Cienc Tecn UTEQ (2020) 13(1) p 97-104 ISSN 1390-4051; e-ISSN 1390-4043 https://doi.org/10.18779/cyt.v13i1.357

Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura

Characterization of Phishing Attacks and Techniques to Mitigate These Attacks: A Systematic Review of The Literature

Benavides Eduardo[1,2]; Fuertes Walter[1,2]; Sanchez Sandra[1]
[1]Escuela Politécnica Nacional, [2]Universidad de las Fuerzas Armadas
[1]diego.benavides@epn.edu.ec, [2]debenavides@espe.edu.ec, [1]walter.fuertes@epn.edu.ec, [2]wmfuertes@espe.edu.ec, [1]sandra.sanchez@epn.edu.ec

Rec.: 19.03.2019. Acept.: 21.01.2020.
Publicado el 30 de junio de 2020

Resumen

En la Seguridad Informática, no importa que equipamiento de Software o Hardware se tenga instalado, porque siempre el eslabón más débil en esta cadena de seguridad es el usuario final. De esta premisa se valen los diferentes tipos de ataque de Ingeniería Social, cuyo objetivo principal es obtener información casi directamente de los usuarios, con la finalidad de usar esta información en contra de ellos mismos. Existen varios vectores de ataque de Ingeniería Social, entre los que sobresalen: páginas web falsificadas, mensajes malignos en redes sociales, y correos malignos que piden información confidencial de los usuarios o incluso pueden redireccionar a los usuarios a una página web falsificada (Phishing). El objetivo de este trabajo es proveer a los usuarios finales y a otros investigadores, una visión de los tipos de ataques de Phishing existentes y de cómo estos pueden ser mitigados. Para esto, primeramente, se realiza una revisión sistemática de la literatura en las principales fuentes científicas, para caracterizar y clasificar los diferentes tipos de ataque de ingeniería social, y posteriormente, se exponen y clasifican los medios por los que estos ataques pueden ser mitigados, que van desde la concientización al usuario, hasta la utilización de técnicas de Machine Learning y Deep Learning.

Palabras clave: Ingeniería Social, Phishing, Machine Learning, Deep Learning, Ciber Seguridad

Abstract

In Computer Security, it does not matter which Software or Hardware equipment is installed, because always the weakest link in this security chain, is the end user. From this premise are used the different types of Social Engineering attacks, whose main objective is to obtain information almost directly from the users, with the purpose of using this information against themselves. There are several attack vectors of Social Engineering, among which stand out: fake web pages, malign messages on social networks, and malicious emails that ask for confidential information from users or even redirect users to a fake web page (Phishing). The objective of this paper is to provide end users and other researchers with a look at the types of Phishing attacks that exist, and how they can be mitigated. For this, first, a systematic review of the literature in the main scientific sources is carried out, to characterize and classify the different types of Phishing attacks, and subsequently, the means by which these attacks can be mitigated are exposed and classified, ranging from a user awareness to the use of Machine Learning (ML) and Deep Learning (DL) techniques.

Keywords: Social Engineering, Phishing, Machine Learning, Deep Learning, Cybersecurity

Introducción

Ingeniería Social (IS) es el acto de obtener información de las personas de manera fraudulenta, con la finalidad de usar esta información, en contra de ellas mismas o de sus organizaciones. Existen varias formas de obtener esta información, pero la manera más utilizada es mediante el uso de Phishing. Así, Phishing es el ataque de Ingeniería Social, que busca obtener esta información sensible, pero por medios electrónicos. Los medios más comunes de ataques de Phishing son por Phishing Emails y por Phishing Websites. El objetivo principal del Phisher (Persona que realiza el Phishing) es obtener una retribución económica, es decir, estafar a su víctima.

En la actualidad no existe un estudio completo, que permita conocer todos los pormenores y características de los ataques de Phishing, ni de los enfoques necesarios para mitigarlos. Es así que el objetivo principal de este trabajo es aportar con un documento útil para investigadores y el público en general, en que pueda conocer las características de los ataques de Phishing, enfoques que se utilizan para mitigar estos ataques, información de repositorios de donde se pueden obtener gran cantidad de direcciones de phishing, y un conjunto de las herramientas más utilizadas en la actualidad para medir la efectividad de las últimas soluciones.

El resto del documento está estructurado de la siguiente manera: En la sección 2, se hace una descripción de los conceptos básicos de Phishing y sus características. En la sección 3, se hace una descripción de la metodología utilizada en esta Revisión Sistemática de la Literatura (RSL). En la sección 4, se muestran los resultados encontrados en base a nuestra búsqueda de enfoques aplicados al combate de Phishing. Finalmente, en la sección 5, se declaran las conclusiones y trabajo futuro de este estudio.

1. BACKGROUND

1.2. ¿Qué es Phishing?

Phishing es la combinación de Ingeniería Social y exploits técnicos [1], diseñados para convencer a una víctima de proporcionar información personal, generalmente realizado para obtener una ganancia monetaria por parte del atacante. La mayoría de los ataques de Phishing son influenciados cuando se envía un correo electrónico falso, que contiene un enlace (Uniform Resource Locator, URL). Esta URL conduce a un sitio web falso, cuando se hace clic en él. A pesar de la importante atención que se le ha otorgado a lo largo de los años, aún no existe una solución definitiva, para resolver este tipo de ataque [2].

Por su parte, en [3] se define que: "una página de Phishing, es aquella que, como cualquier página web, sin permiso, alega actuar en nombre de un tercero; con la intención de confundir a los espectadores en la realización de una acción".

1.3. ¿Cómo se clasifican los ataques de Phishing?

De acuerdo con Herrera et al., en [4], los ataques se podrían clasificar, tomando en cuenta las siguientes consideraciones:

1.3.1 Según el servicio que ataquen. Por ejemplo: Bancos y cajas, Pasarelas de pago en línea, Redes sociales, Páginas de compraventa o subastas, Juegos en línea, Soporte Técnico / Mesas de ayuda, Almacenamiento en la nube, Servicios o empresas públicas, Servicios de mensajería, Falsas ofertas de empleo.

1.3.2. Según el modus operandi. Por ejemplo: Phishing engañoso, Software malicioso, DNS o pharming, Introducción de contenidos, Man in the middle Phishing, Search Engine Phishing

1.4. Técnicas más usadas

Existen diversas técnicas para perpetuar el ataque de phishing, pero de ellas las más comunes son dos: Por medio de una cuenta de correo de phishing y por medio de una página web de phishing. En los emails phishing, comúnmente se les anuncia a las víctimas que han ganado algún tipo de premio, a cambio del cual deben ingresar alguna información confidencial. En los websites de phishing, comúnmente se muestra a la víctima una página web falsificada, muy parecida a una página web legítima, incluso su URL es muy parecida, como en el siguiente ejemplo. Por ejemplo, en el link http: //www.nombredetubancoCE.com/ejemplo1, se ha introducido las letras CE, para indicar que es un Carácter Extraño, incrustado en el nombre del banco al que se quiere ingresar, por lo tanto, esa URL abrirá una página web falsificada.

Otro ejemplo de métodos para disfrazar enlaces, es utilizar direcciones que contengan caracteres especiales, como el símbolo arroba: @. Tomemos el ejemplo de la URL http:/www.google.com@members.tripod.com/. En este enlace se puede engañar a un observador casual y hacerlo creer que el vínculo mostrado, va a abrir en la página de www.google.com, cuando en realidad, el enlace envía al navegador a la página de members.tripod.com. Luego en este sitio, se le pedirá a la víctima, el nombre de usuario y contraseña de www.google.com, pero en sin saberlo, esta víctima le estará entregando estos datos al sitio members.tripod.com.

Estas son solo algunas de las técnicas de ataques más usadas de Phishing. Más adelante en este paper se muestran otras técnicas, con sus características individuales.

1.5. Motivaciones del Phisher

De acuerdo con Yu en [5], los motivos principales detrás de los ataques de Phishing, desde la perspectiva de un atacante, son: (1) Ganancia financiera: usar credenciales bancarias robadas para sus beneficios financieros. (2) ocultar la identidad: en lugar de usar identidades robadas directamente, se podrían vender las identidades robadas, a otros que podrían ser criminales que buscan formas de ocultar sus identidades y actividades (por ejemplo, para compra de bienes), (3) Fama y notoriedad: En que se ataca a las víctimas por el reconocimiento de sus pares.

1.6. Impacto

En el año 2011 se ejecutó una serie notable de ataques de Phishing contra empresas de seguridad con alto prestigio, entre ellas RSA [6], lo que originó más ataques en contra de sus usuarios, como el cliente Lockheed Martin [7]. Esto demostró que los peligros de los ataques de Phishing, o vulnerabilidades de seguridad debido al factor humano, no se limitan a la ingenuidad de los usuarios finales, ya que los técnicos también pueden ser víctimas.

1.7. Ciclo de vida

El proceso de Phishing implica esencialmente cinco etapas [8], como se muestra en la Fig 1:

Fig. 1. Etapas de un ataque de Phishing

1.7.1. Planificación y configuración: en esta etapa se identifica la organización, individuo o un país entero. El objetivo principal es extraer detalles esenciales sobre la víctima y la red, para lo cual se puede hacer un análisis de tráfico. Posterior a este reconocimiento, se configuran los ataques mediante el despliegue de medios viables como el sitio web, correos electrónicos que contienen enlaces maliciosos, etc. Estas herramientas fundamentalmente redirigen a la víctima hacia una página web fraudulenta.

1.7.2. Ataque de Phishing: Esta es la segunda fase del ciclo donde tiene lugar la actividad real. Los atacantes envían correos electrónicos falsificados a la víctima, usando direcciones de correo electrónico recolectadas, que solicitan información confidencial a la víctima. Generalmente los emails de Phishing, se disfrazan de alguna página de una organización bancaria de buena reputación, que necesita la información personal de la víctima para actualizar sus registros, e indica a la víctima que debe responder urgentemente haciendo clic en algún enlace malicioso.

1.7.3. Ruptura/Infiltración: En esta fase, la víctima hace clic en el enlace malicioso y, en cuanto lo hace, un malware se instala automáticamente en su dispositivo, lo que permite al atacante acceder al sistema y comprometerlo, cambiar sus configuraciones y derechos de acceso. En algunos casos, hacer clic en el enlace malicioso, también puede dar lugar a que el usuario común sea re direccionado a alguna página falsa.

1.7.4. Recopilación de datos: Una vez que los atacantes acceden al sistema de la víctima, extraen los datos requeridos. Por ejemplo, si la víctima proporciona datos confidenciales de una cuenta bancaria, el atacante puede acceder a ella, lo que eventualmente puede conducir a pérdidas financieras para la víctima. En el caso de ataques de malware, los atacantes obtienen acceso remoto al sistema de la víctima y extraen los datos requeridos o realizan cualquier cambio según su voluntad. En casos más graves, los sistemas comprometidos pueden utilizarse para ataques de denegación de servicio (DOS).

1.7.5. Extracción: Esta es la fase final del ciclo. Después de obtener el acceso y la información requerida, se elimina toda la evidencia como las cuentas falsas del sitio web. Finalmente, se evalúa el grado de éxito de su ataque, para afinar sus futuros ataques.

MÉTODO

Para realizar esta revisión sistemática de la literatura (SLR, por sus siglas en inglés), se ha seguido la metodología propuesta por Barbara Kitchenham [9]. Se han realizado cuatro pasos consecutivos. Primero se realizó la búsqueda general, para luego escoger los artículos relevantes. A continuación, se realiza la extracción de datos y finalmente se muestran los resultados de la información encontrada. A continuación, se describe brevemente cada una de estas fases:

3.1. Búsqueda de la Información. Para esto primero se definió la cadena de búsqueda, la cual se encontró conformada por dos partes, Phishing y Review. Luego, se modificó la cadena de búsqueda

por sinónimos de cada una de sus dos partes. Ya con la cadena de búsqueda definida, se procedió a buscar en todos los artículos relacionados al tema en cuestión.

3.2. Criterios de Inclusión. Una vez definidas las palabras claves de búsqueda, solo se incluyen los siguientes documentos de entre los encontrados: (1) Cuyo tema principal se trate de Phishing y Review; (2) Escritos solamente en inglés; (3) Procurar que su publicación sea únicamente de máximo 5 años atrás;

3.3. Criterios de exclusión. (1) Artículos cuyo tema solo sea de Phishing o solo se Review, es decir que no haya una combinación de los dos, o de sus Sinónimos; (2) No sean escritos en inglés; (3) Artículos de antes del año 2014.

3.4. Criterio de Calidad. Para cumplir con el criterio de calidad de la búsqueda, decidimos realizar el escrutinio, solo en páginas reconocidas a nivel científico, y que sean del área de tecnología en la información. Los sitios escogidos fueron: IEEE Explore, Taylor and Francis, Springer Linker, ACM Portal y Science Direct.

3.5. Extracción de Datos. Una vez realizada la búsqueda de información, se pudieron encontrar 30 artículos.

3.6. Síntesis. Luego de proceder a leer y analizar los 75 artículos encontrados inicialmente, se puede resumir que únicamente 36 artículos fueron útiles para el presente estudio.

3.7. Reporte. En base a la síntesis realizada en el paso anterior, se procede a realizar el presente informe, y se muestra la información recabada por el análisis del mismo.

RESULTADOS

Conjuntos de datos

Para encontrar nuevas soluciones a los problemas de phishing, es necesario usar grandes cantidades de datos, para poder evaluar la efectividad y rendimiento de dicha solución. Así, en internet se pueden encontrar diversos sitios, que son de importante utilidad para esta tarea. Del documento [8], se pueden rescatar algunas cuatro de las cinco opciones que se describen a continuación:

4.1.1. Phishtank. Es el sitio web más visitado para saber si una URL es o no de Phishing. En este sitio se pueden obtener características adicionales de las URLs infectadas, repostadas por los usuarios. Cuenta además con una base datos descargable.

4.1.2. Anti-Phishig Work Group (APWG) Archives. En este archivo se guarda una extensa base de datos de todas las URLs de los sitios que han sido reportados o detectados por APWG.

4.1.3. Phishload. Este sitio contiene información acerca de páginas web Phisheados, tales como: URL Address, código HTML, y otra información relacionada. También contiene información de sitios verificados como legítimos.

4.1.4. Corpora. En este sitio se puede encontrar tanto de URLs ilegítimas como legitimas. Estos conjuntos de datos dividen en tres: easy ham, que es fácilmente distinguible de los spams, y hard ham, que es más difícil de distinguir. La tercera parte está compuesta por easy ham2 y spam 2.

4.1.5. Alexa. En los estudios de investigación, no solamente es necesario saber que URLs son Phishing, sino también es necesario saber cuáles son legítimas. Esto es lo que nos ofrece el sitio Alexa, en el cual se cuenta únicamente con URLs verificadas como benignas.

4.2.Herramientas de evaluación de exactitud

En la Fig. 2. realizada por [8], se exponen varias herramientas que son utilizadas en el desarrollo de nuevas soluciones y medición en la exactitud de soluciones de Phishing. La mayoría de estas herramientas son utilizadas para el uso de los algoritmos de Machine Learning y Deep Learning.

Fig. 2. Herramientas utilizadas en soluciones Anti-Phishing

Por otra parte, en los últimos años los enfoques basados en listas negras o blancas son ineficientes para detectar ataques de Phishing Zero Day, es decir, ataques que recién aparecen. Para realizar una detección temprana de este tipo de ataques, es importante analizar las características de los sitios web phishiados. Estas características pueden darnos una alta probabilidad de si una página web es de Phishing o no. En la Fig. 3, se detallan las principales características recopiladas por [10]. Por otra parte, en la Fig. 4, se detallan la principales características usadas en los enfoques de detección de

websites de Phishing.

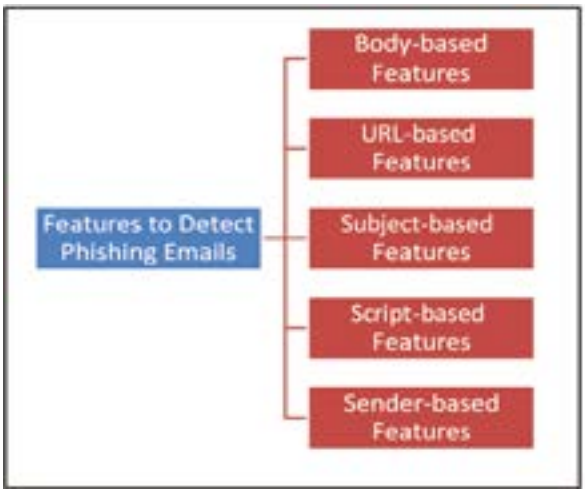

Fig. 3. Características en Phishing Emails

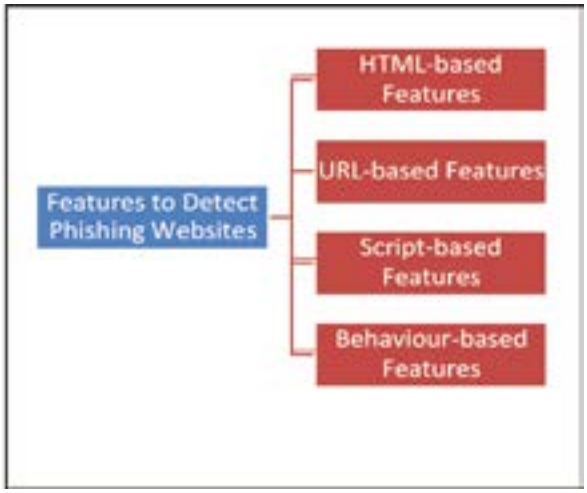

Fig. 4. Características en Phishing Websites

4.3. Enfoques de Mitigación de Ataques de Phishing basados en su vector de ataque

Para contratacar los ataques de Phishing, es importante conocer sus vectores de ataque. Según [11], estos vectores se clasifican en Spoofing Email, Fake Social Network Accounts, Hacking y Trojan Horse:

4.3.1. Spoofing Email: Esta es la manera más común de enviar un ataque de phishing. Para esto, el atacante envía un email spam a muchos usuarios, esperando que al menos alguien caiga en la trampa. Estos spams comúnmente ofrecen un beneficio grande a los usuarios, como alguna lotería o alguna herencia ganada.

4.3.2. Fake Social Network Accounts: Por medio de la creación de una falsa cuenta, en alguna red social como Facebook o Twitter, el Phisher (Persona que realiza ataques de phishing), puede obtener información disponible por los usuarios en sus redes sociales. Información útil para el usuario, tal como: Lugar de trabajo, cargo en el trabajo, apreciación de ingresos económicos, etc.

4.3.3. Hacking: Este tipo de ataque es más técnico que los anteriores y es realizado por un hacker. En este tipo de ataque, el hacker trata de obtener información, mediante el uso de herramientas más sofisticadas de software, con la finalidad de obtener usuarios y contraseñas de los usuarios comunes. Incluso puede hacer que el usuario ejecute intencionalmente un código maligno, para enviar esa información sensible al hacker.

4.3.4.Trojan Horse: Se denomina caballo de Troya al tipo de ataque que se realiza a través de código maligno ejecutado en el sistema. Este código está oculto comúnmente tras un mensaje inofensivo, sin embargo, es capaz de capturar información sensible de nuestro sistema y enviarla al Phisher. La forma más básica de este ataque es en la cual debemos llenar un formulario con información privilegiada y luego enviarlo.

Por lo tanto, de acuerdo a los vectores de ataque antes descritos, los enfoques de detección de Phishing se pueden clasificar en: Spoofed Email Detection, Fake Social networking accounts detection, Hacking Detection y Trojan Horse Detection.

Sin embargo según [12], los vectores de ataque más comunes de Phishing son dos: Por Spoof Email, y por Spoof Website. Phishing Email es la técnica preferida por los Phishers, debido a que, por medio de un simple spam, se les pide a los usuarios que envíen información privilegiada. Por su parte, Spoof Website hace referencia a una página web cuya apariencia es una copia de una página web original, en la que igualmente se induce a que él usuario ingrese información sensible.

4.4. Enfoques de Mitigación de Ataques de Phishing basados en el contenido de la página web

Por otra parte, según el enfoque de [13], los ataques de Phishing se pueden detectar por el contenido de la misma página web, es decir por: Starting URL, Landing URL, Redirection chain, Logged links, HTML code y Screenshot. A continuación, describimos brevemente cada uno:

4.4.1. Starting URL. Es la dirección que hace que se abra una página web determinada.

4.4.2. Landing URL. Es la URL que aparece en la barra de direcciones del navegador, una vez que la página web ya está abierta.

4.4.3. Redirection Chain. Son las cadenas que se escriben en la barra de direcciones del navegador, sin necesidad de tener que escribir la URL que buscamos.

4.4.4. Logged links. Son los enlaces a los que nos conectamos mientras se carga una página, por ejemplo, al cargar imágenes externas a la página.

4.4.5 HTML Code. Es el código o el texto HTML

contenido en la misma página web. Screenshot es la captura de una imagen de la página web cuando ya está abierta.

4.5. Enfoques de Mitigación de Ataques de Phishing basados en la conciencia y conocimiento de las personas

Los artículos revisados coinciden en que, el eslabón más débil de la cadena de la seguridad de la información es el mismo usuario. Es por esta razón que en [14], se realiza una completa revisión de trabajos en los que se utiliza la concientización de los usuarios como principal escudo para enfrentar los ataques de Ingeniería Social (SE). Por eso es importante conocer los pasos seguidos por un Phisher [15] en un ataque de ingeniería social. En [15], además los autores realizan un framework de ataques de SE, basados en el ciclo de ataque de SE de Kevin Mitnick. En este, se hace una completa descripción de los pasos del ataque, desde la determinación de meta de un ataque, hasta la exitosa completitud de ese ataque. Si bien en este paper no se propone una solución a los ataques, es importante para que los profesionales y personas comunes entiendan cada uno de sus pasos. Ya en [16], los autores proponen la implementación de una metodología de defensa a ataques de Ingeniería Social (mediante la conciencia de las personas, no es solución tecnológica), mediante múltiples capas, siendo estas de los siguientes niveles: nivel básico, nivel de fortaleza, nivel de persistencia, nivel ofensivo y el nivel de gotcha o de minas terrestres. En [17], se hace un completo estudio para clasificar los ataques de Ingenierías Social, separándolos en Psicológicos y Físicos, entendiéndose como Psicológicos, los que se hacen de manera remota, mientras que Físicos, los que se hacen directamente, por ejemplo, espiar sobre el hombro una contraseña. Finalmente, el artículo hace un grupo de recomendaciones, como: usar herramientas de listas negras y uso de procedimientos, sin embargo, carece de propuestas para mitigar ataques desconocidos de IS.

En [18], primero se establecen los principios de influencia que usan los atacantes de Ingeniería Social (autoridad, compromiso y consistencia, reciprocidad, simpatía, prueba social, escasez), lo cual posteriormente los autores relacionan con los rasgos comunes de las víctimas de estos ataques (conciencia, extraversión, afabilidad, franqueza, neurotismo). Los autores no solamente definen relaciones directas entre estos grupos de características,

sino que además les dan pesos a esas relaciones. En el artículo [11], se hace un estudio únicamente sobre el tipo de ataque de Ingeniería Social, Phishing. Se definen según este estudio, cuatro tipos de ataques de Phishing: Spoofing email, Fake Social Network Accounts, Hacking, y, Trojan horse. Posteriormente este trabajo propone sus respectivos enfoques como medios de mitigación, para cada tipo de ataque, los cuales principalmente consisten en la concientización y precaución de las personas.

Si bien el trabajo propuesto en [19] es del 2010, quisimos resaltarlo, en razón de que es uno de los primeros trabajos en los que los autores proponen un modelo estructurado, denominado Social Engineering Attack Detection Model (SEADM), para identificar si existe o no una amenaza de una ataque de Ingeniería Social. Por su contemporaneidad, el trabajo está orientado a detectar tales amenazas en los Call Centers. Sim embargo, es importante entender este trabajo para entender los trabajos de los mismos autores en [8] y [9] . En [8], los autores revisan y realizan una nueva versión de su modelo SEADM propuesto en [19], en la que los ataques se pueden realizar por tres vías de comunicación: Bidireccional, Unidireccional, y Comunicación Indirecta. Por otra parte, mientras el modelo propuesto en [8] sirve como una plantilla de procedimiento general, en el modelo propuesto en [9], los autores implementan una máquina de estados finita, que resalta las interconexiones entre tareas asociadas con diferentes escenarios. En [22], los autores hacen un estudio basado en recolectar y analizar los incidentes de Amenazas Internas No Intencionales (AIN). Pero el aporte más importante es el análisis que se hace a casos similares, lo que le permite caracterizar los tipos de ataque a AIN, y como contrarrestarlos de manera general. En este artículo se puede obtener una buena taxonomía de Ingeniería Social.

4.6. Últimos enfoques Anti Phishing

Al día de hoy, el enfoque basado en blacklists es el más usado, sin embargo, este se queda corto cuando aparece una amenaza del tipo Zero Day, porque para que una página web sea detectada con blacklists, esta amenaza debe de ya haber sido clasificada con anterioridad. Para combatir este último tipo de ataques, la forma más efectiva es trabajar con el enfoque basado en Machine Learning. Con este enfoque, se puede pronosticar si una página es de Phishing o no, simplemente basándose en las características de la página. Pero hay que mencionar que una desventaja al usar Machine Learning, es que hay que seleccionar cuidadosamente las características que tienen tanto los Spoof Emails como los Spoof Websites. Esto puede llevar a que sea necesaria la intervención de un experto en el área específica de Phishing. Otra desventaja de ML es que la precisión de su exactitud es limitada.

Para resolver el problema de seleccionar las características, lo que conlleva a esfuerzo técnico y conocimiento de un experto en un tema particular, se

cuenta con un enfoque aún más novedoso, este es Deep Learning, el cual es una rama de Machine Learning. Con este enfoque, las características importantes para predecir una página de phishing, las va seleccionando el mismo algoritmo de Deep Learning por sí mismo, incluso DL puede predecir con una mayor exactitud que un algoritmo de ML tradicional. El único inconveniente al usar Deep Learning, es que se necesita un gran volumen de datos y una gran cantidad de procesamiento de computadora, lo que se resume en mayor tiempo en la ejecución de sus algoritmos. Sin embargo, la exactitud de este enfoque es más exacto, siempre y cuando se disponga de gran cantidad de datos.

Después de haber realizado una revisión exhaustiva, se sintetiza en la Tabla I, un grupo de soluciones en que se han aplicado algoritmos de Deep Learning. Esencialmente, se puede observar que las soluciones se han realizado en base a cuatro algoritmos de DL: Recurrent Neural Network (RNN), Deep Boltzmann Machine (DBN), Deep Neural Network (DNN) y Convolutional Neural Network (CNN).

CONCLUSIONES Y TRABAJO FUTURO

Este trabajo es una guía para que otros investigadores puedan utilizarla en el desarrollo de sus propios trabajos, orientados a la solución de estos ataques de Phishing en la Ingeniería Social. Además, es una lectura apropiada para que personas naturales puedan entender los conceptos básicos de este tipo de ciberataque, cumpliendo también con uno de los enfoques anti-phishing establecidos, que es la concientización.

Como hallazgos importantes, se puede determinar por los estudios realizados, que los vectores más comunes de ataques de Phishing son los de Spoofing Email y de Spoofing Website. Se puede observar también, que existe un gap en el uso de varios algoritmos de Deep Learning en este tipo de problema.

Los medios de mitigación más efectivos para Zero Day en phishing, son mediante los algoritmos tradicionales Machine Learning y mediante Deep Learning. Consideramos que otro gap en la investigación, está en la falta de un algoritmo que acelere la velocidad de los algoritmos de Deep Learning, sin disminuir su exactitud.

Como trabajo futuro se realizará un específica Revisión Sistemática de la Literatura, acerca de los medios de mitigación de ataques de Phishing, pero únicamente usando algoritmos de Deep Learning, y de cómo se usaron esas técnicas. Además, se espera desarrollar un nuevo algoritmo o metodología, usando Deep Learning, para evitar este tipo de ataques.

Category	Deep Learning Algorithm	Articles found
Unsupervised	SAE - Stacked AE	
	SDAE- Stacked DAE	
	SPN - Sum Product Network	
	RNN - Recurrent Neural Network	[23], [24], [25]
	DBM - Deep BM	[26], [27], [28]
	DBN - Deep Belief Network	
Hybrid	DNN - Deep Neural Network	[29], [30], [31], [32]
Supervised	CNN - Convolutional Neural Network	[33], [34], [35], [36]

1. Tabla I. Soluciones de Phishing con Algoritmos de Deep Learning

BIBLIOGRAFÍA

[1] J. Hajgude and L. Ragha, "Phish mail guard: Phishing mail detection technique by using textual and URL analysis," in 2012 World Congress on Information and Communication Technologies, 2012, pp. 297–302.

[2] S. Marchal, G. Armano, T. Grondahl, K. Saari, N. Singh, and N. Asokan, "Off-the-Hook: An Efficient and Usable Client-Side Phishing Prevention Application," IEEE Trans. Comput., vol. 66, no. 10, pp. 1717–1733, Oct. 2017.

[3] C. Whittaker, B. Ryner, and M. Nazif, "Large-Scale Automatic Classification of Phishing Pages."

[4] E. Á. Herrera Calderón and E. Ángel, "El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal.," 2016.

[5] W. D. Yu, S. Nargundkar, and N. Tiruthani, "A phishing vulnerability analysis of web based systems," in 2008 IEEE Symposium on Computers and Communications, 2008, pp. 326–331.

[6] "Details of the RSA Hack - Schneier on Security," Schneier on Security, 2011. [Online]. Available: https://www.schneier.com/blog/archives/2011/08/details_of_the.html. [Accessed: 13-Jan-2018].

[7] "Lockheed Martin Hack Linked to RSA's SecurID Breach - Schneier on Security," Scheneier, 2011. [Online]. Available: https://www.schneier.com/blog/archives/2011/05/lockheed_martin.html. [Accessed: 13-Jan-2018].

[8] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," Neural Comput. Appl., vol. 28, no. 12, pp. 3629–3654, Dec. 2017.

[9] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," Inf. Softw. Technol., vol. 51, no. 1, pp. 7–15, Jan. 2009.

[10] F. Toolan and J. Carthy, "Phishing detection using classifier ensembles," in 2009 eCrime Researchers Summit, 2009, pp. 1–9.

[11] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing
attack," in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 537–540.

[12] A. N. Shaikh, A. M. Shabut, and M. A. Hossain, "A literature review on phishing crime, prevention review and investigation of gaps," in 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), 2016, pp. 9–15.

[13] S. Marchal, K. Saari, N. Singh, and N. Asokan, "Know Your Phish: Novel Techniques for Detecting Phishing Sites and Their Targets," in 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 2016, pp. 323–333.

[14] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," in 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 2018, pp. 62–68.

[15] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in 2014 Information Security for South Africa, 2014, pp. 1–9.

[16] J. Long and K. D. (Kevin D. Mitnick, No tech hacking : a guide to social engineering, dumpster diving, and shoulder surfing. Syngress, 2008.

[17] E. U. Osuagwu, G. A. Chukwudebe, T. Salihu, and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity," in 2015 International Conference on Cyberspace (CYBER-Abuja), 2015, pp. 91–100.

[18] S. Uebelacker and S. Quiel, "The Social Engineering Personality Framework," in 2014 Workshop on Socio-Technical Aspects in Security and Trust, 2014, pp. 24–30.

[19] M. Bezuidenhout, F. Mouton, and H. S. Venter, "Social engineering attack detection model: SEADM," in 2010 Information Security for South Africa, 2010, pp. 1–8.

[20] F. Mouton, L. Leenen, and H. S. Venter, "Social Engineering Attack Detection Model: SEADMv2," in
2015 International Conference on Cyberworlds (CW), 2015, pp. 216–223.

[21] F. Mouton, A. Nottingham, L. Leenen, and H. . Venter, "Finite State Machine for the Social Engineering Attack Detection Model: SEADM," SAIEE Africa Res. J., vol. 109, no. 2, pp. 133–148, Jun. 2018.

[22] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of
Unintentional Insider Threats Deriving from Social Engineering Exploits," in 2014 IEEE Security and Privacy Workshops, 2014, pp. 236–250.

[23] A. Vazhayil, R. Vinayakumar, and K. Soman, "Comparative Study of the Detection of Malicious URLs Using Shallow and Deep Networks," in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1–6.

[24] W. Chen, W. Zhang, and Y. Su, "Phishing Detection Research Based on LSTM Recurrent Neural Network," Springer, Singapore, 2018, pp. 638–645.

[25] J. Zhao, N. Wang, Q. Ma, and Z. Cheng, "Classifying Malicious URLs Using Gated Recurrent Neural Networks," Springer, Cham, 2019, pp. 385–394.

[26] S. Selvaganapathy, M. Nivaashini, and H. Natarajan, "Deep belief network based detection and
categorization of malicious URLs," Inf. Secur. J. A Glob. Perspect., vol. 27, no. 3, pp. 145–161, May 2018.

[27] J. Zhang and X. Li, "Phishing Detection Method Based on Borderline-Smote Deep Belief Network," Springer, Cham, 2017, pp. 45–53.

[28] P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, and T. Zhu, "Web Phishing Detection Using a Deep Learning Framework," Wirel. Commun. Mob. Comput., vol. 2018, pp. 1–9, Sep. 2018.

[29] D. Aksu, Z. Turgut, S. Üstebay, and M. A. Aydin, "Phishing Analysis of Websites Using Classification Techniques," Springer, Singapore, 2019, pp. 251–258.

[30] M. Pereira, S. Coleman, B. Yu, M. DeCock, and A. Nascimento, "Dictionary Extraction and Detection of Algorithmically Generated Domain Names in Passive DNS Traffic," Springer, Cham, 2018, pp. 295– 314.

[31] C. Sur, "DeepSeq: learning browsing log data based personalized security vulnerabilities and counter intelligent measures," J. Ambient Intell. Humaniz. Comput., pp. 1–30, Oct. 2018.

[32] G. Vrbančič, I. Fister, and V. Podgorelec, "Swarm Intelligence Approaches for Parameter Setting of Deep Learning Neural Network," in Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics - WIMS '18, 2018, pp. 1–8.

[33] J. Woodbridge, H. S. Anderson, A. Ahuja, and D. G. Endgame, "Detecting Homoglyph Attacks with a Siamese Neural Network."

[34] J. Saxe and K. Berlin, "eXpose: A Character-Level Convolutional Neural Network with Embeddings For Detecting Malicious URLs, File Paths and Registry Keys," Feb. 2017.

[35] K. Shima et al., "Classification of URL bitstreams using Bag of Bytes," 2018.

[36] J. Jiang et al., "A Deep Learning Based Online Malicious URL and DNS Detection Scheme," Springer, Cham, 2018, pp. 438–448.