| | |
|---|---|
| Alerta de seguridad informática | 2CMV23-00437-01 |
| 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 que suplanta al Servicio de impuestos Internos.

Si la víctima interactúa con el fichero malicioso incluido en estos correos de phishing fraudulentos, 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 |
|---|---|
| 3250311de041c22eab029c97e95b6d2710f5f026ebaf2ea90e85afca6ae14007 | Boleta_Pendiente_6564e9b5b88292.81012419.zip |
| ff06652a3243b538a50715d9a8d44c3b8ca34aff98cc8d1cf6b2fd0a0c139982 | ENEL91928001237N0320B127S7.msi |

### URL-Dominio

| Dominio | Relación |
|---|---|
| http://lucacocinas.com[.]ar/swf/abs/TGR/VF9IU7TS9S8D3_Boleta_Pendiente_3171_4D2F_8B51_9C5E_002839921.php | Descarga del Fichero |
| http://medulashvili[.]ge/Data/Boleta/Sii/H6F3VB881I0/home.php?hash=P0s&CAYdj1=sII | Contenedor Malware |
| support@orientbethlehem[.]net | Correo de salida |
| 18.228.28[.]141:9795 | C2 |

### 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

Fw: Informe importante.

S SII <Contacto-S7DTY@Sii.cl>
Para ghuertas@interior.gob.cl

Responder | Responder a todos | Reenviar | ...
lunes 27-11-2023 14:24

Estimado contribuyente.

**¡Atención! Servicio de Impuestos internos.**

Advertencia! Encontramos problemas en la Emision de sus boletas electrónicas, verifique la emisión de su boletas electrónicas.

Se adjunta su boletín electrónico con error de información

**[ Descargar Boletín ]**

© 2023 SII Servicio Servicio Impuestos internos. Todos los derechos reservados www.sii.cl



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.28 15:50:48 -03'00'