infraestructura empresarial, el segundo proteger las aplicaciones de comunicación de las redes convergentes y el tercero asegurar los servicios y el acceso de mantenimiento. La limitación aquí es que se han tomado todas las medidas para proteger la red convergente, pero aún no pueden proporcionar servicios de seguridad y aún son vulnerables a las amenazas. Algunos son contramedidas y algunos todavía están allí como ataque DDoS. Algunas medidas a tomar frente a este tipo de ataques son:

Analizar las amenazas de seguridad a las redes inalámbricas y se ha realizado el análisis de las amenazas según el nivel de riesgos a WiMAX/802.16. Se describen las amenazas a la capa Mac y la capa física de WiMAX. Los protocolos inalámbricos robustos con técnicas de encriptación sólidas junto con el uso de sistemas de prevención de intrusiones son efectivos para eliminar muchas amenazas inalámbricas. La capa física de WiMAX es vulnerable a las amenazas en comparación con la capa MAC. Los ataques a la capa física son interferencias y codificación.

Los protocolos inalámbricos robustos con técnicas de encriptación sólidas junto con el uso de sistemas de prevención de intrusiones son efectivos para eliminar muchas amenazas inalámbricas. La capa física de WiMAX es vulnerable a las amenazas en comparación con la capa MAC. Los ataques a la capa física son interferencias y codificación.

El enfoque principal está en el análisis de amenazas de las dos capas; Capa física y capa MAC en detalle.

No había protección para la integridad del tráfico de datos de 802.16, pero 802.16e introduce este tipo de mecanismo de protección para la protección de datos. Se ha discutido la autenticación de los mensajes de tráfico. La modificación de mensajes es posible cuando no se utiliza AES, y la modificación del tráfico se convierte en una amenaza importante.

Las amenazas a la seguridad de la red convergente son simplemente similares a las de la infraestructura de la red WiMAX. WiMAX está diseñado con una gran cantidad de mecanismos de seguridad para hacerlo seguro frente a las amenazas, pero aún no tan seguro frente a las amenazas.

QoS en SDN: SDN desacopla las funciones de control y reenvío de datos. El plano de control programable permite la aplicación de políticas utilizando un controlador SDN centralizado. El plano de gestión consta de un programa de aplicación. El plano de datos consta de elementos de reenvío, como conmutadores de software, como Open VSwitch (OVS). Un OVS puede configurarse dinámicamente actualizando las reglas de enrutamiento a través de algoritmos de enrutamiento reactivos, proactivos o híbridos. OpenFlow API se usa comúnmente como protocolo de comunicación

SDN que utiliza OpenFlow permite el control de calidad por flujo de una manera más flexible y granular. OpenFlow 1.0 implementa QoS por flujo mediante el uso de la acción opcional "poner en cola". Reenvía los paquetes coincidentes entrantes de un flujo a través de una cola predefinida adjunta a un puerto específico de un conmutador. Un conmutador puede tener varias colas y el controlador OpenFlow puede recuperar su información.

Seguridad de WiMAX y redes convergentes: Ha habido una gran evolución en las comunicaciones inalámbricas en los últimos años. WiMAX es una tecnología inalámbrica emergente que se utiliza para implementar una red de área metropolitana inalámbrica de banda ancha (WMAN). WiMAX es una tecnología inalámbrica que ofrece muchas características con mucha flexibilidad. WiMAX ha reemplazado muchas de las tecnologías de telecomunicaciones existentes y brinda conectividad de última milla con mayor velocidad a distancias más largas, de 0 a 50 millas y su tasa de transferencia es de hasta 70 Mbps.

Principalmente, las amenazas en WiMAX son para la capa física y la capa MAC. Pero la capa física es mucho más vulnerable a las amenazas en comparación con la capa MAC. La capa física (PHY) maneja la conectividad de la señal, la corrección de errores, el rango inicial, el registro, las solicitudes de ancho de banda y los canales de conexión para la gestión y los datos. La capa MAC gestiona las conexiones y la seguridad.

Para una gestión eficiente de los recursos de la red, los operadores inalámbricos deben conocer la calidad de servicio (QoS) de un servicio ofrecido, la duración del uso del servicio y la tasa de flujo aplicable. El servicio de aplicación se asigna a un portador de que tiene en cuenta sus requisitos de QoS. Si la red no tiene información sobre el tipo de aplicación, se puede crear un portador predeterminado para el flujo de tráfico. Sin embargo, es posible que el portador predeterminado no satisfaga los requisitos de QoS de un servicio de aplicación. Un usuario puede experimentar un servicio degradado debido a un aumento en la pérdida y demora de paquetes, así como a una velocidad de datos reducida. Además, cuando hay una falta de recursos en la red, los servicios de alta prioridad pueden liberarse, mientras que los servicios de baja prioridad pueden no liberarse. Por lo tanto, es necesario identificar el tipo de servicio para un aprovisionamiento de QoS eficiente.

Para obtener información sobre el tipo de servicio, se han utilizado convencionalmente la inspección profunda de paquetes, los métodos basados en firmas y los métodos basados en puertos, Sin embargo, es posible que los métodos convencionales no funcionen cuando los desarrolladores de aplicaciones utilizan puertos dinámicos para los servicios o cuando los proveedores de red utilizan la traducción de direcciones de red. El problema se vuelve más grave cuando los paquetes en el tráfico de red están encriptados. Además, con el aumento de los números y tipos de aplicaciones, se requieren nuevos métodos y protocolos.

DNS: cuando se creó el DNS, nadie esperaba que se convertiría en la base de la economía digital y en un objetivo principal para los ciberdelincuentes. Y nadie esperaba que uno de los principales activos de la economía digital fueran los hábitos de navegación de los usuarios, poniendo en riesgo su privacidad. El DNS se diseñó e implementó de acuerdo con criterios de velocidad, escalabilidad y confiabilidad, mientras que la seguridad y la privacidad no entraban en los objetivos. Aunque los primeros ataques ya se concibieron hace unos treinta años, la infraestructura DNS, con un montón de mejoras pero con su diseño original, sigue desempeñando un papel fundamental para permitir el acceso a servicios, datos y dispositivos. Y, a pesar de la adopción bastante generalizada de extensiones de seguridad de DNSSEC en los últimos años, los ataques de DNS son cada vez más frecuentes, sofisticados y peligrosos. Son globales, variados, dinámicos y pueden eludir los sistemas de seguridad tradicionales, como los firewalls de próxima generación y los sistemas de prevención de pérdida de datos. Se ha propuesto una revisión de los supuestos del DNS de formas muy diferentes, reflejando diversos puntos de vista en términos de gobernanza de Internet y libertad del usuario, y los organismos de estandarización, los consorcios de la industria y la investigación académica están realizando un gran esfuerzo para converger hacia un diseño actualizado. e implementación.

En los últimos diez años ha habido un creciente interés y un cuerpo de trabajo relacionado con las actualizaciones de la arquitectura del Sistema de nombres de dominio (DNS), a fin de cumplir con los requisitos de seguridad y privacidad de los paradigmas informáticos modernos y los casos de uso. La atención prestada al DNS desde una perspectiva de seguridad cibernética es triple.

En primer lugar, se justifica por el hecho de que un direccionamiento DNS correcto suele ser un requisito previo para acceder a servicios cruciales de Internet (p. ej., servicios financieros y en la nube), datos confidenciales (p. ej., información personal, secretos comerciales) y dispositivos críticos (p. ej., sensores y actuadores que permiten servicios inteligentes, laboratorio portátil en chips para información de diagnóstico personal). Los problemas que plantea el DNS en relación al acceso a servicios digitales e información sensible se han magnificado con la llegada de la pandemia del COVID-9, debido al recurso masivo al funcionamiento. Los remotos hacen uso de la infraestructura de sus proveedores de servicios (ISP) para volver a conectarse al sistema de TI de su organización y consumir servicios y aplicaciones SaaS o en la nube. Desde el punto de vista de una organización, la infraestructura DNS del ISP no es fácil de controlar ni de confiar; por otro lado, la alternativa de confiar en un servicio de DNS público centralizado propiedad de uno de los gigantes de Internet puede ser riesgosa con respecto a la privacidad de los datos.

En segundo lugar, se deriva precisamente de las amenazas que se plantean a la privacidad de las personas y las organizaciones. En la última década se han producido varios episodios de violaciones de la privacidad de los ciudadanos tanto por parte de empresas con fines comerciales, como por parte de agencias de inteligencia por motivos políticos y estratégicos. En particular, ha habido algunos ejemplos sensacionales de actividades de vigilancia y creación de perfiles a gran

escala relacionadas con el abuso del DNS, como los relacionados con el caso Snowden y la corporación minorista estadounidense Target, que han sensibilizado fuertemente a la opinión pública en todo el mundo.

En tercer lugar, existe una creciente preocupación por el mal uso de la infraestructura y el protocolo DNS, especialmente por medio de malware. De hecho, los atacantes, cada vez más gracias al uso de software malicioso, están distorsionando el propósito para el que se diseñó el DNS, utilizándolo como vector de ataque contra otros recursos y servicios. Las técnicas como la tunelización de datos, la amplificación del ancho de banda y los nombres generados algorítmicamente se aplican cada vez con más éxito al protocolo DNS y se implementan a través de infraestructuras DNS, por lo que para ocultar las verdaderas identidades de red de los nodos que pertenecen a las redes de boots, obtenga una comunicación sigilosa con el comando y así controlar servidores botnet, propagar malware o realizar ataques de denegación de servicio (DoS) y otros tipos de ataques contra servicios y sistemas fuera del DNS.

Conclusiones

Para utilizar las técnicas de la esteganografía se necesita simplemente de un medio de transmisión que contenga muchos bits para que el cambio de alguno de ellos no altere significativamente el archivo original y pueda transmitir el mensaje oculto sin que sea percibido. El ocultamiento de información utilizando las técnicas de la esteganografía sigue siendo confiable y válido en procesos que exigen privacidad en el tránsito de la información. • El éxito de la esteganografía se basa en la escogencia deliberada del vehículo en el que se desea camuflar la información, existiendo tantos mecanismos para llevar a cabo camuflaje de información como la imaginación lo permita.

Una vez que se descubre la existencia de un mensaje oculto en un estego-objeto, se pueden realizar cuatro acciones: destruir el objeto, agregar/cambiar información, cambiar el formato del objeto o comprimir el objeto.

La más simple de todas es la destrucción del objeto. Como sugiere el nombre de este tipo de ataque, es simplemente la erradicación del estego-objeto. Esta forma de ataque genera dudas sobre la utilidad de la esteganografía debido a que, una vez que se descubre la existencia de un mensaje oculto, un simple ataque destruirá la información.

La adición/alteración de información es un ataque donde se inserta nueva información, con el fin de sobrescribir o cambiar la anterior. De esta forma, el receptor del estego-objeto recibirá información errónea.

Cambiar el formato del objeto es un ataque que consiste en cambiar simple y puramente la extensión del objeto, por ejemplo, de .jpg a .png o incluso a .mp3. Como cada tipo de formato

se lee de forma diferente, cambiar el formato puede hacer que ya no se encuentre información oculta. Tenga en cuenta que este tipo de ataque no está garantizado.

Finalmente, la compresión de objetos es un ataque que supone que, así como la compresión busca eliminar información extra del archivo para reducir su tamaño, esta reducción también elimina el mensaje oculto, incluso porque se coloca en lugares que no modifican drásticamente el archivo, por ejemplo en los bits menos significativos.

Una mejor manera de pensar en las redes es como una solución holística convergente, donde las redes y la ciberseguridad funcionan juntas como un sistema unificado. En lugar de centrarse en las redes o la seguridad por separado, las organizaciones deben desarrollar una estrategia de redes impulsada por la seguridad que integre estrechamente la infraestructura de red y la arquitectura de seguridad de la organización. Esto permite que la red escale, cambie y se adapte sin comprometer la seguridad. Para defender con eficacia los entornos altamente dinámicos de la actualidad, las organizaciones necesitan una aplicación constante que pueda abarcar y adaptarse a perímetros de red flexibles. Para hacer esto, la seguridad debe integrarse profundamente en la propia red.

En lugar de depender de una serie de componentes de seguridad discretos, una estrategia de seguridad moderna debe comenzar con una plataforma de seguridad unificada que abarque todo el ciclo de vida de desarrollo e implementación de la red. Este enfoque ayuda a garantizar que la seguridad funcione como la consideración central para todas las decisiones de infraestructura impulsadas por el negocio.

Bibliografía

Agarwal, m. (2013). Text Steganographic approaches: a comparison. International Journal of Network Security & Its Applications (IJNSA),

Antivirus eset. (2022). antivirus eset. Obtenido de antivirus eset:v https://www.eset.com/es/hogar/nod32-antivirus-windows/

Antivirus eset. (2022). ESET Captures 53rd Virus Bulletin VB100 Award. Obtenido de https://eset.version-2.sg/html/86/734/

BBC News Mundo, (2022). Cómo el emoji de la zanahoria se convirtió en uncódigo secreto en internet para camuflar contenido antivacunas. https://www.bbc.com/mundo/noticias-62936770.

Bestantivirus.org,(2022). Revisión del antivirus de ESET. https://es.bestantiviruspro.org/review/eset-antivirus-review/.

Cámara de comercio de Bogotá, (2017). Altos estándares de seguridad pueden cerrar la puerta al cibercrimen. https://www.ccb.org.co/Sala-de-prensa/Noticias-CCB/2017/Septiembre-2017/Altos-estandares-de-seguridad-pueden-cerrar-la-puerta-al- cibercrimen

Cámara Colombiana de Informática y Telecomunicaciones, (2022). Estudiotrimestral de ciberseguridad: Ataques a entidades de gobierno. https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

Castro Lechtaler, A. R., & Fusario, R. J. (2013). Comunicaciones, Una introducción a las redes digitales de transmisión de datos y señales isócronas. BuenosAires: Alfaomega

David García Cano, Análisis de herramientas estenográficas, Universidad CarlosIII de Madrid Escuela Politécnica Superior, diciembre 2004.

Duran, E. (10 de Noviembre de 2021). Cyclonis. Obtenido de Cyclonis: https://www.cyclonis.com/es/asi-es-como-los-hackers-estan-usando-la-esteganografia-en- ataques-ciberneticos

Duran, E. (10 de Noviembre de 2021). Cyclonis. Obtenido de Cyclonis: https://www.cyclonis.com/es/asi-es-como-los-hackers-estan-usando-la-esteganografia-en- ataques-ciberneticos/

Eset antivirus. (2022). Tecnología antivirus legendaria. Obtenido de https://www.eset.com/es/hogar/nod32-antivirus-windows/

El Laboratorio de Investigación de ESET Latinoamérica. (2016).

Ataques dirigidos, implicaciones, razones y objetivos. In Tendencias 2016: (In) Security Everywhere (pp. 18-23). Buenos Aires, Argentina.

García-cuerva, j. (2010). Creación de una herramienta para la generación deanalizadores estenográficos para imágenes. Leganés, España.

Hard zone. (2022). Qué es el firmware, y por qué es importante que estéactualizado. Obtenido de https://hardzone.es/reportajes/que-es/firmware-sirve- actualizarlo/

Hernández López, G., 2013. esteganografía en protocolos de

Red. Maestría. Instituto Politécnico Nacional México.

Google maps. (2022). Barrancabermeja, edificio cámara de comercio de.

Obtenido de

https://www.google.com/maps/place/Camara+de+Comercio+de+Barrancabermeja/@7.05

93224,-

73.8646595,3a,75y,125.11h,77.07t/data=!3m6!1e1!3m4!1s7SiKRnCMlpmPQ1b6Tq7nO

A!2e0!7i16384!8i8192!4m5!3m4!1s0x8e42eca2054e2fb3:0x22210c7d85780903!8m2!3d

7.0590896!4d-73.864968

Google maps. (2022). Barrancabermeja, edificio cámara de comercio de.

Obtenido de

https://www.google.com/maps/place/Camara+de+Comercio+de+Barrancabermeja/@7.05

93224,-

73.8646595,3a,75y,125.11h,77.07t/data=!3m6!1e1!3m4!1s7SiKRnCMlpmPQ1b6Tq7nO

A!2e0!7i16384!8i8192!4m5!3m4!1s0x8e42eca2054e2fb3:0x22210c7d85780903!8m2!3d

7.0590896!4d-73.864968

Iglesias, P. (2015). Esteganografía, el arte de ocultar información sensible.

Obtenido de https://www.pabloyglesias.com/mundohacker-esteganografia/

Journal of King Saud University – Computer and Information Sciences 34 (2022)

1343–1356. https://www.sciencedirect.com/journal/journal-of-king-saud-university-

computer-and-information-sciences

Martínez, Alejandro, Compeán, Isaac, Fosado, Rosa E., & Ávila, Raquel. (2018). Codificación Esteganográfica usando la Transformada de Onditas Haar Discreta Multi-resolución. Información tecnológica, 29(4), 317-328. https://dx.doi.org/10.4067/S0718-07642018000400317

Moreno, j. (7 de noviembre de 2022). Capacitación a funcionarios de la cámara de comercio de Barrancabermeja. Barrancabermeja, Santander, Colombia.

Navas, P. (2010). Investigación, análisis y pruebas de los Procesos de Esteganografía. Obtenido de www.bibliotecasdelecuador.com/Record/oai:oai:repositorio.utc.edu.ec.../Description

Portaltic. (2020, 1 febrero). La esteganografía digital, la técnica que oculta información en archivos multimedia. europapress.es. https://www.europapress.es/portaltic/ciberseguridad/noticia-esteganografia-digital-tecnica-oculta-informacion-archivos-multimedia-20200201112957.html

Renza, D., & Ballesteros L., D., & Rincón, R. (2016). Método de ocultamiento depíxeles para esteganografía de imágenes en escala de gris sobre imágenes a color. Ingeniería y Ciencia, 12(23), 145-162.

Rodríguez, J. F. D. (2020, 26 mayo). En Colombia hay seis millones de personas trabajando desde casa por la pandemia de covid-19. elpais.com.co. https://www.elpais.com.co/economia/en-colombia-hay-seis-millones-de-personas-trabajando-desde-casa-por-la-pandemia-de-covid-19.htm

Rodríguez, M. (2016). Análisis de las técnicas de esteganografía para elocultamiento de la información. Obtenido de http://www.dspace.uce.edu.ec/handle/25000/6356

Romero, Alberto (2002). Las redes de información y su importancia para la investigación científica. Revista Venezolana de Gerencia, 7(19) ,425-441. [Fecha deConsulta 9 de mayo de 2021]. ISSN: 1315-9984. Disponible en: https://www.redalyc.org/articulo.oa?id=29001906

Segura, g., & Díaz, a. (2014). Implementación del algoritmo estenográfico LSB (least significant bit) estándar en archivos de audio mp3. Retrieved from Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas UPIITA-IPN: http://www.boletin.upiita.ipn.mx/index.php/ciencia/215-cyt-numero-33/109-implementacion-del-algoritmo-esteganografico-lsb-least-significant-bit-estandar-en-archivos-de-audio-mp3

Solano Solano, L. O. (08 de Agosto de 2018). Universidad Nacional de Loja Repositorio Digital. Obtenido de https://dspace.unl.edu.ec/jspui/bitstream/123456789/21411/1/Solano%20Solano%2c%20Luis%20Omar.pdf

Telstra. (17 de Marzo de 2021). Telstra. Obtenido de https://www.telstra.com.au/content/dam/shared-component-assets/tecom/campaigns/security-report/Summary-Report-2019-LR.pdf

Telstra. (17 de Marzo de 2021). Telstra. Obtenido de https://www.telstra.com.au/content/dam/shared-component-assets/tecom/campaigns/security-report/Summary-Report-2019-LR.pdf

This emerging malware sends secret messages and is practically impossible to detect. (Disponible en: http://qz.com/238561/this-emerging-malware-sends-secret-messages-and-is-practically-impossible-to-detect/. Consultado el: 26 de marzo de 2021)

Titulares.ar, (2022). Los consumidores pagan el precio de las filtraciones de datos empresariales / Titulares de Tecnología. https://titulares.ar/los-consumidores-pagan-el- precio-de-las-filtraciones-de-datos-empresariales-titulares-de-tecnologia/

Zona Infiltrados, (2011). Ventajas y Desventajas del Nod32. https://zonainfiltrados.wordpress.com/tag/ventajas-y-desvemtajas-del-nod32/