Emsisoft, fabricante de antivirus, afirmó haber encontrado un error en la aplicación de descifrado del ransomware Ryuk. Esta aplicación es la que los hackers proporcionan a las víctimas para recuperar sus archivos después de pagar el rescate.

Según Emsisoft, el error causa una recuperación incompleta de algunos tipos de archivos, lo que lleva a la pérdida de datos, incluso después de haber pagado el rescate.

El problema es que el descifrador trunca un byte desde el final de cada archivo que descifra, según la compañía antivirus.

Aunque por lo general el último byte en la mayoría de los archivos está como relleno y no se usa, para algunas extensiones de archivo, esos bytes contienen información crucial, que cuando se elimina causa un daño permanente de los datos.

> *«Muchos archivos de tipo de disco virtual como VHD/VHDX, así como muchos archivos de base de datos como Oracle, almacenan información importante en ese último byte y los archivos dañados de esta forma no se cargarán correctamente después de descifrarlos»,* dice Emsisoft.

También dijo que la compañía fue capaz de rastrear y corregir errores y que podría *«arreglar»* los descifradores de Ryuk para poder descifrar los archivos sin truncar el último byte y corromper los archivos.

Sin embargo, existe otro problema, y es que el descifrador de Ryuk también elimina los archivos cifrados originales, lo que significa que las víctimas no pueden volver a ejecutar la operación de descifrado nuevamente.

Debido a esto, Emsisoft publicó hoy un anuncio de servicio público (PSA) urgente, recomendando que las víctimas creen una copia de los archivos encriptados, para tener como respaldo en caso de que el descifrador falle y destruya los archivos.

> *«Esperamos correr la voz sobre esto lo más rápido y ampliamente posible para que las organizaciones afectadas puedan evitar la pérdida de datos»,* dijo Brett Callow, portavoz de Emsisoft.

La compañía también informó que las víctimas pueden comunicarse por medio de ryukhelp@emsisoft.com para que sus analistas arreglen el descifrador que recibieron por parte de los piratas informáticos, aunque este es un servicio de pago.

Ryuk es una de las variantes de ransomware más activas en la actualidad. El ransomware desplegado por bandas de hackers en redes empresariales utiliza una infección de malware anterior como punto de entrada, generalmente por medio de los troyanos Emotet o TrickBot.

Las infecciones atribuidas a Ryuk incluyen el proveedor de servicios de gestión T-Systems, el proveedor de servicios financieros ASD Audit, el fabricante de tecnología de aislamiento TECNOL, el fabricante de herramientas de automatización Pliz, la ciudad de New Bedford, Tribune Publishing, el proveedor PerCSoft, el proveedor de atención médica CorVel, el proveedor de TI CloudJumper, la ciudad de Lake City, entre muchos otros.