Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°179	Fecha: 01-08-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Nuevo malware de Android roba registros de llamadas, ubicaciones y contactos		
Tipo de Ataque	Spyware	Abreviatura	Spyware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C04
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Según los informes de los investigadores de CYFIRMA, circula un nuevo malware para Android bajo la apariencia de una aplicación de chat falsa que se distribuye a través de WhatsApp, que en realidad son Phishing. Los atacantes buscan que la víctima descargue esa app, que es lo que contiene el malware, y comenzar a robar mensajes y datos.

Se descubre que este malware pertenece a APT Bahamut y tiene algunas huellas de tácticas utilizadas por DoNot APT.

Esta aplicación maliciosa de Android se denomina inicialmente "Coverlm" y se instala con el nombre "SafeChat" en los dispositivos Android.

La interfaz de usuario de esta aplicación parece engañosa y convencería a cualquier usuario de Android de que es una aplicación de chat legítima.

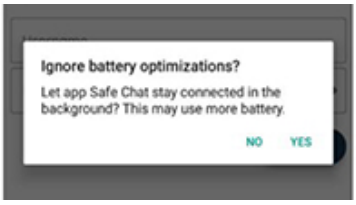
Sin embargo, una vez instalado, el malware explota bibliotecas de Android insospechadas para extraer y transmitir los datos a un servidor C&C (Command and Control).

2. DETALLES:

Como se indicó anteriormente, la aplicación parece realmente un programa de mensajería normal. Eso puede hacer que la víctima piense en todo momento que está usando un software legítimo, pero la realidad es que está exponiendo su privacidad y seguridad. La aplicación roba datos de aplicaciones de comunicación como Telegram, Signal, WhatsApp, Viber y Facebook Messenger.

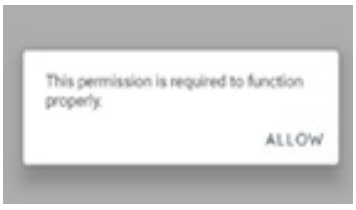
Un paso crítico en la infección es la adquisición de permisos para usar los Servicios de Accesibilidad, que posteriormente se abusan para otorgar automáticamente más permisos al spyware.

Estos permisos adicionales permiten que el spyware acceda a la lista de contactos de la víctima, SMS, registros de llamadas, almacenamiento de dispositivos externos y obtenga datos de ubicación GPS precisos del dispositivo infectado.



Uno de los permisos es "ignorar la optimización de la batería", el cual permite que la aplicación se ejecute en el backend y se comunique con el C&C sin problemas.

Al proporcionar el permiso, aparece la página de registro.



Continuando, la aplicación solicita otro permiso bajo la pregunta, "Este permiso es necesario para funcionar correctamente".

Este permiso aparece una y otra vez hasta que se habilita. Una vez que el usuario concede este permiso, la aplicación lleva al usuario al panel de configuración de accesibilidad.

La revisión del código en el archivo de manifiesto de Android de esta aplicación mostró que el actor de amenazas declaró muchos permisos para realizar comportamientos maliciosos con esta aplicación.

Además, la aplicación utilizó el puerto 2053 para comunicarse con el servidor C&C.

Los módulos de la aplicación representaron el uso del marco Ktor desarrollado con Kotlin, que se utilizó para comunicarse con los servidores de comando y control.

Anteriormente, DoNot APT implementó la biblioteca de actualización para la comunicación.

La aplicación es capaz de recopilar información como IMEI, ID del dispositivo, detalles de la SIM y ubicación.

Algunos de los permisos peligrosos incluyen:

PERMISOS	DESCRIPCIÓN
ACCES_FINE_LOCATION	Permite al atacante obtener ubicaciones precisas y rastrear el movimiento en vivo de los teléfonos móviles
LEER_CONTACTOS	Este permiso le permite al atacante leer y buscar contactos
LEER_ALMACENAMIENTO_EXTERNO	Este permiso permite al atacante acceder al almacenamiento de archivos del móvil
LEER_SMS	Esto permite que el atacante lea todos los SMS del dispositivo
LEER_LLAMADA_REGISTRO	Este permiso permite que el atacante lea los registros de llamadas
LEER_CONTACTOS	Este permiso le permite al atacante leer todos los contactos guardados en el dispositivo

"Otro fragmento del archivo de manifiesto de Android muestra que el actor de amenazas diseñó la aplicación para interactuar con otras aplicaciones de chat ya instaladas", explica CYFIRMA.

"La interacción se llevará a cabo mediante intenciones, el permiso OPEN_DOCUMENT_TREE seleccionará directorios específicos y accederá a las aplicaciones mencionadas en la intención".

Un módulo de exfiltración de datos dedicado transfiere información desde el dispositivo al servidor C2 del atacante a través del puerto 2053.

Los datos robados se cifran mediante otro módulo compatible con RSA, ECB y OAEPPadding. Al mismo tiempo, los atacantes también usan un certificado "letsencrypt" para evadir cualquier intento de interceptación de datos de la red en su contra.

3. RECOMENDACIONES:

- Instalar aplicaciones siempre desde fuentes oficiales o revisar muy bien el origen del software.
- Tener un buen antivirus instalado para detectar rápidamente posible software malicioso.

Fuente de Información:	• https://gbhackers.com/android-malware-whatsapp/#google_vignette • https://www.bleepingcomputer.com/news/security/hackers-steal-signal-whatsapp-user-data-with-fake-android-chat-app/ • https://www.redeszone.net/noticias/seguridad/robar-chats-whatsapp-comprobar/