CENTRO CIBERNÉTICO POLICIAL

B@CIB – 004 | Boletín de Análisis en CIBERSEGURIDAD

RANSOMWARE migra a DISPOSITIVOS MÓVILES

Ransomware es un tipo de malware que tiene como propósito restringir el acceso a los archivos contenidos en un dispositivo móvil. De esta manera, el ciberdelincuente exige el pago de una recompensa a cambio de quitar las restricciones que afecta la información electrónica de la víctima.

Alcance Internacional

Al respecto, la Organización de los Estados Americanos pone a disposición en su portal Web, diferentes guías o modelos para la atención de incidentes informáticos. En estos documentos se explica como detectar el incidente, limitar el impacto del ataque, remover la amenaza y recobrar el estado de los sistemas a una etapa normal, así como delinear y mejorar los procesos afectados.

Ref.: https://www.sites.oas.org

CENTRO CIBERNÉTICO POLICIAL

B@CIP - 004 | Boletín de Análisis en CIBERSEGURIDAD

Métodos de propagación

El ransomware se transmite como un troyano infectando el sistema operativo, por ejemplo, mediante la descarga de archivos o mediante las vulnerabilidades del software existente en un dispositivo móvil, cifrando los archivos de manera parcial o completa. Finalemtente, esta información únicamente es accesible mediante un método de cifrado que sólo conoce el ciberdelincuente. En ese sentido, la víctima recibe un mensaje donde se le indica que debe dar una recompensa a cambio de la información. Para ello, la persona afectada en caso de efectuar el pago, recibe una clave e instrucciones para restaurar los archivos encriptados o cifrados.

Vector de ataque

Simplocker, se presenta en forma de una aplicación que resulta ser un troyano, aunque su apariencia resulta ser la de un complemento de Flash Player. Por otra parte, este malware es el primer ransomware desarrollado para sistemas operativos Android, el cual cuenta con la siguiente suma de verificación:

SHA256: d765e722e295969c0a5c2d90f549-db8b89ab617900bf4698db41c7cdad993bb9

Recomendaciones

El Centro Cibernético Policial ofrece los siguientes consejos para prevenir y constrarrestar este fenómeno delictivo:

1. Instalar un software antivirus en el móvil que nos ayude a prevenir o que al menos nos alerte sobre la instalación de aplicaciones maliciosas.

2. Descargar siempre aplicaciones de fuentes y tiendas oficiales. En caso de duda, los comentarios de otros usuarios pueden ayudarnos a elegir las aplicaciones legítimas.

3. Evite abrir o ejecutar ficheros contenidos en correos electrónicos; recuerde este es el principal medio de propagación del ransomware.