Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°142	Fecha: 17-06-2023
		Página: 4 de 28

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	GravityRAT, un malware que va en busca de la copia de seguridad de WhatsApp		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES

- El grupo de investigadores de la compañía ESET detectan versiones troyanizadas de la aplicación legitima de código abierto OMEMO Instant Messenger para Android de GravityRAT. El troyano de acceso remoto se distribuye a través de aplicaciones de mensajería tales como: BingeChat y Chatico.
- GravityRAT es una herramienta de acceso remoto que es conocida desde 2015.
- Desde agosto 2022 sigue activa la campaña de BingeChat ofreciendo servicio de mensajería gratuita y uso compartido de archivos. Sin embargo, la campaña que utiliza Chatico ya no se encuentra activa.
- Los ciberdellincuentes aún permanecen desconocidos, pero internamente los investigadores rastrean al grupo SpaceCobra.

2. DETALLES:

La versión de GravityRAT puede recibir comandos para eliminar archivos y extraer archivos de la copia de seguridad de WhatsApp.
Luego de descargar la aplicación maliciosa, solicita a la víctima inicie sesión, para esto emplea una dirección IP particular, geolocalización, una URL personalizada que funciona dentro de un periodo de tiempo específico.
GravityRAT comienza a interactuar con su servidor C&C, filtrando datos de la víctima y esperando se ejecuten comandos. Los datos que ex filtra son: registro de llamadas, lista de contactos, mensajes SMS, archivos de extensiones específicas, ubicación del dispositivo, información básica del dispositivo, estos datos son almacenados en un archivo de texto en medios externos, luego se extraen al servidor de C&C y finalmente se eliminan.

Se ha tomado conocimiento que existe un usuario de India que fue atacado con la versión actualizada de esta amenaza, para esto emplearon como señuelo la app Chatico.
La versión distribuida de BingeChat la socializaron a través de un sitio web, por lo que la víctima requirió registrarse, se presume que los ciberdelincuentes crean estas campañas que son dirigidas a víctimas específicas, ya que el sitio web que descarga la aplicación maliciosa se abre por un periodo de tiempo limitado.

A. Indicadores de Compromiso

Archivos

SHA-1	Nombre del Paquete	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.

Red

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.
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 ex filtración 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

B. Productos afectados

- WhatsApp (copias de seguridad).

3. RECOMENDACIONES:

- Tener cuidado cuando una aplicación le solicita que habilite todos los permisos para que funcione correctamente. A excepción por el permiso para leer los registros de llamadas los otros permisos son típicos de cualquier aplicación de mensajería.

Fuente de Información:	• hxxps://www.welivesecurity.com/la-es/2023/06/16/gravityrat-malware-roba-copias-seguridad-whatsapp/ • hxxps://www.forbesargentina.com/innovacion/eset-identifica-software-espia-va-busca-copia-seguridad-whatsapp-n35455

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 142**	**Fecha: 17-06-2023**
		Página 21 de 28

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades críticas en los servicios de Microsoft Azure		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES

Los expertos en ciberseguridad de Orca Security han identificado dos vulnerabilidades de severidad CRÍTICA de tipo secuencias de comandos entre sitios (XSS) en los servicios de Microsoft Azure (Azure Bastion y Azure Container Registry) que permiten Cross-Site Scripting (XSS) al explotar una debilidad en el iframe posterior al mensaje. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar scripts maliciosos, lo que podría comprometer las sesiones de los usuarios y los datos confidenciales.

2. DETALLES:

- Los expertos en ciberseguridad de Orca Security descubrieron dos vulnerabilidades críticas en Azure Bastion y Azure Container Registry, que permitieron a un atacante lograr un ataque Cross-Site Scripting (XSS) mediante el uso de iframe-postMessages.
- **Azure Bastion** es un servicio proporcionado por Microsoft Azure que ofrece una forma segura y sin inconvenientes de acceder a máquinas virtuales (VM) dentro del entorno de nube de Azure. Actúa como un servidor de salto, proporcionando una puerta de enlace dedicada y reforzada para conectarse a máquinas virtuales de forma segura sin exponerlas a la Internet pública.
- **Azure Container Registry** es un servicio de nube administrado proporcionado por Microsoft Azure que permite a los usuarios almacenar, administrar e implementar imágenes de contenedores. Proporciona una ubicación centralizada para alojar las imágenes de su contenedor, lo que le permite administrarlas y crear versiones de manera eficiente.
- Las vulnerabilidades de iframe postMessage que se descubrió en Azure Bastion y Azure Container Registry permitió a los atacantes incrustar puntos finales en servidores remotos mediante la etiqueta iframe. Aprovechando esta debilidad, combinada con la falta de una validación adecuada del origen de postMessage, los adversarios habrían podido ejecutar código JavaScript malicioso y comprometer datos confidenciales.
- Cabe señalar que Microsoft Azure ofrece varios servicios y características que aprovechan los iframes para incorporar contenido de terceros o permitir la comunicación entre dominios. Desafortunadamente, si estos iframes son susceptibles a ataques XSS a través del mecanismo postMessage, abre la puerta para que los atacantes manipulen el contenido que se muestra dentro del iframe, lo que podría comprometer datos confidenciales o ejecutar acciones maliciosas dentro del entorno de Azure.
- Estas vulnerabilidades podrían permitir el acceso no autorizado a la sesión de la víctima dentro del iframe del servicio de Azure comprometido, lo que puede tener graves consecuencias, incluido el acceso no autorizado a los datos, las modificaciones no autorizadas y la interrupción de los iframe de los servicios de Azure. A pesar de varias mejoras de seguridad de Azure para mitigar la vulnerabilidad XSS del iframe posterior al mensaje, se logró descubrir dos servicios de Azure, Azure Bastion y Azure Container Registry, que se podían explotar a través de esta vulnerabilidad.
- La vulnerabilidad de tipo XSS ocurre cuando un atacante inyecta scripts maliciosos en un sitio web confiable, que luego son ejecutados por los navegadores de los usuarios desprevenidos. Esto puede provocar acceso no autorizado, robo de datos e incluso el compromiso total del sistema afectado. En el caso de las vulnerabilidades que discutimos en este blog, la vulnerabilidad del iframe postMessage actuó como el punto de entrada para que los atacantes explotaran las fallas de XSS.

A. Productos afectados:

- Microsoft Azure: servicios de Azure Bastion y Azure Container Registry.

3. RECOMENDACIONES:

- Microsoft ha implementado varias mejoras de seguridad relacionadas en Azure que aborda estas vulnerabilidades. Estos incluyen políticas de seguridad de contenido (CSP) más estrictas para evitar la ejecución de scripts no confiables, mecanismos de validación de entrada sólidos y capacidades mejoradas de monitoreo y registro para detectar y responder a posibles ataques XSS en tiempo real.

- Por otro lado, para mitigar los controladores postMessage mal configurados y prevenir vulnerabilidades XSS, se recomienda seguir las prácticas:
  - **Validar y desinfectar los datos de entrada**: asegurarse de que todos los datos generados por el usuario o que no sean de confianza se validen y desinfecten correctamente en el lado del servidor. Utilice técnicas de validación de entrada para rechazar cualquier entrada que no se ajuste a los patrones esperados. Además, codifique correctamente los datos generados por el usuario cuando los muestre.
  - **Lista blanca de dominios y orígenes confiables para la comunicación posterior al mensaje**: especificar explícitamente una lista de dominios que se consideran seguros y confiables para la comunicación a través de la publicación posterior al mensaje. Solo se aceptarán y procesarán los mensajes que se originen en estos dominios incluidos en la lista blanca, mientras que los mensajes de cualquier otro dominio se ignorarán o bloquearán.
  - **Limitar los tipos y formatos de mensajes aceptados**: determinar los tipos específicos de mensajes que su aplicación puede procesar. Esto puede incluir la restricción de mensajes a estructuras de datos específicas o formatos predefinidos.
  - **Implementar la política de seguridad de contenido (CSP) para restringir la ejecución de secuencias de comandos**: CSP le permite definir y aplicar un conjunto de políticas para su aplicación web, incluidas las restricciones sobre qué secuencias de comandos externas se pueden ejecutar. Al configurar un CSP estricto, puede evitar la ejecución de scripts maliciosos inyectados a través de ataques XSS.

Fuentes de información	• hxxps://orca.security/resources/blog/examining-two-xss-vulnerabilities-in-azure-services/#h-vulnerability-1-azure-bastion-svg-exporter-xss • hxxps://orca.security/resources/blog/examining-two-xss-vulnerabilities-in-azure-services/#h-vulnerability-2-azure-container-registry-quick-start-xss • hxxps://orca.security/resources/blog/examining-two-xss-vulnerabilities-in-azure-services/#h-vulnerability-2-azure-container-registry-quick-start-xss