Pedagogía y Sociedad
UNIVERSIDAD DE SANCTI SPÍRITUS José Martí Pérez
ISSN: 1608-3784
RNPS: 1903

Recibido: 13/10/2023, Aceptado: 22/1/2024, Publicado: X/X/202X

Volumen 27 | Número 69 | Marzo-Junio, 2024

Artículo original

Proceso de phishing y pautas para la identificación de sitios web falsos

A phishing process and guidelines for identifying fake websites

Cristian Camilo Barrantes Bernal[1]

E-mail: ccamilobarrantes@ucundinamarca.edu.co

https://orcid.org/0009-0003-1515-9313

Snattan Andrey Espitia Velásquez[1]

E-mail: saespitia@ucundinamarca.edu.co

https://orcid.org/0009-0000-8592-4998

[1] Universidad de Cundinamarca. Cundinamarca, Colombia.

¿Cómo citar este artículo?

Barrantes Bernal, C. C. y Espitia Velásquez, S. A. (2024). Proceso de phishing y pautas para la identificación de sitios web falsos. *Pedagogía y Sociedad, 27* (69), x-x.

RESUMEN

Introducción: El phishing es una forma de ataque cibernético que se basa en la ingeniería social, que sigue siendo una amenaza latente en el mundo digital. En este artículo, se explora un proceso de phishing en un entorno local, centrados en la creación de un sitio web falso, donde se destaca la importancia de la capacitación en la mitigación de este riesgo.

Objetivo: Analizar el proceso de phishing en internet mediante la clonación de un sitio web en un ambiente controlado y la generación de pautas para la identificación de sitios web falsos.

Métodos: La investigación es de tipo explicativa y de laboratorio.

Resultados: Se ofrecen pautas fundamentales para identificar sitios web falsos, que incluyen: verificar la fuente de la comunicación, evitar hacer clic en enlaces sospechosos y utilizar la autenticación de dos factores. Esto se realizó teniendo en cuenta las diferentes partes del phishing en un entorno local.

Conclusiones: La importancia de la capacitación, la educación constante y la toma de conciencia sobre el phishing y sus técnicas para detectarlo, en un mundo digital en constante cambio, son las herramientas clave en la protección de la información confidencial y mitigación del phishing.

Palabras clave: cibernética; informática; ingeniería social; protección de datos; seguridad informática.

ABSTRACT

Introduction: Phishing is a form of cyber-attack that relies on social engineering and remains a latent threat in the digital world. In this article, a phishing process is explored in a local environment, focusing on the creation of a fake website, where the importance of training in mitigating this risk is highlighted.

Objective: To analyze the process of phishing on the Internet by cloning a website in a controlled environment and generating guidelines for the identification of fake websites.

Methods: The research is explanatory and laboratory-based.

Results: Key guidelines for identifying fake websites are provided, including: verifying the source of the communication, avoiding clicking on suspicious links,

and using two-factor authentication. This was done taking into account the different parts of phishing in a local environment.

Conclusions: The importance of training, constant education and awareness of phishing and its techniques to detect it, in an ever-changing digital world, are the key tools in protecting confidential information and mitigating phishing.

Keywords: computer science; computer security; cybernetics; data protection; social engineering.

Introducción

Internet es uno de los principales pilares tecnológicos sobre los cuales se ha construido la sociedad contemporánea, convirtiéndose en sinónimo de comunicación, lo que ha permitido tener acceso a un cúmulo de conocimientos con solo hacer clic en un botón. Se utiliza para acceder a bancos, realizar compras, descargar aplicaciones y esto, sin comprobar su origen, aceptar términos y condiciones sin leer los permisos que negligentemente se otorgan, sin darle la importancia que indiscutiblemente representan los datos personales. Lamentablemente, su acelerada evolución es un problema latente en el ámbito de la seguridad informática.

Uno de los mayores peligros en internet es el phishing, se presenta en forma de suplantación de páginas web con la finalidad de robar información para obtener algún beneficio económico, según señala el reporte de crímenes en internet proporcionado por la Oficina Federal de Investigación (Internet Crime Report, 2021), el phishing es uno de los crímenes reportados con mayor pérdida para las víctimas en el año 2021, el uso de este tipo de fraudes se ha ido diversificando con los años, lo que implica un crecimiento en el volumen de los ataques y la complejidad de las técnicas usadas por los cibercriminales. De acuerdo con el Instituto Nacional de Ciberseguridad los empleados son un elemento clave para prevenir este tipo de fraude porque son quienes tienen acceso y control sobre las herramientas de la empresa, lo que los convierte en el objetivo de los ciberdelincuentes. Uno de los mayores retos a la hora de mitigar el phishing, tiene que ver con el factor humano, pues la efectividad de

este tipo de fraude depende en mayor medida del error del usuario, es por ello que la concientización es fundamental para la prevención.

La investigación tiene como objetivo analizar el proceso de phishing en internet, mediante la clonación de un sitio web en un ambiente controlado y la generación de pautas para la identificación de sitios web falsos, con la finalidad de concientizar al usuario de internet frente a la seguridad de sus datos.

El objetivo general de esta investigación es: analizar el proceso de phishing en internet mediante la clonación de un sitio web en un ambiente controlado y la generación de pautas para la identificación de sitios web falsos, con la finalidad de concientizar al usuario de internet frente a la seguridad de sus datos.

Marco teórico o referentes conceptuales

En la actualidad la seguridad informática es un factor muy importante en la protección de la privacidad de cualquier individuo, puesto que la información es guardada en medios tecnológicos, según Baca Urbina en su libro: *Introducción a la seguridad informática*, esta podría definirse como:

> La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. (2016, p. 12)

Por esta razón, es importante que tanto las personas como las organizaciones protejan la información y los datos confidenciales, ya que no hacerlo, los expone a una variedad de amenazas que pueden tener consecuencias significativas a nivel personal y empresarial, los datos se han convertido en el núcleo de las operaciones cotidianas, lo que implica un aumento en la cantidad de información sensible almacenada y procesada, que va desde datos financieros y personales hasta secretos comerciales.

El avance de la tecnología aumenta de manera exponencial y desafortunadamente la seguridad informática no avanza a la misma velocidad, lo que lleva a los sistemas a estar en un constante estado de vulnerabilidad de una u otra forma, con el paso del tiempo las tecnologías de la información se

vuelven cada vez más importantes en la vida humana, lo que hace que los usuarios de Internet sean más susceptibles a diversas amenazas virtuales cuyo objetivo es el robo de información confidencial, entre estas amenazas se encuentra el Phishing definido por Belisario Méndez de la Universidad de Buenos Aires como:

> Phishing es un tipo de ataque de ingeniería social que ha existido desde hace más de 20 años. Consiste en engañar a la víctima, a través de la suplantación de identidad de fuentes confiables, de modo que proporcione voluntariamente información sensible. (2014, p. i)

A pesar de ser una modalidad de estafa antigua, el phishing sigue siendo una amenaza que va en aumento con los años, incluso se podría decir que ha mejorado a tal punto que podría ser definido como un conjunto de técnicas utilizadas por los ciberdelincuentes, donde se origina la suplantación de identidad de una compañía, los medios más recurrentes sobre los que se suelen desarrollar este tipo de ataques fraudulentos son el correo electrónico, redes sociales, SMS y llamadas telefónicas. De acuerdo con los ataques de phishing son con poca diferencia, el tipo de amenaza virtual más común, y su prevalencia se debe a su versatilidad, este tipo de estafa se ha convertido en una amenaza generalizada que se puede combinar con el uso de malware o exploits que se introducen dentro de archivos que al ser ejecutados infectan el dispositivo de la víctima o ejecutan una secuencia de código para aprovecharse de las vulnerabilidades del sistema. Uno de los más conocidos actualmente es el ransomware, un tipo de malware que consiste en la encriptación de información que le impide el acceso al propietario del dispositivo, con el fin de solicitar un pago o rescate por los datos (secuestro de información), el uso de los keyloggers también resulta ser muy común en el phishing, este es un tipo de spyware que permite registrar las teclas presionadas en una computadora. Por otro lado están los exploits que por medio de una secuencia de comandos pueden generar una conexión inversa con el atacante de manera que pueda tomar el control total del dispositivo a través de un puerto, es por ello que el phishing se ha convertido en una problemática a nivel mundial.

Existen varias recomendaciones para identificar el phishing, puesto que los ciberdelincuentes que aplican este conjunto de técnicas siguen unos patrones similares, en muchos casos los atacantes suelen enviar mensajes alarmistas con el objetivo de asustar al usuario y hacerle creer que debe resolver un problema de manera inmediata accediendo a links o a archivos adjuntos al comunicado en cuestión, también es común que el cuerpo del mensaje contenga errores gramaticales o de redacción puesto que muchos de estos atacantes utilizan traductores para poder realizar envíos de un mismo mensaje en varios idiomas y así extender el alcance de su estafa. En el campo de la ciberseguridad si un atacante desea vulnerar un sistema, este debe dirigir sus esfuerzos hacia el eslabón más débil, una de las razones por las que es tan eficaz el phishing es por que explota una vulnerabilidad humana. El uso de la ingeniería social, la clonación de páginas oficiales y técnicas varias, para hacer que la URL sea lo más idéntica posible a la página suplantada, hace que aumente la complejidad en su detección.

Según señala el reporte de crímenes en internet proporcionado por la Oficina Federal de Investigación (Internet Crime Report, 2021) el phishing implica que existe una ineficiencia en la mitigación del mismo, a pesar de la variedad de técnicas empleadas actualmente para erradicar el problema, no basta solo con aumentar la eficiencia de las técnicas, también debe existir una capacitación y concientización por parte de los usuarios de internet, con el objetivo de fortalecer el eslabón más débil del sistema, de acuerdo con el Instituto Nacional de Ciberseguridad (INCIBE) los empleados son fundamentales para la prevención de este tipo de fraudes, pues ellos son los utilizados por los cibercriminales para perpetrar sus estafas.

Algunas de las técnicas de detección de phishing más utilizadas por las organizaciones se apoyan sobre métodos basados en listas, métodos heurísticos, machine learning, minería de texto y procesamiento de lenguaje natural tal como lo mencionan los autores (Hernández Dominguez y Baluja García, 2021).

Los métodos basados en listas consisten en verificar una gran cantidad de bases de datos donde ya se encuentran clasificados como phishing algunos

sitios web, el problema de este método radica en los falsos positivos, es decir aquellas páginas que se clasifican como phishing sin serlo, y los falsos negativos que son phishing pero no se clasifican como tal, en los métodos heurísticos se utilizan técnicas de similitud visual usando reconocimiento óptico de caracteres, este tipo de detección se realiza tomando las mismas listas mencionadas anteriormente para realizar las diferentes comparaciones y clasificar las páginas web sospechosas, es por esto que arrastra los mismos problemas de las listas, gracias al avance en los algoritmos y creación de modelos en machine learning se tiene a disposición una serie de técnicas de clasificación que se han empleado a la hora de identificar y clasificar el phishing, los resultados de estos algoritmos son variados ya que todos utilizan cálculos matemáticos muy diferentes y que presentan mayor eficiencia de acuerdo a las condiciones del problema que se pretende resolver, entre estos algoritmos podemos tener árboles de decisión (DT), bosques aleatorios (RF), bayes ingenuos (NB) y redes bayesianas, redes neuronales (NN) y aprendizaje profundo (DL), por último la minería de texto en conjunto con el procesamiento de lenguaje natural, permite establecer relaciones en el cuerpo de los mensajes de texto o correos electrónicos, que logre determinar si se trata de un mensaje fraudulento o no.

Para el desarrollo de la metodología es importante tener presentes las diferentes leyes y repercusiones legales dentro del país de Colombia respecto a la intervención de sistemas informáticos. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273:

> Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (párr.1)

Tipificado dentro de los Artículos 269A: Acceso abusivo a un sistema informático y el Artículo 269C que indican lo siguiente:

> Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un

> sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. (Ley 1273, 2009)
>
> Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. (párr. 4)

Para no incurrir en delitos relacionados con intrusión, en este laboratorio todos los equipos y dispositivos empleados son propiedad de los miembros implicados en la creación del artículo, por consiguiente, hay autorización directa para acceder a los dispositivos.

Dentro del marco legal también se debe tener en cuenta la obstaculización de los sistemas involucrados en la red tipificado en el Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación de la ley 1273 de 2009 que indica lo siguiente:

> Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor. (párr. 3)

Para este caso el desarrollo del laboratorio se realizará completamente en red privada para evitar inconvenientes a la hora de intervenir comunicaciones para las que no se tiene permisos.

Finalmente, los artículos encargados de la tipificación en cuanto al uso de software malicioso y la suplantación de sitios web son el Articulo 269E: Uso de

software malicioso y el Articulo 269G: Suplantación de sitios web para capturar datos personales de la ley 1273 de 2009 que indican lo siguiente:

> Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. (párr. 6)
>
> Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. (párr. 8)

Por esta razón el proceso realizado dentro de la metodología del artículo no puede mostrar código que pueda considerarse malware, tampoco se puede difundir el procedimiento detallado del laboratorio y las etapas que involucren la violación de las leyes mencionadas dentro de este marco legal.

Metodología empleada

La siguiente investigación es de tipo explicativa y de laboratorio, consta del desarrollo de un ambiente controlado de phishing donde se adoptó la postura de víctima y atacante, con la finalidad de mostrar de qué manera los ciberdelincuentes obtienen las credenciales de las cuentas personales de sus víctimas por medio de la suplantación de sitios web oficiales, aprovechándose de la incredulidad y desconocimiento de los usuarios en internet, siendo este uno de los factores más influyentes en la eficiencia y rentabilidad de este tipo de delitos. El objetivo de la investigación fue brindar al usuario las pautas necesarias para identificar un ataque de este tipo a medida que se desarrolló el proceso de phishing con la finalidad de generar conciencia en el lector.

En el siguiente proceso se tendrán en cuenta las siguientes etapas, creación de un sitio web falso, identificación del tipo de ataque, determinar las técnicas de phishing para el laboratorio y finalmente generar el despliegue del ataque.

Primera etapa:

Debido a su simplicidad, en este caso experimental se utilizó el inicio de sesión de Facebook, cabe señalar, que no todas las páginas requieren la misma cantidad de trabajo, el código se puede crear manualmente desde cero o generar mediante herramientas de clonación, ambas opciones con sus pros y contras; la clonación brinda acceso a una plantilla más rápidamente, pero debido a la longitud del código, la modificación puede ser más difícil y compleja, por el contrario, crear una plantilla manualmente brinda un mayor control pero requiere amplios períodos de tiempo y extensos conocimientos en el desarrollo de software.

Imagen 1

Sitio web falso

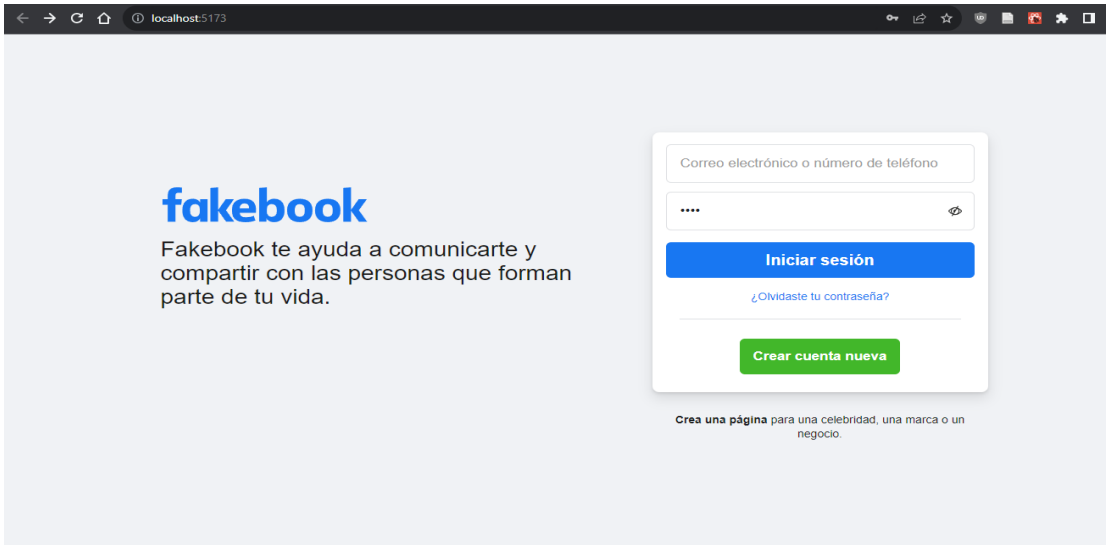
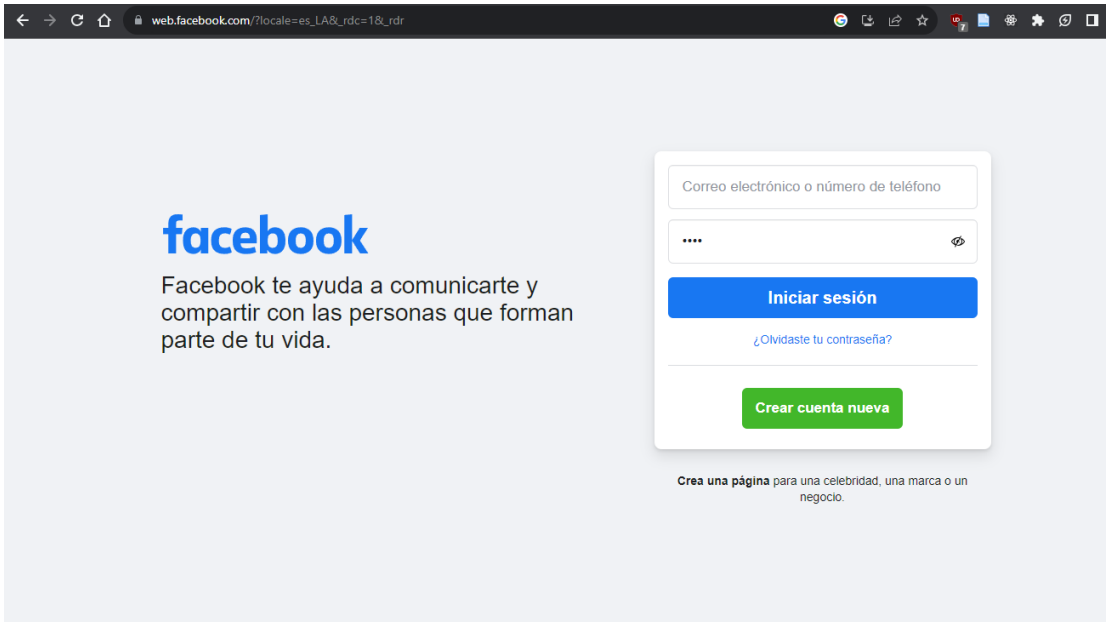


Imagen 2

Sitio web original



Segunda Etapa:

En esta etapa se evaluó el tipo de ataque que podría lanzarse dado que el objetivo puede ser específico o generalizado, el phishing se caracteriza por ser un conjunto de técnicas versátiles, que se pueden integrar para obtener un ataque más robusto y sofisticado, en el caso de este laboratorio se realizó un ataque especifico teniendo en cuenta las diferentes técnicas que podrían ser más adecuadas.

En un ataque generalizado se utiliza con frecuencia la ingeniería social y el cebo normalmente se despliega a través de un mensaje que se puede recibir por correo electrónico o mensaje de texto; también es común que el asunto del mensaje sea alarmista o urgente, solicitándole a las víctimas que hagan clic en enlaces que conducen a la URL del sitio web falso.

En un ataque específico, el objetivo o víctima es alguien en particular, debido a esto es común el uso de técnicas determinadas como man in the middle (MITM), DNS cache poisoning (DNS Spoofing), uso de spyware como keyloggers o malware de diversos tipos que permiten monitorear y/o enviar directamente la información al atacante.

Imagen 3

Esquema MITM

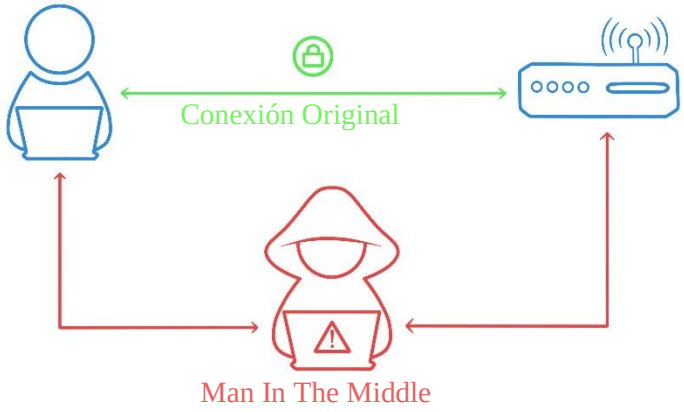


Imagen 4

Esquema DNS Spoofing

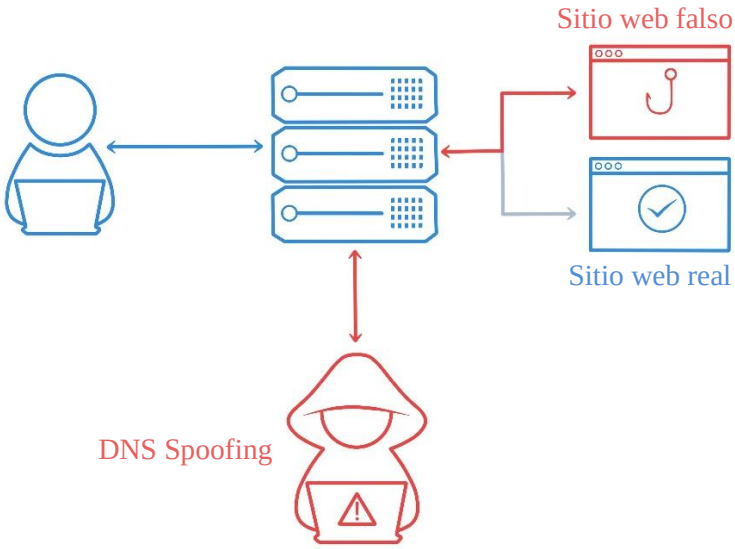
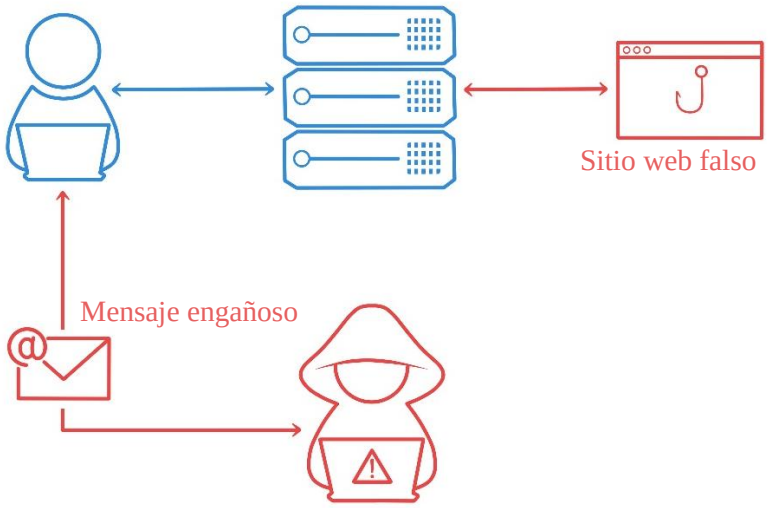


Imagen 5

Esquema mensaje engañoso



Tercera etapa:

Para esta etapa se emplearán las técnicas de man in the middle (MITM) y el DNS cache poisoning (DNS Spoofing) debido a que el tipo de ataque definido en la anterior etapa fue el dirigido o específico.

DNS Spoofing

El DNS SPOOFING consiste en redireccionar a un usuario víctima de este ataque a un sitio web falso que no es el mismo que él quiere acceder, pero que tiene el mismo nombre de dominio del sitio que el usuario desea visitar. Existen dos variantes de este ataque que son:

Cache poisoning (Envenenamiento de la caché): Se basa en modificar la información contenida en un servidor de dominios, es decir que el atacante redirecciona las peticiones que hace un usuario a un dominio llamémoslo “X” a un dominio distinto “Y” para crear así un tipo de cortina de humo en donde el usuario proporciona las peticiones al atacante en el sitio web real “X” pero estas llegan al sitio falso “Y”.

Para esto el atacante debe estar conectado al servidor y red del usuario víctima en donde tendrá acceso para revisar todos los paquetes y peticiones que el usuario haga en un dominio, crea así un registro DNS falso en el servidor con el cual va a desviar la dirección IP a un dominio falso. Luego el atacante envía una petición al dominio verídico para que el usuario víctima proporcione datos sensibles y que estos registros lleguen a su DNS falso y sean guardados en la caché. (Pastor Iglesias, 2022)

ID Spoofing: Esta alternativa es básicamente hacer creer al usuario víctima que la máquina del atacante es un servidor DNS que captura el ID del UDP (User datagram protocol) el cual “es un protocolo orientado a las transacciones, y la entrega y la protección contra duplicados no están garantizados” (Pastor Iglesias, 2022, p. 8).

Siendo uno de los protocolos de internet que permiten enviar información sin la necesidad de tener un receptor ni esperar una respuesta, haciéndolo uno de los protocolos más rápidos y sin retardos.

El ID Spoofing directamente conecta al usuario víctima, al dominio falso y le hace creer que están conectados al dominio verídico al que se quiere acceder.

Man in the middle

MITM: Se refiere a Man In the Middle que al español traduce como Hombre en el Medio, lo cual se refiere a un ciberataque en el atacante se sitúe entre medias de dos partes que intentan comunicarse para interceptar sus mensajes o datos. Los principales objetivos de estos ataques son obtener datos bancarios o credenciales de inicio de sesión, por ejemplo, ya que es como pueden sacarle más rentabilidad. Al ser en tiempo real estos ataques suelen pasar inadvertidos hasta que es demasiado tarde (Martínez Pérez, 2022).

Imagen 6

MITM

Ip de la puerta de enlace y su MAC

```
Interfaz: 192.168.[redacted] --- 0xd
  Dirección de Internet          Dirección física      Tipo
  192.168.[redacted].1           f0-63-[redacted]      dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
```

Dispositivo del atacante suplantando la Ip de la puerta de enlace

```
Interfaz: 192.168.[redacted] --- 0xd
  Dirección de Internet          Dirección física      Tipo
  192.168.[redacted].1           94-de-[redacted]      dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
```

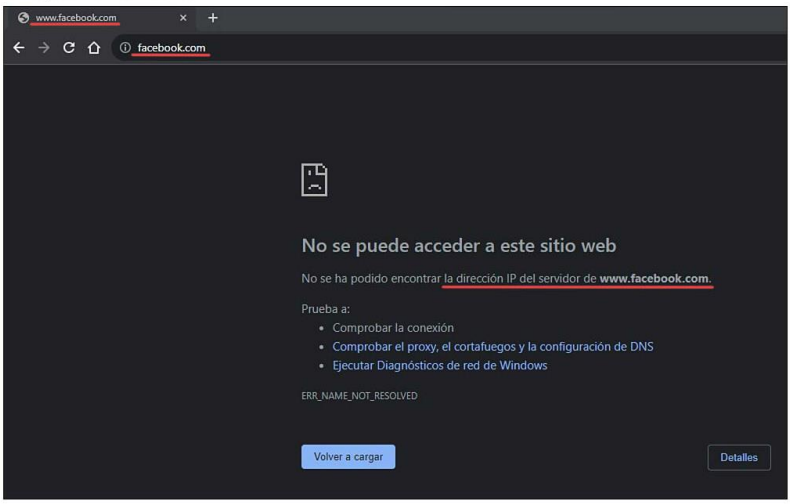
Imagen 7

DNS Spoofing

Dominio original con Ip modificada

```
###[ DNS ]###
        length    = 79
        id        = 62627
        qr        = 1
        opcode    = QUERY
        aa        = 0
        tc        = 0
        rd        = 1
        ra        = 1
        z         = 0
        ad        = 0
        cd        = 0
        rcode     = ok
        qdcount   = 1
        ancount   = 1
        nscount   = 0
        arcount   = 0
        \qd        \
         |###[ DNS Question Record ]###
         |  qname     = 'www.facebook.com.'
         |  qtype     = A
         |  qclass    = IN
        \an        \
         |###[ DNS Resource Record ]###
         |  rrname    = 'www.facebook.com.'
         |  type      = A
         |  rclass    = IN
         |  ttl       = 0
         |  rdlen     = None
         |  rdata     = 192.168.1.100
        ns        = None
        ar        = None
```

Navegador de la victima



En la imagen 6, se pueden observar dos screenshots que fueron tomadas desde la consola del sistema operativo Windows de la víctima, donde se observa el cambio de la dirección MAC asociada a la primera dirección IP que corresponde a la puerta de enlace de la red, esto indica que el dispositivo del atacante esta en medio de la comunicación y suplanta la IP de la puerta de

enlace, es por esa razón que la MAC es distinta, ya que esta corresponde a la MAC del dispositivo del atacante.

Para la imagen 7, se tienen dos screenshots igualmente, la primera corresponde a la terminal del atacante, aquí se observa la información del paquete recibido con el dominio real de Facebook y una IP modificada por el atacante asociada a este dominio, esta IP no lleva a ningún sitio web en realidad, por otro lado la segunda imagen muestra lo que ocurre en el navegador de la víctima, la URL es original pero devuelve un error ya que la IP alterada no se encuentra en internet, sin embargo si esa IP estuviera asociada a un dominio que contenga la página de phishing la víctima seria redireccionada allí.

Cuarta etapa:

Para obtener las credenciales en esta etapa final se creó el backend que estará conectado al inicio de sesión de "Fakebook", también se implementaron un MITM y un DNS Spoofer, como parte del ataque para interceptar la comunicación en una red local y redirigir a la víctima al sitio web falso, que tendrá la misma URL que la página original, una vez enviada la información al back la víctima será dirigida al inicio de sesión de la página suplantada de manera que para el usuario parecerá un error de digitación en sus credenciales.

Imagen 8:

Envío de formulario

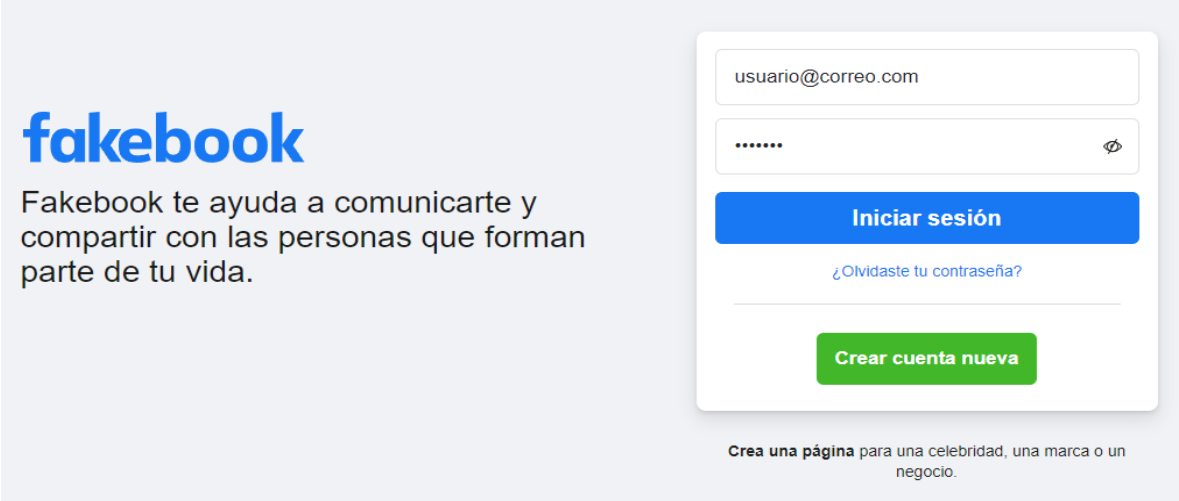
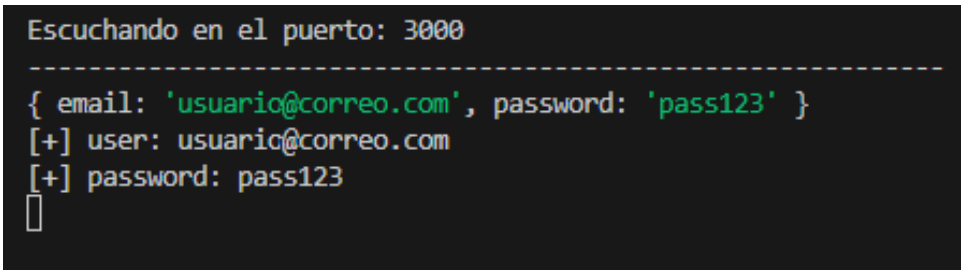


Imagen 9:

Datos recibidos por el Back-end



Resultados

En el proceso realizado en el artículo, el ataque está focalizado sobre una víctima en específico, por lo general los ataques en su mayoría suelen ser generalizados y es por ello por lo que las pautas para identificar este tipo de fraudes cambian con respecto al objetivo de los atacantes, debido a la variedad de los medios y la ingeniería social aplicados para captar a la víctima, sin embargo, existen algunos procesos que se emplean en la mayoría de los casos.

Dicho esto, se empieza con los ataques dirigidos, estos son los más difíciles de identificar debido a que actúan sobre una o un grupo de víctimas específicas, normalmente los ataques de phishing que usan técnicas de persuasión e ingeniería social enfocados a los temas de interés de la víctima se conocen como spear phishing, añadido a esto las técnicas empleadas en el fraude son más complicadas de detectar y requieren un mayor cuidado, como se logra observar en el desarrollo del laboratorio la URL es la misma que la del sitio web suplantado, lo que hace el proceso de identificación a simple vista sea inútil, es necesario el uso de software y herramientas especializadas que permitan identificar la IP asociada al dominio o monitorear los paquetes de la red para visualizar una trazabilidad, la identificación de este tipo de ataques la podría seccionarse de acuerdo a las diferentes partes del phishing la primera: el cebo, la segunda: el anzuelo, tercera: la captura.

La primera: el cebo, lo primero a tener en cuenta es que siempre hay un contacto inicial del atacante con la víctima, los medios más recurrentes son los correos electrónicos, SMS o llamadas telefónicas, es importante no dar

información privada usando estos medios sin cerciorarse que se tratan de canales de comunicación confiables en el caso de los SMS es difícil identificar su legitimidad, existen servicios de mensajería que permiten enviar mensajes personalizando el remitente y el cuerpo de mensaje, para los atacantes es tan simple como redactar de manera creíble un mensaje con un remitente solicitando la apertura de algún enlace para iniciar sesión, realizar el cambio de contraseña o simplemente solicitando al usuario que acceda por un motivo en específico relacionado con la cuenta, las recomendaciones en este tipo de casos son las siguientes:

- No acceder a enlaces desde medios de comunicación que no sean los oficiales.
- Revisar que el cuerpo del mensaje no tenga incoherencias o problemas de redacción, esto dependerá de lo descuidado que sea el atacante, en los ataques más generalizados suele ser habitual encontrar inconsistencias.
- No abrir ni descargar documentos adjuntos sin asegurarse de la originalidad del remitente o hacerlo directamente desde las fuentes oficiales.
- Revisar a quien va dirigido el mensaje, en los ataques generalizados se referirán a la víctima sin usar su nombre, sustituyéndolo por señor usuario o usted.

La segunda: el anzuelo, una vez que se accede a este tipo de mensajes, ya sea porque la víctima paso por alto los detalles de inconsistencia o por negligencia, en el caso de descargar archivos adjuntos de dudosa procedencia lo recomendable es tener los servicios de antivirus actualizados, de forma que si estos detectan que los archivos no son inofensivos evitara la ejecución de procesos que puedan poner en peligro la integridad de la información del dispositivo o su funcionalidad, adicional a esto si el enlace realiza un redireccionamiento como en el laboratorio, se recomienda ingresar datos erróneos, muchos de los ataques de phishing redireccionan a la página real una vez se realiza el registro de los datos, recordar que su objetivo es robar las

credenciales y no validar si estas son correctas o no, teniendo en cuenta la información anterior las recomendaciones son las siguientes:

- Tener antivirus y sistemas operativos actualizados en los dispositivos para evitar todo tipo de malware, en caso de descargar archivos sospechosos.
- Digitar datos erróneos la primera vez que se ingresa al sitio web y estar atento al comportamiento de la página, si es phishing habrá un redireccionamiento, es decir parecerá que la página se recargó de nuevo, si es legítima vera errores de inicio de sesión típicos, las páginas de phishing no realizan validaciones.
- Verifique desde otro dispositivo el sitio web oficial de su cuenta y compare si existen diferencias notables, esto es algo que no es 100% efectivo, la similitud de la página dependerá del trabajo empleado por el atacante.
- Verificar la URL y si el sitio es seguro o no, los navegadores representan esto con un candado antes de la URL, hay una gran variedad de técnicas para que la URL sea igual a la original, algunas más complejas que otras, pero es un detalle a tener en cuenta.

La tercera: la captura, en esta última hay que tener en cuenta que las acciones ya no son preventivas si no reactivas, se da por hecho que el atacante ya tiene las credenciales así que las recomendaciones son las siguientes:

- Tener activa la verificación en dos pasos en todas sus cuentas, en caso de que su contraseña y usuario sea obtenida por el atacante la doble verificación impedirá el acceso.
- Si recibe notificaciones de la verificación en dos de sus cuentas, sin intentar acceder a su cuenta, es probable que el atacante este intentando acceder, cambie las credenciales y deniegue todo intento de acceso que no sea solicitado por usted mismo.

Conclusiones

A modo de conclusión, el phishing es un problema muy extendido que engloba un conjunto de métodos que incorporan varias disciplinas relacionadas con los

sistemas de información, dándole un grado de versatilidad que hace que sea difícil de detectar, en este artículo se toman un grupo de técnicas específicas para demostrar justamente cómo funcionan este tipo de fraudes y sus falencias, a pesar de su versatilidad y complejidad, no siempre tiene éxito, debido a que explota el desconocimiento de los usuarios, es indudable que la capacitación y la divulgación de pautas para identificar el phishing son indispensables para la mitigación del mismo, las pautas formuladas en este artículo se basan en el laboratorio donde se realizó el proceso de phishing en un entorno local, incluyendo pautas para los ataques más generalizados, ya que estos tienen como objetivo alcanzar a la mayor cantidad de usuarios posibles, lo que da paso a fallos identificados en la sección de resultados del presente artículo.

Referencias bibliográficas

Baca Urbina, G. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria. https://books.google.com.ec/books?id=IhUhDgAAQBAJ&printsec=copyright#v=onepage&q&f=false

Belisario Méndez, A. N. (2014). *Análisis de Métodos de Ataques de Phishing*. [Trabajo final de Carrera, Universidad de Buenos Aires]. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0840_BelisarioMendezAN.pdf

Hernández Dominguez, A. y Baluja García, W. (2021). Principales mecanismos para el enfrentamiento al phishing en las redes de datos. *Revista Cubana de Ciencias Informáticas, 15*(1), 413-441. http://scielo.sld.cu/pdf/rcci/v15n4s1/2227-1899-rcci-15-04-s1-413.pdf

Internet Crime Report 2021_IC3Report.pdf. (2021). *Federal bureau of investigation.* https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Ley 1273 de 2009. Normatividad sobre delitos informáticos. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Martínez Pérez, F. J. (2022). *Análisis de los ciberataques. El ataque Man-in-the-middle y el SSLSTRIP* [Tesis final de grado, Universidad Politécnica de Madrid]. https://oa.upm.es/76147/1/TFG_FRANCISCO_JAVIER_MARTINEZ_PEREZ.pdf

Pastor Iglesias, R. (2022). *Análisis actual de los Ataques Man-In-The-Middle por DNS Spoofing* [Trabajo final de grado, Universidad Politécnica de Madrid]. https://oa.upm.es/71578/1/TFG_RAUL_PASTOR_IGLESIAS.pdf

Conflicto de intereses

Los autores declaran no tener conflictos de intereses.

Contribución de los autores

C.C.B.B.: Escritura y redacción del artículo, estructuración y la expresión de las ideas, la recopilación de datos y el análisis de estos.

S.A.E.V.: Revisión de la literatura. Recopiló datos.