www.eysglobal.com

TEMA:
ATAQUES INFORMATICOS FRECUENTES
PARTE 2

3. PHISHING

El phishing es un método usado por los atacantes para suplantar la identidad de un usuario o de una empresa mediante una comunicación electrónica (correo, mensajería instantánea, etc.), con la finalidad de obtener datos personales y bancarios.

Si bien el phishing no es un ataque directo contra una web o sus servidores, este método busca desviar el flujo de clientes, ingresos o búsquedas hacia un portal falso. Aunque focaliza sus ataques a tiendas o portales de venta online, el phishing es también frecuente en sitios que ofrecen servicios financieros o en aquellas webs que mantienen un flujo de crédito constante. Una forma persistente de forzar la confusión del usuario es que se anuncia la aparición del sitio falso en la red e, incluso, se paga por aparecer primero en los buscadores.

Cómo actúa el Phishing

La mayoría de los ataques de phishing comienzan con la recepción de un correo electrónico o un mensaje directo en el que el remitente se hace pasar por un banco, una empresa u otra organización real con el fin de engañar al destinatario. Este correo electrónico incluye enlaces a un sitio web preparado por los criminales -que imita al de la empresa legítima- y en el que se invita a la víctima a introducir sus datos personales.

Cómo protegerse contra el Phishing

- Después de leer el correo no hagas clic en ningún enlace. Realiza las verificaciones pertinentes en tu espacio personal de cliente, acudiendo directamente desde la Url del navegador.
- Mejora la seguridad de su ordenador. El sentido común y el buen juicio son tan vitales como mantener tu equipo protegido, pero además, siempre debes tener las actualizaciones más recientes de tu sistema operativo y navegador web.
- Además, lo ideal es que cuentes con una capa adicional con un antivirus profesional.

Cómo protegerse contra el Phishing

- Introduce tus datos confidenciales sólo en sitios web seguros. Para que un sitio se pueda considerar como ‘seguro’, el primer paso -aunque no el único- es que empiece por "https://", lo que implica que sigue el protocolo de transferencia de hipertexto, y que el navegador muestre el icono de un candado cerrado.
- Revisa periódicamente tus cuentas. Nunca está de más revisar facturas y cuentas bancarias cada cierto tiempo para estar al tanto de cualquier irregularidad en las transacciones.
- Ante cualquier duda, no te arriesgues. El mejor consejo ante el phishing es siempre fomentar la prudencia entre todas las personas que forman parte de la organización. Asegurar la autenticidad del contenido ante la más mínima sospecha es la mejor política.

4. Baiting

Consiste en un ataque dirigido a infectar equipos y redes a partir de dispositivos de almacenamiento extraíbles como pen-drives, tarjetas SD o discos duros externos. A través de estos equipos, los atacantes introducen archivos infectados con malwares. Al ser un software malicioso que ingresa de forma externa al ordenador, la estrategia de ataque suele ser colocar estos dispositivos de almacenamiento externo en las inmediaciones de la empresa, a fin de que sean utilizados y conectados a los equipos corporativos por el personal.

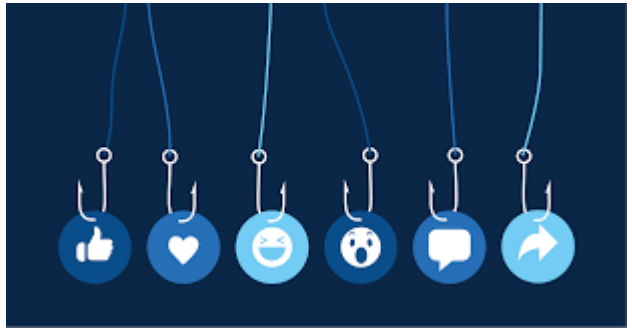
Lógicamente, la mejor forma de evitar un ataque de este tipo será concientizar a sus colaboradores sobre la importancia de no conectar dispositivos de almacenamiento desconocidos y de solo utilizar aquellos inventariados por la empresa.

Métodos físicos en ataques Baiting

Pero no solo hablamos de páginas webs, de enlaces que vemos al navegar. No solo son ataques virtuales o a través de los dispositivos. También utilizan equipos físicos, como por ejemplo una memoria USB.

Es algo que está extendido en algunos países. Los piratas informáticos sueltan pendrives en lugares como bibliotecas, universidades, parques… Y simplemente esperan que la víctima lo conecte a un ordenador para que se ejecute el malware. Son memorias USB infectadas, preparadas para recopilar todo tipo de datos una vez se conecte a un equipo.

¿CÓMO SE HACE EL BAITING?



Pongamos por ejemplo un escenario industrial: con el objetivo último de infiltrar la red de una empresa, el ingeniero social puede distribuir memorias flash infectadas con malware o dispositivos similares a sus empleados, con la esperanza de que este hardware se inserte en ordenadores conectados a redes como medio para diseminar el código malintencionado. Las memorias flash infectadas pueden ser presentadas a los empleados como regalos promocionales, o como recompensa por participar en una encuesta.

¿Cómo proteger su sistema contra el Baiting?

La mejor defensa contra el baiting y cualquier otro esquema de ingeniería social es formar a su equipo y a usted mismo. Cada uno de nosotros debe procurarse una robusta cultura de seguridad en nuestros alrededores: el hogar, la oficina, etc., donde cada individuo debe considerar la «seguridad de la empresa» como parte integral de sus responsabilidades individuales. Específicamente en el caso del baiting, cada individuo debe discutir el tema abiertamente con sus familiares, colegas y amigos, y hacerlos conscientes acerca de los peligros que puede entrañar la falta de precaución.