Alerta de seguridad informática	2CMV23-00429-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de septiembre de 2023
Última revisión	06 de septiembre de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware que suplanta al Servicios de Impuestos Internos en un mail falso sobre una supuesta factura no pagada.

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario que destaca por el uso de una base de datos SQL como servidor de comando y control.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
65dd04ec6ea0baf56b2ef31e170c826d7f10797be56f13c476bf669b4419c75b	siiFactmarzover.zip
6f1322c3e2a7869f0ff396a0b6d8df069a61af4b04fa65b924bab9fab1aa843f	siiFactmarzover.msi

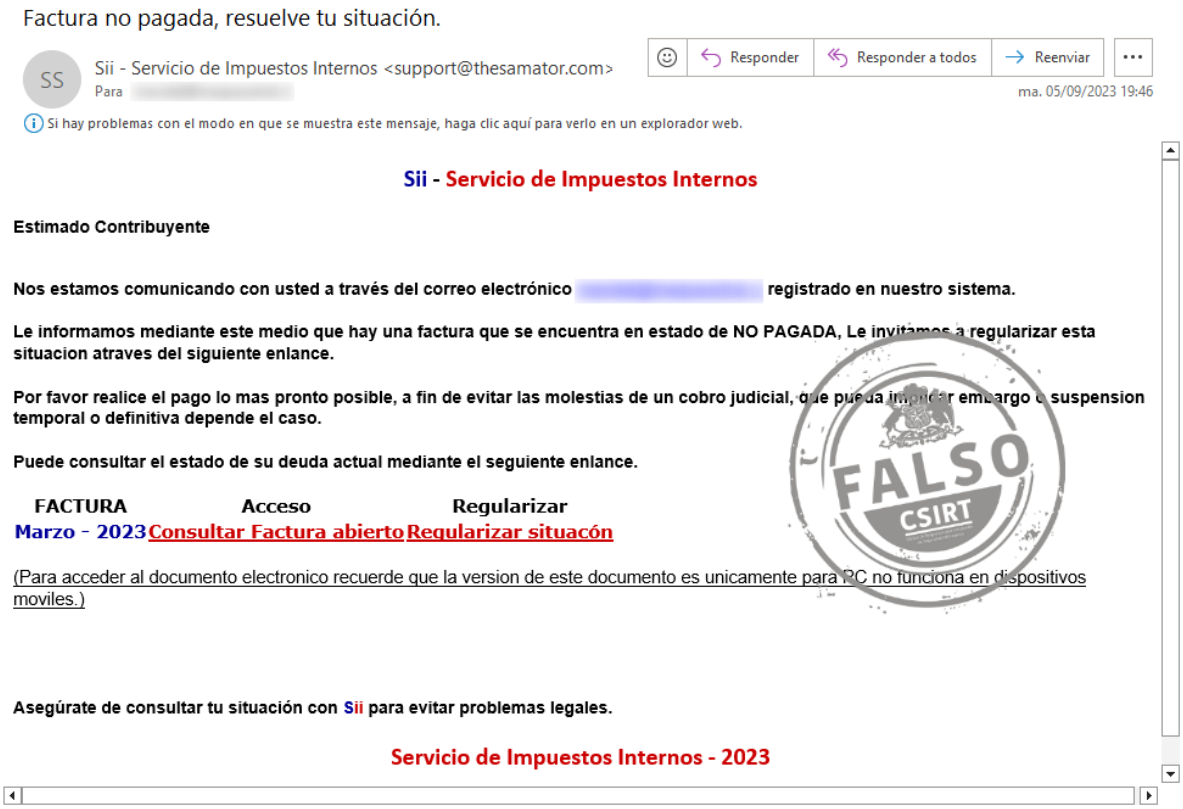
URL-Dominio

Dominio	Relación
https://www.stivsolutions[.]com/factsiimarzonopagada/verfact/?hash={mail}	Descarga del Fichero
https://www.stivsolutions[.]com/factsiimarzonopagada/	Contenedor Malware
support@thesamator[.]com	Correo de salida

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Descubrimiento (Consulta del Registro)	T1012
Descubrimiento (Información del Sistema)	T1082
Descubrimiento (Equipos Perimetrales)	T1120

Imagen del mensaje



Factura no pagada, resuelve tu situación.

SS Sii - Servicio de Impuestos Internos <support@thesamator.com>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
ma. 05/09/2023 19:46

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 nuestro sistema.

Le informamos mediante este medio que hay una factura que se encuentra en estado de NO PAGADA, Le invitamos a regularizar esta situacion atraves del siguiente enlance.

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

Puede consultar el estado de su deuda actual mediante el seguiente enlance.

FACTURA	Acceso	Regularizar
Marzo - 2023	Consultar Factura abierto	Regularizar situacón

(Para acceder al documento electronico recuerde que la version de este documento es unicamente para PC no funciona en dispositivos moviles.)

FALSO CSIRT

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

Servicio de Impuestos Internos - 2023

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.06 17:49:44 -03'00'