Nro. Alerta:	AL-2024-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	14-nov-2024	**FakeCall – Malware Android**	Pág.: **1** of **16**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Troyano en Android – Phishing de voz (Vishing)

Nivel de riesgo: Media

II. ALERTA

Figura 1.- FakeCall – Malware Androide
Fuente: https://www.zimperium.com/blog/mishing-in-motion-uncovering-the-evolving-functionality-of-fakecall-malware/

III. INTRODUCCIÓN

El código malicioso (malware) llamado ***FakeCall***, emplea una técnica conocida como **Vishing** (Phishing de voz), así, a través del uso de llamadas telefónicas o mensajes de voz fraudulentos, los ciberdelincuentes engañan a las víctimas para que revelen información confidencial, como credenciales de inicio de sesión, números de tarjetas de crédito o datos bancarios. El Vishing es una forma de "**Mishing**", que se refiere a un término que abarca técnicas de **Phishing** dirigidas a dispositivos móviles que los ciberdelincuentes (atacantes) utilizan para explotar las características únicas de los dispositivos móviles, como llamadas de voz, mensajes de texto (SMS) y cámaras; FakeCall es un tipo de Vishing extremadamente sofisticado que aprovecha el malware, junto con llamadas fraudulentas.

IV. VECTOR DE ATAQUE:

FakeCall es un ataque de Vishing muy sofisticado que aprovecha el malware para tomar el control casi completo del dispositivo móvil, incluido la interceptación de llamadas entrantes y salientes. Las víctimas son engañadas para que llamen a números de teléfono fraudulentos controlados por el atacante e imiten la experiencia normal del usuario en el dispositivo.

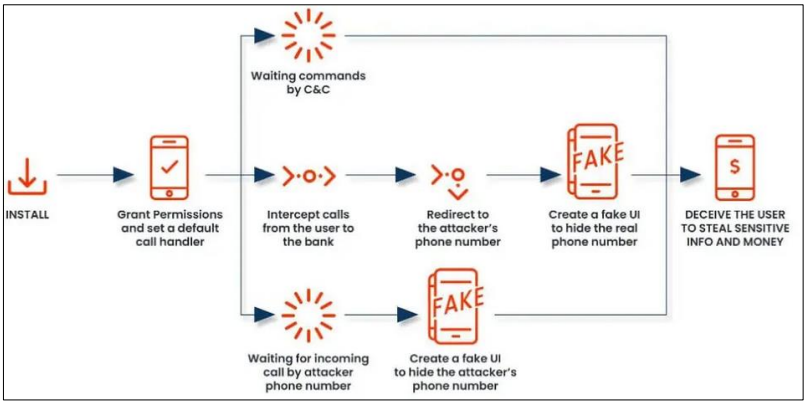

Figura 2.- Diagrama de ataque de FakeCall

Fuente: https://www.zimperium.com/blog/mishing-in-motion-uncovering-the-evolving-functionality-of-fakecall-malware/

El ataque comienza cuando las víctimas descargan un archivo APK en un dispositivo móvil Android mediante un ataque de Phishing, actuando como un dropper. La función principal del dropper es instalar la carga útil maliciosa real (la segunda etapa) en el dispositivo de la víctima.

El malware FakeCall está diseñado para comunicarse con un servidor de Comando y Control (C2), lo que le permite ejecutar varias acciones destinadas a engañar al usuario final. Esta interacción se produce a través de una serie de intercambios de mensajes entre el malware y el servidor C2.

Las variantes recién descubiertas de este malware están muy ofuscadas, pero siguen siendo consistentes con las características de las versiones anteriores.

El malware permite a los atacantes remotos tomar el control total de la IU del dispositivo de la víctima, lo que les permite simular interacciones del usuario, como clics, gestos y navegación entre aplicaciones. Esta capacidad permite al atacante manipular el dispositivo con precisión.

Al iniciarse, la aplicación solicita al usuario que la configure como el controlador de llamadas predeterminado. Una vez que se la designa como el controlador de llamadas predeterminado, la aplicación obtiene la capacidad de administrar todas las llamadas entrantes y salientes. Junto con OutgoingCallReceiver, captura la intención android.intent.action.NEW_OUTGOING_CALL y extrae el número de teléfono mediante getResultData(). Luego, la aplicación muestra una interfaz personalizada que imita la aplicación nativa com.android.dialer, integrando a la perfección su funcionalidad maliciosa.

V. IMPACTO:

Esta táctica se basa en realizar llamadas fraudulentas o enviar mensajes de voz para engañar a las víctimas y obtener datos confidenciales como números de tarjetas de crédito, credenciales de acceso y otros detalles bancarios.

Cuando un usuario de Android descarga e instala un archivo APK infectado, FakeCall solicita establecerse como la aplicación predeterminada de llamadas.

Con los permisos necesarios, el malware toma el control del dispositivo a través del servicio de Accesibilidad, registrando todas las llamadas entrantes y salientes.

Una vez instalado, este malware también es capaz de grabar la pantalla, tomar capturas, desbloquear el dispositivo y desactivar el bloqueo automático.

A diferencia de la mayoría de los malware móviles, FakeCall es especialmente difícil de detectar, ya que engaña a los usuarios con una interfaz falsa idéntica a la de las llamadas de Android, mostrando incluso el número real de contacto.

FakeCall se ha estado propagando a través de sitios web que imitan la apariencia de Google Play Store. Según Zimperium, existen al menos 13 aplicaciones utilizadas para distribuir el malware, aunque aún no se ha identificado a todas.

VI. INDICADORES DE COMPROMISO

Descargo de responsabilidad: Se recomienda investigar o verificar estos indicadores antes de tomar medidas, como bloquearlos.

Archivos maliciosos asociados

Nombre del archivo	Hash (SHA-256) / Info / Dominio / IP	Descripción
apk-dex.csv	473afda00aaf2bbff5d7c9aaa5933ba5f201b469b8546932c60119b1cf40471b ce154ff877691c22380cc0e67979f8d9f3ab59986b66c7b03bdab36805cfef8e 71073653f9992633dfbb38550cd196a7f201a8da6bea6ef88173ee2817ba023e fbdce3dd097f4a01814a14fa0e37c0e9a7618c0801adffb7c4dbd2e6927c220f 543734a2bb06d0433283a3b49d48f38b7ed500af82b47209a6087090bf1796cc fabdf6f305ed33293ffaac8651657426a6fa4a5bba79d95bf6b3ff481e9e6400 APK 099fce4dd0f15f591f59d9e39d68c669c7ec4e421c113d86605626318e4751b5 f886026ae6b194440eb135329bc9c6b56218560303207bd3ca45134cc6e66eeb d1b6ba52a08cc1eb508cb4abd236a27f5fa4d2299718485969b179cd70ffc072 c1d412b16811f0698dec4276f9ce6f92774e0dd8eb22ffcd386b0341312ef8a5 2629eaf1a4477638d44797d3eab9bba1b40aeb3dfd46462813923a3ca149ff28 baad3941f6e291aa8288ceb9f72c06c3d3fd802e89865777832f20bd5127e4fd 2bb50b25ecf6263514bf1922967cb93e4768f96485ee3d9f9bb6417c950cc1c7	apk and dexes added

Nombre del archivo	Hash (SHA-256) / Info / Dominio / IP	Descripción
	9d39ace2806389638878646a90af23c716ad9f2c6d142f 91f321b2324cbc2e6e 5daac96d677763c6e4b802501d56251960cc38f2e74fe 81e8cf921672aa57c3b	
package-names.csv	com.qaz123789.serviceone com.sbbqcfnvd.skgkkvba com.securegroup.assistant com.seplatmsm.skfplzbh eugmx.xjrhry.eroreqxo gqcvctl.msthh.swxgkyv ouyudz.wqrecg.blxal plnfexcq.fehlwuggm.kyxvb xkeqoi.iochvm.vmyab	package names added
urls-ips.csv	47.242.149.4 47.242.20.245 47.242.38.176 47.245.63.185 47.91.14.5 8.209.241.108 8.209.250.15 8.210.198.162 8.218.68.96 allcallpush01.com allcallpush02.com allcallpush09.com allcallpush12.com allcallpush15.com chaowen000.com chaowen006.com chaowen105.com ending052.com tewen006.com tewen007.com vipyaooba.com wending015.com	urls-ips added

Tabla 1.- IoC de Malware FakeCall
Fuente: https://github.com/Zimperium/IOC/blob/master/2024-10-FakeCall/urls-ips.csv

IOCs de red:

- Direcciones IP sospechosas:
  - 185.38.13.159
  - 185.38.13.160
  - 185.38.13.161
- Dominios sospechosos:
  - fakecall[.]ru
  - callfake[.]ru
  - otherfake[.]ru
- Puertos sospechosos:
  - 443 (HTTPS)
  - 80 (HTTP)

IOCs de sistema de archivos:

- Archivos sospechosos:
  - fakecall.exe
  - callfake.exe
  - otherfake.exe
- Rutas de archivo sospechosas:
  - %AppData%\Fakecall
  - %LocalAppData%\Callfake
  - %Temp%\Otherfake
- Claves de registro sospechosas:

- HKCU\Software\Fakecall
- HKLM\Software\Callfake

IOCs de comportamiento:

- Actividad sospechosa:
  - Conexiones a servidores de comando y control (C2)
  - Descarga de archivos maliciosos
  - Ejecución de procesos sospechosos
- Cambios en la configuración del sistema:
  - Modificación de la configuración de red
  - Cambios en la política de seguridad

IOCs de tráfico:

- Patrones de tráfico sospechosos:
  - Tráfico HTTPS hacia direcciones IP sospechosas
  - Tráfico DNS hacia dominios sospechosos
- Tamaño y frecuencia de los paquetes:
  - Paquetes pequeños y frecuentes hacia servidores de C2

IOCs de memoria:

- Procesos en memoria sospechosos:
  - fakecall.exe
  - callfake.exe
- Módulos en memoria sospechosos:

- fakecall.dll
- callfake.dll

El mapeo de la actividad maliciosa conforme a la matriz de MITRE ATT&CK, se presenta a continuación:

Táctica	ID	Nombre	Descripción
Initial Access	T1660	Phishing	Los atacantes pueden enviar contenido malicioso a los usuarios para obtener acceso a sus dispositivos móviles. Todas las formas de phishing son ingeniería social que se transmite electrónicamente. Los atacantes pueden realizar tanto phishing no dirigido, como campañas de spam de malware masivo, como phishing más dirigido a un individuo, empresa o industria específicos, conocido como "spearphishing". Llamadas telefónicas: los atacantes pueden llamar a las víctimas (conocido como "vishing") para persuadirlas de que realicen una acción, como proporcionar credenciales de inicio de sesión o navegar a un sitio web malicioso. Esto también podría usarse como técnica para realizar el acceso inicial en un dispositivo móvil, pero luego pasar a una computadora/otra red haciendo que la víctima realice una acción en una computadora de escritorio.
Persistence	T1398	Boot or Logon Initialization Scripts	Las aplicaciones maliciosas pueden abusar del método API startForeground( ) para continuar ejecutándose en primer plano, mientras presentan una notificación al usuario que simula ser una aplicación genuina. Esto permitiría un acceso sin obstáculos a los sensores del dispositivo, suponiendo que se haya otorgado previamente el permiso.
	T1541	Foreground Persistence	Los atacantes pueden abusar del método API startForeground( ) de Android para mantener un acceso continuo a los sensores. A partir de Android 9, las aplicaciones inactivas que se ejecutan en segundo plano ya no tienen acceso a los sensores del dispositivo, como la cámara, el micrófono y el giroscopio. Las aplicaciones pueden conservar el acceso a los sensores si se

Táctica	ID	Nombre	Descripción
			ejecutan en primer plano, mediante el método API startForeground( ) de Android. Esto informa al sistema de que el usuario está interactuando activamente con la aplicación y no debe cerrarse. El único requisito para iniciar un servicio en primer plano es mostrar una notificación persistente al usuario.
Defense Evasion	T1406.002	Obfuscated Files or Information: Software Packing	Los atacantes pueden realizar el empaquetado de software para ocultar su código. El empaquetado de software es un método de compresión o cifrado de un ejecutable. El empaquetado de un ejecutable cambia la firma del archivo en un intento de evitar la detección basada en firmas. La mayoría de las técnicas de descompresión descomprimen el código ejecutable en la memoria. Las utilidades que se utilizan para realizar el empaquetado de software se denominan empaquetadores. Un ejemplo de empaquetador es FTT. Hay disponible una lista más completa de empaquetadores conocidos, pero los atacantes pueden crear sus propias técnicas de empaquetado que no dejen los mismos artefactos que los empaquetadores conocidos para evadir las defensas.
	T1407	Download New Code at Runtime	Los atacantes pueden descargar y ejecutar código dinámico no incluido en el paquete original de la aplicación después de la instalación. Esta técnica se utiliza principalmente para evadir los controles de análisis estático y los análisis previos a la publicación en las tiendas de aplicaciones oficiales. En algunos casos, las técnicas de análisis dinámico o de comportamiento más avanzadas podrían detectar este comportamiento. Sin embargo, junto con las técnicas de protección de ejecución, la detección de código malicioso descargado después de la instalación podría resultar difícil.
	T1575	Native API	Los atacantes pueden usar el kit de desarrollo nativo (NDK) de Android para escribir funciones nativas que puedan ejecutar archivos binarios o funciones. Al igual

Táctica	ID	Nombre	Descripción
			que las llamadas del sistema en un sistema operativo de escritorio tradicional, el código nativo logra la ejecución en un nivel inferior al de las llamadas normales del SDK de Android.
	T1628.001	Hide Artifacts: Suppress Application Icon	Una aplicación maliciosa podría impedir que su icono se muestre al usuario en el iniciador de aplicaciones. Esto oculta el hecho de que está instalada y puede dificultar al usuario la desinstalación de la aplicación. Ocultar el icono de la aplicación mediante programación no requiere ningún permiso especial.
Credential Access	T1417.002	Input Capture: GUI Input Capture	Los atacantes pueden imitar los componentes de la interfaz gráfica de usuario de los sistemas operativos comunes para solicitar a los usuarios información confidencial con un mensaje aparentemente legítimo. El sistema operativo y las aplicaciones instaladas suelen tener necesidades legítimas de solicitar al usuario información confidencial, como credenciales de cuenta, información de cuenta bancaria o información de identificación personal (PII). En comparación con las PC tradicionales, el tamaño de pantalla limitado de los dispositivos móviles puede perjudicar la capacidad de proporcionar a los usuarios información contextual, lo que hace que estos sean más susceptibles al uso de esta técnica.
Discovery	T1420	File and Directory Discovery	Los atacantes pueden enumerar archivos y directorios o buscar en ubicaciones específicas de dispositivos la información deseada dentro de un sistema de archivos. Los atacantes pueden usar la información de File and Directory Discovery durante el descubrimiento automático para dar forma a los comportamientos posteriores, incluida la decisión de si el adversario debe infectar completamente el objetivo y/o intentar acciones específicas.
	T1430	Location Tracking	Los atacantes pueden rastrear la ubicación física de un dispositivo mediante el uso de API estándar del sistema

Táctica	ID	Nombre	Descripción
			operativo a través de aplicaciones maliciosas o explotadas en el dispositivo comprometido. En Android, las aplicaciones que tienen los permisos ACCESS_COAURSE_LOCATION o ACCESS_FINE_LOCATION brindan acceso a la ubicación física del dispositivo.
Collection	T1429	Audio Capture	Los atacantes pueden capturar audio para recopilar información aprovechando las API estándar del sistema operativo de un dispositivo móvil. Algunos ejemplos de información de audio a la que pueden apuntar los atacantes incluyen conversaciones del usuario, el entorno, llamadas telefónicas u otra información confidencial.
	T1616	Call Control	Los atacantes pueden realizar, reenviar o bloquear llamadas telefónicas sin autorización del usuario. Esto podría utilizarse para objetivos del adversario, como vigilancia de audio, bloqueo o reenvío de llamadas del propietario del dispositivo o comunicación C2.
	T1417.002	Input Capture: GUI Input Capture	Los atacantes pueden imitar los componentes de la interfaz gráfica de usuario de los sistemas operativos comunes para solicitar a los usuarios información confidencial con un mensaje aparentemente legítimo. El sistema operativo y las aplicaciones instaladas suelen tener necesidades legítimas de solicitar al usuario información confidencial, como credenciales de cuenta, información de cuenta bancaria o información de identificación personal (PII).
	T1430	Location Tracking	Los atacantes pueden rastrear la ubicación física de un dispositivo mediante el uso de API estándar del sistema operativo a través de aplicaciones maliciosas o explotadas en el dispositivo comprometido. En Android, las aplicaciones que tienen los permisos ACCESS_COAURSE_LOCATION o ACCESS_FINE_LOCATION brindan acceso a la ubicación física del dispositivo. En Android 10 y versiones posteriores, la declaración del permiso

Táctica	ID	Nombre	Descripción
			ACCESS_BACKGROUND_LOCATION en el manifiesto de una aplicación permitirá que las aplicaciones soliciten acceso a la ubicación incluso cuando la aplicación se esté ejecutando en segundo plano. Algunos atacantes han utilizado la integración de los servicios de mapas de Baidu para recuperar la ubicación geográfica una vez que se obtuvieron los permisos de acceso a la ubicación.
	T1636.002	Protected User Data: Call Log	Los atacantes pueden utilizar las API estándar del sistema operativo para recopilar datos del registro de llamadas. En Android, esto se puede lograr mediante el proveedor de contenido del registro de llamadas. iOS no proporciona ninguna API estándar para acceder al registro de llamadas. Si el dispositivo ha sido liberado o rooteado, un adversario puede acceder al registro de llamadas sin el conocimiento o la aprobación del usuario.
	T1636.003	Protected User Data: Contact List	Los atacantes pueden utilizar las API estándar del sistema operativo para recopilar datos de la lista de contactos. En Android, esto se puede lograr mediante el proveedor de contenido de contactos. En iOS, esto se puede lograr mediante el marco de contactos. Si el dispositivo ha sido liberado o rooteado, un adversario puede acceder a la lista de contactos sin el conocimiento o la aprobación del usuario.
	T1636.004	Protected User Data: SMS Messages	Los atacantes pueden utilizar las API estándar del sistema operativo para recopilar mensajes SMS. En Android, esto se puede lograr mediante el proveedor de contenido SMS. iOS no ofrece ninguna API estándar para acceder a los mensajes SMS. Si el dispositivo ha sido liberado o rooteado, un adversario puede acceder a los mensajes SMS sin el conocimiento o la aprobación del usuario
	T1513	Screen Capture	Los atacantes pueden usar la captura de pantalla para recopilar información adicional sobre un dispositivo objetivo, como aplicaciones que se ejecutan en primer plano, datos de usuario, credenciales u otra información

Táctica	ID	Nombre	Descripción
			confidencial. Las aplicaciones que se ejecutan en segundo plano pueden capturar capturas de pantalla o videos de otra aplicación que se ejecuta en primer plano mediante el MediaProjectionManager de Android (generalmente requiere que el usuario del dispositivo otorgue el consentimiento).
	T1512	Video Capture	Un adversario puede aprovechar las cámaras de un dispositivo para recopilar información mediante la captura de grabaciones de vídeo. También se pueden capturar imágenes, posiblemente en intervalos específicos, en lugar de archivos de vídeo. El malware o los scripts pueden interactuar con las cámaras del dispositivo a través de una API disponible proporcionada por el sistema operativo. Los archivos de vídeo o imagen se pueden escribir en el disco y exfiltrarse más tarde. Esta técnica difiere de la captura de pantalla debido al uso de las cámaras del dispositivo para la grabación de vídeo en lugar de capturar la pantalla de la víctima.
Command and Control	T1616	Call Control	Los atacantes pueden realizar, reenviar o bloquear llamadas telefónicas sin autorización del usuario. Esto podría utilizarse para objetivos del adversario, como vigilancia de audio, bloqueo o reenvío de llamadas del propietario del dispositivo o comunicación C2.
Exfiltration	T1646	Exfiltration Over C2 Channel	Los atacantes pueden robar datos filtrándolos a través de un canal de comando y control existente. Los datos robados se codifican en el canal de comunicaciones normal utilizando el mismo protocolo que las comunicaciones de comando y control.
Impact	T1616	Call Control	Los atacantes pueden realizar, reenviar o bloquear llamadas telefónicas sin autorización del usuario. Esto podría utilizarse para objetivos del adversario, como vigilancia de audio, bloqueo o reenvío de llamadas del propietario del dispositivo o comunicación C2.
	T1582	SMS Control	Los atacantes pueden eliminar, alterar o enviar mensajes SMS sin la autorización del usuario. Esto podría usarse

Táctica	ID	Nombre	Descripción
			para ocultar mensajes SMS de C2, propagar malware o diversos efectos externos.
	T1516	Input Injection	Una aplicación maliciosa puede inyectar información en la interfaz de usuario para imitar la interacción del usuario mediante el abuso de las API de accesibilidad de Android.

Tabla 2.- Técnicas MITRE ATT&CK.

VII. RECOMENDACIONES:

Para protegerse de FakeCall siga las siguientes recomendaciones:

- Evitar descargar aplicaciones fuera de Google Play Store y otras fuentes no verificadas.
- Prestar atención a los permisos que solicitan las aplicaciones y si realmente los necesitan. Denegar permisos, sobre todo aquellos potencialmente peligrosos o que invadan la privacidad, como el acceso a micrófono, salida de audio, llamadas, mensajes de texto, accesibilidad, entre otros,
- Reiniciar el teléfono semanalmente y realice escaneos con herramientas antivirus, así se podría prevenir infecciones de este tipo de troyanos móviles.
- Mantener actualizado su sistema operativo y software.
- Utilizar un antivirus y un firewall confiables.
- Evitar hacer clic en enlaces sospechosos o descargar archivos de fuentes desconocidas.
- Utilizar contraseñas seguras y únicas para cada cuenta.

- Verificar la autenticidad de los mensajes y llamadas que recibe.
- Verificar la identidad del llamante antes de responder a una llamada.
- No proporcionar información personal o financiera a desconocidos.
- Utilizar un bloqueador de llamadas y mensajes spam.
- Mantener actualizada su lista de contactos y elimine números sospechosos.

Para una institución, empresa u organización considere las siguientes recomendaciones:

- Implemente políticas de seguridad de la información para los empleados.
- Realice capacitaciones sobre Ciberseguridad
- Utilice soluciones de seguridad avanzadas (EDR, IPS, otras).
- Monitoree el tráfico de red y los logs de seguridad.
- Realice copias de seguridad regulares.

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:

- **Kaspersky (2024).** *Fakecalls: un troyano que habla* https://www.kaspersky.es/blog/fakecalls-banking-trojan/27063/
- **Zimperium (2024).** *Mishing in Motion: Uncovering the Evolving Functionality of FakeCall Malware* https://www.zimperium.com/blog/mishing-in-motion-uncovering-the-evolving-functionality-of-fakecall-malware/
- **Github (2024).** *2024-10-FakeCall/urls-ips.csv.* https://github.com/Zimperium/IOC/blob/master/2024-10-FakeCall/urls-ips.csv
- **MITRE ATT&CK (2024).** *Techniques* https://attack.mitre.org/techniques