Aumentan los ataques con códigos QR contra ejecutivos que evaden la seguridad del correo electrónico

El uso de códigos QR para entregar cargas útiles maliciosas aumentó en el cuarto trimestre de 2023, especialmente contra los ejecutivos, que vieron 42 veces más phishing con códigos QR que el empleado promedio.

Imagen de Robert Lemos, escritor colaborador

Robert Lemos, escritor colaborador

8 de febrero de 2024

Lectura de 5 minutos

seguridad del código QR

FUENTE: SASIN PARAKSA A TRAVÉS DE SHUTTERSTOCK

Los ataques por correo electrónico basados en códigos QR aumentaron en el último trimestre, y los atacantes se dirigieron específicamente a ejecutivos y gerentes corporativos, lo que refuerza las recomendaciones de que las empresas coloquen protecciones digitales adicionales en torno a su liderazgo empresarial.

Para empeorar las cosas, los correos electrónicos de phishing que utilizan códigos QR (también conocidos como "quishing") a menudo pueden pasar los filtros de spam, y los ataques dirigidos a los usuarios de Microsoft 365 y DocuSign llegan con éxito a las bandejas de entrada de los correos electrónicos, según un informe publicado esta semana por Abnormal Security, un proveedor. de la seguridad del correo electrónico en la nube.

En el cuarto trimestre de 2023, el alto ejecutivo promedio de la alta dirección sufrió 42 veces más ataques de phishing utilizando códigos QR en comparación con el empleado promedio. Otros roles gerenciales también sufrieron un aumento en los ataques, aunque significativamente menores, y estos ejecutivos que no pertenecen a la alta gerencia encontraron cinco veces más ataques de phishing basados en códigos QR, según el informe de la compañía.

En general, los datos demuestran que los atacantes tienen ejecutivos (y otros usuarios privilegiados) en sus sitios, dice Mike Britton, CISO de Abnormal Security.

"Si soy un atacante, quiero atacar a las personas que tienen la capacidad de recibir pagos y credenciales que me dan acceso a la información más interesante", dice. "O quiero fingir ser esas personas, porque una vez más, la ingeniería social requiere esa confianza, [para que una víctima piense,] oye, este vicepresidente de ventas o este vicepresidente de recursos humanos me está pidiendo que haga algo, [haciéndolos] por lo general es más probable... que tome medidas".

Si bien los códigos QR existen desde hace tres décadas, se volvieron mucho más populares durante la pandemia, cuando los restaurantes y otras empresas dirigieron a los clientes a realizar pedidos en línea y sin contacto. En un contexto empresarial, uno de los principales casos de uso de los códigos QR es ofrecer enlaces para facilitar el proceso de registro para la autenticación multifactor (MFA). Los ciberatacantes se han sumado: más de una cuarta parte de los ataques a códigos QR (27%) en el cuarto trimestre fueron avisos falsos de MFA, por ejemplo, mientras que aproximadamente uno de cada cinco ataques (21%) fueron notificaciones falsas sobre un documento compartido, según Informe de Seguridad Anormal.

gráfico de barras de ataques qr por rol

Los altos ejecutivos ven 42 veces más ataques utilizando códigos QR que los empleados regulares. Fuente: Seguridad anormal

Debido a que los atacantes ocultan su enlace de phishing en una imagen, el phishing con códigos QR evita las sospechas de los usuarios y algunos productos de seguridad del correo electrónico. Además, se pueden colocar códigos QR maliciosos en espacios físicos mediante una simple pegatina, evitando por completo la seguridad digital.

"Los ataques explotan la confianza inherente de los usuarios en los códigos QR, incrustándolos en elementos cotidianos como parquímetros o carteles", dice Monique Becenti, directora de producto de la firma de seguridad móvil Zimperium. "La tasa de éxito del phishing con códigos QR superará a los métodos de phishing tradicionales porque a menudo evitan los típicos desencadenantes de sospecha de los usuarios, como los errores tipográficos en la URL, lo que lleva a una mayor probabilidad de escanearlos".

Otra forma más de robar las credenciales de los ejecutivos

En su mayor parte, los atacantes que se centran en los ejecutivos buscan las credenciales (nombres de usuario y contraseñas) de usuarios privilegiados. El phishing de credenciales es la forma más popular de ataque por correo electrónico y representa el 73 % de todos los ataques a través del vector y el 84 % de los ataques que utilizan un código QR; y a menudo conducen a compromisos más importantes, dice Britton de Abnormal Security.

"El objetivo principal es conseguir que un usuario robe sus credenciales", afirma. "Una vez que tengo tus credenciales, puedo causar mucho más daño, y puedo causar mucho daño duradero. Si tengo tus credenciales, puedo iniciar sesión en tu cuenta, puedo ver a quién le has enviado correos electrónicos, puedo Puedo enviar correos electrónicos haciéndome pasar por usted y puedo crear reglas de filtrado de correo".

Ese último punto es una forma común de abusar de las credenciales de correo, afirma Britton. El atacante creará una regla de copia oculta (BCC) que reenvía todos los correos electrónicos a la cuenta del atacante.

Además, "los actores de amenazas también reconocen que a menudo varias personas tienen acceso a la bandeja de entrada de un ejecutivo, como los asistentes ejecutivos", afirma el informe. "En consecuencia, cada individuo que conoce las credenciales de inicio de sesión de la bandeja de entrada de un VIP representa un punto de entrada potencial que puede ser explotado por un atacante".

Para frustrar el quishing se necesita tecnología y capacitación del ser humano

La buena noticia es que, desde octubre, el phishing con códigos QR ha disminuido en gran medida, después de representar el 22% de los ataques de phishing, según la firma de gestión de riesgos humanos Hoxhunt. "Desde octubre pasado, hemos visto evidencia de que los filtros de correo electrónico se están poniendo al día con la técnica de phishing QR", dice Jon Gellin, líder del equipo de amenazas de Hoxhunt. "Como menos ataques de este tipo son perpetrados por

Al evaluar filtros de correo electrónico, ha habido una disminución resultante en su popularidad".

Sin embargo, incluso si el quishing disminuye, seguirá siendo una herramienta para los atacantes, de la misma manera que las URL acortadas y el spam de imágenes siguen utilizándose en los ciberataques. La mejor manera de proteger a los usuarios es capacitarlos, afirma Gellin. Alrededor del 5% de los usuarios responden a un ataque de phishing en los primeros minutos, lo que sugiere que un grupo de empleados bien capacitados puede ayudar a mitigar un ataque.

"Como ha demostrado la tendencia del phishing QR, algunas amenazas siempre escapan incluso a los filtros más sofisticados", afirma. "En ese momento, depende de la capa humana tener las habilidades y herramientas para enfrentar la amenaza de manera efectiva".

La capacitación es importante, pero debido a que una sola falla puede tener un impacto significativo, se necesitan controles técnicos, dice Britton de Abnormal Security.

"He visto algunos ataques de phishing en los que incluso yo tengo que pedir una segunda opinión a la gente porque parecen muy reales", afirma. "¿Cómo espero que una persona de RRHH acierte siempre? ¿Cómo espero que una persona de cuentas por pagar? ¿Cómo espero que un analista financiero?"

"La formación es importante, pero vamos a fracasar, y sólo hace falta un fracaso", afirma.