Internet y nuevas tecnologías

ROBERTO PLÁ
Coronel de Aviación
http://robertopla.net/

HACKING

INGENIERIA SOCIAL

Creo que no es injusto decir que en cualquier sistema, el elemento más vulnerable es el factor humano. Puede que esta norma solo se cumple en sistemas que superen un determinado grado de complejidad, pero en cualquier caso, en materia de seguridad, para cualquier atacante es un buen flanco de ataque y hay que considerarlo. La violencia, el error fortuito o sistemático o el engaño son los principales factores de debilidad en los elementos humanos de los sistemas que pueden provocar brechas en la seguridad o correcto funcionamiento de los mismos.

En cuanto a las Tecnologías de la información se refiere, podemos poner como ejemplo de la violencia la posibilidad de que un componente humano de un sistema se vea sometido a cualquier tipo de extorsión para desvelar sus claves de acceso a un sistema o actuar de forma desleal. El error fortuito o sistemático puede ser provocado al actuar de forma errónea, dejando 'abierto' un sistema que debería estar 'cerrado' o incurriendo en prácticas viciadas, como el uso de canales de comunicación inseguros, elección de claves débiles, uso de software inapropiado o soportes infectados...Pero en esta ocasión quisiera centrarme en el engaño, una táctica militar probablemente tan antigua como la propia guerra y que forma parte de ejemplos clásicos que se estudian desde el primer curso en cualquier academia militar desde hace cientos de años.

En en lenguaje de los hackers, el uso de la mentira mediante las relaciones sociales, es decir, engañar a alguien para que nos revele información se llama "ingeniería social" y es una técnica y un término usado desde los mismos inicios del hacking, aunque reconozco que no he podido encontrarlo ni en el Jargon-1 (el diccionario original de la jerga de los hackers) ni en posteriores recopilaciones de este documento histórico. Para los puristas, no es ingeniería social aquello que no implica iteración humana. Los caballos de Troya y otras intrusiones que pueden inducir a error no son ingeniería social, aunque las fronteras entre la falsedad, la mentira y el engaño son difusas.

En su Historia del hacking español publicada en la red como "Hack Story", Mercé Molist asocia la aparición de esta técnica en España a los primeros grupos importantes de hackers y proporciona una interesante referencia al trabajo de "LeSteR ThE TeAcHeR", "Ingeniería Social 1.0" donde se menciona a uno de los primeros y misterioso hacker español que utilizaba esta técnica: "Agnus Young".

La acción de ingeniería social típica consiste en llamar a alguien para haciéndose pasar por el servicio técnico o alguien del departamento de informática de la compañía pedirle información sobre su ordenador, alegando que es necesario para repararlo, actualizarlo o hacer "una comprobación", estas posibilidades incluyen el uso de la autoridad que proporciona la jerarquía y también puede darse a la inversa: hacerse pasar por un usuario que ha perdido sus claves, aunque hoy en día los técnicos y responsables de redes se han convertido en blancos mucho menos vulnerables debido a su mayor formación en seguridad y su conocimiento de estas técnicas.

Un famoso hacker, convertido tras su paso por la cárcel en consultor de seguridad, Kevin Mitnick ha expresado que la efectividad de la ingeniería social se basa en 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.

¿Como podemos evitar ser blanco de estas técnicas?. En un interesante documento publicado en OUCH!, Alissa Torres expone una serie de medidas para evitar ser víctima de los maliciosos seductores. Yo me he permitido inspirarme en sus recomendaciones y propugnar estas tres reglas:

1) Seguir las normas de seguridad. Especialmente en cuanto a la discreción y el uso de canales seguros. Y sobre todo no compartiendo nuestras claves de acceso, que por algo son "secretas".

2) Ser discreto. No divulgar detalles de nuestro trabajo ni en redes sociales ni entre amigos, ni siquiera en familia. El que no sabe algo, no puede revelarlo. Pequeños detalles, aparentemente insignificantes, pueden ayudar a un asaltante.

3) Verifica la información. Si alguien de la organización te llama, di que colgarás y le llamarás para verificar la llamada. Para autorizar cualquier acceso físico a tu ordenador, comprueba antes con el servicio técnico o el administrador del sistema que la acción está autorizada. Los administradores tienen sus cuentas de acceso, no necesitan la tuya. Si tu clave se ve expuesta, incluso ante compañeros de trabajo, ¡cámbiala! .

Puede que a muchos les parezca que estas medidas son propias de paranoicos, pero lo cierto es que un poco de paranoia da muchísima más seguridad que una pizca de confianza y sobre todo, muchísimos menos problemas.

http://delicious.com/rpla/raa856a

HARDWARE

VIGILAR AL VIGILANTE

Con frecuencia he mencionado el peligro que suponen las pequeñas porciones de software oculto y no revisable, opaco como una caja negra que controla aspectos, muchas veces vitales, de los sistemas que tratamos de proteger.

Según el experto en seguridad Damien Zammit, existe la posibilidad de que los ordenadores basados en los procesadores más modernos de la familia x86 de Intel tengan una importante vulnerabilidad, a través de un procesador, el Intel ME, que tiene como finalidad gestionar el procesador principal, actuando al mismo tiempo como una especie de policía y de servicio técnico, sin que el procesador principal tenga ninguna posibilidad de interferir en sus acciones.

Actualizar el hardware o el software de forma remota por parte del fabricante es una posibilidad establecida hace mucho tiempo por la industria informática porque reduce muchísimo los costes de mantenimiento, permite corregir fallos de forma discreta y rápida. Sin embargo, todo sistema de control y actualización supone un importante peligro porque para poder gestionar el procesador principal, debe poder controlarlo, de forma que si alguien a su vez pudiera controlar esos circuitos que controlan al procesador principal, tendrían el ordenador a su merced.

En el caso de Intel, el 'chipset' o conjunto de procesadores auxiliares incluyen un procesador independiente, el Intel Management Engine (ME) que forma parte un subsistema conocido como Active Management Technology.

Este procesador puede hacer prácticamente cualquier cosa en el ordenador sin que el procesador principal pueda impedirlo, controlarlo o ni siquiera saberlo y es independiente del sistema operativo que utilice el ordenador.

Naturalmente este procesador auxiliar está a su vez protegido, principalmente por una fuerte encriptación de su software, pero es bien sabido que no hay protección inviolable y de la misma forma que esta tecnología puede permitir a intel actualizar todos sus procesadores para protegerlos, podría proporcionar, en malas manos, el arma definitiva para inutilizarlos.

Algunos expertos apuntan que si el software de estos procesadores fuera público podrían detectarse modificaciones maliciosas o fallos de seguridad. En definitiva reclaman un modelo opensource para una herramienta tan poderosa, a fin de que la vigilancia de la comunidad la haga más segura.

http://delicious.com/rpla/raa856b

SEGURIDAD

PRUEBA DE CONCEPTO

Los ensayos atómicos son detectados por otras potencias debido al movimiento sísmico que una explosión de esa magnitud produce. Los nuevos prototipos de aviones son avistados en vuelo, fotografiados en los momento de aterrizaje o despegue o a través de los sensores de satélites de reconocimiento. El radar da información sobre las pruebas de misiles cuya trayectoria, junto a los datos de otros sensores puede ser analizada, y pone de manifiesto las características del proyectil.

Pero ¿como se pueden detectar las nuevas armas de la ciberguerra antes de convertirnos en sus víctimas? En un campo donde la discreción, el secreto, la sorpresa y el engaño son la norma habitual, saber algo del ponente es un tarea tan compleja como necesaria.

En el campo de la seguridad informática, desarrollar un software solo para demostrar que es posible explotar una vulnerabilidad de un sistema, introducirse en él o perturbar su funcionamiento, se llama realizar una "prueba de concepto".

Las pruebas de concepto son desarrollos frecuentes de hackers y expertos en seguridad y se presentan en congresos o publicaciones para promover el desarrollo de la seguridad de los sistemas vulnerables.

Sin embargo, los desarrolladores de malware, bien sea con intenciones criminales o con destino al arsenal de ciberguerra de algún gobierno, también desarrollan pruebas de concepto y tienen que experimentar en ataques reales para comprobar si funcionan.

Algunas de estos ataques son detectados y es muy importante que las actividades sospechosas o malware desconocido se publique con sus características, para poder contar con un catálogo de amenazas e ir pensando en la posible neutralización de un ataque basado en ese malware detectado.

Recientemente se ha detectado un malware conocido como “Irongate”, que comparte características con el célebre Stuxnet y del que se sospecha que es una prueba de concepto de alguien que está desarrollando armas para atacar infraestructuras críticas. Como Stuxnet, este malware tiene por objetivos los pequeños autómatas que gobiernan procesos industriales, suplantando su comunicación con el ordenador que los controla y cambiando sus órdenes por otras que pueden conducir a la destrucción del sistema controlado, deteniendo una industria, o interrumpiendo servicios básicos como el suministro eléctrico, la gestión de recursos hidráulicos, el tráfico,..

Los equipos de vigilancia de la red y de investigación de seguridad observan atentos cualquier comportamiento anómalo para analizarlo en busca de un intruso que pueda dar pistas sobre amenazas desconocidas.

http://delicious.com/rpla/raa856c

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto