Ingeniería Social: Ataques y Estrategias de Defensa

Alejandra Di Gionantonio, Laura Ligorria
Universidad Tecnológica Nacional, Facultad Regional Córdoba. Maestro M. López esq. Cruz Roja Argentina, CP (X5016ZAA)
Ciudad Universitaria – Córdoba – Argentina.
emails: ing.alejandradg@gmail.com

Resumen - *Los ataques de Ingeniería Social están generando preocupación en las organizaciones, ya que vulneran los mecanismos de defensa tradicionales pese a las grandes inversiones en temas de seguridad informática.*

El presente trabajo explica el funcionamiento de los ataques de Ingeniería Social, su significado, formas de ataque y medidas de protección para defender a la empresa.

Palabras claves: *hackers, phishing, spam, chat, Spyware*

Social Engineering: Attacks and Defense Strategies

Abstract - *Social Engineering attacks are generating concern in organizations, because this type of attack violates the traditional defense mechanisms despite their large investments in computer security issues.*

This paper explains the functioning of Social Engineering attacks, its meaning, forms of attack and protective measures to defend the company.

Keywords: *hackers, phishing, spam, chat, Spyware*

1. INTRODUCCIÓN

La Ingeniería Social es una disciplina del campo de la Seguridad Informática cuyo objetivo es recabar información sobre una empresa o sujeto para analizarla, definir lo que está haciendo y diseñar la estrategia de ataque. Logra sus propósitos manipulando a las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizarían y que revelarán todo lo necesario para superar barreras de seguridad (Fig.1) (Borghello, 2011).

El principio que la sustenta es que en cualquier sistema los usuarios son el eslabón más débil (Ardita, 2008; Solms, 2004).

Se vale de técnicas psicológicas y de la ingenuidad de las personas que tienden a reaccionar de manera predecible ante ciertas situaciones. En primer lugar, genera una empatía con la víctima y luego explota la situación de confianza lograda. Así, por ejemplo, los usuarios renuevan una clave ante el pedido de un supuesto administrador del sistema o confían detalles financieros ante un aparente funcionario bancario o dan datos personales ante un atribuido acierto en un imaginario sorteo. Esta técnica es sencilla y rápida, no requiere conocimiento técnico. (Visentini, 2006).

Este artículo se organiza de la siguiente manera: en la sección 2 mencionamos los tipos de atacantes, en la sección 3 mecanismos más comunes de ataque, en la sección 4 se analiza la efectividad de la Ingeniería Social, en la sección 5 se hace referencia a las medidas de protección, y finalmente en la sección 6 se exponen las conclusiones finales.

Fig. 1 - *El arte de manipular a las personas*

2. TIPOS DE ATACANTES

Estas actividades son efectuadas por personas clasificadas en los siguientes grupos (Universidad Virtual del Tecnológico de Monterrey, 2003; Asier et al,, 2011):

2.1 El Hacker

El Hacker es una persona con amplios conocimien-

tos en tecnología, bien puede ser informática, electrónica o comunicaciones. Se mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos encriptados y las posibilidades de acceder a cualquier tipo de "información segura".

Su formación y las habilidades que posee les dan una experticia mayor para superar, sin ser detectado por las barreras de seguridad que tienen los sistemas. Por lo general no hacen daño, sólo se contentan con ingresar, algunas veces dejar un mensaje, salir sin ser descubiertos y también les dan la posibilidad de difundir sus conocimientos para que las demás personas se informen de cómo funciona la tecnología y conozcan las vulnerabilidades de sus propios sistemas de información.

2.2 El Cracker

Es una persona que presenta un comportamiento compulsivo, que alardea de su capacidad para destruir sistemas electrónicos e informáticos.

Es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para liquidar software y comunicaciones como el teléfono, el correo electrónico o el control de otras computadoras remotas. Ingresa a los sistemas informáticos de una manera maliciosa, rompiendo computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas. Muchos de ellos "cuelgan" páginas Web por diversión o envían a la red su última creación de virus polimórfico.

2.3 El Lammer

A este grupo pertenecen aquellas personas deseosas de alcanzar el nivel de un hacker pero su poca formación y sus conocimientos les impiden realizar este sueño. Su trabajo se reduce a ejecutar programas creados por otros, a bajar, en forma indiscriminada, cualquier tipo de programa publicado en la red.

Es el más numeroso que existe en la red; sus más frecuentes ataques se caracterizan por bombardear permanentemente el correo electrónico para colapsar los sistemas, emplear de forma habitual programas sniffers para controlar la red, interceptar contraseñas y correos electrónicos, y después enviar mensajes con direcciones falsas, en muchas ocasiones, amenazando el sistema, lo que en realidad no es cierto: su alcance no va mucho más allá de poseer el control completo del disco duro, aun cuando el ordenador esté apagado.

También emplean los Back Oriffice, Netbus o virus con el fin de fastidiar, sin dimensionar las consecuencias de sus actos. Su única preocupación es su satisfacción personal.

2.4 El Copyhacker

Son una nueva generación de falsificadores dedicados al crackeo de Hardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura y después venderlos a los "bucaneros". Los Copyhackers se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.

2.5 Bucaneros

Son los comerciantes de la red más no existen en ella; aunque no poseen ningún tipo de formación en el área de los sistemas, sí poseen un amplio conocimiento en el área de los negocios.

Su objetivo es comercializar los productos que los Copyhackers les proporcionan bajo un nuevo nombre comercial, obteniendo lucro personal en corto tiempo y con el mínimo esfuerzo.

2.6 Phreaker

Poseen vastos conocimientos en el área de telefonía terrestre y móvil. Con el auge de los celulares han tenido que ingresar también al mundo de la informática y del procesamiento de datos.

Su actividad está centrada en romper las seguridades de las centrales telefónicas, desactivando los contadores con el fin de realizar llamadas sin ningún costo.

Actualmente las tarjetas prepagas son su campo de acción predilecto. Suelen operar desde cabinas telefónicas o móviles y a través de ellas pueden captar los números de abonado en el aire y así crear clones de tarjetas telefónicas a distancia.

2.7 Newbie

Es el típico "cacharrero" de la red. Sin proponérselo tropieza con una página de Hacking y descubre que en ella existen áreas de descarga de buenos programas de Hackeo, baja todo lo que puede y empieza a trabajar con ellos.

Es un aprendiz paciente e inofensivo, puede detectar sistemas de fácil acceso y también programas con un grado de dificultad mayor, para lo cual tiene que recurrir nuevamente a la red en busca de instrucciones que le permitan lograr su objetivo.

Son más precavidos y cautelosos que los lammers, aprenden de los métodos de hacking, sacan provecho de todo lo que aprenden, por lo general llegan tanto a apasionarse por la informática, la electrónica y las telecomunicaciones que aspiran a llegar a ser hacker.

2.8 Script Kiddie

Denominados también "Skid kiddie", son simples usuarios de Internet, sin conocimientos sobre Hack o Crack. Aunque aficionados a estos temas no los comprenden realmente, simplemente son internautas que sólo recopilan información de la red y buscan programas que luego ejecutan sin ningún tipo de conocimientos, infectando en algunos casos de virus a sus propios equipos.

3. FORMAS DE ATAQUE

A pesar de los constantes esfuerzos por parte de las organizaciones de concientizar a los usuarios, la Ingeniería Social se ha expandido a través de Internet afectando numerosas computadoras (Abraham et al., 2010).

Además, los empleados han comenzado a usar sus dispositivos móviles personales, tabletas, netbooks, smartphones, superando las capacidades y ventajas de los equipos ofrecidos por las organizaciones. De este modo realizan su trabajo conectándose directamente a los recursos de información internos con el riesgo que esto conlleva (Durbin, 2011).

3.1 Teléfono

Es uno de los ataques más eficientes por tratarse de un medio familiar e impersonal. Debido a que las expresiones del rostro no son reveladas, el atacante puede utilizar todo su potencial de persuasión. Es una de las formas más antiguas y más usadas (Fig. 2) (Microsoft, 2006).

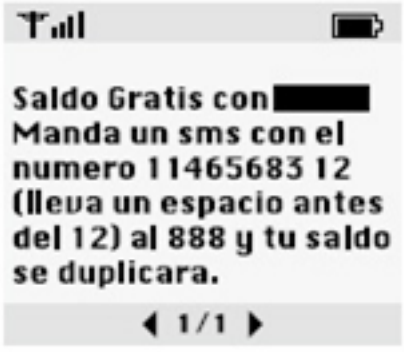

Fig. 2 - *Ataques telefónicos*

3.2 Ataques Vía Web

A mediados de abril del 2009 surgió otra técnica de engaño que consistió en que los usuarios accedieran a visualizar un video en Internet debiendo realizar la descarga del mismo a través de un código. Si los usuarios completaban las instrucciones solicitadas, implicaba la descarga de un código malicioso detectado por ESET NOD32 como parte de la familia TrojanDropper.Agent.

En la misma época se registró un incremento importante en la cantidad y variedad de phishing Scam, siendo uno de los casos más vistos el de supuestas cartas de amor que en realidad apuntaban a que el usuario entregara su dinero a los atacantes (ESET, 2011).

- ***Phishing***

El intruso pide información mediante un mensaje de correo electrónico enviado a través de una cuenta normalmente falsificada, que procede aparentemente de un negocio o empresa legítima y digna de confianza (banco o compañía de crédito) solicitando verificación de los datos y advirtiendo sobre las consecuencias que le acarrearía al receptor no hacer dicha verificación. Si un usuario standard lee una petición que parece provenir de una dirección válida, hay posibilidades de que no dude en responder.

- ***Chat***

En estos medios los crackers mandan mensajes a cientos de usuarios, con la seguridad de que algunos caerán en la trampa, en los que se hacen pasar por operarios del sistema y advierten al usuario que requiere un programa, o bien le ofrecen software gratis.

El software que el usuario recibe puede ser un caballo de Troya, que le permitirá al cracker controlar la computadora de manera remota y copiar o destruir la información. O bien puede ser un keylogger o grabador de teclas, que guarda en memoria todo lo que se escribe en el teclado y luego lo envía al intruso; analizando las teclas oprimidas, el cracker puede deducir fácilmente las contraseñas del usuario.

- ***Spyware***

El Spyware o software espía recopila información desde una computadora sin el consentimiento del usuario (particular o empresa). Busca información especial del mismo para conocer las actividades que realiza en Internet para luego generar estadísticas. Este método se utiliza para vender información a las empresas y ofrecer productos a medida.

No es el ataque más dañino de Ingeniería Social, pero sigue siendo invasión a la privacidad.

Los Spyware más perjudiciales son los que capturan, guardan y envían al atacante todo lo que se ingresa desde el teclado. Incluso los más avanzados pueden hasta vigilar a un usuario con su propia web-cam o micrófono sin que el mismo usuario sepa que estos dispositivos se encuentran activados. Éstos pueden ser instalados en una computadora personalmente, o mediante virus o un troyano que se distribuye a través de correo electrónico.

3.3 Ataques cara a Cara

Son los más eficientes pero los más difíciles de realizar, ya que el intruso debe hacerse presente de forma física, lo que representa un mayor peligro para el mismo. La víctima ha de ser alguien con un alto nivel de

desinformación y de desconocimiento. También son susceptibles aquellos en los que su mente no está preparada para tal maldad (ancianos, niños, personas insanas), lo cual es una condición suficiente pero no necesaria. En realidad este tipo de ataque tiene éxito a causa de una mala cultura organizacional acerca del problema de la seguridad informática. Por ejemplo los operarios de los sistemas no son los responsables mayores. Si este ataque surte efecto es porque los directivos de la organización fallaron en inculcar en la empresa las medidas de prevención necesarias para evitar los ataques. Por otra parte, la efectividad del ataque dependerá notablemente de la experiencia del atacante. Por ejemplo Kevin Mitnick dio una conferencia en el año 2005 en Buenos Aires y mostró cómo pudo acceder fácilmente al código de un teléfono móvil que aún estaba en etapa de desarrollo (todavía no se había anunciado al mercado). Para ello sólo hizo seis llamadas telefónicas, en unos cuantos minutos.

3.4 Redes inalámbricas WI-FI

Las redes inalámbricas presentan riesgos para la seguridad de los usuarios. Entre las amenazas informáticas que pueden propagarse por medio de una conexión Wi-Fi podemos mencionar: sniffing, fuga de información, interceptación de accesos por medio de una red gemela y los intentos de ataque 0-day o Día cero.

Utilizar una conexión gratis puede tener un alto costo ya que las credenciales de acceso y el tráfico de la red puede ser espiado y capturado y la información que está siendo transmitida robada. El truco ocurre por medio de una tecnología proxy que intercepta, captura y almacena una copia de las comunicaciones Wi-Fi en el equipo del ciberatacante, enviando luego la información a la red inalámbrica correcta. Esto ralentizará el tráfico del equipo levemente, pero en el caso de conexiones muy congestionadas es difícil saber si estamos siendo víctimas de un ataque o simplemente hay demasiados usuarios conectados al mismo tiempo, aseguró Cameron Camp, investigador de ESET (ESET, 2011).

3.5 Redes Sociales

La propagación de amenazas informáticas por medio de redes sociales se ha vuelto muy popular en el último tiempo por la alta concentración de usuarios que presentan y la posibilidad de obtener mayores beneficios económicos.

Durante mayo de 2011, el engaño del falso botón "No me gusta" de Facebook originó una campaña de propagación que redirigía a la víctima a un página de suscripción de servicios de SMS pagos.

En primer lugar, el usuario recibe un mensaje de un contacto invitándolo a descargar el supuesto nuevo botón. Al acceder al enlace se da inicio al proceso de instalación, que en uno de sus pasos solicita la inclusión de un código en javascript que permite que el mensaje continúe su propagación hacia los contactos de la víctima. Una vez concluido el procedimiento se redirige a la víctima a una página de suscripción de SMS, servicio del que luego es muy difícil solicitar la baja.

Además Facebook sufrió un ataque multi-stage, confirmando la tendencia a utilizar las redes sociales como plataforma de ataque. En este caso, se trató de una amenaza muy elaborada que por medio de la combinación de diversas técnicas de ataque recopila datos de la víctima, infecta su equipo y así propaga códigos maliciosos.

El ataque comienza con la infección del equipo del usuario utilizando técnicas de Ingeniería Social. Luego la víctima es redirigida a una página falsa donde se le solicitan las credenciales de inicio de sesión de Facebook que serán robadas para continuar con la propagación de malware. A su vez se hace uso de la vulnerabilidad CVE-2010-1885 de Internet Explorer que fuerza la ejecución de un código malicioso y luego ejecuta la descarga de otro código malicioso, tomando el control completo de un sistema afectado pudiendo instalar software, ver, cambiar o eliminar datos o crear cuentas nuevas con todos los derechos de usuarios.

CVE-2010-1885 es una vulnerabilidad de ejecución remota de código en la forma en que el Centro de ayuda y soporte técnico de Microsoft valida las URL especialmente diseñadas. Esta vulnerabilidad podría permitir la ejecución remota de código si un usuario consulta una página web especialmente diseñada mediante un explorador web o hace clic en un vínculo especialmente diseñado de un mensaje de correo electrónico (Microsoft, 2010).

El segundo foco de ataque fueron los usuarios de sistemas operativos Mac OS a partir de la aparición de un nuevo rogue para la plataforma de Apple, distribuido bajo el nombre de MacDefender. El código malicioso, al igual que el resto de los falsos antivirus, se caracteriza por simular infecciones en el sistema y tentar al usuario a la compra de una supuesta licencia de software por la cual será estafado.

Luego del descubrimiento de la amenaza, diversas variantes comenzaron a circular en Internet, como "MacProtector", "Apple Security Center" y "MacSecurity", entre otras. Una de las últimas detectadas, MacGuard, se caracteriza por no necesitar credenciales de administrador para su instalación.

El mismo día en que se dio a conocer la noticia de que Twitter había alcanzado las 200 mi-

llones de cuentas de usuario se detectó la propagación de un gusano que utilizaba el acortador de direcciones URL de Google para su propagación en la popular red social de microblogging (Fig. 3).

Fig. 3 - *Acortador de direcciones URL de Google*

Mediante el envío de mensajes masivos por medio de Twitter, con textos breves y atractivos y un enlace con un acortador de URL, se invita al usuario a hacer clic. Cuando esto ocurre, el usuario es direccionado a diversos sitios web donde se lo alerta sobre una supuesta infección en sus equipos y se ofrece la descarga de la aplicación llamada Security Shield, que no es otra cosa que un rogue.

El rogue es un software que, simulando ser una solución de seguridad, en realidad instala códigos maliciosos en el equipo de la víctima. Si bien los ataques en Twitter para propagar esta amenaza ya han sido bloqueados, es importante que el usuario tenga en cuenta los riesgos de hacer clic en enlaces de dudosa procedencias.

Además se descubrió un nuevo troyano para la plataforma de dispositivos móviles Android que recibió el nombre de Geimini. Entre las principales capacidades de este código malicioso se encuentra la posibilidad de recibir instrucciones desde un C&C (Centro de Comando y Control) haciendo que el dispositivo infectado pase a formar parte de una botnet y envíe información del teléfono a una serie de dominios externos posiblemente maliciosos.

Una vez que el dispositivo ha sido comprometido, el malware envía cada un período aproximado de 5 minutos información tanto del usuario como del equipo. Además Geinimi cuenta con la posibilidad de recibir comandos remotos y de esta manera puede ejecutar acciones tales como la descarga e instalación de aplicaciones, el envío y borrado de mensajes de texto, la realización de llamadas o el acceso a páginas web. Además esta infección puede derivar en la instalación de otros códigos maliciosos o incluso la explotación de vulnerabilidades que pueden llevar al robo de información.

Esta amenaza se ha encontrado en varias aplicaciones que se distribuyen a través de canales no oficiales para la descarga, entre ellas: Monkey Jump 2, Sex Positions, President vs. Aliens, City Defense y Baseball Superstars 2010 (ESET, 2011).

3.6 Ataques en fechas especiales

Durante el mes de diciembre de 2010 la Ingeniería Social enfocada en las fiestas fue una de las principales estrategias utilizadas por los ciberatacantes. Además se han descubierto dos casos de rogue de rápida propagación en la red.

En enero de 2011 fueron registrados nuevos códigos maliciosos que utilizaban la Navidad como temática de engaño para propagarse. También dos casos de falsos antivirus que buscaban robar dinero al usuario lograron una rápida propagación en la red, según informa la compañía de seguridad informática ESET.

En este mes se recibió en el Laboratorio de Análisis e Investigación de ESET Latinoamérica una muestra de un archivo script con el nombre Christmas que tiene como objetivo el robo de licencias de soluciones de seguridad. Para ello crea una serie de carpetas con nombres normalmente utilizados por programas peer-to-peer y posteriormente copia dentro de ellas todos los archivos con nombres referentes a licencias dentro del disco rígido para luego compartirla.

También aprovechando la víspera de Navidad se distribuyó un hoax - correo electrónico enviado masivamente que contiene una información falsa- cuya función era recolectar información de correos electrónicos válidos para luego ser utilizados con fines maliciosos. Para atraer la atención de los usuarios el mismo prometía la posibilidad de regalar cheques de 1000 dólares con motivo de las fiestas.

Para acceder al premio el usuario debe luego seguir un enlace que permite al ciberatacante validar una cuenta activa de Facebook y continuar propagando la amenaza por medio de un mensaje en el muro de la víctima (Fig. 4).

Durante diciembre de 2010 se descubrieron además dos casos de rogue con una amplia tasa de infec-

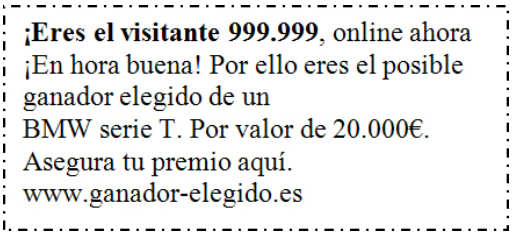

Fig - 4. *Ataque web*

ción en la red, conocidos con el nombre de "Privacy Guard 2010" y "Antivirus 2010". Como la mayoría de estas amenazas son ataques que muestran en la pantalla del usuario advertencias llamativas respecto a la existencia de infecciones en el equipo. La persona es invitada luego a descargar la versión completa de la supuesta solución de seguridad y a pagar por ella, de modo que el fin de estas amenazas es robar dinero al usuario.

La particularidad de estos casos es su creciente profesionalización ya que con el objetivo de obtener mayores beneficios económicos las interfaces gráficas son cada vez más prolijas y se encuentran traducidas a varios idiomas (ESET, 2011).

4. EFECTIVIDAD DE LA INGENIERÍA SOCIAL

Según Kevin Mitnick , uno de los personajes más famosos del mundo por delitos utilizando la Ingeniería Social como arma principal, afirmó que se puede tener la mejor tecnología, firewall, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es un llamado a un empleado desprevenido e ingresar sin más.

El éxito de la Ingeniería Social radica en la combinación de factores, que en realidad son debilidades que el ingeniero social conoce y utiliza.

- ***Factor Humano***

♦ Tendencia natural humana a confiar.
♦ Ignorancia, desconocimiento.
♦ Curiosidad, ambición, motivación.
♦ No poder decir que no.

- ***Factor Tecnológico***

La seguridad en la información está enfocada principalmente en seguridad técnica.

- ***Factor Laboral***

♦ Personal externo que tiene acceso a recursos de la organización.
♦ Interacción virtual con socios del negocio, vendedores y proveedores.
♦ El concepto de seguridad como una pérdida de tiempo o un estorbo para su trabajo.
♦ No seguir los procedimientos políticos de seguridad de la empresa.

5. MEDIDAS DE PROTECCIÓN

La mejor defensa contra esto es muy sencilla: la educación. Educar es explicar a todos los empleados la importancia de la seguridad informática y darles a conocer que existe gente preparada que intentará manipularlos para conseguir acceso a los sistemas. Esto implica invertir en educar e informar al personal y, finalmente tratar de cambiar su comportamiento hacia una "seguridad positiva" (Durbin, 2011).

Simplemente previniendo a la gente sobre posibles ataques futuros en contra de sus propios intereses y que todas las entidades involucradas, tales como gobiernos, organizaciones, proveedores de Internet, cuerpos internacionales y usuarios finales asuman la responsabilidad para luchar contra el malware de Ingeniería Social (Abraham et al., 2010) hará que estén alertas, siendo necesario formar a todo el personal inclusive al de limpieza (Ardita, 2008; Universidad Virtual del Tecnológico de Monterrey, 2003).

Se proponen las siguientes soluciones a los ataques de Ingeniería Social:

♦ No revelar información confidencial ni passwords a ninguna persona, ni siquiera al personal de sistemas.
♦ No bajar, instalar o correr programas de origen dudoso.
♦ Ignorar advertencias recibidas por chat o e-mail.
♦ No asumir que un correo electrónico proviene de la dirección que aparece en él.
♦ Considerar que una llamada recibida de una extensión interna en la empresa no implica que su interlocutor sea un colega.
♦ Reportar a seguridad cualquier llamada o mensaje sospechoso, dependiendo de las políticas de la empresa.
♦ Establecer oficialmente la política de seguridad que normará la protección de la información.
♦ Elaborar un programa institucional para incrementar el nivel de conciencia hacia la seguridad de la información.
♦ Efectuar auditorias para medir el nivel de cumplimiento de la política mediante un muestreo.
♦ Publicar los resultados de las auditorías, junto con las acciones correctivas.
♦ Realizar una campaña motivacional para que el cumplimiento de las prácticas se haga lo más rápidamente posible.
♦ Destruir toda la documentación que se tira a la basura que pudiera contener información confidencial.
♦ No colocar ni escribir claves de acceso en lugares visibles o de fácil acceso.

6. CONCLUSIONES

Reconocemos a la Ingeniería Social como principal fuente de inseguridad informática debido a que ataca al punto más débil del eslabón que es el ser humano, a través de engaños y otras tácticas, en vez de recurrir a la búsqueda de fallas de seguridad en los sistemas informáticos.

Consideramos que es una técnica suficientemente elaborada, lo que justifica su éxito y efectividad.

Es de vital importancia comprender que no hay tecnología capaz de proteger contra la Ingeniería Social, como tampoco hay usuarios ni expertos que estén a salvo de esta forma de ataque.

La Ingeniería Social no pasa de moda, se perfecciona constantemente en el arte de manipular a las personas y solo tiene la imaginación de los ingenieros sociales como límite.

Las principales armas contra la Ingeniería Social son la educación y el entrenamiento de los usuarios en la aplicación de políticas de seguridad. Se debe controlar que las mismas sean acatadas por todos los empleados de la empresa.

AGRADECIMIENTOS

Queremos agradecer especialmente a nuestros revisores por el valioso aporte recibido por parte de ellos en la elaboración de este trabajo de investigación.

Mag. Ing. Laura Vargas. Facultad de Ciencias Exactas, Físicas y Naturales; Universidad Nacional de Córdoba. Universidad Tecnológica Nacional Facultad Regional Córdoba.
E-mail: laura.m.vargas@gmail.com

Ing. Julio Castillo. Jefe del Laboratorio de Investigación de Software Microsoft (LIS). Universidad Tecnológica Nacional Facultad Regional Córdoba.
E-mail: jotacastillo@gmail.com

GLOSARIO

Ataque: Acción en la que alguien rompe las reglas de seguridad y preservación de la intimidad de un sistema informático.

Cracker: Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

E-mail o Casilla de correo: Dirección de correo electrónico que utiliza una persona o empresa que le permite recibir, enviar y almacenar correos.

Hacker: Experto de programación, sistemas, redes en general, Internet, computadoras y no tiene intenciones malas a diferencia de lo que se escucha comúnmente. Le gusta acceder a lugares prohibidos por diversión, alimento de ego y demostrar que hasta los sistemas más costosos son vulnerables.

Información: Elemento fundamental que manejan las computadoras en forma de datos binarios.

Ingeniería Social: Técnicas y métodos utilizados para engañar a las personas y conseguir información valiéndose de su ignorancia e inocencia.

Ingeniero Social: Persona con alta capacidad de convicción y facilidad para engañar a otras personas y lograr que le digan información confidencial que necesita. Éste utilizará como herramientas un teléfono, una charla por chat o en el mejor de los casos lo hará personalmente.

Internet: Conjunto de redes interconectadas que permiten la comunicación entre millones de usuarios de todo el mundo. Para el acceso a ella los usuarios necesitan tener un prestador de servicios que le provea un nombre de usuario y contraseña.

Keylogger: Programa malicioso que registra cada vez que se pulsa una tecla en el teclado y se almacenan en un archivo de texto.

Malware o Malicious Software: Programa diseñado para hacer algún daño a un sistema. Puede presentarse en forma de virus, gusanos, caballos de Troya, etc.

Password o contraseña: En español palabra clave. Código personal y privado que fue asignado previamente a un usuario determinado. Para comenzar cualquier operación esta clave es requerida.

Phishing: Técnica que consiste en utilizar algún medio de información como puede ser el correo electrónico o llamada telefónica para engañar a personas y "robarles" su dinero. Al parecer estos mensajes proceden de un negocio digno de confianza (un banco o compañía de crédito) que solicita "verificación" de los datos por un supuesto problema.

Spam: Mensaje de correo masivo con contenido publicitario no solicitado.

Spyware: Software espía que se encarga de recopilar información de usuarios para luego enviarla al servidor de la empresa que le interesa conocer dicha información. Utilizado para conocer gustos de los usuarios para luego hacerles ofertas a medida.

Troyano: Programa dañino, utilizado normalmente como herramienta para espiar, que suele presentarse disfrazado o incluido dentro de otro programa. Cuando este programa es ejecutado el troyano realiza la acción prevista.

Virus: Programa maligno que infecta un sistema o unidad física de almacenamiento y tiene la capacidad de auto-replicarse. Éste necesita un porta-

dor o archivo donde incluirse para poder replicarse.

Sniffing: Software o hardware que puede capturar y guardar el tráfico de una red.

Fuga de información: Los cibercriminales pueden modificar el tráfico de la red de modo de obtener datos confidenciales, como credenciales bancarias.

Interceptación de accesos por medio de una red gemela: configuración de redes para simular una conexión Wi-Fi segura.

Intentos de ataque 0-day a sistemas operativos y aplicaciones: Ataques a través de exploits previamente desconocidos.

Rogue: Software que simula ser una solución de seguridad, pero en realidad instala códigos maliciosos en el equipo de la víctima.

Hoax: correo electrónico enviado masivamente que contiene una información falsa.

Botnet: red de computadoras zombie las cuales son controladas remotamente desde una computadora generalmente con fines maliciosos. El término zombie se refiere a que normalmente el usuario no tiene conocimiento que su máquina está infectada y está siendo utilizada para fines maliciosos.

REFERENCIAS

Borghello C., "Seguridad Informática sus implicancias e implementación." Tesis UTN. Setiembre, 2011.

Ardita J. C., "Ingeniería Social: El arte de manipular a las personas." CISM, Director de CYBSEC S.A. Security, Setiembre 2008.

Solms R.V., From policies to culture. B.V. Solms. Computers & Security, 23 (2004), pp. 275-279.

Visentini M., "La Ingeniería Social: Oportunidades que le brindan las nuevas amenazas." Alumno de la Facultad Regional Córdoba de la UTN. Este trabajo forma parte del proyecto de Educación que organizó ESET conjuntamente con la Universidad Tecnológica Nacional (UTN) de Argentina, Diciembre 2006.

Universidad Virtual del Tecnológico de Monterrey. Seguridad en Proyectos de Gobierno Electrónico. Módulo 6. DR. México, 2003.

Asier E., Goyanes M., Frutos K., "El movimiento Hacker. Reporte técnico. Universidad Autónoma de Barcelona. Mayo, 2011.

Abraham, Sherly and Chengalur-Smith InduShobha. An overview of Social Engineering Malware: Trends, tactics, and implications. Technology in Society, Volume 32-2010 page 183-196.

Durbin S., "Tackling converged threats: building a security-positive environment, Network Security." Volume 2011, Issue 6, June 2011, Pages 5-8.

Microsoft. Cómo Proteger la información confidencial de las Amenazas de la ingeniería social. Publicado en: www.technet.microsoft.com.es. Agosto, 2006.

ESET. Informes de las amenazas informáticas más destacadas según ESET (compañía de seguridad informática). 2011.

Microsoft. Boletín de Seguridad de Microsoft MS10-42 Crítico. Publicado en: http://www.microsoft.com/latam/technet/seguridad/boletines/2010. Julio, 2010.