I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: GravityRAT es un software espía para Android, considerado como código malicioso, que roba archivos de la copia de seguridad de WhatsApp y tiene la capacidad de recibir comandos para borrar archivos.

Nivel de riesgo: Alto

II. ALERTA

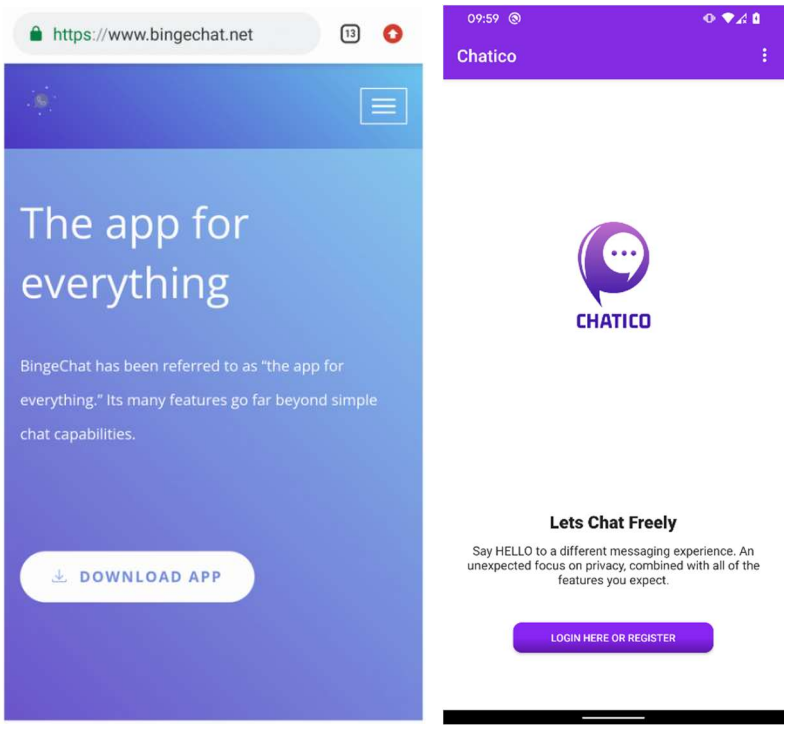

Figura 1.- Sitio Web que distribuye la aplicación de mensajería maliciosa BingeChat. Inicio de sesión en la aplicación CHATICO. Fuente: https://www.welivesecurity.com/la-es/2023/06/16/gravityrat-malware-roba-copias-seguridad-whatsapp/

Se descubrió una nueva versión para Android del software espía GravityRAT que se distribuye como versiones troyanizadas de la aplicación legítima de código abierto OMEMO Instant Messenger para Android.

La aplicación BingeChat troyanizada está disponible para su descarga desde un sitio Web que la presenta como un servicio gratuito de mensajería y uso compartido de archivos.

La versión de GravityRAT ha sido mejorada con dos nuevas capacidades:

- Puede recibir comandos para eliminar archivos
- extraer archivos de la copia de seguridad de WhatsApp.

III. INTRODUCCIÓN

El malware **GravityRAT** tiene características similares al de la aplicación OMEMO Instant Messenger (IM) que es de código abierto y tiene la marca BingeCHAT; así OMEMO IM es una reconstrucción del cliente para Android Conversations.

Lukas Stefanko, del equipo de investigación de ESET señala en su publicación en el portal de welivesecurity, que se identificó una versión actualizada para Android de GravityRAT, considerado como un código malicioso de tipo troyano de acceso remoto que se distribuye como una aplicación de mensajería denominados como BingeChat y Chatico.

El malware GravityRAT es una herramienta de acceso remoto que tiene sus antecedentes del año 2015 y que fue usado en ataques dirigidos en India, así existen versiones disponibles de este malware para Windows, Android y MacOS.

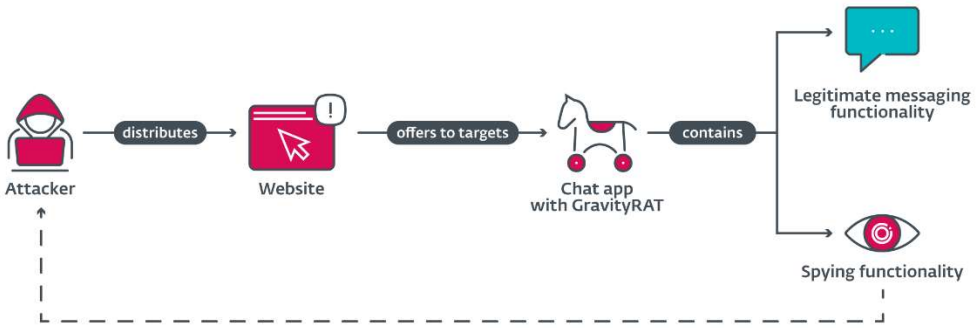

Figura 2.- Mecanismo de distribución de GravityRAT.
Fuente: https://www.welivesecurity.com/la-es/2023/06/16/gravityrat-malware-roba-copias-seguridad-whatsapp/

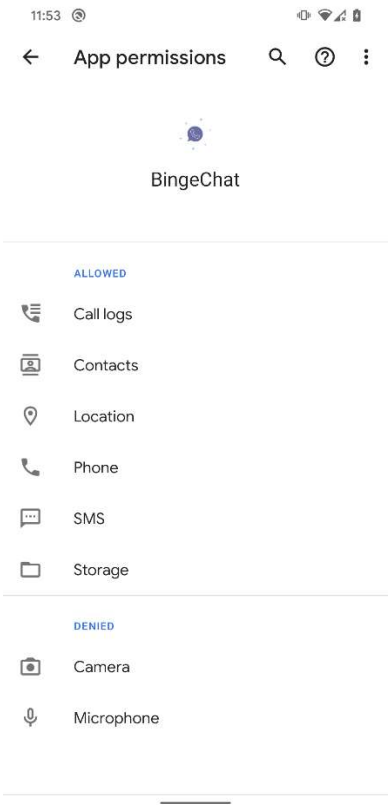

Figura 3.- Permisos que solicita BingeCHAT.
Fuente: https://www.welivesecurity.com/la-es/2023/06/16/gravityrat-malware-roba-copias-seguridad-whatsapp/

Después de iniciarse, la aplicación solicita al usuario que habilite todos los permisos necesarios para funcionar correctamente, como se muestra en la Figura 3. Excepto por el permiso para leer los registros de llamadas, los otros permisos solicitados son típicos de cualquier aplicación de mensajería, por lo que es posible que el usuario del dispositivo no se alarme cuando la aplicación los solicite.

IV. VECTOR DE ATAQUE:

Manipulación de datos, enlaces en aplicaciones de mensajería para teléfonos Android.

El grupo detrás de este malware utiliza el código de la app de mensajería instantánea legítima llamada OMEMO para proporcionar la funcionalidad de chat en las aplicaciones de mensajería maliciosas BingeChat y Chatico.

V. IMPACTO:

GravityRAT elimina archivos con extensiones particulares del dispositivo y elimina todos los registros de llamadas de los usuarios y la lista de contactos.

Según la telemetría de ESET, un usuario de india fue atacado con la versión actualizada de este RAT utilizando como señuelo la app Chatico y la campaña comparte características con otras campañas previamente documentadas.

Como parte de la funcionalidad legítima, la aplicación ofrece opciones para crear una cuenta e iniciar sesión. Antes de que el usuario inicie sesión en la aplicación, GravityRAT comienza a interactuar con su servidor C&C, filtrando datos del usuario del dispositivo y esperando que se ejecuten los comandos. GravityRAT es capaz de exfiltrar:

- Registros de llamadas
- Lista de contactos
- Mensajes SMS

- Archivos con extensiones específicas: jpg, jpeg, log, png, PNG, jpg, jpeg, txt, pdf, xml, doc, xls, xlsx, ppt, pptx, docx, opus, crypt14, crypt12, crypt13, crypt18, crypt32
- ubicación del dispositivo
- Información básica del dispositivo

Los datos que se exfiltrarán se almacenan en archivos de texto en medios externos, luego se envían al servidor de C&C y finalmente se eliminan.

VI. INDICADORES DE COMPROMISO

- **Archivos:**

SHA-1	Nombre del archivo	Nombre de detección de ESET	Descripción
2B448233E6C9C4594E385E799CEA9EE8C06923BD	eu.siacs.bingechat	Android/Spy.Gravity.A	GravityRAT impersonating BingeChat app.
25715A41250D4B9933E3599881CE020DE7FA6DC3	eu.siacs.bingechat	Android/Spy.Gravity.A	GravityRAT impersonating BingeChat app.
1E03CD512CD75DE896E034289CB2F5A529E4D344	eu.siacs.chatico	Android/Spy.Gravity.A	GravityRAT impersonating Chatico app.

- **Red:**

Dirección IP	Dominio	Proveedor de alojamiento	Visto por primera vez	Detalles
75.2.37[.]224	jre.jdklibraries[.]com	Amazon.com, Inc.	2022-11-16	Chatico C&C server.

Dirección IP	Dominio	Proveedor de alojamiento	Visto por primera vez	Detalles
104.21.12[.]211	cld.androidadbserver[.]com adb.androidadbserver[.]com	Cloudflare, Inc.	2023-03-16	BingeChat C&C servers.
104.21.24[.]109	dev.jdklibraries[.]com	Cloudflare, Inc.	N/A	Chatico C&C server.
104.21.41[.]147	chatico.co[.]uk	Cloudflare, Inc.	2021-11-19	Chatico distribution website.
172.67.196[.]90	dev.androidadbserver[.]com ping.androidadbserver[.]com	Cloudflare, Inc.	2022-11-16	BingeChat C&C servers.
172.67.203[.]168	bingechat[.]net	Cloudflare, Inc.	2022-08-18	BingeChat distribution website

- **Rutas**

  Los datos para exfiltración son presentados en las siguientes rutas:

  /storage/emulated/0/Android/ebc/oww.log
  /storage/emulated/0/Android/ebc/obb.log
  /storage/emulated/0/bc/ms.log
  /storage/emulated/0/bc/cl.log
  /storage/emulated/0/bc/cdcl.log
  /storage/emulated/0/bc/cdms.log
  /storage/emulated/0/bc/cs.log
  /storage/emulated/0/bc/location.log

- **Virus Total señala:**

SHA-256:
caf0a39318cfc1e65eae773a28de62ce08b7cf1b9d4264e843576165411e2a84
Archivo: BingeChat.apk
Tamaño: 34.56 MB

Propiedades:

MD5	c24cd0dfeb7ead78cc963802f8dfcfb9
SHA-1	2b448233e6c9c4594e385e799cea9ee8c06923bd
SHA-256	caf0a39318cfc1e65eae773a28de62ce08b7cf1b9d4264e843576165411e2a84
Vhash	3968ab2ad3c32c58bd25278f8f6de0c7
SSDEEP	786432:8OlxsCM0rkGrNcme9cHRFJOUbXV+NmcDRGgqvjFp37L+:8OsCHkGhHVUscD4g2jFp37a
TLSH	T12B8723D7B3D8E81AC5339077C96A11A635DB4CA59E53CB532918BB1C38F75E08E09BC8
Permhash	a2a348848f18a7db18d5eae98b2033629d4df4a6e78f459f2208e78d4fba19b9
File type	Android executable mobile android apk
Magic	Zip archive data, at least v0.0 to extract, compression method=store
TrID	Android Package (63.7%) Java Archive (26.4%) ZIP compressed archive (7.8%) PrintFox/Pagefox bitmap (640x800) (1.9%)
File size	34.56 MB (36233841 bytes)

Fuente:
https://www.virustotal.com/gui/file/caf0a39318cfc1e65eae773a28de62ce08b7cf1b9d4264e843576165411e2a84/details

SHA-256:
4ebdfa738ef74945f6165e337050889dfa0aad61115b738672bbeda648a59dab
Popular threat label: trojan.gravity/gravityrat
Tamaño: 34.49 MB

Propiedades:

MD5	3f827039964a09f1179f66d6b2f9fe31
SHA-1	25715a41250d4b9933e3599881ce020de7fa6dc3
SHA-256	4ebdfa738ef74945f6165e337050889dfa0aad61115b738672bbeda648a59dab
Vhash	d7a4edf6dcca6828e4ea5d9768f275c0
SSDEEP	786432:8OlxsCM0rkGrNTbmV9DJOK0iJzbXV+i7LZmcDRGgqvjFpe:8OsCHkYaf0MUi7scD4g2jFpe
TLSH	T1E98723D7B3D8E81AC4339077C97A12A6759B4C659E53CB572818BB1C38F75E08E09BC8
Permhash	a2a348848f18a7db18d5eae98b2033629d4df4a6e78f459f2208e78d4fba19b9
File type	Android executable mobile android apk
Magic	Zip archive data, at least v0.0 to extract, compression method=store
TrID	Android Package (63.7%) Java Archive (26.4%) ZIP compressed archive (7.8%) PrintFox/Pagefox bitmap (640x800) (1.9%)

File size	34.49 MB (36170184 bytes)

Fuente:
https://www.virustotal.com/gui/file/4ebdfa738ef74945f6165e337050889dfa0aad61115b738672bbeda648a59dab/details

SHA-256:
e9edf3dce24f4e5057f56a3a68c8f4bc3528158e4431be64c031b7a738b312ab
Archivo:
e9edf3dce24f4e5057f56a3a68c8f4bc3528158e4431be64c031b7a738b312ab.bin
Tamaño: 17.33 MB
Popular threat label: trojan.gravity/gravityrat

Propiedades:

MD5	dc00d22c2c04c49a40cb7cbd81080a7a
SHA-1	1e03cd512cd75de896e034289cb2f5a529e4d344
SHA-256	e9edf3dce24f4e5057f56a3a68c8f4bc3528158e4431be64c031b7a738b312ab
Vhash	9e5f8ad782425d431433347a6ac2f2e6
SSDEEP	393216:BxQkK+vfI9t6BaxoPdZPT9pm5IiZ54H9vt9qL3Ax4Nf+x7lLpU1:BxQB8BauPdZPpab4Zt9qjAxjx5pU1
TLSH	T1F507129BF7CDB62AC137803786B2517675E98C6AAE52C6132018F22C78F75E48745FC8
Permhash	57050f1ca32d507e1d16fd765325bba479a15cb9b974edda83b8214a9fb565b1
File type	Android executable mobile android apk

Magic	Zip archive data, at least v2.0 to extract, compression method=deflate
TrID	Android Package (63.7%) Java Archive (26.4%) ZIP compressed archive (7.8%) PrintFox/Pagefox bitmap (640x800) (1.9%)
File size	17.33 MB (18172002 bytes)

Fuente:
https://www.virustotal.com/gui/file/e9edf3dce24f4e5057f56a3a68c8f4bc3528158e4431be64c031b7a738b312ab/details

VII. RECOMENDACIONES:

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

- Se debe considerar que desde al menos 2015, el grupo SpaceCobra ha resucitado a GravityRAT ampliando sus funcionalidades para exfiltrar las copias de seguridad de WhatsApp Messenger y recibir comandos de un servidor C&C para eliminar archivos. Al igual que antes, esta campaña utiliza aplicaciones de mensajería como señuelo para para distribuir el backdoor GravityRAT. El grupo detrás de este malware utiliza el código de la app de mensajería instantánea legítima llamada OMEMO para proporcionar la funcionalidad de chat en las aplicaciones de mensajería maliciosas BingeChat y Chatico; se recomienda no instalar aplicaciones que su fuente sea de dudosa procedencia.

- Para mitigar el incidente, considere utilizar las siguientes técnicas de MITRE ATT&CK:

Táctica	ID	Nombre	Descripción
Persistencia	T1398	Scripts de inicialización de arranque o inicio de sesión	GravityRAT recibe la intención de transmisión BOOT_COMPLETED para activarse al iniciar el dispositivo.
	T1624.001	Ejecución activada por eventos:	La funcionalidad GravityRAT se activa si ocurre uno de estos eventos: DISPOSITIVO_USB_CONECTADO,

Táctica	ID	Nombre	Descripción
		receptores de difusión	ACCIÓN_CONEXIÓN_ESTADO_CAMBIADO, USUARIO_DESBLOQUEADO, ACCIÓN_PODER_CONECTADO, ACCIÓN_PODER_DESCONECTADO, MODO AVIÓN, BATERIA BAJA, BATERÍA_OK, FECHA_CAMBIADO, REINICIAR, TIME_TICK, o CONECTIVIDAD_CAMBIO.
Evasión de defensa	T1630.002	Eliminación del indicador en el host: Eliminación de archivos	GravityRAT elimina los archivos locales que contienen información confidencial extraída del dispositivo.
Descubrimiento	T1420	Descubrimiento de archivos y directorios	GravityRAT enumera los archivos disponibles en el almacenamiento externo.
	T1422	Descubrimiento de la configuración de la red del sistema	GravityRAT extrae el IMEI, IMSI, dirección IP, número de teléfono y país.
	T1426	Descubrimiento de información del sistema	GravityRAT extrae información sobre el dispositivo, incluido el número de serie de la tarjeta SIM, el ID del dispositivo y la información común del sistema.
Recopilación	T1533	Datos del sistema local	GravityRAT extrae archivos del dispositivo.
	T1430	Seguimiento de ubicación	GravityRAT rastrea la ubicación del dispositivo.

Táctica	ID	Nombre	Descripción
	T1636.002	Datos de usuario protegidos: registros de llamadas	GravityRAT extrae los registros de llamadas.
	T1636.003	Datos Protegidos del Usuario: Lista de Contactos	GravityRAT extrae la lista de contactos.
	T1636.004	Datos de usuario protegidos: mensajes SMS	GravityRAT extrae mensajes SMS.
Comando y control	T1437.001	Protocolo de capa de aplicación: protocolos web	GravityRAT usa HTTPS para comunicarse con su servidor C&C.
Exfiltración	T1646	Exfiltración sobre el canal C2	GravityRAT extrae datos mediante HTTPS.
Impacto	T1641	Manipulación de datos	GravityRAT elimina archivos con extensiones particulares del dispositivo y elimina todos los registros de llamadas de los usuarios y la lista de contactos.

Fuente: https://www.welivesecurity.com/la-es/2023/06/16/gravityrat-malware-roba-copias-seguridad-whatsapp/

En general se debe considerar las siguientes recomendaciones:

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.

- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 “Concienciación con educación y capacitación en seguridad de la información” o NIST PR.AT-1: “Todos los usuarios se encuentran entrenados e informados”, a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

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:

- **Stefanko, L (2023)**. *GravityRAT: un malware que va en busca de la copia de seguridad de WhatsApp.* Welivesecurity by ESET; recuperado de: https://www.welivesecurity.com/la-es/2023/06/16/gravityrat-malware-roba-copias-seguridad-whatsapp/

- **Opeyemi, O (2023).** *Nuevo GravityRAT para Android dirigido a las copias de seguridad de WhatsApp.* TuxCare**;** recuperado de: https://tuxcare.com/es/blog/new-android-gravityrat-targets-whatsapp-backups/

- **Virus Total (2023).** BingeChat.apk, recuperado de: https://www.virustotal.com/gui/file/e9edf3dce24f4e5057f56a3a68c8f4bc3528158e4431be64c031b7a738b312ab/detection

- **Virus Total (2023).** 4ebdfa738ef74945f6165e337050889dfa0aad61115b738672bbeda648a59dab, recuperado de: https://www.virustotal.com/gui/file/4ebdfa738ef74945f6165e337050889dfa0aad61115b738672bbeda648a59dab

- **Virus Total (2023).** e9edf3dce24f4e5057f56a3a68c8f4bc3528158e4431be64c031b7a738b312ab, recuperado de: https://www.virustotal.com/gui/file/caf0a39318cfc1e65eae773a28de62ce08b7cf1b9d4264e843576165411e2a84