Cuaderno Activa
Revista científica de la Facultad de Ingeniería

Técnicas de detección y control de phishing.

Detection and Control of Phishing Techniques.

Diana Sastoque Mesa*
Ricardo Botero Tabares**

Tipo de artículo: Revisión.

Recibido: 18 de Agosto, 2015.
Aceptado: 28 de Septiembre, 2015.

Resumen

La globalización de la economía y el uso masivo de Internet, han originado nuevos espacios para la comisión de fraudes en sistemas de cómputo con el uso de las nuevas tecnologías. En el presente artículo se describen de manera general los principales delitos informáticos, como la interceptación ilícita de correspondencia electrónica y el uso no autorizado de tarjetas y claves falsas, enfatizando en el phishing como uno de los fraudes de mayor crecimiento en los últimos años. Se describen las principales formas de introducir el phishing entre los clientes y usuarios por medio de la creación de un sitio web falso similar al sitio original; se exponen trabajos relacionados con el tema, como la clonación del perfil en una red social, el diseño de un prototipo de sistema que puede ser empleado por los usuarios para investigar si han sido víctimas de un ataque de phishing y el malware que ataca en redes sociales. Finalmente, se identifican algunas técnicas para la detección de phishing.

Palabras clave: Delitos informáticos, phishing, técnicas anti-phishing.

Abstract

The globalization of the economy, and the widespread use of Internet have led to new spaces for committing fraud in computer systems with the use of new technologies. This article describes, in general, major computer-related crimes, such as unlawful interception of e-mail correspondence, the unauthorized use of cards, and false PINs, emphasizing phishing as one of fastest-growing scams in recent years. The main ways to phish customers and users are described through the creation of a fake web site similar to the original site. Related studies are discussed, such as the cloning of profiles on social networks, the design of a prototype system that can be used by users to investigate whether they have been victims of a phishing attack and malware that attacks on social networks. Finally, some techniques for detecting phishing are identified.

Keywords: cybercrime, phishing, anti -phishing techniques.

* Ingeniera de Software. Estudiante Especialización en Seguridad de la Información. Tecnológico de Antioquia - Institución Universitaria. sastoque30@gmail.com

** Magíster en Ingeniería (Área Sistemas y Computación). Profesor Facultad de Ingeniería. Tecnológico de Antioquia - Institución Universitaria. rbotero@tdea.edu.co

Introducción

La expansión de Internet ha conllevado múltiples beneficios para la humanidad, que van desde los motores de búsqueda para la consulta de todo tipo de información, la prestación de servicios en los sitios web corporativos y los diarios online, hasta el esparcimiento con videos y juegos. Sin embargo, no todo es beneficioso en la red de redes, porque de forma oculta se presentan fraudes o delitos informáticos de variada índole: la suplantación de identidad en redes sociales, la pornografía infantil, la interceptación ilícita de correo electrónico, el acceso ilegitimo a un sistema informático, la estafa en mercados virtuales y los desfalcos por phishing. Sobre este último trataremos en este artículo.

El phishing, contracción de "passwod harvesting fishing"(cosecha y pesca de contraseñas), consiste en duplicar una página web para hacer creer al visitante que se encuentra en la página original de una entidad, empresa o institución de confianza, con el objetivo de obtener de forma fraudulenta información personal como contraseñas, números de tarjetas de crédito, documentos de identidad o cualquier otro dato de interés para el ciberdelincuente (Usera, 2007).

Este artículo tiene la siguiente estructura: Se presenta un bosquejo teórico de los principales delitos informáticos. Se describe el delito de phishing y las maneras como se introduce entre los clientes y usuarios. Se exponen algunos trabajos relacionados con los delitos informáticos, enfatizando en el phishing y se identifican algunas técnicas para detección de phishing; finalmente se presentan las conclusiones del trabajo.

Marco teórico

Los delitos informáticos

La historia de la humanidad evidencia delitos desde tiempos inmemoriales, denunciados por periodistas en los medios masivos de comunicación, descritos por literatos en obras inmortales y desdeñados por profetas en textos sagrados; delitos que han originado controles y condenas, legislados en los diferentes pueblos y naciones. La cultura digital y la globalización han causado otros tipos de transgresiones denominadas delitos informáticos, dando origen a un nuevo vocabulario de términos como ciberdelincuente, cracker, hacker, ciberdelito, malware y phishing, entre otras denominaciones.

Un delito informático es una nueva forma de conducta que tiene por medio o finalidad los sistemas informáticos e Internet (Díaz, 2010). Existe una amplia posibilidad de tipificación para estos delitos, como se ilustra en la Tabla 1, algunos de ellos tipificados en la legislación común. Teniendo en cuenta la Teoría del delito (Radbruch, 2010), la informática avanza más rápido que la legislación, por lo cual existen conductas criminales por vías informáticas que aún no se tipifican como delitos.

Tabla 1. Principales delitos informáticos

No.	Descripción
1	Interceptación ilícita de correspondencia electrónica
2	Acceso ilegítimo a un sistema o dato informático
3	Revelación de secretos en una empresa
4	Ataques a la integridad de los datos personales
5	Falsificación informática
6	Delitos relacionados con la pornografía infantil
7	Uso no autorizado de tarjetas y claves falsas
8	Phishing

Fuente: elaboración propia (2015).

Una breve descripción de cada uno de estos delitos es la siguiente:

- Interceptación ilícita de correspondencia electrónica: consiste en interceptar por cualquier medio mensajes de correo electrónico con el objetivo de conocer información confidencial de personas o corporaciones.

- Acceso ilegítimo a un sistema o dato informático: es el uso ilegítimo de contraseñas para la entrada en un sistema informático sin la autorización del propietario.

- Revelación de secretos en una empresa: comete este delito quien se apodere por cualquier medio de datos, documentos escritos o electrónicos o soportes informáticos para descubrir un secreto de empresa; también puede incurrir en este delito quien intercepte telecomunicaciones o utilice artificios técnicos de escucha, grabación, transmisión o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, con el objetivo de transmitirlos a personas no autorizadas.

- Ataques a la integridad de los datos personales: la Ley de Protección de Datos Personales reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

- Falsificación informática: es la alteración, imitación, falsificación de documentos electrónicos. Con la invención de fotocopiadoras computarizadas en color a base de rayos láser surgieron nuevas técnica de adulteración. Estas máquinas pueden hacer copias de alta resolución, modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, tan "reales" que sólo un experto puede diferenciarlos de los documentos auténticos.

- Delitos relacionados con la pornografía infantil: se refiere al abuso y explotación sexual de menores de edad con algún fin de lucro, se cataloga como delito trasnacional penado con cárcel en cualquier parte del mundo. Este delito se propaga por medio de vendedores de DVD, CD, etc., bandas de personas que se encargan de la prostitución o venta de menores por medio de la publicación de videos, fotos o acuerdos en citas de encuentro.

- Uso no autorizado de tarjetas y claves falsas: el desarrollo del comercio electrónico explica la obtención de dinero en cajeros automáticos mediante el uso de tarjetas de crédito o débito falsificadas o sustraídas.

- Phishing: luego de obtener los datos personales de un individuo, se procede a realizar todo tipo de operaciones para provecho del victimario, fingiendo ser la persona a la que se extrajo su información sensible.

El phishing y su propagación

Una red social está diseñada para crear y mantener vínculos con otros; junto a los blogs y las páginas de contactos online, son "portales de identidad" (Escobar & Román, 2011) en los que los usuarios construyen y expresan su "yo", publicando características de sí mismos y agregando y compartiendo su actividad en Internet. Y es precisamente en las redes sociales donde se propaga el phishing: cualquier intento de acceder a información confidencial del usuario, como su contraseña y número de tarjeta de crédito por técnicas de ingeniería social.

Según informe publicado por el grupo de trabajo Anti-Phishing (APWG, 2013), las entidades financieras y en general las divisiones de intercambio de dinero, fueron expuestas a constantes ataques de phishing. Para aumentar su tasa de éxito, los atacantes intentan presentarse de manera que las víctimas confían en ellos y los aceptan como agentes legales de bancos auténticos. En este tipo de ataques, los phishers (personas que llevan a cabo ataques de phishing) diseñan una página web similar a la original, y luego sugestionan a sus víctimas para ir a su página web e introducir su información confidencial. El phisher trata de atraer la atención de sus víctimas con productos interesantes, para obtener su nombre, dirección, número de teléfono o cualquier información que pueda utilizar para avanzar en sus intenciones.

Como se ilustra en la Figura 1 (Dadkhah & Davarpanah, 2014a), el proceso de realización de un ataque de phishing tiene cuatro pasos:

1. Se crea un sitio web falso similar al sitio original.
2. El atacante envía a muchos usuarios de organizaciones y empresas el enlace de la página web falsa, y trata de animar a los usuarios a visitar su sitio web.
3. Las víctimas ingresan sus datos al visitar el sitio web falso.

4. El atacante roba información de las víctimas y empieza el fraude.

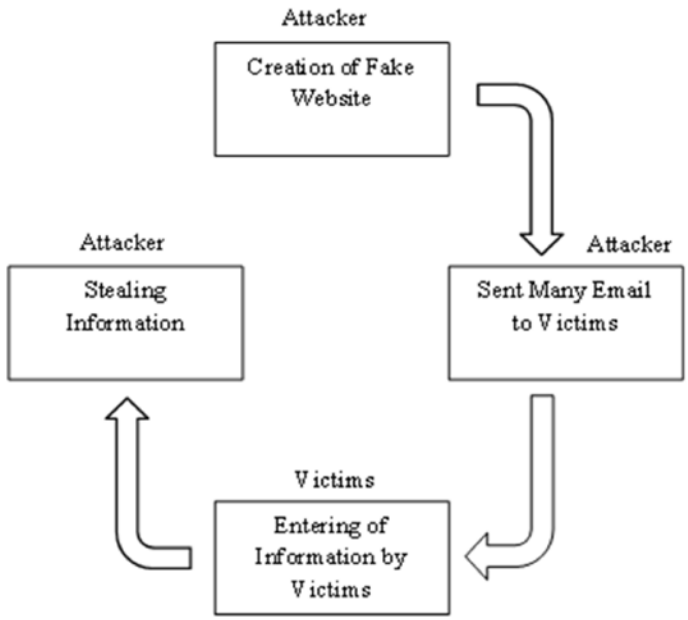

Figura 1. Proceso de un ataque de phishing.
Fuente: Dadkhah & Davarpanah (2014).

El phishing se clasifica en diferentes grupos basados en su método de ataque, que incluye phishing engañoso (Mahmood & Rajamani, 2012), phishing basado en malware (Li & Schmitz, 2009), phishing por envenenamiento de archivos Hosts (Dadkhah & Davarpanah, 2014b), inyección de contenido phishing (Alkhateeb et al., 2012), secuestro de dominio (Chandavale & Sapkal, 2010), archivo PDF phishing (Hong, 2012) y spear phishing (Agarwal et al., 2009). En su conjunto, para la identificación y reconocimiento de los ataques de phishing, es necesario el conocimiento de gran volumen de la información que no siempre está disponible.

Trabajos relacionados con el phishing

El phishing en redes sociales ha sido tema de estudio de muchos investigadores. Encuestas recientes con dos grupos de perfiles personales de usuarios que no tienen amigos y perfiles de usuarios con amigos ficticios, muestran que la ingeniería social puede ser mal utilizada por los atacantes sobre redes sociales, con la finalidad de obtener información confidencial. Hay un conflicto entre la conciencia de seguridad de los usuarios y su comportamiento real, llamada paradoja de privacidad. Interesa la cantidad de información que la gente está dispuesta a revelar en sus perfiles y se ha descubierto el comportamiento de los usuarios que conduce a la insuficiente protección de la información publicada, sensibles para todo tipo de phishing y otros ataques similares (Coronges et al., 2012).

(Kontaxis et al., 2011) propone una metodología para detectar la clonación del perfil en una red social; además, presenta el diseño de la arquitectura y los detalles de la implementación de un prototipo de sistema que pueden ser empleadas por los usuarios para investigar si han sido víctimas de un ataque de ese tipo. Los resultados experimentales del uso de este sistema por los usuarios habituales, demuestran su eficacia y simplicidad. Nagy & Pecho (2009) indican que es probable que un clic en un enlace a una página web que aparece en un mensaje de un amigo en Facebook o Twitter, puede ser aprovechado por atacantes para suplantar a ese individuo. La creciente

popularidad de estas redes de amigos ha conducido a un aumento correspondiente en el spam, el phishing y malware en sitios de redes sociales.

Una clase de malware que ataca en redes sociales son los botnets (Quanyan et al., 2013), término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y se usan para diversas actividades criminales. Los delincuentes distribuyen software malintencionado (también conocido como malware) que puede convertir su equipo en un bot (también conocido como zombie). Cuando esto sucede, un equipo puede realizar tareas automatizadas a través de Internet sin que su propietario y usuario habitual lo sepa.

Técnicas de detección de phishing

Muchos intentos y estudios se han realizado para hacer frente a ataques de phishing y se han creado muchas soluciones diferentes para la detección de ellos, como el sello de inicio de sesión (Aburrous et al., 2013), desarrollo de un sistema experto basado en las características de las páginas web para detectar sitios web de phishing (Shreeram et al., 2010), algoritmo genético basado en técnicas anti-phishing (Chen & Guo, 2006), detección de ataques de phishing basado en la categorización de enlaces (Atighetchi & Pal, 2009), prevención de ataques de phishing basada en atributos (Dunlop et al., 2010), contenido basado en antiphishing (Mishra & Gaurav, 2012), confrontación a los ataques de phishing por la identificación de dos etapas (Liu et al., 2010), detección de páginas phishing basada en relaciones asociadas (Reddy et al., 2011), uso de algoritmos de minería de datos (Nikulchev & Pluzhnik, 2014) y teoría del caos (Dadkhah et al., 2015). Todas las técnicas mencionadas se centran en detectar y contrarrestar ataques de phishing. Al mismo tiempo, para la identificación y prevención de ataques de phishing es necesario conocer su periodicidad para llevar a cabo el análisis detallado de este tipo de ataques.

Existen sitios antiphishing que analizan en "tiempo real" cualquier URL solicitado por los usuarios, para comprobar los riesgos de phishing usando cientos de las "funciones" del sitio. Estas funciones evalúan el contenido de la página, la información de reputación del dominio, además de muchos otros factores. El aprendizaje mecanizado por inteligencia artificial determina cuáles son las funciones significativas para cada URL revisada y el peso que se debe aplicar a cada una de ellas en la clasificación.

Un mecanismo que se ha propuesto para reducir los correos de phishing en tiempo real es el método denominado IBC (Intelligent Based Classification), el cual utiliza un algoritmo de filtrado y clasificación inteligente que detecta los correos electrónicos de phishing por sus propias características. El algoritmo de clasificación detecta ataques de phishing y protege a los usuarios de los enlaces poco fiables, mensajes instantáneos y páginas web, además, puede detectar hasta un 96% de los ataques de phishing en tiempo real.

Otra alternativa en la investigación de los ataques de phishing es la aplicación de la teoría del caos. La metodología dada ha encontrado amplia aplicación en la investigación de los contenidos de información relacionada con datos sobre el tráfico de las redes informáticas. Pero, como se ha dicho antes, el análisis y la investigación de los ataques de phishing se complican por dos motivos: primero, la escasa información acerca de tales ataques, y segundo, la complejidad en la recepción de la correspondiente información sobre phishing. Sin embargo, desde el punto de vista de la investigación de los ataques de phishing, como regla general, hay datos que caracterizan a la cantidad diaria de ataques padecidos o identificados. Tales datos, al menos, permiten juzgar la capacidad de ataques a partir de su recálculo diario a durante un periodo de tiempo. Por lo tanto, en su conjunto, es posible identificar el cambio de la capacidad de ataques de phishing en un periodo de tiempo que permite asignar valores de incidencia o intensidad de estos ataques en ciertos intervalos, o su uniformidad. De esta manera, tales conclusiones pueden ser útiles para la posterior predicción

de crecimiento de los ataques de phishing y su prevención. Esta alternativa tiene , como objetivo principal la consideración y la investigación del cambio de la capacidad de ataques de phishing por medio de métodos de la teoría del caos.

Conclusiones

Hoy en día, detectar los delitos informáticos, en especial phishing, es uno de los grandes desafios de la comunidad de Internet. Una vez franqueado el proceso de autenticación, no resulta complicado para el delincuente realizar un fraude informático. Por tal motivo se ha propuesto una serie técnicas de detección de phishing, que aunque no constituyen una solución definitiva, sí controlan en gran medida estos ataques. Entre estas técnicas se encuentran el algoritmo inteligente basado en clasificación (IBC) para detectar los correos electrónicos de phishing, un sistema experto basado en las características de las páginas web, y algoritmos de minería de datos, entre otros.

Resulta llamativo que no exista en el Código Penal una regulación específica contra la suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico. Esta ausencia provoca una serie de consecuencias indeseables: desde la falta de datos oficiales fiables sobre el fenómeno -lo cual que permite la manipulación interesada de algunos estudios no precisamente imparciales, elaborados por fundaciones o instituciones creadas con el apoyo de empresas que ofrecen productos de seguridad informática-, hasta la inseguridad jurídica que provoca la diversidad de tratamientos que a una misma conducta dan los jueces y tribunales, creando desconcierto en los aplicadores del Derecho y desigualdad entre los condenados por hechos similares, si es que no idénticos.

Referencias

Aburrous M., Hossain M. A., Dahal, K. & Thabat, F. (2010). Intelligent Phishing Detection System for E-Banking Using Fuzzy Data Mining. Expert Systems with Applications, 37, 7913–7921.

Agarwal, N., Renfro, S. & Bejar, A. (2009). Yahoo Sign-In Seal and Current Anti-Phishing Solutions. eCrime Researchers Summit, 1-4.

Alkhateeb, F., Manasrah, A. & Bsoul, A. (2012). Bank Web Sites Phishing Detection and Notification System Based on Semantic Web technologies. International Journal of Security & Its Applications, 6(4), 1-14.

APWG: Anti-phishing Work Group. (2013). Phishing Activity Trends Report, 2nd Quarter 2013. Recuperado de: http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf

Atighetchi, M. & Pal, P. (2009). Attribute-based Prevention of Phishing Attacks. Eighth International Symposium on Network Computing and Applications (IEEE). Cambridge, England.

Chandavale, A. A. & Sapkal, A. M. (2010). Algorithm for Secured Online Authentication Using CAPTCHA. Third International Conference on Emerging Trends in Engineering and Technology, 19-21.

Chen, J. & Guo C. (2006). Online Detection and Prevention of Phishing Attacks. First International Conference on Communications and Networking (IEEE), China.

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J. & Rovira, E. (2012). The Influences of Social Networks on Phishing Vulnerability. 45th Hawaii International Conference on Year: 2012. Hawaii, USA.

Dadkhah, M. & Davarpanah, J. M. (2014a). Secure Payment in E-commerce: Deal with Keyloggers and Phishings. International Journal of Electronics Communication and Computer Engineering, 5(3), 656-660.

Dadkhah, M. & Davarpanah, J. (2014b). A Novel Approach to Deal with Keyloggers. Oriental Journal of Computer Science & Technology, 7(1), 25-28.

Dadkhah, M., Lyashenko, V. & Jazi, M. (2015). Methodology of the Chaos Theory in research of phishing attacks. International Journal of Academic Research, 7(1).

Díaz, G. A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución. REDUR, (8), 169-203.

Dunlop, M., Groat, S. & Shelly, D. (2010). Gold Phish: Using Images for Content-Based Phishing Analysis. Fifth International Conference on Internet Monitoring and Protection. Barcelona, España.

Escobar, M. & Román, H. (2011). La presentación del yo en el ciberespacio: un análisis de las autodefiniciones personales en blogs y redes sociales. Revista de Psicología Social, 26 (2), 207-222.

Hong, J. (2012). The State of Phishing Attacks. Communications of the acm, 55(1), 74-81.

Kontaxis, G., Polakis, I., Ioannidis, S. & Markatos, E. P. (2011). Detecting social network profile cloning. Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE International Conference. Sydney, Australia.

Li, S. & Schmitz, R. (2009). A Novel Anti-Phishing Framework Based on Honeypots. eCrime Researchers Summit (IEEE), 1-13.

Liu, G., Qiu, B. & Wenyin, L. (2010). Automatic Detection of Phishing Target from Phishing Webpage. International Conference on Pattern Recognition (IEEE). Istanbul, Turkey.

Mahmood, A. & Rajamani, L. (2012). APD: ARM Deceptive Phishing Detector System Phishing Detection in Instant Messengers Using Data Mining Approach. Springer. Verlag Berlin Heidelberg, 269, 490-502.

Mishra, M. & Gaurav, J. (2012). A Preventive Anti-Phishing Technique using Code word. International Journal of Computer Science and Information Technologies, 3(3), 4248-4250.

Nagy, J. & Pecho, P. (2009). Social Networks Security. Emerging Security Information, Systems and Technologies. SECURWARE '09. Third International Conference on Year: 2009. Athens/Glyfada, Greece.

Nikulchev, E. & Pluzhnik, E. (2014). Study of Chaos in the Traffic of Computer Networks. International Journal of Advanced Computer Science and Applications, 5(9), 60-62.

Quanyan, Z., Clark, A., Poovendran, R. & Başar, T. (2013). Deployment and Exploitation of Deceptive Honeybots in Social Networks. 52nd IEEE Conference on Decision and Control, Florence, Italy.

Radbruch, G. (2010). Sobre el sistema de la teoría del delito. Revista electrónica de ciencia penal y criminología, (12). Recuperado de: http://criminet.ugr.es/recpc/12/recpc12-r1.pdf

Reddy, V., Radha, V. & Jindal, M. (2011). Client Side protection from Phishing attack. International Journal of Advanced Engineering Sciences and Technologies, 3(1), 39-45.

Shreeram, V., Suban, M., Shanthi, P. & Manjula, K. (2010). Anti-phishing detection of phishing attacks using genetic algorithm. IEEE International Conference on Communication Control and Computing Technologies (ICCCCT).Ramanathapuram, India.

Usera, L. (2007). Desfalcos por "phishing". Escritura pública, (46), 24-26.

Dianthus / Autor: Diego Alonso Rivera Vergara