PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 19 de junio de 2022

N° 164-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 164	Fecha: 19-06-2022
		Página 4 de 6

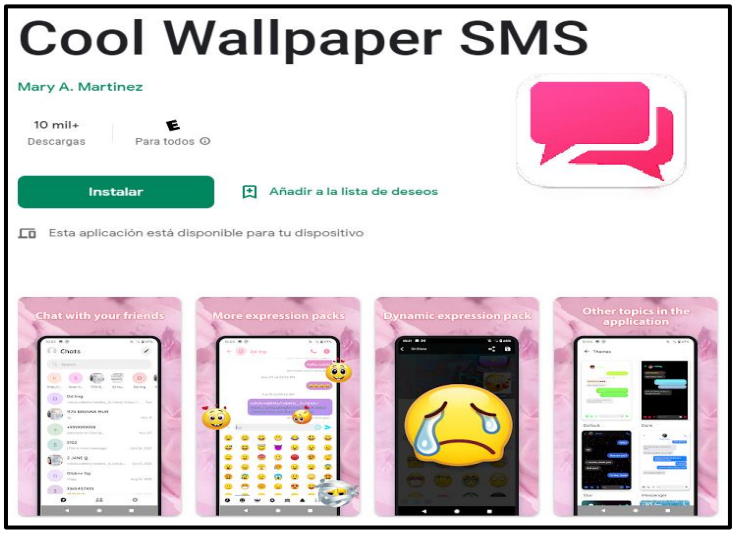
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Propagación de Troyano a través del aplicativo móvil COOL WALLPAPER SMS		
Tipo de ataque	Troyano	Abreviatura	Troyano
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que actores de amenazas vienen realizando una campaña de propagación de troyanos a través del aplicativo gratuito denominado COOL WALLPAPER SMS, que se encuentra disponible en la plataforma de distribución digital de aplicaciones móviles para los dispositivos con sistema operativo Android Google Play Store.

2. El aplicativo COOL WALLPAPER SMS, tiene la finalidad para que el usuario realice comunicación digital (SMS, MMS) a través de la red de internet; asimismo, puede personalizar el color y estilos del chat. Siendo fácil de descargar e instalar en el teléfono móvil.

3. ***APLICATIVO MÓVIL***



4. ***DETALLES DEL APLICATIVO MÓVIL:***

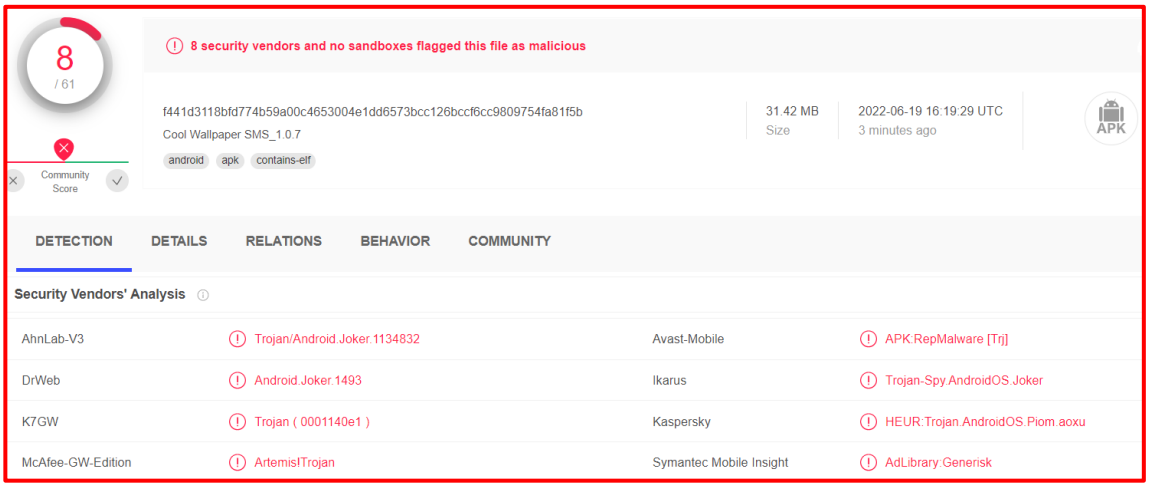
- ✓ Versión : 1.0.7
- ✓ Tamaño de archivo : 30.65 MB.
- ✓ Nombre del paquete : com.eztcool.wallpaper.forcool.eztsms
- ✓ Actualizado : 09JUN2022
- ✓ Precio : Gratis

5. ***PERMISOS SOLICITADOS:***

- ✓ Acceso a la galería de fotos y archivos multimedia.
- ✓ Acceso a cámara y video
- ✓ Acceso al almacenamiento del dispositivo móvil
- ✓ Información de contactos del dispositivo
- ✓ Información sobre las conexiones de red

- ✓ Información del ID del dispositivo móvil

6. ***PROVEEDORES DE SEGURIDAD INFORMÁTICA ALERTAN COMO MALICIOSO AL APLICATIVO DE ANÁLISIS.***

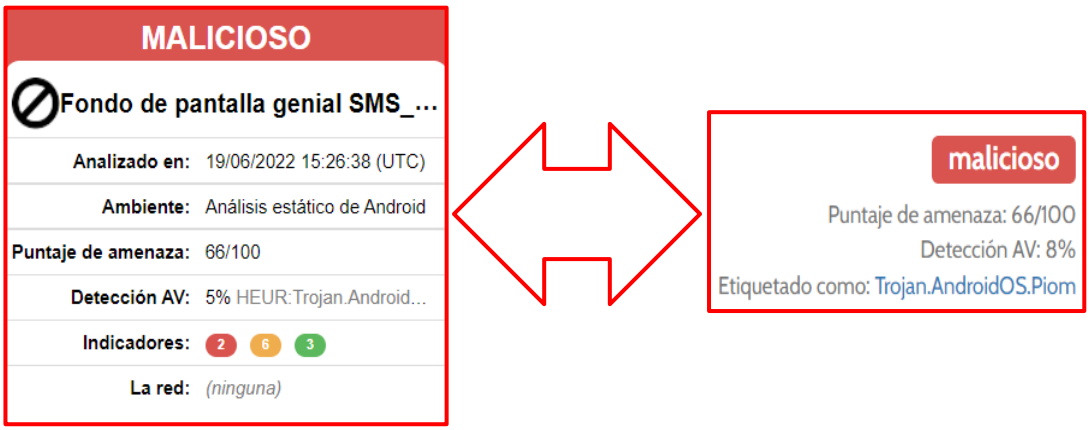


TROJAN/ANDROID: Es una aplicación maliciosa que se ejecuta en segundo plano en un dispositivo móvil sin que el usuario lo sepa. Espera silenciosamente las órdenes de un servidor de Comando y Control (C&C). Estos comandos pueden, desde robar y enviar información personal a servidores remotos, hasta actuar como bots DDoS contra las víctimas objetivo.

7. ***INDICADORES DE COMPROMISO (IoC)***

- ✓ MD5 : e95f6905e005d69bb7fc6ea78cec08d8
- ✓ SHA-1 : 19444100a96bc946f1dbf0aeaff1eca1f28a5155
- ✓ SHA-256 : f441d3118bfd774b59a00c4653004e1dd6573bcc126bccf6cc9809754fa81f5b

8. ***OTRAS DETECCIONES***:



9. Que los actores de amenazas a través de la plataforma de distribución digital de aplicaciones móviles para dispositivos con sistema Android "Google Play Store", vienen propagando troyanos, siendo el caso del aplicativo denominado COOL WALLPAPER SMS, lo que ocasiona un riesgo a la seguridad de los dispositivos móviles, toda vez que los ciberdelincuentes pueden ejecutar software espías, tomar el control y comando (C&C) o simplemente robar información sensible de las víctimas; lo que se recomienda lo siguiente:

- ✓ Desinstalar el aplicativo de análisis.
- ✓ Analizar los permisos que otorgan a las aplicaciones móviles.
- ✓ No abrir archivos sospechosos.
- ✓ Instalar y mantener actualizado el antivirus.
- ✓ Actualizar el sistema operativo del dispositivo móvil.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético