REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMÁTICA

CÁTEDRA: CIBERSEGURIDAD

INGENIERÍA SOCIAL POR EMAIL PHISHING COMO DESENCADENANTE DE GRANDES AMENAZAS PARA LAS ORGANIZACIONES

Profesora:

Francis Ferrer Zapata

Equipo N ° 2:

Francis Bompart	C.I: 29 686 086
Gabriel Delgado	C.I: 29 553 027
Ángel Hernández	C.I: 27 222 633
Arturo Hung	C.I: 29 621 867
Javier Rojas	C.I: 28.472.023
Germán Oropeza	C.I: 27 660 324

Caracas, 14 de enero de 2024

TABLA DE CONTENIDO

INTRODUCCIÓN

Con la irrupción de la Cuarta Revolución Industrial en pleno siglo XXI, se ha desencadenado una serie de avances tecnológicos que han transformado radicalmente la forma en que las personas trabajan y se relacionan con su entorno. Este fenómeno ha dado lugar a la digitalización y al surgimiento del internet, que actualmente se ha consolidado como el medio de comunicación universal de toda la humanidad. Desde el correo electrónico y la mensajería instantánea hasta los servicios web y la tendencia hacia la automatización mediante la descentralización de la información en servicios en la nube y la implementación de la inteligencia artificial, estos cambios han redefinido la manera en que el hombre lleva a cabo sus tareas cotidianas.

Lo anterior, alineado a ello con la ocurrencia de una pandemia mundial en los últimos años, ha hecho que empresas hagan que su personal adopte un modelo de trabajo orientado hacia la flexibilidad, permitiéndoles que utilicen equipos propios para desempeñar sus cargos (*Bring Your Own Device* - BYOD), surgiendo con ello una amplia variedad de canales de comunicación creados con el uso de herramientas de colaboración con soporte computacional, que en sí representan nuevas amenazas para la seguridad de la información. Uno de los riesgos más potenciales que se presentan con dicho cambio de paradigma laboral son los ataques de ingeniería social, los cuales implican llevar a cabo la manipulación del comportamiento humano para así obtener acceso no autorizado a datos con fines no éticos.

En ese contexto, uno de los ataques de ingeniería social más conocidos es el phishing, el cual consiste en el intento de adquirir información sensible o persuadir a alguien para que actúe

de la manera deseada, haciéndose pasar por una entidad de confianza en un medio de comunicación digital. Este tipo de ataque representa una grave amenaza debido a su prevalencia y al impacto significativo que puede tener en la seguridad de la información, especialmente en lo que respecta a la autenticidad de las partes involucradas.

Un ejemplo destacado de la magnitud al cual pueden llegar este tipo de ataques ocurrió en marzo de 2022 con el juego P2E (Play-to-Earn) del metaverso criptográfico Axie Infinity, desarrollado por Sky Mavis. Este incidente es considerado el mayor *hacking* en la historia de las finanzas descentralizadas, donde un grupo de ciberatacantes de Corea del Norte conocido como Lazurus, se hicieron pasar por reclutadores de la plataforma de empleo LinkedIn, engañando a un ingeniero senior de Sky Mavis para que participara en un proceso de entrevistas falsas para un puesto de trabajo. Posteriormente, le hicieron llegar por correo electrónico una carta de oferta con un paquete de compensación generoso, a través de un archivo PDF que tenía consigo un *spyware* incrustado (Weeks, 2022).

Al descargar el documento, el spyware permitió a los criminales acceder a la red blockchain de Axie Infinity, conocida como Ronin, donde los usuarios realizaban transferencias de criptomonedas basadas en Ethereum dentro y fuera del juego. Utilizando las firmas de los nodos comprometidos, el Grupo Lazarus logró retirar alrededor de 173.600 ETH y 25,5 millones de USDC, totalizando así un robo de 625 millones de dólares. Dos tercios de los fondos robados pertenecían a usuarios, mientras que el resto constituía la tesorería de ingresos de Axie Infinity. Este ataque al puente Ronin se describe como un compromiso de múltiples firmas y pasó desapercibido en la infraestructura de la compañía durante seis días (Kshetri, 2023).

Durante el desarrollo de este documento, se abordará un caso de estudio detallado sobre un ataque de ingeniería social, específicamente centrado en la captura de información a través del uso de computadoras, como es en el caso de la técnica del phishing. Asimismo, se examinarán aspectos como la modalidad de la amenaza, la anatomía del ataque, su potencial impacto en una organización propuesta, las herramientas y métodos utilizados, las vulnerabilidades explotadas y estadísticas relevantes. Además, se analizará el impacto del daño en la seguridad y privacidad, se propondrán acciones de remediación técnica y organizativa, y se ofrecerán recomendaciones para fortalecer la resiliencia organizacional frente a este tipo de amenazas.

DECLARACIÓN DEL PROBLEMA

Según el reporte anual de Verizon referente a las investigaciones por fugas de datos (DBIR), se registró que el 92% de las empresas en Estados Unidos, Reino Unido, Canadá, Australia y Alemania experimentaron al menos un ataque de ingeniería social en el 2022. El costo promedio de cada incidente fue de más de $2 millones, lo que convierte a ataques de esta índole en la principal amenaza en materia de seguridad informática a día de hoy.

A raíz del auge de la digitalización y la adopción de modelos de trabajo flexibles, la amenaza de ataques de ingeniería social, en particular mediante técnicas de phishing, se ha intensificado. Este fenómeno se convierte en una seria preocupación para las organizaciones, ya que los atacantes continúan ideando nuevos modus operandi con el objetivo de explotar la confianza de los individuos, obteniendo así acceso no autorizado a información sensible o manipulando a las personas para que realicen acciones no deseadas.

Dicho cambio ha generado nuevas oportunidades para el phishing, contribuyendo al aumento de casos de este tipo de ataques de ingeniería social asistidos por computadora. En ese contexto, en un informe publicado por Proofpoint Threat Insights en el transcurso de este año, se registró un incremento del 18% en los ataques bajo esta categoría en comparación con el año anterior, resaltando que la modalidad de ataque dirigido a organizaciones e individuos (*spear-phishing*) es la más prevalente dentro de esta clasificación.

A medida que los sistemas de seguridad se vuelven más sofisticados para prevenir este tipo de amenazas, el phishing también evoluciona en complejidad (Bitaab, 2020). Los atacantes

ya no dependen únicamente de la trivial técnica de enviar correos electrónicos de forma masiva (SPAM) a diversas direcciones para inducir y engañar a los usuarios a que realicen acciones inseguras. De acuerdo a lo comentado por Hong en el año 2021, la labor de los ciberdelincuentes (*phishers*) no solo se ha adaptado a esta serie de nuevas metodologías, sino que también ha conseguido facilitarse con el desarrollo de kits de phishing: software moderno capaz de crear automáticamente copias engañosas de redes sociales o sitios web populares. Inclusive, el uso de alfabetos locales en los dominios de Internet ha generado una vulnerabilidad que puede ser aprovechada mediante el uso de técnicas de phishing (Workspace, 2021). Esta situación destaca la importancia de abordar y comprender la complejidad asociada con el uso de caracteres específicos en los nombres de dominio, lo cual puede ser explotado por los atacantes para llevar a cabo esta clase de ataques de ingeniería social de forma más efectiva y personalizada.

El fenómeno del phishing ha sido objeto de numerosos informes en los últimos años, destacando un método en el que los ciberatacantes se hacen pasar por entidades legítimas para engañar a las personas y obtener información confidencial. Según reportajes de medios como CBS News o Business Insider, se ha observado un aumento en la actividad criminal en la plataforma de comercio electrónico de Amazon. Los estafadores han empleado tácticas como llamadas telefónicas y correos electrónicos fraudulentos para intentar obtener acceso a las cuentas de los clientes (Cerullo, 2023).

En particular, los mensajes de correo electrónico falsos suelen ser engañosos, indicando la suspensión de la cuenta del usuario o bien, felicitándolo con una tarjeta de regalo o una prueba gratuita de su servicio de Amazon Prime (Amazon Web Services, s. f.).

Considerando lo previamente establecido, surge la imperiosa necesidad de evaluar los actuales mecanismos de ataque, con el propósito de identificar y destacar no solo los fallos que podrían ser aprovechados por los atacantes, sino también para identificar posibles vulnerabilidades que podrían ser objeto de explotación y, en consecuencia, proponer estrategias efectivas de mitigación.

OBJETIVOS

OBJETIVO GENERAL

1. Evaluar las vulnerabilidades explotadas y llevar a cabo la simulación del ataque, así como los riesgos asociados a la seguridad de la información, por parte de los ataques spear-phishing y pharming desencadenados por el email phishing.

OBJETIVO ESPECÍFICOS

1. Determinar el perfil del objetivo normalmente susceptible a este tipo de ataque, en conjunto del ambiente virtual que permitirá realizar la simulación.

2. Diseñar el ataque con el uso de diferentes herramientas para la suplantación de sitios web y envío de emails falsos, todo esto en función de los objetivos establecidos que representan la información confidencial a comprometer

3. Efectuar el ataque.

4. Medir el nivel de efectividad del ataque en base a las metas establecidas en el objetivo dos.

ANATOMÍA DEL ATAQUE

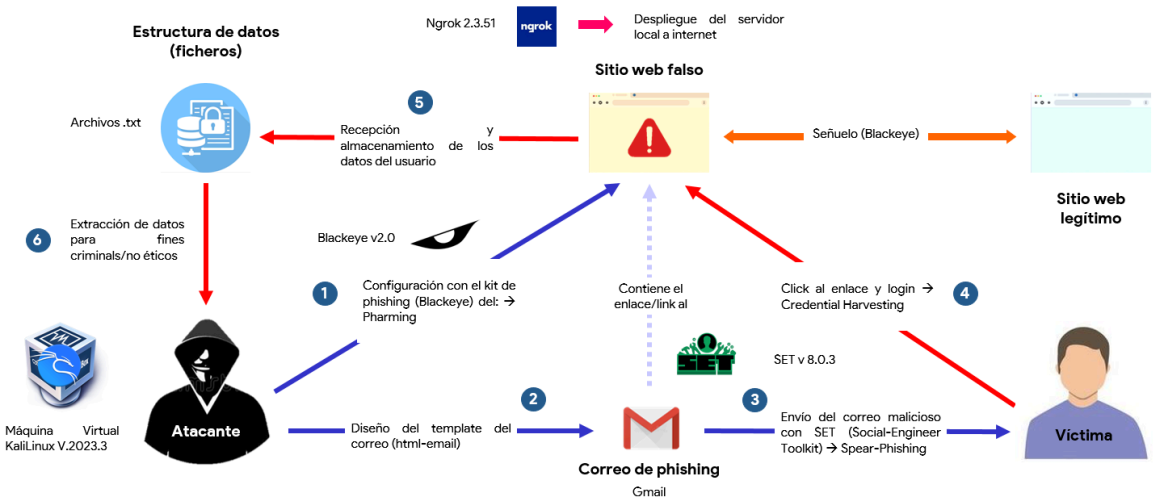

Figura 1. Anatomía del ataque de phishing propuesto

Del esquema anterior, se explican a continuación cada uno de los elementos descritos en la anatomía del ataque propuesto:

1. **Pharming:** Durante la ejecución de esta etapa, se lleva a cabo la creación del sitio web falsos haciendo uso del kit de phishing del cual se dispone. En este caso, se emplea Blackeye, una herramienta que permite realizar ataques de phishing a un determinado objetivo, y que a su vez cuenta con un apartado de plantillas (*templates*). Lo anterior facilitará el poder ejecutar en primera instancia un pharming, un ataque que consiste en redirigir el tráfico de un sitio o página web legítima a un señuelo (versión falsa) del mismo sin que el usuario(víctima) tenga conocimiento de ello.

   Para llevar a cabo esta acción, se despliega el servidor local configurado en la máquina del atacante usando Ngrok, a través de Internet. Esto permite alojar

temporalmente el sitio web falso creado para ejecutar el phishing. La configuración de este servidor local es esencial para asegurar que el usuario objetivo sea redirigido al sitio falso de manera efectiva sin levantar sospechas

2. **Diseño del correo malicioso**: En esta fase, se procede a diseñar un correo malicioso con el propósito de engañar al objetivo, que tendrá el link a la página web falsa. Para llevar a cabo este diseño, se utilizará una plantilla configurada en HTML y la herramienta empleada para este proceso es el Social Engineer Toolkit (SET), la cual permite enviar el documento ya sea en formato de texto plano o en HTML. Se optará por este último formato al simular un mensaje corporativo (en este caso, de una compañía como lo es Amazon. Igualmente, el diseño del correo también considerará datos relevantes del contexto del objetivo para aumentar su credibilidad.

3. **Spear-phishing**: Se procede con la fase de spear-phishing mediante el envío del correo malicioso al objetivo seleccionado. En este caso, al tratarse de un ataque específico dirigido a un único usuario, se configura un ataque de spear-phishing utilizando las opciones disponibles en el Social Engineer Toolkit (SET). El spear-phishing implica la personalización del ataque para adaptarse al destinatario específico, aumentando así la probabilidad de éxito

4. **Credential Harvesting:** Tras el envío del correo, se aguarda a que el usuario abra el mensaje y acceda al enlace, que está discretamente integrado en el diseño del template. Al hacer clic en dicho enlace, el usuario será redirigido a una página web fraudulenta que simula un formulario de inicio de sesión. En este formulario, se llevará a cabo la recopilación de sus credenciales de acceso, incluyendo correo electrónico, nombre de usuario y contraseña. Este proceso específico se conoce con el nombre de *Credential Harvestin*g.

5. **Recepción y almacenamiento de los datos del usuario:** Después de que el usuario complete el formulario de registro en la página falsa, será redirigido a la página web legítima para llevar a cabo el proceso genuino. Sin embargo, sus credenciales ya han sido capturadas por el atacante y almacenadas en una estructura o base de datos correspondiente. En este caso, al utilizar Blackeye, los datos se guardan tanto de forma individual como colectiva en archivos de texto (txt).

6. **Extracción y uso de datos para fines criminales/no éticos:** En la etapa final, una vez que se han capturado todos los datos del usuario, que incluyen no solo la dirección de correo electrónico y la contraseña, sino también la dirección IP, la ubicación geográfica desde la cual se realizó la solicitud de ingreso a la página, el proveedor de servicios de Internet (ISP) e incluso el navegador web y el sistema operativo de la máquina desde la cual se conecta; el atacante está en condiciones de tomar posesión de la identificación del usuario. Estos datos recopilados son valiosos para el atacante y pueden ser utilizados con fines criminales o no éticos, comprometiendo la seguridad y privacidad del individuo afectado.

Ataques derivados del Phishing

Derivación Directa (Variantes del Phishing)

- **Spear-phishing:** El spear-phishing es una forma dirigida de phishing en la que los atacantes personalizan sus mensajes engañosos para un individuo, organización o grupo de personas específicos. A diferencia del phishing comúnmente conocido, caracterizado por el envío masivo de correos maliciosos, esta variante implica una investigación mucho más cuidadosa sobre el objetivo para hacer que los mensajes sean más convincentes y/o creíbles. El atacante puede utilizar información personal, roles laborales o eventos recientes relevantes para aumentar la probabilidad de éxito de su ejecución.

- **Smishing:** El smishing es una variante de phishing que se realiza a través de SMS o mensajes de texto en dispositivos móviles. De igual forma, los mensajes son utilizados para engañar a individuos y hacer que proporcionen información sensible o hagan clic en enlaces malicioso; aunque al ser de carácter instantáneo y de elaboración sencilla, llevan consigo un sentido de urgencia arraigado, creando con ello la necesidad de una acción inmediata por parte de la víctima.

- **Vishing**: El vishing, o Voice Phishing, implica el uso de llamadas de voz para engañar a las personas y obtener información confidencial. Los atacantes suelen hacerse pasar por entidades legítimas, como bancos, centros de llamadas (*call centers*) o agencias gubernamentales, bien sea directamente desde una llamada telefónica o mensajes de audio.

- **Whaling:** Es un tipo específico de spear-phishing que apunta a individuos de alto perfil/rango o ejecutivos dentro de una organización, para así obtener ganancias potencial y significativamente más altas que aquellas que se pueden obtener de un objetivo común.

Derivación Indirecta

- **Pharming:** En lugar de depender de la interacción directa con los usuarios, como en el phishing tradicional, el pharming es una especie de ciberataque que busca comprometer la infraestructura de red para dirigir a los usuarios a sitios web fraudulentos sin su conocimiento.
- **Credential Harvesting:** Comprende un proceso de recopilación sistemática de información de inicio de sesión y otros datos confidenciales de usuarios sin su conocimiento o consentimiento. En ese orden de ideas, para realizar dicho proceso de recolección de credenciales, se emplean diversas técnicas entre las que se menciona el uso de malware, keyloggers o phishing, para así lograr tener acceso no autorizado a cuentas protegidas.
- **DNS Hijacking:** El secuestro de DNS implica manipular o modificar el proceso de resolución de DNS para redirigir a los usuarios desde sitios web legítimos a sitios maliciosos. Este ataque compromete servidores DNS o altera la configuración en routers, switches o el dispositivo del usuario para tener control sobre las consultas en ese sistema; y a diferencia del pharming, este enfoque se centra específicamente en manipular el sistema de nombres de dominio para modificar el proceso de resolución, sin incluir técnicas adicionales.

VULNERABILIDADES A EXPLOTAR

Según MITRE ATT&CK ®, la cual es una base de conocimiento globalmente accesible sobre tácticas y técnicas utilizadas por los actores adversarios al mundo de la ciberseguridad, existen ciertas acciones maliciosas que se presentan a los largo del ciclo de vida de un ataque. Este marco integral abarca desde las fases iniciales de acceso hasta la persistencia.

Sin embargo, nos enfocaremos en dos grupos de técnicas críticas que destacan en el impacto y la manipulación de credenciales, aspectos fundamentales en la estrategia de phishing y las consecuencias asociadas.

1. Impacto:

El primer grupo, denominado “Impacto”, se centra en la capacidad del adversario para afectar directamente a una organización, ya sea a través de acciones destructivas, como la eliminación de datos críticos o la desactivación de sistemas claves. Este tipo de ataques pueden tener consecuencias significativas, no sólo en términos de pérdidas de información y funcionalidad, sino también en la reputación y la confianza de la organización afectada.

Técnicas Implementadas

Identificación	Nombre	Descripción
T1657	Robo financiero	Los actores maliciosos buscan obtener beneficios financieros a expensas de sus objetivos, empleando diversas estrategias como la extorsión, la ingeniería social, el robo técnico u otros métodos. Su objetivo principal es la extracción de recursos monetarios, y este propósito se materializa a través de tácticas comunes como la extorsión mediante ransomware, el compromiso y el fraude por correo electrónico.
T1531	Eliminación de acceso a la cuenta	Los actores maliciosos tienen la capacidad de afectar la disponibilidad de los recursos del sistema y redes al obstruir los accesos a las cuentas utilizadas por los usuarios autorizados. Los mismos pueden llevar a cabo acciones como la eliminación, bloqueo o manipulación de cuentas, tales como cambiar las credenciales con el fin de restringir el acceso futuro al sistema.

Tabla 1. Técnicas implementadas con vulnerabilidades de Impacto

2. Acceso a credenciales:

El segundo grupo, “Acceso a credenciales”, se enfoca en el intento del adversario de robar nombres de cuentas y contraseñas, lo cual no solo le proporciona el acceso no autorizado a sistemas, sino que también actúa como un medio para operar de manera sigilosa. Esta discreción dificulta la detección y brinda a los atacantes la oportunidad de crear nuevas cuentas, contribuyendo así a alcanzar sus objetivos de manera más efectiva.

Técnicas Implementadas

Identificación	Nombre	Descripción
T1187	Autenticación forzada	Los actores maliciosos pueden recopilar las credenciales invocando u obligando a un usuario a proporcionar automáticamente información de autenticación a través de un mecanismo que puedan para poder lograr la intersección de la data de autenticación.
T1056	Captura de entrada	Los actores maliciosos pueden utilizar métodos para capturar la información del usuario para obtener credenciales o recopilar información. El usuario hace uso normal del sistema, proporcionando credenciales dentro de formularios de páginas/portales de inicio de sesión, sin darse cuenta de que su información está siendo captada por el atacante.

Tabla 2. Técnicas implementadas con vulnerabilidades de acceso a credenciales

IMPACTO

El phishing, como técnica de ciberataque, tiene como impacto significativo y generalizado en la seguridad de la información a nivel global. Esta amenaza se manifiesta de diversas formas, comprometiendo la confidencialidad, integridad y disponibilidad de datos tanto a nivel personal como organizacional. Algunos de los impactos más relevantes incluyen la pérdida financiera, la violación de la provacdad, la propagación de malwares y la afectación de la confianza en línea.

En términos de pérdida financiera, el phishing busca explotar la confianza de los usuarios para obtener información sensible, como datos bancarios y contraseñas. Esto puede conducir a transacciones tanto para individuos como para empresas. Además, los ataques de phishing también pueden tener consecuencias legales, ya que las víctimas pueden ser responsables de actividades delictivas realizadas con sus credenciales comprometidas.

La violación de la privacidad es otro impacto importante del phishing, ya que los atacantes buscan obtener información personal y confidencial. Esto puede incluir datos de identificación, números de seguro, información médica y otros detalles sensibles. La exposición de esta información puede tener consecuencias graves, como el robo de identidad y la suplantación de cuentas.

La propagación de malwares es una consecuencia común del phishing, ya que los enlaces maliciosos y los archivos adjuntos fraudulentos pueden contener software malicioso. Una vez que un usuario hace clic en un enlace o descarga un archivo infectado, el malware puede

comprometer la seguridad de todo el sistema, permitiendo a los atacantes acceder y controlar dispositivos, robar información adicional o incluso utilizarlos para lanzar ataques más amplios.

La confianza en línea también se ve afectada negativamente por el phishing, ya que los usuarios pueden envolverse más cautelosos y desconfiados al interactuar en línea. La pérdida de confianza puede tener un impacto duradero en la adopción de servicios en línea, transacciones electrónicas y la participación en plataformas digitales.

Por lo cual podemos afirmar que el phishing no solo representa una amenaza para la seguridad de la información, sino que también tiene repercusiones económicas, legales y sociales. La concienciación, la educación y la implementación de medidas de seguridad sólidas son esenciales para mitigar estos impactos y proteger la integridad del entorno digital.

ESTADÍSTICAS

Áreas más afectadas

Según el informe APWG de 2021, los ataques de phishing alcanzaron un máximo histórico en 2021, con más de 300.000 ataques registrados solo en diciembre. Esto representaría un aumento significativo en la frecuencia de estos incidentes, que se han triplicado en menos de dos años. En donde las industrias más afectadas en ese periodo fueron las siguientes:

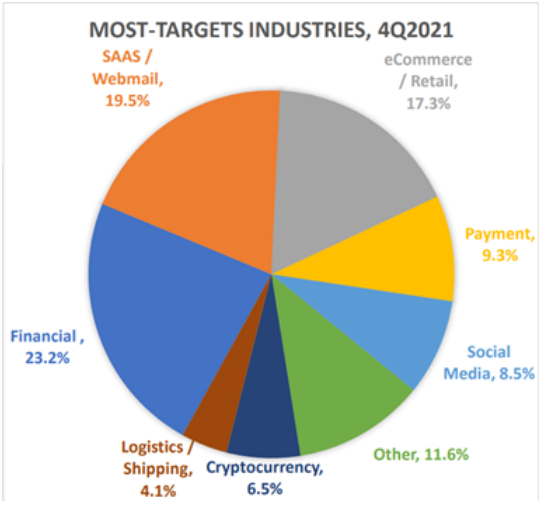

Figura 2. Gráfico - Industrias mas atacadas por phishing

Siendo el área financiera la más afectada por ataques de phishing en comparación con las otras en ese año.

También en dicho periodo se detectó un aumento de los ataques en el mes de diciembre logrando una cantidad de 316,747 ataques en el periodo de diciembre de 2021 siendo el mayor mes de dicho año con una mayor cantidad de ataques de phishing según APWG.

Months	Number of unique phishing Web sites (attacks) detected
January	248,876
February	162,432
March	202,714
April	201,102
May	198,987
June	210,765
July	262,542
August	258,435
September	225,876
October	267,530
November	304,308
December	316,747

Tabla 3. Muestreo del número de ataques de phishing realizados por mes (2021)

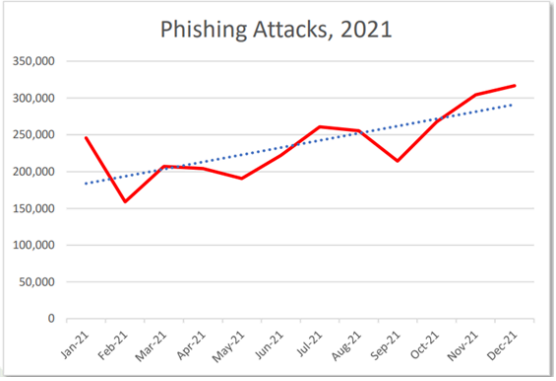

Figura 3. Gráfica - Cantidad de ataques de phishing por mes (2021)

Porcentajes de temáticas más populares utilizados en emails de phishing

Según el volumen 24 del ITRS publicado en 2019, las facturas representan el mayor porcentaje de temas utilizados en los ataques de phishing, con un 15,7%. Esto significa que los correos electrónicos de phishing que se disfrazan como facturas son la táctica más comúnmente utilizada por los ciberdelincuentes en ese periodo.

TOP EMAIL THEMES (YEAR)

SUBJECT TOPIC	PERCENT
Bill	15.7
Email delivery failure	13.3
Package delivery	2.4
Legal/law enforcement	1.1
Scanned document	0.3

TOP EMAIL KEYWORDS (YEAR)

WORDS	PERCENT
invoice	13.2
mail	10.2
sender	9.2
payment	8.9
important	8.5
message	7.7
new	7.2
returned	6.9
:	6.9
delivery	6.6

Tabla 4. Muestreo del porcentaje de tópicos usados en emails de phishing (2019)

Medios de mensajería más utilizados para realizar phishing

Según los datos recopilados, la mayoría de estos ataques se realizaron a través de WhatsApp, que representó el 82,71% de los ataques de phishing en aplicaciones de mensajería instantánea. Esto no es sorprendente, dado que WhatsApp es una de las aplicaciones de mensajería más populares en todo el mundo, con miles de millones de usuarios.

El segundo lugar lo ocupa Telegram, con un 14,2% de los ataques. Aunque Telegram tiene menos usuarios que WhatsApp, su creciente popularidad y características de seguridad han hecho que sea un objetivo atractivo para los ciberdelincuentes.

Viber, otra aplicación de mensajería popular, representó el 3,17% de los ataques. Aunque Viber tiene una base de usuarios más pequeña en comparación con WhatsApp y Telegram, sigue siendo un objetivo para los atacantes.

Estos ataques de phishing suelen tomar la forma de mensajes que parecen provenir de fuentes legítimas y solicitan al destinatario que haga clic en un enlace o proporcione información personal. Los ciberdelincuentes pueden utilizar esta información para robar identidades, acceder a cuentas bancarias o cometer otros tipos de fraude.

Pérdidas generadas por los ataques de Phishing

El costo de los ataques de phishing a las empresas ha aumentado significativamente a lo largo de los años, siendo quizás uno de los ejemplos más infames la pérdida de 100 millones de dólares que enfrentaron Facebook y Google en 2017. Otros ejemplos incluyen:

- Las estadísticas mostraron que en 2018 el costo promedio por violación de datos fue de alrededor de $150 por cada registro comprometido.
- En 2020, el IC3 recibió alrededor de 791,790 quejas con una pérdida registrada que superó los 4.1 mil millones de dólares.
- La diferencia de costo entre las empresas en gran medida conformes y las que no lo son fue de alrededor de $2.3 millones.
- Estados Unidos tuvo la tasa más alta de costosas violaciones de datos en 2021 a $9.05 millones según IBM.

Tipos de phishing mas utilizado

Según el portal web astra de auditorías de seguridad, el spear phishing representa la principal opción de los atacantes al momento de realizar dicho ataque en el 2023.

- El 65% de los atacantes han optado por el spear phishing como su método principal de ataque.
- Casi el 71% de todos los ataques dirigidos se realizan a través de spear phishing.
- En 2012, casi el 90% de los ataques cibernéticos fueron a través de spear phishing.

DESCRIPCIÓN DEL ESCENARIO DE PRUEBAS

Herramienta / Stack Tecnológico Empleado

Instalación de Blackeye (v 2.0)

Blackeye es una herramienta de código abierto especializada en phishing. Se está volviendo popular hoy en día y se utiliza para realizar ataques de phishing contra objetivos específicos. Es un kit de herramientas de ingeniería social fácil de usar que contiene plantillas generadas. Estas plantillas facilitan la realización de ataques de phishing, permitiendo mucha creatividad para que las páginas parezcan lo más legítimas posible. Blackeye ofrece plantillas de páginas web de phishing para 33 sitios populares como Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Protonmail, Spotify, Netflix, Linkedin, WordPress, Origin, Steam, Microsoft, etc.

Uso de Ngrok (Ngrok 2.3.51) para el despliegue posterior del servidor local en internet

Ngrok es una herramienta que levanta un servidor local a internet para que los sitios web falsos de los atacantes puedan ser accesibles desde cualquier lugar. Esto les permite a ellos crear una página de inicio de sesión falsa y utilizarla para obtener información de inicio de sesión de la víctima. Esta funcionalidad resulta extremadamente útil para llevar a cabo pruebas y demostraciones, especialmente cuando es necesario que el tráfico, que puede incluir credenciales u otros parámetros, transite a través de la máquina del usuario.

Social-Engineer Toolkit (SET/Setoolkit - 8.0.3)

Setoolkit es una herramienta popular entre los ciberdelincuentes para llevar a cabo ataques de phishing, ya que les permite configurar el envío de correos electrónicos falsos de manera rápida y sencilla. Esta herramienta incluye una amplia gama de opciones de personalización que permiten a los atacantes hacer que los correos electrónicos falsos parezcan más auténticos y persuasivos. Pueden utilizar información personal de la víctima, como su nombre y posición en la empresa, para hacer que el correo electrónico sea más convincente.

Configuración de clonación

Como se mencionó anteriormente, Blackeye proporciona la funcionalidad llamada "clonación de sitios web" que permite clonar sitios web legítimos y crear páginas de inicio de sesión falsas, por medio de las 37 plantillas +1 personalizable que proporciona la herramienta. Esta herramienta es muy útil para los atacantes ya que les permite hacer que sus sitios web falsos sean más convincentes y persuasivos para sus víctimas. También ofrece opciones de personalización y la capacidad de utilizar técnicas de ingeniería social para aumentar la efectividad del ataque.

Al clonar el sitio web, la herramienta genera una réplica falsa de la página original, incluyendo su apariencia y estructura. Esta réplica se utiliza para engañar a los usuarios y puede ser diseñada para capturar credenciales u otros parámetros sensibles cuando los usuarios interactúan con la página falsa.

Configuración de servidor Ngrok

Ngrok nos facilita una URL para permitir el acceso público a un servidor local que hemos iniciado en nuestra máquina. Esta URL es esencialmente una dirección en Internet que se vincula a nuestro servidor local a través de un túnel seguro, manipulando las configuraciones del Setoolkit para que el sitio clonado en el paso anterior se muestra en esta nueva ruta.

Configuración envío de correo electrónico (email)

Para este paso se configuró el envío de correo electrónico utilizando Setoolkit, el cual permite enviar mensajes que parecen provenir de una fuente legítima y engañar a la víctima para que abra enlaces o archivos adjuntos maliciosos.

Para efectos de este escenario de pruebas, la víctima recibirá un correo electrónico supuestamente proveniente de Amazon, indicando que ha recibido como regalo un mes gratis para la plataforma de Amazon Prime Video y además de una recompensa de 5$ al aceptar la promoción. El e-mail contendrá un botón de inicio de sesión para que la víctima acceda a su cuenta de Amazon por medio del correo electrónico. La idea es que el botón de inicio de sesión, dirija la víctima a la página web de inició de sesión falsa, previamente alojada en el servidor levantado con Ngrok.

Captura de datos

La herramienta Blackeye también permite captar los datos del atacante cuando éste ingresa algún dato en el sitio web clonado. En el momento en que la víctima intente realizar el inicio de sesión por medio de la página web clonada, Blackeye capturará todos los datos que ingrese en los campos de email/número telefónico y contraseña. Blackeye recopila estos datos y enviará esta información al atacante.

Blackeye también le enviará al atacante, bastante información de la víctima en el momento que ingrese al sitio web, así como el país, ciudad, región, código postal, coordenadas google maps y hasta la IP de la víctima.

Consideraciones para la ejecución del escenario de pruebas

Se llevará a cabo un ejercicio de spear-phishing utilizando una máquina virtual con el sistema operativo Kali Linux versión 2023.3 de la distribución Debian. El objetivo principal será simular un ataque mediante el envío de un correo electrónico malicioso en la plataforma de Gmail. En este escenario, el correo estará diseñado para emular una invitación legítima de Amazon, ofreciendo a la víctima la oportunidad de reclamar una prueba gratuita de Amazon Prime Video.

El contenido del correo buscará persuadir a la víctima al indicar que, por cada video visualizado por completo en la plataforma, recibirán un incentivo económico de aproximadamente 5$. La premisa falsa de obtener ganancias adicionales podría aumentar la probabilidad de que la víctima, de la que además se entiende que es un consumidor frecuente de los servicios de Amazon, acceda al sitio web y por lo tanto, puedan ser capturadas sus credenciales de acceso.

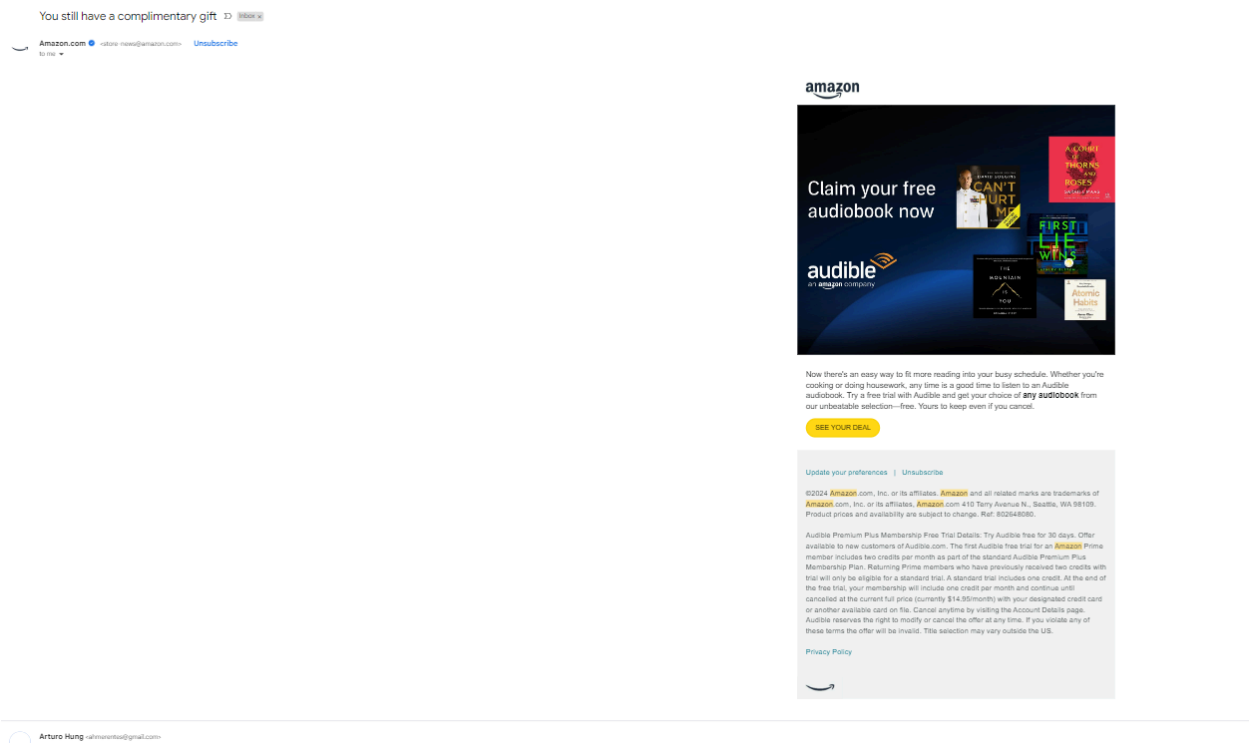

Figura 4. Ejemplo de correo electrónico de Amazon a diseñar en el ataque de spear-phishing

Enlaces de referencia para el diseño de la plantilla de correo electrónico:

- https://github.com/ckissi/responsive-html-email-templates

NOTA: Detalles y pasos de ejecución del ataque indicados en la ficha de práctica

RECOMENDACIONES

Luego de conocer el ataque en profundidad, que busca el atacante y cómo funciona el ataque, se hace importante tomar en cuenta las siguientes recomendaciones para evitar ser víctima de ataques de phishing y derivados:

1. **Habilitar filtros de spam (*spam filters*):** El spam representa cualquier comunicación no solicitada enviada de forma masiva. Se puede distribuir a través de mensajes de texto (SMS), redes sociales o llamadas telefónicas, aunque generalmente se suele presentar en forma de correos electrónicos promocionales inofensivos (aunque molestos) y en algunas ocasiones, llevar consigo una estafa fraudulenta o maliciosa. Es por ello que se aconseja a todo usuario activar dicha configuración al momento de usar una plataforma o sistema de correos electrónicos como lo son Gmail, Yahoo, Outlook, entre otros.

2. **Verificar el remitente:** Validar la autenticidad del remitente del correo electrónico, dado que los ataques de phishing a menudo usan direcciones falsas para engañar a los usuarios. Para lograr ello , se deben tener en cuenta las siguientes consideraciones al momento de detallar lo que se ha enviado en el correo:

    - Abrir la cabecera del mensaje y comprobar la legitimidad del remitente. En el caso de las organizaciones o empresas, estas tienen su propio correo corporativo (por ejemplo @txn-email.playstation.com @ucab.edu.ve) y generalmente verificado (visto azul), por lo que es inusual observar una dirección de correo de una gran empresa o de una organización con una estructura como

nombreempresa@gmail.com o nombreorganizacion@outlook.com, o con algún error en la redacción de sus respectivos dominios oficiales. Si el correo que recibiste te parece sospechoso, elimínalo o márcalo como spam.

- Igualmente en la cabecera del mensaje, verificar que el correo tenga soporte de cifrado estándar TLS/SSL y que igualmente, tenga una firma certificada por la corporación misma.

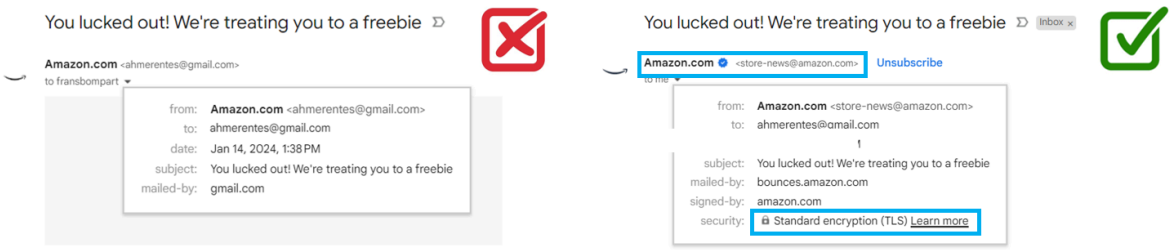

Figura 5. Ejemplo comparativo de la recepción de un correo malicioso (lado izquierdo) y un correo verídico de Amazon

3. **Examinar siempre la barra de direcciones del navegador:** En caso de hacer click en el enlace e ingresar al sitio web, verificar que sea legítimo y por ende, posea un certificado TLS/SSL válido. El nombre del sitio web y la organización que emitió el certificado deben estar siempre visibles en la barra de direcciones.

4. **Reconocer los signos de alerta:** Como errores ortográficos, estructuras inusuales(enlaces/hipervínculos no fiables, imágenes no cargadas correctamente, entre otros) en los correos recibidos habitualmente por una supuesta organización o empresa, o

mensajes urgentes; que bien, indican sobre algo un fallo de la cuenta del usuario en cierta aplicación o le proponen alguna especie de regalo/bonificación.

5. **Usar un software de seguridad actualizado que proteja de los virus, el spyware y el ransomware**: En el caso de la apertura de un correo cuyo archivo adjunto o enlace traiga consigo alguno de estos software malicioso, es recomendable tener instalado un sistema que permita protegerse ante estas amenazas en el caso de acceder a tal archivo.
6. **Educar y emplear plataformas de correo electrónico o mensajería generalmente aceptadas por la comunidad:** Al estas ser partícipes constantemente de ciberataques y pertenecer a compañías de renombre en la industria de la tecnología, poseen su propio personal o equipo de operaciones de seguridad (SOC), el cual constantemente está mejorando la infraestructura de su plataforma de mensajería para mitigar dichos ataques. Esto se puede evidenciar en la siguiente imagen presentada a continuación, donde esto sucede en Gmail cuando se reportan a Google tipos similares de correos electrónicos como "*phishing*".

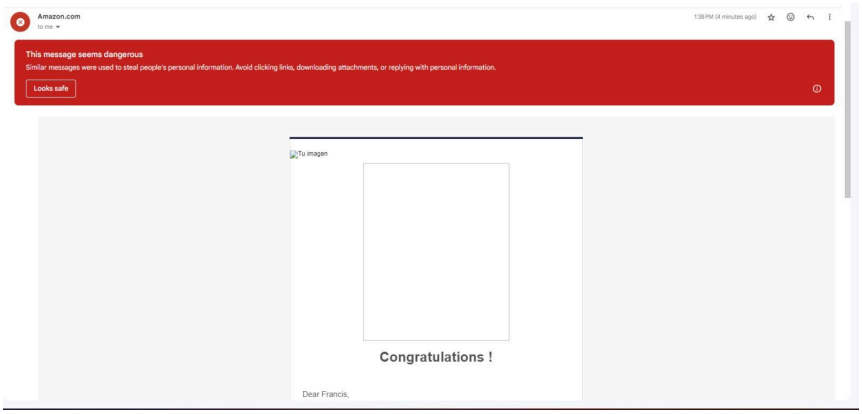

Figura 6. Reporte de recepción de correo electrónico malicioso (Gmail)

CONCLUSIONES

El phishing y los ataques de ingeniería social por correo, se puede concluir que son técnicas que utilizan los ciberdelincuentes para engañar a los usuarios y obtener su información personal o financiera. Estos ataques se basan en la suplantación de identidad mediante correos electrónicos falsos que imitan a empresas o entidades legítimas.

Esto significa que los atacantes se hacen pasar por alguien de confianza para que el usuario les proporcione sus datos o acceda a un enlace malicioso. Por ejemplo, pueden enviar un correo que parece ser de un banco, una compañía de servicios o una institución pública, solicitando que se verifique una cuenta, se pague una factura o se actualice una información. Ya habiendo observado cómo funciona, vemos que es bastante sencillo clonar una página web, y las diferencias son inexistentes o casi inexistentes en cuanto a la estructura.

Como resultado los usuarios que caen en estos engaños pueden sufrir pérdidas económicas, robo de identidad o daños en sus sistemas.

Esto es debido a que los atacantes pueden usar la información obtenida para acceder a las cuentas bancarias, tarjetas de crédito, redes sociales o correos electrónicos de las víctimas, y realizar transacciones fraudulentas, extorsiones, chantajes o difusión de información sensible. Además, los enlaces o archivos adjuntos que se envían en los correos falsos pueden contener virus, troyanos, ransomware u otros programas maliciosos que infectan los dispositivos de los usuarios y comprometen su seguridad y privacidad.

Para protegerse de estos ataques, es importante desconfiar de los correos sospechosos, no ingresar datos personales en sitios web no seguros, no hacer clic en enlaces o descargar archivos adjuntos desconocidos y contar con un software de seguridad actualizado, entre otras recomendaciones que previamente fueron mencionadas.

Esto implica que los usuarios deben estar atentos a las señales que pueden indicar que un correo es falso o que una página web es ilegítima, como errores ortográficos, direcciones de remitente extrañas, asuntos alarmantes o urgentes, o solicitudes de información confidencial. Asimismo, deben evitar abrir o descargar cualquier contenido que no hayan solicitado o que no esperen recibir, y tener instalado un antivirus o antimalware que proteja sus dispositivos de posibles amenazas.

El phishing y los ataques de ingeniería social, se aprovechan del desconocimiento o el descuido de las personas para tener éxito en su tarea, que es obtener información valiosa para su posterior uso o hacer que la persona haga clic en enlaces con cualquier tipo de virus.

Por lo tanto, podemos concluir que la educación y la prevención son las mejores armas contra la ingeniería social y el phishing. Esto significa que los usuarios deben informarse sobre los riesgos y las formas de evitar estos ataques, y estar al día con las noticias y las alertas sobre las campañas de phishing más recientes. También deben reportar cualquier correo sospechoso que reciban a las autoridades competentes o a las entidades que supuestamente lo envían, y ayudar a difundir la conciencia sobre este problema entre sus contactos y redes. De esta manera, se puede reducir el impacto y la efectividad de estos ataques, contribuyendo a la seguridad cibernética de todos.

BIBLIOGRAFÍA

[1] 11 consejos para evitar los ataques de ingenieria social. https://blog.mailfence.com/es/11-consejos-para-evitar-los-ataques-de-ingenieria-social/.

[2] 2023 State of the PhISH Report—Phishing Stats and Trends | ProofPoint US. (2023, 15 agosto). Proofpoint. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[3] Ariani, P. C., Jayanti, K. S., Atmaja, I. G. B. W., Dewi, I. G. A. A. A., Saskara, G. A. J., & Listartha, I. M. E. (2023). Comparative Analysis of Phishing Tools on Social Media Sites. Ultimatics: Jurnal Teknik Informatika, 15(1), 22-27.

[4] Cerullo, M. (2023, 16 noviembre). Amazon says prime scams are on the rise as the holidays near. CBS News. https://www.cbsnews.com/news/amazon-prime-scams-emails-calls/

[5] Consecuencias de caer en el phishing: cómo evitar la ingeniería social. https://vanbig.es/ciberseguridad/las-consecuencias-del-phishing-en-la-ingenieria-social-como-protegerse-y-prevenir-ataques/.

[6] G. Workspace, Advanced phishing and malware protection, March 2021, [online] Available: https://support.google.com/a/answer/9157861.

[7] Ingeniería social, ciberataques más comunes y cómo prevenirlos. https://www.piranirisk.com/es/blog/ingenieria-social-ciberataques-y-prevencion.

[8] Ingeniería social: protección y prevención - Kaspersky. https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks.

[9] Internet Security Threat Report Volume 24 | February 2019. (s. f.). ISTR istr-24-2019-en (broadcom.com).

[10] J. Hong, "The state of phishing attacks", Communications of the ACM, vol. 55, no. 1, pp. 74-81, 2021.

[11] Kshetri, N. (2023). Privacy violations, security breaches and other threats of Web3 and the metaverse.

[12] M. Bitaab, H. Cho, A. Oest, P. Zhang, Z. Sun, R. Pourmohamad, et al., "Scam pandemic: How attackers exploit public fear through phishing", eCrime Symposium on Electronic Crime Research, 2020.

[13] MITRE ATT&CK®. (n.d.). https://attack.mitre.org/

[14] Niemeyer, K. (2023, 21 diciembre). Amazon sent an email that sounded like a gift card scam to warn about gift card scams, confusing customers. Business Insider. https://www.businessinsider.com/amazon-gift-card-scam-warning-feels-like-scam-puzzling-customers-2023-10

[15] Palatty, N. J. (2023, 21 diciembre). 81 Phishing attack Statistics 2024: The Ultimate insight. Astra Security Blog.https://www.getastra.com/blog/security-audit/phishing-attack-statistics//

[16] PHISHING ACTIVITY TRENDS REPORT | December 2021. (s. f.). APWG report

[17] Principales estadísticas de ciberataques, cifras para 2021 | Fortinet. (s. f.).Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/cybersecurity-statistics.

[18] Suspicious email Reporting - Amazon Web Services (AWS). (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/security/report-suspicious-emails/

[19] Verizon. (2023). 2023 Data Breach Investigations Report. Basking Ridge, NJ: Verizon Business.

[20] Weeks, R. (2022, 6 julio). How a fake job offer took down the world's most popular crypto game. The Block. https://www.theblock.co/post/156038/how-a-fake-job-offer-took-down-the-worlds-most-popular-crypto-game