

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Alerta de seguridad informática	2CMV23-00423-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de julio de 2023
Última revisión	12 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 que se difunde a través de emails que suplantan al Ministerio de Transportes y Telecomunicaciones, aduciendo una supuesta multa (que en realidad es inexistente)

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario que apunta principalmente a Brasil, Chile, México, España, Perú y Portugal, y cuya característica más destacada en las variantes más recientes es el uso de una base de datos SQL como servidor de C2.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
bc5b31facbde74c5fd435198a28ffad8e9191bcb7af3fccd6671de3849e08af	MTT0001221000MULT4411s4a000. zip
be77fceb122776f894dea1a78d076cf4e667044a9fcadf781a613a4bc93d16ee	MTT0001221000MULT4411s4a000. msi

URL-Dominio

Dominio	Relación
https://p-tekng.com/wp-content/themes/--/NEX/dasssashytsrfwewdw4w432dcadsswe32dsfwywyw67wjehnsbvcdfreyd.php	Descarga del Fichero

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

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Imagen del Mensaje

MTT.GOB.CL - Atencion [redacted], NOTIFICAMOS INFRACCION DE TRANSITO 15736

MM

MTT MULTAS <MTT-MULTAS26197@65-108-78-58.cprapid.com>

Para



Responder


Responder a todos

Reenviar



ma. 11/07/2023 18:49



 Ministerio de Transportes
y Telecomunicaciones

Estimado(a), [redacted]

Detectamos en nuestro sistema un registro de multa de tránsito no pagada.
Debido a que usted no se notificó en el tribunal de faltas correspondiente le reenviamos las Fotos via internet.
Si usted no regulariza las infracciones correspondientes en los próximos 90 días a partir de la fecha de emisión de este comunicado, su vehículo será informado como deudor y pasará a formar parte del Veraz, conforme Ley n. 12.799 de 1/04/2009.
A inclusión de su vehículo en el Veraz le impedirá la venta regular de su vehículo por 2 años en la República de Chile.





Para mayor información sobre la multa de tránsito, descargue el detalle en los siguientes links:

[FOTO 1](#)

[FOTO 2](#)



CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>