	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 069	**Fecha: 21-03-2023**
		Página 11 de 29

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Aumento de sitios web fraudulentos de aplicaciones de mensajería instantánea como Telegram y Whatsapp para distribuir malware cryptocurrency clipper e infectar a los usuarios de Android y Windows.		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

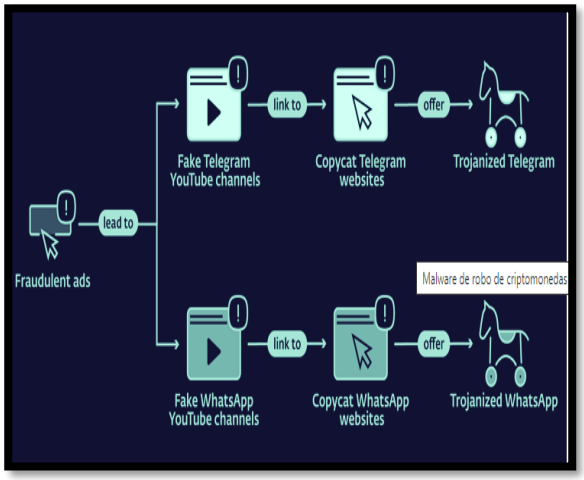
Descripción

ANTECEDENTES:

El 19 de marzo del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que en la actualidad se observa que hay un aumento exponencial de sitios web fraudulentos de aplicaciones de mensajería instantánea como Telegram y Whatsapp, con el objeto de distribuir versiones troyanas e infectar a los usuarios de Android y Windows con el malware cryptocurrency Clipper.

DETALLES:

El malware clipper se remonta a 2019 en Google Play Store, el desarrollo marca la primera vez que este malware basado en Android se integra en aplicaciones de mensajería instantánea.



Estas aplicaciones utilizan el reconocimiento óptico de caracteres (OCR) para reconocer el texto de las capturas de pantalla almacenadas en los dispositivos comprometidos, siendo una nueva capacidad del malware de Android.

La cadena de ataque comienza con usuarios desprevenidos que hacen clic en anuncios fraudulentos en los resultados de búsqueda de Google que conducen a cientos de canales de YouTube incompletos, que luego los dirigen a sitios web similares a Telegram y WhatsApp.

Un cuarto conjunto de cortadores de Android viene con capacidades para recopilar información del dispositivo y datos de Telegram, como mensajes y contactos. Los nombres de los paquetes APK de Android falsos se enumeran a continuación:

- org.telegram.messenger
- org.telegram.messenger.web2
- org.tgplus.messenger
- io.busniess.va.whatsapp
- com.whatsapp

RECOMENDACIONES:

- No ingresar a enlaces ni páginas web de dudosa procedencia.
- No instalar apps inseguras o de dudosa procedencia.
- Tener instalado un antivirus con protección antimalware.

Fuentes de información	▪ hxxps://thehackernews.com/2023/03/lookalike-telegram-and-whatsapp.html