Resumen ejecutivo

Ataques al sistema operativo humano

Raj Samani, Director de tecnología (CTO) para EMEA

Charles McFarland, Ingeniero jefe de investigación de MTIS

intel Security

Muchos ciberataques incorporan un elemento de ingeniería social cuyo fin es persuadir a la víctima para que realice una acción que infecte su sistema o revele información de utilidad.

Aunque la respuesta a un ataque es una cuestión fundamentalmente técnica, el lado humano acaba cargando la culpa sobre la víctima y genera una necesidad de concienciación en ciberseguridad. Sin embargo, la realidad es que la mayoría de las organizaciones hacen poco por averiguar las razones que llevaron a la víctima a caer en la trampa y, lo que es más preocupante, qué medidas deben adoptar más allá de una política de concienciación para reducir el riesgo de futuros ataques.

El término ingeniería social puede definirse como:

> *El uso deliberado de técnicas engañosas diseñadas para manipular a alguien con el fin de que divulgue información o realice acciones que podrían resultar en la revelación de dicha información.*

Durante un ataque de ingeniería social, la víctima no es consciente del daño que pueden causar sus actos. El "ingeniero social" aprovecha la inocencia de la víctima, no sus instintos delictivos. Los ataques pueden dividirse en dos categorías:

- *Hunting* o "caza", cuyo objetivo es extraer información con una interacción mínima con la víctima. Normalmente, en esta estrategia el agresor necesita un solo encuentro y, una vez conseguida la información, pone fin a la comunicación.
- *Farming* o "recolección", cuyo objetivo es establecer una relación con la víctima y "extraer" la información durante un periodo más largo.

En general, los ataques de ingeniería social que recurren al correo electrónico como canal de comunicación utilizan la caza como forma principal de ataque. Hay excepciones, como las "estafas nigerianas 419", que intentan alargar el ataque durante un período prolongado para intentar extraer la mayor cantidad de fondos posible. Tanto los ataques de caza como los de recolección suelen constar de cuatro fases:

1. Investigación: esta fase es opcional y su fin es reunir información sobre la víctima. El agresor busca información que le ayude a configurar un anzuelo eficaz, como las aficiones, el lugar de trabajo o el proveedor de servicios financieros de la persona elegida.
2. Anzuelo: el anzuelo está pensado para crear una "representación" convincente, un pretexto de interacción en el que involucrar a la víctima. El psicólogo Robert Cialdini cita seis importantes resortes que ayudan a servirse del subconsciente de la víctima:
   - Reciprocidad: a la víctima se le ofrece algo por lo que más tarde se sentirá obligada a devolver el favor.
   - Escasez: la gente tiende a querer comprar algo cuando cree que escasea.
   - Coherencia: cuando la víctima promete hacer algo, cumple su promesa, porque no desea parecer una persona indigna de confianza.
   - Afinidad: la víctima es más propensa a acceder cuando el ingeniero social es alguien con quien coincide.
   - Autoridad: aprovecha la inclinación humana a obedecer cuando la petición proviene de una figura de autoridad.
   - Validación social: es la tendencia a acceder a una petición cuando los demás también lo hacen.

3. Representación: puesta en marcha de la parte principal del ataque. Puede tratarse de la revelación de información, la transferencia de fondos, hacer clic en un enlace, etc.
4. Retirada: la interacción finaliza. Aunque para muchos ataques de recolección puede ser ventajoso retirarse sin despertar sospechas, quizá no sea preciso. Por ejemplo, si un agresor manipula a la víctima para que le facilite los datos de su tarjeta de crédito, normalmente no quiere despertar sospechas para evitar que la víctima notifique la pérdida o robo de su tarjeta y la cancele. Sin embargo, si el agresor consigue robar el código fuente u otra información personal, aun cuando la víctima sospeche algo no podrá recuperar los datos robados.

Los ataques de ingeniería social no son necesariamente lineales; un solo ataque puede formar parte de una campaña mucho mayor para reunir datos distintos relacionados entre sí. Por ejemplo, los agresores pueden realizar un ataque, hacerse con la información y desaparecer, o bien pueden lanzar varios ataques de caza y, con la información reunida, iniciar un ataque de recolección.

Canales de ataque

Los ingenieros sociales pueden utilizar varias vías de ataque.

- Sitios web: los ataques de ingeniería social a menudo utilizan sitios web maliciosos como canal de ataque. Según el *2014 Verizon Data Breach Investigations Report* (Informe sobre las investigaciones de fugas de datos de 2014 de Verizon), "el 20 % de los ataques de espionaje comprometen sitios web estratégicos para distribuir malware".
- Correo electrónico: las formas más habituales de ingeniería social a través del correo electrónico son el phishing y el phishing selectivo. El correo electrónico es un método eficaz para los ciberdelincuentes porque, según el informe de Verizon, "el 18 % de los usuarios visitan los enlaces incluidos en los mensajes de phishing".
- Teléfono: es un canal particularmente apreciado por los revendedores de información.
- Cara a cara: el agresor aborda físicamente a un empleado y, a continuación, lo engaña o presiona para que le proporcione información.
- Servicio postal: aunque este canal parece menos utilizado que los demás, todavía se dan casos de ataque de ingeniería social por esta vía.
- Fax: entre los ejemplos figuran mensajes de correo electrónico de supuestos servicios de pago online.

Medidas contra la ingeniería social

Para reducir el riesgo de sufrir un ataque de ingeniería social, pueden utilizarse las siguientes medidas de control, que se dividen en tres categorías: personas, procesos y tecnología. Conviene resaltar que no son exhaustivas y quizá no sean aplicables a todas las organizaciones.

Personas

- Establecimiento de límites claros: todos los empleados deben conocer perfectamente las normas relativas a la revelación de información y disponer de canales de notificación bien definidos si reciben una petición que excede sus límites.
- Formación continua: ponga en práctica un programa de concienciación en ciberseguridad para que sus empleados sepan en todo momento cómo actuar. Utilice herramientas como el cuestionario de McAfee sobre phishing para dar a conocer las tácticas específicas que suelen emplearse en los ataques.
- Estimulación de las verificaciones: anime a sus empleados a cuestionarse hasta las peticiones aparentemente más inofensivas. Por ejemplo, interpelar a personas desconocidas que intentan acceder de manera aparentemente normal a las instalaciones de la empresa.

- Sensibilización sobre la importancia de la información: incluso la información a priori más insignificante, como un número de teléfono, puede utilizarse para preparar un ataque (información facilitadora).
- Entorno indulgente: las personas objeto de ataques de ingeniería social son, pura y llanamente, víctimas. Si castiga a los empleados engañados solo conseguirá que los demás estén menos dispuestos a admitir si han revelado información. Es posible que, una vez engañados, sigan bajo el control del agresor y sean objeto de extorsión.

Procesos

- Informes de llamadas falsas: cuando se produce una actividad sospechosa, los empleados deben redactar un informe que describa la interacción. Estos informes son útiles para la investigación.
- Páginas de bloqueo informativas: cuando los empleados llegan a una página web maliciosa, utilice una página de bloqueo para informarles de por las que el acceso a dicha página no está autorizado. De este modo reflexionarán sobre lo que han hecho inmediatamente antes y quizá puedan identificar el origen del ataque.
- Notificación a los clientes: cuando una organización deniega información a un solicitante, debe notificárselo y verificar si estaba autorizado a solicitarla. Las organizaciones también deben reflexionar sobre cómo se comunican con los clientes. Por ejemplo, PayPal incluye directrices para que los usuarios identifiquen si los mensajes de correo electrónico que reciben son genuinos. "PayPal nunca le solicitará por correo electrónico el número de su cuenta bancaria ni de su tarjeta de crédito o débito, etc. Tampoco le pedirá en un mensaje de correo electrónico su nombre completo, la contraseña de su cuenta ni la respuesta a sus preguntas de seguridad para PayPal".
- Vía de notificación: debe establecerse una vía de notificación clara para que los empleados en primera línea puedan exponer a sus superiores cualquier sospecha de interacción con mensajes potencialmente fraudulentos.
- Comprobación experta: compruebe periódicamente la susceptibilidad de sus empleados de ser víctimas de los ataques de ingeniería social en los distintos canales de comunicación. Así dispondrá de una herramienta para medir la eficacia de los programas de formación.

Tecnología

- Grabación de llamadas: grabe sistemáticamente las llamadas telefónicas entrantes para facilitar la investigación.
- Líneas falsas: desvíe las llamadas sospechosas a un número supervisado.
- Filtrado de correo electrónico: elimine los mensajes fraudulentos que contengan malware tanto conocido como desconocido.
- Filtrado web: bloquee el acceso a sitios web maliciosos y detecte el malware activo con acceso a Internet.
- Autenticación fuerte: aunque aplicar una autenticación multifactor no elimina el riesgo de que los usuarios sean víctimas de un ataque de ingeniería social y revelen sus credenciales, complicará notablemente la tarea de los posibles ciberdelincuentes.

Siga a McAfee Labs

Resumen

La ingeniería social es una amenaza tangible, aprovechada por los ciberdelincuentes para obtener información de forma ilegal y darle distintos usos maliciosos. Para luchar eficazmente contra este problema, es imprescindible entender la naturaleza de este tipo de ataques. Esto implica la identificación de los autores probables, sus métodos y sus recursos... y la aplicación de las correspondientes medidas de control para reducir el riesgo de éxito de un ataque.

Encontrará una copia del informe completo en **www.mcafee.com/hacking-human-os**.

Twitter@Raj_Samani

Twitter@CGMcFarland

1. **http://www.verizonenterprise.com/DBIR/2014/**
2. **https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ**

McAfee. Part of Intel Security.
Avenida de Bruselas n.°22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com