5. Ingeniería Social

1. Introducción a la Ingeniería Social

1.1 Introducción

La seguridad de la información se encuentra estrechamente ligada a la vanidad humana. En el ambiente informático, es muy conocido el dicho “una computadora apagada es un computadora segura”. Ahora bien, si la computadora está apagada, ¿quién es el objetivo? El usuario. No hay un solo sistema en el mundo que no dependa de un ser humano, lo que conlleva una vulnerabilidad independiente de la plataforma tecnológica.

Por eso, la Ingeniería Social continúa siendo el método de propagación de ataques informáticos más utilizado por los creadores de malware, quienes aprovechan las ventajas de cualquier medio de comunicación para engañar a los usuarios y lograr que éstos terminen cayendo en una trampa que suele apuntar a un fin económico.

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.

Entonces, a raíz de variados tipos de engaños, tretas y artimañas se apunta a que el usuario comprometa al sistema y revele información valiosa a través de acciones que van desde un clic hasta atender una llamada telefónica y que pueden derivar en la pérdida de información confidencial –personal o de la empresa para la que el usuario trabaja- o, peor aún, en ponerla en manos de personas maliciosas que buscan un rédito económico.

En palabras de Kevin Mitnick, uno de los personajes más famosos del mundo por delitos utilizando la Ingeniería Social como principal arma: "*usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es una llamada a un empleado desprevenido e ingresar sin más. Tienen todo en sus manos*".

Toda persona padece las mismas debilidades dentro y fuera del sistema informático o de la red de trabajo. En este sentido, las técnicas de engaño conocidas mundialmente y vigentes desde los inicios de la humanidad, sólo deben ser adaptadas al nuevo medio por el cual las personas maliciosas apuntan a concretar sus ataques. La efectividad de tal adaptación es complementaria con el aprovechamiento, para su explotación, de cualidades propias del ser humano como, por ejemplo: credulidad, inocencia, curiosidad, ambición, desconocimiento, confianza, modos de relacionarse con otros, gusto por el morbo, etc.

Si bien parece poco creíble que con sólo preguntar por la información que a uno le interesa se obtenga lo que se desea; esta técnica puede resultar de una efectividad absoluta, si la persona con fines maliciosos se gana la confianza de la víctima a la que intenta engañar.

Así entonces, la Ingeniería Social, se centra en lograr la confianza de las personas para luego engañarlas y manipularlas para el beneficio propio de quien la implementa. La persuasión es una habilidad clave, ya que el secreto no está en preguntar sino en la forma de realizar la pregunta.

Este “arte de engañar” puede ser utilizado por cualquiera, desde un vendedor que se interesa en averiguar las necesidades de sus compradores para ofrecerles un servicio, hasta creadores de malware y atacantes que buscan que un usuario revele su contraseña de acceso a un determinado sistema. Más allá de las coincidencias, o no, en el límite de lo éticamente correcto, todo intento de obtener información confidencial para un uso inapropiado, resulta una actividad altamente cuestionable.

En el mundo de la seguridad de la información, el “arte de engañar” es utilizado para dos fines específicos, principalmente:

1. El usuario es tentado a realizar una acción necesaria para vulnerar o dañar un sistema: esto ocurre cuando el usuario recibe un mensaje que lo lleva a abrir un archivo adjunto, abrir la página web recomendada o visualizar un supuesto video.

Un caso de “éxito” de este tipo de infecciones es el gusano Sober que, mediante un sencillo mensaje, logró ser el de mayor propagación del año 2005. Este malware alcanzó una distribución masiva con asuntos de correos tales como “Re:Your Password” o “Re:Your email was blocked”.

2. El usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos. Este es el caso del Scam y el Phishing, en los que el usuario entrega información al delincuente creyendo que lo hace a una entidad de confianza o con un pretexto de que obtendrá algo a cambio, generalmente un “gran premio”.

Estos casos evidencian otra importante característica de la Ingeniería Social: la excelente relación costo/beneficio obtenida con su aplicación, la convierte en una técnica de lo más seductora: con sólo una llamada telefónica, un correo electrónico o un mensaje de texto vía SMS el atacante puede obtener acceso a información valiosa del usuario, la empresa o incluso acceder a una red de sistemas.

Si bien se podría entrar en particularidades según cada caso, es fundamental 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 y sólo tiene la imaginación como límite.

Así mismo, existe una única y efectiva forma de estar prevenido contra ella: la educación. No se trata aquí de una educación estrictamente técnica sino más bien una concientización social que permita al usuario estar prevenido y alerta para evitar ser un blanco fácil de este tipo de ataques.

Cualquier atacante con algo de experiencia puede engañar con facilidad a un usuario ingenuo. Si éste, en cambio, se encuentra debidamente capacitado e informado podrá descubrir la treta y evitarla. Además, la educación de los usuarios suele ser una importante técnica de disuasión.

1.2 La Ingeniería Social aplicada al malware

La Ingeniería Social es ampliamente utilizada por creadores de malware y delincuentes informáticos debido al alto nivel de eficacia logrado engañando al usuario.

Es en la preparación de un engaño en particular, donde la Ingeniería Social comienza a ser aplicada por parte los creadores de códigos maliciosos y otro tipo de atacantes. Cuanto más real parezca el mensaje, más confiable sea la fuente y más crédulo sea el usuario, mayores posibilidades tendrá el atacante de concretar con éxito sus propósitos y llevar a cabo la reproducción del malware.

1.2.1 Noticias sobre Catástrofes

La lluvia de correos sobre las tormentas en Europa del 2007 confirma la efectividad de la Ingeniería Social: la ingenuidad y la morbosidad humana fueron utilizadas como vehículos para la propagación de una de las principales epidemias de los últimos años. Esas tormentas fueron el inicio de una familia de malware conocida como Nuwar (o Gusano de la Tormenta), que utilizó cientos de asuntos y mensajes distintos durante dos años para formar una gran Botnet con millones de usuarios infectados.

Incidentes de este tipo, junto con acontecimientos de relevancia para una sociedad en particular, o para el mundo en general, son utilizados constantemente por los creadores de malware con varios fines. En el pasado se han encontrado gusanos de correo electrónico que eran enviados como adjuntos de mensajes que pretendían contener fotos o videos de catástrofes naturales (el Tsunami del 2004, Katrina en el 2005), atentados terroristas (Las Torres Gemelas en el 2001, Atocha en Madrid en el 2004, etc.) y guerras (Invasión de Iraq en el 2003, etc.), la ciberguerra entre Rusia y Estonia en 2007 o contra Georgia en 2008, noticias falsas creadas para estos fines en 2009, etc.

Muchas personas sienten curiosidad por las imágenes o videos de situaciones como las anteriores y, por ello, son ampliamente utilizados como recursos para engañar a los usuarios y llevarlos a infectarse con distintos tipos de malware.

Esto no es todo. A lo largo del tiempo, fraudes informáticos de todo tipo se han valido de la buena voluntad de los usuarios para llevar efectivizar estafas de diversa índole. En cada una de las situaciones antes descritas, siempre ha habido ejemplos de engaños por correo electrónico u otro medio, en los que se busca lograr que una persona, con interés en donar dinero para ayudar a los afectados, termine depositándolo en la cuenta del inescrupuloso responsable del fraude.

1.2.2 Famosos

Los programadores de malware también se valen de personajes famosos y políticos para lograr que sus creaciones se propaguen engañando a los usuarios desprevenidos o demasiado curiosos.

A lo largo de la historia del malware, existen casos en los que se menciona a cantantes (Michael Jackson, Britney Spears, etc.), actrices y/o actores (Jennifer López o Angelina Jolie, por ejemplo), deportistas (Anna Kournikova) y personalidades mundialmente reconocidas (Bill Gates, Osama Bin Laden, Saddam Hussein, etc.); entre muchos otros.

Muchos de estos códigos maliciosos no hacen más que lograr repercusión en la prensa, como los recordados casos en que se hacía mención a la fallecida Lady Di o a Britney Spears o el aún mencionado Kamasutra (que en realidad es el gusano VB.NEI, Nyxem o Blackmal; según la casa antivirus) cuya mayor propagación fue a través de las noticias, en lugar de utilizar los equipos informáticos de los usuarios.

Existen otros casos de gusanos de correo electrónico que, apoyándose en mensajes atractivos al usuario y la mención de un famoso, logran una gran reproducción a través de la red (correo, mensajería, P2P, etc). Actualmente, las redes sociales vienen cobrado relevancia al reproducir este tipo de amenazas con supuestas imágenes o videos de personalidades famosas, que en realidad terminan descargando todo tipo de malware.

1.2.3 Marcas y Eventos Conocidos

Una de las prácticas más usuales es el aprovechamiento de la confianza que el usuario tiene en alguna empresa o marca reconocida.

El uso de nombres de compañías u organizaciones no sólo se aplica al malware adjunto a mensajes de correo electrónico, sino también en troyanos, phishing y scam.

Una práctica altamente frecuente para la propagación de gusanos y otros códigos maliciosos, tiene como base el envío de mensajes como si proviniesen de una reconocida empresa de software, con información sobre una supuesta vulnerabilidad y asegurando que el archivo adjunto o el enlace es un parche de seguridad crítico.

En muchos de los casos de utilización de marcas, los creadores de códigos maliciosos incluyen una leyenda al pie del correo electrónico informando que el mismo ha sido analizado por algún antivirus reconocido y que está libre de malware con el objetivo de darle una mayor credibilidad al mensaje.

También suelen registrarse casos en los que hay un aprovechamiento de eventos como el mundial de fútbol, los juegos olímpicos o el Super Bowl estadounidense, por mencionar algunos.

Muchos de estos mensajes, cuando son enviados masivamente a través del correo electrónico, suelen estar armados en formato HTML o texto enriquecido, incluyendo logos y el formato típico de la empresa u entidad organizadora del evento.

En el caso del Scam y el phishing, la metodología es similar, diferenciándose en que no se suelen incluir archivos adjuntos. Además, los mensajes creados para favorecer el phishing suelen utilizar nombres de compañías relacionadas con el ambiente financiero (bancos, tarjetas de crédito, etc.), sitios de Internet reconocidos (como Google, Yahoo!, PayPal, eBay, etc.), compañías de telefonía y muchas otras.

Dado que la mayoría de las empresas y organizaciones tienen políticas de uso en las que explican que no enviarán mensajes de correo electrónico con archivos adjuntos, los usuarios nunca deben hacer caso a este tipo de mensajes.