



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 256

semana del 24 al 30 de mayo de 2024

# LA SEMANA EN CIFRAS

## IP INFORMADAS

3

IP advertidas en múltiples campañas de phishing y de fraude.



## URL ADVERTIDAS

4

URL asociadas a sitios fraudulentos y campañas de phishing y malware



## PARCHES COMPARTIDOS

1

Las mitigaciones son útiles en productos de Check Point.



## HASH REPORTADOS

8

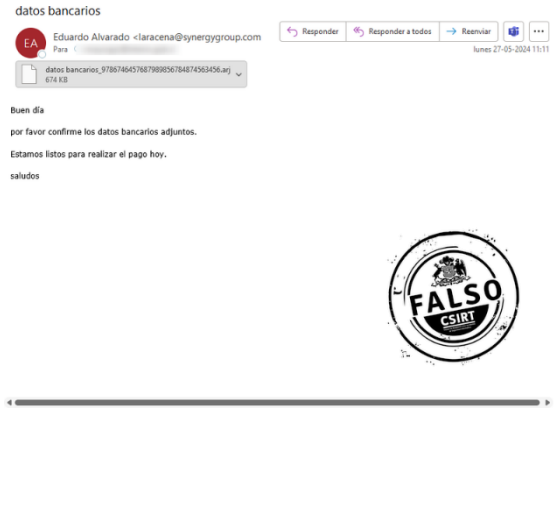
Hashes asociados a múltiples campañas de phishing con archivos que contienen malware.

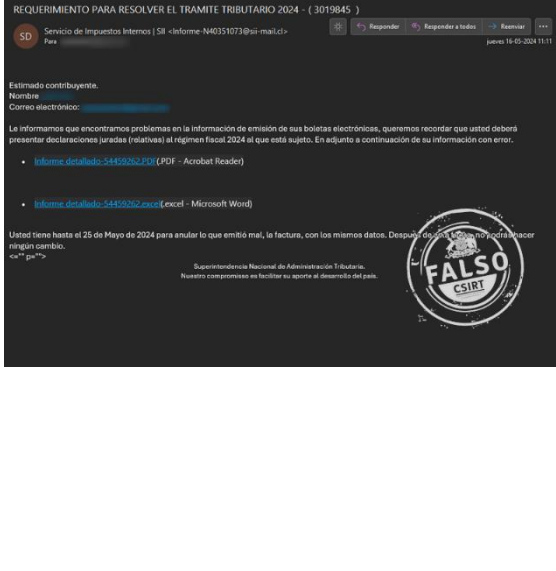


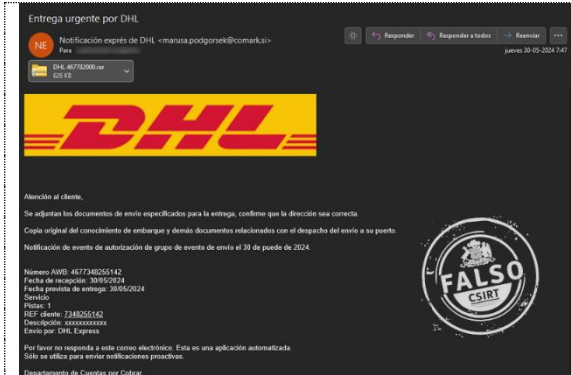
# CONTENIDO

1. Malware.....	3
2. Phishing .....	5
3. Vulnerabilidades.....	7
4. Recomendaciones y buenas prácticas .....	8
5. Muro de la Fama .....	9

## 1. Malware

 <p>datos bancarios</p> <p>Eduardo Alvarado &lt;laracena@synergygroup.com&gt;          Para: datos bancarios_97f87465786798995678474563456.arj          674 KB</p> <p>Buen día</p> <p>por favor confirme los datos bancarios adjuntos.</p> <p>Estamos listos para realizar el pago hoy.</p> <p>saludos</p> <p><b>FALSO</b></p>	<p><b>Solicitud fraudulenta de datos bancarios - Suplantación con malware</b></p> <table border="1"> <tr><td>Código de alerta</td><td>CMV24-00464</td></tr> <tr><td>Clase de alerta</td><td>Fraude</td></tr> <tr><td>Tipo de incidente</td><td>Malware</td></tr> <tr><td>Nivel de riesgo</td><td>Alto</td></tr> <tr><td>TLP</td><td>Blanco</td></tr> <tr><td>Fecha de lanzamiento original</td><td>27 de mayo de 2024</td></tr> <tr><td>Última revisión</td><td>27 de mayo de 2024</td></tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>Asunto</b>          Datos bancarios</p> <p><b>Correo de salida</b>          laracena@synergygroup.com.do</p> <p><b>SHA256</b>          977131718295bb0d52814d2d30da09646abbbc32ced7a0a21500b59678e3195          9e87201967f5b16c669301ad815198837b8a9e7b50b9e9226e49f72fd2717363</p> <p><b>Enlace para revisar IoC:</b>  <a href="https://csirt.gob.cl/alertas/cmv24-00464/">https://csirt.gob.cl/alertas/cmv24-00464/</a></p>	Código de alerta	CMV24-00464	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	27 de mayo de 2024	Última revisión	27 de mayo de 2024
Código de alerta	CMV24-00464														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	27 de mayo de 2024														
Última revisión	27 de mayo de 2024														

 <p>REQUERIMIENTO PARA RESOLVER EL TRAMITE TRIBUTARIO 2024 - ( 3019845 )</p> <p>SD Servicio de Impuestos Internos   SII &lt;Informe-N40351073@sii-mail.cl&gt;          Para: jueves, 16 de mayo de 2024 11:11</p> <p>Estimado contribuyente,</p> <p>Nombre: [REDACTED]          Correo electrónico: [REDACTED]</p> <p>Le informamos que encontramos problemas en la información de emisión de sus boletas electrónicas, queremos recordar que usted deberá presentar declaraciones juradas (rotativas) al régimen fiscal 2024 al que está sujeto. En adjunto a continuación de su información con error.</p> <ul style="list-style-type: none"> <li>Informe detallado: 54450262.pdf (PDF - Acrobat Reader)</li> <li>Informe detallado: 54450262.docx (Excel - Microsoft Word)</li> </ul> <p>Usted tiene hasta el 25 de Mayo de 2024 para anular lo que emitió mal, la factura, con los mismos datos. Después de esa fecha no podrá hacer ningún cambio.</p> <p>Superintendencia Nacional de Administración Tributaria.          Nuestro compromiso es facilitar su aporte al desarrollo del país.</p> <p><b>FALSO</b></p>	<p><b>Conaset - Suplantación con malware</b></p> <table border="1"> <tr><td>Código de alerta</td><td>CMV24-00465</td></tr> <tr><td>Clase de alerta</td><td>Fraude</td></tr> <tr><td>Tipo de incidente</td><td>Malware</td></tr> <tr><td>Nivel de riesgo</td><td>Alto</td></tr> <tr><td>TLP</td><td>Blanco</td></tr> <tr><td>Fecha de lanzamiento original</td><td>28 de mayo de 2024</td></tr> <tr><td>Última revisión</td><td>28 de mayo de 2024</td></tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>Asunto</b>          REQUERIMIENTO PARA RESOLVER EL TRAMITE TRIBUTARIO 2024 – ( 3019845 )</p> <p><b>Correo de salida</b>          Informe-N40351073@sii-mail.cl</p> <p><b>SHA256</b>          69917b3dc70ffe5c6bfabff6ac0938c3ab2402826d0298bca26c1d72f698c22d          7e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910a          91a3d5c44efe38c16b038480db835d34b7f3151cda18fd066a7ee4c2270bd280          e28e34fbdaff077669586dcdb4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7</p> <p><b>Enlace para revisar IoC:</b>  <a href="https://csirt.gob.cl/alertas/cmv24-00465/">https://csirt.gob.cl/alertas/cmv24-00465/</a></p>	Código de alerta	CMV24-00465	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	28 de mayo de 2024	Última revisión	28 de mayo de 2024
Código de alerta	CMV24-00465														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	28 de mayo de 2024														
Última revisión	28 de mayo de 2024														



## DHL - Suplantación con malware

Código de alerta	CMV24-00466
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2024
Última revisión	30 de mayo de 2024

## Indicadores de compromiso

### Asunto

Entrega urgente por DHL

### Correo de salida

barbara.kosi@colby.si





### SHA256

739aa9e81a4963bce4521386fed3e464f0573125dc503249ab0d60000346d28f  
ea07a13d0955fc66206df074a3beb333201e126389c224a045f9932a2b87d2ce

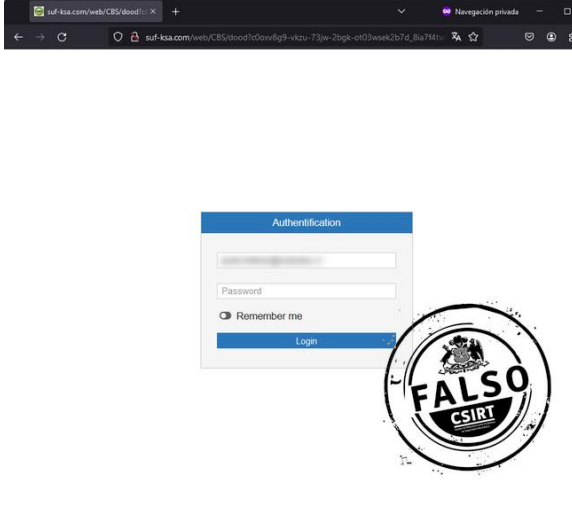
### Enlace para revisar IoC:

<https://csirt.gob.cl/alertas/cmv24-00466/>

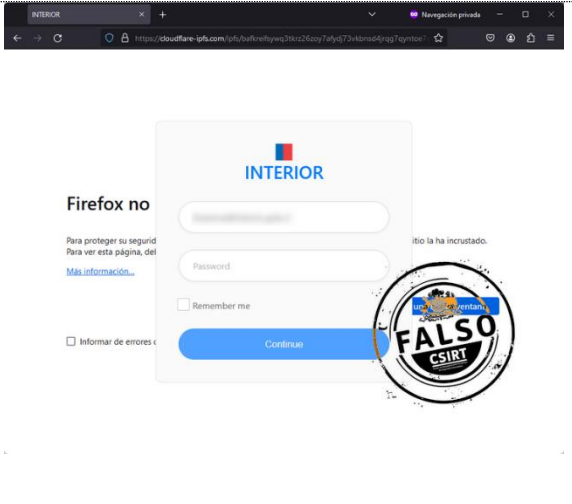
## CONTACTO Y REDES SOCIALES CSIRT

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

## 2. Phishing







Falso email llamando a cambiar contraseña - Phishing	
Alerta de seguridad cibernética	FPH24-00960
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2024
Última revisión	27 de mayo de 2024
<b>Indicadores de compromiso</b>	
<b>URL redirección</b>	
<a href="http://suf-ksa.com/web/CBS/index.php?email={Correoelectronico}">http://suf-ksa.com/web/CBS/index.php?email={Correoelectronico}</a>	
<b>URL del sitio falso</b>	
<a href="http://suf-ksa.com/web/CBS/dood?">http://suf-ksa.com/web/CBS/dood?</a>	
<b>Dirección IP sitio falso</b>	
[162.215.249.101]	
<b>Enlace para revisar loC:</b>	
<a href="https://csirt.gob.cl/alertas/fph24-00960/">https://csirt.gob.cl/alertas/fph24-00960/</a>	



Ministerio del Interior y Seguridad Pública - Phishing	
Alerta de seguridad cibernética	FPH24-00961
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de mayo de 2024
Última revisión	28 de mayo de 2024
<b>Indicadores de compromiso</b>	
<b>URL del sitio falso</b>	
<a href="https://cloudflare-ipfs.com/ipfs/bafkreifsywq3tkrz26zoy7afydj73vkbnsd4jrqg7qyntoe7m4xibpdvyy?filename=Login-INBOX%2520%25281%2529last.html#{Correoelectronico}">https://cloudflare-ipfs.com/ipfs/bafkreifsywq3tkrz26zoy7afydj73vkbnsd4jrqg7qyntoe7m4xibpdvyy?filename=Login-INBOX%2520%25281%2529last.html#{Correoelectronico}</a>	
<b>Dirección IP sitio falso</b>	
[45.137.22.144]	
<b>Enlace para revisar loC:</b>	
<a href="https://csirt.gob.cl/alertas/fph24-00961/">https://csirt.gob.cl/alertas/fph24-00961/</a>	


### CONTACTO Y REDES SOCIALES CSIRT

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

# Boletín de Ciberseguridad N° 256

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

BOLETÍN 13BCS24-00265-01 | Semana del 24 al 30 de mayo de 2024

<p>Atención</p> <p>ADMINISTRADOR DE SISTEMA &lt;postemergencia&gt; Para [Redacted] <span>Responder</span> <span>Responder a todos</span> <span>Reenviar</span> <span>...</span> martes 28-05-2024 4:55</p> <p>Su correo electrónico ha excedido el límite de almacenamiento establecido por el administrador y no puede enviar ni recibir mensajes nuevos hasta que valide su correo electrónico</p> <p>Para validar su correo electrónico haga clic <a href="#">aquí</a></p> <p>Administrador de sistema</p> 	<h3>Ministerio del Interior y Seguridad Pública - Phishing</h3> <table border="1"><tr><td>Alerta de seguridad cibernética</td><td>FPH24-00962</td></tr><tr><td>Clase de alerta</td><td>Fraude</td></tr><tr><td>Tipo de incidente</td><td>Phishing</td></tr><tr><td>Nivel de riesgo</td><td>Alto</td></tr><tr><td>TLP</td><td>Blanco</td></tr><tr><td>Fecha de lanzamiento original</td><td>28 de mayo de 2024</td></tr><tr><td>Última revisión</td><td>28 de mayo de 2024</td></tr></table> <p><b>Indicadores de compromiso</b></p> <p><b>URL del sitio falso</b> <a href="https://msellagolan001.wixsite.com/validar">https://msellagolan001.wixsite.com/validar</a></p> <p><b>Dirección IP sitio falso</b> [34.117.60.144]</p> <p><b>Enlace para revisar IoC:</b> <a href="https://csirt.gob.cl/alertas/fph24-00962/">https://csirt.gob.cl/alertas/fph24-00962/</a></p>	Alerta de seguridad cibernética	FPH24-00962	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	28 de mayo de 2024	Última revisión	28 de mayo de 2024
Alerta de seguridad cibernética	FPH24-00962														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	28 de mayo de 2024														
Última revisión	28 de mayo de 2024														

## CONTACTO Y REDES SOCIALES CSIRT

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

## 3. Vulnerabilidades



VSA24-01022  
**Alerta de Vulnerabilidades**  
 Check Point Remote Access VPN

CSIRT



Detalles e informe en <https://csirt.gob.cl/alertas>

Check Point Remote Access VPN y otros - Vulnerabilidades		
Código de alerta	VSA24-01022	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	30 de mayo de 2024	
Última revisión	30 de mayo de 2024	
CVE y puntaje CVSS y EPSS al momento de la publicación		
CVE-2024-24919	7.5	1.85%
Fabricante		
Check Point		
Productos afectados		
Check Point Remote Access VPN		
R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20		
Quantum Security Gateway		
R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20		
CloudGuard Network Security		
R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20		
Quantum Maestro		
R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20		
Quantum Scalable Chassis		
R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20		
Quantum Spark Gateways		
R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20		
Enlaces para revisar el informe:		
<a href="https://csirt.gob.cl/alertas/vsa24-01022/">https://csirt.gob.cl/alertas/vsa24-01022/</a>		





### CONTACTO Y REDES SOCIALES CSIRT



## 4. Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar que los sitios web a los que se ingrese sean los oficiales.

### CONTACTO Y REDES SOCIALES CSIRT

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




## 5. Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (<https://www.csirt.gob.cl> o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Jimmy Ávila
- María José Fuentes Urrutia
- Alejandro Cuzmar
- Natalia Valeska Hace Hernández
- Miguel Becerra
- Kevin Andrés Douglas Riquelme
- Monitoreo Universidad de Chile

### CONTACTO Y REDES SOCIALES CSIRT

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