

# Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT  
Ministerio del Interior y Seguridad Pública  
Subsecretaría del Interior



Alerta de seguridad informática	2CMV23-00417-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de junio de 2023
Última revisión	08 de junio de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ





## Resumen

El CSIRT de Gobierno ha identificado una nueva campaña de phishing con malware suplantando al Servicio de Impuestos Internos con una falsa factura no pagada.

Si la víctima interactúa con el fichero malicioso, se encuentra con Mekotio, un troyano bancario que apunta principalmente a Brasil, Chile, México, España, Perú y Portugal y cuya característica más notable en las variantes más recientes es el uso de una base de datos SQL como servidor de C2.

Esta es una variante a la campaña de Conaset, donde se atraía al destinatario a hacer clic en un enlace de email con la excusa de contener una falsa multa de tránsito, la cual si no era pagada desencadenaría una acción judicial.

### CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>  
 Teléfonos: 1510 | + (562) 24863850 | Correo: [soc-csirt@interior.gob.cl](mailto:soc-csirt@interior.gob.cl)  
 @csirtgob  
 <https://www.linkedin.com/company/csirt-gob>

## Indicadores de Compromiso Asociados

### Archivos que se encuentran en la amenaza

#### SHA256

Indicador	Relación
203d8a6e596cad036eae854e7484509a11ee35547ca5e1f2b2249ae825ec714f	nopagadafacSiimarzo.zip
3d5f0dbce1204d0db72b9574800bef878015fdbbe7b24dc5b553caed5da4dc5a	nopagadafacSiimarzo.msi
6d2f67ddd2438baa14e2565e02e015296db31daf3d03410e7c783e89c785e614	Siifactmarzo.zip
3d5f0dbce1204d0db72b9574800bef878015fdbbe7b24dc5b553caed5da4dc5a	Siifactmarzo.msi
f178861e00b0a2ba7d50c103ac41ac6eb89e7c6232bd25bd1fa8752a8871e445	nopagadafacturaSii.zip
3d5f0dbce1204d0db72b9574800bef878015fdbbe7b24dc5b553caed5da4dc5a	nopagadafacturaSii.msi

#### URL-Dominio

Dominio	Relación
https://gscjgn[.]org/marzosifact/nopagada/Factsii/	Descarga del Fichero
https://cmg-technology[.]ro/zpnuevo/	Contenedor de Malware
103.235.105[.]113	IP Pagina Descarga
188.240.2[.]189	IP Pagina Contenedora
50.116.72.199	IP Correo
158.69.109.191	IP Correo
162.214.157.170	IP Correo

#### MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Colección (Datos del sistema local)	T1005
Acceso a Credenciales (Credenciales en Archivos)	T1081
Evasión de Defensa (Modificación de registro)	T1112
Evasión de Defensa (Evasión de Virtualización/Sandboxing)	T1497
Descubrimiento (Consulta del Registro)	T1012

### CONTACTO Y REDES SOCIALES CSIRT

## Imagen del Mensaje

Factura no pagada, resuelve tu situación.

 Sii - Servicio de Impuestos Internos <support@followthetrolley.com>  
Para [Redacted] lu. 05/06/2023 18:47

 [Responder](#) [Responder a todos](#) [Reenviar](#) [...](#)

 Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

**Sii - Servicio de Impuestos Internos**

Estimado Contribuyente

Nos estamos comunicando con usted a través del correo electrónico [Redacted] registrado en nuestra [Redacted] sistema.

Le informamos mediante este medio que hay una factura que se encuentra en estado de NO PAGADA. Le invitamos a regularizar esta situación a través del siguiente enlace.

Por favor realice el pago lo mas pronto posible, a fin de evitar las molestias de un cobro judicial, que pueda implicar embargo o suspensión temporal o definitiva depende el caso.

Puede consultar el estado de su deuda actual mediante el siguiente enlace.

**FACTURA**      **Acceso**      **Regularizar**  
**Marzo - 2022** [Consultar Factura abierto](#) [Regularizar situación](#)





(Para acceder al documento electrónico recuerde que la versión de este documento es únicamente para PC no funciona en dispositivos móviles.)

Asegúrate de consultar tu situación con **Sii** para evitar problemas legales.

**Servicio de Impuestos Internos - 2023**



## CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>  
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl  
 @csirtgob  
 <https://www.linkedin.com/company/csirt-gob>