

Alerta de Seguridad de la Información

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	2CMV23-00425-01
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 a la Policía de investigaciones (PDI) 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 (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.

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 de la Información

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
462a814f8b26279cfc71dbdf874d7c9c626f61811516d5705da9eb0dd32e441b	23F000R33V21L94IR7vZp.zip
969c4d790314beca402ba8cc253ceb9af856c1ed22aae512e245a9538ea86b95	23F000R33V21L94IR7vZp.msi

URL-Dominio

Dominio	Relación
https://www.elo.net[.]br/wp-content/languages/pdi/dassashytsrfwewdw4w432dcadsswe32dsfwywyw67wjehnsbvcdfreyd.php	Descarga del Fichero
http://servers.itresources[.]am/itr/public/teams/mobilforstarkare@65-108-78-58[.]cprapid.com	Contenedor Malware 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

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>

Imagen del Mensaje

PDI Virtual - [Redacted] Solicitamos su presencia ante el tribunal de justicia.



PDI VIRTUAL <proceso_de_denuncia13594@pdichile.cl>
Para [Redacted]

← Responder ← Responder a todos → Reenviar ...

ju. 13/07/2023 13:21



CITACIÓN POLICIAL
Radicado:
1100160002532008
Procedencia: Policía de
Investigaciones de
Chile
Decisión: Citación
Santiago, Chile
Página 1 de 1



ÓRDEN DE CITACIÓN

En cumplimiento de lo acordado por el Juzgado de lo Penal, en virtud de las Diligencias previas Número 2677/23, Pieza Separada Número Veintidós, se le hace una citación policial por parte de la Policía de Investigaciones de Chile debido a que la resolución en su contra ha sido determinada y en consecuencia solicitamos su presencia Sr(a) [Redacted] en este despacho sin [Redacted] el día 14 de Julio del presente año, a las 2:35 p.m..





Dicha audiencia será realizada con el fin de rendir indagatoria ante un fiscal de la Unidad Nacional de Delitos por los cargos de Hurto Agravado en primera persona en el caso contra el señor Carlos Humberto Gómez. En caso de no presentarse, será liberada una orden de presentación con el uso de la fuerza pública.

Es importante que lleve los documentos requeridos para agilizar la audiencia.

Documentos Requeridos para Audiencia por Citación 2023

Del hurto. Artículo 446.-Los autores de hurto serán castigados:
1. Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor de la cosa hurtada excediere de cuarenta unidades tributarias mensuales.
2. Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.
3. Con presidio menor en su grado mínimo y multa de cinco unidades tributarias mensuales, si excediere de media unidad tributaria mensual y no pasare de cuatro unidades tributarias mensuales.
Si el valor de la cosa hurtada excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

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>