Alerta de seguridad informática	2CMV23-00436-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de noviembre de 2023
Última revisión	27 de noviembre 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 citación policial debido a una supuesta resolución en contra de la víctima.

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario dirigido principalmente a naciones de Iberoamérica, 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
87122c413761c8055b76eb3c8e2b1fca3bf64e6b668006705931251d935e0053	facturaSiinopagada.zip
c819d4be69eb4f4de0e31cce25bb9c8235b9a700ccaeba554c44ed144959e036	facturaSiinopagada.msi

URL-Dominio

Dominio	Relación
https://burgerbarsaintlouis[.]com/octubreSiifactura/?hash={mail}	Descarga del Fichero
https://nobreakdesign[.]com.br/exenovo/facturaSiinopagada.zip?210217484	Contenedor Malware
support@orientbethlehem[.]net	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

Atención - Tienes una factura electrónica pendiente de pago.

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

Responder | Responder a todos | Reenviar | ...
lunes 27-11-2023 6:51

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
Octubre - 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: 2023.11.27 11:29:11 -03'00'