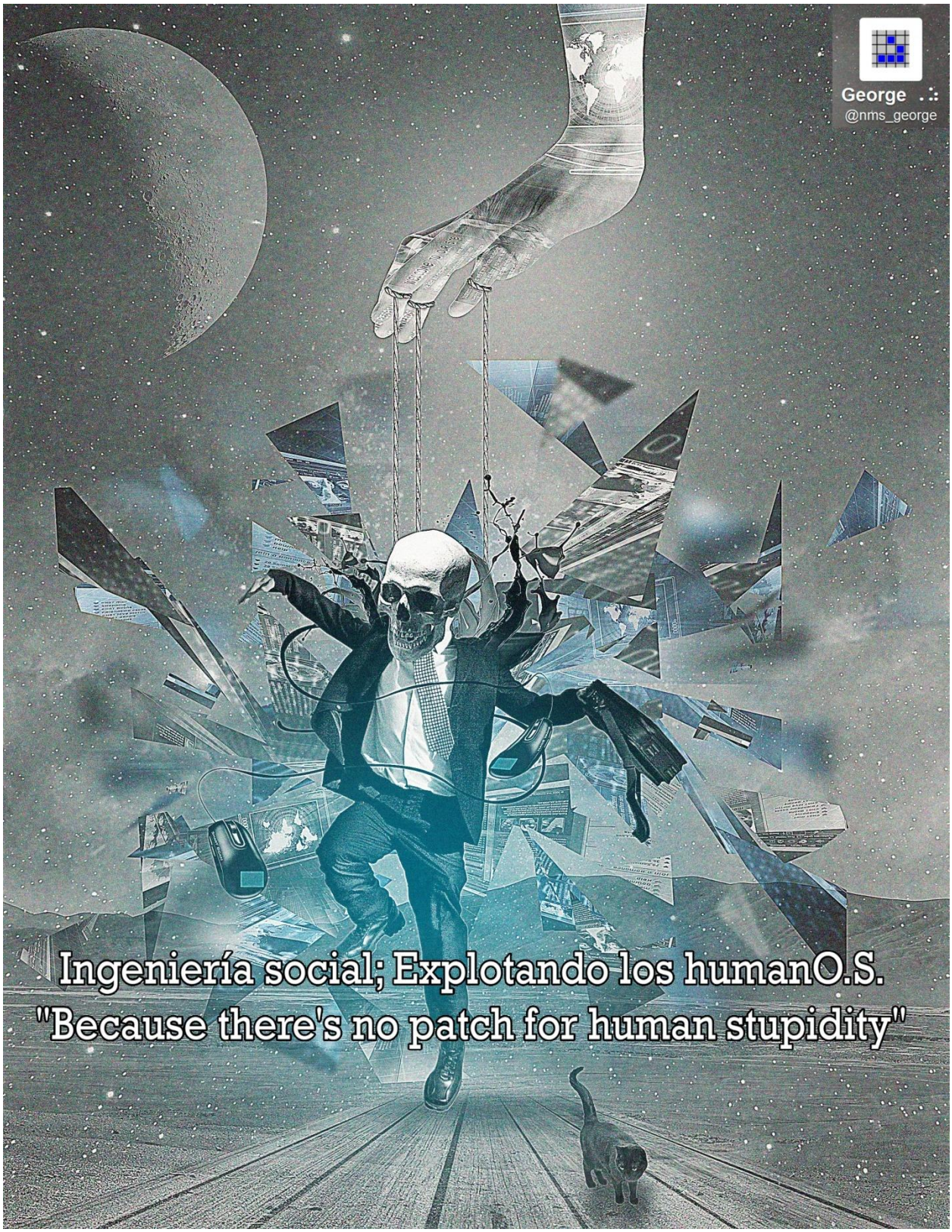

SCAM
BOX


George .:
@nms_george
Ingeniería social; Explotando los humanO.S.
"Because there's no patch for human stupidity"

ÍNDICE

1. Introducción 4

2. Ingeniería Social; Explotando los humanO.S. 5

3. Que es la ingeniería socia 5

4. Cuál es la relación entre ingeniería social y seguridad informática 7

5. Caso de análisis; Experimento práctico 8

- 5.1 Herramientas usadas 8
- 5.2 Procedimiento 8
- 5.3 El Exploit 8
- 5.4 El Flayer 9
- 5.5 El Blog 9
- 5.6 El Formulario 11

6. Análisis y hallazgos 13

- 6.1 Resultados 13

7. Aspectos psicológicos vulnerados 14

8. Conclusiones 15

9. Bibliografía 17

Abstract

The following paper aims to demonstrate how human factors may compromise the security of an entire company. For this purpose, an experiment was conducted at University Foundation Luís Amigó, Medellin, Colombia at Faculty of Engineering. This exercise was to audit people's susceptibility to social engineering attacks, through a physical attack vector. Also the high importance of awareness and education as security strategies oriented to the human factor to combat such attacks was demonstrated.

1. INTRODUCCIÓN

En lo que va corrido del año, América latina ha sido el nuevo objetivo en la mira para los ciberdelincuentes, el crimen cibernético marcó una subida de hasta un 40% en 2012 [1]. Si se hace un análisis más detallado mes a mes se tiene que en febrero mediante el uso de novedosas técnicas de Ingeniería Social, *MSIL/Agent.NKY* mejor conocido como poker agent y el falso video sobre Justin Bieber con Selena Gómez hicieron estragos en las redes sociales [2]. En marzo ESET Latinoamérica detectó un correo electrónico que simulaba provenir de Mercado Libre y en donde se informaba que el destinatario "ha sido suspendido para operar", se trataba de un caso de ingeniería social y phishing. [3] Finalmente el mes pasado, nuevamente el protagonismo fue para los ataques de ingeniería social y phishing, las amenazas más destacadas fueron suplantación a la banca en panamá y el famoso ataque a la agencia de prensa The *Associated Press (AP)* [4] hecho que repercutió incluso en wallstreet.

El éxito de éste tipo de técnicas, es la explotación de vulnerabilidades no en la parte técnica ni tecnológica de la organización sino en el factor humano. Se aprovecha el conocimiento de la parte psicosocial del individuo y de metodologías de manipulación para explotar sentimientos como la confianza, la curiosidad, la inocencia, la desinformación, la atracción física y la sexualidad, la reciprocidad, las ganas de ayudar, la lástima, la aprobación social entre otros muchos.

Teniendo en cuenta el contexto latinoamericano descrito anteriormente, se realizó un trabajo de investigación con fines netamente académicos, se contó con la aprobación de la decanatura en la facultad de ingeniería de sistemas de la Fundación Universitaria Luís Amigó para la realización de un experimento social en sus laboratorios. Dicho ejercicio consistió en básicamente tratar de explotar múltiples vulnerabilidades del sistema operativo más frágil, el de los humanO.S. ; Motivando y generando expectativa alrededor de publicidad falsa ofreciendo servicios gratuitos inexistentes a los usuarios a cambio del registro de sus datos personales, además la alta posibilidad de ganar un iPad 3.

Este reporte tiene por objetivo documentar el experimento realizado además de demostrar la susceptibilidad de los usuarios a ataques de ingeniería social dirigidos. También se describe como se realizó el experimento sin siquiera tener manejo de tecnologías avanzadas o lenguaje de programación de tal modo que cualquier persona puede realizar este tipo de ataque.

2. INGENIERÍA SOCIAL; EXPLOTANDO LOS HUMANOS

"Hecha la ley, hecha la trampa". Conforme avanza la tecnología, se mejoran y reestructuran los sistemas de seguridad avanzando a la par de ésta, pero también los atacantes hacen lo mismo, desarrollan rápidamente formas de evadir los perímetros de seguridad de las empresas apoyados en nuevos vectores de ataque o mejorando los ya existentes por ejemplo el caso de las APT (Advanced persistent threat) que son amenazas persistentes como la ingeniería social. Ésta no es algo nuevo, el fraude como la famosa estafa nigeriana, timo 419 ó timo nigeriano, llamado así porque la mayor parte de estas estafas provienen de ese país, ya había explotado la inocencia y los buzones postales de las víctimas desde antes de la existencia de la internet. Dicho timo, consiste en motivar a la víctima con un premio o dinero inexistente y persuadirla para que realice una consignación de dinero por adelantado "para realizar los trámites pertinentes" como única condición para acceder al supuesto dinero o premio. Las sumas solicitadas son bastante elevadas, pero insignificantes comparadas con la suma de dinero ó el gran premio que las víctimas esperan recibir. Pues bien, este tipo de engaños ahora usan las Tics para lograr su cometido.

3. PERO ENTONCES, ¿QUÉ ES LA INGENIERÍA SOCIAL?

Podría definirse como la explotación de la seguridad de un sistema, orientada al factor humano, no a la parte técnica ni tecnológica de la organización, mediante el uso de técnicas de manipulación y engaños para obtener información sensible. La información sensible no es más que datos personales e "intransferibles" de una persona que la identifica en la red o en la vida real.

Según laboratorios ESET "La Ingeniería Social puede definirse como una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema. Es el arte de conseguir de un tercero aquellos datos de interés para el atacante por medio de habilidades sociales. Estas prácticas están relacionadas con la comunicación entre seres humanos." [5]

No se puede hablar de ingeniería social sin citar al hacker considerado el más peligroso del mundo en su época, el genio Kevin Mitnick especialista en ingeniería social, fue el pionero en entender que las personas son activos de información y pueden ser explotadas

mediante técnicas psicológicas y de manipulación. Según su opinión, la ingeniería social se basa en estos cuatro principios:

1. Todos queremos ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No nos gusta decir No.
4. A todos nos gusta que nos alaben.” [6]

4. ¿CUÁL ES LA RELACIÓN ENTRE LA INGENIERÍA SOCIAL Y LA SEGURIDAD INFORMÁTICA?

La seguridad de la información busca mantener la integridad, confidencialidad y disponibilidad de la información mediante estrategias y tecnologías que protejan los activos de información. Hay que entender que las personas deben ser consideradas como dichos activos puesto que conoce procesos críticos, almacena datos e información sensible.

Cuando se realiza un ataque dirigido a infraestructura con herramientas y técnicas avanzadas de penetración de sistemas y hacking demanda mucho tiempo, dinero y esfuerzo porque implica planear el ataque: Recopilar suficiente información pasiva antes de intentar vulnerar la seguridad de la red sin mencionar que si ésta tiene una topología de red segura serán varios anillos de seguridad los que van a complicar el trabajo; Por otro lado es ejecutar el ataque: Para ello, el intruso debe tener amplia experiencia en software libre y herramientas de penetración para poder romper las múltiples capas de seguridad sin generar alarmas y con el menor ruido posible para evitar dejar evidencias. Además, tendrá que estar familiarizado con la tecnología empleada dentro de la organización a la que se está infiltrando. Como puede verse, se necesita mucho tiempo dinero y esfuerzo para investigar, planear y ejecutar un ataque de este tipo.

Mientras que cuando un ataque es dirigido a los activos de información humanO.S.(Human Operate System) mediante métodos de ingeniería social, el intruso realiza el mismo proceso de investigación planeación y ejecución del ataque pero el consumo de recursos es mínimo ya que al atacar directamente al usuario, el hacker evitará todos los sistemas de control y tecnologías de seguridad haciéndole un bypass al sistema completo como muestra la figura a continuación.

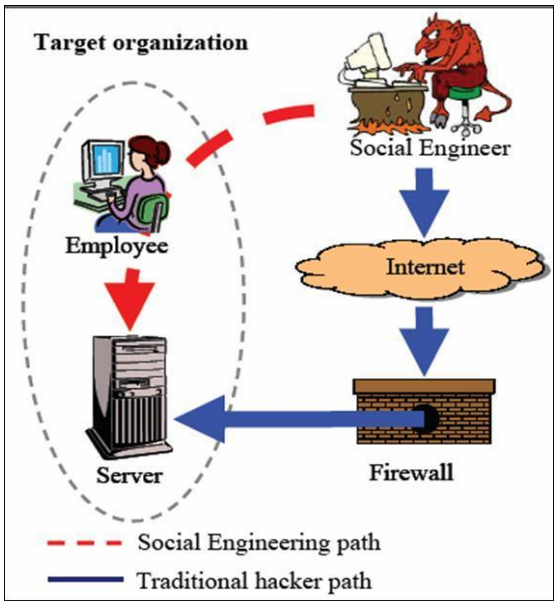


Figura 1: Cortesía flickr

Social Engineering path: Ataque directo al usuario, evadiendo todos sistemas de control y tecnologías de seguridad.
Traditional hacker path: Ataque directo a la infraestructura, romper todos y cada uno de los anillos de seguridad.

Por lo tanto, Las empresas pueden comprar las mejores soluciones, las más costosas del mercado –Software o Hardware- y tener los mejores controles de seguridad para proteger sus activos, pero no será de gran utilidad si los empleados no son conscientes del valor de la información con la que trabajan. “la seguridad de una compañía es tan fuerte como el eslabón más débil de la cadena”. De nada sirve tener el mejor Firewall, IDS, HoneyPOT, Antivirus, HIPS, Endpoint Protection, ni conexiones cifradas, si un usuario inocente, inconsciente ó simplemente desinformado da clic a cualquier link, instala software de sitios de dudosa confianza y da permisos a cuanto proceso le solicita, un eslabón débil en la cadena puede zombificar toda una organización. Las malas prácticas arrojan por la ventana la seguridad de miles de dólares de la empresa. Por esto es muy importante tener en cuenta dentro de las estrategias de seguridad de la empresa la concienciación, capacitación y educación de los usuarios. Hay que enseñarles a identificar el valor de la información con la que trabajan diariamente, la importancia de sus acciones y hábitos para mantener un nivel adecuado de seguridad.

5. CASO DE ANÁLISIS.

Se efectuó un experimento social con fines educativos, éste consistió en vulnerar diferentes aspectos psicológicos a un grupo de estudiantes de ingeniería de sistemas de la Fundación Universitaria Luís Amigó de Medellín (Desde ahora FUNLAM), el objetivo era obtener información sensible de ellos. El ejercicio se realizó usando herramientas libres y sin usar técnicas de programación, de manera tal que cualquiera pudiera hacerlo.

5.1 HERRAMIENTAS USADAS

Para la ejecución del experimento se usaron las siguientes herramientas:

- Blog: elperiodicoen.blogspot.com
- Publicidad: Flayer impreso.
- Formulario de registros, Embebido desde http://jotform.co/
- Exploit social

5.2 PROCEDIMIENTO:

Con la colaboración de mi hermosa esposa, se entregaron 50 volantes en los laboratorios de ingeniería de sistemas de la FUNLAM bajo el siguiente argumento o pretexto:

5.3 EL EXPLOIT:

"Hola, soy Laura Celis, modelo y publicista de la universidad EAFIT (Prestigiosa universidad local) y vine aquí a regalarles suscripciones gratis a nuestro periódico. Haber les cuento de que se trata! Somos un nuevo servicio de prensa tecnológica que está incursionando en el mercado local, nos dedicamos a difundir y compartir información sobre los principales avances y noticias tecnológicas de interés. Vinimos a esta institución porque actualmente estamos realizando una campaña de publicidad en solo dos universidades en ésta (FUNLAM) y en ESUMER (Otra institución universitaria de la región). Estamos regalando 3 meses gratis de suscripciones a nuestra versión escrita, solo necesitan registrarse en la página elperiodicoen.blogspot.com llenarla con tus datos personales y además podrán participar en la rifa de 50 iPads 3. Nol olviden que tienen muchas probabilidades de ganarlo porque la campaña publicitaria solo se está llevando a cabo en las facultades de ingeniería de las dos universidades que les comenté. No olviden que por cuestiones legales no podrán recibir el premio menores de edad ni quienes ingresen documentos o datos inválidos. Los ganadores que no deseen el iPad 3 podrán reclamar el valor comercial del premio a través de su entidad bancaria de preferencia"

5.4 EL FLAYER:

El ejercicio de ingeniería social se decidió orientar hacia el vector de ataque físico para lo cual se diseñó e imprimió (La publicidad falsa impresa da más credibilidad) un volante con características puntuales por ejemplo, la tipografía empleada, muy similar a la de la prensa local, las palabras "gratis" y "un iPad 3" fueron resaltadas de tal manera que pudiera influir a simple vista. En el pie de página, el argumento que hace más dirigido aún el ataque de ingeniería social y motiva enormemente al usuario a registrar sus datos, porque creerá en la alta probabilidad de ganar el premio.

Figura 2: Volante de publicidad falsa.

Se entregaron 50 volantes en los laboratorios de sistemas de la Fundación Universitaria Luís Amigó, se abordaron a los usuarios allí porque tenían a mano las computadoras para hacer el registro inmediatamente recibieran la publicidad falsa.

5.5 EL BLOG:

Con la ayuda de una excelente plantilla corporativa, se publicó un blog fachada, se llenó con copias de varios artículos muy interesantes encontrados en internet y se postearon allí con un buen tiempo de anticipación antes de la ejecución del experimento. El portal quedó así (Ver figuras 3 y 4)

Figura 3: Blog usado como fachada

El blog tiene sus detalles pensados para persuadir al usuario, hacerlo sentir que está en un sitio sólido, serio, de confianza. En varias partes hay posteado un modulo que dice “Suscripción a versión impresa GRATIS” acompañado de un gran botón rojo llamando a la acción (Call to action) de registrarse para obtener el beneficio gratuito.

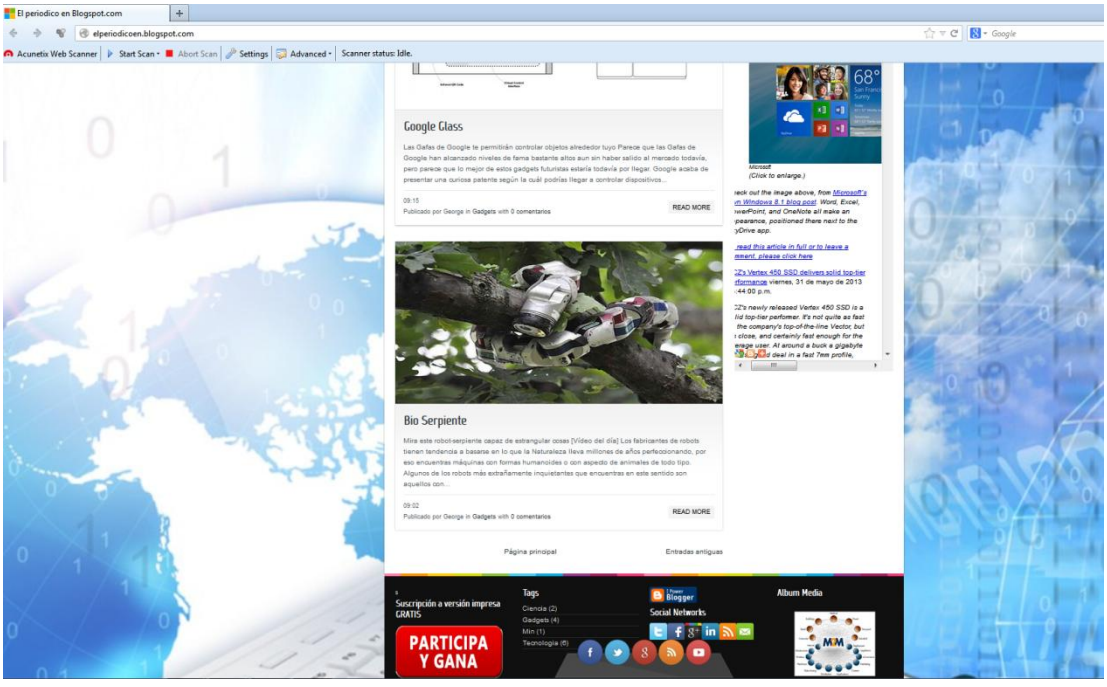


Figura 4:

Cuando el usuario entra a elperiodicoen.blogspot.com una ventana emergente es cargada 10 segundos después del ingreso al sitio, capturando la atención del usuario e invitándolo a registrarse. La ventana luce así: (Figura 5)

5.6 EL FORMULARIO:

Figura 5: Formulario y campos de registro

Este formulario (Figura 5) fue creado a través de un aplicativo llamado jotform.co sin necesidad de emplear lenguajes de programación, fácilmente se pueden crear formularios en línea y embeberlos a gusto. Como se puede observar está compuesto por un banner con publicidad, debajo un pretexto para motivar al usuario; “Concurso válido sólo para estudiantes de ingeniería de la FUNLAM o el ESUMER”; “Participas también en el sorteo de 50 iPads 3”. En la parte inferior un botón, no cualquier botón plano, si no un “push button” de color rojo para ser coherente con las teorías de la psicología del color y persuadir pasivamente lo mejor posible.

El contenido del formulario está dirigido a capturar los siguientes datos sensibles del usuario:

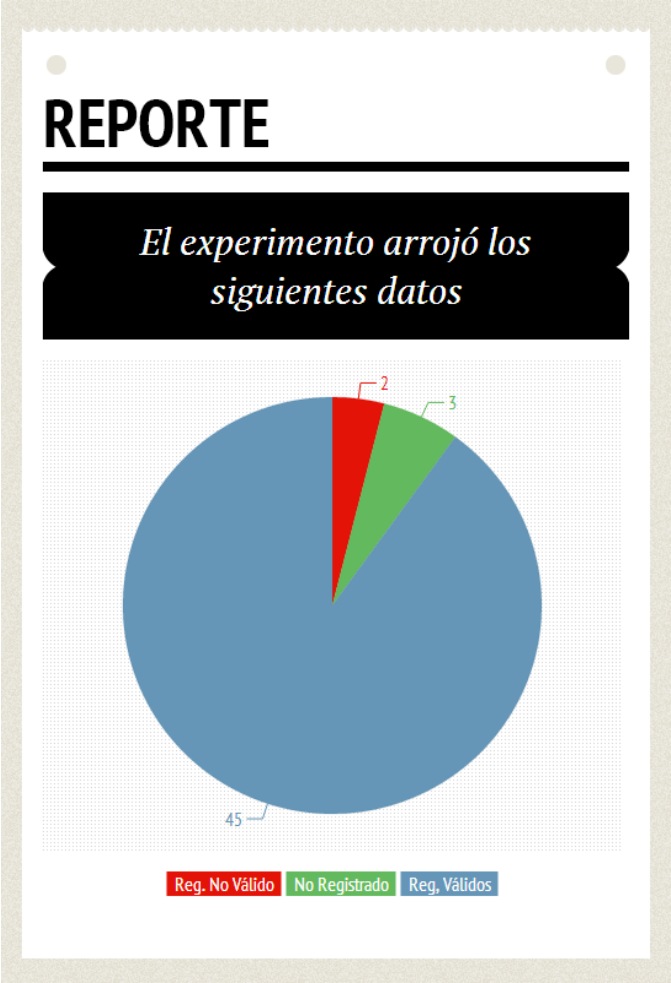
Nombres y apellidos
Cedula de ciudadanía
Correo Electrónico
Teléfono Celular
Fecha de nacimiento
Usuario
Contraseña
Dirección física
Banco de preferencia.

Lo que siguió fue esperar el registro de los usuarios. Acción que fue llevada a cabo el mismo día, la técnica de haber suministrado publicidad en los laboratorios antes de clase resultó ser muy eficiente, ya que entre más personalizado y dirigido sea el ataque, mejores serán los resultados.

6. ANÁLISIS Y HALLAZGOS

6.1 RESULTADOS:

Registros	Total
Registros Válidos	45
Registros no válidos	2
No Registrados	3
Volantes repartidos	50



El experimento tuvo una eficacia del 90%. Se atribuye el poder del ataque a la creatividad del escenario, buena planeación y ejecución del mismo. Los usuarios indudablemente fueron susceptibles a la técnica de ingeniera social con vector de ataque físico. Con los datos capturados se puede hacer robo de identidad y por extensión cualquier tipo de estafa. En este caso los datos no serán liberados ni usados para pos explotación, lo contrario, se realizará una charla de concientización y sensibilización a los estudiantes.

La ingeniería social es un riesgo real de alto impacto. Imaginemos que pasaría si el ejercicio se repitiera en la salida de un banco a medio día cuando el gerente sale almorzar

al restaurante que acostumbra, supongamos que conocemos el hobby del gerente, las motos, que podría pasar si se pone a una niña hermosa a repartir volantes publicitarios con invitación a un súper evento de motociclismo y Freestyle; “gana un pase doble al gran evento registrando únicamente tu correo electrónico y tu cedula” te enviaremos la boleta para ingresar al evento totalmente gratis… Es innegable que la ingeniería social llega hasta donde la creatividad, imaginación y las mañas lo decidan, no hay límites.

7. ASPECTOS PSICOLÓGICOS VULNERADOS

- Confianza: Los seres humanos tienden a confiar por naturaleza en quienes tienen aspecto confiable o cierto aire de autoridad. La confianza es uno de los principales aspectos psicológicos que aprovechan los atacantes. En el experimento, las personas confiaron en el aspecto agradable de quien promovió la campaña publicitaria, supusieron que realmente era modelo porque es hermosa y elegante, también creyeron que era publicista porque nadie pregunto nada sobre el asunto, nadie dudó de sus palabras. Por medio de su aspecto, del buen diseño, calidad de la publicidad y del blog, ella generó esa confianza y credibilidad para persuadir a las personas a participar en el concurso para ganar un iPad 3. Los usuarios también fueron muy confiados al enviar esos datos tan sensibles por conexiones sin cifrar.

- El deseo de obtener algo a cambio de nada: Esta vulnerabilidad es la más explotada por los estafadores, ¡acaso quien no quiere ganar un iPad 3 y tres meses de suscripción a prensa escrita gratis, sea cual sea el producto, si es gratuito hay motivación!

- Atracción física: a las personas les agradan los rasgos físicos lindos, simétricos y al igual que la sexualidad, son armas casi infalibles de manipulación.

- Validación social: También conocido como el error común, es hacer algo “porque todo el mundo lo hace”.

- Ingenuidad: Falta de malicia de experiencia y paranoia, no se puede pretender creer que todas las personas son buenas o que siempre dicen la verdad, desafortunadamente siempre hay que desconfiar y dudar de todo.

- Subestimación: No estar preparado para un ataque te hace vulnerable a él. En temas de seguridad hay que ser siempre proactivos.

8. CONCLUSIONES.

El éxito de los desarrolladores de malware, virus y spammers depende casi en su totalidad de su capacidad de disfrazar el malware y el spam con ingeniería social. Según Microsoft el 45% del malware necesita interacción con el usuario [7]. La idea es subir un poco el nivel de paranoia, ser muy prudentes, no dar clic a cuanto link aleatorio llega, no dar permisos a cuanto proceso lo solicita, leer muy bien y pensar antes de actuar. La mayoria de usuarios no leen, solo ven colores.

Es de vital importancia generar y definir estrategias de seguridad que cubran no solo la parte técnica y procesos críticos de la organización, también las vulnerabilidades del sistema operativo más frágil; El de los HumanO.S.

En cuestión de seguridad hay que ser muy proactivos, el subestimar un ataque te hace vulnerable a este, porque no se está preparado. La protección anticipada ahorra tiempo, dinero y esfuerzo al prevenir pérdida de información de manera proactiva en lugar de los costos generados a partir de las respuestas a un incidente en forma reactiva.

Nunca suministrar información sensible a desconocidos o en lugares públicos ni mucho menos en redes sociales, anuncios, páginas web etc. También hay que tener en cuenta la reputación de los sitios donde se van a entregar los datos personales y de no ser estrictamente necesario, nunca envíe datos sensibles por conexiones no cifradas, podría alguien estar “escuchando” la red y capturar esa información.

Para asegurar el factor humano contra la ingeniería social es muy necesario fomentar mediante la educación, comportamientos, conductas y hábitos seguros tanto en el manejo de la información, como en la navegación a través de Internet. Al final el usuario estará en la capacidad de reconocer y evitar ataques de tipo ingeniería social y phishing. En América latina el 96% de las empresas considera que la importancia de la educación es alta o esencial.[8]

No hay usuarios ni expertos que estén a salvo de un ataque de ingeniería social, esta no pasa de moda y avanza, mejora con el tiempo por eso está catalogada como una APT (Advanced Persistent Threat)

El entrenamiento y la capacitación continua mantienen los niveles de riesgo bajos, y ayuda a minimizar el impacto/costo de nuevos ataques. Anqué la cultura del entrenamiento no es un habito de las empresas Latino Americanas pues tan solo un 10% de las empresas realizan regularmente actividades de concientización al personal [9] lo que no debería ser así, pues cultivar la concientización y el sentido común como única forma de combatir la ingeniería social y el fraude es la estrategia adecuada. Podrán existir programas "Site advisor" y numerosos plugins para combatir el phishing y la ingeniería social los cuales realizan verificaciones, análisis toman decisiones por el usuario al momento de navegar advirtiendo si una página es confiable o no, pero lo correcto es empapar al usuario con información por que el usuario frente a una situación hostil o sospechosa tiene la ventaja sobre el programa, puede improvisar, el programa no.

9. BIBLIOGRAFÍA.

[1] Trend Micro – Latin American and Caribbean Cybersecurity Trends and Government Responses
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf
[2] ESET Latinoamérica – Laboratorio » Blog Archive » Resumen de amenazas de Febrero
http://blogs.eset-la.com/laboratorio/2013/02/28/resumen-amenazas-febrero-2013/
[3] ESET Latinoamérica – Laboratorio » Blog Archive » Resumen de amenazas de marzo
http://blogs.eset-la.com/laboratorio/2013/04/04/resumen-amenazas-marzo-2013/
[4] ESET Latinoamérica – Laboratorio » Blog Archive » Resumen de amenazas de abril
http://blogs.eset-la.com/laboratorio/2013/05/02/resumen-amenazas-abril-2013/
[5] ESET Centro de Amenazas - El arma infalible: la Ingeniería Social
http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf
[6] Wikipedia – Ingeniería social (seguridad informática)
http://es.wikipedia.org/w/index.php?title=Ingeniería_social_(seguridad_informática)
[7] Microsoft Security – Intelligence Report volume 11
http://www.microsoft.com/en-us/download/details.aspx?id=27605
[8] ESET – Prensa – Security Report Latam 2012
http://www.eset-la.com/pdf/prensa/informe/eset-report-security-latinoamerica-2012.pdf
[9] ESET – Prensa – Security Report Latam 2012
http://www.eset-la.com/pdf/prensa/informe/eset-report-security-latinoamerica-2012.pdf