Nro. Alerta:	EC-2022-082	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	28-julio-2022	**MALWARE DE ANDROID PARA SUSCRIBIR A SERVICIOS PREMIUM**	V 1.2

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Código malicioso
Nivel de riesgo: Medio

II. ALERTA.

El equipo de investigación de Microsoft 365 Defender compartió recientemente una publicación que explica cómo un malware de fraude telefónico puede suscribir a los usuarios a servicios premium sin que ellos lo descubran ni se den cuenta. El malware ha mejorado mucho a lo largo de los años y es capaz de ocultar todos sus rastros, vaciando la billetera virtual de los usuarios.

Figura 1.- lustraciones distintivas de un código malicioso **Fuente:** DRA

III. INTRODUCCIÓN.

En una nueva publicación, Microsoft 365 Defender explicó cómo funciona el malware Toll Fraud y cómo se puede usar para engañar a los usuarios para que se suscriban a servicios premium sin que ellos lo sepan. El malware tiene muchos comportamientos únicos. Y puede apuntar fácilmente a operadores específicos y cubrir sus huellas.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-082	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	28-julio-2022	**MALWARE DE ANDROID PARA SUSCRIBIR A SERVICIOS PREMIUM**	V 1.2

Microsoft ha compartido más detalles técnicos de este malware en un informe destacando que funciona sobre el Protocolo de aplicación inalámbrica (WAP), que permite esa suscripción a los contenidos de pago que se cargan en la factura telefónica.

Según Microsoft, el malware hace todos estos pasos automáticamente sin que el usuario se dé cuenta:

- Deshabilita la conexión Wifi o espera a que el usuario cambie a una red móvil.
- Posteriormente, navega hasta la página de suscripción y hace clic automáticamente en el botón para suscribirse interceptando la OTP, código de confirmación de la suscripción, y cancela las notificaciones de SMS.

Otro de los aspectos interesantes es que el malware usa 'NetworkCallbak' para monitorizar el estado de la red y obtener la variable 'networktype' para vincular el proceso a una red específica, lo que obliga al dispositivo a ignorar una conexión Wifi disponible y usar la del operador móvil.

El malware también puede interceptar y acceder a las contraseñas de un solo uso (OTP) que normalmente se envían para autenticar las compras. El malware también oculta todas las notificaciones y puede completar la información en nombre del usuario, ocultando por completo todos sus rastros. Los usuarios a menudo se enteran del malware demasiado tarde y tienen que pagar al final de su contrato o al final del mes.

La única forma en que el usuario puede evitar esto es deshabilitar manualmente los datos móviles. Si el operador de telefonía móvil de la víctima está en la lista de objetivos, el malware procede a buscar una lista de sitios web que brindan servicios Premium e intenta suscribirse a ellos automáticamente.

Si bien existen múltiples escenarios de suscripción, los usuarios normalmente hacen clic en un elemento HTML y luego envían un código de verificación al servidor. Microsoft señala que a veces se puede requerir una verificación adicional. Las muestras de malware de fraude telefónico que ha analizado la compañía también tienen métodos para conseguirlo.

Algunos operadores finalizan la suscripción solo después de verificar que el usuario lo autorizó a través de un código OTP entregado a través de SMS, HTTP o USSD (datos de servicio complementarios no estructurados).

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-082	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	28-julio-2022	**MALWARE DE ANDROID PARA SUSCRIBIR A SERVICIOS PREMIUM**	V 1.2

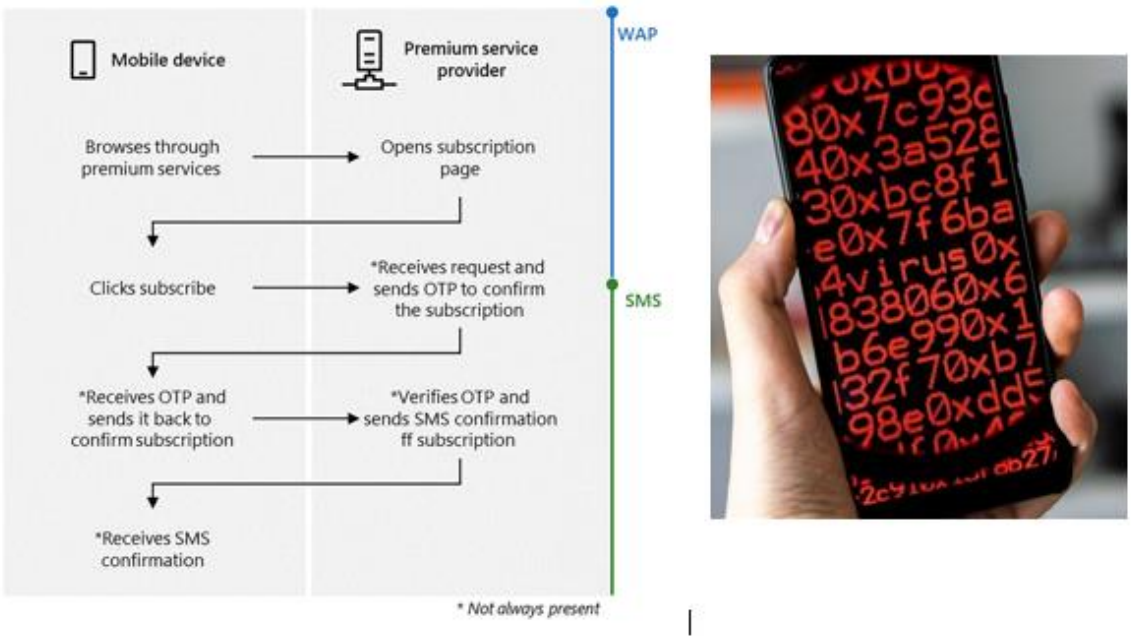

Figura 2.- Funcionamiento facturación WAP malware Android **Fuente:** DRA

IV. VECTOR DE ATAQUE

Red

V. IMPACTO.

El malware de fraude telefónico es una de las amenazas que más sigue proliferando en Android. Según advierten desde Microsoft, se está extendiendo una amenaza de seguridad en dispositivos con este sistema operativo que se basa en un malware telefónico. Los atacantes desactivan la red Wifi y suscriben al usuario a servicios Premium.

Para llevar a cabo esta amenaza, los ciberdelincuentes engañan a las víctimas para que llamen o envíen un SMS a un número Premium, es decir, que tienen una tarificación adicional y un mayor costo. Aquellos que caen en esta estafa, quedan suscritos a un servicio de pago y comienzan a recibir cargos en sus facturas telefónicas.

Nro. Alerta:	EC-2022-082	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	28-julio-2022	**MALWARE DE ANDROID PARA SUSCRIBIR A SERVICIOS PREMIUM**	V 1.2

Una de las características de este fraude es que no funciona cuando los usuarios están conectados a redes Wifi, por lo que obligan a los usuarios a conectarse a la red del operador móvil al que estén suscritos.

De este modo, cuando el usuario envía ese SMS o llama al teléfono Premium, el malware actúa de forma automática y, sin que el usuario sea consciente, deshabilita la red Wifi para que el usuario se conecte a la red móvil.

Una vez realizado este paso, inicia la página de suscripción a servicios Premium, interceptando los códigos de un solo uso OTP, suprimiendo las notificaciones y SMS que podrían alertar al usuario de que está siendo suscrito a estos servicios.

Para deshabilitar la red Wifi, el malware utiliza funciones de Android para monitorizar el estado de la red y evita que se conecte a la red Wifi, lo que obliga a que el dispositivo esté conectado a la red móvil.

En Android 9 (nivel de API 28) o inferior, esto es posible con un nivel de permiso de protección normal. Para un nivel de API más alto, existe la función 'requestNetwork' que se incluye en el permiso CHANGE_NETWORK_STATE, que también viene con un nivel de protección normal. Con este malware, los ciberdelincuentes consiguen hacerse con los datos de las víctimas, como la operadora a la que está suscrito o el país en el que se encuentra.
La técnica del fraude de telecomunicaciones estaba muy extendida en el pasado y ha recuperado protagonismo en los últimos años. También es un método popular en los países en desarrollo, ya que la mayoría de las personas a menudo solo usan servicios SIM mensuales o de prepago, lo que permite a los atacantes saquear una gran suma de dinero.

No hay señales de que este método se ralentice en el corto plazo, y se sospecha que está aquí para quedarse a largo plazo. Una vez que el malware se ha ejecutado correctamente, todo lo que tiene que hacer es seguir los pasos para recolectar dinero de usuarios no sospechosos.

El malware Toll Fraud también es el tipo más frecuente en Android desde 2017. El malware representó el 34,8% de las aplicaciones potencialmente dañinas (PHA) instaladas desde Google Play Store en el primer trimestre de 2022, ocupando el segundo lugar después del spyware.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-082	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	28-julio-2022	**MALWARE DE ANDROID PARA SUSCRIBIR A SERVICIOS PREMIUM**	V 1.2

VI. RECOMENDACIONES.

El EcuCERT de la ARCOTEL recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Disponer de un antivirus para el dispositivo móvil.
- Las posibilidades de que los usuarios generales se vean afectados son bajas, pero puede ocurrir cuando se accede a aplicaciones de terceros y desconocidas desde fuera de Google Play Store.
- Se recomienda que solo descargue archivos que pueda verificar. Siempre existen riesgos asociados con el uso de servicios de terceros y no recomendamos usarlos.
- Se recomienda que los usuarios eviten otorgar permisos de SMS, acceso de escucha de notificaciones o acceso de accesibilidad a las aplicaciones sin comprender exactamente por qué la aplicación lo necesita.
- Se recomienda a los usuarios que actualicen sus dispositivos tan pronto como dejen de esperar más actualizaciones. Se pueden descargar nuevos parches de seguridad periódicamente para protegerlo contra malware y otras acciones fraudulentas.

VII. DESCARGO DE RESPONSABILIDAD.

- La información en la presente alerta; se proporciona solo con fines informativos. El EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
  Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS.

- https://pocketnow.com/android-toll-fraud-malware
- https://www.xataka.com/basics/system-update-como-funciona-nuevo-malware-android-como-evitar-infectarte
- https://www.infobae.com/america/tecno/2022/07/04/cuidado-este-malware-suscribe-a-los-usuarios-de-android-a-servicios-premium/