I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Malware / Android

Nivel de riesgo: Alto

II. ALERTA

CherryBlos es el nombre de un malware dirigido a sistemas operativos Android. Este programa malicioso se clasifica como un stealer y un clipper. Funciona extrayendo o exfiltrando credenciales de monederos de criptomonedas y redirigiendo las transacciones de criptomonedas a monederos propiedad de los atacantes.

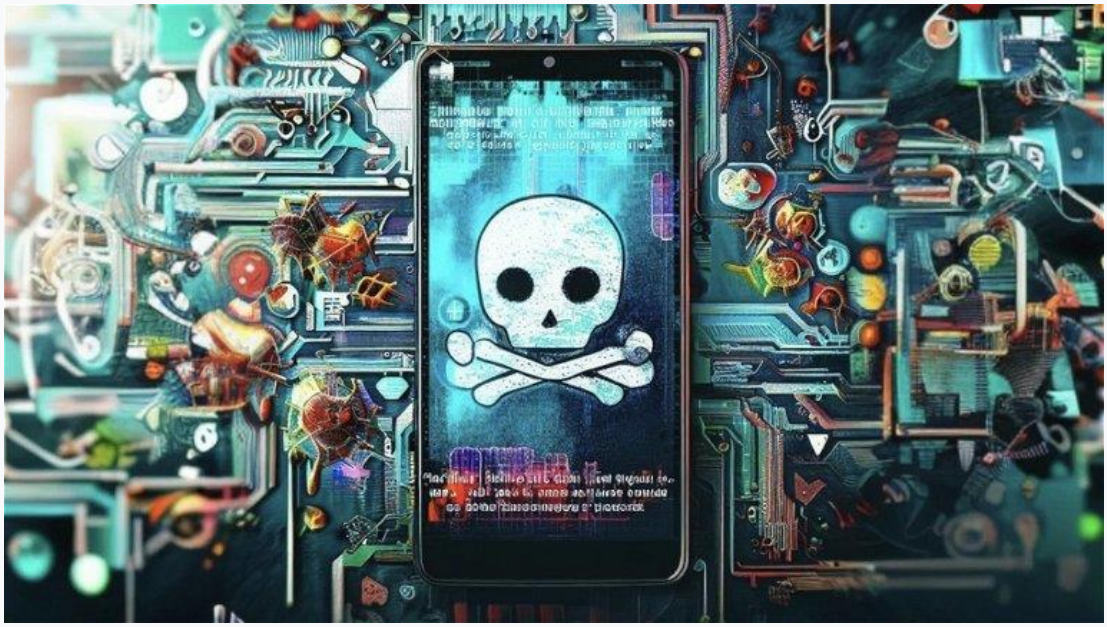

Figura 1.- Ataque CherryBlos – figura referencial

III. INTRODUCCIÓN

CherryBlos un malware con capacidad de utilizar técnicas de reconocimiento óptico de caracteres (OCR) para obtener las credenciales del usuario mientras las escribe en la pantalla del dispositivo.

En todo el mundo son millones los usuarios de dispositivos móviles con sistema operativo Android**,** ya sea de tablets o smartphones. Es por esta razón que los ciberdelincuentes los tienen en la mira y constantemente desarrollan nuevos programas maliciosos con los que intentan conseguir la mayor cantidad de datos sensibles. En esta ocasión, **CherryBlos** es el nuevo malware que acaba de surgir fuera de **Play Store** y te contamos cómo opera para robar tu información.

Investigadores de TrendMicro descubrieron el virus para móviles y notaron que emplea técnicas de reconocimiento óptico de caracteres para conseguir tus credenciales cuando las escribes en la pantalla. En general, son aplicativos disponibles en tiendas de terceros que promueven estafas para ganar dinero.

Es importante mencionar que los desarrolladores del malware usaron un software capaz de cifrar el código para evitar que eventuales análisis detecten la funcionalidad maliciosa. Las apps infectadas incorporan métodos que garantizan que el servicio permanezca activo a todas horas.

Este malware es capaz de reemplazar las direcciones utilizadas cuando se retiran activos de las wallets de criptoactivos. Para ello, lo primero que hace es solicitar la habilitación de permisos de accesibilidad que aparece como una ventana emergente.

Luego, puede actuar de diferentes formas. Una es a través del robo de credenciales a través de una interfaz falsa de usuario, en la cual los usuarios introducen sus contraseñas. Otra, es mediante la suplantación de la interfaz real de usuario para modificar la dirección a la cual se transfieren las criptodivisas, para que el usuario envíe ese dinero directamente a una cuenta de *Binance* controlada por los *hackers*.

IV. VECTOR DE ATAQUE:

Cuando uno abre una aplicación de compras o ventas, el malware se superpone sobre la pantalla simulando que es legítimo y, en el proceso de retiro de fondos, **CherryBlos** cambia la dirección del destino de la transferencia. El delito es posible gracias a los permisos de accesibilidad de Android, por lo que es normal que uno no se dé cuenta de ello y mucho menos piense en desinstalar la plataforma infectada.

Hasta el momento, son cuatro las apps que te pueden poner en riesgo si las has instalado en tu teléfono. Son estas:

- GPTalk.
- Happy Miner.
- Robot 999
- SynthNet.

Todas ellas fueron descubiertas fuera de Google Play. Sin embargo, también se han encontrado otras apps sospechosas tanto en el catálogo de la tienda de aplicaciones de Android, aunque **Google** asegura haberlas eliminado tras recibir el aviso de TrendMicro.

V. IMPACTO:

Aunque existen aplicaciones con funcionalidades interesantes fuera de Play Store de Google, lo cierto es que son espacios en los cuales no hay filtros de privacidad y seguridad en beneficio del usuario. Por lo tanto, si se procede con la instalación de un programa, es muy probable que la información personal quede a merced de terceros y se puede tardar mucho tiempo en darse cuenta de las modalidades de ciberataque.

En la mayoría de casos, existe la posibilidad de que suplanten la identidad, roben datos sensibles, se obtenga los accesos a redes sociales o cuentas bancarias e incluso difundan contenido malicioso mediante spam a los contactos.

Adicionalmente, Trend Micro alertó que CherryBlos es capaz de utilizar el OCR para reconocer contraseñas mnemotécnicas de acceso a una cuenta. Esto lo hace a través de la toma de una imagen de la pantalla y traducir lo que dice en ella a texto. Si bien muchas aplicaciones bancarias no permiten las capturas de pantallas, este *malware* elude estas restricciones gracias a la obtención de permisos de accesibilidad utilizados por personas no videntes o con problemas de visión.

VI. INDICADORES DE COMPROMISO

Es pertinente mencionar que CherryBlos está vinculado a otra campaña de malware apodada ***FakeTrade***. Esta operación consiste en aplicaciones fraudulentas para ganar dinero que prometen recompensas monetarias por realizar compras u otras tareas. Sin embargo, las víctimas son incapaces de cobrar sus ganancias.

Las aplicaciones de FakeTrade estaban alojadas en **Google Play Store**, pero las conocidas han sido retiradas en el momento de redactar este informe. Esta campaña se dirigía a usuarios de todo el mundo, con regiones predominantes como Malasia, México, Indonesia, Filipinas, Uganda y Vietnam.

Luego, las aplicaciones se promocionan en Telgram y TikTok entre inversores desprevenidos en criptomonedas.

VII. RECOMENDACIONES:

Se recomienda evitar recurrir a fuentes externas a Google Play a la hora de descargar las aplicaciones, así como asegurarse del tipo de permisos que se otorga a cada una de ellas.

Otras recomendaciones son:

- No descargar apps a través de webs sospechosas.
- No abrir enlaces con los que no estemos totalmente seguros.
- Sospechar de las descargas que nos soliciten datos personales.
- Descargar sólo las apps desde las webs y distribuidores oficiales.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- https://www.tripwire.com/state-of-security/cherryblos-malware-steals-cryptocurrency-your-photos-what-you-need-know
- https://www.lavanguardia.com/andro4all/android/cherryblos-el-peligroso-malware-android-que-lee-la-pantalla-de-tu-movil-para-robarte-contrasenas
- https://cso.computerworld.es/cibercrimen/cherryblos-el-malware-que-utiliza-el-reconocimiento-optico-de-caracteres-para-robar-credenciales
- https://www.audea.com/cherryblos-un-nuevo-malware/
- https://www.pcrisk.es/guias-de-desinfeccion/12149-cherryblos-malware-android
- https://larepublica.pe/tecnologia/smartphone/2023/07/31/cherryblos-asi-es-el-nuevo-malware-que-puede-infiltrarse-en-telefonos-y-espia-movimientos-1868308
- https://www.linkedin.com/posts/antoniojosetena_as%C3%AD-es-cherryblos-el-nuevo-malware-oculto-activity-7101240924780834816-84DS