beazley

Conocimiento de la industria

La amenaza del Phishing: ¿qué deben saber las empresas?

Los ataques de phishing han sido durante mucho tiempo un desafío de ciberseguridad para las organizaciones de todo tamaño. A día de hoy son responsables de más del 80% de los incidentes de seguridad reportados. Según el informe 2021 Cybersecurity Threat Trends de CISCO, alrededor del 90% de las violaciones de datos se producen debido al phishing. El spear phishing (práctica de enviar correos electrónicos que parecen provenir de un remitente de confianza con el fin de obtener información confidencial) es el tipo más común de ataque de phishing, que comprende el 65% de todos los ataques de phishing.

Quizá una de las razones de la proliferación de estos ataques sea que las campañas de phishing son relativamente fáciles y baratas de llevar a cabo gracias a la automatización (por ejemplo, utilizando la plataforma de phishing as a service "Caffeine"). Hoy en día, el spear phishing puede requerir esfuerzos manuales, pero se está volviendo más fácil con la abundancia de datos personales accesibles desde la web. En un futuro veremos campañas de spear phishing automatizadas y personalizadas impulsadas por la Inteligencia Artificial (IA).

El impacto de un ataque de phishing exitoso puede variar desde la obtención de información privada hasta el despliegue de malware y la obtención de acceso remoto. Como ninguno de estos resultados son intrusiones bienvenidas, las organizaciones hacen bien en aprender a protegerse de un ataque de phishing. Enumeramos a continuación una serie de técnicas que deben tenerse en cuenta:

Reduzca el número de correos electrónicos de phishing a los que está expuesto

Las organizaciones deben asegurar la configuración de su solución de correo electrónico (SPF, DKIM, DMARC y SID) para bloquear los correos electrónicos recibidos de fuentes desconocidas o sospechosas. Además, es aconsejable implantar una solución de protección contra

amenazas de correo electrónico con funciones que incluyan filtrado de spam, escaneado de enlaces, sandboxing de adjuntos y bloqueo de los tipos de adjuntos maliciosos más comunes (HTA, docm, xlsm, exe, PS1, VBS, js, etc.).

Aprenda a reconocer mejor los correos electrónicos de phishing

Enseñe y entrene a sus empleados a detectar dominios falsos en sitios web y direcciones de correo electrónico a través de la concienciación sobre seguridad y la formación anti phishing (por ejemplo, los servicios ofrecidos por KnowBe4 y CybeReady). La suplantación de dominios es una forma de phishing en la que un actor de amenazas crea un sitio web o un dominio de correo electrónico falsos para hacerse pasar por una empresa o persona de confianza. Normalmente, el dominio parece legítimo a primera vista, y las diferencias pueden ser muy sutiles y difíciles de detectar (una W que en realidad son dos V, una R y una N minúsculas imitando una M, o una L minúscula que en realidad es una I mayúscula).

Un ejemplo de nombre de dominio falsificado es O365.rnicrosoft.fr. Fíjese en la "rn" en lugar de la "m". Otro nombre de dominio con potencial para engañar a los empleados es https://beazley.changepassword.com. Se trata de un subdominio que pertenece a changepassword.com y no a Beazley.com. Por el contrario, https://subscribe.beazley.com es un subdominio que pertenece a Beazley.com. Esto puede resultar contraintuitivo, ya que estamos acostumbrados a leer las frases de izquierda a derecha, pero los sitios web y los nombres de dominio deben leerse de derecha a izquierda.

Los objetivos son engañados para que revelen información confidencial, envíen su contraseña (y potencialmente el token MFA), envíen dinero o hagan clic en enlaces maliciosos sin darse cuenta de que están interactuando con una entidad desconocida y/o descargando un archivo malicioso.

Además de educar a los empleados sobre esta amenaza, añadir el encabezado "[Externo]" a los correos electrónicos recibidos de direcciones de correo electrónico externas puede ayudar a recordar a los empleados que estén más atentos a las direcciones de correo electrónico potencialmente falsificadas.

Limitar el impacto de un ataque de phishing

Los correos electrónicos de phishing se utilizan principalmente con dos fines. Pueden emplearse para redirigir a los usuarios a sitios web falsos y robar sus contraseñas, o bien pueden utilizarse como medio para desplegar y ejecutar código o software malicioso en las estaciones de trabajo de los usuarios. En este caso, el malware se adjunta al propio correo electrónico o se descarga desde un enlace que abre el usuario o mediante una macro incrustada en un documento adjunto de Word, Excel o PowerPoint.

Hay varias medidas que una organización puede tomar para limitar el impacto de que un usuario haga clic en un enlace malicioso, o doble

clic en un archivo malicioso. Un buen primer paso sensato es disponer de software antivirus actualizado y restringir la ejecución de archivos descargados reconocidos como malware. También se pueden bloquear las macros que intentan ejecutar comandos en el sistema o abrir enlaces externos. Por último, tener un agente EDR desplegado con la corrección automática activada en las estaciones de trabajo puede ayudar a detectar y bloquear la ejecución de nuevos contenidos maliciosos (previamente desconocidos).

Implemente medidas de seguridad y restricciones en los terminales de los usuarios, como AppLock, para garantizar que no se ejecutan scripts ni software no firmado, y que no se pueden utilizar dispositivos USB (por ejemplo, siguiendo el benchmark CIS). Impida el acceso al proceso "Lsass" del Servicio de Servidor de Autoridad de Seguridad Local (LSASS) que almacena las contraseñas de los usuarios localmente en los terminales aplicando la protección de credenciales, reduciendo a 1 el número de credenciales almacenadas localmente en caché y ejecutando Lsass como PPL.

Limitar los derechos de acceso de los usuarios también es clave. Esto incluye asegurarse de que los usuarios con acceso al correo electrónico no tengan acceso privilegiado (o de administrador), asegurarse de que los usuarios habituales no puedan inscribir nuevos dispositivos en el Directorio Activo y asegurarse de que las cuentas de administrador de dominio no se conecten a las estaciones de trabajo.

Por último, elabore procedimientos y forme a su equipo de seguridad informática para responder mejor a los ataques de phishing que tengan éxito.

Aislarse completamente de Internet, aunque es la solución más segura, rara vez es una opción. Pero con un poco de previsión, una organización puede armarse contra los ataques de phishing asumiendo proactivamente la responsabilidad de la seguridad de sus operaciones y de los datos de sus usuarios. Como las técnicas y los protocolos de prevención cambian con frecuencia, la formación continua y la reevaluación frecuente de los procedimientos de seguridad pueden ser a menudo las mejores defensas de una organización.

beazley