Si utilizas Agama Wallet, de Komodo, para almacenar tus criptomonedas KMD y BTC, te tenemos una mala noticia, pues posiblemente tus fondos se transfirieron sin autorización.

Sin embargo, según la compañía, con un poco de suerte se podrán recuperar los fondos. Komodo, un proyecto de criptomonedas y almacenamiento de las mismas, mediante su aplicación Agama, adoptó una forma sorprendente de proteger los fondos de sus clientes.

La compañía hackeó a sus clientes y transfirió sin autorización casi 8 millones de KMD y 96 Bitcoins de sus billeteras a una nueva dirección de la empresa. Esto con el fin de asegurar los fondos contra ataques de hackers.

Komodo se enteró recientemente de una biblioteca de JavaScript de código abierto malintencionada que la compañía estaba usando en su aplicación Agama Wallet.

La biblioteca llamada *«electron-native-avis»*, hace dos meses recibió una actualización de su autor anónimo que incluyó una puerta trasera secreta en el nuevo código que fue diseñado para robar y enviar claves privadas y otras frases de acceso de los usuarios de la cartera de Agama a un servidor remoto.

Debido a esto, si iniciaste sesión en cualquier versión de la cartera de Agama descargada del sitio oficial de Komodo o sus apps de Android e iOS después del 13 de abril, es probable que hayan robado tus credenciales.

La actualización de la biblioteca maliciosa en cuestión, fue detectada en un principio por un equipo de seguridad en el servicio de repositorio de paquetes npm JavaScript, que después informó a Komodo sobre el problema.

> *«El ataque se llevó a cabo utilizando un patrón que se está volviendo cada vez más popular, publicando un paquete útil (electron-native-not) en npm, esperando hasta que el objetivo lo esté utilizando, y después actualizándolo para incluir una carga útil maliciosa»*, dice el blog de npm.

El blog de npm también compartió un video de demostración sobre cómo la versión de puerta trasera de la billetera de Agama ha estado enviando de forma secreta la clave privada de una billetera a un servidor remoto en segundo plano.

Después de descubrir la vulnerabilidad, Komodo decidió usar una técnica similar de robo de contraseñas en contra de sus usuarios para obtener acceso a la mayor cantidad posible de carteras afectadas y transferir los fondos a una cartera segura antes de que los piratas informáticos puedan haberlos robado.

> *«Las carteras seguras RSgD2cmm3niFRu2kwwtrEHoHMywJdkbkeF (KMD) and 1GsdquSqABxP2i7ghUjAXdtdujHjVYLgqk (BTC), están bajo el control del Equipo Komodo, y los activos pueden ser recuperados por sus dueños»*, dijo Komodo.

Sin embargo, es importante tener en cuenta que no todas las carteras de usuarios afectadas han sido vaciadas por la compañía.

Por lo tanto, si tu billetera no ha sido barrida, te recomendamos mover inmediatamente todos tus fondos de Agama a una nueva dirección.

Komodo también informó que la versión Verus de la billetera Agama no se ve afectada por la vulnerabilidad y aún es completamente segura, ya que no incluye la biblioteca maliciosa en cuestión. Por lo tanto, los usuarios de la versión Verus de Agama no se vieron afectados por el incidente de seguridad.