Malware para móviles

Malware Tipo Distribución	Características	Objetivo
USB Thief Troyano Dispositivo USB	Emplea mecanismos especiales para protegerlo de una copia o reproducción haciéndolo más difícil de detectar y analizar. Puede atacar sistemas que se encuentran aislados de Internet. puede no ser detectado mientras se mantenga en el dispositivo USB y se borre de la máquina al haber terminado su misión.	 Robo de información
Jigsaw *Ransomware* SPAM y Redes Sociales, USB, Sitios Web	Reconoce más de 225 tipos de archivos, utiliza el algoritmo AES para el cifrado, los archivos tienen la extensión. fun. Pide pago, pero este informa que cada hora si no se hace el pago del rescate se eliminarán ficheros secuestrados de manera aleatoria, aunque el usuario reinicie.	 Pago de rescate
Manamecrypt o CryptoHost *Ransomware* SPAM y Redes Sociales, USB, Sitios Web	Cifra los archivos afectados (en un archivo comprimido protegido con contraseña) borrando los originales, impide la ejecución de algunos programas instalados en las computadoras de las víctimas.	 Pago de rescate
"My video", "Private video", "My first video" Publicación Facebook	Al ingresar a un enlace el usuario se redirige a una página parecida a YouTube, se reproducirá el video, pide descargar una extensión para ver el contenido, siendo el malware que se expande en el navegador publicando videos falsos y etiquetando a los contactos del usuario.	 Robo de información
AutoLocky *Ransomware* SPAM y Redes Sociales, USB, Sitios Web	Utiliza un icono Adobe Reader (PDF) y podría estar circulando como adjunto en correos electrónicos. Una vez instalado, AutoLocky escaneará las unidades de disco y los cifrará mediante el algoritmo AES-128 anexando la extensión. locky al nombre del archivo.	 Pago de rescate
CryptFile2 *Ransomware* SPAM y Redes Sociales, USB, Sitios Web	Con algoritmo de cifrado RSA de 2048 bits, el más rudimentario para recuperar el acceso a los archivos, el usuario debe contactar con el ciberdelincuente a través del correo electrónico.	 Pago de rescate
BrLock *Ransomware* SPAM y Redes Sociales, USB, Sitios Web	Bloquea la pantalla del equipo.	 Pago de rescate
MM Locker *Ransomware* SPAM y Redes Sociales, USB, Sitios Web	Añade una extensión. locked y solicita una recompensa a través de un mensaje guardado en un archivo, el ciberdelincuente intenta convencer al usuario para que realice el pago, ya que según informan, no envía la clave de descifrado.	 Pago de rescate
CryptMix *Ransomware* Correos electrónicos basura y ataques *drive-by*	Asegura que el dinero de los rescates será para niños en dificultades. Puede cifrar cualquier extensión de archivo del equipo y además de afectar al disco duro local también tendrá efecto sobre los discos duros alojados en red.	 Pago de rescate
Lost Door Troyano Facebook, Youtube y Blogspot	Se adquiere a través de servicios de Internet populares. Catalogada como RAT (Remote Access Trojan), se puede adquirir entre 50 y 100 dólares dependiendo de las funciones.	 Ocultar el tráfico generado y recibido gracias al *port fowarding*, dificultando la detección de su actividad para enmascarar el tráfico procedente del servidor de control.
badBIOS Virus Dispositivo USB	A través de una memoria USB el virus badBIOS se introduce en los equipos e infecta la BIOS tomando el control de los altavoces y el micrófono, utilizando sonido de alta frecuencia, inaudible para el oído humano, se transmite y comunica con otros equipos haciendo posible intercambiar información.	 Robo de información