ANUNCIO DE SERVICIO PÚBLICO

BURÓ FEDERAL DE INVESTIGACIONES [FBI, por su siglas en inglés]

[sello: Departamento de Justicia
Buró Federal de Investigaciones]

[sello: Buró Federal de Investigaciones
Centro de Quejas de Crímenes en Internet]

14 de agosto, 2023

Número de aviso
I-081423-PSA

Favor de dirigir sus preguntas relacionadas con este anuncio de servicio público [PSA, por sus siglas en inglés] a su **Oficina Regional del FBI.**

Ubicaciones de Oficinas Regionales:
www.fbi.gov/contact-us/field-offices

Los ciberdelincuentes se dirigen a víctimas a través de aplicaciones móviles en prueba beta

El FBI le advierte al público que los ciberdelincuentes están incorporando código malicioso en aplicaciones móviles en prueba beta (apps) para defraudar a posibles víctimas. Las aplicaciones en prueba beta son servicios en línea para probar aplicaciones móviles antes de su lanzamiento oficial. Las aplicaciones beta por lo general, no están sujetas a los procesos de revisión de los sistemas operativos móviles.

Las aplicaciones maliciosas permiten el robo de información de identificación personal [PII, por sus siglas en inglés], el acceso a cuentas financieras o la toma de control del dispositivo. Las aplicaciones pueden parecer legítimas mediante el uso de nombres, imágenes o descripciones similares a las aplicaciones populares. Los ciberdelincuentes suelen utilizar fraudes de phishing o estafas románticas para establecer comunicaciones con la víctima, y después, dirigen a la víctima a descargar una aplicación móvil en prueba beta alojada en un entorno de aplicaciones móviles en prueba beta, prometiendo incentivos como grandes pagos financieros.

El FBI está al tanto de los esquemas de fraude en los que ciberdelincuentes no identificados contactan a las víctimas a través de interconexión de redes y aplicaciones de citas y las dirigen a descargar aplicaciones móviles en prueba beta, tales como una plataforma de intercambios de criptomonedas, que permiten el robo. Las víctimas ingresan los detalles legítimos de la cuenta en la aplicación, enviando dinero que creen será invertido en criptomonedas, pero en su lugar, los fondos de la víctima son enviados a los ciberdelincuentes.

Si una víctima descarga una de estas aplicaciones en prueba beta fraudulentas y enmascarada como una aplicación legitima de inversión en criptomonedas, la aplicación puede extraer dinero de la víctima a través de inversiones falsas.

Indicadores

Las señales de alerta de una aplicación maliciosa incluyen:

- La batería móvil se agota más rápido de lo habitual
- El dispositivo móvil se demora al procesar una solicitud
- Aplicaciones no autorizadas instaladas sin el conocimiento del usuario
- Anuncios emergentes persistentes
- Un alto número de descargas con pocas o ninguna reseña

- Aplicaciones que solicitan acceso a permisos que no tienen nada que ver con la funcionalidad anunciada
- Errores de ortografía o gramaticales, información vaga o genérica, o falta de detalles sobre la funcionalidad de la aplicación dentro de la descripción de la aplicación
- Ventanas emergentes [Pop-ups] que parecen anuncios, advertencias del sistema o recordatorios

Recomendaciones

- Consulte los comentarios de los creadores de las aplicaciones y las opiniones de los clientes antes de descargar.
- No envíe un pago a alguien con quien solo ha hablado en línea, incluso si cree que ha establecido una relación con el individuo.
- No proporcione información personal o financiera por correo electrónico o mensaje y no responda a solicitudes de correo electrónico o mensaje, incluyendo enlaces.
- No descargue ni utilice aplicaciones que parezcan sospechosas como herramientas para invertir a menos que pueda verificar la legitimidad de la aplicación.
- Sea consciente de una sensación de urgencia o de amenazas, tales como "su cuenta se cerrará" o "actúe ahora".
- Tenga cuidado con los archivos adjuntos no solicitados, incluso de personas que conoce. Los ciberdelincuentes pueden "suplantar" la dirección del remitente, haciendo que parezca que el mensaje procede de un asociado de confianza. No responda.
- Si un correo electrónico, un archivo adjunto a un correo electrónico o un mensaje le parece sospechoso, no lo abra, aunque el software antivirus indique que el mensaje está limpio. Los atacantes lanzan nuevos virus continuamente y es posible que el software antivirus no tenga la firma.
- No haga clic en los enlaces de correos electrónicos o mensajes de texto. Muchos ciberdelincuentes utilizan mensajes de aspecto legítimo para engañar a los usuarios a fin de que proporcionen detalles de inicio de sesión. Verifique la dirección URL pasando el mouse sobre el enlace y compruebe si hay incoherencias.
- Examine los archivos adjuntos y los hipervínculos de sitios web contenidos en los correos electrónicos, incluso de personas que cree que conoce y guarde y haga un análisis de los archivos adjuntos antes de abrirlos.
- Mantenga el software actualizado.
- Limite los permisos de las aplicaciones y elimine las aplicaciones que no utiliza.

El FBI solicita a las víctimas que denuncien actividades fraudulentas, sospechosas o delictivas al Centro de Quejas de Crímenes en Internet del FBI en www.ic3.gov.