Análisis y simulación de un ataque de phishing en el uso de un Framework Gophish en la cooperativa de taxis "San Fernando de Babahoyo"

Analysis and simulation of a phishing attack in the use of a gophish framework in the "San Fernando de Babahoyo" taxi cooperative

https://doi.org/10.5281/zenodo.12726297

AUTORES: Lisbeth Dayana Baños Galeas [1]*

Fabián Eduardo Alcoser Cantuña [2]

Jhon Eduardo Villacrés Sampedro

Kelly Karina Esparza Cruz [4]

[1]* *Trabajador independiente, 0009 – 0008 – 2674 – 4266, lisbeth847dayana@gmail.com*
[2] *Universidad Técnica de Babahoyo, 0000 – 0002 – 3422 – 2096, falcoserc@utb.edu.ec*
[3] *Escuela Superior Politécnica del Chimborazo, 0000 – 0002 – 8064 – 9680, jhon.villacres@espoch.edu.ec*
[4]*Universidad Técnica de Babahoyo, 0000 – 0002 – 1916 – 5150, nesparza@utb.edu.ec*

DIRECCIÓN PARA CORRESPONDENCIA: lisbeth847dayana@gmail.com

Fecha de recepción: 05 / 10 / 2023

Fecha de aceptación: 12 / 12 / 2023

Fecha de publicación: 04 / 01 / 2024

RESUMEN

Gophish de código abierto es un framework de acceso gratuito para realizar simulaciones de ataques phishing, está escrito en lenguaje go, es fácil de instalar y acceder a esta herramienta tecnológica que utiliza la api json, permitiendo a los desarrolladores y administradores de sistemas automatizar campañas de phishing simuladas, una de las características al ejecutarlo envía correos electrónicos falsificando la identidad de alguna empresa de confianza para que algún usuario ingrese sus datos, los mismos que son capturados y utilizados con fines no

éticos. Por tanto, el objetivo del presente estudio fue la simulación de un ataque phishing a la página web de la Cooperativa de Taxis "San Fernando de Babahoyo" para poder detectar los riesgos potenciales de suplantación de identidad, técnica que ha crecido exponencialmente la última década, para lo cual metodológicamente se utilizó la investigación exploratoria por medio de la observación con enfoque experimental logrando demostrar que la página es altamente vulnerable, el uso de técnicas de recolección de datos. Obteniendo como resultado que los usuarios no están capacitados ni tienen conocimiento sobre las posibles técnicas phishing para suplantar la información y obtener información sensible de la empresa y hacen mal uso de sus datos privados en un 75% en páginas de internet, de lo cual se concluye que los usuarios proporcionan información sensible de forma fácil y serán engañados para ingresar a la Información de la Cooperativa de forma auténtica pero no legal y poder malversar la información de los socios taxistas.

PALABRAS CLAVES: Phishing, Servidor, Dominio, Ingeniería Social, Spam, Framework Gophish.

ABSTRACT

Open source Gophish is a free access framework to perform phishing attack simulations, it is written in the go language, it is easy to install and access this technological tool that uses the json API, allowing developers and system administrators to automate phishing campaigns. Simulated phishing, one of the features when executed sends emails falsifying the identity of a trusted company so that a user enters their data, which is captured and used for unethical purposes. Therefore, the objective of this study was the simulation of a phishing attack on the website of the "San Fernando de Babahoyo" Taxi Cooperative in order to detect the potential risks of identity theft, a technique that has grown exponentially in the last decade. For which, methodologically, exploratory research was used through observation with an experimental approach, demonstrating that the page is highly vulnerable, the use of data collection techniques. The result is that users are not trained or have knowledge about possible phishing techniques to impersonate information and obtain sensitive information from the company and they misuse their private data by 75% on internet pages, from which

it is concluded that users provide sensitive information easily and will be deceived into entering the Cooperative Information authentically but not legally and being able to misappropriate the information of the taxi driver members.

KEY WORDS: Phishing, Server, Domain, Social Engineering, Spam, Gophish Framework.

INTRODUCCIÓN

En el Ecuador aún en la actualidad, se escuchan casos de individuos que han perdido información y recursos económicos de manera inadvertida a causa de actividad delictiva mediante el uso de sistemas informáticos. Inicialmente, los objetivos preferidos eran los clientes de entidades bancarias, ya que muchos carecían de un conocimiento adecuado sobre estos riesgos, lo que los hacía vulnerables a ser engañados, sin embargo, se ha observado que el personal administrativo de las empresas también se convierte en un blanco fácil debido a su escasa experiencia con la tecnología, lo que permite a los criminales tomar el control de los sistemas de manera parcial o total. Por lo tanto, se ha vuelto imperativo asegurar los sistemas informáticos para prevenir este tipo de incidentes.

La cooperativa de taxis “San Fernando de Babahoyo” no cuenta con herramientas tecnológicas que proporcionen seguridad por lo que la usar el internet los datos quedan expuestos a cualquier amenaza o ataques por medio de sitios web. En los últimos años los ataques phishing aumentaron significativamente a nivel mundial alcanzando los 245.771 de páginas fraudulentas por tanto puede variar la cifra dependiendo los meses y años debido a la actividad de los ataques (Harán, 2021). Ecuador no es la excepción en 2020 y 2021 se encuentra en 5to lugar entre los países que más se practica este tipo de ataques en Latinoamérica (Pichincha, 2022) .

El desconocimiento sobre seguridad informática en varias empresas, organizaciones o en la vida diaria permite confiar en mensajes que son creados para causar daño. La cooperativa de taxis “San Fernando de Babahoyo” tiene varios problemas entre ellos está la inseguridad física y la inseguridad informática. Por lo que se pretende utilizar la inseguridad informática ya que es una problemática existente en el campo tecnológico para enfocarlo hacia la

cooperativa de servicios dedicada al transporte privado, mediante la utilización de herramientas que nos permitan mantener la información segura y prevenir posibles pérdidas.

El framework GoPhish open-source de código abierto, nos permite crear una simulación sobre este ataque de Phishing conectando con el servidor https://127.0.0.1:3333 en el puerto https://0.0.0.0:80 como usuario administrador. En la cooperativa de taxis San Fernando de Babahoyo al utilizar constantemente el correo electrónico para recibir documentos importantes, está expuesta a que ingrese este tipo de ataques en la red por lo que todo el personal de la cooperativa de taxis necesita estar preparado para cualquier tipo de ataque que trate de violentar la integridad de la información de la cooperativa de servicios de transporte privado y de sus socios.

El principal objetivo del presente estudio es la simulación de un ataque phishing por medio del uso del framework gophish al sitio web de la Cooperativa de Taxis San Fernando de Babahoyo. La simulación de phishing desempeña un papel fundamental en fortalecer las defensas cibernéticas de las organizaciones al mejorar la conciencia, la educación y la capacidad de respuesta de los usuarios ante las amenazas de ingeniería social en constante evolución.

La ciberseguridad es un campo complejo y en constante evolución que aborda la protección de sistemas, redes y datos contra amenazas cibernéticas. Al considerar la ciberseguridad, es fundamental abordar una variedad de aspectos para garantizar una protección efectiva. Aquí hay algunos aspectos clave que deben ser tenidos en cuenta:

Políticas de Seguridad: Desarrollar y aplicar políticas de seguridad claras y robustas que aborden el uso adecuado de los recursos tecnológicos y establezcan pautas para la protección de la información.

Gestión de Identidad y Acceso: Implementar sistemas de gestión de identidad y acceso para garantizar que solo usuarios autorizados tengan acceso a recursos específicos y que la autenticación sea sólida.

Actualizaciones y Parches: Mantener todos los sistemas y software actualizados con los últimos parches de seguridad para remediar vulnerabilidades conocidas.

Protección de Datos: Enfocarse en la privacidad y seguridad de los datos, implementando medidas de cifrado y asegurando la integridad y confidencialidad de la información almacenada.

Concientización y Formación: Educar a los empleados y usuarios sobre las mejores prácticas de seguridad, incluyendo la identificación de ataques de phishing, el uso de contraseñas seguras y la conciencia general de las amenazas cibernéticas.

Firewalls y Seguridad Perimetral: Implementar firewalls y medidas de seguridad perimetral para monitorear y controlar el tráfico entrante y saliente, protegiendo así contra intrusiones no autorizadas.

Gestión de Incidentes: Establecer un plan de respuesta a incidentes que permita una acción rápida y eficiente en caso de una violación de seguridad, minimizando el impacto y restaurando la normalidad lo antes posible.

El internet es una red de comunicación que utiliza líneas telefónicas, cables, satélites y comunicaciones inalámbricas para conectar computadoras y otros dispositivos a la world wide web. Todas las computadoras modernas pueden conectarse a Internet, así como muchos teléfonos celulares, algunos televisores, consolas de juegos y otros dispositivos. (Delgado, 2021). Internet es una red de comunicación que conecta computadoras y otros dispositivos a la world wide web mediante líneas telefónicas, cables, satélites y comunicaciones inalámbricas.

Ventajas del Internet:

Acceso a la información: Es que contiene una gran cantidad de información a la que se puede acceder rápidamente sin ningún conocimiento técnico especial. Con su uso se puede obtener una buena fuente de información de una manera rápida. (MarcaGo, 2022)

Comunicación: Siempre que ambas partes tengan acceso a Internet, puede mantenerse en contacto con cualquier persona, independientemente de la distancia entre ellos. No hay barreras que los separen. Por lo tanto, la comunicación se vuelve más fácil. (MarcaGo, 2022)

Hacer que las personas trabajen juntas: Internet no solo brinda acceso a la información y un medio de comunicación, sino que también proporciona un marco que permite que diferentes personas trabajen juntas para lograr un propósito particular". (MarcaGo, 2022)

Permite más opciones para el aprendizaje: Además de buscar información, las redes de Internet también han creado nuevos métodos, herramientas o métodos alternativos de aprendizaje para reemplazar los métodos tradicionales". (Go, 2022)

Facilita la gestión y la organización: A medida que Internet ha creado mejores formas de administrar el tiempo y las actividades, hay más formas de construir una buena organización. Para planificar o buscar información sobre una determinada gestión". (MarcaGo, 2022)

Desventajas del internet

Fraude y ciberdelincuencia: El inconveniente más común del internet es el riesgo de fraude y ciberdelincuencia, ya que proporciona una gran cantidad de datos personales importantes que pueden utilizarse de manera negativa para obtener ganancias de personas externas. Estos incluyen casos de ciberacoso, amenazas, robo de información personal, fraude y robo de datos personales. (MarcaGo, 2022). El inconveniente más frecuente que presenta el internet es la inseguridad y el peligro de que seguridad sea vulnerada.

La privacidad está amenazada: Internet es para que las personas se conecten, pero compartir información presenta un inconveniente porque brinda todos parte de la privacidad de alguien. Otro punto relacionado con esto es que a las empresas les interesan los datos de las personas y existen empresas profesionales encargadas de recopilar datos de los internautas y venderlos a otras empresas. (MarcaGo, 2022).

La información puede saturarse: Hay mucha información a lo que puede contener datos incorrectos o fuentes defectuosas. Por lo tanto, debe tener cuidado de encontrar información realmente confiable. Otro punto relevante es la sobresaturación. Esto se debe a que tiene demasiados datos y no sabe exactamente cómo manejarlos y dónde usarlos. (MarcaGo, 2022).

Servicios de internet

Búsqueda y transferencia de información: La información se puede encontrar y ransferir fácilmente, sobre cualquier tema en cualquier momento. Esta característica ha dejado obsoletas a las enciclopedias del mismo modo a los libros físicos. Algunas búsquedas arrojan decenas de miles de coincidencias, por lo que debe acotar su búsqueda utilizando ciertos criterios y filtros que limiten el número de resultados obtenidos. (Garcia, 2019).

Correo electrónico (e-mail): Concede a los usuarios enviar y recibir correo electrónico que contiene texto, imágenes, videos y archivos adjuntos". (Garcia, 2019)

Servicios como foros, redes sociales: Facebook, Twitter e Instagram han demostrado ser excelentes plataformas de marketing, permitiendo el rápido intercambio y difusión de información entre grupos sociales con características similares". (Garcia, 2019)

Chats en línea: Chat en línea es uno de los servicios de Internet más utilizados para enviar y recibir varios tipos de mensajes electrónicos. Los mensajes pueden ser leídos por cualquiera chat público o solo por personas autorizadas chat privado. (Garcia, 2019)

El comercio electrónico en los últimos años, la compra de productos y servicios en Internet utilizando métodos de pago electrónico como tarjetas de crédito se ha incrementado de forma espectacular. Proveedores como Amazon están transformando la forma en que hacen negocios en todo el mundo al abrir cientos de miles de productos al público a precios asequibles. (Garcia, 2019). El internet permite realizar compra y venta de los productos con la facilidad de pagar los productos de manera digital con beneficios en distintas empresas como Amazon.

Según MSc César A y Delgado B (2021), un sitio web es una colección de páginas web agrupadas y conectadas entre sí, a menudo en el mismo dominio o subdominio. Un sitio web

en internet es una colección de archivos electrónicos y páginas relacionados con un contexto en particular, incluida la primera página de inicio, accesible a través de un nombre de dominio y una dirección de internet específica. (César, 2021)

La seguridad informática nace por los avances en la integración de las Tecnologías de la Información y la Comunicación están revolucionando la forma de intercambiar información entre empresas. Esta transformación digital ha abierto la puerta a un tipo de ciber delincuentes con capacidad de penetrar en el sistema para secuestrar o robar información de gran valor para las empresas de todos los sectores, incluso afectar la sostenibilidad del negocio. (E&L, 2021).

Este tipo de tecnología ofrece desventajas, entre ellas está la inseguridad donde intervienen los ciber delincuentes denominados como personas que intentan forzar la seguridad con el objetivo de extraer la información para causar daño.

La ingeniería social es la principal causa del aumento de los ciberataques es la mayor dependencia de la población en internet. La ingeniería social es la base principal de ataques como el phishing. Es un conjunto de técnicas que tienen como objetivo engañar a los usuarios con principios como la reciprocidad, la urgencia, la confianza, la autenticación social o la autoridad. Los ciberdelincuentes desarrollan una estrategia discursiva mediante la cual convencen a los usuarios para que entreguen sus datos personales. (Bello, 2021)

Spam es la palabra utilizada en el mundo para referirse a correos electrónicos no solicitados. El que envía el mismo mensaje de correo electrónico a miles o millones de personas a un costo mínimo, mucho menor que el correo tradicional, a la empresa a la que lo envía el por ello, el envío masivo de correos está a la orden del día. Si deja su dirección de correo electrónico en grupos, chats, foros de noticias es probable que su bandeja de entrada se inunde con mensajes promocionales que intentan venderle cualquier cosa. (Aranda, 2022)

DigitalOcean es un servicio de alojamiento y hospedaje en la nube que incluye VPS servidor privado virtual especialmente para desarrolladores. Con solo un clic, puede implementar la seguridad en su sitio web, juego o aplicación. Este servicio de alojamiento tiene un montón de características entre ellos esta: privacidad, seguridad, usabilidad y velocidad. (Smith, 2021). El término dominio es el nombre de una página web. Todos los sitios web tienen una dirección única que consta de números y una conexión al servidor que almacena los datos del sitio web; esta dirección se llama ip. (Valois, 2019).

El botón identificación del sitio (un candado) aparece en la barra de direcciones cuando visita un sitio seguro. Puede averiguar rápida y fácilmente si la conexión al sitio está encriptada y a quién pertenece la conexión. Esta información lo ayudará a evitar sitios maliciosos que solo intentan obtener y robar su información personal. (García, 2022).

El phishing es un tipo de estafa implica el uso de varios métodos correo electrónico, sitio web, chat, para dirigir a las víctimas a un sitio web falsa y convencerlas de que están navegando en el sitio real. De esta forma, los atacantes obtienen información confidencial sobre los usuarios y sus cuentas, como números de tarjetas de crédito o débito, números de cédula de identidad o pasaporte, códigos secretos, contraseñas, dirección, número de teléfono, es decir, cualquier información útil para ellos cometer robo o fraude. Los sitios con este ataque tienen colores, íconos y formatos similares para confundir a los usuarios. (Pichincha, 2022)

> Tipos de phishing Phishing por e-mail: Podría decirse que este es el tipo más común de ataque de Phishing. Básicamente, lo que está haciendo el atacante es hacerse pasar por una empresa u organización. Pueden utilizar direcciones de correo electrónico similares a las direcciones de correo oficiales, copiar logotipos, texto. Intentan hacer creer a la víctima que se trata de un mensaje importante y utilizan frases de advertencia para que los usuarios presten más atención y acaben visitando ese enlace malicioso. (Jiménez, redeszone, 2020).

Vishing: Son ataques de voz. Allí utilizan mensajes sonoros reemplazan la identidad de una empresa u organización. Hacen que la víctima piense que está tratando con algo legítimo. De esta manera recopilarán información". (Jiménez, redeszone, 2020)

Qrishing: Los códigos QR están muy presentes en nuestro día a día. Se utilizan para recopilar información en ciertos lugares. El problema ocurre cuando se modifica maliciosamente este código QR. Pueden ponerlo en lugares públicos donde el código suele ser legal. Al acercar el dispositivo móvil y leer este código, nos redirige a una web falsa que pone en riesgo nuestra seguridad. (Jiménez, redeszone, 2020).

Phishing basado en malware: El hacker agrega un archivo malicioso por lo general, reciben el correo y en lugar de un enlace a un sitio de phishing, el correo electrónico contendrá malware". (Jiménez, Redes Zone, 2020)

Gophish es un software de código abierto que es completamente gratuito para que cualquiera lo use para simular un ataque phishing. Está escrito en el lenguaje de programación go, esto tiene la ventaja de que los lanzamientos gophish son binarios compilados sin dependencias esto hace que la instalación sea tan simple como descargar y ejecutar esta implementado con el api json para la automatización. (Dewall, 2022). Gophish de código abierto es un framework completamente gratuito para realizar simulación de ataque phishing, está escrito en lenguaje go y es fácil de instalar y acceder a esta herramienta tecnológica que utiliza la api json.

El lenguaje de programación go también conocido como go lang es creado por Robert Griesemer, Rob Pike y Ken Thompson, con la empresa google. Es un lenguaje concurrente, hace algunos cálculos de formas diferentes sin afectar el resultado y es compilado, ya que el código fuente tiene que pasar por las etapas de traducción del código máquina para poder ser ejecutado. Aunque sus funciones son similares a la sintaxis de C. Go toma características de otros lenguajes y las implementa de una manera que hace que el código esté escrito para ser más fácil de usar. (Guerrero, 2021)**.** El lenguaje go es creado por Robert Griesemer, Rob Pike y Ken Thompson en conjunto con google realiza cálculos que no afectan al resultado final y se maneja la traducción de código por lo cual el lenguaje go es muy parecido a lenguaje c.

El api de json permite a los desarrolladores y administradores de sistemas automatizar campañas de phishing simuladas. Al ejecutarlo, se inician dos servidores web, una base de datos y agentes en segundo plano, que se encargarán de enviar correos electrónicos". (Land, 2022)

En el apartado de configuración (settings), podemos cambiar las credenciales del usuario o crear una nueva. La desventaja es que no hay un apartado donde se muestren todos los usuarios creados, por lo que para conocer este dato tendremos que acceder a la base de datos para ejecutar la consulta. También disponemos de la clave API que nos permitirá interactuar con la herramienta desde cualquier lenguaje de programación o scripting, por si preferimos utilizar otro método diferente a su interfaz web. (Rodríguez, 2018)

En perfiles de envio (sending profiles), muestra la dirección válida en el campo from y el servidor junto al puerto al que se enviará el dispositivo. Indica si tiene un certificado de la cuenta que desea utilizar para el envío. Si hay un problema con el certificado, ya sea un certificado autofirmado, un certificado de un certificado que no es de confianza (CA) o un certificado que no es de confianza. (Rodríguez, 2018)

La página destino (landing page), es aconsejable crear una página lo más parecida posible a la que pretendemos reemplazar hay una opción para importar páginas. Esta página se almacena en la base de datos configurada en el sistema, asignándole un id, parámetro rid para crear la URL completa que utilizaremos en las campañas en las que participe. (Rodríguez, 2018)

En la sección plantilla de email (email template), deberá crear un correo electrónico para enviar a las víctimas. Este correo electrónico contiene una enlace que redirige a la página donde tenemos el formulario para obtener la información de inicio de sesión de la víctima. (Rodríguez, 2018). En la sección de usuarios y grupos (users & groups), se registra el grupo de víctimas que serán objeto de la simulación. La información opcional a completar es: nombre, apellido, puesto en la empresa y el campo obligatorio es correo electrónico, ya que sin él no permitirá la creación de un usuario o grupo. (Rodríguez, 2018)

En la sección campañas (campaigns), crearemos una campaña para enviar. Nombre de campaña, plantilla de envío de campaña creada previamente. Se suele crear un sitio web donde se redirige a la víctima para recuperar sus datos. Envía el perfil al servidor de correo electrónico que se usa para la campaña. (Bastian, 2018). Una vez que se crea la campaña, puede acceder a los eventos para ver si la víctima abrió el mensaje, ingresa a la página del enlace y envíe el formulario con la información que tiene que llenar la víctima. La opción de publicidad por correo electrónico está en versión beta y tiene como objetivo proporcionar un contexto para que las víctimas las alerten sobre el phishing y se aseguren de que estén al tanto de este riesgo. (Bastian, 2018).

En la sección panel (dashboard), puede encontrar una recopilación de todas las configuraciones del proyecto, ya sea completada o no, así como datos internacionales para cada torneo. Además se puede modificar las estadísticas para cada campaña. (Bastian, 2018)

METODOLOGÍA

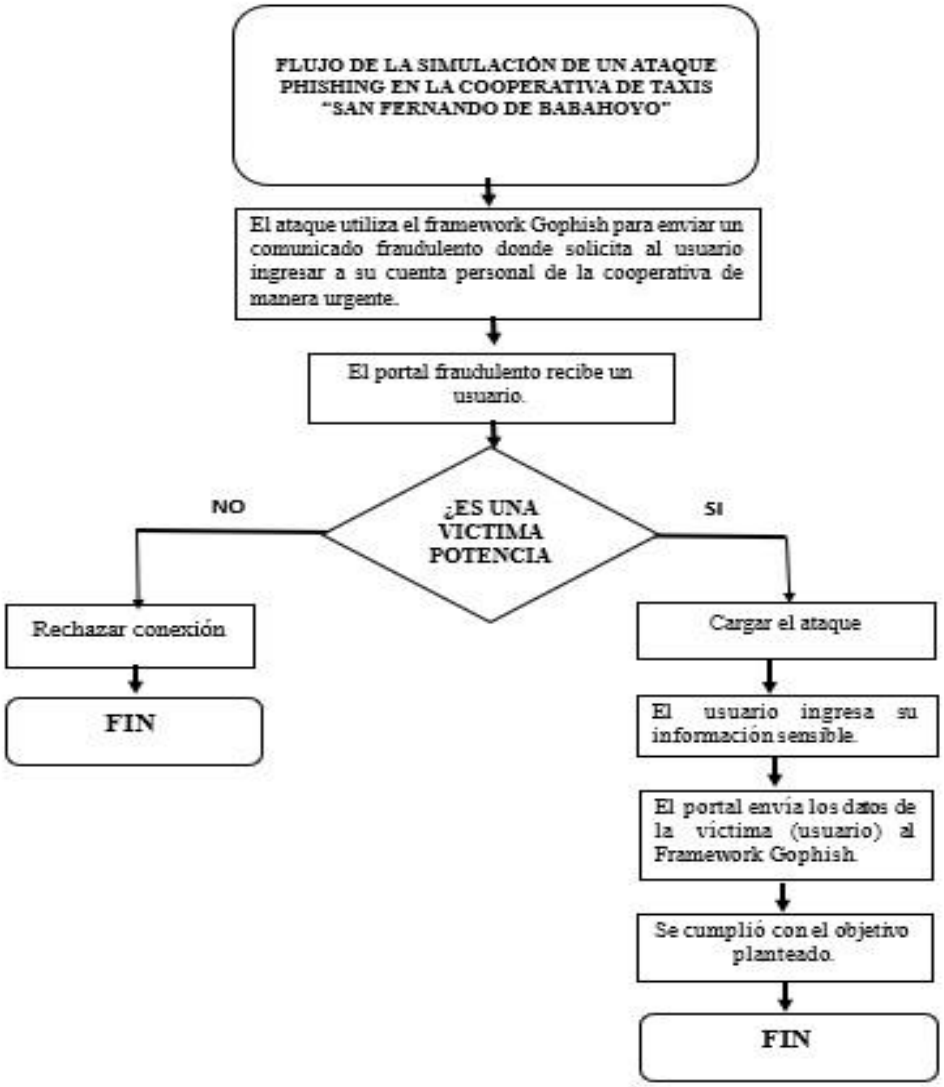
En la presente investigación se utilizó la metodología de enfoque experimental ya que se evaluarán aspectos de la simulación de un ataque phishing en la cooperativa de taxis San Fernando de Babahoyo, por medio de la observación y problemática existente se validará el tema mediante cuestionarios estadísticos.

Adicionalmente, se requiere de una investigación exploratoria donde se toman en cuenta varios puntos importantes en la investigación, por tanto, se analiza el planteamiento del problema de la cooperativa, objetivos y los procesos que debe realizar. La población son todos los usuarios que conforman la cooperativa de taxis San Fernando que está conformado por el presidente, gerente, secretaria, comisiones especiales, consejo de administración y socios.

Las técnicas que se utilizaron fueron la recolección de datos por lo que se usó la entrevista y la observación que es necesaria en la ejecución de la simulación de un ataque phishing en la cooperativa de taxis San Fernando de Babahoyo.

RESULTADOS

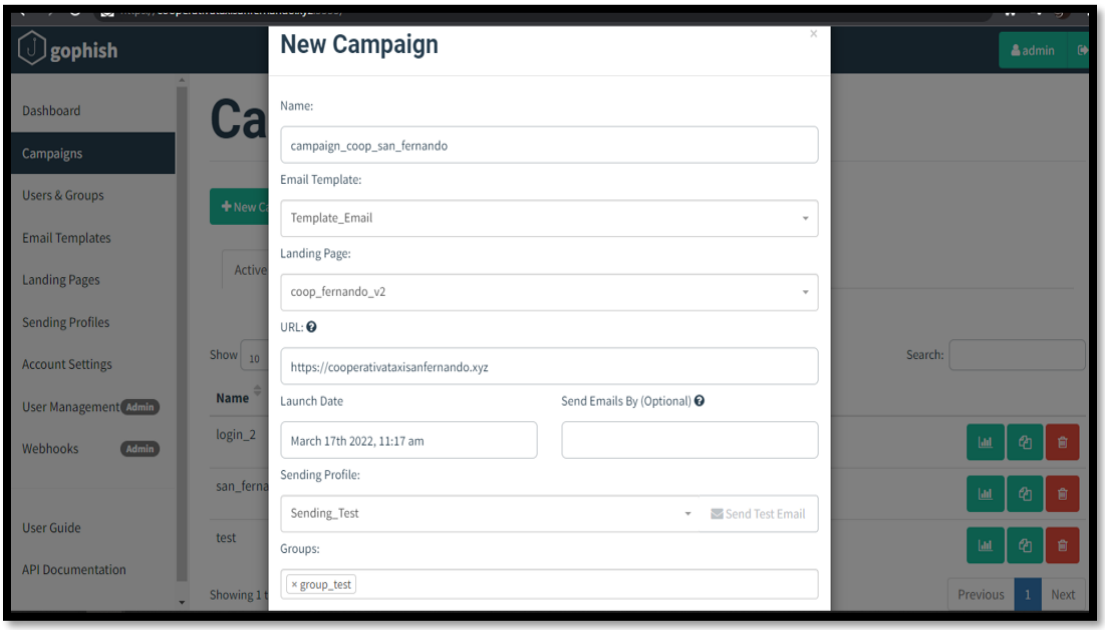
A continuación, se detalla un diagrama de procesos para realizar la simulación como se



detalla en la Figura 1.

Figura 1. Diagrama de procesos de la simulación

Se puede observar en la Figura 2, el proceso de la simulación de un ataque phishing en la Cooperativa “San Fernando”, donde se pudo evidenciar el desconocimiento sobre seguridad hace que la Cooperativa sean muy vulnerable a este tipo de ataques.



Como podemos observar en la Figura 3, se puede visualizar el proceso para la configuración del framework gophish en la opción de nueva campaña.

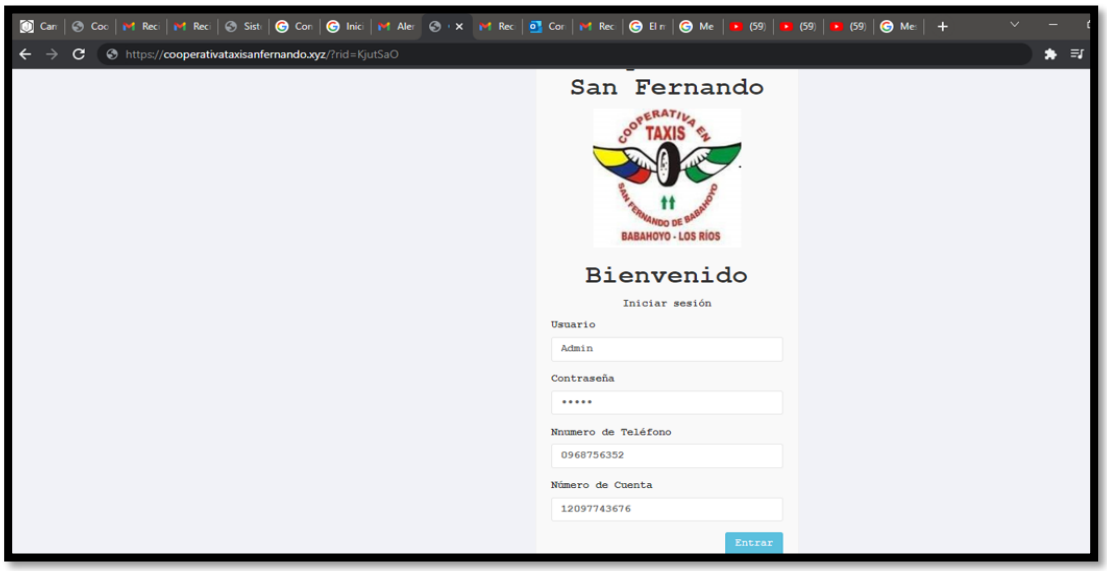


Figura 3. Utilizando el url se duplica la página real a una página fraudulenta

Se puede visualizar en la Figura 4, que el login de la página fraudulenta se ha duplicado como una real donde los usuarios ingresan sus datos para así realizar el ataque phishing, de esta manera lograr robar datos sensibles de los usuarios de la Cooperativa de Taxis “San Fernando”

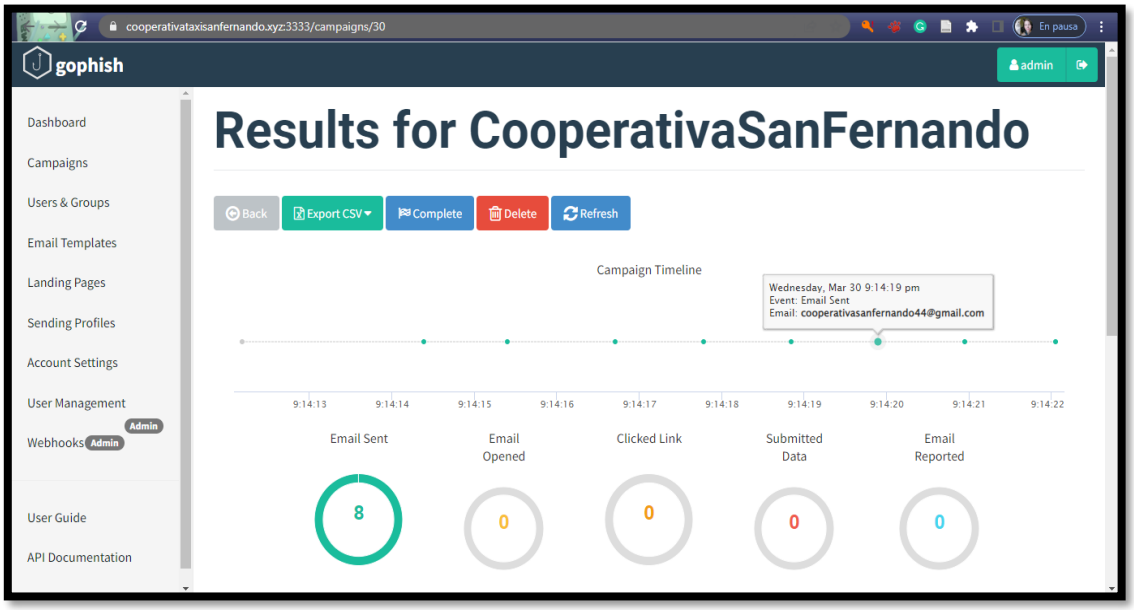


Figura 4. Resultados de los grupos de e-mail enviados al personal Como podemos evidenciar en la Figura 5, ya se visualiza los resultados favorables del ataque de phishing.

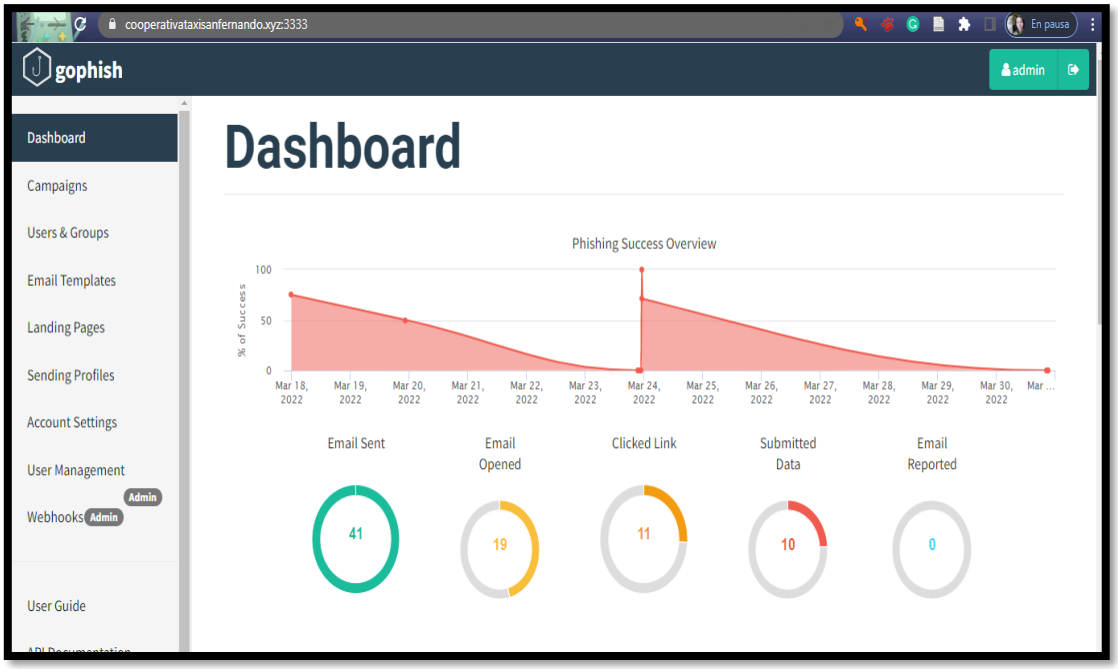


Figura 5. **Dashboard refleja las veces que se realizaron los ataques phishing.**

Mediante la encuesta realizadas a los directivos de la Cooperativa “San Fernando” luego del análisis tenemos los siguientes resultados:

Apenas el 10% de los usuarios conocen que es un phishing, y un 90% desconoce los peligros y los ataques de phishing. Podemos concluir, que, si llegase a dar un ataque phishing los usuarios de la Cooperativa “San Fernando”, caerían de forma muy fácil en el engaño.

Los usuarios entregan o llenan sus datos en páginas desconocidas en un 75%. Con frecuencia los realizan en un 15,63%, A veces lo realizan con un 6,25% y los que son evitan dar información apenas son un 3,13%. Lo que conlleva un gran riesgo de que les puedan fraudulentar sus datos e información sensible ya sea personal o de la Cooperativa.

El 60% de usuarios siempre confía en el correo electrónico, seguido de un 25% que a veces confía en los emails y finalmente un 15% que nunca confía los mensajes de correo electrónico

de extraños. Lo que nos sugiere que existe una alta probabilidad de engañar a los usuarios e ingresar a sus correos electrónicos.

Los usuarios en un 60% siempre ingresan a enlaces por medio de mensajería, en un 10% a veces ingresan a enlaces de mensajería, seguido de un 20% que ingresa con frecuencia a mensajes, y un 10% nunca ingresa a link de mensajería. Lo que nos indica que la probabilidad de phishing es alta.

Un 77.5% de usuarios no confían nada en la seguridad de internet, en un 17.5 % que confían en algo en la seguridad, finalmente un 5% que confían bastante en la seguridad de internet. Podríamos concluir, que los usuarios no están confiados de la seguridad del internet.

DISCUSIÓN

Los contratiempos que presento el análisis y simulación de un ataque de phishing en el uso de un framework gophish en la cooperativa San Fernando de Babahoyo. Fueron que al realizar de manera local no logro funcionar correctamente y es necesario que la web donde se aloja el framework gophish sea de origen seguro con protocolos ssl para permitir hacer las campañas o ataques a los usuarios.

Se tuvo que configurar un servidor privado en digitalocean en el que fue necesario una cuenta bancaria para poder acceder a los servicios de un servidor, en este caso se utilizó el servidor en Ubuntu de otra manera no permite acceder sin tarjeta de crédito ya que requiere un número de tarjeta de crédito para poder continuar.

Una vez que se pudo adquirir el servicio se empleó el programa putty que usualmente se lo utiliza para ejecutar servidores con distintos protocoles, por ende, se realizó con el protocolo ssl, y se configuró por medio de comandos del api json así mismo para abrir los puertos necesarios, se asigna una ip de servidor para ingresar al framework gophish en la que se tiene una conexión del servidor y el framework gophish.

También se tuvo que contratar un dominio en la página de zerossl del mismo modo que en el servidor fue necesario poseer una tarjeta de crédito para poder proveer de su servicio en la web, dependiendo el valor y el nombre de la página se coloca el .com,.xyz, .live, .art. En este caso se utilizó el http://dominio cooperativataxisanfernando.xyz. Ya obtenido el dominio se procedió a configurar en el programa putty los certificados crt, key y remplazar los puertos.

La página de la Cooperativa de Taxis “San Fernando” de Babahoyo, está compuesta por un panel principal, un login donde deben ingresar los usuarios autorizados como: presidente, gerente, vocales del consejo de administración, secretaria, comisiones especiales, socios, que ingresarán a su cuenta que contiene todos sus datos confidenciales. Al comenzar a utilizar esta página web se le coloco un dominio http://dominio cooperativataxisanfernando.xyz y poderla suplantar para que el usuario no sospeche de su autenticación y se configura los parámetros de gophish.

En la opción de campaings se llenaron los datos necesarios y se colocó el url de la página de la Cooperativa de taxis “San Fernando” de Babahoyo donde se visualiza una página exactamente igual, pero de origen desconocido.

Al realizar distintas pruebas los resultaros fueron óptimos y eficaces al verificar que por medio de un framework gophish se puede obtener información importante de las empresas y crear un tipo de ataque como phishing para así cumplir con los objetivos planteados como resultado se puede observar el número de email enviados, opositora de email, numero de enlaces en la que se hizo click, los datos presentados, y el informe del correo electrónico.

El personal que conforma la Cooperativa San Fernando destacó que es un tema nuevo para ellos y por el cual cayeron en este tipo de ataque por ende aprendieron a identificar las páginas autentica de las páginas que son fraudulentas.

CONCLUSIONES

Aplicando el proceso de la presente investigación, se logró conocer un método de ataque a la seguridad informática como es el phishing, que es un delito informático muy peligroso y puede llegar a exponer datos sensibles de una entidad a través de correos electrónicos falsificando la identidad de alguna empresa de confianza para que algún usuario ingrese sus datos.

El uso del framework gophish ha cumplido con la funcionabilidad de realizar las prácticas de ataques phishing incluso es una herramienta gratuita, fácil de configurar y contiene una interfaz muy intuitiva, se logró conocer el grado de impacto en la seguridad informática que existe en la cooperativa de taxis San Fernando mediante ataques phishing.

En las encuestas realizadas al personal de la cooperativa de taxis San Fernando de Babahoyo se dio a conocer el porcentaje de 90% de desconocimiento sobre el ataque phishing, en un 75% el mal uso de sus datos privados en páginas de internet, además el porcentaje de 60% en confiar en los mensajes de correo electrónico, por lo que el porcentaje de 60% de socios ingresan a link de servicios de mensajería sin seguridad alguna y un porcentaje de 77.5% no confía en la seguridad de internet.

REFERENCIAS BIBLIOGRÁFICAS

Aranda, V. T. (14 de Marzo de 2022). acta.es. Obtenido de Historia y evolución del internet: https://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf

Bastian, S. (Diciembre de 20 de 2018). tiraquelibras. Obtenido de https://blog.tiraquelibras.com/?p=335

Bello, E. (8 de Marzo de 2021). IEBS. Obtenido de https://www.iebschool.com/blog/ingenieria-social-tecnologia/

César, D. (14 de Marzo de 2021). upanama.e-ducativa. Obtenido de https://upanama.e-ducativa.com/archivos/repositorio/6000/6126/html/3_qu_es_.htm

Delgado, H. (8 de Junio de 2021). akus.net. Obtenido de Diseño web: https://disenowebakus.net/internet.php

Dewall, B. (5 de Enero de 2022). whiteoaksecurity. Obtenido de https://www.whiteoaksecurity.com/blog/gophish-setup-part-1/

E&L. (2021). Seguridad Informatica. Empresrial & Laboral, 1-5.

Ecuador, G. d. (7 de Enero de 2021). gobiernoelectronico. Obtenido de https://www.gobiernoelectronico.gob.ec/boletincampanasphishing/

Garcia, H. (11 de Agosto de 2019). tallerinformatica. Obtenido de http://tallerinformaticai.blogspot.com/2018/07/servicios-que-ofrece-internet.html

García, P. (24 de Marzo de 2022). support.mozilla. Obtenido de https://support.mozilla.org/es/kb/boton-de-identidad-de-sitio#:~:text=El%20bot%C3%B3n%20de%20Identidad%20del,casos%2C%20qui%C3%A9n%20es%20el%20proprietario.

Go, M. (12 de Marzo de 2022). Obtenido de https://marcago.com/marketing/ventajas-y-desventajas-del-internet/

Guerrero, L. E. (14 de Agosto de 2021). Programación estructurada. Obtenido de http://memoriascimted.com/wp-content/uploads/2021/08/Programacion-estructurada-en-Go-lang.pdf

Harán, J. M. (15 de Junio de 2021). welivesecurity. Obtenido de APWG: https://www.welivesecurity.com/la-es/2021/06/15/2021-registro-pico-historico-cantidad-sitios-phishing/

Jiménez, J. (30 de Marzo de 2020). Redes Zone. Obtenido de https://www.redeszone.net/tutoriales/seguridad/tipos-ataques-phishing/

Land, H. (14 de Marzo de 2022). hacking.land. Obtenido de https://www.hacking.land/2017/05/gophishing-entrenar-usuarios-contra-el.html

MarcaGo. (12 de Marzo de 2022). Obtenido de https://marcago.com/marketing/ventajas-y-desventajas-del-internet/

Pichincha, B. (14 de Marzo de 2022). pichincha. Obtenido de https://www.pichincha.com/portal/seguridad/internet

Rodríguez, S. B. (20 de Diciembre de 2018). Tiraquelibras. Obtenido de Ciberseguridad y TI: https://blog.tiraquelibras.com/?p=335

Smith, G. (24 de Marzo de 2021). hostingvictory. Obtenido de https://hostingvictory.com/es/opiniones/digitalocean/

Valois, M. (16 de Mayo de 2019). hostgator. Obtenido de https://www.hostgator.mx/blog/que-es-un-dominio-en-internet/

.