Alerta de seguridad informática	2CMV24-00448-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de marzo de 2024
Última revisión	1 de marzo de 2024

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 Servicios de Impuestos Internos con un falso problema en la emisión de boletas electrónicas, donde luego citan para anular la emisión de una factura.

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 comandos de base de datos SQL para obtener información del sistema infectado y enviarlo al servidor de Comando y Control.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
657755a59be263e7cf3a5b2d769a276a06e60c6f7ddeab579141b14508d8b43b	informacion_001.zip
126c90a8396077de034acf0a4a38927ec3d807533e6e2c247807ccebfec5da28	informacion_0012F99311.msi
e28e34fbdaff077669586dcdb4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7	libeay32.dll

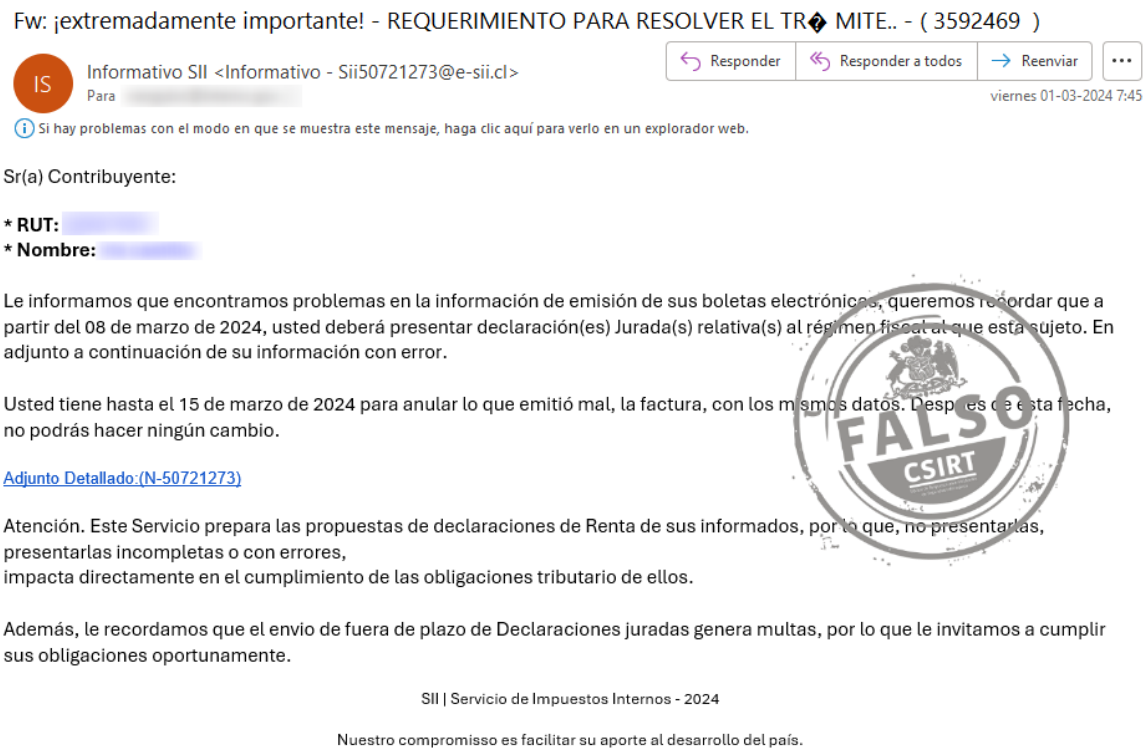
URL-Dominio

Dominio	Relación
https://kindersurge.com/well-mail/Descargar/03/?/ID/AQMkADAwATYwMAItZjIyAGUtZGU5My0wMAItMDAKAEYAAAON7YLP5Z99SqeVMkDuw2FoTBwCnwQJz51N6QLeL72BoUAOpjAAAcASIAAACnwQJz51N6QLeL72BoUAOpjAAc	Descarga del Fichero
https://plataforma.olmuenatura[.]cl/well-known/validation/3.1/index.php	Redirección
https://alldata[.]com.br/images/images/images/informacion_001.zip?template=77ab79783602f981b3f2ca86a0191a47=Initiate&valid=true&session=dd77ab79783602f981b3f2ca86a0191a47	Contenedor del Malware
'Informativo - Sii50721273'@e-sii.cl	Correo de salida
'Informativo - Sii77683503'@e-sii.cl	Correo de salida
'Contacto Sii85858743'@e-sii.cl	Correo de salida
3.135.233[.]216:9795	C2
34.117.186.192:443	Whois

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
Comando y control (Puerto no estándar)	T1571

Imagen del mensaje



Fw: ¡extremadamente importante! - REQUERIMIENTO PARA RESOLVER EL TR MITE.. - (3592469)

IS Informativo SII <Informativo - Sii50721273@e-sii.cl>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
viernes 01-03-2024 7:45

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

Sr(a) Contribuyente:

*** RUT:** [redacted]
*** Nombre:** [redacted]

Le informamos que encontramos problemas en la información de emisión de sus boletas electrónicas, queremos recordar que a partir del 08 de marzo de 2024, usted deberá presentar declaración(es) Jurada(s) relativa(s) al régimen fiscal al que está sujeto. En adjunto a continuación de su información con error.

Usted tiene hasta el 15 de marzo de 2024 para anular lo que emitió mal, la factura, con los mismos datos. Después de esta fecha, no podrás hacer ningún cambio.

Adjunto Detallado:(N-50721273)

Atención. Este Servicio prepara las propuestas de declaraciones de Renta de sus informados, por lo que, no presentarlas, presentarlas incompletas o con errores,
impacta directamente en el cumplimiento de las obligaciones tributario de ellos.

Además, le recordamos que el envio de fuera de plazo de Declaraciones juradas genera multas, por lo que le invitamos a cumplir sus obligaciones oportunamente.

SII | Servicio de Impuestos Internos - 2024

Nuestro compromisso es facilitar su aporte al desarrollo del país.

FALSO
CSIRT

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.03.01 14:39:28 -03'00'