Alerta de seguridad informática	2CMV23-00424-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2023
Última revisión	13 de julio 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 suplantando al Servicio de impuestos internos con una falsa factura electrónica emitida.

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario dirigido principalmente a naciones de Iberoamérica (con distintas campañas que apuntan a distintos países, como la actual, preparada para Chile), y 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
0ffc01fec8cc27af51fa6796db3225562d40f92008ea0877f28876a91b4357f4	MTT009T8d10i2qB0sG1Fs952C.zip
0c2094a3608e9f3fe6a874a61097137c8118671a79b25e2a5b989c5cabbfe89b	MTT009T8d10i2qB0sG1Fs952C.msi

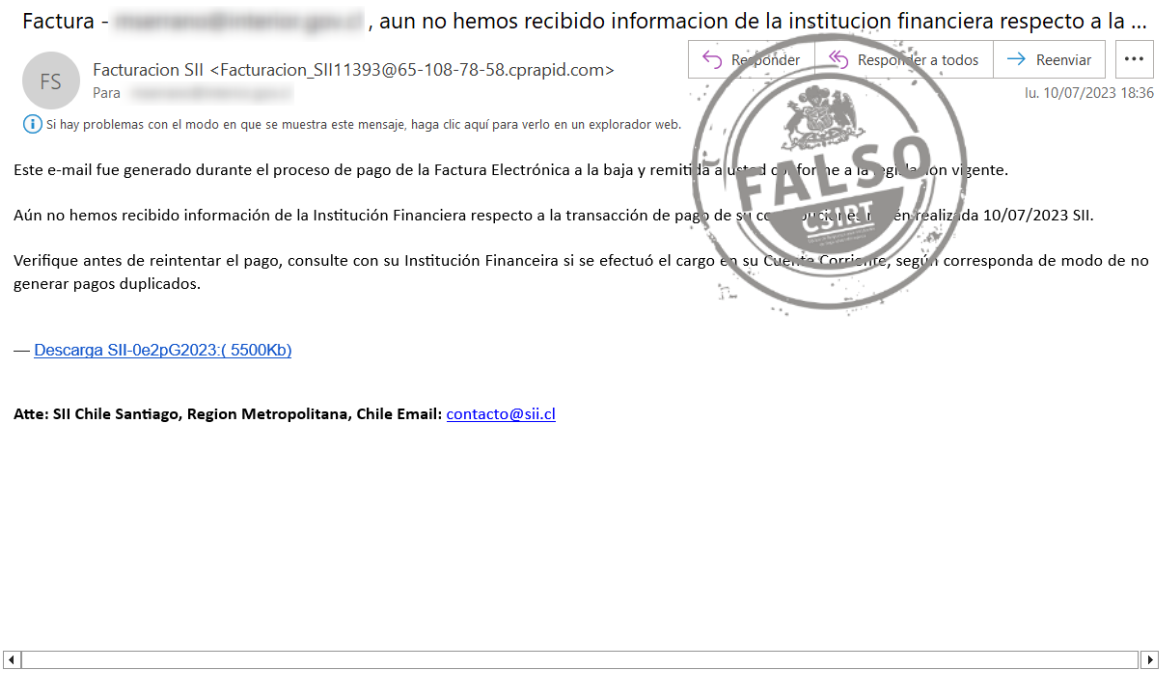
URL-Dominio

Dominio	Relación
https://khojney[.]com/wp-content/plugins/--/factura/	Descarga del Fichero
34.210.155[.]57:9995	Comando y Control
mobilforstarkare@65-108-78-58.cprapid.com	Correo de salida
dh_isqdy3@richard-stockton.dreamhost.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 - [redacted], aun no hemos recibido informacion de la institucion financiera respecto a la ...

FS Facturacion SII <Facturacion_SII11393@65-108-78-58.cprapid.com>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
lu. 10/07/2023 18:36

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

Este e-mail fue generado durante el proceso de pago de la Factura Electrónica a la baja y remitida a usted conforme a la legislación vigente.

Aún no hemos recibido información de la Institución Financiera respecto a la transacción de pago de su consulta [illegible] en realizada 10/07/2023 SII.

Verifique antes de reintentar el pago, consulte con su Institución Financeira si se efectuó el cargo en su Cuenta Corriente, según corresponda de modo de no generar pagos duplicados.

— Descarga SII-0e2pG2023:(5500Kb)

Atte: SII Chile Santiago, Region Metropolitana, Chile Email: contacto@sii.cl

FALSO

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.13 16:47:11 -04'00'