La compañía de seguridad Emsisoft, con sede en Nueva Zelanda, creó un conjunto de herramientas de descifrado para Stop, una familia de ransomware que incluye a Djvu y Puma, que según sus informes, podrían ayudar a las víctimas a recuperar algunos de sus archivos.

Según cifras de ID-Ransomware, Stop es el ransomware más activo del mundo, con más de la mitad de todas las infecciones globales. Pero Emsisoft cree que es probable que esa cifra sea mucho más alta.

El ransomware es una de las formas más comunes actualmente para que los delincuentes cibernéticos ganen dinero, mediante la infección de computadoras con el malware que bloquea todos los archivos de la computadora víctima con procesos de cifrado.

Una vez que Stop infecta, cambia el nombre de los archivos de usuario por otro con extensión diferente, reemplazando los archivos .jpg y .png con .radman, .djvu y .puma, como ejemplo.

Las víctimas pueden desbloquear sus archivos realizando un pago en criptomonedas, aunque muchas veces no es seguro recibir la solución luego de realizar el pago.

No todos los ransomware son iguales, algunos expertos en seguridad han logrado desbloquear archivos de algunas víctimas sin tener que pagar el rescate, encontrando vulnerabilidades en el código que activa el ransomware, lo que permite en algunos casos, revertir el cifrado.

Sin embargo, Stop es el último ransomware que la compañía Emsisoft no ha podido descifrar.

> *«Es una herramienta de descifrado más complicada de lo que normalmente se obtendría. Es un ransomware muy complicado»*, dijo Michael Gillespie, desarrollador de las herramientas e investigador de Emsisoft.

En el caso de Stop, se encriptan los archivos de los usuarios con una clave en línea que se extrae del servidor del atacante, o una clave sin conexión, que encripta los archivos de los usuarios cuando no pueden comunicarse con el servidor.

Gillespie dijo que muchas víctimas han sido infectadas con claves fuera de línea porque la infraestructura web de los atacantes generalmente estaba inactiva o inaccesible para la computadora infectada.

Los atacantes de ransomware brindan a cada víctima una *«llave maestra»*, dijo Gillespie. Esta masterkey se combina con los primeros cinco bytes de cada archivo que encripta el ransomware. Algunos tipos de archivos, como los de imagen .png, comparte los mismos cinco bytes en cada archivo .png. Al comparar un archivo original con uno cifrado y aplicar algunos cálculos matemáticos, se puede descifrar no solo ese archivo png, sino otros del mismo tipo.

La mayoría de los documentos modernos de Microsoft Office, como .docx y .pptx, comparten los mismos cinco bytes que los archivos .zip. Con cualquier archivo antes y después, cualquiera de estos tipos de archivos puede descifrar los demás.

> *«La víctima tiene que encontrar un buen antes y un después de básicamente todos los formatos que quieren recuperar»,* dijo Gillespie.

Una vez que el sistema se encuentre libre del ransomware, las víctimas deberían tratar de buscar cualquier archivo que haya sido respaldado. Esos pueden ser fondos de pantalla predeterminados de Windows, o puede significar revisar el correo electrónico y encontrar el archivo original que se envió, para combinarlo con el archivo cifrado.

Cuando el usuario carga archivos *«antes y después»* en el portal de envío, el servidor hará los cálculos y determinará si el par de archivos es compatible y explicará qué extensiones de archivo se pueden descifrar.

> *«Para cualquier infección después de finales de agosto de 2019, desafortunadamente, no hay mucho que podamos hacer a menos que esté encriptada con la clave fuera de línea. Si se extrajo una clave en línea del servidor del atacante, las víctimas no tienen suerte»,* dijo el investigador.

También mencionó que los archivos enviados al portal deben tener un tamaño superior a 150 kilobytes o las herramientas de descifrado no funcionarán, porque esa es la cantidad de archivos serán difíciles, si no imposibles de recuperar, porque cada extensión de archivo maneja los primeros cinco bytes del archivo de forma diferente.

Anteriormente, Gillespie estaba procesando manualmente las claves de descifrado para las víctimas cuyos archivos habían sido cifrados con una clave fuera de línea.

Creó una herramienta de descifrado rudimentaria, llamada STOPDecrypter, que logró descifrar los archivos de algunas víctimas. Pero mantener actualizada la herramienta era algo complicado. Cada vez que encontraba una solución alternativa, los atacantes sacaban nuevas extensiones de archivos cifrados en un esfuerzo por burlarlo.

Desde el lanzamiento de STOPDecrypter, Gillespie recibió miles de mensajes de personas cuyos sistemas han sido encriptados por el ransomware Stop. Al publicar en los foros de Bleeping Computer, ha podido mantener a las víctimas actualizadas con sus hallazgos y actualizaciones de su herramienta de descifrado.

Pero a medida que algunas víctimas se desesperaron por recuperar sus archivos, Gillespie se enfrentó a la peor parte de sus frustraciones.

> *«Los moderadores del sitio respondieron pacientemente. Han mantenido la paz. Un par de otros voluntarios en los foros también han estado ayudando a explicar las cosas a las víctimas».*

Gillespie agregó que la herramienta también se incluirá en el proyecto No More Ransom de Europol, para que las futuras víctimas sean notificadas de que haya una herramienta de descifrado disponible.