Advierten por un aumento en las aplicaciones de banca maliciosa

27/07/2020

El FBI emitió una advertencia sobre el mayor uso de aplicaciones de banca móvil por parte de los estadounidenses que significaría una mayor amenaza de los ciberdelincuentes que atacan a las mismas. La agencia de investigación de ese país, estima que más del 75% de la población usó la banca móvil en 2019. Otro estudio indicó un aumento del 50% en la banca móvil este año.

Estas vulnerabilidades se presentan como aplicaciones bancarias falsas, páginas de inicio de sesión falsas y troyanos que se superponen a una página de inicio de sesión falsa en un inicio de sesión bancario legítimo.

La página maliciosa envía cualquier información que ingrese directamente a los ciber actores maliciosos. El FBI también advirtió que algunos troyanos pueden permanecer inactivos en el dispositivo de la víctima durante largos períodos de tiempo hasta que abra ciertas aplicaciones como una aplicación bancaria.

«En 2018, se detectaron casi 65.000 aplicaciones falsas en las principales tiendas de aplicaciones, lo que lo convierte en uno de los sectores de más rápido crecimiento del fraude basado en teléfonos inteligentes», advirtió el FBI.

La alerta continúa para proporcionar en su mayoría buenos consejos sobre cómo evitar estas vulnerabilidades, como solo descargar una aplicación de la tienda de aplicaciones oficial del teléfono o del sitio web bancario. Además, nunca descargar una aplicación bancaria de un tercero.

Otra buena idea es usar MFA (autenticación multifactor) para todos los inicios de sesión. El uso de esta aplicación detendrá la toma de control de una cuenta con una contraseña comprometida.

El informe establece que «habilitar cualquier forma de autenticación de dos factores será una ventaja para el usuario», pero algunos métodos de autenticación funcionan mejor que otros. Si un troyano en su teléfono puede mostrar una página de inicio de sesión, es probable que pueda leer sus mensajes de texto.

Si usa un mensaje SMS para su segundo factor, el troyano puede enviarlo a los actores de la amenaza. Recomendamos usar aplicaciones MFA seguras o tokens de hardware como segundo factor siempre que sea posible.

El MFA basado en notificaciones push, donde la aplicación proporciona una notificación de aprobación o denegación, proporciona una opción más segura. El consejo más importante es no entregarle nunca a nadie la contraseña de un solo uso o el token de la aplicación.

El FBI también recomienda crear una contraseña de al menos ocho caracteres usando letras mayúsculas, minúsculas y símbolos.

Sin embargo, la recomendación en la advertencia del FBI sobre el uso de contraseñas no considera estudios recientes sobre el comportamiento humano y la rapidez con que los programas pueden descifrar los hash. Por ejemplo, dado un algoritmo hash moderno de una contraseña que usa los requisitos mínimos, podríamos forzar la contraseña por fuerza bruta en menos de 21 segundos. No tenemos equipos especiales, excepto una tarjeta gráfica de alta gama utilizada para pruebas como esta.

En tanto, especialistas de WatchGuard recomiendan una frase de contraseña de al menos 16 caracteres. Usar una frase que pueda recordar, como nombres y lugares o fechas, por ejemplo,

«SierraTerrierTexas». Esto proporciona una contraseña mucho más segura que nunca podríamos imponer. Además, evite las palabras comunes que uno podría adivinar fácilmente. Esto protege contra ataques de diccionario donde el actor de ciberamenaza combina listas de palabras comunes para descifrar contraseñas.

Otra recomendación es estar siempre atento a los mensajes de texto o llamadas telefónicas que le solicitan información privada. Chase Bank advierte a sus usuarios de estafas como esta en su sitio web «No responda a un correo electrónico, llamada telefónica o mensaje de texto que le indique que su cuenta ha sido comprometida, luego le pide que brinde o confirme su información personal o de cuenta».

Por último, no clickear ningún enlace directamente desde un mensaje o correo electrónico o si detecta una aplicación o inicio de sesión sospechoso.

Si el servicio tiene problemas con su cuenta, puede resolverlo yendo directamente al sitio web o comunicarse directamente con la institución financiera desde un número de teléfono publicado en su sitio web oficial para verificar su autenticidad.