La extensión de Mega para Chrome fue hackeada y utilizada para robar contraseñas, poniendo en peligro millones de carteras de criptomonedas.

Luego de recibir el aviso sobre el cambio de la extensión legítima por una maliciosa, Google eliminó dicha extensión de la Chrome Web Store, sin embargo, los usuarios que la tenían instalada podrían haber comprometido sus credenciales.

SerHack, desarrollador e ingeniero de seguridad, fue quien llevó a cabo la investigación, y al identificar el problema, publicó rápidamente un aviso por medio de su cuenta de Twitter. Según su hallazgo, la versión 3.39.4 de la extensión de Mega para Chrome era maliciosa, capturaba el nombre de usuario y contraseña de servicios como Amazon, GitHub, Google y Microsoft.

Luego de este aviso, otros investigadores de seguridad se pusieron a trabajar para analizar la extensión y descubrieron que además de robar las credenciales de diversos servicios, la extensión también supervisaba el envío de cualquier formulario que contuviera cadenas de Registro o Inicio de sesión, además de variables username, email, user, login, usr, pass, password, passwd, entre otros.

Además, la extensión también podía robar las claves privadas de wallets como MyMonero o MyEtherWallet para robar las criptomonedas de los usuarios.

Después de detectar las claves de inicio de sesión de servicios de carteras, la extensión copiaba los datos y los enviaba a un servidor ubicado en Ucrania.

Según análisis de los investigadores de seguridad, la extensión de Mega fue hackeada en algún momento luego de 2 de septiembre. Mientras tanto, Mega confirmó que su cuenta en la Chrome Web Store fue hackeada el 4 de septiembre y hasta ahora siguen investigando lo sucedido.

Si tenías instalada esta extensión, debes eliminarla inmediatamente y cambiar todas tus contraseñas.