Un nuevo ransomware llamado CryCryptor, está dirigido a usuarios canadienses de Android. Se distribuye a través de distintos sitios web que se hacen pasar por portales para una aplicación de rastreo de COVID-19 respaldada por el gobierno.

Según una investigación de ESET, CryCryptor fue detectado pocos días después de que el gobierno de Canadá anunciara oficialmente su intención para respaldar el desarrollo de una aplicación de rastreo voluntaria a nivel nacional, llamada Alerta COVID.

> *«Una vez que el usuario es víctima de CryCryptor, el ransomware cifra los archivos en el dispositivo, todos los tipos de archivos más comunes, pero en lugar de bloquear el dispositivo, deja un archivo 'readme' con el correo electrónico del atacante en cada directorio con archivos cifrados»,* dice ESET.

los investigadores de ESET analizaron la aplicación y descubrieron un error de tipo *«exportación incorrecta de componentes de Android»*, que MITRE etiqueta como CWE-926.

Debido a dicho error, cualquier aplicación que esté instalada en el dispositivo afectado puede iniciar cualquier servicio exportado proporcionado por el ransomware. Gracias a esto, los investigadores pudieron desarrollar una herramienta de descifrado.

Funcionamiento de CryCryptor

Una vez que el dispositivo se infecta, el ransomware solicita acceso a los archivos. Después de obtener el acceso, cifra los archivos en medios externos con algunas extensiones.

Los archivos se cifran en AES con una clave de 16 caracteres generada aleatoriamente. Después de que el ransomware cifra un archivo, se crean tres archivos nuevos y se elimina el original. El archivo cifrado tiene la extensión .enc, y el algoritmo genera una «salt» única para cada archivo cifrado, almacenado con la extensión .enc.salt y un vector de inicialización, .enc.iv.

Después de encriptar todos los archivos, CryCryptor muestra una notificación que dice *«Archivos personales encriptados, consulte readme_now.txt».*

El servicio responsable del descifrado de archivos en CryCryptor almacena la clave de cifrado en las preferencias compartidas, por lo que no se tiene que contactar a ningún C&C para recuperarla. Cabe destacar que el servicio se exporta sin restricciones en el Manifiesto de Android (vulnerabilidad de seguridad CWE-926).

> *«En base a esto, creamos una aplicación de descifrado de Android para aquellos afectados con el ransomware CryCryptor. Naturalmente, la aplicación de descifrado solo funciona en esta versión de CryCryptor»,* dijeron los investigadores.

ESET menciona también que el ransomware CryCryptor está basado en un código fuente abierto en GitHub, denominado por los desarrolladores del ransomware como CryDroid.