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

Lima, 31 de julio de 2022

N° 206-2022-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

Los anuncios de Facebook impulsan adware en Android 4
Propagación de Troyano Joker a través del aplicativo móvil CAMERA TRANSLATOR.....6
Índice alfabético 8

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 206	Fecha: 31-07-2022
		Página 04 de 08

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los anuncios de Facebook impulsan adware en Android		
Tipo de ataque	Adware	Abreviatura	Adware
Medios de propagación	Software infectado, Enlaces de internet.		
Código de familia	C	Código de Subfamilia	C01
Clasificación temática familia	Código Malicioso		

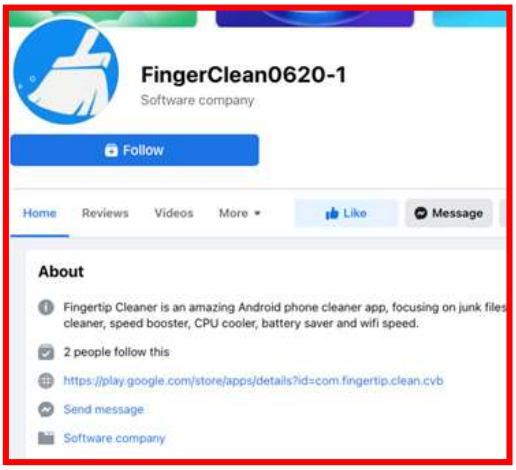
Descripción

FECHA DEL EVENTO:

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 30 de julio del 2022, se tomó conocimiento a través de la publicación realizada en la página web de **"BleepingComputer"**, sobre anuncios de Facebook que impulsan adware de Android con más de 7 millones de descargas de Play Store.

ANTECEDENTES:

Varias aplicaciones de adware promocionadas agresivamente en Facebook como limpiadores y optimizadores de sistemas para dispositivos Android cuentan con millones de instalaciones de la tienda Play Store. Las aplicaciones carecen de toda la funcionalidad prometida y empujan anuncios mientras intentan durar el mayor tiempo posible en el dispositivo.



DETALLES:

Las aplicaciones para evadir la eliminación se ocultan en el dispositivo de la víctima cambiando constantemente los íconos y los nombres, haciéndose pasar por Configuración o Play Store.

Las aplicaciones de adware abusan del componente de Android Contact Provider, que les permite transferir datos entre el dispositivo y los servicios en línea.

Los investigadores de McAfee descubrieron las aplicaciones de adware. Señalan que los usuarios no tienen que ejecutarlos después de la instalación para ver los anuncios porque el adware se inicia automáticamente sin ninguna interacción. La primera acción de estas molestas aplicaciones es crear un servicio permanente para mostrar los anuncios. Si el proceso se "mata" (termina), se vuelve a iniciar de inmediato.

Esto ha resultado descargas inusualmente altos para el tipo particular de aplicaciones, como se muestra en la lista a continuación:

1. **Junk Cleaner** , cn.junk.clean.plp, 1M+ descargas
2. **EasyCleaner** , com.easy.clean.ipz, más de 100 000 descargas
3. **Power Doctor**, com.power.doctor.mnb, más de 500 000 descargas
4. **Super Clean** , com.super.clean.zaz, 500K+ descargas
5. **Limpieza completa: limpieza de caché**, org.stemp.fll.clean, más de 1 millón de descargas
6. **Fingertip Cleaner** , com.fingertip.clean.cvb, más de 500 000 descargas
7. **Limpiador rápido** , org.qck.cle.oyo, más de 1 millón de descargas
8. **Keep Clean** , org.clean.sys.lunch, más de 1 millón de descargas
9. **Windy Clean** , in.phone.clean.www, más de 500 000 descargas
10. **Limpieza de alfombras** , og.crp.cln.zda, más de 100 000 descargas
11. **Cool Clean** , syn.clean.cool.zbc, más de 500 000 descargas
12. **Strong Clean** , in.memory.sys.clean, más de 500 000 descargas
13. **Limpieza de meteoros** , org.ssl.wind.clean, más de 100 000 descargas

Los limpiadores y optimizadores de sistemas son categorías de software populares a pesar de los bajos beneficios que brindan. Los ciberdelincuentes saben que una gran cantidad de usuarios probarían estas soluciones para prolongar la vida útil de sus dispositivos y, a menudo, disfrazan este tipo de aplicaciones maliciosas.

RECOMENDACIONES:

- Asegúrese de que Play Protect esté activo en su dispositivo y supervise regularmente sus datos de Internet y el consumo de batería para identificar cualquier proceso sospechoso que se ejecute en segundo plano.
- Si instaló aplicaciones que se encuentran en la lista deberá desinstalarlas de su dispositivo manualmente y ejecutar un escaneo de antivirus (pero debes asegurarte que este AV tenga buena reputación; además debes descargarlo de un sitio web confiable) para limpiar cualquier remanente.
- También puede eliminar el adware activando el modo seguro en su dispositivo Android, para detener la ejecución de las apps instalas por ti. (esta es una medida de protección temporal instalada por el sistema operativo Android; para detectar y solucionar problemas que afectan al equipo, sin la necesidad de borrar información).
- Otra opción efectiva es restablecer a configuración de fábrica su dispositivo (lo cual involucra la pérdida total de la información del equipo).
- Verificar las reseñas y calificaciones de las aplicaciones antes de descargarlos y visitar el sitio web del desarrollador, leer la política de privacidad y prestar atención a los permisos solicitados durante la instalación.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/facebook-ads-push-android-adware-with-7-million-installs-on-google-play/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 206	**Fecha: 31-07-2022**
		Página 06 de 08

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Propagación de Troyano Joker a través del aplicativo móvil CAMERA TRANSLATOR.		
Tipo de Ataque	Troyano	Abreviatura	Troyano
Medio 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 del troyano Joker a través del aplicativo gratuito denominado **CAMERA TRANSLATOR**, que se encuentra disponible en la plataforma de distribución digital de aplicaciones móviles Google Play Store para los dispositivos con sistema operativo Android.

2. El aplicativo **CAMERA TRANSLATOR**, permite la traducción instantánea de palabras, frases, oraciones u otra información de texto en diferentes idiomas, siendo fácil de descargar e instalar en el Smartphone (teléfono inteligente).

3. ***APLICATIVO MÓVIL***

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

- Versión : 6.36890.070
- Tamaño de archivo : 13 MB.
- Nombre del paquete : com.rinhyapp.ocrcameratitle.fasttranslator
- Actualizado : 20JUL2022
- Descargas : 10 mil+
- 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-JOKER: 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 para realizar ataques de denegación de servicio distribuido (DDoS) contra las víctimas objetivo.

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

- MD5 : 66a087f289fe87df874d31f5723a3d11
- SHA-1 : 51a757f4a249d638b1b1a3f9bffd0042a23c073a
- SHA-256 : 6d5b52f19dac70e7330f4dd56c1298dcdca6c78f03e938dc50c59027ca6b4734

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 **CAMERA TRANSLATOR**, 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

Adware 4, 5
Aplicativo 6, 7
Ciberespacio 4, 6
Google..... 5, 6, 7
Troyano.....6, 7