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, 29 de julio de 2022

N° 204-2022-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° 204	Fecha: 29-07-2022
		Página 04 de 07

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los ciberespías usan la extensión de Google Chrome para robar correos electrónicos sin ser detectados		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

FECHA DEL EVENTO:

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 29 de julio del 2022, se tomó conocimiento a través de la publicación realizada en la página web de **"BLEEPINGCOPUTER"**, sobre un grupo de amenazas respaldado por Corea del Norte rastreado como Kimsuky está usando una extensión de navegador malicioso para robar correos electrónicos de los usuarios de Google Chrome o Microsoft Edge que leen su correo web.

ANTECEDENTES:

- La extensión, denominada SHARPEXT por los investigadores de Volexity que detectaron esta campaña en septiembre, admite tres navegadores web basados en Chrome (Chrome, Edge y Whale) y puede robar correo de cuentas de Gmail y AOL.

DETALLES:

- Los atacantes instalan la extensión maliciosa después de comprometer el sistema de un objetivo utilizando un script VBS personalizado al reemplazar los archivos de 'Preferencias' y 'Preferencias seguras' con los descargados del servidor de comando y control del malware.
- Una vez que los nuevos archivos de preferencias se descargan en el dispositivo infectado, el navegador web carga automáticamente la extensión SHARPEXT. El malware inspecciona y filtra directamente los datos de la cuenta de correo web de la víctima mientras la navega.
- Desde su descubrimiento, la extensión ha evolucionado y actualmente se encuentra en la versión 3.0, basada en el sistema de control de versiones interno, esta última campaña se alinea con los ataques anteriores de Kimsuky, ya que también despliega SHARPEXT "en ataques dirigidos contra la política exterior, la energía nuclear y otras personas de interés estratégico" en los Estados Unidos, Europa y Corea del Sur.

- Al aprovechar la sesión ya iniciada del objetivo para robar correos electrónicos, el proveedor de correo electrónico de la víctima no detecta el ataque, lo que hace que la detección sea muy desafiante, si no imposible.
- Además, el flujo de trabajo de la extensión no activará ninguna alerta de actividad sospechosa en las cuentas de las víctimas, lo que garantiza que la actividad maliciosa no se descubra al consultar la página de estado de la cuenta de correo web en busca de alertas.

RECOMENDACIONES

- Utilizar contraseñas seguras, con más de ocho caracteres de longitud que contengan números, letras mayúsculas, minúsculas y caracteres especiales.
- Cambiar las preguntas y respuestas de seguridad elegidas en el modo de configuración de la cuenta de correo electrónico.
- Evitar hacer clic sobre enlaces o links de descargas de archivos adjuntos de correos electrónicos sospechosos.
- Revisar la actividad de tu cuenta para identificar un posible envío de correos a cuentas destinatarias que no reconoces.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/cyberspies-use-google-chrome-extension-to-steal-emails-undetected/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 204	Fecha: 29-07-2022
		Página 05 de 07

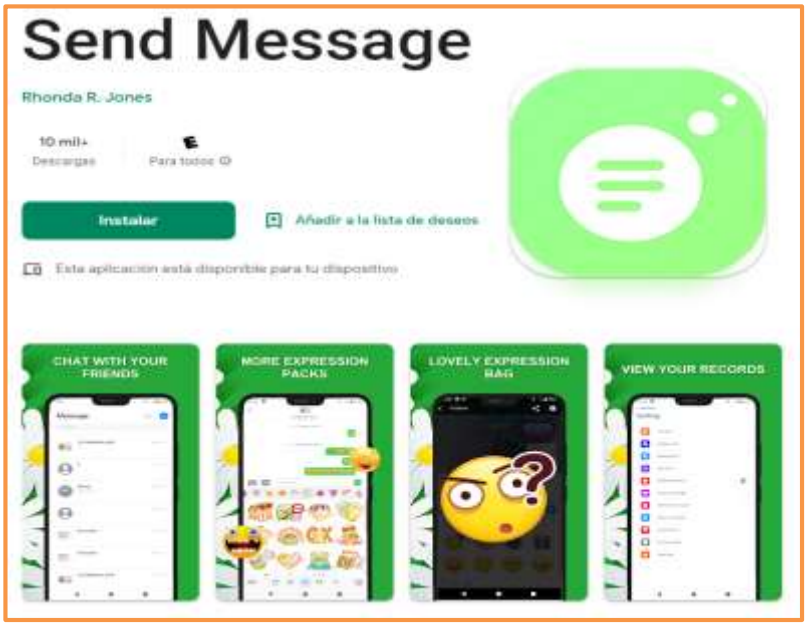
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Propagación de Troyano Joker a través del aplicativo móvil SEND MESSAGE.		
Tipo de Ataque	Troyano	Tipo de Ataque	Troyano
Medio de Propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de familia	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 **SEND MESSAGE**, 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 **SEND MESSAGE**, es una aplicación de mensajería y tiene la finalidad que el usuario realice comunicación digital (SMS, MMS) a través de la red de internet.

3. ***APLICATIVO MÓVIL***



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

- Versión : 1.40.0.32
- Tamaño de archivo : 5 MB.
- Nombre del paquete : hilandev.ttf.messages
- Actualizado : 16JUL2022
- 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

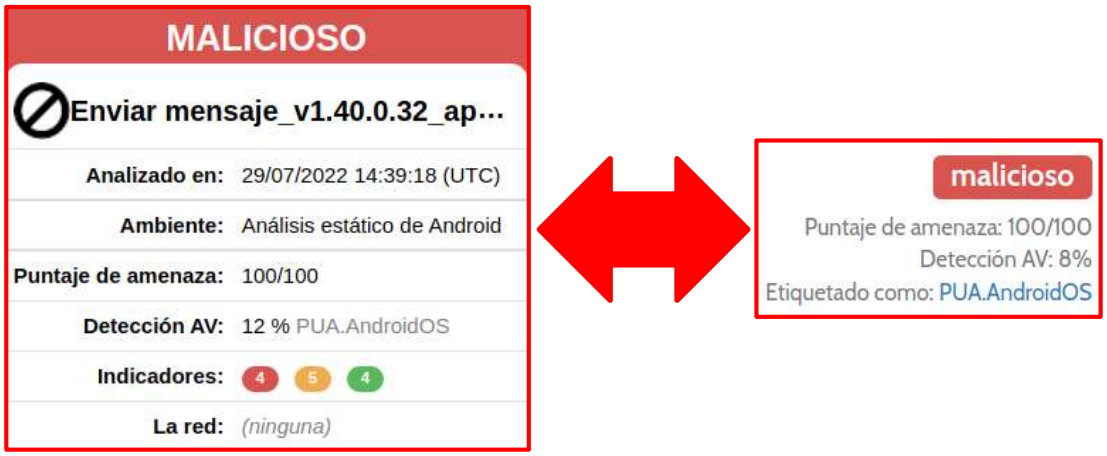
6. ***PROVEEDORES DE SEGURIDAD INFORMÁTICA ALERTAN COMO MALICIOSO AL APLICATIVO DE ANÁLISIS***.

TROJAN/ANDROID-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 DDoS contra las víctimas objetivo.

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

- MD5 : 96eb503694c64b90e310446341c6b245
- SHA-1 : 194c8895673ed10379bd3a270960ad4ff564033c
- SHA-256 : dbce490990479b81585b524d2360325ecfe781e5ae84e9dfb9c3037ce69b55c0

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 **SEND MESSAGE**, 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