Dom. Cien., ISSN: 2477-8818
Vol. 4, núm. 1, enero, 2018, pp. 115-130

Número Publicado el 01 de Enero de 2018

http://dx.doi.org/10.23857/dom.cien.pocaip.2017.4.1.enero.115-130
URL:http://dominiodelasciencias.com/ojs/index.php/es/index

Artículo Científico

Seguridad por capas frenar ataques de *Smishing*

Layered security stops smuggling attacks

Carlos José Martínez Santander [I]
Universidad Católica de Cuenca
carlos4553@hotmail.com-cmartinezs@ucacue.edu.ec

Yolanda de la Nube Cruz Gavilanes [II]
Corporación Nacional de Telecomunicaciones
nube5502@gmail.com-yolanda.cruz@cnt.gob.ec

Tania Magdalena Cruz Gavilanes [III]
Universidad Católica de Cuenca

María Isabel Álvarez Lozano [IV]
Universidad Católica de Cuenca

Recibido: 20 de octubre de 2017 ***** **Corregido:** 20 de noviembre de 2017 ***** **Aceptado:** 01 enero de 2018

I. Universidad Católica de Cuenca.
II. Corporación Nacional de Telecomunicaciones
III. Universidad Católica de Cuenca.
IV. Universidad Católica de Cuenca

Resumen

Hoy en día la tecnología móvil se ha convertido en una necesidad vital para la comunicación de los seres humanos. La convergencia digital ha hecho que a través de un dispositivo móvil podamos realizar múltiples tareas. Sin embargo, los atacantes han visto como oportunidad este avance para perpetrar diferentes ataques. Las técnicas usadas para los ciberatacantes es la de Ingeniería Social con sus variantes. En este artículo nos enfocamos en dar una solución ante el ataque de Smishing SMS dirigida a teléfonos celulares conocidos como Smartphone. La seguridad en capas ayuda a filtrar y detectar un porcentaje mayor de ataques. Un aspecto importante de esta propuesta es el valor que se da al usuario que usas las diferentes tecnologías, sin embargo, no tiene conocimiento de Seguridad Informática por lo que se toma en consideración dentro de un nivel de seguridad.

Para la construcción de la propuesta propuso en base a los estudios existentes, comprende una solución integra en donde se toman en cuenta a todos los actores inmiscuidos en un ataque de Smishing. Por otra parte, las empresas proveedoras del servicio de telefonía, deberían mejorar sus seguridades con soluciones de hardware, software y de recursos humanos.

Palabras clave: Smishing, SMS, Ingeniería Social, Phishing.

Abstract

Nowadays mobile technology has become a vital necessity for the communication of human beings. The digital convergence has made that through a mobile device we can perform multiple tasks. Nevertheless, the attackers have seen as an opportunity this advance to carry out different attacks. The techniques used for cyberattacks are Social Engineering with its variants. In this article we focus on providing a solution to the attack of Smishing SMS addressed to cell phones known as Smartphone. Layered security helps filter and detect a higher percentage of attacks. An important aspect of this proposal is the value that is given to the user that uses the different technologies, however, he is not aware of Computer Security so it is taken into consideration within a level of security.

For the construction of the proposal proposed based on existing studies, it comprises an integrated solution where all actors involved in a Smishing attack are taken into account. On the other hand, the companies that provide the telephony service, should improve their security with hardware, software and human resources solutions.

Key words: Smishing, SMS, Social Engineering, Phishing.

Introducción.

Las convergencias de las diferentes tecnologías han facilitado la comunicación entre los seres humano (Roco & Bainbridge, 2002), en la actualidad estamos en la capacidad de adquirir dispositivos móviles en los cuales: buscamos información, enviamos mensajes, realizamos llamadas telefónicas, etc. A si mismo los ciberfradudes han tenido una incidencia considerable en los últimos años (Cumming, Johan, & Schweizer, 2017). Cada vez es mayor el número de personas que han sido estafados por medio de estas tecnologías. Una de las practicas más usadas es la de Ingeniería Social, las técnicas abordadas son: Phishing, Farming, Vishing, Smishing, Grooming, entre otras (Wall, 2017).

Los hackers y personas curiosas son los que siempre están buscando nuevos métodos para violentar la privacidad a través de la explotación de alguna vulnerabilidad. Asegurar millones de computadoras resulta difícil y más aún dispositivos móviles que a diario se incrementa su uso. Una de las técnicas utilizadas para comprometer, robar o vulnerar las seguridades de estos dispositivos es la denominada Smishing (SMS Phishing) (Jonghyun BAEK & Heung Youl YOUM, 2015).

Smishin según Woong (Joo, Moon, Singh, & Park, 2017) en su investigación, define a este término como la combinación de la palabra “Phishing” y “SMS”. Smishing es un nuevo tipo de técnica de Phishing que roba la información de un usuario, usando el servicio de mensajería de texto (SMS) de un teléfono móvil, el nombre de Smishing fue dado por McAfee [(Anna Kang, Jae Dong Lee, Won Min Kang, Leonard Barolli, & Jong Hyuk Park, 2014) p. 467].

Es necesario definir medidas de seguridad para frenar estos ataques, varias empresas de seguridad han desarrollado módulos de defensa para prevenir o detectar estos delitos, sin embargo,

los ciberfradudes perpetrados por medio de esta técnica, siguen siendo perjudiciales, por lo que, es necesario tomar medidas correcticas a nivel de usuario.

El presente artículo propone medidas de seguridad a nivel de usuario ante los ataques de Smishing. Como sabemos el usuario final (persona que usa el dispositivo) es el eslabón más débil de la cadena de seguridad informática, razón por la cual, debe tener conocimiento de las medidas para minimizar el riesgo de ser víctima de este nuevo modo de ataque que afecta principalmente a la integridad y a la confidencialidad de la información.

Background

Smishing

Según (Joo, Moon, Singh, & Park, 2017)esta técnica se caracteriza por el engaño a los usuarios por medio del envío de mensajes de texto a los dispositivos móviles. Estos mensajes adjuntan links de URL maliciosas. Al remitente lo enmascara para que el receptor crea que es de confianza y acceda al link, esto desencadenara en el vector de ataque de esta técnica. Por consiguiente, se instala una aplicación malware que controla los teléfonos inteligentes, robando una gran cantidad de información personal guardada en el teléfono.

Fig. 1 Ataque Smishing

La Fig. 1 Presenta un esquema de cómo funciona el Smishing: (i) El atacante envía un SMS suplantando a un emisor confiable, con una URL del servidor falso, contiene el malware a ser instalado en el Smartphone. (ii) El usuario recibe el mensaje, asume que es real y abre el link. (iii) Lo siguiente es que automáticamente se instala un malware en el teléfono para de la misma manera, enviar toda la información contenida en su memoria hacia el servidor falso al que accede el atacante(Anna Kang, Jae Dong Lee, Won Min Kang, Leonard Barolli, & Jong Hyuk Park, 2014; Joo et al., 2017). Además de tener toda la información de la víctima, puede ejecutar comandos para ataques secundarios según sea el caso

Clasificación del Smishing

Según Kang *et al.*(Anna Kang et al., 2014) el Smishing se caracteriza por tener dos clasificaciones o dos vectores de ataque. El primero es cuando el atacante envía un mensaje de texto SMS con información de una compra, cambios, rembolsos o cancelaciones. El usuario se alarma por esta transacción y se deja engañar, el mensaje incluye un número de teléfono del atacante. El teléfono Smart permite la llamada a este número, comunicándose con el atacante quien solicita información personal del usuario o códigos necesarios para un micro pago en línea.

Esta forma de ataque se resume al robo de información mediante una conversación telefónica entre la víctima y el atacante. La segunda forma es a través del envió de un mensaje de texto SMS, este incluye una dirección URL que, al ser visitada por el usuario, un malware es instalado en su teléfono. Después replica toda la información del usuario almacenada en el teléfono al servidor del atacante.

Impacto del Smishing

Una de las causas para que los ciberdelincuentes usen la variante del Phishing es debido a que un mensaje de texto puede causar más pánico que un correo electrónico.

Generalmente este ataque contiene información de una institución Bancaria (Mun & Li, 2017) con un link al sitio web de la misma o un número de teléfono. Entonces el principal impacto que ha desencadenado este ataque es económico para los usuarios víctimas, perdidas por proveer datos de sus tarjetas o cuentas bancarias.

Otro impacto según (O. Salem, A. Hossain, & M. Kamala, 2013) es en la seguridad de las organizaciones, empresas o instituciones. Con el avance de la tecnología, son más los servicios empresariales a los que acceden sus trabajadores para buscar, modificar o crear nueva información por medio de dispositivos móviles ya sean celulares o tabletas. En la actualidad se puede utilizar dispositivos móviles hasta para iniciar sesión y hacer uso de algún servicio. Todo esto es un potencial peligro ya que los ciberdelincuentes y ciber espías han usado la técnica de Smishing para robar información valiosa.

APIs o librerías usadas para Smishing

Antes de iniciar cualquier ataque, es necesario para los atacantes conocer la información de las víctimas. Para esto se han desarrollado varias técnicas y a su vez el uso de APIs (Interfaz de Programación de Aplicaciones) para recolectar información de sus víctimas. Entre estas también se usan librerías («Procesamiento del lenguaje natural con NLTK para Ingeniería social automatizada», 2015) como por ejemplo la NLTK (Natural Language Tool Kit). Permite recolectar la información de las víctimas de redes sociales, donde normalmente exponemos nuestros datos sin ninguna seguridad.

Según Park (Wonjoo PARK, Sun-joong Kim, & Won Ryu, 2015) las APIs detectadas en ataques de Ingeniera Social son: ADRD, AnServerBot, DroidDream, DroidDreamLight, Genimi, GoldDream, jSMSHider, Kmin, Plankton, YZHC. Las librerías de Java Script son otras alternativas para recolectar la Información de las víctima.(«SAVE», 2017)

Trabajos relacionados

Para la realización del siguiente trabajo es necesario citar las siguientes investigaciones que están relacionadas directamente con el tema se estudió.

Krombholz (Krombholz, Hobel, Huber, & Weippl, 2015) en su investigación proporciona una clasificación y una visión general de los ataques más conocidos y avanzados de Ingeniería Social (IS), describe escenarios de ataque comunes para ataques modernos a personas con conocimientos de IS. Esta investigación consiste en una taxonomía completa de los ataques, a partir de canal de ataque, operador y tipos de ingeniería social y la segunda trata de ofrecer una variedad de vectores de ataque avanzados utilizados en los canales de comunicación populares y las

cuestiones específicas de la colaboración del personal conocedor de IS como los servicios en la nube, las redes sociales y los dispositivos móviles, como parte de las políticas de BYOD. Los autores no solo dan a conocer complejos escenarios avanzados de ataque, sino que también proporcionan una clasificación completa que puede servir como base para desarrollar contramedidas y más investigación interdisciplinaria en el campo, obteniendo el conocimiento necesario y detallado puede proteger a los trabajadores conocedores de ataques de ingeniería social.

En esta investigación *et al.* (Anna Kang et al., 2014) los autores discuten crímenes tales como Phishing, Phishing de voz y Smishing, que ocurren con frecuencia en un entorno de teléfonos inteligentes. El aporte de los investigadores es dar consideraciones de seguridad frente a los ataques de Smishing en teléfonos inteligentes.

La proliferación de servicios móviles basados en Near Field Communication (NFC) (Jonghyun BAEK & Heung Youl YOUM, 2015) en entornos móviles puede causar amenazas de seguridad en los servicios de aplicaciones móviles actualmente los problemas de ataques Phishing y Smishing móviles son uno de los dificultades de seguridad más graves en los servicios de aplicaciones móviles sobre todo os que están basados en etiquetas NFC ya que presentan una vulnerabilidad de seguridad, el dispositivo que utiliza esta etiqueta puede comunicarse por medio de utilizando el formato de datos especificado, denominado Formato de intercambio de datos (NDEF) este formato por texto, URI, mensaje inteligente (texto y URL). Por lo tanto, si un atacante sobrescribe el mensaje NDEF en una etiqueta o reemplaza una etiqueta NFC con una etiqueta hacheada, puede entregar un malware móvil a un dispositivo habilitado para NFC. Los autores en este documento proponen un protocolo de autenticación seguro y ligero para los servicios basados en etiquetas NFC que efectivamente logra la seguridad con la prevención de la falsificación, la modificación de datos y el ataque de

Phishing y Smishing. Además, estos protocolos de autenticación también requieren menos almacenamiento de memoria y poder computacional para etiquetas NFC de bajo costo muestra la Fig. 2.

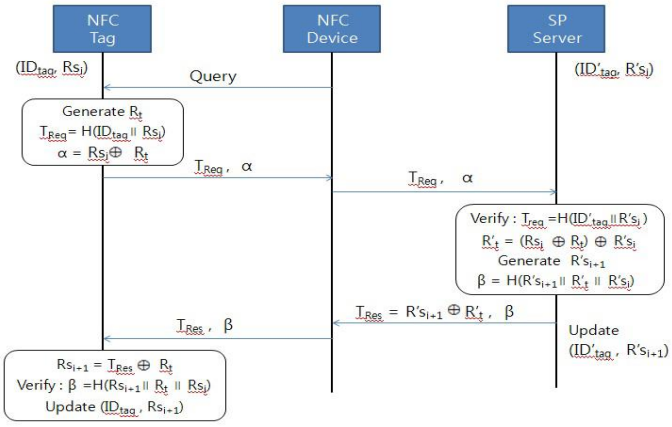

Fig. 2 Protocolo de autentificación NFC

El protocolo de autenticación propuesto tiene como objeto confirmar que la etiqueta actual es legítima antes de intercambiar datos entre etiquetas NFC y el dispositivo habilitado NF, además el protocolo confirmara que está listo para ser sobrescrito en la etiqueta del dispositivo confirmando su legitimidad, aquí proponen los autores utilizar la función hash y la operación XOR para la etiqueta y el dispositivo NFC (Jonghyun BAEK & Heung Youl YOUM, 2015).

Mun (Mun & Li, 2017) basado en que los atacantes quieren distribuir los códigos maliciosos por la URL corta a través de SMS, los hackers aprovechan esta vulnerabilidad para los ataques Drive-by-download Attack, Phishing y Smishing. La vulnerabilidad de la URL corta es que no puede averiguar la URL de destino hasta que haga clic. Con todo lo expuesto anteriormente se propone un método que escribe la información de destino al generar una URL corta para que un usuario pueda comprobar si el destino es un documento web o un archivo. El proveedor de servicios

de URL corta supervisa el riesgo de la página URL de destino de la URL corta generada y decide si debe proporcionar el servicio. Mediante el monitoreo de la modificación de un documento web, mide y evalúa el riesgo de la página web y decide si bloquea la URL corta de acuerdo con el umbral, lo que evita ataques como " unidad por descarga " a través de la URL corta.

Los autores del artículo (Joo et al., 2017) constataron la necesidad de adquirir elementos seguros para proteger la información de servicios móviles contra amenazas de seguridad. En particular, el daño de Phishing (Smishing) del servicio de mensajes cortos ha seguido aumentando con la normalización del entorno de computación móvil. Los autores analizaron las consideraciones de seguridad sobre Smishing en entornos de computación móvil y proponen un modelo de seguridad mejorado para detectar el ataque de Smishing (llamado "S-Detector"), El modelo propuesto se aplica a un clasificador Naive Bayes para mejorar la detección de ataques Smishing en dispositivos inteligentes. Este modelo distingue el mensaje de texto normal y el mensaje de Smishing. Y esto se utiliza principalmente para filtrar utilizando el método de aprendizaje estadístico. Como resultado, es posible analizar un mensaje de texto y detectar de forma efectiva el Phishing.

Este artículo (O. Salem et al., 2013) es una encuesta de literatura y un análisis sobre los ataques Phishing, Vishing y Smishing para explotar el conocimiento en la implementación de una herramienta inteligente para la detección y protección ya que es un problema de ingeniería social. Esta investigación ha prestado especial interés al correo electrónico Phishing, ya que se considera uno de los ataques más comunes a la vulnerabilidad individual. Está claramente demostrado que al determinar las principales diferencias entre los correos electrónicos legítimos y el Phishing, se puede reducir el riesgo de este tipo de ataque. Además, se ha explorado un sistema experto inteligente

basado en lógica difusa para evaluar su idoneidad para la detección y protección en tiempo real. Esta técnica puede ser aplicada al Smishin.

Park en su investigación (Wonjoo PARK et al., 2015) dice que el Smishing ataca e instala la aplicación maliciosa de ahí es explotado y comienza la fuga de información privada almacenada en el teléfono inteligente. Para esto presenta una solución que intercepta y reúne la aplicación maliciosa y la analiza en lugar del teléfono inteligente ya que puede bloquear la instalación de aplicaciones maliciosas en teléfonos inteligentes y también analizar de forma rápida y precisa. Además, una serie de aplicaciones maliciosas que apuntan al sistema operativo de Android son similares al malware conocido y vuelven a empaquetar una aplicación maliciosa existente. Presenta una característica única de que las aplicaciones descargadas pueden compararse con malware acumulados. En este artículo, se propone el sistema de detección de la aplicación maliciosa Android mediante el análisis estático junto con la similitud de características maliciosas del ataque.

Propuesta para Disminuir los Ataques Smishing

La siguiente propuesta está desarrollada en base a la literatura y al análisis de las diferentes propuestas para frenar los ataques de Smishing. Se presenta una solución por capas y como se pudo analizar el usuario no es tomado en consideración en otras conclusiones por lo que en este estudio se enfatiza en esta parte.

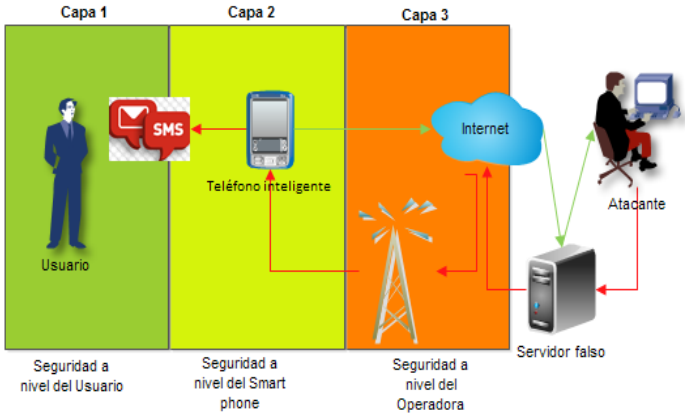

Fig. 3 Seguridad por capas para frenar ataques Smishing

Programa educacional sobre estos ataques. Esta medida de seguridad se debería abordar desde los primeros años del colegio, explicando que es el Smishing, cual es el vector de ataque, las variedades de estos ataques, se pueden usar ejemplos reales para que los futuros usuarios de teléfonos, conozcan normas de seguridad y así evitar que sean víctimas por desconocimientos de estos ataques. El usuario nunca debe dar detalles de datos bancarios ni de tarjetas de crédito por teléfono. Ignorar mensajes de textos de remitentes y texto desconocido. Reportar estas anomalías al departamento de seguridad de las operadoras móviles.

Las empresas dentro de sus políticas de seguridad deben instruir a sus empleados en temas de seguridad informática, también. Como se aborda al inicio de este artículo, el usuario final (Persona que utiliza el servicio o dispositivo y no conoce de seguridad informática) es una amanease para la cadena de seguridad informática, por tanto, al enfocarnos en su educación en estos temas, estamos fortaleciendo una debilidad y disminuyendo el número de posibles víctimas de estos ataques.

La Capa 2 asegura la información del usuario por medio de medios convencionales es decir con soluciones de software para dispositivos móviles. Una de estas soluciones es antivirus para

móvil, debe ser original y descargado de una fuente confiable, pagar un valor por su uso (licencia). Si el ataque llega a su último nivel que es la descarga y ejecución del malware, el antivirus debe estar en la capacidad de reconocer y eliminar o a su vez bloquear la amenaza.

Uso de una aplicación móviles de validación de URL(Anna Kang et al., 2014). Esta aplicación revisa y confirma si el link es seguro o malicioso. Para mejorar el proceso, se debe agregar una base de datos que todos los links analizados es decir una lista blanca y una negra.

La capa 3 se centra en Seguridad a Nivel de la Operadora móvil. En este punto las operadoras deben proteger a sus usuarios de estos ataques, deberían ser un porcentaje bajo de Smishing que llegue hasta el nivel 1 de usuario, los dos niveles deben ser filtros que detecten este ataque y no lo dejen pasar. En los servidores de las operadoras móviles se deben implementar soluciones de hardware y software para hacer frente a estos ataques. Métodos de detección y reconocimiento de URL cortas (Mun & Li, 2017). Para fortalecer más aun la seguridad, aplicar métodos como los que proponen en la investigación (Joo et al., 2017). Análisis a través de técnicas estadísticas como Bayesiana y la comparación de textos usados en estos ataques mediante técnicas de IA (Inteligencia Artificial) y Machine Learning (Aprendizaje de Maquina).

Conclusiones.

Como se hizo mención en esta investigación, el usuario que utiliza el dispositivo, es el que menos se considera en el proceso del aseguramiento de la información. Justamente la mayoría de ataques son perpetrados a través de ellos.

La literatura demuestra que al momento tenemos varias opciones que detectan Smishing, sin embargo, el porcentaje de ataques sigue siendo alarmante.

El modelo se propuso en base a los estudios existentes, comprende una solución integra en donde se toman en cuenta a todos los actores inmiscuidos en un ataque de Smishing.

Por otra parte, las empresas proveedoras del servicio de telefonía, deberían mejorar sus seguridades con soluciones de hardware, software y de recursos humanos.

Bibliografía.

1. Anna Kang, Jae Dong Lee, Won Min Kang, Leonard Barolli, & Jong Hyuk Park. (2014). Security Considerations for Smart Phone Smishing Attacks. *Springer-Verlag Berlin Heidelberg}, 1*, 467-473. https://doi.org/10.1007%2F978-3-642-41674-3_202

2. Cumming, D., Johan, S., & Schweizer, D. (2017). Information systems, agency problems, and fraud. *Information Systems Frontiers*, *19*(3), 421-424. https://doi.org/10.1007/s10796-017-9761-3

3. Jonghyun BAEK, & Heung Youl YOUM. (2015). Secure and Lightweight Authentication Protocol for NFC Tag Based Services. *Joint Conference on Information Security*, 1-6. https://doi.org/10.1109/AsiaJCIS.2015.35

4. Joo, J. W., Moon, S. Y., Singh, S., & Park, J. H. (2017). S-Detector: an enhanced security model for detecting Smishing attack for mobile computing. *Telecommunication Systems*, *66*(1), 29-38. https://doi.org/10.1007/s11235-016-0269-9

5. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

6. Mun, H.-J., & Li, Y. (2017). Secure Short URL Generation Method that Recognizes Risk of Target URL. *Wireless Personal Communications*, *93*(1), 269-283. https://doi.org/10.1007/s11277-016-3866-8

7. O. Salem, A. Hossain, & M. Kamala. (2013). Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks. *IEEE Internet Computing*, 1-3. https://doi.org/10.1109/CIT.2010.254

8. Procesamiento del lenguaje natural con NLTK para Ingeniería social automatizada. (2015, Febrero 17). Recuperado a partir de https://thehackerway.com/2015/02/17/procesamiento-del-lenguaje-natural-con-nltk-para-ingenieria-social-automatizada/

9. Roco, M. C., & Bainbridge, W. S. (2002). Converging Technologies for Improving Human Performance: Integrating From the Nanoscale. *Journal of Nanoparticle Research*, *4*(4), 281-295. https://doi.org/10.1023/A:1021152023349

10. SAVE: libro gratuito sobre Ingeniería Social. (2017, Marzo 30). Recuperado a partir de http://hackeruna.com/2017/03/30/save-libro-gratuito-sobre-ingenieria-social/

11. Wall, D. (2017). *Crime and Deviance in Cyberspace*. Routledge.

12. Wonjoo PARK, Sun-joong Kim, & Won Ryu. (2015). Detecting Malware with Similarity to Android applications. *Intelligent Convergence Media Research Department*, 1-3. https://doi.org/10.1109/ICTC.2015.7354788