Masterhacks – La compañía Eltima Software, desarrolladora del reproductor de video Elmedia Player y el gestor de descargas Folx, anunció que las dos aplicaciones estaban infectadas con un malware conocido como OSX.Proton.

La compañía de seguridad ESET alertó a Elmedia, luego la empresa responsable tomó las acciones necesarias. Descubrieron que hackers lograron entrar en los servidores de los desarrolladores para infectar con el malware los archivos de descargas.

Proton es un troyano que controla de forma remota las computadoras Mac, abriendo una puerta trasera que permite el acceso en línea de comandos, con lo que los hackers logran robar información sensible.

El 19 de octubre, ESET registró el malware en las descargas del programa, Eltima ya eliminó el malware a las 3:10 PDT del mismo día. Si cuentas con este software y se actualizó automáticamente, ya no deberías tener el malware, pero puedes analizar los siguientes archivos para evitar dudas:

/tmp/Updater.app/
/Library/LaunchAgents/com.Eltima.UpdaterAgent.plist
/Library/.rand/
/Library/.rand/updateragent.app/